ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΤΜΗΜΑ ΔΙΔΑΚΤΙΚΗΣ ΤΗΣ ΤΕΧΝΟΛΟΓΙΑΣ ΚΑΙ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΚΑΤΕΥΘΥΝΣΗ : "ΨΗΦΙΑΚΕΣ ΕΠΙΚΟΙΝΩΝΙΕΣ & ΔΙΚΤΥΑ"

UNIVERSITY OF PIRAEUS

DEPARTMENT OF TECHNOLOGY EDUCATION AND DIGITAL SYSTEMS

POSTGRADUATE PROGRAM
COURSE: "DIGITAL COMMUNICATIONS & NETWORKS"

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Θέμα: ***Ασφάλεια δικτύων υποδομών οπτικών ινών***

Σπουδαστής: ***Κουρούκλης Ευάγγελος*** ***ΑΜ: ΜΕ/0540***

Επιβλέπων: ***Κάτσικας Σωκράτης***
Καθηγητής Πανεπιστημίου Πειραιώς

ΠΕΙΡΑΙΑΣ
- 2008 -

Πρόλογος

Η παρούσα διπλωματική εργασία εκπονήθηκε στα πλαίσια του Προγράμματος Μεταπτυχιακών Σπουδών του τμήματος Διδακτικής της Τεχνολογίας και Ψηφιακών συστημάτων του Πανεπιστημίου Πειραιώς (Κατεύθυνση Ψηφιακές Επικοινωνίες και Δίκτυα), σε συνεργασία με τον Καθηγητή του τμήματος κ. Κάτσικα Σωκράτη. Το αντικείμενο ουσιαστικά εμπίπτει στην ευρύτερη περιοχή της ασφάλειας Τηλεπικοινωνιών και Δικτύων και εξειδικεύεται σε ζητήματα ασφάλειας δικτύων με υποδομές οπτικών ινών.

Ευάγγελος Π. Κουρούκλης

Περιεχόμενα

Εισαγωγή

Το πλέον τεχνολογικά προηγμένο ενσύρματο μέσο μετάδοσης είναι τα καλώδια οπτικών ινών. Τα καλώδια οπτικών ινών χρησιμοποιούνται σήμερα, σαν μέσο μετάδοσης πληροφοριών, σε όλα τα σύγχρονα τηλεπικοινωνιακά συστήματα και στα τοπικά δίκτυα υπολογιστών μεγάλων επιχειρήσεων ή εκπαιδευτικών και νοσηλευτικών ιδρυμάτων, λόγω του ότι επιτυγχάνουν πολύ μεγάλο ρυθμό μετάδοσης πληροφοριών.

Τα συστήματα τηλεπικοινωνιών με υποδομές οπτικών ινών αποτελούν τη σπονδυλική στήλη όλων των σύγχρονων δικτύων επικοινωνιών. Είτε πρόκειται για φωνή, δεδομένα, βίντεο, fax, ραδιόφωνο, ηλεκτρονικό ταχυδρομείο, TV, πάνω από 180 εκατομμύρια μίλια καλωδίων οπτικών ινών μεταφέρουν παγκοσμίως την, συνεχώς αυξανόμενη, πλειοψηφία των πληροφοριών και επικοινωνιών μας. Οι σύγχρονες κοινωνίες και οικονομίες στηρίζονται στη διαθεσιμότητα, την εμπιστευτικότητα και την ακεραιότητα των εν λόγω υποδομών. Η ασφάλεια των δικτύων με υποδομές οπτικών ινών είναι συχνά αντικείμενο υποτιμημένο.

Ο κυρίως σκοπός της παρούσας εργασίας είναι η μελέτη ασφάλειας των δικτύων των οποίων οι υποδομές βασίζονται σε καλώδια οπτικών ινών. Τα δίκτυα αυτά έχουν αδυναμίες ασφάλειας, είτε πρόκειται για IP δίκτυα και το πρόβλημα που παρουσιάζεται είναι η φυσική πρόσβαση στο μέσο, κάτι που σήμερα θεωρείτε μια απλή διαδικασία, είτε για δίκτυα καναλιού οπτικών ινών, όπου πρόκειται για ένα πρωτόκολλο με παρόμοιες αδυναμίες με αυτές του IP πρωτοκόλλου στα επιμέρους στρώματά του.

Η εργασία διαιρείται σε πέντε κεφάλαια. Στο πρώτο κεφάλαιο αναλύονται θέματα της τεχνολογίας μετάδοσης πληροφοριών μέσω οπτικών ινών, καθώς και θέματα ασφάλειας του φυσικού στρώματος των δικτύων με υποδομές οπτικών ινών. Παρουσιάζονται οι κίνδυνοι και οι μέθοδοι υποκλοπής οπτικών σημάτων, καθώς και οι λύσεις ασφάλειας που προσφέρονται. Στα επόμενα τρία κεφάλαια περιγράφονται έννοιες και αναλύονται οι κίνδυνοι επιθέσεων, στα ανώτερα από το φυσικό στρώματα, δικτύων, τα οποία χρησιμοποιούν για πρωτόκολλο επικοινωνίας μία gigabit-speed τεχνολογία, το κανάλι οπτικών ινών Fiber channel. Τέλος, στο πέμπτο κεφάλαιο παρουσιάζονται λύσεις των προβλημάτων ασφαλείας των δικτύων καναλιού οπτικών ινών όπως αυτές διαμορφώνονται έως και σήμερα.

1ο Κεφάλαιο

1.1. Οπτικές Ίνες

Το μεγάλο κέρδος από τη χρησιμοποίηση των καλωδίων οπτικών ινών είναι ότι ο φορέας μετάδοσης της πληροφορίας είναι το φως και όχι κάποιο ηλεκτρικό σήμα. Αυτό έχει σαν αποτέλεσμα να μπορεί να μεταδοθεί τεράστιος όγκος πληροφοριών με υψηλότατους ρυθμούς μετάδοση χωρίς απώλειες.

1.1.1. Πλεονεκτήματα και μειονεκτήματα οπτικών ινών

Τα καλώδια οπτικών ινών σε σχέση με τα άλλα μέσα μετάδοσης πληροφοριών, όπως είναι τα συνεστραμμένα καλώδια από χαλκό, παρουσιάζουν πολλά πλεονεκτήματα. Μερικά από αυτά είναι:

- Έχουν μεγάλο εύρος ζωής συχνοτήτων που έχει σαν αποτέλεσμα την επίτευξη υψηλών ρυθμών μετάδοσης πληροφοριών.
- Είναι ανεπηρέαστα από θόρυβο ο οποίος δημιουργείται από ηλεκτρικά και μαγνητικά πεδία.
- Ο ρυθμός εμφάνισης σφαλμάτων (error rate) είναι σε χαμηλά επίπεδα.
- Το υλικό κατασκευής τους απαιτεί πολύ μικρές διαστάσεις και ελάχιστο βάρος.
- Είναι πιο ασφαλές μέσο μετάδοσης πληροφοριών και με αυτό τον τρόπο εξασφαλίζουν προστασία των δεδομένων από υποκλοπή ή παρεμβολή.

Στα μειονεκτήματα των οπτικών ινών καταλογίζονται κύρια το υψηλό κόστος τους αλλά και οι δύσκολοι τρόποι σύνδεσης (βυσμάτωσης), προσαρμογής και ευθυγράμμισης της κάθε οπτικής ίνας, ούτως ώστε το φως σαν φορέας μετάδοσης της πληροφορίας να μην αποκλίνει, γιατί ακόμα και πολύ μικρές αποκλίσεις των βυσμάτων σύνδεσης προξενούν διασπορά και απώλεια του σήματος.

Ακόμα παρουσιάζουν πολύ μεγάλη ευαισθησία σε μηχανικές καταπονήσεις. Η διαδικασία εγκατάστασής τους απαιτεί μεγάλη εξειδίκευση και ειδικό εξοπλισμό. Επίσης, βασικό μειονέκτημα είναι η δυσκολία σύνδεσης πολλών χρηστών καθώς και η δυσκολία διαχωρισμού ενός ζεύγους ινών από ένα καλώδιο πολλών ινών, γεγονός που τις καθιστά κατάλληλες κυρίως για συνδέσεις σημείου προς σημείο. Αυτό γίνεται διότι απαιτείται υψηλή προσαρμογή και ευθυγράμμιση της φωτεινής πηγής, για να μην υπάρχει διασπορά και να ελαχιστοποιηθούν οι απώλειες. Όμως η πρόοδος της τεχνολογίας, που έχει σημειωθεί τα τελευταία χρόνια στην περιοχή των οπτικών ινών, αντιμετώπισε με επιτυχία την παραπάνω δυσκολία , με αποτέλεσμα να είναι δυνατή η χρήση τους και για συνδέσεις σημείου προς πολλά σημεία. Παρόλα αυτά, η χρήση τους σε τέτοιες συνδέσεις δεν έχει ακόμα ευρέως εξαπλωθεί, ιδιαίτερα λόγω του αυξημένου κόστους, που παρουσιάζουν τέτοια συστήματα. Αποτέλεσμα αυτού είναι, τα καλώδια οπτικών ινών στην Ελλάδα να χρησιμοποιούνται σχεδόν αποκλειστικά για την υλοποίηση του τμήματος κορμού μεγάλων δικτύων και στην οριζόντια καλωδίωση όπου το απαιτούν ειδικές εφαρμογές, όπως είναι η επίτευξη μεγάλων ταχυτήτων για μεταδόσεις πληροφοριών με υψηλές απαιτήσεις ασφάλειας (Εθνική Υπηρεσία Πληροφοριών, στρατιωτικές εφαρμογές, δίκτυα αποθήκευσης δεδομένων κ.τ.λ.)

1.1.2. Βασικές αρχές οπτικών ινών

Η βασική αρχή λειτουργίας των οπτικών ινών στηρίζεται στη μετάδοση παλμών μονοχρωματικού φωτός (φως μιας συχνότητας) μέσα από μια γυάλινη ή πλαστική ίνα. Εδώ, η οπτική ίνα χρησιμοποιείται ως μέσο μετάδοσης (αντί π.χ. του χάλκινου σύρματος) και το φως σαν φορέας της πληροφορίας αντί για το ρεύμα ή την τάση που χρησιμοποιούμε στα ενσύρματα μέσα. Οι οπτικές ίνες κατασκευάζονται από λεπτές ίνες καθαρού γυαλιού ή διάφανου πλαστικού με υψηλή τιμή δείκτη διάθλασης, που έχουν τη ιδιότητα να “εγκλωβίζουν” και να “οδηγούν” τις ακτίνες φωτός. Οι ίνες αυτές, που αποτελούν τον πυρήνα της οπτικής ίνας, περιβάλλονται από μια επίστρωση (cladding) και ένα προστατευτικό κάλυμμα. Η φωτεινή δέσμη η οποία μεταφέρει την πληροφορία, εισάγεται από τη μία άκρη του πυρήνα της οπτικής ίνας και οδεύει με διαδοχικές ανακλάσεις στα τοιχώματα της ίνας προς την άλλη

άκρη, εγκλωβισμένη μέσα στον πυρήνα τής οπτικής ίνας με ελάχιστες απώλειες, ακόμα και στην περίπτωση που η οπτική ίνα καμπυλωθεί. Αυτή η μετάδοση της φωτεινής δέσμης στηρίζεται στην αρχή της ολικής εσωτερικής ανάκλασης. Βασική προϋπόθεση για να συμβεί ολική ανάκλαση είναι, πρώτον ο δείκτης διάθλασης του εξωτερικού υλικού (επίστρωση) να είναι μικρότερος από το δείκτη διάθλασης του εσωτερικού υλικού (πυρήνας) και δεύτερον η γωνία πρόσπτωσης της ακτίνας στο εσωτερικό υλικό να είναι μεγαλύτερη από κάποια τιμή που λέγεται "ορική" γωνία, τότε, η φωτεινή δέσμη εγκλωβίζεται και ταξιδεύει σε μεγάλες αποστάσεις με χιλιάδες εσωτερικές ανακλάσεις. Οι οπτικές ίνες διακρίνονται σε δύο κατηγορίες, ανάλογα με την πορεία που ακολουθούν οι δέσμες φωτός μέσα στον πυρήνα. Έτσι έχουμε τις μονότροπες ή ενιαίας τροχιάς και τις πολύτροπες ή πολλαπλής τροχιάς οπτικές ίνες. Οι μονότροπες οπτικές ίνες πλεονεκτούν έναντι των πολύτροπων οπτικών ινών, γιατί οι δέσμες φωτός ακολουθούν μια μοναδική τροχιά(κατά μήκος του άξονα του πυρήνα) και έτσι επιτυγχάνουν μεγαλύτερους ρυθμούς μετάδοσης δεδομένων (υψηλότερες ταχύτητες) και επιφέρουν μικρότερη εξασθένηση σήματος. Από αυτή την κατηγορία οπτικών ινών χρησιμοποιούμε περισσότερο αυτές που έχουν πυρήνα με διάμετρο 9μm και επίστρωση με διάμετρο 125 μm (OS1). Από τις πολύτροπές οπτικές ίνες χρησιμοποιούνται περισσότερο αυτές που έχουν πυρήνα με διάμετρο 62,5μm και επίστρωση με διάμετρο 125 μm (OM1), ενώ έχει αρχίσει και η χρήση του τύπου OM3 50/125μm ο οποίος επιτυγχάνει ταχύτητα 10Gbs.

Η χρησιμοποίηση καλωδίων οπτικών ινών διασφαλίζει:

- Μεγάλο εύρος περιοχής διερχομένων συχνοτήτων (bandwidth) άρα αντίστοιχα μεγάλη ικανότητα στην μετάδοση ψηφιακών δεδομένων data με πολύ υψηλούς ρυθμούς (ταχύτητα).
- Προστασία από ηλεκτρομαγνητικές παρεμβολές οι οποίες μπορεί είτε να υποβαθμίσουν την ποιότητα του μεταδιδόμενου σήματος με προσθήκη θορύβου είτε να προκαλέσουν εκτεταμένες φυσικές βλάβες στον εξοπλισμό λόγω υπερτάσεων, π.χ. λόγω πτώσεως κεραυνού.
- Μικρή απόσβεση σήματος (ATTENUATION)
- Εξαφάνιση του φαινόμενου της παραδιαφωνίας (NEXT).
- Μικρότερο μέγεθος (βάρος και όγκος) καλωδίων.

Γενικά η οπτική ίνα αποτελείται από τρία μέρη:

- Core - Πυρήνας
- Cladding - Περίβλημα ή επένδυση πυρήνος
- Coating - Προστατευτική επικάλυψη

Το κεντρικό τμήμα, ο πυρήνας, είναι το μέσον στο οποίο διαδίδεται το φως. Ο πυρήνας αποτελείται από εμπλουτισμένο με γερμάνιο πυρίτιο (doped silica) για να του προσδώσει μεγαλύτερο δείκτη διαθλάσεως (n=1,48). Το Cladding, που περιβάλλει τον πυρήνα, αποτελείται από καθαρό πυρίτιο και έχει χαμηλότερο δείκτη διαθλάσεως από τον πυρήνα (n=1,46). Αυτή η διαφορά στον δείκτη διαθλάσεως του συστήματος core / cladding υποχρεώνει την όδευση του φωτός εντός του πυρήνα κατά μήκος του καλωδίου. Επειδή η διαχωριστική επιφάνεια μεταξύ των δύο μέσων είναι τελείως λεία και έχει μεγαλύτερο δείκτη διαθλάσεως προς την μέσα πλευρά (προς τον πυρήνα), προκαλείται ολική ανάκλαση του φωτός και στρέφει τις ακτίνες του φωτός που πέφτουν επάνω της από την περιφέρεια του πυρήνα και πάλι προς το εσωτερικό του πυρήνα. Το εξωτερικό περίβλημα – coating αποτελείται από δύο στρώσεις ακρυλικού υλικού και είναι η προστατευτική επικάλυψη της ίνας στην φάση της κατεργασίας της για την κατασκευή των καλωδίων οπτικών ινών καθώς επίσης και στην φάση της εγκαταστάσεως του δικτύου, τερματισμού, ενώσεων κλπ.

1.1.3. Γενικές προδιαγραφές καλωδίων οπτικών ινών

Τα καλώδια οπτικών ινών που χρησιμοποιούνται πρέπει να υποστηρίζουν πρωτόκολλα και ταχύτητες δεδομένων τουλάχιστον Gigabit Ethernet έως και 10 Gigabit Ethernet και να είναι συμβατά με πηγές vertical cavity surface emitting laser (VCSEL). Ανάλογα με τις αποστάσεις, σύμφωνα με τα πρότυπα χρησιμοποιούνται:

- Για αποστάσεις έως και 550 μέτρα για Gigabit Ethernet πολύτροπο καλώδιο τύπου 62,5/125.
- Για τις εισαγωγές του ΟΤΕ μονότροπο καλώδιο τύπου 9/125 για Gigabit Ethernet (αποστάσεις έως 5000 μέτρα πλήρους link)

- Στα 300 μέτρα, για εφαρμογές 10 Gigabit Ethernet για λειτουργία στο παράθυρο 850 nm χρησιμοποιούνται οπτικά καλώδια, αντίστοιχα υλικά τερματισμού και οπτικά patch cords τύπου 50/125 OM3.

Μηχανικά χαρακτηριστικά:

Mean Numerical Aperture:	0,20
Min Bandwidth at 1300 nm :	1200 MHz/Km / 1500 MHz/Km OM3
Min Bandwidth at 850 nm :	500 MHz/Km
Max Attenuation at 850 nm :	2,7 dB/Km
Max Attenuation at 1300 nm :	0,7 dB/Km
Crush resistance:	250 N/cm
Maximum Pulling Force:	1000 N
Tube:	PBT polyester
Fire behaviour:	IEC 60332-1

Επιπλέον χαρακτηριστικά:

- Ιδιαίτερα εύκαμπτη κατασκευή με ελάχιστη ακτίνα καμπυλότητας κατά την εγκατάσταση, 50mm ή μικρότερη.
- Τύπου LSZH (low smoke zero halogen) σύμφωνα με το πρότυπο IEC 61034 (low smoke) και IEC-60754-1&2 (halogen free) καθώς επίσης και τύπου Flame Retardant με βάση τα πρότυπα IEC 60332-1&3 έτσι ώστε να αποφευχθούν εκπομπές καπνού και τοξικών ουσιών σε περίπτωση πυρκαγιάς.
- Μεγάλο θερμοκρασιακό εύρος λειτουργίας, τουλάχιστον -5ºC έως και +55ºC
- Να μη χρησιμοποιούνται μεταλλικά στοιχεία σε κανένα σημείο της κατασκευής του καλωδίου (πλήρως διηλεκτρική κατασκευή).
- Το χρώμα του εξωτερικού μανδύα των καλωδίων να είναι ιδιαίτερο (π.χ. όχι μαύρο, άσπρο ή γκρι), έτσι ώστε να ξεχωρίζει από τα υπόλοιπα ηλεκτρολογικά καλώδια και καλώδια ασθενών ρευμάτων.
- Τα καλώδια οπτικών ινών θα πρέπει οπωσδήποτε να έχουν κατασκευαστεί σε εργοστάσιο πιστοποιημένο κατά ISO 9000 ή 9001 ή 9002 ή νεότερο.

Το σύνολο του εξοπλισμού θα πρέπει να είναι πλήρως συμβατό με όλες τις υφιστάμενες απαιτήσεις λειτουργίας, απόδοσης και ταχύτητας όλων των γνωστών δικτυακών πρωτοκόλλων – προτύπων συμπεριλαμβανομένων και των IEEE802.3u και IEEE802.3z (Gigabit Ethernet).

1.2. Ασφάλεια φυσικού στρώματος δικτύων οπτικών ινών

Με την εισαγωγή των τηλεπικοινωνιακών συστημάτων οπτικών ινών υπήρχε η πεποίθηση ότι μεταδόσεις με την ίνα ως μέσο είναι εγγενώς ασφαλείς. Από τότε έχει αποδειχθεί ότι τα συστήματα οπτικών ινών είναι εύκολο να απομαστευτούν. Στην πραγματικότητα, πολλές τεχνικές απομάστευσης οπτικών ινών χρησιμοποιούν τυποποιημένο εξοπλισμό συντήρησης δικτύων που χρησιμοποιείται από τους παρόχους παγκοσμίως. Χρησιμοποιημένες παρανόμως, εντούτοις, τέτοιες συσκευές επιτρέπουν την υποκλοπή μεταδόσεων φωνής και δεδομένων εγκαταστάσεων με υποδομές οπτικών ινών.

Αυτό επιτυγχάνεται επειδή το φως, μέσα στο καλώδιο, περιέχει όλες τις πληροφορίες στο διαβιβασθέν σήμα και μπορεί εύκολα να αποσπαστεί, ερμηνευθεί και χρησιμοποιηθεί με τον τυποποιημένο off-the-shelf εξοπλισμό. Τα ιδιωτικά και δημόσια δίκτυα σήμερα δεν ενσωματώνουν μεθόδους για ανίχνευση οπτικών απομαστευτών σε πραγματικό χρόνο, πράγμα που προσφέρει σε έναν εισβολέα μια σχετικά ασφαλή υποκλοπή δεδομένων. Δεδομένου ότι τα συστήματα οπτικών ινών διαβιβάζουν μεγάλους όγκους δεδομένων, ως φως μέσα σε μια οπτική ίνα, τέτοιες μέθοδοι είναι χαμηλού κινδύνου μέθοδοι συλλογής μεγάλου όγκου πληροφοριών. Από πλευράς υποκλοπής και κατασκοπείας τα οφέλη είναι προφανή.

1.2.1. Εταιρική κατασκοπεία

Σήμερα ζούμε σε μια κοινωνία όπου η εταιρική κατασκοπεία έχει γίνει άθλημα. Δεδομένου ότι τα συστήματα επικοινωνιών που χρησιμοποιούν οπτικές ίνες γίνονται όλο και περισσότερο διαδεδομένα, τόσο δίνεται η δυνατότητα για παράνομη απομάστευση και κλοπή εμπιστευτικών και εμπορικά ευαίσθητων δεδομένων.

Υπολογίζεται ότι πάνω από $100 δισεκατομμύρια χάθηκαν από Αμερικάνικες επιχειρήσεις μόνο το 2000 λόγω των εταιρικών δραστηριοτήτων κατασκοπείας, ενώ $20 δισεκατομμύρια χάθηκαν μέσω των καθαρά τεχνικών μέσων. Διεθνώς πάνω από 100 ξένα κυβερνητικά πρακτορεία λαμβάνουν και παρέχουν ευαίσθητες πληροφορίες στις εσωτερικές εταιρίες τους. Σε μία έρευνα του Ομοσπονδιακού Γραφείου Ερευνών (FBI) και του Ιδρύματος Ηλεκτρονικού Εγκλήματος οι σημαντικές Αμερικανικές επιχειρήσεις και οργανώσεις δήλωσαν ότι η πλέον πιθανή πηγή επίθεσής τους ήταν από τις συνδυασμένες δραστηριότητες κατασκοπείας που προέρχονται από Αμερικάνους ανταγωνιστές, ξένες εταιρίες και ξένες κυβερνήσεις. Ανεξάρτητοι χάκερ και δυσαρεστημένοι υπάλληλοι, ενώ πάντα είναι κίνδυνοι που πρέπει να προσεχθούν, ταξινομούνται ως δευτερεύουσες απειλές, πίσω από τις συνδυασμένες απειλές κατασκοπείας.

Πρόσφατα παραδείγματα περιλαμβάνουν την υποκλοπή τηλεφωνικών κλήσεων του Έλληνα πρωθυπουργού, των μελών Υπουργικού Συμβουλίου, και 100 άλλων αριθμών, συμπεριλαμβανομένων μερικών από την Αμερικανική πρεσβεία στην Αθήνα, τις γαλλικές απομαστεύσεις στα βρετανικά ασύρματα δίκτυα για υποκλοπή συνομιλιών στελεχών σε δημοπρασίες, απομαστεύσεις εγκληματιών στα δίκτυα της ολλανδικής αστυνομίας, οπτικές απομαστεύσεις που τοποθετήθηκαν από την πρώην ανατολικογερμανική μυστική αστυνομία (STASI) στις οπτικές συνδέσεις μεταξύ του Δυτικού Βερολίνου και Δυτικής Γερμανίας και ακόμη και το πρόσφατο χτύπημα των οπτικών γραμμών ενός σημαντικού με έδρα τη Βοστόνη οικονομικού οργάνου.

1.2.2. Optical tapping

Οι οπτικές συσκευές απομάστευσης όταν τοποθετούνται σε δημόσια και ιδιωτικά οπτικά δίκτυα επιτρέπουν την αδέσμευτη πρόσβαση σε όλη την πληροφορία που διέρχεται οποιοδήποτε τμήμα του δικτύου. Διαθέσιμες νόμιμα και ανέξοδα από τους πολυάριθμους κατασκευαστές οι οπτικές συσκευές απομάστευσης είναι τυποποιημένος εξοπλισμός συντήρησης δικτύων που χρησιμοποιείται σε καθημερινή βάση. Όταν χρησιμοποιούνται κακόβουλα, παρέχουν μια άριστη μέθοδο υποκλοπής των μεταδόσεων φωνής και δεδομένων με μικρή πιθανότητα ανίχνευσης. Οι εισβολείς επομένως ανταμείβονται γενναιόδωρα με μεγάλο όγκο πληροφορίας ενώ

διατρέχουν χαμηλό κίνδυνο σύλληψης. Οι κατασκευαστές οπτικού εξοπλισμού δικτύων δεν ενσωματώνουν αυτήν την περίοδο επαρκείς τεχνολογίες προστασίας και ανίχνευσης στις πλατφόρμες τους για να ελέγξουν τέτοιες παραβιάσεις δικτύων σε πραγματικό χρόνο. Οι φορείς εκμετάλλευσης δικτύου δεν μπορούν έτσι να προστατεύσουν τα οπτικά σήματα στα δίκτυά τους και επομένως δεν μπορούν να αποτρέψουν την έκθεση των ευαίσθητων δεδομένων τους. Τα κυβερνητικά δίκτυα, ενώ θεωρούνται ασφαλέστερα, είναι επίσης τρωτά, όπως προαναφέραμε, σε ορισμένους τύπους προηγμένων παθητικών και ενεργών μεθόδων υποκλοπής.

Γεγονός είναι ότι η μεγάλη πλειοψηφία των οπτικών συσκευών απομάστευσης εμμένει απολύτως μη ανιχνεύσιμη, δεδομένου ότι οι πάροχοι και οι περισσότερες επιχειρήσεις σήμερα δεν υιοθετούν επαρκείς τεχνικές ελέγχου και ανίχνευσης ώστε να προστατεύσουν τα δεδομένα των οπτικών δικτύων τους. Σαφώς σε ένα τέτοιο περιβάλλον, τα δίκτυα οπτικών ινών, που είναι η καρδιά όλων των επικοινωνιών και μεταφοράς δεδομένων στη σύγχρονη κοινωνία, είναι πραγματικοί στόχοι επιθέσεων.

Παραδοσιακά οι κακόβουλες παραβιάσεις πληροφοριακών συστημάτων γίνονταν με απομάστευση ή με υποκλοπή ραδιομεταδόσεων. Τα τελευταία χρόνια, εντούτοις, ο γενικός πληθυσμός έχει στραφεί στο hacking υπολογιστών. Οι χάκερ έχουν διαφόρους στόχους αλλά βασικά τείνουν να επιθυμούν την γνωστοποίηση, της επιτυχούς παρείσφρησής τους, στο κοινό. Τέτοιες υψηλού προφίλ επιθέσεις, όπως οι επιθέσεις άρνησης υπηρεσιών ή ο ιός «I Love You», προσελκύουν πολύ την προσοχή των μέσων. Ενώ η επιθέσεις αυτές έχουν οικονομικό αντίκτυπο για τα θύματα τους, ωχριούν σε σύγκριση με τις τεράστιες απώλειες δεδομένων που μπορούν να προέλθουν από τις μη ανιχνευθείς απομαστεύσεις οπτικών ινών που μπορούν να παραμείνουν σε ισχύ για εκτεταμένες χρονικές περιόδους και να παρέχουν πρόσβαση, σε μία κακόβουλη οντότητα, στο δίκτυο μιας εταιρίας μεταξύ των κτιρίων της, μιας πανεπιστημιούπολης ή μιας ολόκληρης περιοχής. Οι επαγγελματίες επιθυμούν να εξαγάγουν πληροφορίες για όσο το δυνατό περισσότερο χρόνο για ένα συγκεκριμένο οικονομικό ή πολιτικό κέρδος και με στόχο τη μη ανίχνευση ή σύλληψή τους. Οι συσκευές απομάστευσης οπτικών ινών αποτελούν μια πολύ χρήσιμη μέθοδο στο οπλοστάσιό τους, των παράνομων εργαλείων συλλογής πληροφοριών.

Κατά συνέπεια, αντίθετα προς τη κοινή πεποίθηση, τα συστήματα τηλεπικοινωνιών οπτικών ινών είναι εξαιρετικά τρωτά και λίγοι ιδιωτικοί ή δημόσιοι φορείς εκμετάλλευσης δικτύου μπορούν να υποστηρίξουν ότι τα δίκτυά τους είναι προστατευμένα ακόμα και κατ' ελάχιστο από μεθόδους οπτικής απομάστευσης.

1.2.3. Μέθοδοι απομάστευσης δικτύων οπτικών ινών

Τα σύγχρονα δίκτυα ινών αποτελούνται από περισσότερα των 180 εκατομμύριων μιλίων οπτικής ίνας παγκοσμίως. Αυτά τα δίκτυα επιτρέπουν τη διαβίβαση στοιχείων μεγάλων όγκων δεδομένων από σημείο σε σημείο φτηνά και εύκολα, και φέρουν εξαιρετικά σημαντικές και εμπιστευτικές πληροφορίες. Αν και αρχικά θεωρήθηκε ότι αυτά τα συστήματα οπτικών ινών θα ήταν ασφαλή, έχει ανακαλυφθεί ότι η εξαγωγή πληροφοριών από τις οπτικές ίνες είναι σχετικά απλή και υποβοηθούμενη από την αυξανόμενη βελτίωση και διαθεσιμότητα τυποποιημένου εξοπλισμού. Υπάρχουν διάφορες μέθοδοι απομάστευσης οπτικών ινών, αλλά οι περισσότερες εκπίπτουν στις ακόλουθες κύριες κατηγορίες:

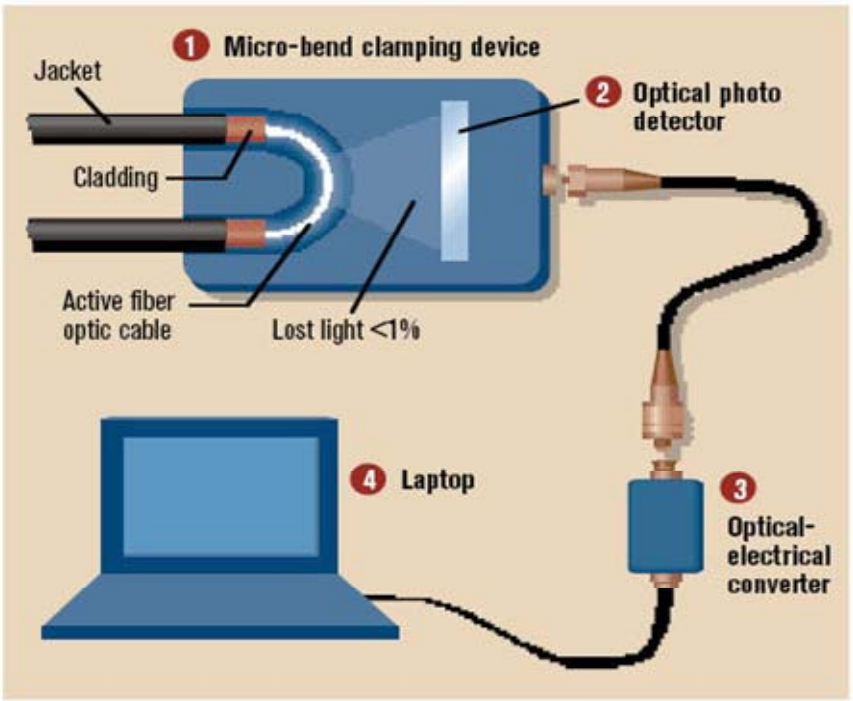
- Συνένωση
- Διαμέριση ή Σύζευξη
- Εξ αποστάσεως

1.2.3.1. Συνένωση οπτικών ινών

Η απλούστερη μέθοδος απομάστευσης είναι με την συνένωση οπτικών ινών και την παρεμβολή εξοπλισμού που επιτρέπει στο σήμα να μεταδοθεί στο ορθά συμβαλλόμενο μέρος αφού πρώτα υποκλαπεί από την κακόβουλη οντότητα. Οι οπτικές συναρμογές προκαλούν ένα στιγμιαίο σφάλμα στη μετάδοση ενώ η ίνα δεν είναι λειτουργική για πολύ μικρό χρονικό διάστημα. Οι πάροχοι, εντούτοις, δεν έχουν τη δυνατότητα να εντοπίσουν σε πραγματικό χρόνο τις διακοπές οπτικών ινών και πρέπει έπειτα συνήθως να στείλουν φορτηγά, τεχνικούς και να παρεμβάλουν πρόσθετο εξωτερικό εξοπλισμό. Κατά συνέπεια, εάν ο χρόνος διακοπής είναι σύντομος, πολλοί χειριστές θα αποδώσουν τη διαταραχή σε μια δυσλειτουργία του δικτύου και θα επιτρέψουν τη διέλευση δεδομένων, χωρίς να γνωρίζουν ότι έχει τοποθετηθεί κάποιος μηχανισμός απομάστευσης. Ο off-the-shelf εξοπλισμός απομάστευσης σήμερα δεν διακόπτει το σήμα και έτσι η μέθοδος αυτή δεν προτιμάται.

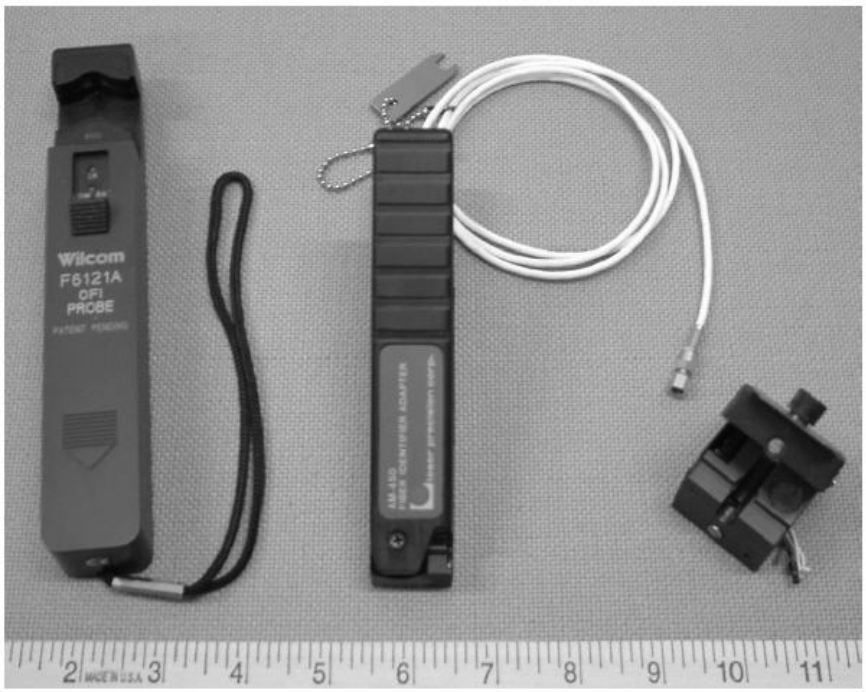
1.2.3.2. Διαμέριση και Σύζευξη οπτικών ινών

Αυτές οι μέθοδοι επιτρέπουν την υποκλοπή σήματος από μία οπτική ίνα χωρίς πραγματικά να σπάσουν την ίνα ή να αναστατώσουν τη ροή των δεδομένων. Μια από τις λιγότερο γνωστές ιδιότητες των οπτικών ινών είναι ότι το φως χάνεται εύκολα και από το jacket και από το cladding της ίνας, ιδιαίτερα εάν η ίνα κάμπτεται ή στερεώνεται κατά τέτοιο τρόπο ώστε να διαμορφώνονται στην επιφάνειά της μικρές κάμψεις ή κυματισμοί. Ακριβώς όπως απλά το ανθρώπινο μάτι εντοπίζει το φως (δεδομένου ότι τα μάτια είναι βιολογικοί οπτικοί ανιχνευτές), έτσι υπάρχει και εξοπλισμός που κάνει την ίδια δουλειά. Αυτό που απλά πρέπει να γίνει για να εξαχθούν πληροφορίες που ταξιδεύουν μέσω μιας οπτικής ίνας είναι μια μικρή κάμψη στην ίνα και τα φωτόνια θα διαρρεύσουν στο δέκτη του εισβολέα. Ο επιτιθέμενος με λιγότερο από 500€ μπορεί να υποκλέψει το οπτικό σήμα και κατά συνέπεια μεγάλο όγκο δεδομένων.



(Sandra Kay Miller, *Information Security Magazine,* November 2006)

Σχήμα 1.1 Παράδειγμα Fibber Tapping



("Fiber Optic Intrusion Detection Systems," NetworkIntegrity Systems, 2005)

Σχήμα 1.2 Μηχανισμός Fiber Tapping

Για μια απλή fiber tapping συσκευή αρκούν 0.2 dB του οπτικού σήματος για να προσδιοριστεί η παρουσία και η κατεύθυνση του σήματος. Κατά συνέπεια είναι αρκετά απλό να χρησιμοποιηθούν πιο ευαίσθητοι οπτικοί ανιχνευτές και πρόσθετος ηλεκτρονικός εξοπλισμός προκειμένου να υποκλαπεί ολόκληρο το οπτικό σήμα. Μόλις ολοκληρωθεί αυτή η διαδικασία, μια συσκευή ανάλυσης δικτύων οπτικών ινών, που είναι ένα σύνηθες όργανο δοκιμής που κατασκευάζεται από διάφορες εταιρίες, μπορεί να χρησιμοποιηθεί για να καθορίσει το πρωτόκολλο επικοινωνίας και να αποκρυπτογραφήσει τις πληροφορίες. Ακόμα και όταν διαρρέει λιγότερο από 0.1 dB (≈2%) του σήματος, περιέχονται όλες οι πληροφορίες που διαβιβάζονται από κάθε φωτόνιο. Ο χρήστης στο άλλο άκρο δεν γνωρίζει ότι οι πληροφορίες του έχουν υποκλαπεί δεδομένου ότι δεν αντιλήφθηκε καμία προφανή παρεμβολή στην επικοινωνία του.

Σχήμα 1.3 Μηχανισμοί Fiber Tapping

Μερικές συσκευές θα μπορούσαν να χρησιμοποιηθούν όχι μόνο παθητικά αλλά και ενεργά, προκειμένου να εισαχθούν ψεύτικες πληροφορίες ή να αλλοιωθούν υπάρχουσες ροές πληροφοριών. Τέτοιες δυνατότητες επιτρέπουν ένα ευρύ φάσμα κακόβουλης χρήσης, από εταιρική παραπληροφόρηση και κατασκοπεία ως ακόμα και τρομοκρατικές επιθέσεις στην κρίσιμη υποδομή επικοινωνιών μιας χώρας. Αντίθετα από τις εμφανείς επιθέσεις στη φυσική υποδομή ενός δικτύου, όπως η κοπή ενός οπτικού καλωδίου, οι οπτικές απομαστεύσεις μπορεί να έχουν ολέθριες επιπτώσεις στην ακεραιότητα και τη διαθεσιμότητα μίας υποδομής.

1.2.3.3. Εξ αποστάσεως απομάστευση οπτικών ινών

Υπάρχουν μέθοδοι υποκλοπής σηματοδοσίας από οπτικές ίνες χωρίς την ανάγκη σπασίματος ή λυγίσματος του καλωδίου οπτικής ίνας. Μία πατέντα των Ηνωμένων Πολιτειών της Αμερικής με αριθμό 6265710 καθώς και Ευρωπαϊκή πατέντα με αριθμό 0915356, που εκδόθηκε από την Deutsche Telekom και εφευρέθηκε από τον H. Walter, περιγράφει «μια μέθοδο ή συσκευή εξαγωγής σημάτων από μια οπτική ίνα χωρίς οποιαδήποτε ανιχνεύσιμη παρεμβολή και χωρίς τα μεταδιδόμενα, μέσω της οπτικής ίνας, σήματα να υποστούν οποιαδήποτε απώλεια μετάδοσης…».

Το εντυπωσιακό είναι ότι αν και τέτοιες μη ανιχνεύσιμες συσκευές δεν είναι διαθέσιμες σήμερα για αγορά, τα έγγραφα ευρεσιτεχνίας περιγράφουν σαφώς τη συνιστώμενη μέθοδο και το πώς μια τέτοια συσκευή κατασκευάζεται και λειτουργεί. Τέτοιες συσκευές είναι μη ανιχνεύσιμες και χωρίς την κατάλληλη φυσική προστασία οπτικών σημάτων σε ισχύ, τα δεδομένα μπορούν να υποκλαπούν ή μετατραπούν κατά τρόπο μη ορατό από το φορέα εκμετάλλευσης του δικτύου ή τον τελικό χρήστη.

1.2.4. Μέθοδοι προστασίας φυσικού στρώματος δικτύων οπτικών ινών

1.2.4.1. Συστήματα ελέγχου ραδιοσυχνότητας (Radio Frequency Testing System RFTS)

Τα συστήματα ελέγχου ραδιοσυχνότητας είναι αποτελεσματικά μέσα ελέγχου ακεραιότητας διαδρομής πριν οι οπτικές ίνες τεθούν σε λειτουργία. Ενώ ορισμένοι τύποι αποκλίσεων μπορούν να βρεθούν, οι οποίοι θα μπορούσαν να συσχετιστούν με τοποθετημένες συσκευές υποκλοπής σήματος, τα RFTS λειτουργούν μόνο σε «σκοτεινές» ίνες. Κατά συνέπεια, μόλις αποσυναρμολογηθεί το RFTS και η ίνα μπει σε λειτουργία, δεν υπάρχει καμία μορφή ακόμη και βασικής ανίχνευσης παρείσφρησης. Επιπλέον, τα οπτικά σήματα στην ενεργή ίνα δεν προστατεύονται σε καμία περίπτωση, οπότε μια συσκευή απομάστευσης μπορεί εύκολα να υποκλέψει δεδομένα χωρίς δυνατότητα ανίχνευσής της. Εν ολίγης, τα RFTS συστήματα μπορούν να παρέχουν κάποια προστασία στα οπτικά δίκτυα, αλλά πριν το δίκτυο μπει σε λειτουργία.

Σχήμα 1.4 Radio Frequency Testing System από την EXFO

1.2.4.2. Συστήματα ελέγχου μη εξουσιοδοτημένης πρόσβασης (Intrusion Detection System IDS)

Τα συστήματα ελέγχου μη εξουσιοδοτημένης πρόσβασης μπορούν να λειτουργήσουν στο data layer ή στο φυσικό στρώμα. Τα συστήματα ελέγχου μη εξουσιοδοτημένης πρόσβασης που λειτουργούν στο φυσικό στρώμα είναι στην πραγματικότητα αυτά που χρησιμεύουν στην ανίχνευση συσκευών υποκλοπής σήματος. Εντούτοις, τα IDS δεν προστατεύουν τα δεδομένα του δικτύου μας.

Η Network Integrity Systems, έχει αναπτύξει ένα σύστημα ανίχνευσης παρείσφρησης οπτικών ινών που είναι το πιο ευαίσθητο από τις υπάρχουσες συσκευές, οι οποίες ως επί το πλείστον στηρίζονται μόνο στη μέτρηση ισχύος σήματος. Το προς έλεγχο δίκτυο οπτικών ινών μπορεί είτε να είναι ενεργό (κυκλοφορία πληροφοριών) είτε ανενεργό (καμία κυκλοφορία πληροφοριών). Εάν ελέγχεται μια ενεργός ίνα, η ροή δεδομένων δεν διακόπτεται και τα δεδομένα δεν αποκωδικοποιούνται.

Αποκαλούμενο INTERCEPTOR™, το σύστημα ελέγχει ένα σκέλος οπτικής ίνας για διαταραχές του σήματος που θα μπορούσαν να σημαίνουν ζημία στην ίνα ή φυσική παρείσφρηση. Όταν το σύστημα τεθεί σε λειτουργία ανιχνεύονται συνεχώς η ισχύς και η κατανομή ισχύος της ίνας χρησιμοποιώντας πρόσθετα οπτικά φίλτρα και έναν ευαίσθητο δέκτη. Ενώ οι πιο αόριστες μέθοδοι απομάστευσης δεν προκαλούν ανιχνεύσιμη απώλεια ισχύος, η προετοιμασία του καλωδίου οπτικών ινών για την υποκλοπή θα προκαλέσει διαταραχή της ισχύος και της κατανομής της ισχύος που τα οπτικά φίλτρα και ο δέκτης θα ανιχνεύσουν και ενισχύσουν. Τα αποτελέσματα αναλύονται και χρησιμοποιούνται για να προσδιοριστεί αν πρόκειται για προσπάθεια παρείσφρησης. Σε περίπτωση παρείσφρησης ενεργοποιείται συναγερμός και απαιτούνται ενέργειες από το προσωπικό που είναι υπεύθυνο για το δίκτυο.

Χρησιμοποιώντας ευφυή φίλτρα, οι κανονικές διαταραχές από τη θέρμανση, τα συστήματα ψύξης, κινητήρες, ανεμιστήρες και άλλα δομικά συστήματα μπορούν να φιλτραριστούν. Αυτό θα επιτρέψει τη μέγιστη ευαισθησία στις προσπάθειες παρείσφρησης ελαχιστοποιώντας την πιθανότητα ψεύτικων συναγερμών. Ο στόχος είναι να προσδιοριστούν οι προσπάθειες παρείσφρησης ενώ οι επιτιθέμενοι είναι ακόμα στο εξωτερικό στρώμα της δομής του καλωδίου. Αυτό θα επιτρέψει την

ταχύτερη παρεμπόδιση οποιουδήποτε εισβολέα, προτού αυτός αποκτήσει οποιαδήποτε πρόσβαση στα δεδομένα του δικτύου μας.

Σχήμα 1.5 Fiber Optic Intrusion Detection System INTERCEPTOR™

Τα IDS είναι επιρρεπή στο ανθρώπινο λάθος, καθώς οι συναγερμοί πρέπει να ερμηνευθούν σωστά και γίνουν οι απαραίτητες ενέργειες, διαφορετικά τα μη προστατευμένα δεδομένα μας θα συνεχίσουν να υποκλέπτονται. Στην πραγματικότητα, οι εξ αποστάσεως μέθοδοι υποκλοπής σήματος είναι εξ ορισμού μη ανιχνεύσιμες, έτσι εάν τα δεδομένα δεν προστατεύονται, υπάρχει κίνδυνος ασφάλειας. Κατά συνέπεια ενώ τα IDS διαδραματίζουν έναν σημαντικό ρόλο στην ασφάλεια δικτύων οπτικών ινών, θα πρέπει να αποτελούν τμήμα ενός συνόλου μέτρων ασφάλειας και ελέγχου, τα οποία ενσωματώνουν επίσης άλλους αποτελεσματικούς μηχανισμούς προστασίας δεδομένων δικτύων οπτικών ινών.

1.2.4.3. Κρυπτογράφηση

Η κρυπτογράφηση είναι ένας αποτελεσματικός τρόπος ασφάλειας μεταφοράς δεδομένων από σημείο σε σημείο σε ένα δίκτυο. Παρόλα αυτά δεν λύνει το πρόβλημα των οπτικών συσκευών υποκλοπής σήματος. Συγκεκριμένα, δεν προστατεύει το φυσικό στρώμα μεταφοράς σημάτων του δικτύου, ούτε μπορεί να ανιχνεύσει αν έχει τοποθετηθεί μια συσκευή απομάστευσης, τι τύπος είναι και που ακριβώς έχει εγκατασταθεί. Χωρίς τη δυνατότητα να ανιχνευθεί και να βρεθεί ένας πιθανός εισβολέας, δεν είναι δυνατόν να εφαρμοστούν αποτελεσματικές ενέργειες επιβολής του νόμου. Επομένως οι εισβολείς είναι όχι μόνο σε θέση συνεχώς και κατά τρόπο αόρατο να υποκλέπτουν τα δεδομένα και την κίνηση ενός δικτύου. Η κρυπτογράφηση

είναι εξ ορισμού ένας μαθηματικός αλγόριθμος αποτελούμενος από ένα προκαθορισμένο σύνολο και ένα σωστό κλειδί, τα οποία μέσω διάφορων μεθόδων μπορούν να αναπαραχθούν. Οι αποκαλούμενες αδιάσπαστες μέθοδοι κρυπτογράφησης, όπως έχει αποδείξει η ιστορία κατ' επανάληψη, έχουν σπάσει με έξυπνες μεθόδους, γρηγορότερους επεξεργαστές, νέες τεχνολογίες και την απλή brute force επίθεση. Πολλά εργαλεία αποκρυπτογράφησης, υλικό και λογισμικό, είναι ευρέως διαθέσιμα για τους χάκερ και είναι αρκετά επιτυχή στο να παρέχουν παράνομη πρόσβαση σε ευαίσθητα δεδομένα.

Η κρυπτογράφηση έχει επίσης ένα σχετικό υψηλό κόστος και δυσκολίες στην εφαρμογή της. Η ευχρηστία είναι επίσης ένα ζήτημα δεδομένου ότι θα πρέπει να υπάρχει διαλειτουργικότητα με τα διαφορά μέρη που πρόκειται να επικοινωνούν. Θα πρέπει να γίνεται ο κατάλληλους προγραμματισμός και συμφωνία για τους τύπους προτύπων κρυπτογράφησης που θα χρησιμοποιούνται κάθε φορά. Δεδομένου ότι η κρυπτογράφηση πολλές φορές δεν είναι μια διαφανής για τον χρήστη διαδικασία, οι χρήστες πρέπει να μάθουν τις διάφορες διεπαφές, οι οποίες δεν είναι τυποποιημένες στις εφαρμογές ή τις πλατφόρμες. Ακόμα και τότε, η κρυπτογράφηση είναι μόνο αποτελεσματική εάν τα κλειδιά ενημερώνονται συχνά και χρησιμοποιούνται ισχυροί κωδικοί πρόσβασης. Οι πολυεθνικές με γραφεία σε όλη την υφήλιο πρέπει επίσης να εξετάσουν τις διαφορετικές πολιτικές και νόμους της κάθε χώρας σχετικά με τις τεχνολογίες κρυπτογράφησης.

Η κρυπτογράφηση επομένως έχει ένα σχετικά χαμηλό ποσοστό εφαρμογής και ουσιαστικά όλη η κυκλοφορία φωνής και το μεγαλύτερο ποσοστό της κυκλοφορίας δεδομένων δεν κρυπτογραφούνται σήμερα. Επίσης το μικρό ποσοστό που κρυπτογραφείται, εντούτοις, πρέπει να έχει μη κρυπτογραφημένες επιγραφές (headers) προκειμένου να διέλθει επιτυχώς και να δρομολογηθεί στα δημόσια δίκτυα. Κατά συνέπεια, με την ανάλυση κυκλοφορίας μπορεί να παραγάγει κανείς μεγάλους όγκους χρήσιμων πληροφοριών και η κρυπτογραφημένη επικοινωνία μεταξύ δύο συμβαλλόμενων μερών χρησιμεύει πραγματικά ως μια κόκκινη σημαία για πληροφορίες που είναι ενδεχομένως ιδιαίτερα χρήσιμες και μπορεί να αξίζουν την προσπάθεια να αποκρυπτογραφηθούν εκτός δικτύου.

Οι εξελίξεις στην κβαντική κρυπτογράφηση έχουν κάνει σημαντικά βήματα πρόσφατα. Είναι σημαντικό να σημειωθεί ότι ενώ τέτοιες προσπάθειες αρχικά προστατεύουν το αρχικό κλειδί κρυπτογράφησης, κατά την αποστολή του, μόλις εγκατασταθεί η σύνοδος, οι πραγματικές πληροφορίες στέλνονται με ένα κανονικό

αλγόριθμο κρυπτογράφησης που είναι ακόμα ευαίσθητος και μπορεί να αποκρυπτογραφηθεί. Επομένως, ενώ η κρυπτογράφηση μπορεί να χρησιμεύσει ως ένας αποτρεπτικός παράγοντας στο data layer γενικά, μια δεύτερη αμυντική γραμμή στο φυσικό στρώμα απαιτείται για να προστατευθεί πραγματικά το δίκτυο οπτικών ινών από τις υποκλοπές σήματος.

1.2.4.4. Ασφαλείς οπτικές επικοινωνίες βασισμένες στο νόμο του Kirchhoff και στον Johnson-like θόρυβο.

Η βασισμένη στο νόμο του Kirchhoff και στον Johnson-like θόρυβο επικοινωνία είναι ασφαλής, γρήγορη, ανέξοδη, δυνατή, χωρίς ιδιαίτερα κόστη συντήρησης και χαμηλής ισχύος. Γενικά οι καταστάσεις των bit πληροφορίας αναπαρίστανται από δύο τιμές αντίστασης. Ο αποστολέας και ο δέκτης έχουν τέτοιους αντιστάτες διαθέσιμους και επιλέγουν τυχαία και συνδέουν έναν απ' αυτούς στο κανάλι επικοινωνίας στην αρχή κάθε περιόδου. Η θερμικός θόρυβος τάσης και ρεύματος μπορούν να παρατηρηθούν αλλά ο νόμος Kirchhoff παρέχει μόνο μια δευτεροβάθμια εξίσωση. Ένα ασφαλές bit αποστέλλεται όταν οι τιμές των πραγματικών αντιστάσεων στην πλευρά του αποστολέα και την πλευρά του δέκτη διαφέρουν. Κατόπιν η δευτεροβάθμια εξίσωση παράγει τις δύο τιμές αντίστασης αλλά ο επιτιθέμενος είναι ανίκανος να καθορίσει τις πραγματικές θέσεις των αντιστατών και να ανακαλύψει την κατάσταση του bit του αποστολέα. Ο δέκτης ξέρει ότι ο αποστολέας έχει το αντίστροφο bit απ' αυτόν. Ο ωτακουστής μπορεί να αποκωδικοποιήσει το μήνυμα εάν, για κάθε bit, εγχέει ρεύμα στο καλώδιο και μετρά την αλλαγή τάσης και ρεύματος και στις δύο κατευθύνσεις. Με αυτό τον τρόπο όμως ο επιτιθέμενος γίνεται αντιληπτός από το πρώτο κιόλας bit που υποκλέπτει.

Στην περίπτωση μιας επίθεσης, όπως προαναφέραμε, ο επιτιθέμενος μπορεί να εξαγάγει το πολύ ένα ενιαίο bit προτού ανακαλυφθεί. Κατά συνέπεια αυτό το σχέδιο επικοινωνίας είναι ασφαλέστερο από τους εξιδανικευμένους κβαντικούς τρόπους επικοινωνίας. Η πρακτική ασφάλεια των wave based μεθόδων εξαρτάται από το πόσο καλά η μελέτη εφαρμογής μπορεί να πλησιάσει την εξιδανικευμένη θεωρία και αυτό περιορίζεται από τις αποστάσεις (λίγα χιλιόμετρα). Ένα άλλο πρακτικό πλεονέκτημα του προτεινόμενου σχεδίου είναι ότι μπορεί να εφαρμοστεί μέσω των

ήδη εγκατεστημένων οπτικών ινών χρησιμοποιώντας διαφορετικά μήκη κύματος, οπτικούς συζευκτήρες και κατάλληλα φίλτρα για κανονική επικοινωνία και ασφαλή επικοινωνία, αντίστοιχα.

Υπάρχουν διάφορα ερωτήματα σχετικά με την man-in-the-middle και άλλες πιθανές επιθέσεις. Το σχέδιο είναι εφαρμόσιμο και έχει ορισμένα πλεονεκτήματα έναντι των κβαντικών καναλιών, όπως υψηλότερη ασφάλεια και τη δυνατότητα χρησιμοποίησης των, αυτήν την περίοδο, ήδη χρησιμοποιούμενων γραμμών. Εντούτοις, για πρακτικούς λόγους όπως η απόσταση, ασφάλεια, ταχύτητα, ευρωστία, λειτουργική ενοποίηση τσιπ και καρτών υπολογιστών, τα βασισμένα στο καλώδιο συστήματα επικοινωνίας KLJN είναι ανώτερα από οποιαδήποτε wave-based λύση συμπεριλαμβανομένου και του γιγαντιαίου λέιζερ οπτικών ινών των Scheuer-Yariv.

1.2.4.5. Optical Time Domain Reflectometer

Τα εμπορικά δίκτυα οπτικών ινών και ο εξοπλισμός τους δεν ενσωματώνουν μηχανισμούς προστασίας ενάντια στις μεθόδους οπτικής απομάστευσης. Οι εισβολείς γνωρίζουν ότι μπορούν να αποκτήσουν μια αφθονία στοχοθετημένων πληροφοριών με ελάχιστη ή καμία πιθανότητα ανίχνευσης των αθέμιτων δραστηριοτήτων τους, είτε από τον πάροχο είτε από τους εταιρικούς πελάτες του. Τα κυβερνητικά δίκτυα, εντούτοις, ενσωματώνουν πιο ισχυρή προστασία ενάντια σε αυτές τις μεθόδους. Οι διαμορφώσεις ασφάλεια εξαρτώνται από τον τύπο του δικτύου, τη σημασία των διαβιβασθέν δεδομένων και τη φύση της εφαρμογής. Για παράδειγμα, πολλά κυβερνητικά δίκτυα κρυπτογραφούν προσεκτικά τα περισσότερα ή όλα τα δεδομένα προς μετάδοση. Επιπλέον, μερικά κυβερνητικά δίκτυα πραγματοποιούν τυχαίες καθημερινές οπτικές μετρήσεις με Optical Time Domain Reflectometer («OTDR») για να ανιχνεύσουν πιθανές αλλαγές στις ίνες, ένδειξη πιθανής κακόβουλης δραστηριότητας. Σε αυτές τις περιπτώσεις οι εξ' αποστάσεως μέθοδοι απομάστευσης οπτικών δικτύων εξακολουθούν να είναι μη ανιχνεύσιμες επιτρέποντας την κατασκοπεία και την υποκλοπή.

Σχήμα 1.6 OTDR σύστημα μετρήσεων της EXFO (αριστερά) και Test Module δικτύων καναλιού οπτικών ινών (δεξιά)

1.2.4.6. Αρχιτεκτονική ασφαλούς μετάδοσης από την Oyster Optics

Η Oyster Optics έχει αναπτύξει και έχει κατοχυρώσει με δίπλωμα ευρεσιτεχνίας μία αρχιτεκτονική ασφάλειας, ελέγχου, ανίχνευσης παρείσφρησης και εντοπισμού παραβιάσεων για τα σημερινά παγκόσμια οπτικά δίκτυα. Οι τεχνολογίες της επιχείρησης είναι δίχως κρυπτογράφηση (αλλά συμβατές με συστήματα κρυπτογράφησης), ανεξάρτητες πρωτοκόλλου και προβλέπουν το υψηλότερο επίπεδο ασφάλειας στις ήδη υπάρχουσες οπτικές υποδομές. Λόγω του ότι το φυσικό στρώμα εξασφαλίζεται εντελώς, όλα τα υψηλότερα στρώματα δικτύωσης και οι τύποι δεδομένων επίσης θεωρούνται ασφαλή. Η Oyster Optics έχει ήδη χορηγήσει με άδεια τις τεχνολογίες της σε κατασκευαστές τηλεπικοινωνιακού εξοπλισμού και οργανισμούς υπευθύνους για την ασφάλεια για την εφαρμογή τους σε δημόσια και ιδιωτικά δίκτυα. Επίσης είναι διαθέσιμες και ειδικές διαμορφώσεις για απόλυτα ασφαλή κυβερνητικά δίκτυα και εφαρμογές.

Οι μέθοδοι μετάδοσης της Oyster Optics επιφέρουν νέα πρόοδο στους τομείς της ασφάλειας, του ελέγχου, της ανίχνευσης παρείσφρησης και της συντήρησης δικτύων οπτικών ινών. Ο συνδυασμός τεσσάρων χαρακτηριστικών προσφέρει μια εξαιρετική ασφάλεια ενάντια στις επιθέσεις υποκλοπής σε δίκτυα οπτικών ινών.

1. ***Ασφάλεια φυσικού στρώματος***: Εξασφαλίζει πλήρως τα στρώματα μεταφορών δικτύων οπτικών ινών πράγμα που καθιστά τα δεδομένα ουσιαστικά αδύνατο να ανακτηθούν και να διαβαστούν.
2. ***Ανίχνευση μη εξουσιοδοτημένης πρόσβασης:*** Ο ιδιαίτερα ευαίσθητος έλεγχος των διάφορων γεγονότων παρείσφρησης και συντήρησης, με τα κατώτατα όρια να είναι δυνατό να ρυθμιστούν, επιτρέπει τις άμεσες ειδοποιήσεις των προσπαθειών διείσδυσης.
3. ***Εντοπισμός παραβιάσεων:*** Υπολογίζει την ακριβή θέση γεγονότων κατά μήκος των οπτικών ινών σε πραγματικό χρόνο. Οι ενέργειες επιβολής νόμου ενάντια σε κακόβουλες οντότητες και οι ενέργειες συντήρησης και επισκευής είναι ταχύτερες και πιο αποτελεσματικές.
4. ***Βελτιστοποίηση εξαγομένων σημάτων***: Η διαχείριση λογισμικού περιορίζει το γενικά διαθέσιμο φως στις εγκαταστάσεις οπτικών ινών. Ο αποδεκτός σηματοθορυβικός λόγος και bit-error-rate είναι μεγέθη τα οποία μπορούν να ρυθμιστούν από λογισμικό, δημιουργώντας έτσι ισχυρές οπτικές συνδέσεις. Επίσης περιορίζεται το περιττό φως, που βρίσκεται χαρακτηριστικά στις εγκαταστάσεις οπτικών ινών, το οποίο θα παρείχε περισσότερες δυνατότητες σε μία κακόβουλη οντότητα που θα ήθελε να επιχειρήσει μια επίθεση φυσικού στρώματος.

Ως μία ολοκληρωμένη λύση, η τεχνολογική λύση ασφάλειας της Oyster Optics υπόσχεται τη μέγιστη ακεραιότητα, εμπιστευτικότητα και διαθεσιμότητα των εγκαταστάσεων οπτικών ινών.

2ο Κεφάλαιο

2. Ασφάλεια δικτύων οπτικού καναλιού

Η τεχνολογία οπτικών δικτύων σε συνδυασμό με τη προστασία δεδομένων και τη μυστικότητα έχει κάνει την ασφάλεια αποθήκευσης και μετάδοσης δεδομένων σε δίκτυα αποθήκευσης δεδομένων, ένα σημαντικό ζήτημα. Οι κίνδυνοι ασφαλείας των οπτικών δικτύων είναι συχνά υποτιμημένοι.

Ο σκοπός αυτού του κεφαλαίου είναι να συζητηθούν οι διαρροές ασφαλείας δικτύων οπτικών καναλιών (Fiber Channel). Κάθε κίνδυνος θα περιγραφεί και στη συνέχεια θα αναλυθεί πλήρως.

Τα ακόλουθα είναι τα βασικά θέματα αυτού του κεφαλαίου:

- Κίνδυνοι δικτύων οπτικών ινών
- Κίνδυνοι οπτικών καναλιών
    - Αδυναμίες πλαισίων οπτικών καναλιών, πειρατεία συνόδου (session hijacking)
    - Αδυναμίες διευθύνσεων οπτικών καναλιών, επιθέσεις ενδιάμεσης οντότητας (Man-in-the-Middle attacks)

2.1. Κίνδυνοι ασφάλειας δικτύων οπτικών ινών

Προκειμένου να συζητηθούν οι κίνδυνοι στις αρχιτεκτονικές δικτύων οπτικών ινών, πρέπει να γίνει αξιολόγηση με βάση τους έξι τομείς της ασφάλειας.

Αυθεντικοποίηση (Authentication)

Τα Fibre Channel Authentication Protocol (FCAP) , DH-CHAP (Diffie-Hielman CHAP) και Fiber Channel Security Protocol (FC-SP), δημιουργηθήκαν προκειμένου να καλυφθεί η σημαντική έλλειψη αυθεντικοποίησης σε δίκτυα οπτικών

καναλιών. Εντούτοις, πολλοί θεωρούν ότι η αυθεντικοποίηση έχει πραγματοποιηθεί κάπου αλλού στην αρχιτεκτονική του δικτύου. Παραδείγματος χάριν, αρκετοί οργανισμοί υποθέτουν συχνά ότι η αυθεντικοποίηση που πραγματοποιείται στα στρώματα αρχείων/δεδομένων (βάσεις δεδομένων) είναι αρκετή και αγνοούν την αυθεντικοποίηση σε χαμηλότερα επίπεδα δικτύων. Αυτό θα ήταν παρόμοιο με την απαίτηση αυθεντικοποίησης σε μια εφαρμογή Ιστού αλλά την μη απαίτηση αυθεντικοποίησης σε μία Telnet ή SSH σύνδεση με ένα web server. Και στα δύο σενάρια, τα δεδομένα θα μπορούσαν να εκτεθούν πλήρως.

Τα FCAP, DH-CHAP και FC-SP, καθώς επίσης και μερικές άλλες τεχνικές αυθεντικοποίησης, έχουν αναπτυχθεί για την αυθεντικοποίηση κόμβου με κόμβο, κόμβου με switch και switch με switch.

Εξουσιοδότηση (Authorization)

Οι παράμετροι εξουσιοδότησης παρέχονται συνήθως με World Wide Names (WWNs) από τους host bus adapters καναλιού οπτικών ινών. Τα WWNs μπορεί να είναι port WWNs, τα οποία προσδιορίζουν μία πόρτα, ή node WWNs, τα οποία προσδιορίζουν ένα κόμβο.

Κρυπτογράφηση (Encryption)

Οι πτυχές κρυπτογράφησης στα περισσότερα περιβάλλοντα δικτύων αποθήκευσης δεδομένων δεν υπάρχουν. Συνήθως, στα κανάλια οπτικών ινών σε δίκτυα αποθήκευσης δεδομένων δεν χρησιμοποιείται κρυπτογράφηση σε κανένα από τα στρώματά τους (στρώμα 0 - στρώμα 4).

Έλεγχος (Auditing)

Έλεγχος στα περισσότερα κανάλια οπτικών ινών πραγματοποιείται σε επίπεδο συσκευής (Fiber channel switch) ή στο επίπεδο εφαρμογής (management application).

Ακεραιότητα (Integrity)

Δεν υπάρχει, αυτήν την περίοδο, καμία εγγενής μέθοδος για τον έλεγχο ακεραιότητας των πλαισίων των καναλιών οπτικών ινών.

Διαθεσιμότητα (Availability)

Η διαθεσιμότητα ή Quality of Service (QoS) είναι έμμεσα διαθέσιμη στο στρώμα 2 των πλαισίων των καναλιών οπτικών ινών στους τομείς ελέγχου λάθους του πλαισίου. Η διαθεσιμότητα είναι αδιαμφισβήτητα η σημαντικότερη πτυχή ασφάλειας ενός δικτύου. Εάν τα δεδομένα είναι μη διαθέσιμα, το δίκτυο καθώς επίσης και οι εφαρμογές καταρρέουν.

2.2. Κίνδυνοι ασφάλειας καναλιού οπτικών ινών

Στο μέσο επικοινωνιών καναλιού οπτικών ινών απουσιάζουν διάφορες οντότητες προαπαιτούμενες για την ασφαλή μετάδοση δεδομένων. Αρκετές από τις αδυναμίες είναι παρόμοιες με τις αδυναμίες της IP έκδοσης 4 (IPv4). Σε αυτό το τμήμα αναλύονται τα ακόλουθα θέματα:

- Περιγραφή του καναλιού οπτικών ινών
- Clear-text επικοινωνία

2.2.1. Περιγραφή του καναλιού οπτικών ινών

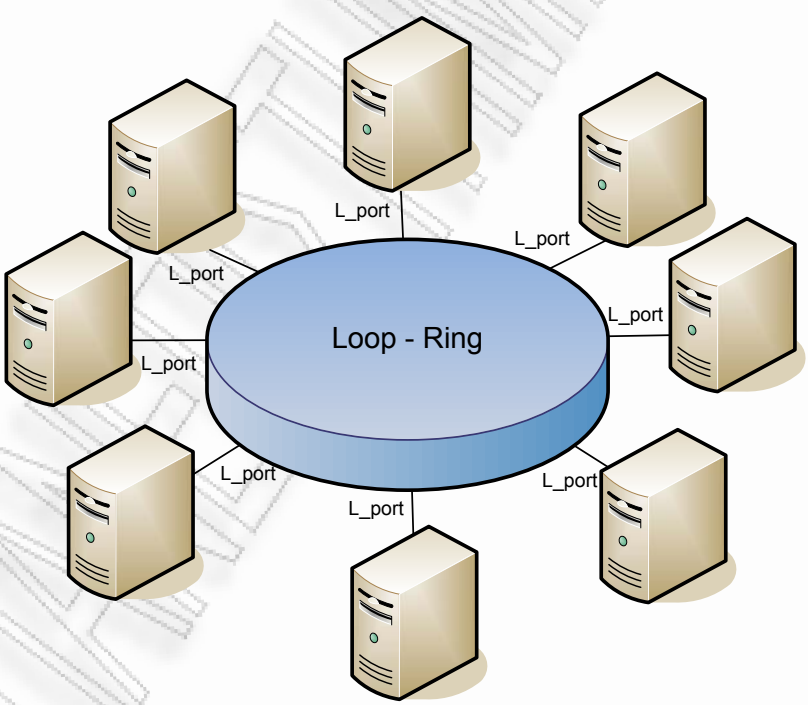
Προκειμένου να γίνουν κατανοητά τα θέματα ασφαλείας των καναλιών οπτικών ινών, πρέπει να συζητήσουμε την αρχιτεκτονική των επικοινωνιών καναλιού οπτικών ινών. Το κανάλι οπτικών ινών χρησιμοποιεί πλαίσια μεταξύ των κόμβων (παρόμοια με τα IP δίκτυα που χρησιμοποιούν πακέτα). Κάθε πλαίσιο περιέχει πέντε στρώματα. Το κάθε στρώμα μέσα στο πλαίσιο συνεργάζεται με το κατώτερό του στρώμα και το ανώτερό του στρώμα για να παρέχουν τις διάφορες λειτουργίες μέσα σε μια τοπολογία καναλιού οπτικών ινών.

Υπάρχουν τρεις βασικές τοπολογίες:

- Point to point (FC-P2P). Δύο συσκευές είναι συνδεδεμένες πλάτη με πλάτη. Αυτό είναι η απλούστερη τοπολογία, με περιορισμένη συνδεσιμότητα.

Σχήμα 2.1 Τοπολογία Point to point (FC-P2P)

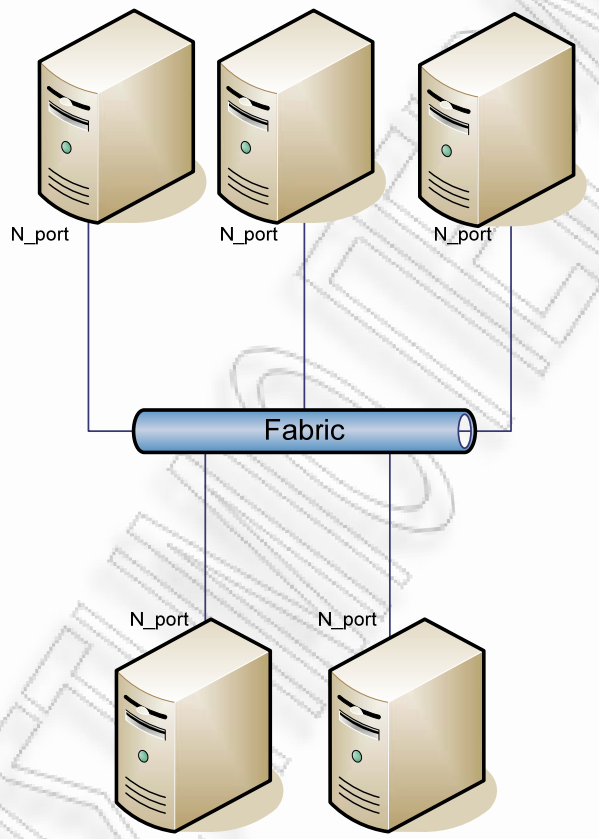
- Arbitrated loop (FC-AL). Σε αυτή τη τοπολογία, όλες οι συσκευές είναι σε έναν βρόχο ή ένα δακτύλιο, παρόμοια με token ring. Η προσθήκη ή η αφαίρεση μιας συσκευής από το βρόχο αναγκάζει όλη τη δραστηριότητα στο βρόχο για να διακοπεί. Η αποτυχία μιας συσκευής προκαλεί ένα σπάσιμο στο δακτύλιο. Hubs καναλιού οπτικών ινών υπάρχουν για να συνδέσουν τις πολλαπλάσιες συσκευές και μπορούν να παρακάμψουν τις αποτυχημένες πόρτες.



Σχήμα 2.2 Τοπολογία Arbitrated loop (FC-AL)

- Switched Fabric (FC-SW). Όλες οι συσκευές ή οι βρόχοι των συσκευών συνδέονται με fiber channel switches, παρομοίως

εννοιολογικά με τις σύγχρονες εφαρμογές Ethernet. Τα switches διαχειρίζονται την κατάσταση του δικτύου, παρέχοντας τις βέλτιστες διασυνδέσεις.



Σχήμα 2.3 Τοπολογία Switched Fabric (FC-SW)

Ακολουθούν οι τύποι θυρών που υπάρχουν σε δίκτυα οπτικών καναλιών:

Node ports

- N_port (πχ host ή storage device) χρησιμοποιείται με FC-P2P ή FC-SW τοπολογίες. Γνωστή ως Node port.
- NL_port είναι ένας τύπος πόρτας που χρησιμοποιείται σε FC-AL τοπολογίες. Γνωστή ως Node Loop port

Switch/router ports (FC-SW topology)

- F_port είναι μία πόρτα που συνδέει ένα switch με ένα κόμβο (N_port) point-to-point. Γνωστή ως Fabric port. Μία F_port δεν είναι loop capable.
- FL_port είναι μία πόρτα που συνδέει ένα switch με ένα FC-AL loop (NL_port). Γνωστή ως Fabric Loop port. Να σημειώσουμε εδώ ότι μία πόρτα στο switch μπορεί να γίνει F_port ή FL_port ανάλογα με το πού έχει συνδεθεί.
- E_port είναι η πόρτα σύνδεσης μεταξύ fibre channel switches. Γνωστή ως Expansion port. Όταν E_ports μεταξύ switches σχηματίζουν ένα link, αυτό το link ονομάζεται inter-switch link (ISL).
- EX_port port είναι η πόρτα σύνδεσης μεταξύ fibre channel router και fibre channel switch. Από την πλευρά του switch είναι μία κανονική E_port, αλλά από την μεριά του router είναι μία EX_port.
- TE_port είναι ένας όρος που χρησιμοποιείται για πολλές trunked E_ports προκειμένου να δημιουργηθεί ένα ευρείας ζώνης κανάλι μεταξύ switches. Γνωστή ως Trunking Expansion port.

General (catch-all)

- G_port ή generic port σε ένα switch μπορεί να λειτουργήσει ως E_port ή F_port.
- L_port είναι ένας «χαλαρός» όρος και χρησιμοποιείται για οποιαδήποτε arbitrated loop port, NL_port ή FL_port. Γνωστή ως Loop port
- U_port είναι ένας «χαλαρός» όρος και χρησιμοποιείται για οποιαδήποτε arbitrated port. Γνωστή ως Universal port.

Σε καθεμία τοπολογία, κάθε στρώμα εκτελεί μια συγκεκριμένη λειτουργία ανάλογα με την αρχιτεκτονική που έχει αναπτυχθεί. Τα πέντε διαφορετικά στρώματα των πλαισίων οπτικών καναλιών είναι τα ακόλουθα:

- Upper Layer Protocol Mapping — FC Layer 4
- Common Services Layer — FC Layer 3
- Signalling / Framing Layer — FC Layer 2
- Transmission Layer — FC Layer 1
- Physical Layer — FC Layer 0

FC0 το φυσικό στρώμα, το οποίο περιλαμβάνει τα καλώδια οπτικών ινών, patch cords, connectors, pinouts κ.λπ.

FC1 το Transmission layer, το οποίο εφαρμόζει 8b/10b κωδικοποίηση/ αποκωδικοποίηση των σημάτων.

FC2 το Signalling / Framing layer, το οποίο αποτελεί τον πυρήνα του καναλιού οπτικών ινών και καθορίζει τα κύρια πρωτόκολλα.

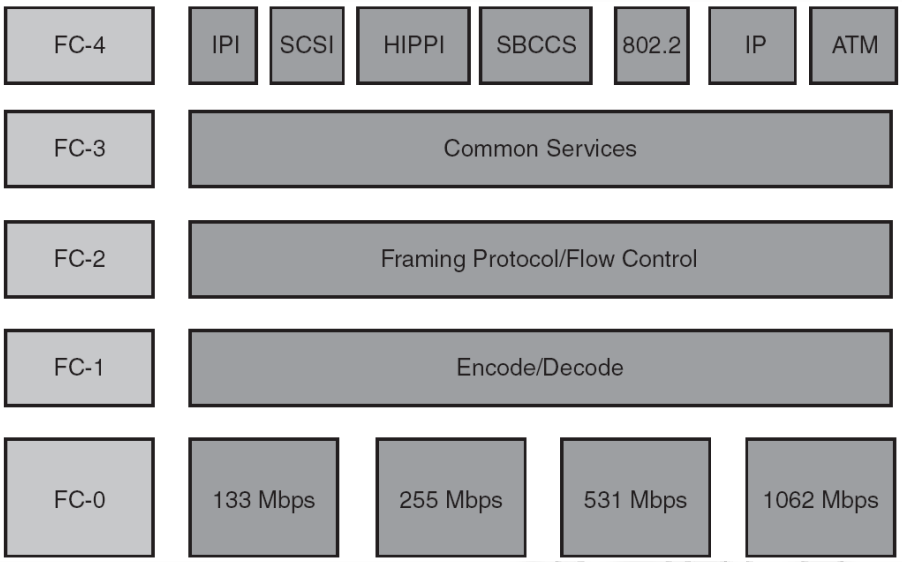
FC3 το Common Services layer, ένα "λεπτό" στρώμα που θα μπορούσε να εφαρμόσει λειτουργίες όπως κρυπτογράφηση ή Raid.

FC4 το Protocol Mapping layer στο οποίο άλλα πρωτόκολλα, όπως SCSI, ενθυλακώνονται σε μια μονάδα πληροφοριών για παράδοση στο FC2.

Οι routers καναλιού οπτικών ινών λειτουργούν μέχρι το επίπεδο FC4 (δηλ. είναι στην πραγματικότητα δρομολογητές SCSI), τα switches μέχρι FC2, και τα hubs στο FC0 μόνο.

Τα προϊόντα καναλιού οπτικών ινών είναι διαθέσιμα σε ταχύτητες 1Gbit/s, 2Gbit/s, 4Gbit/s, 8Gbit/s και 10Gbit/s. Η αγορά 10Gbit/s αυτήν την περίοδο ακόμα αναπτύσσεται ενώ αναμένεται και η εμφάνιση των 100Gbit/s.

Ομοίως με ένα δίκτυο IP, τα πλαίσια καναλιού οπτικών ινών κινούνται από το φυσικό στρώμα, στρώμα 0, προς τα ανώτερα στρώματα. Οι ομοιότητες των δύο μεθόδων επικοινωνίας τελειώνουν πρωτίστως στο φυσικό στρώμα. Εντούτοις, μοιράζονται αδυναμίες ασφάλειας και απουσία ελέγχων ασφαλείας. Δυστυχώς, αρκετοί από τους τύπους επίθεσης των IP δικτύων είναι επίσης διαθέσιμοι στο κανάλι οπτικών ινών. Οι αδυναμίες των πλαισίων οπτικών καναλιών εμφανίζονται κυρίως στο $2^{ο}$ στρώμα, γνωστό ως framing/flow control layer (στρώμα 2 στο κανάλι οπτικών ινών και Data/Networking (layer 2/layer 3) σε ένα πακέτο IP). Οι ομοιότητες, από την άποψη των αδυναμιών ασφάλειας και της έλλειψης αυθεντικοποίησης, εξουσιοδότησης, ακεραιότητας, και κρυπτογράφησης, είναι αρκετές.



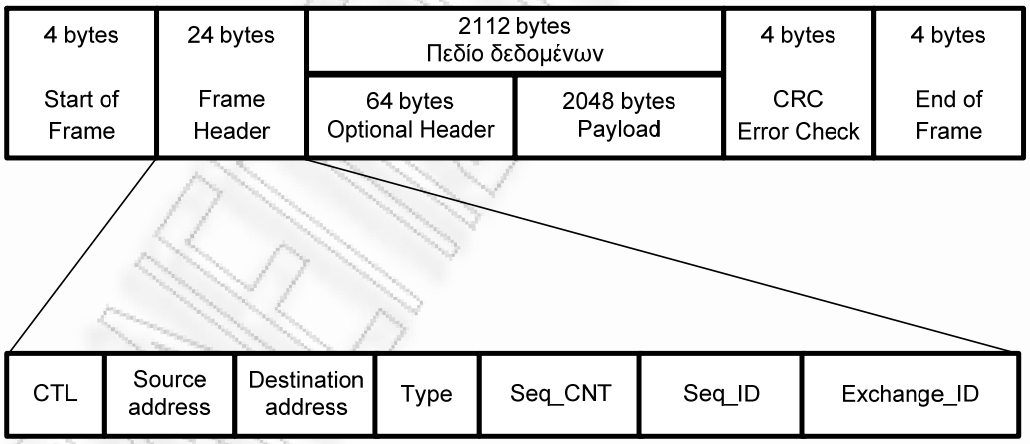
Σχήμα 2.4 Στρώματα πλαισίου καναλιού οπτικών ινών.

Το στρώμα 2, Framing Protocol/Flow Control layer, είναι το βασικό σημείο των αδυναμιών ασφάλειας πλαισίων. Το στρώμα αυτό περιέχει τις πληροφορίες των headers για κάθε πλαίσιο. Το περιεχόμενο ενός header περιλαμβάνει μια διεύθυνση 24bit (επίσης γνωστή ως port identity) του κόμβου προέλευσης, τη διεύθυνση 24bit του κόμβου προορισμού, τον αριθμό ελέγχου ακολουθίας, τον αριθμό αναγνώρισης ακολουθίας και τις πληροφορίες ανταλλαγής. Οι ακόλουθες οντότητες βρίσκονται μέσα στο header των πλαισίων:

- **Source Address (S_ID)** — Μία 24-bit διεύθυνση που προσδιορίζει τη διεύθυνση της προέλευσης κατά τη δρομολόγηση των πλαισίων.
- **Destination Address (D_ID)** — Μία 24-bit διεύθυνση που προσδιορίζει τη διεύθυνση του προορισμού κατά τη δρομολόγηση των πλαισίων.
- **Sequence ID (SEQ_ID)** — Ένας στατικός αριθμός που διαβιβάζεται με κάθε πλαίσιο σε μια ακολουθία που προσδιορίζει το πλαίσιο ως τμήμα μιας συνόδου. Κάθε πλαίσιο στην ίδια σύνοδο έχει την ίδια ταυτότητα ακολουθίας.
- **Sequence Count (SEQ_CNT)** — Ένας αριθμός (μετρητής) ο οποίος χρησιμοποιείται για αναγνώριση των πλαισίων σε μία ακολουθία. Για κάθε πλαίσιο μέσα στην ιδία ακολουθία αυξάνεται κατά 1 επιτρέποντας την τοποθέτηση των πλαισίων στη σωστή σειρά.

- **Exchange ID** — Πληροφορία που αφορά την ποσότητα των πλαισίων που μπορεί να δεχτεί ένας κόμβος. Αυτή η πληροφορία μεταβιβάζεται από κόμβο σε κόμβο.
- **Originator Exchange ID (OX_ID)** — Πληροφορία συναλλαγής του αποστολέα.
- **Recipient Exchange ID (RX_ID)** — Πληροφορία συναλλαγής του παραλήπτη.
- **Type** — Σε αυτό το τμήμα εμπεριέχονται τα byte του Upper Layer Protocol.
- **Routing Control (R_CTL)** — Περιέχει τις πληροφορίες όπως τα bits δρομολόγησης και την κατηγορία πληροφοριών, η οποία λέει στο δέκτη τον τύπο των πληροφοριών που περιλαμβάνονται στο πλαίσιο.

Κάθε κόμβος σε ένα δίκτυο αποθήκευσης δεδομένων έχει μια 24bit διεύθυνση που χρησιμοποιείται για ποικίλα πράγματα, συμπεριλαμβανομένων της δρομολόγησης και πληροφοριών που αφορούν κεντρικούς υπολογιστές. Παρόμοια με το πώς δρομολογείται ένα πακέτο IP, η διεύθυνση των 24bit χρησιμοποιείται για δρομολόγηση των πλαισίων από τον ένα κόμβο στον άλλο.



Σχήμα 2.5 Header information in Fibre Channel layer 2.

Κάθε πλαίσιο αρχίζει και τελειώνει με έναν οριοθέτη. Μετά το start of frame ακολουθεί το Header του πλαισίου. Το header του πλαισίου χρησιμοποιείται για να ελέγξει τις εφαρμογές συνδέσεων, τις μεταφορές πρωτοκόλλου συσκευών και να ανιχνεύσει ελλιπή ή εκτός σειράς πλαίσια. Ένας τομέας, το μέγιστο, 2112

ψηφιολέξεων (ωφέλιμο φορτίο) περιέχει τις πληροφορίες που μεταφέρονται από μια πηγή σε έναν προορισμό. Ο κυκλικός έλεγχος πλεονασμού 4 ψηφιολέξεων (CRC) προηγείται του οριοθέτη end of frame. Το CRC χρησιμοποιείται για να ανιχνεύσει λάθη μετάδοσης.

2.2.2. Clear text επικοινωνία

Η επικοινωνία μέσο καναλιού οπτικών ινών είναι clear-text. Η έλλειψη ασφάλειας στα διαφορετικά στρώματα των πλαισίων σε συνδυασμό με το γεγονός ότι η επικοινωνία είναι clear-text, επιτρέπει σε ορισμένες απειλές ασφάλειας να είναι πολύ επιτυχείς.

Η έλλειψη κρυπτογράφησης στο επίπεδο πλαισίων δεν είναι ένα σημαντικά αρνητικό ζήτημα, αν λάβουμε υπόψη μας τον αντίκτυπο που θα είχαμε στην απόδοση του δικτύου εάν όλα τα πλαίσια ήταν κρυπτογραφημένα. Επιπλέον, το sniffing είναι δύσκολο σε ένα κανάλι οπτικών ινών δεδομένου ότι μπορεί μόνο να πραγματοποιηθεί εάν μια συσκευή συνδέεται με έναν κόμβο στο δίκτυο αποθήκευσης δεδομένων ή εάν ένα switch της Cisco έχει κακόβουλα διαμορφωθεί έτσι ώστε να στέλνει την κυκλοφορία απομακρυσμένα σε ένα λογισμικό αποκαλούμενο Ethereal. Εντούτοις, η έλλειψη κρυπτογράφησης στοιχείων που περιέχουν ευαίσθητη πληροφορία μπορεί να επιτρέψει σε αναρμόδιους χρήστες να αποκτήσουν πρόσβαση σε πληροφορίες χρήσιμες για να ολοκληρώσουν μια επίθεση. Σημείο κλειδί για τους επιτυχείς επιτιθεμένους είναι η δυνατότητα να κάνουν επίθεση sniffing σε clear-text επικοινωνία, η οποία μπορεί να πραγματοποιηθεί με οποιαδήποτε συσκευή ανάλυσης κυκλοφορίας.

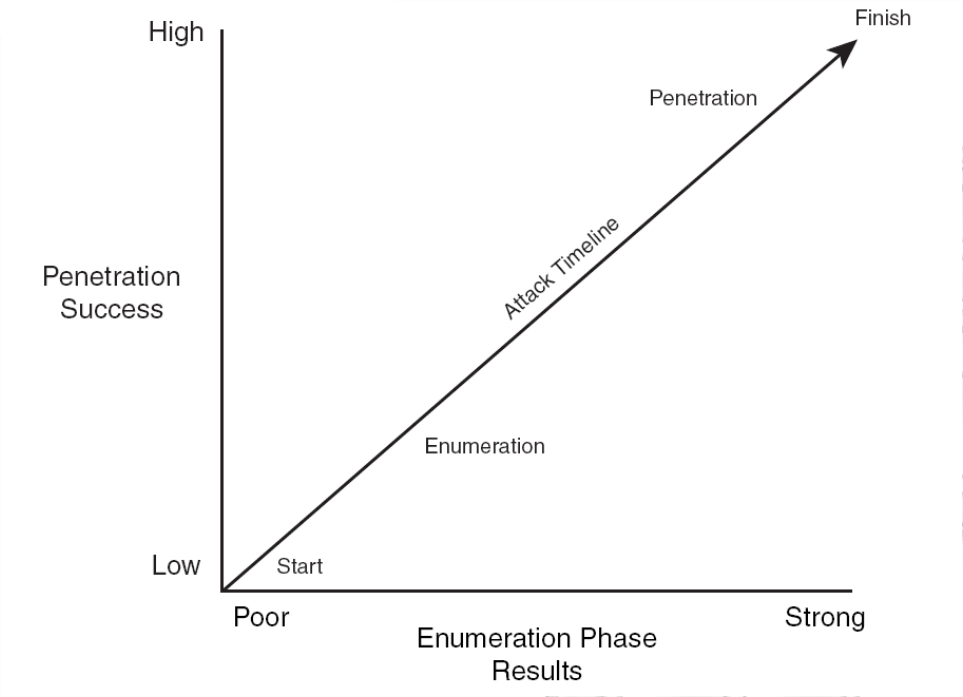
Η Clear-text επικοινωνία μπορεί να ικανοποιεί τα τεράστια ζητήματα απόδοσης και χωρητικότητας, αλλά εκθέτει επίσης ευαίσθητη πληροφορία σε κακόβουλες οντότητες. Τα cear-text πρωτόκολλα σε δίκτυα IP, όπως Rsh, Rsysnc, Rlogin, FTP, Telnet, SNMP, POP3, SMTP, ARP, iSCSI, επιτρέπουν στο να είναι πραγματοποιήσιμοι πολλοί τύποι επιθέσεων. Το γεγονός ότι η ευαίσθητη πληροφορία, όπως τα ονόματα χρήστη/κωδικός πρόσβασης, hashes, ή/και πληροφορίες δρομολόγησης, ανταλλάσσονται μέσο clear-text επικοινωνίας, επιτρέπει στους κακόβουλους χρήστες να υποκλέψουν ευαίσθητη πληροφορία χωρίς να κάνουν τίποτα παρά μόνο tapping της σύνδεσης.

Πολλοί IPv4 administrators αγνοούν την clear-text επικοινωνία λόγω της ψεύτικης αίσθησης ασφαλείας των switched δικτύων. Στα δίκτυα IP, η switch τεχνολογία καθιστά δυσκολότερο το να πραγματοποιηθεί sniffing εντούτοις, πολλές επιθέσεις, όπως η επίθεση της ενδιάμεσης οντότητας (MITM), μπορούν να υπονομεύσουν τα switched IP δίκτυα καθώς και τα switched FC δίκτυα.

Τα δίκτυα καναλιών οπτικών ινών μπορούν να χρησιμοποιήσουν τις FC-AL ή FC-SW τοπολογίες. Προκειμένου να πραγματοποιηθεί μια sniffing επίθεση σε ένα arbitrated loop δεν είναι απαραίτητη η MITM τεχνική μιας και πρόκειται για μια τοπολογία βρόχων (Ring), όπου κάθε συνδεδεμένος κόμβος στον ίδιο βρόχο μπορεί να δει την επικοινωνία του κάθε κόμβου με ένα άλλο μέσα στο βρόχο. Με τη χρησιμοποίηση παρόμοιων τεχνικών που χρησιμοποιούνται σε IPv4 δίκτυα το sniffing σε ένα δίκτυο καναλιών οπτικών ινών δεν είναι κάτι απραγματοποίητο, αλλά σημαντικά δυσκολότερο από ότι σε ένα IPv4 δίκτυο.

Ο κίνδυνος και οι αδυναμίες καναλιού ινών αρχίζουν με τη clear-text μετάδοση της ευαίσθητης πληροφορίας, η οποία οδηγεί άμεσα στην παρακολούθηση/καταγραφή (το πρώτο βασικό βήμα για έναν επιτιθέμενο). Η παρακολούθηση/καταγραφή είναι μια φάση όπου ένας αναρμόδιος χρήστης συγκεντρώνει τις πληροφορίες για το δίκτυο, την αρχιτεκτονική, τη συσκευή, ή την εφαρμογή που θέλει να εκθέσει. Το αποτέλεσμα από αυτήν την φάση είναι τα πραγματικά εργαλεία που χρησιμοποιούνται για να εκτελεστεί μια επίθεση.

Τα αποτελέσματα της φάσης παρακολούθησης/καταγραφής καθορίζουν το πόσο επιτυχής θα είναι μία επίθεση. Παραδείγματος χάριν, εάν κατά τη φάση παρακολούθησης/καταγραφής ο επιτιθέμενος συλλέξει σημαντικές πληροφορίες για το δίκτυο, συσκευές, εφαρμογές, λειτουργικά συστήματα, δρομολογητές, WWNs και IQNs, κατόπιν η φάση της διείσδυσης όχι μόνο θα είναι επιτυχής αλλά και πολύ πιο καταστρεπτική. Αντιθέτως, εάν η φάση παρακολούθησης/καταγραφής δεν παράγει τα αναμενόμενα αποτελέσματα για έναν επιτιθέμενο, η πραγματική φάση διείσδυσης θα είναι σύντομη και πιθανώς ανεπιτυχής.



Σχήμα 2.6 Σχέση μεταξύ φάσης παρακολούθησης/καταγραφής και πραγματοποίησης της επίθεσης.

Στο σχήμα 2.3, παρατηρούμε την άμεση σχέση μεταξύ των αποτελεσμάτων της φάσης παρακολούθησης/καταγραφής και της επιτυχίας επίθεσης. Όπως φαίνεται όσο περισσότερη επιτυχία έχουμε στη φάση παρακολούθησης/καταγραφής, η πιθανότητα της επιτυχίας στη διαδικασία επίθεσης αυξάνεται.

Ακολουθούν αναφορικά αρκετά από τα στοιχεία που ένας μη εξουσιοδοτημένος χρήστης μπορεί να υποκλέψει από έναν κόμβο που συνδέεται με το δίκτυο. Κάθε μια από αυτές τις πληροφορίες δίνει «πυρομαχικά» στον επιτιθέμενο για να ολοκληρώσει μια επιτυχή επίθεση:

- Όνομα δικτύου
- Πληροφορίες κεντρικού υπολογιστή ονομάτων του διακόπτη.
- Αριθμός ελέγχου ακολουθίας συνόδου
- Ταυτότητα ακολουθίας συνόδου
- World Wide Names που χρησιμοποιούνται στο δίκτυο
- Πληροφορίες πλαισίου στρώματος 2
- Διευθύνσεις 24-bit

- Πληροφορίες δρομολόγησης
- Πληροφορίες διαχείρισης

Καταλήγουμε στο συμπέρασμα ότι η παρακολούθηση/καταγραφή ενός καναλιού οπτικών ινών δεν σημαίνει απαραίτητα ότι θα αποκαλυφθεί ευαίσθητη πληροφορία, αλλά βοηθά σημαντικά τη διαδικασία επίθεσης.

2.3. Επιθέσεις δικτύων αποθήκευσης δεδομένων

Επίθεση σε ένα δίκτυο αποθήκευσής δεδομένων μεταφράζεται ως μη εξουσιοδοτημένη πρόσβαση είτε σε μια οντότητα ή σε δεδομένα σε ένα δίκτυο αποθήκευσης δεδομένων. Θα ακολουθήσει ανάλυση των παρακάτω επιθέσεων.

- Πειρατεία συνόδου (Session hijacking)
- Επιθέσεις ενδιάμεσης οντότητας (Man-in-the-Middle)
- Μεταβολή δεδομένων κεντρικών υπολογιστών ονομάτων (Name server pollution)
- Υποκλοπή και αντιγραφή World Wide Names
- LUN masking επιθέσεις
- Διαπίδυση ζωνών (Zone hopping)
- Επιθέσεις διακοπτών

Πίνακας 2.1 Αδυναμίες δικτύων αποθήκευσης δεδομένων και ο συσχετισμός με τις επιθέσεις.

Αδυναμίες	**Επιθέσεις**
Αδυναμίες ακολουθίας (Sequence weaknesses)	Πειρατεία συνόδου
Αδυναμίες διευθύνσεων (Fabric address weaknesses)	Επιθέσεις ενδιάμεσης οντότητας
FLOGI/PLOGI αδυναμίες	Μεταβολή δεδομένων κεντρικών υπολογιστών ονομάτων
Αδυναμίες Host Bus Adapter	LUN masking/ Υποκλοπή και αντιγραφή WWN
Αδυναμίες διακοπτών καναλιού οπτικών ινών	Διαπίδυση ζωνών

Κάτι βασικό που θα πρέπει να σημειώσουμε είναι η διαφορά μεταξύ μιας έγκυρης επίθεσης και ενός έγκυρου κινδύνου. Σε ένα δίκτυο, υπάρχουν αρκετές επιθέσεις που είναι δυνατόν να εκδηλωθούν, αλλά μόνο λίγες απ' αυτές μπορούν πραγματικά να θεωρηθούν επικίνδυνες λόγω της φύσης του δικτύου ή της επιχείρησης. Ως εκ τούτου, για κάθε επίθεση που περιγράφεται θα συζητείται το πόσο εύκολη ή δύσκολη είναι η εκτέλεση της και ποιο είναι το επίπεδο κινδύνου.

Οι αδυναμίες που θα αναλυθούν είναι οι εξής:

- Αδυναμίες ακολουθίας
- Αδυναμίες διευθύνσεων
- Αδυναμίες συνδέσεων δικτύου, θυρών και κόμβων
- Υποκλοπή και αντιγραφή FLOGI και PLOGI.

2.3.1. Αδυναμίες πλαισίων καναλιού οπτικών ινών

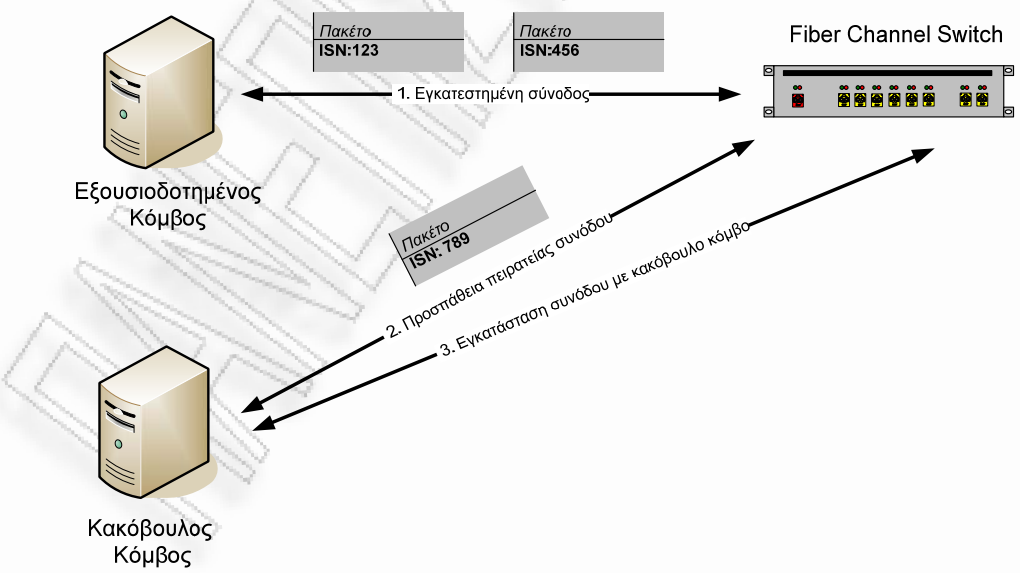
Στη συνέχεια συζητούνται οι αδυναμίες στο κανάλι οπτικών ινών στο επίπεδο πλαισίων.

2.3.1.1. Αδυναμίες ακολουθίας

Μια ακολουθία είναι ένα σύνολο πλαισίων που διαβιβάζονται αμφίδρομα από μια οντότητα σε μια άλλη προκειμένου να διατηρηθεί μια σύνοδος μεταξύ δύο κόμβων. Κάθε πλαίσιο έχει μια ταυτότητα ακολουθίας (Seq_ID) και μια αρίθμηση ακολουθίας (Seq_CNT) προκειμένου να αναγνωρίζεται, ελέγχεται και να διατηρείται η σύνοδος. Η ταυτότητα ακολουθίας (Seq_ID) που προσδιορίζει τη μοναδική σύνοδο που ανήκει το κάθε πλαίσιο. Παραδείγματος χάριν, εάν ένας κόμβος επικοινωνούσε με διάφορες διαφορετικές οντότητες, κάθε σύνοδος θα είχε ένα μοναδικό Seq_ID για να προσδιορίσει ποιο πλαίσιο ανήκει σε ποια σύνοδο. Εκτός από την ταυτότητα ακολουθίας, η αρίθμηση ακολουθίας χρησιμοποιείται επίσης για να εξασφαλίσει ότι τα πλαίσια τοποθετούνται στη σωστή σειρά από τις οντότητες. Το Seq_CNT αυξάνεται κατά 1 για κάθε επόμενο πλαίσιο της ίδιας συνόδου.

Η ταυτότητα ακολουθίας και η αρίθμηση ακολουθίας έχουν παρόμοια χρήση με τον αρχικό αριθμό ακολουθίας (Initial Sequence Number ISN) σε ένα πακέτο IP. Το ISN σε ένα πακέτο IP είναι επίσης η παράμετρος για τη διατήρηση μιας συνόδου μεταξύ δύο κόμβων σε ένα δίκτυο IP.

Για να διατηρηθεί μια σύνοδος μεταξύ δύο κόμβων, πρέπει να διατηρηθούν και όλες οι πληροφορίες της συνόδου. Η αδυναμία ασφάλειας με τα δίκτυα IP είναι το προβλέψιμο (εικάσιμο) ISN. Το ISN είναι το μέσο εκείνο που επιτρέπει σε ένα πακέτο να είναι κομμάτι μιας συνόδου. Εάν το ISN ήταν προβλέψιμο, θα επέτρεπε ενδεχομένως σε μη εξουσιοδοτημένα πακέτα να εισέλθουν σε μία σύνοδο. Μια τρίτη οντότητα θα μπορούσε να εισάγει πακέτα με το σχετικό ISN και να πάρει τον έλεγχο της συνόδου. Παραδείγματος χάριν, εάν υποθέσουμε ότι στα δύο από τα πρώτα τρία πακέτα σε μια σύνοδο έχουμε το ISN 123 για το πακέτο ένα και το 456 για το πακέτο δύο. Ένας επιτιθέμενος θα μπορούσε πιθανώς να προβλέψει ότι το τρίτο πακέτο πρέπει να έχει ένα ISN 789 για να είναι μέρος της υπάρχουσας συνόδου. Εάν ο επιτιθέμενος στείλει το πακέτο στο στόχο πρώτος και χρησιμοποιήσει το ISN 789, η σύνοδος θα παραδοθεί έπειτα στον επιτιθέμενο και όχι στο νόμιμο κόμβο. Αυτό σημαίνει ότι εάν μια οντότητα ήταν σε θέση να υποθέσει το επόμενο ISN στην ακολουθία και η οντότητα ήταν σε θέση να αποστείλει πακέτα σε μια σύνοδο, η οντότητα αυτή θα είχε τον έλεγχο της συνόδου.

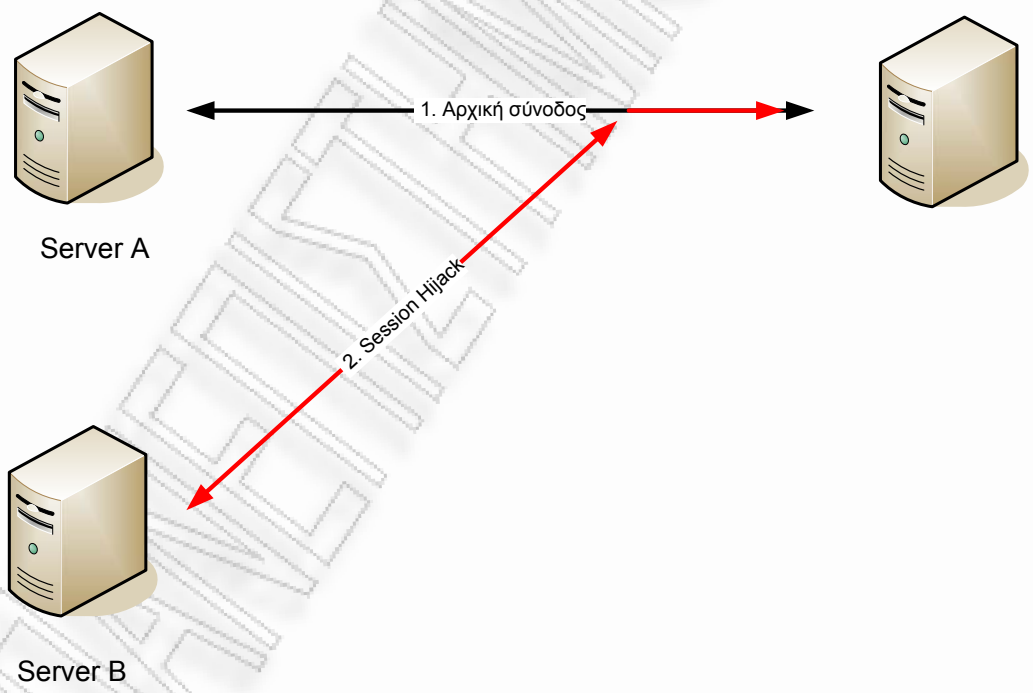


Σχήμα 2.7 Επίθεση πειρατείας συνόδου με χρήση ISN

Όπως φαίνεται στο σχήμα 2.7, ένα αδύναμο ή προβλέψιμο ISN μπορεί να καταστήσει μια σύνοδο τρωτή σε μια επίθεση πειρατείας συνόδου. Οι τιμές ISN πρέπει να είναι απρόβλεπτες και μοναδικές και όχι απρόβλεπτες ή μοναδικές.

2.3.1.2. Πειρατεία συνόδου

Η πειρατεία συνόδου είναι η πράξη μίας μη έμπιστης τρίτης οντότητας που παρεμποδίζει ή ελέγχει (πειρατεία) μια εγκατεστημένη σύνοδο μεταξύ δύο εμπίστων οντοτήτων. Το Telnet είναι ένα καλό παράδειγμα μιας έμπιστης συνόδου μεταξύ δύο οντοτήτων που μπορούν να δεχθούν επίθεση από έναν τρίτο εάν χρησιμοποιούνται προβλέψιμα ISNs για τα TCP πακέτα.



Σχήμα 2.8 Παράδειγμα πειρατείας συνόδου μεταξύ δύο εμπίστων οντοτήτων

Η πειρατεία συνόδου εμφανίστηκε πριν από πολλά χρόνια στα IP δίκτυα με τους προβλέψιμους αρχικούς αριθμούς ακολουθίας στα TCP headers των πακέτων IP.

Η επίθεση έγινε αρκετά εύκολο να εκτελεστεί με τα εργαλεία όπως το Hunt (http://lin.fsid.cvut.cz/~kra/#HUNT) και Ettercap (http://ettercap.source-forge.net/).

Η πειρατεία συνόδου ήρθε πάλι στην επιφάνεια όταν αδύναμα και προβλέψιμα IDs συνόδου χρησιμοποιήθηκαν στα cookies εφαρμογών που χρησιμοποιούνται στην επικοινωνία στο web (HTTP).

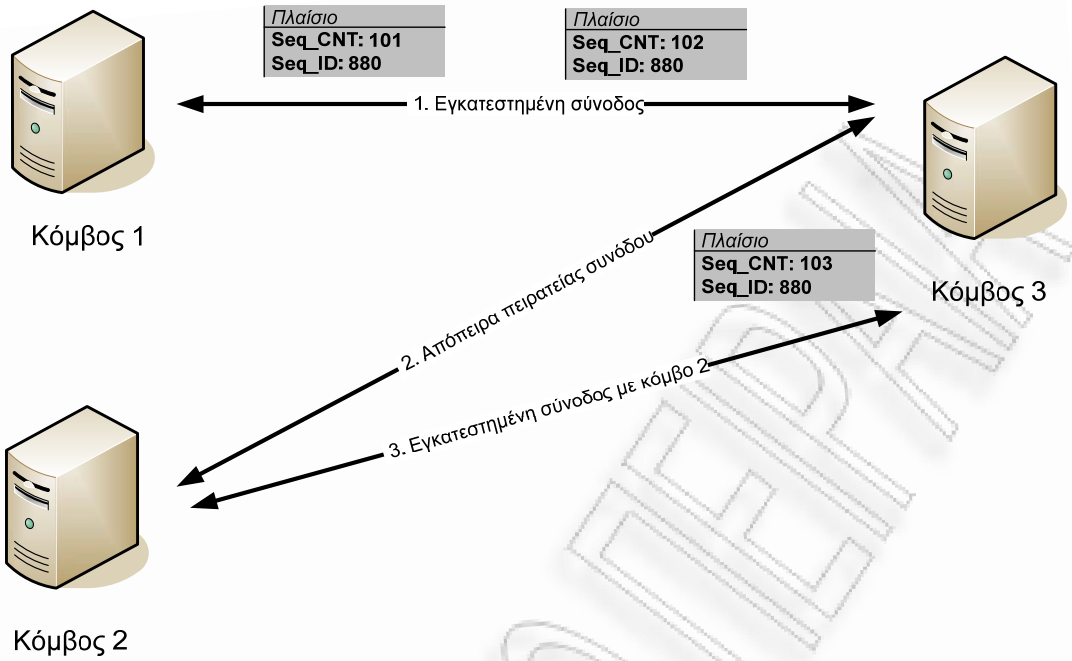
Όπως έχει αναφερθεί ήδη οι επιθέσεις δεν αλλάζουν, αλλά τροποποιούνται, έτσι και η πειρατεία συνόδου μπορεί να εφαρμοστεί στα πλαίσια καναλιού οπτικών ινών.

2.3.1.3. Πειρατεία συνόδου – Οπτικό κανάλι

Στην αρχιτεκτονική οπτικού καναλιού για να επικοινωνούν δύο κόμβοι μεταξύ τους θα πρέπει να έχει εγκατασταθεί μία σύνοδος. Οι πληροφορίες συνόδου ρυθμίζονται από τον μετρητή της ακολουθίας (SEQ_CNT) και την ταυτότητα ακολουθίας (SEQ_ID).

Οι πληροφορίες συνόδου μεταξύ δύο κόμβων FC είναι υπεύθυνες για τη διατήρηση μιας συνόδου. Παραδείγματος χάριν, εάν 100 πλαίσια παραδόθηκαν από διάφορους κόμβους σε έναν κόμβο, πρέπει να διαχωριστεί ποιο πλαίσιο προήλθε από ποιο κόμβο και να τοποθετηθούν τα πλαίσια στη σωστή διάταξή τους. Το Seq_ID και το Seq_CNT θα συσχετίσουν κάθε πλαίσιο σε μια συγκεκριμένη σύνοδο και θα το τοποθετήσουν στη σωστή διάταξή του.

Το ζήτημα με τη διαχείριση της συνόδου αρχίζει με την έλλειψη επικύρωσης κατά την αποστολή ή τη λήψη των πλαισίων. Προκειμένου να επιτεθεί σε μία σύνοδο, ένας κακόβουλος χρήστης, θα μπορούσε να στείλει πλαίσια σε έναν εξουσιοδοτημένο κόμβο με τα σωστά Seq_ID και Seq_CNT (χρησιμοποιώντας τη διεύθυνση προέλευσης (S_ID) του και όχι αυτή του εξουσιοδοτημένου χρήστη), μεταφέροντας έτσι τον έλεγχο της συνόδου στα χέρια του. Επιπλέον, δεδομένου ότι το Seq_ID δεν αλλάζει ποτέ (που το καθιστά πολύ εύκολο να βρεθεί) και η αύξηση του μετρητή Seq_CNT κατά ένα (που το καθιστά πολύ εύκολο να προβλεφθεί) η διαδικασία πειρατείας συνόδου είναι αρκετά τετριμμένη.



Σχήμα 2.9 Τοπολογία πειρατείας συνόδου

Αν και η επίθεση είναι πολύ τετριμμένη, όπως καταδεικνύεται με εφαρμογές IP/Hunt, Ιστού και session identifiers, αυτήν την περίοδο δεν υπάρχει κανένα αυτοματοποιημένο εργαλείο που να εκτελεί αυτόν τον τύπο επίθεσης. Μια συσκευή ανάλυσης καναλιού οπτικών ινών θα έπρεπε να χρησιμοποιηθεί προκειμένου να εκτελεστεί αυτού του είδους η επίθεση σε FC πλαίσια, κάτι που καθιστά την επίθεση ως υψηλής απειλής όσο αφορά την ασφάλεια, αλλά χαμηλού κινδύνου.

2.3.1.4. Πειρατεία συνόδου – Σύνοψη επιθέσεως

Περιγραφή επίθεσης - Πειρατεία μιας συνόδου με την εικασία του αριθμού ελέγχου ακολουθίας (SEQ_CNT) και του αριθμού αναγνώρισης ακολουθίας (SEQ_ID) ενός πλαισίου καναλιών ινών.

Επίπεδο κινδύνου - Υψηλό. Μια αναρμόδια οντότητα θα μπορούσε να αποκτήσει πρόσβαση σε μια εξουσιοδοτημένη σύνοδο ή να τροποποιήσει απλά τους αριθμούς ακολουθίας τυχαία και να προσπαθήσει να εκτελέσει μια επίθεση άρνησης υπηρεσιών (Dos).

Δυσκολία - Υψηλή. Είναι μια περίπλοκη επίθεση που απαιτεί τη βαθιά γνώση των πλαισίων καναλιού οπτικών ινών και τη χρήση συσκευής ανάλυσης κυκλοφορίας υλικού και λογισμικού.

Best practice - Καμία μέχρι σήμερα εντούτοις, η χρήση ισχυρού ή απρόβλεπτου SEQ_CNT ή SEQ_ID θα μετρίαζε τον κίνδυνο αυτό και μελλοντικά.

2.3.2. Αδυναμίες διευθύνσεων καναλιού οπτικών ινών

Η πλαστογράφηση μίας 24bit fabric διεύθυνσης μπορεί να προκαλέσει σημαντικά προβλήματα και DoS σε ένα δίκτυο.

Κάθε κόμβος σε ένα δίκτυο έχει μια 24bit fabric διεύθυνση που χρησιμοποιείται, μεταξύ άλλων, για τη δρομολόγηση. Μαζί με την δρομολόγηση των πλαισίων σωστά από/προς την πηγή και τον προορισμό, η διεύθυνση αυτή χρησιμοποιείται επίσης για τις πληροφορίες ονομάτων κεντρικών υπολογιστών (Name Server Information). Η NSI είναι μια λογική βάση δεδομένων σε κάθε FC switch που συσχετίζει τη 24bit fabric διεύθυνση ενός κόμβου με το 64bit WWN του. Επιπλέον, η NSI είναι επίσης αρμόδια για τη χαρτογράφηση (mapping) της 24bit fabric διεύθυνσης και του 64bit WWN στα εξουσιοδοτημένα LUNs (Logical Unit Numbers) σε ένα δίκτυο αποθήκευσης δεδομένων. Επιπλέον, οι NSIs χρησιμοποιούνται επίσης για soft και hard zoning. Η 24bit fabric διεύθυνση ενός κόμβου καθορίζει τις λειτουργίες δρομολόγησης με τις soft και hard zonings, συγκεκριμένα εάν ένα πλαίσιο επιτρέπεται να περάσει από μια ζώνη σε μια άλλη. Ενώ υπάρχουν και άλλες χρήσεις της 24bit διεύθυνσης, η χρήση της διεύθυνσης στις NSI και στις διαδικασίες zoning είναι κατά πολύ οι σημαντικότερες από την άποψη της ασφάλειας.

Το σημαντικό με τη 24bit διεύθυνση είναι ότι χρησιμοποιείται για λόγους ταυτοποίησης (identification), στις NSI και για soft/hard zoning δρομολόγηση, σχεδόν όπως μια διαδικασία αυθεντικοποίησης, αλλά είναι μια οντότητα που μπορεί εύκολα ένας κακόβουλος χρήστης να αντιγράψει. Χρησιμοποιώντας οποιαδήποτε συσκευή ανάλυσης κυκλοφορίας, η διεύθυνση προέλευσης 24bit ενός πλαισίου καναλιών ινών θα μπορούσε να υποκλαπεί δεδομένου ότι εκτελεί διαδικασίες και PLOGI (Port Login) και FLOGI (Fabric Login).

Στο κανάλι οπτικών ινών υπάρχουν τρεις διαφορετικοί τρόποι για σύνδεση:

- Port Login (PLOGI)
- Fabric Login (FLOGI)

και

- Node Login (NLOGI)

Δύο από αυτούς μπορούν να υποστούν επίθεση με την αντιγραφή μίας 24bit διεύθυνσης.

2.3.2.1. Fabric Login, Port Login και Node Login

Η διαδικασία Fabric Login (FLOGI) επιτρέπει σε έναν κόμβο να συνδεθεί στο δίκτυο και να λάβει μια ορισμένη διεύθυνση από ένα switch. Το FLOGI συμβαίνει με τον κάθε κόμβο (N_Port ή NL_Port) που είναι συνδεμένος με το fabric. Το N_Port ή το NL_Port θα πραγματοποιήσει FLOGI με ένα κοντινό switch. Ο κόμβος (N_Port ή NL_Port) θα στείλει ένα πλαίσιο FLOGI που θα περιέχει το όνομα του, το όνομα του N_Port του, και οποιεσδήποτε παραμέτρους υπηρεσιών. Όταν ο κόμβος στέλνει τις πληροφορίες του στη διεύθυνση 0xFFFFFE, χρησιμοποιεί τη διεύθυνση προέλευσης 24bit 0x000000 επειδή δεν έχει λάβει ακόμα μια νόμιμη διεύθυνση 24bit από το fabric. Το FLOGI θα σταλεί στη γνωστή διεύθυνση 0xFFFFFE, η οποία είναι παρόμοια με τη διεύθυνση broadcast μετάδοσης σε ένα δίκτυο IP. Τα FC switches και το δίκτυο θα λάβουν το FLOGI στη διεύθυνση 0xFFFFFE. Αφότου λάβει ένα switch το FLOGI, θα δώσει στο N_Port ή το NL_Port μία 24bit διεύθυνση που να σχετίζεται με το δίκτυο. Αυτή η διεύθυνση 24bit σχετίζεται με το μοναδικό Domain name του δικτύου, το μοναδικό area name που βρίσκεται το switch και το Port που είναι η μοναδική ονομασία κάθε πόρτας του switch.

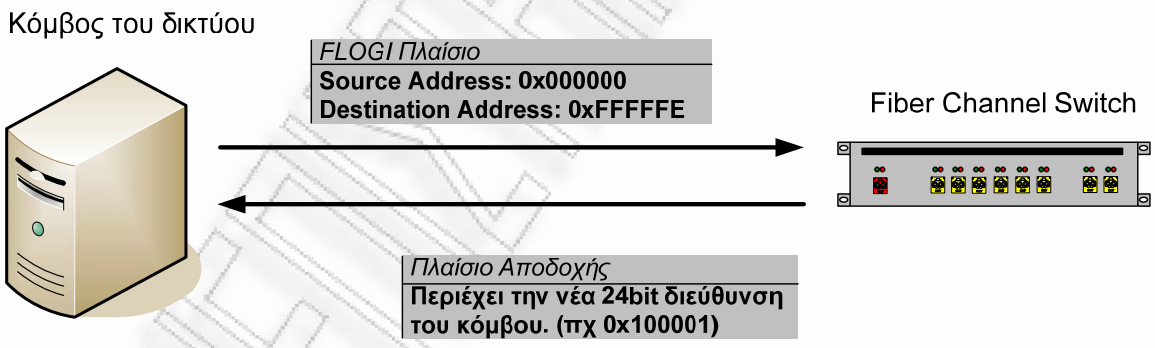
Πίνακας 2.2 Τα τμήματα μιας 24bit fabric διεύθυνσης

Περιγραφή τμημάτων διευθύνσεως 24-Bit	
8-bit domain name	Μοναδικό domain ID σε ένα δίκτυο. Αποδεκτά domain IDs μεταξύ 1 και 239.
8-bit area name	Μοναδικό area ID ενός διακόπτη του δικτύου. Αποδεκτά area IDs μεταξύ 0 και 255.
8-bit port name	Μοναδικό port ID του διακόπτη. Αποδεκτά port IDs μεταξύ 0 και 255.

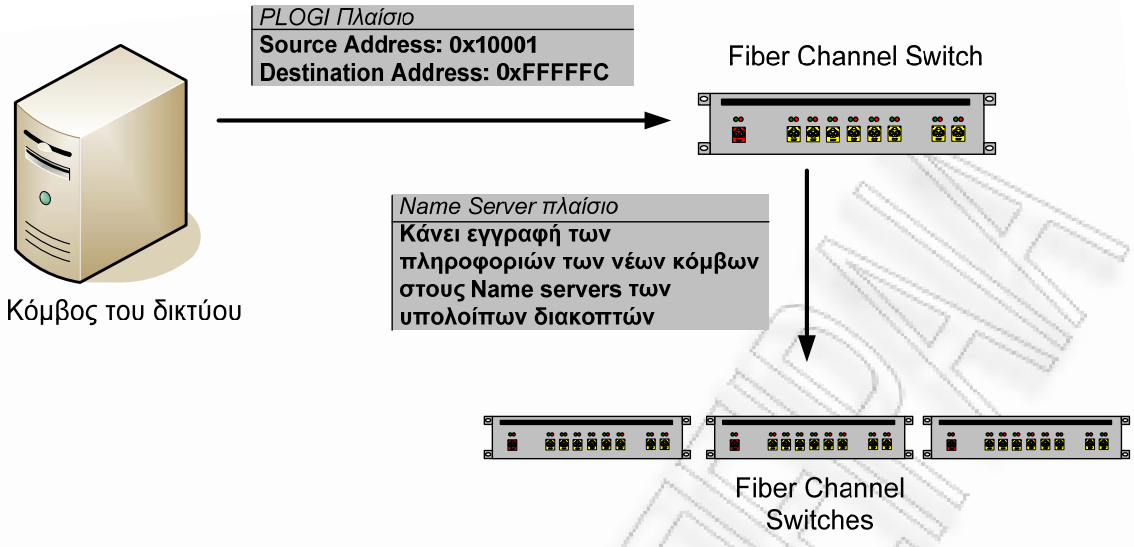
Προκειμένου να υπολογιστεί μία 24-bit address (port ID) χρησιμοποιείται η παρακάτω φόρμουλα.

Domain_ID x 65536 + Area_ID x 256 + Port_ID = 24 bit Address

Αφότου έχει ολοκληρώσει ο κόμβος το FLOGI και έχει μια έγκυρη διεύθυνση 24bit, θα εκτελέσει μια Port Login (PLOGI) στη γνωστή διεύθυνση 0xFFFFFC για να καταχωρήσει τη νέα διεύθυνση του στον name server του switch, καθώς επίσης και να υποβάλει τις πληροφορίες που αφορούν τα 64-bit port WWN, 64-bit node WWN, port type και class of service. Το switch έπειτα καταχωρεί τη διεύθυνση, μαζί με όλες τις άλλες πληροφορίες που υποβάλλονται, στον name server και αντιγραφει τις πληροφορίες και σε άλλους name servers στο δίκτυο.



Σχήμα 2.10 FLOGI



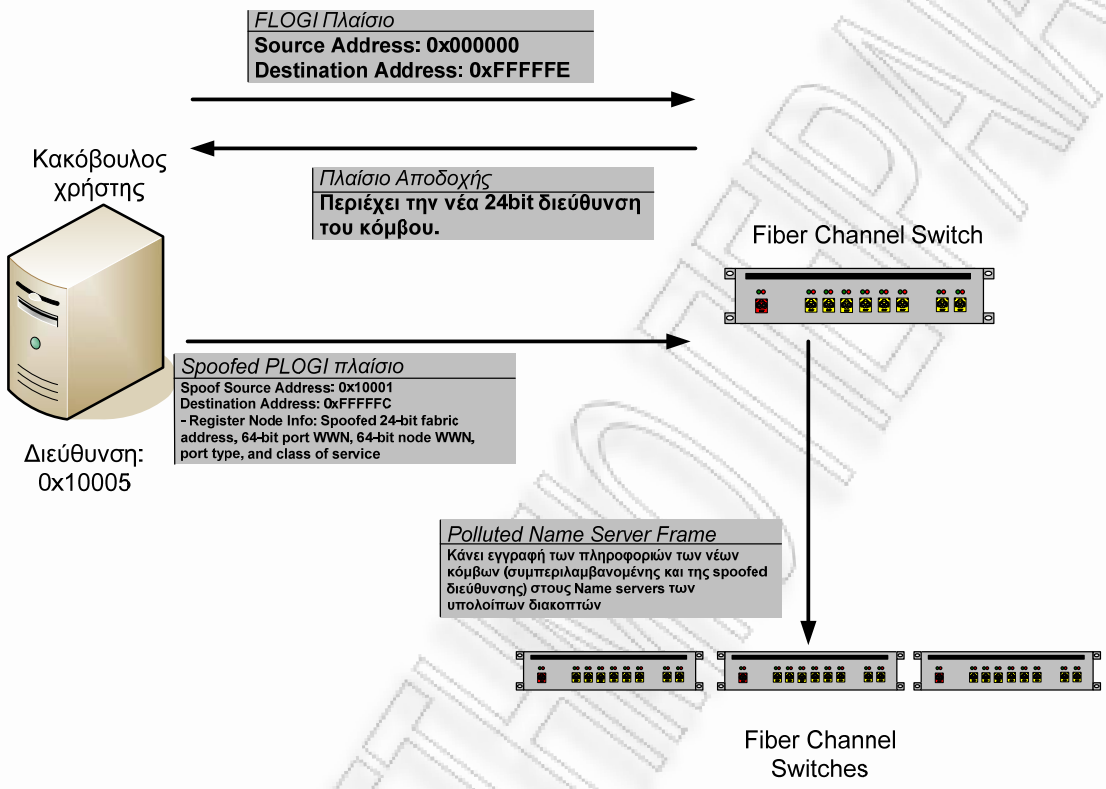
Σχήμα 2.11 PLOGI.

Ένα Node Login είναι κάπως παρόμοιο με Fabric Login, αλλά αντί να συνδεθεί ένας κόμβος με το δίκτυο, ο κόμβος συνδέεται σε έναν άλλο κόμβο άμεσα (node to node). Ο κόμβος δεν θα λάβει πληροφορίες που αφορούν το δίκτυο, αλλά θα λάβει τις πληροφορίες από τον άλλο κόμβο που θα αφορούν την ανταλλαγή IDs (OX_ID και RX_ID) και τις πληροφορίες συνόδου (Seq_ID και Seq_CNT). Αφότου έχουν ανταλλαχθεί αυτές οι πληροφορίες, οι δύο κόμβοι θα αρχίσουν να επικοινωνούν ο ένας με τον άλλον άμεσα.

2.3.2.2. FLOGI, PLOGI και address spoofing

Μετά την εκτέλεση της διαδικασίας FLOGI, ένας κόμβος FC πρέπει να εκτελέσει ένα PLOGI στη γνωστή διεύθυνση 0xFFFFFC. Το PLOGI καταχωρεί έπειτα τη διεύθυνση του κόμβου στον name server του switch. Εάν μια οντότητα επρόκειτο να κάνει spoof την διεύθυνση του και να την στείλει στη διεύθυνση 0xFFFFFC, τα switches αυτό που θα έβλεπαν θα ήταν έναν κόμβο να προσπαθεί να κάνει PLOGI. Μόλις λάβει το switch τις πληροφορίες από το πλαίσιο PLOGI, θα καταχωρήσει τη spoofed διεύθυνση του κόμβου στον name server, έτσι μολύνει τον κεντρικό υπολογιστή ονομάτων (name server pollution) με τις ανακριβείς πληροφορίες. Η απλή αυτή διαδικασία δίνει στον επιτιθέμενο τη δυνατότητα να

δρομολογηθεί (hop) σε ζώνες στις οποίες δεν θα μπορούσε να στείλει πακέτα λόγω hard και soft zoning rules.



Σχήμα 2.12 FLOGI/PLOGI spoofing.

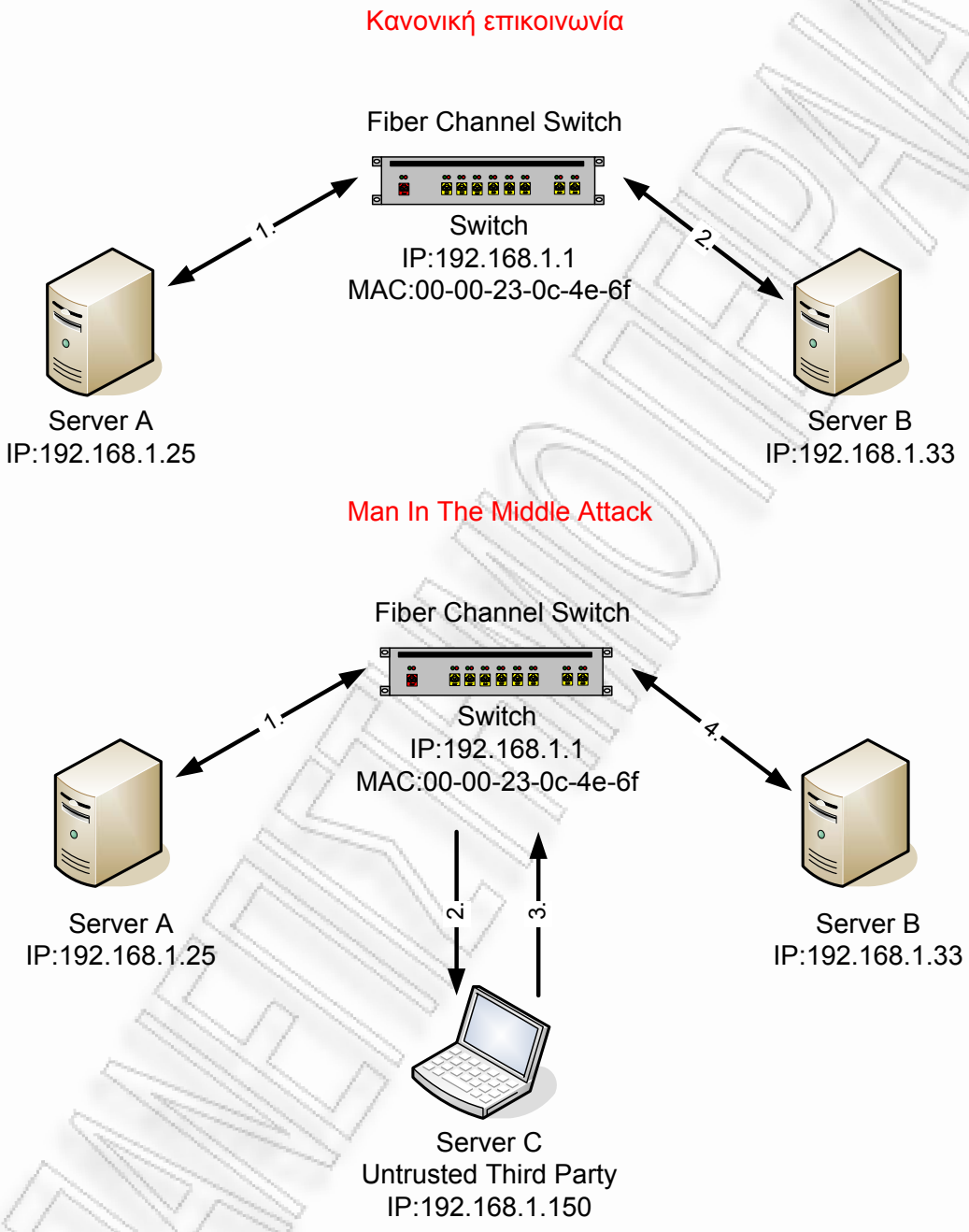
Γεγονός είναι ότι αυτή η επίθεση είναι πολύ ισχυρή και μπορεί να παρακάμψει οποιουσδήποτε κανόνες hard ή soft zoning. Εντούτοις, μια συσκευή ανάλυσης κυκλοφορίας απαιτείται για να εκτελεστεί αυτή η επίθεση, κάτι που καθιστά την εκτέλεση της σχετικά δύσκολη.

2.3.3. Επιθέσεις ενδιάμεσης οντότητας (Man In The Middle Attacks)

Μια επίθεση ενδιάμεσης οντότητας (MITM) είναι η πράξη υποκλοπής, από μία κακόβουλη οντότητα, μιας επικοινωνίας μεταξύ δύο εμπίστων οντοτήτων.

Στον ψηφιακό κόσμο, τον ρόλο της κακόβουλης οντότητας διαδραματίζει ένας δρομολογητής ο οποίος, αντίθετα από έναν εξουσιοδοτημένο δρομολογητή, δεν

θα έπρεπε να έχει άδεια πρόσβασης, τροποποίησης, παρακολούθησης οποιασδήποτε επικοινωνίας μεταξύ των δύο έμπιστων οντοτήτων.



Σχήμα 2.13 Παράδειγμα Man-in-the-Middle επίθεσης.

Οι Man-in-the-Middle επιθέσεις εμφανίστηκαν αρχικά πριν από πολλά χρόνια στον κόσμο των IP δικτύων. Μη αυθεντικοποιημένα OSI layer 2 Address Resolution

Protocol (ARP) πακέτα μπορούσαν να ανανεώσουν τις πληροφορίες ARP πινάκων (πίνακες που αντιστοιχούν IPs κόμβων με τα MAC addresses των μηχανημάτων τους) σε switches ή/και σε λειτουργικά συστήματα. Ο σκοπός του MITM είναι να κάνει sniffing σε ένα switch. Ένα switch διαβιβάζει τις πληροφορίες μόνο στο σωστή πόρτα, μην επιτρέποντας σε πόρτες να δουν πληροφορία που δεν απευθύνεται σε αυτές. Απ' την άλλη, ένα hub είναι μια συσκευή λιγότερο έξυπνη που επιτρέπει σε όλες τις πόρτες να δουν όλη την επικοινωνία, κάτι που καθιστά αρκετά εύκολο να γίνει sniffing στην κυκλοφορία ενός «γείτονα». Πολλά switches είναι layer 2 συσκευές, που σημαίνει ότι μπορούν να διαβιβάσουν πακέτα από μία πόρτα ενός switch σε μια άλλη πόρτα κάποιου άλλου switch χωρίς την χρήση μιας IP διεύθυνσης, αλλά με τη MAC διεύθυνση της συσκευής του κόμβου. Η layer 2 δρομολόγηση είναι κάτι κοινό για λόγους απόδοσης, αφού επιτρέπει στα πακέτα να κινούνται γρήγορα μέσα στο δίκτυο. Μόλις φτάσουν τα πακέτα σε μία layer 3 συσκευή (router) κατόπιν χρησιμοποιείται η διεύθυνση IP του κόμβου.

Δεδομένου ότι το ARP είναι ένα layer 2 πρωτόκολλο, χρησιμοποιεί τη MAC διεύθυνση κόμβου για να προσδιορίσει τους κόμβους και να μεταφέρει τα πακέτα. Το ARP είναι παρόμοιο με τους Name Servers σε ένα οπτικό κανάλι, όπου οι Name Servers συσχετίζουν το World Wide Name (WWN) του Host Bus Adapter (HBA) με την 24bit fabric διεύθυνση (καθώς επίσης και μερικά άλλα στοιχεία, όπως τις ζώνες και την Logical Unit Number (LUN) πρόσβαση).

2.3.3.1. Επιθέσεις ενδιάμεσης οντότητας IP δικτύων

Μια οντότητα που χρησιμοποιεί μια IP, όπως ένα switch ή ένα λειτουργικό σύστημα, θα στείλει ARP αιτήματα όταν προσπαθεί να επικοινωνήσει με άλλες οντότητες. Παραδείγματος χάριν, εάν ο κεντρικός υπολογιστής Α θελήσει να επικοινωνήσει με τον κεντρικό υπολογιστή Β, ο οποίος έχει τη διεύθυνση IP 172.16.1.1 και τη διεύθυνση MAC 00-0A-CC-69-89-74, ο κεντρικός υπολογιστής Α θα έστελνε ένα ARP αίτημα, το « Who is 172.16.1.1?» Κατόπιν το switch ή το λειτουργικό σύστημα θα αποκρινόταν, στέλνοντας τη MAC διεύθυνσή του, η οποία είναι 00-0A-CC-69-89-74. Το πρόβλημα με το ARP, που θα εξετάσουμε και με τους Name servers καναλιού οπτικών ινών, είναι ότι οποιαδήποτε κακόβουλη οντότητα θα μπορούσε να στείλει μια ARP απάντηση αντί του πραγματικού κεντρικού

υπολογιστή. Έτσι δουλεύει το ARP, χωρίς οποιαδήποτε αυθεντικοποίηση. Ένας κακόβουλος χρήστης θα μπορούσε να στείλει ARP απαντήσεις με τις ανακριβείς πληροφορίες. Δεδομένου ότι δεν υπάρχει αυθεντικοποίηση στο ARP, όπως και στο PLOGI στο fabric οπτικών καναλιών, μια οντότητα που λαμβάνει μια ARP απάντηση από έναν επιτιθέμενο θα ενημέρωνε τον πίνακα δρομολόγησής της με ανακριβείς πληροφορίες. Επιπλέον, ακόμα κι αν ένας νόμιμος κόμβος δεν έστειλε ένα ARP αίτημα, το οποίο θα ζητούσε τη διεύθυνση της MAC μιας συγκεκριμένης διεύθυνσης IP, δεν σημαίνει ότι δεν θα λάβει μια ARP απάντηση ενός κακόβουλου χρήστη και δεν θα ενημερώσει τον πίνακα δρομολόγησής του. Παραδείγματος χάριν, ένας κακόβουλος χρήστης θα μπορούσε να στείλει ARP απαντήσεις σε ολόκληρο το δίκτυο, λέγοντας σε κάθε οντότητα ότι η MAC διεύθυνση του δρομολογητή, που είναι το 172.16.1.1, είναι πραγματικά η MAC διεύθυνση της κακόβουλης οντότητας. Όταν λοιπόν ένας κόμβος προσπαθήσει να επικοινωνήσει με οποιοδήποτε άλλο κόμβο περνώντας αρχικά από τον προεπιλεγμένο δρομολογητή, θα δρομόλογείται, στην πραγματικότητα, πρώτα στην κακόβουλη οντότητα, δεδομένου ότι χρησιμοποιεί τη MAC διεύθυνση της κακόβουλης οντότητας.

2.3.3.2. Επιθέσεις ενδιάμεσης οντότητας καναλιού οπτικών ινών

Στα Fibre Channel fabrics, οι Man-in-the-Middle επιθέσεις είναι πιο δύσκολες απ' ότι στα IP Networks και έτσι υπάρχει μικρότερος κίνδυνος. Παρόλα αυτά ο κίνδυνος και οι αδυναμίες είναι υπαρκτές.

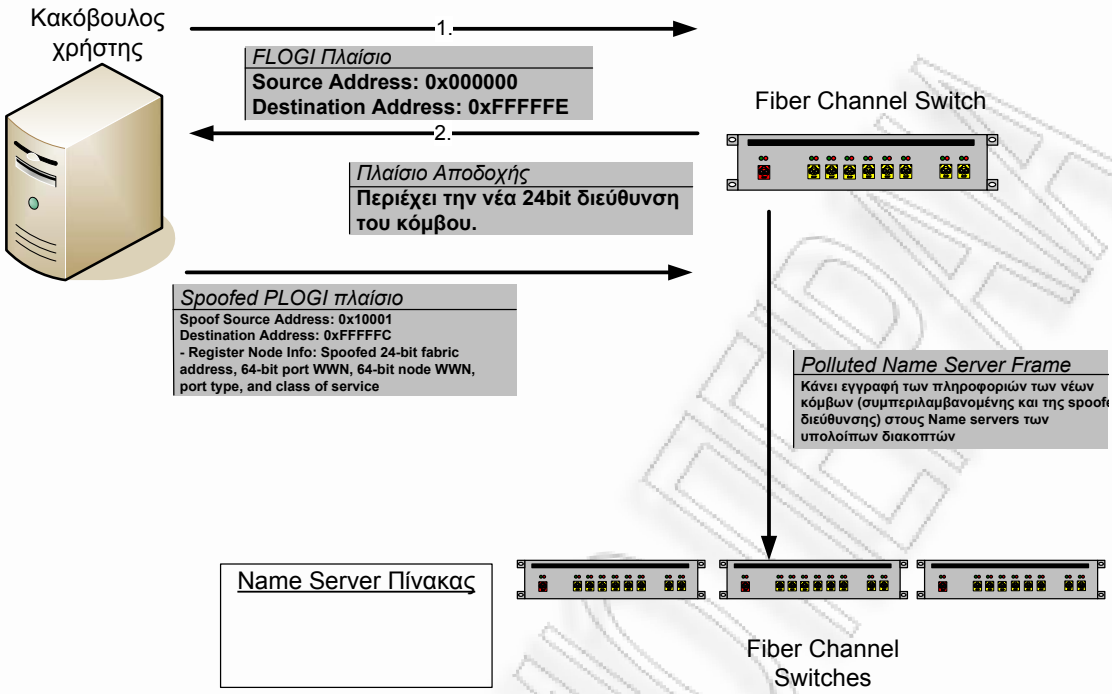
2.3.3.3. Μόλυνση κεντρικών υπολογιστών ονομάτων

Προκειμένου να πραγματοποιηθεί μια MITM επίθεση σε ένα δίκτυο καναλιού οπτικών ινών, προαπαιτείται η Name server Pollution επίθεση. Όπως περιγράψαμε νωρίτερα, υπάρχουν σημαντικές αδυναμίες στις διαδικασίες FLOGI και PLOGI που μπορούν να χρησιμοποιηθούν για να μολύνουν τον κεντρικό υπολογιστή ονομάτων Name Server.

Κατά την εκτέλεση ενός FLOGI, ένας κόμβος θα χρησιμοποιήσει τη διεύθυνση προέλευσης 0x000000 επειδή δεν έχει ένα έγκυρο S_ID ακόμα. Ο κόμβος

θα στείλει το πλαίσιό του στη διεύθυνση προορισμού (D_ID) 0xFFFFFE. Αφότου λάβουν τα switches το πλαίσιο στη διεύθυνση 0xFFFFFE, θα επιστρέψουν ένα Accept πλαίσιο, γνωστό ως ACC, στον κόμβο με τη νέα 24bit διεύθυνση του, που δίνει στον κόμβο μια έγκυρη fabric διεύθυνση. Αφότου έχει λάβει ο κόμβος το πλαίσιο ACC και τη νέα διεύθυνση του, θα εκτελέσει έπειτα ένα PLOGI. Στο PLOGI θα στείλει τη νέα διεύθυνση του στη διεύθυνση 0xFFFFFC, που καταχωρεί τη νέα διεύθυνσή του στους Name Server του switch.

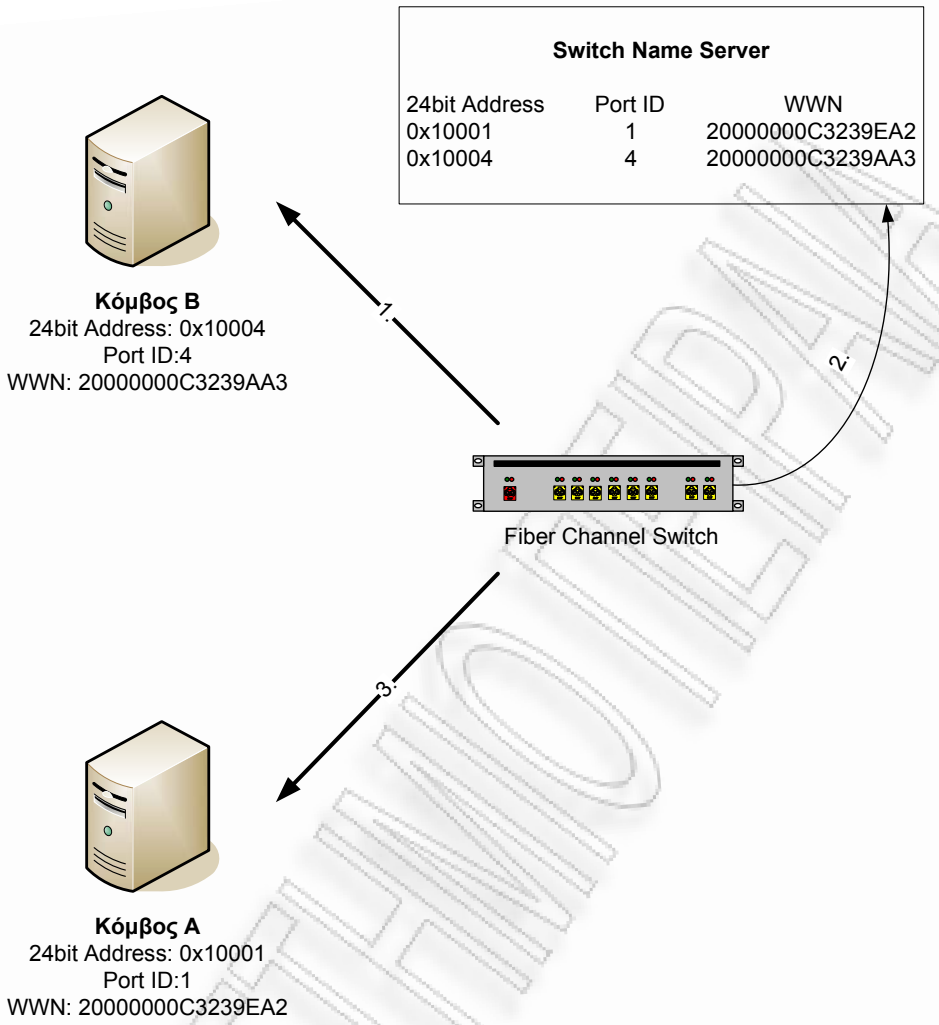
Η αδυναμία ασφάλειας είναι ότι ένας κακόβουλος κόμβος μπορεί να επεξεργαστεί ένα πλαίσιο PLOGI και να το στείλει στη διεύθυνση 0xFFFFFC. Ο κακόβουλος κόμβος θα μπορούσε να ολοκληρώσει τη διαδικασία FLOGI, αλλά αντί να απαντήσει με την πραγματική διεύθυνση του, θα μπορούσε να χρησιμοποιήσει μία 24bit διεύθυνση ενός στόχου κατά τη διάρκεια του PLOGI. Δεδομένου ότι ο κακόβουλος κόμβος ξέρει τη διεύθυνση όπου θα στέλνει τις απαντήσεις PLOGI (0xFFFFFC), η πράξη της παρεμβολής της 24bit διεύθυνσης δεν είναι κάτι δύσκολο. Ο Name server των switches θα λάμβανε το spoofed PLOGI πλαίσιο στη διεύθυνση 0xFFFFFC και θα ενημέρωνε τον Name server του με τις ανακριβείς πληροφορίες. Σε μια επίμονη επίθεση, ο κακόβουλος κόμβος θα συνέχιζε να στέλνει τα πλαίσια PLOGI στη διεύθυνση 0xFFFFFC, συνεχώς ενημερώνοντας τον Name server με ανακριβείς πληροφορίες και αφήνοντας το στόχο με την πραγματική 24bit διεύθυνση εντελώς εκτός διαδικασιών. Μια λεπτομερής περιγραφή του περιεχομένου κάθε πλαισίου απεικονίζεται στο σχήμα 2.14.



Σχήμα 2.14 Διαδικασία Name server pollution.

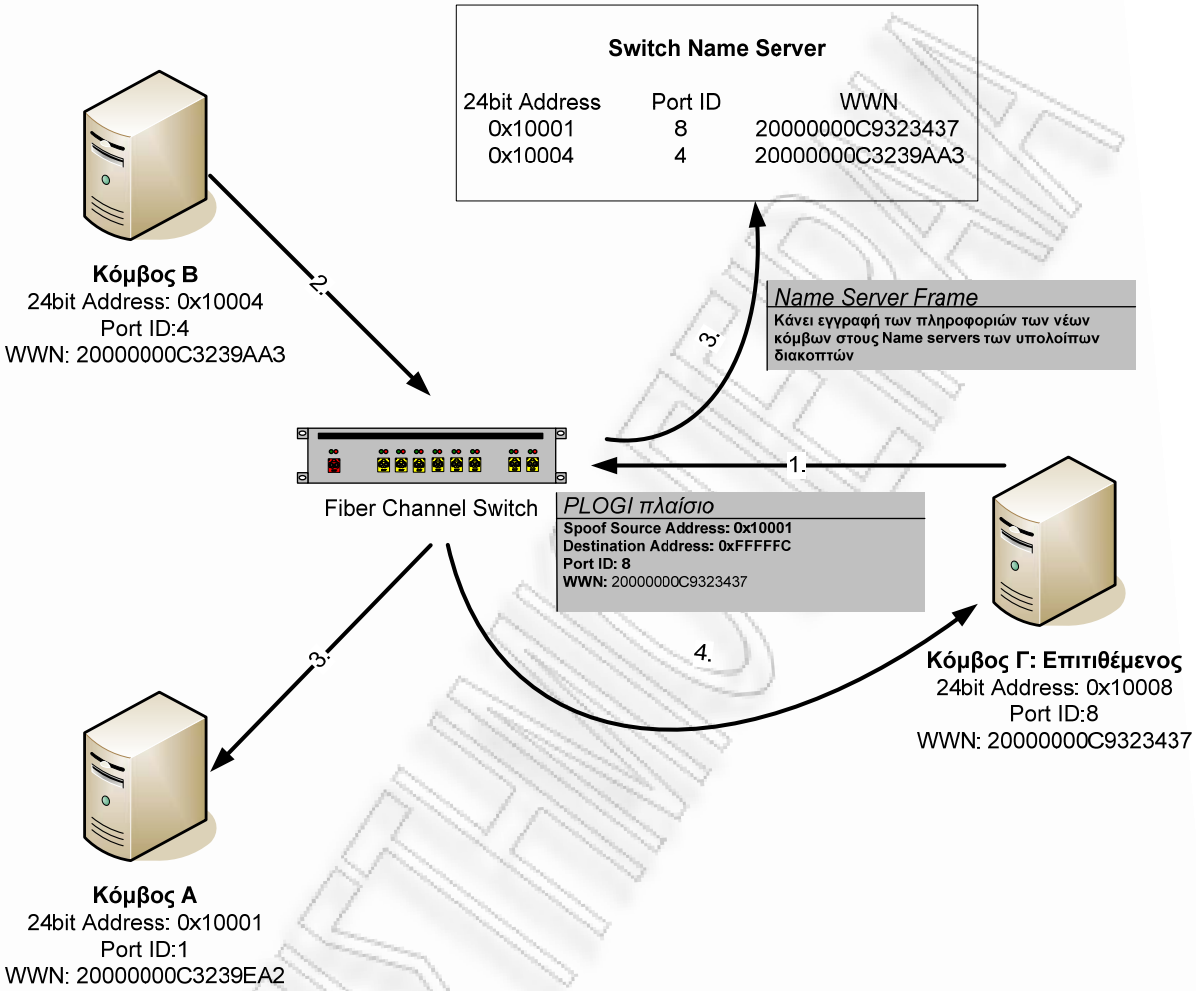
Man in the middle attack

Προκειμένου δύο κόμβοι οπτικού καναλιού να επικοινωνούν ο ένας με τον άλλον, πρέπει να ξέρουν την 24bit διεύθυνση και την port ID στο fabric. Η διεύθυνση δίνεται και ενημερώνεται κατά τη διάρκεια των διαδικασιών FLOGI και PLOGI, χωρίς καμία διαδικασία επικύρωσης (παρόμοια με ARP). Η port ID είναι ο φυσικός αριθμός της πόρτας με την οποία ο κόμβος συνδέεται στο switch. Εάν ένας κόμβος ήθελε να επικοινωνήσει με έναν άλλο κόμβο, θα έστελνε πλαίσια στη 24bit διεύθυνση του άλλου κόμβου, τα οποία θα περιείχαν τη διεύθυνση προορισμού (D_ID) στο header τους. Το switch θα λάμβανε το πλαίσιο, θα ταίριαζε τη διεύθυνση με τη σωστή port ID, μέσω του Name Server πίνακα, προκειμένου να βρεθεί η σωστή φυσική πόρτα του κόμβου προορισμού, και θα δρομολογούσε έπειτα το πλαίσιο προς τη σωστή πόρτα.



Σχήμα 2.15 Κανονική επικοινωνία στο fabric.

Προκειμένου να εκτελεστεί μια επίθεση MITM, ένας κακόβουλος κόμβος θα άλλαζε τη διεύθυνση του για να ταιριάξει με τη διεύθυνση του κόμβου που θέλει να επιτεθεί (κόμβος A). Επειδή οι πληροφορίες των Name Servers μπορούν να ενημερωθούν αυτόματα κατά τη διάρκεια της διαδικασίας PLOGI, ο κακόβουλος χρήστης θα εκτελούσε έπειτα ένα PLOGI, στέλνοντας port ID, WWN και τη spoofed 24bit διεύθυνσή του στη διεύθυνση 0xFFFFFC για να την δεχτούν όλα τα switches του δικτύου. Τα switches, με τις ανακριβείς πληροφορίες για τη διεύθυνση, θα ενημέρωναν τους Name Servers με τα port ID, WWN και spoofed 24bit διεύθυνση. Όταν ένας άλλος κόμβος θελήσει να επικοινωνήσει με τον πραγματικό κόμβο, ο πίνακας δρομολόγησης του switch θα δρομολογήσει τη διεύθυνση, σε ένα διαφορετικό port ID οδηγώντας το πλαίσιο σε έναν άλλο κόμβο, τον κακόβουλο κόμβο.



Σχήμα 2.16 Man-in-the-Middle επίθεση στο fabric.

Η αρχική αδυναμία ασφάλειας είναι η έλλειψη επικύρωσης κατά το FLOGI ή PLOGI. Στο σχήμα 2.16, ο κόμβος Α έχει μια 24bit fabric διεύθυνση 0x10001 και ο κόμβος Β έχει μια 24bit fabric διεύθυνση 0x10004. Οι πίνακες και οι κανόνες δρομολόγησης θα επέτρεπαν στις δύο οντότητες να επικοινωνήσουν η μια με την άλλη αρκετά εύκολα χρησιμοποιώντας την port ID 1 και την port ID 2. Σε περίπτωση που ο κακόβουλος κόμβος C, εκτέλεσε μια MITM επίθεση για να παρεμποδίσει την επικοινωνία μεταξύ του κόμβου Α και Β, πραγματοποίησε τα ακόλουθα βήματα:

1. Ο κόμβος C δεν εκτέλεσε ένα FLOGI, επειδή δεν χρειάζεται να έχει μια πραγματική 24bit fabric διεύθυνση, αλλά θα χρησιμοποιήσει τη διεύθυνση του στόχου του, ο οποίος είναι ο κόμβος A.
2. Χρησιμοποιώντας μια συσκευή ανάλυσης κυκλοφορίας, ο κόμβος C δημιουργεί ένα πλαίσιο μιμούμενο ένα πλαίσιο PLOGI, σαν να καταχωρούσε τη διεύθυνση του στο fabric και στα γειτονικά switches, αλλά στην πραγματικότητα καταχωρούσε την spoofed 24bit διεύθυνση του στον εξουσιοδοτημένο Name Server.
3. Ο κόμβος C εκτελεί ένα PLOGI χρησιμοποιώντας τη διεύθυνση 0x10001, που επιτρέπει στο Name Server να θεωρεί ότι η διεύθυνση 0x10001 αντιστοιχεί τώρα στον κόμβο C, την port ID 8 και το WWN 20000000C9323437.
4. Τώρα οποιαδήποτε κυκλοφορία που προορίζεται στη διεύθυνση 0x10001, που θα έπρεπε να είναι κόμβος A αλλά τώρα είναι κόμβος C, θα δρομολογηθεί προς τον κακόβουλο κόμβο με στόχο την υποκλοπή, παρακολούθηση/καταγραφή και έκθεση πληροφοριών.
5. Όταν η διεύθυνση 0x10004 (κόμβος B) προσπαθεί να επικοινωνήσει με τη διεύθυνση 0x10001 (κόμβος A), η κυκλοφορία θα πάει πραγματικά στον κόμβο C, δεδομένου ότι ο πίνακας του Name Server του switch θεωρεί ότι η port ID 8 έχει τη διεύθυνση 0x10001.
6. Προκειμένου μία MITM επίθεση να είναι πλήρως ολοκληρωμένη, μόλις λάβει ο κόμβος C την κυκλοφορία από τον κόμβο B, πρέπει άμεσα να δρομολογήσει τα πλαίσια στον πραγματικό προορισμό (κόμβος A) προκειμένου αμφότερα τα συμβαλλόμενα μέρη να συνεχίσουν την επικοινωνία χωρίς οποιαδήποτε υποψία και έτσι ο κόμβος C να συνεχίσει να λαμβάνει την κυκλοφορία από τον κόμβο B. Εάν ο κόμβος C αποτύχει να διαβιβάσει την κυκλοφορία στον κόμβο A, ο κόμβος B θα καταλάβει ότι η επικοινωνία που προσπαθεί να εκτελέσει δεν λειτουργεί σωστά και σταματά να στέλνει πλαίσια, αφήνοντας κατά συνέπεια τον κόμβο C χωρίς πλαίσια προς υποκλοπή. (Σημείωση: Το τελευταίο μέρος της δρομολόγησης της επίθεσης είναι εξαιρετικά δύσκολο στις ταχύτητες 2gb/sec και πάνω.)

Η FC MITM επίθεση είναι πιθανή κάτι που οφείλεται στην έλλειψη αυθεντικοποίησης στα πλαίσια PLOGI, καθώς επίσης και στις αδυναμίες ασφάλειας κατά τη διάρκεια της διαδικασίας ενημέρωσης των καταχωρήσεων των Name Servers. Όπως καταδεικνύεται η επίθεση είναι δυνατό να πραγματοποιηθεί εντούτοις, υπάρχουν δυσκολίες κυρίως λόγω των υψηλών ταχυτήτων (2gb/sec ή μεγαλύτερες)

με τις οποίες ένας επιτιθέμενος θα έπρεπε να μπορεί να αναμεταδίδει πλαίσια στο δίκτυο αποθήκευσης δεδομένων. Το θέμα αναλογίας όγκου/απόδοσης καθιστά την επίθεση υψηλής επικινδυνότητας αλλά χαμηλής πιθανότητας εμφάνισης.

2.3.4. Επίθεση ενδιάμεσης οντότητας - Σύνοψη επιθέσεως

Περιγραφή επίθεσης – Αποστέλλεται ένα πλαστό πλαίσιο PLOGI στο switch προκειμένου να αντιστοιχηθεί η 24bit διεύθυνση ενός στόχου στο WWN και την port ID του επιτιθεμένου ως εκ τούτου, «μολύνεται» ο Name Server αποστέλλοντας την κυκλοφορία στον κακόβουλο κόμβο.

Επίπεδο κινδύνου - Χαμηλό.

Δυσκολία - Υψηλή. Είναι μια περίπλοκη επίθεση που απαιτεί βαθιά γνώση πλαισίων καναλιών οπτικών ινών και τη χρήση μιας software και hardware συσκευής ανάλυσης κυκλοφορίας.

Best practice – Καμία μέχρι σήμερα, εντούτοις, η χρήση επικυρωμένων πλαισίων FLOGI και PLOGI θα μετρίαζε την πιθανότητα εμφάνισης στο μέλλον.

2.3.5. Μόλυνση κεντρικών υπολογιστών ονομάτων - Σύνοψη επιθέσεως

Περιγραφή επίθεσης – Αλλοίωση των πληροφοριών των Name servers των FC switches όπου ένας επιτιθέμενος αντιστοιχεί τη διεύθυνση του στο WWN ενός στόχου. Εάν οποιοσδήποτε νόμιμος κόμβος προσπαθήσει να επικοινωνήσει με το στόχο, η κυκλοφορία δρομολογείται στον επιτιθέμενο λόγω των αλλοιωμένων πληροφοριών των Name servers (παρόμοια με MITM επίθεση στην IP αρχιτεκτονική).

Επίπεδο κινδύνου - Υψηλό. Μια μη εξουσιοδοτημένη οντότητα θα μπορούσε να αποκτήσει πρόσβαση σε ευαίσθητα στοιχεία με αναξιόλογες επιθέσεις.

Δυσκολία - Υψηλή. Είναι μια περίπλοκη επίθεση που απαιτεί βαθιά γνώση πλαισίων καναλιών οπτικών ινών και τη χρήση μιας software και hardware συσκευής ανάλυσης κυκλοφορίας.

Best practice – Πρέπει να εξασφαλιστεί το ότι τα κακόβουλα PLOGI πλαίσια, που χρησιμοποιούνται για να ενημερώσουν τους Name servers των switches, δεν

μπορούν να αλλοιώσουν τους πίνακες των Name servers. Παράμετροι επιλογών επικύρωσης και ακεραιότητας πλαισίων.

3ο Κεφάλαιο

3. Local Unit Number masking και ασφάλεια Host Bus Adapter

Προκείμενου να συζητήσουμε για τους κινδύνους που υπάρχουν σε αρχιτεκτονικές καναλιού οπτικών ινών θα πρέπει να αξιολογήσουμε τις βασικές συσκευές και εφαρμογές που χρησιμοποιούνται σε δίκτυα δεδομένων. Οι βασικές οντότητες σε ένα δίκτυο δεδομένων οι οποίες σχετίζονται με την ασφάλεια είναι οι HBAs (Host Bus Adapters), storage controllers, storage switches και storage management consoles οι οποίες εμπεριέχουν εφαρμογές διαχείρισης. Κάθε μία από αυτές τις συσκευές παίζει το ρόλο της τόσο σε θέματα αποθήκευσης δεδομένων όσο και σε θέματα ασφάλειας και διαθεσιμότητας δεδομένων.

3.1. Host Bus Adapters

Τα Host Bus Adapters (HBAs) είναι παρόμοια με τα Network Interface Cards (NICs) στα IP δίκτυα. Όλα τα NICs έχουν Machine Address Codes (MACs) τα οποία τους δίνονται από τους κατασκευαστές προκειμένου να αναγνωρίζεται ένα NIC. Ομοίως ένα HBA έχει ένα World Wide Name (WWN) το οποίο επίσης δίνεται από τον κατασκευαστή προκειμένου να αναγνωρίζεται ένας κόμβος στο fabric. Αντίθετα από τα MAC στα IP δίκτυα, τα WWNs έχουν μεγαλύτερη δύναμη και περισσότερες ευθύνες όσο αφορά θέματα ασφάλειας σε ένα δίκτυο αποθήκευσης δεδομένων, στα WWNs πέφτει το μεγαλύτερο βάρος της αυθεντικοποίησης. Λόγω έλλειψης πραγματικής αυθεντικοποίησης η αυθεντικοποίηση με χρήση και παραμετροποίηση των WWNs είναι ζωτικής σημασίας.

Όπως και τα MACs έτσι και τα WWNs μπορούν να αντιγραφούν και να παραποιηθούν από μία κακόβουλη οντότητα. Μάλιστα η δυνατότητα αλλαγής ενός WWN δίδεται στα HBAs από τους κατασκευαστές (δυνατότητα ευελιξίας στην διαχείριση ενός δικτύου από τον administrator). Αυτή η λειτουργία όμως δίνει την δυνατότητα σε μία κακόβουλη οντότητα εύκολα να παραποιήσει το WWN του και να

κλέψει την ταυτότητα ενός νόμιμου κόμβου στο δίκτυο. Με αυτό τον τρόπο εάν ο κόμβος, του οποίου έχει κλαπεί η ταυτότητα, είχε πρόσβαση σε μία προστατευμένη ζώνη, ο κακόβουλος κόμβος αυτόματα αποκτά πρόσβαση σε αυτή τη ζώνη και σε όλα τα LUNs τα οποία θα ευρίσκονταν σε αυτή.

Το πραγματικό πρόβλημα είναι ότι ακόμα μία πηγή, το WWN ενός HBA, η οποία μπορεί να αντιγραφεί/παραποιηθεί, χρησιμοποιείται ως μία απολύτως έμπιστη οντότητα. Πάρα το γεγονός ότι είναι παρόμοια περίπτωση με την 24bit fabric διεύθυνση, που θεωρείται έμπιστη οντότητα από ένα Name Server, αυτή η επίθεση είναι πολύ πιο ισχυρή με κίνδυνο την καταστροφή και απώλεια πολλών και σημαντικών δεδομένων. Εφόσον, στην περίπτωση του zoning, χρησιμοποιούνται WWN προκειμένου να δοθεί πρόσβαση ή όχι σε ένα κόμβο στα LUNs το να παραποιήσει μία κακόβουλη οντότητα μια ταυτότητα και αποκτήσει πρόσβαση ή να καταστρέψει αρχεία είναι κάτι απλό. Το γεγονός όμως ότι ο επιτιθέμενος, προκειμένου να πραγματοποιήσει μια τέτοια επίθεση, θα έπρεπε να έχει πάρει τον έλεγχο κάποιου server ελαχιστοποιεί την πιθανότητα εμφάνισής της αλλά δεν την αποκλείει. Έτσι εξισορροπείται η αδυναμία ασφαλείας του λειτουργικού συστήματος το οποίο είναι εξ αρχής τροποποιημένο έτσι ώστε να μην έχει και πολλές αρμοδιότητες ως αρχή υπεύθυνη για τα terabytes δεδομένων σε ένα δίκτυο αποθήκευσης δεδομένων.

3.2. WWN spoofing

Όπως είδαμε το WWN είναι μία οντότητα η οποία χρησιμοποιείται για να αναγνωριστεί ένας κόμβος σε ένα δίκτυο αποθήκευσης δεδομένων. Δυστυχώς τα δίκτυα αυτά βασίζονται πολύ στα WWNs μίας και είναι η βασική οντότητα ασφάλειας γεγονός που δημιουργεί κινδύνους ασφάλειας. Όπως προαναφέραμε το να παραποιήσει μία κακόβουλη οντότητα ένα WWN είναι αρκετά απλό και κατανοητό, αυτό που μένει είναι να δούμε πώς μπορεί η κακόβουλη οντότητα να αποκτήσει το WWN του στόχου (κόμβου). Εμπόδια υπάρχουν κανένα όμως δεν είναι αξεπέραστο για ένα καλά ενημερωμένο επιτιθέμενο ενώ οι τρόποι είναι παραπάνω από ένας.

Μία μέθοδος είναι η καταγραφή των HBAs που είναι συνδεδεμένα στο fabric μέσω επιλογής του λογισμικού οδηγήσεως το οποίο όλοι οι κατασκευαστές παρέχουν

με τις συσκευές τους. Μία δεύτερη μέθοδος είναι απλά να συνδεθεί η κακόβουλη οντότητα σε ένα IP interface ενός switch οπτικού καναλιού (δεν απαιτείται αυθεντικοποίηση) και να δει τις ρυθμίσεις του switch συμπεριλαμβανομένων και των WWNs του κάθε συνδεδεμένου κόμβου. Μία τελευταία μέθοδος θα ήταν, με την χρήση ειδικού λογισμικού, μία brute force επίθεση. Όλα τα WWNs περιέχουν 16 χαρακτήρες, μόνο δεκαεξαδικές αξίες μπορούν να χρησιμοποιηθούν.

Η πιο τετριμμένη μέθοδος είναι αυτή της παρακολούθησης και καταγραφής μέσο επιλογής που διαθέτουν τα λογισμικά οδηγήσεως των συσκευών. Εάν για παράδειγμα ο κακόβουλος χρήστης χρησιμοποιούσε ένα *Emulex HBA* (σχήμα 3.1) και το λογισμικό *HBAnyware® Centralized Host Bus Adapter Management Suite* (http://www.emulex.com/products/hba/hbanyware/ds.jsp) μπορούσε μέσω της λειτουργίας του προγράμματος "Discovery tree" να ανακαλύψει όλες τις συνδεδεμένες συσκευές στο δίκτυο καθώς επίσης τα WWNs και τα πιθανά LUNs.

Σχήμα 3.1 Emulex HBA

Το πρόγραμμα δίνει πολλές δυνατότητες στον χρήστη συμπεριλαμβανομένων των:

- **Discovery tab.** Περιέχει τις λίστες με τους αριθμούς των ευρισκόμενων κόμβων, hosts, adapters και LUNs στο δίκτυο.
- **Host attributes tab.** Περιέχει συγκεκριμένες πληροφορίες για κάθε host του δικτύου συμπεριλαμβανομένων του ονόματος και του firmware που χρησιμοποιεί.

- **Fabric attributes tab.** Περιέχει πληροφορίες διευθύνσεων των ευρισκόμενων fabrics.
- **Target attributes tab.** Περιέχει πληροφορίες για ένα προβαλλόμενο στόχο όπως κατασκευαστή, product ID, FCID, LUNs χαρτογραφημένα σε αυτόν, το WWN του, όνομα συσκευής κτλ.
- **General tab.** Γενικές πληροφορίες για όλες της κάρτες του δικτύου.
- **Details tab.** Περιέχει πληροφορίες για ένα συγκεκριμένο προβαλλόμενο στόχο.
- **Port attributes tab.** Περιέχει πληροφορίες για ένα όλες τις πόρτες του δικτύου. Ποσότητα, τύπους, τύπο οδηγού οδηγήσεως κτλ.
- **Port statistics tab.** Περιέχει στατιστικές των πορτών.
- **Firmware tab.** Περιέχει πληροφορίες για το firmware της συσκευής

Στην περίπτωση που ο χρήστης προσπαθούσε να χρησιμοποιήσει τη μέθοδο της brute force επίθεσης στην πραγματικότητα δεν θα αντιμετώπιζε μεγάλες δυσκολίες. Τα WWNs συνήθως είναι εύκολο να προβλεφθούν, ας πάρουμε την περίπτωση που ο κεντρικός υπολογιστής μίας βάσης δεδομένων σε ένα δίκτυο αποθήκευσης δεδομένων έχει για WWN το 10000000a239ab22 και ένας άλλος κεντρικός υπολογιστής έχει για WWN το 10000000a234cd82. Παρατηρούμε ότι τα δύο WWNs διαφέρουν μόνο στα 5 τελευταία ψηφία και όπως προαναφέραμε αυτά είναι δεκαεξαδικοί αριθμοί. Επομένως ο επιτιθέμενος έχει να εκτελέσει brute force επίθεση σε 5ψήφιο αλφαριθμητικό με το κάθε ψηφίο να έχει 16 πιθανούς χαρακτήρες (A-F και 0-9). Όπως καταλαβαίνουμε ο επιτιθέμενος δεν θα δυσκολευτεί ιδιαιτέρως καθώς ισχυρό password θεωρείται εκείνο ελάχιστου μεγέθους 8 χαρακτήρων με χρήση αριθμών, γραμμάτων πεζών/κεφαλαίων, κενών, ειδικών χαρακτήρων.

3.2.1 WWN spoofing - Σύνοψη επιθέσεως

Περιγραφή επίθεσης – Μία κακόβουλη οντότητα αλλάζει την WWN της και προσπαθεί να αποκτήσει πρόσβαση στα δεδομένα ενός άλλου κόμβου

Επίπεδο κινδύνου - Υψηλό. Μια αναρμόδια οντότητα θα μπορούσε να αποκτήσει πρόσβαση σε ευαίσθητα στοιχεία με αναξιόλογες επιθέσεις.

Δυσκολία – Χαμηλή. Το να αλλάξει μια οντότητα το WWN της είναι κάτι πολύ απλό.

Best practice – Τα switches οπτικού καναλιού θα πρέπει να απομονώνουν και να περιορίζουν την πρόσβαση μη αυθεντικοποιημένων κόμβων. Θα μπορούσε να χρησιμοποιηθεί Σκληρός διαχωρισμός ζωνών (Hard zoning) προκειμένου να ενισχυθούν οι παράμετροι περιορισμού πρόσβασης. Θα ήταν προτιμότερη η χρήση Port WWN αντί node WWN ως παράμετρος για διαχωρισμό ζωνών.

3.3. Ελεγκτής δικτύων αποθήκευσης δεδομένων

Οι συσκευές αποθήκευσης δεδομένων διαδραματίζουν επίσης έναν σημαντικό ρόλο από στην ασφάλεια και τη διαχείρισης κινδύνου. Οι συσκευές αποθήκευσης δεδομένων καναλιού οπτικών ινών όπως EMC, HP, IBM, Compaq, Sun Microsystems συνήθως δεν λαμβάνονται υπόψη σε ζητήματα ασφάλειας. Ενώ οι περισσότερες από αυτές τις συσκευές δεν είναι άμεσα προσιτές στις κακόβουλες οντότητες, είναι παρόλα αυτά τρωτές σε διάφορους τύπους επιθέσεων.

Στις περισσότερες συσκευές αποθήκευσης δικτύων αποθήκευσης δεδομένων, ο μόνος μηχανισμός ασφάλειας είναι το LUN Masking. Οι περισσότεροι προμηθευτές υλικού υποθέτουν ότι η ασφάλεια θα παρασχεθεί από άλλες οντότητες στο γενικό δίκτυο, όπως τα switches ή τα HBAs στα μηχανήματα των clients. Στη συνέχεια περιγράφονται κίνδυνοι ασφάλειας που σχετίζονται με LUN masking.

3.4. LUN masking

Το LUN χρησιμοποιείται ως μοναδικό SCSI αναγνωριστικό που προσδιορίζει μια λογική μονάδα δεδομένων. Προς χάρη απλότητας, σκεφτείτε μια μονάδα δίσκου 100GB που διαιρείται σε τέσσερα μέρη. Κάθε λογικό μέρος της θα ήταν ένα χωριστό LUN με ένα χωριστό προσδιοριστικό που αντιπροσωπεύει 25GB του διαστήματος αποθήκευσης. Παραδείγματος χάριν, ένα EMC Symmetrix μπορεί να έχει πολλά διαφορετικά LUNs με σχετικά προσδιοριστικά. Τα LUN 0000 και 0001 θα μπορούσαν να είναι τμήματα αποθήκευσης δεδομένων που αντιστοιχούν στη ζώνη 1

του switch, το οποίο συνδέει τα μηχανήματα με NT λειτουργικό με ένα δίκτυο αποθήκευσης δεδομένων. Τα LUN 0002 και 0003 θα μπορούσαν να είναι τμήματα αποθήκευσης δεδομένων που αντιστοιχούν σε μια άλλη ζώνη που συνδέει τα μηχανήματα με UNIX λειτουργικό με ένα δίκτυο αποθήκευσης δεδομένων.

Το LUN masking είναι η διαδικασία αντιστοίχησης LUNs στους σωστούς κεντρικούς υπολογιστές. Σε κάθε κεντρικό υπολογιστή θα δοθεί πρόσβαση σε ένα LUN και στη συνέχεια αυτό θα αποκρυφτεί από τα υπόλοιπα LUNs. Το LUN masking μπορεί να πραγματοποιηθεί σε τέσσερις διαφορετικές περιοχές μέσα στο δίκτυο, συμπεριλαμβανομένων του ελεγκτή αποθήκευσης, το HBA, το switch ή μία εφαρμογή.

Οι ελεγκτές δικτύων αποθήκευσης δεδομένων προσφέρουν το LUN masking ως εργαλείο τμηματοποίησης/ασφάλειας, αντιστοιχίζοντας LUNs στους κεντρικούς υπολογιστές.

Η διαδικασία του LUN masking στον ελεγκτή αποθήκευσης δημιουργεί ένα κίνδυνο ασφάλειας δεδομένου ότι το LUN masking στηρίζεται στα WWNs των HBA. Το WWN του HBA χρησιμοποιείται ως προσδιοριστικό κατά τη διάθεση LUNs σε έναν κόμβο. Παραδείγματος χάριν, εάν οι LUN αριθμοί 0001, 0002 και 0003, ενός ελεγκτή αποθήκευσης, χρειάζονταν σε έναν Windows εξυπηρετητή αρχείων, το WWN του HBA που συνδέεται με το εξυπηρετητή θα χρησιμοποιούνταν για να προσδιορίσει τον εξυπηρετητή αρχείων στο fabric. Υπάρχουν μερικοί κατασκευαστές που μπορούν να εφαρμόσουν LUN masking σε επίπεδο port εντούτοις, οι περισσότεροι εφαρμόζουν κανόνες ασφάλειας στο port του ελεγκτή αποθήκευσης και όχι στο port του switch, καθιστώντας το WWN του HBA το μόνο προσδιοριστικό που χρησιμοποιείται προκειμένου να αναγνωριστεί ένας εξυπηρετητής αρχείων. Όταν ένας ελεγκτής αποθήκευσης λάβει ένα αίτημα για τα LUN 0001, 0002, ή 0003, θα ελέγξει εάν το WWN του HBA ταιριάζει με το WWN στον πίνακα των LUNs. Εάν το LUN masking στον ελεγκτή αποθήκευσης δεν έχει καταχωρημένο το WWN του κεντρικού υπολογιστή, το αίτημα θα απορριφθεί.

Το LUN masking επίπεδο του ελεγκτή αποθήκευσης φαίνεται να παρέχει ένα επαρκές επίπεδο ελέγχου. Το ζήτημα ασφάλειας με το LUN masking οφείλεται στην αβεβαιότητα που εισάγουν τα WWNs. Όπως αναφέρεται και πρωτύτερα το να αλλάζει ένα HBA το WWN του είναι μια τετριμμένη διαδικασία και προσφέρεται ως δυνατότητα από πολλούς οδηγούς συσκευών HBA. Εάν ένας κεντρικός υπολογιστής που συνδέθηκε στο δίκτυο αποθήκευσης δεδομένων άλλαζε το WWN του σε ένα από

τους Windows εξυπηρετητή αρχείων που αναφέρθηκαν στο προηγούμενο παράδειγμά μας και υπέβαλε αίτημα για πρόσβαση στα LUN 0001, 0002, 0003, ο πίνακας LUN masking του ελεγκτή αποθήκευσης θα χορηγούσε πρόσβαση στον κακόβουλο κεντρικό υπολογιστή. Το ζήτημα είναι ότι το LUN masking, όπου και αν εφαρμόζεται στον ελεγκτή αποθήκευσης, το switch καναλιού οπτικών ινών, το HBA ή την εφαρμογή, στηρίζεται στο επίπεδο της ασφάλειας σε μεγάλο ποσοστό στα WWN, κάτι που δεν είναι ιδιαίτερα καλό δεδομένου ότι τα WWNs μπορεί να αλλάξουν, αντιγραφούν και να υποκλαπούν εύκολα με τετριμμένους τρόπους και ελάχιστη προσπάθεια από τους επιτιθεμένους.

Το LUN masking είναι συνήθως η μόνη οντότητα που παρέχεται από τους ελεγκτές αποθήκευσης ως μηχανισμός ασφάλειας, είναι λοιπόν εύκολα κατανοητό ότι οι κίνδυνοι ασφάλειας, με ελεγκτές δικτύων αποθήκευσης να εφαρμόζουν LUN masking ως την μόνη δικλίδα ασφάλειας, είναι μεγάλοι.

3.4.1. LUN masking επιθέσεις

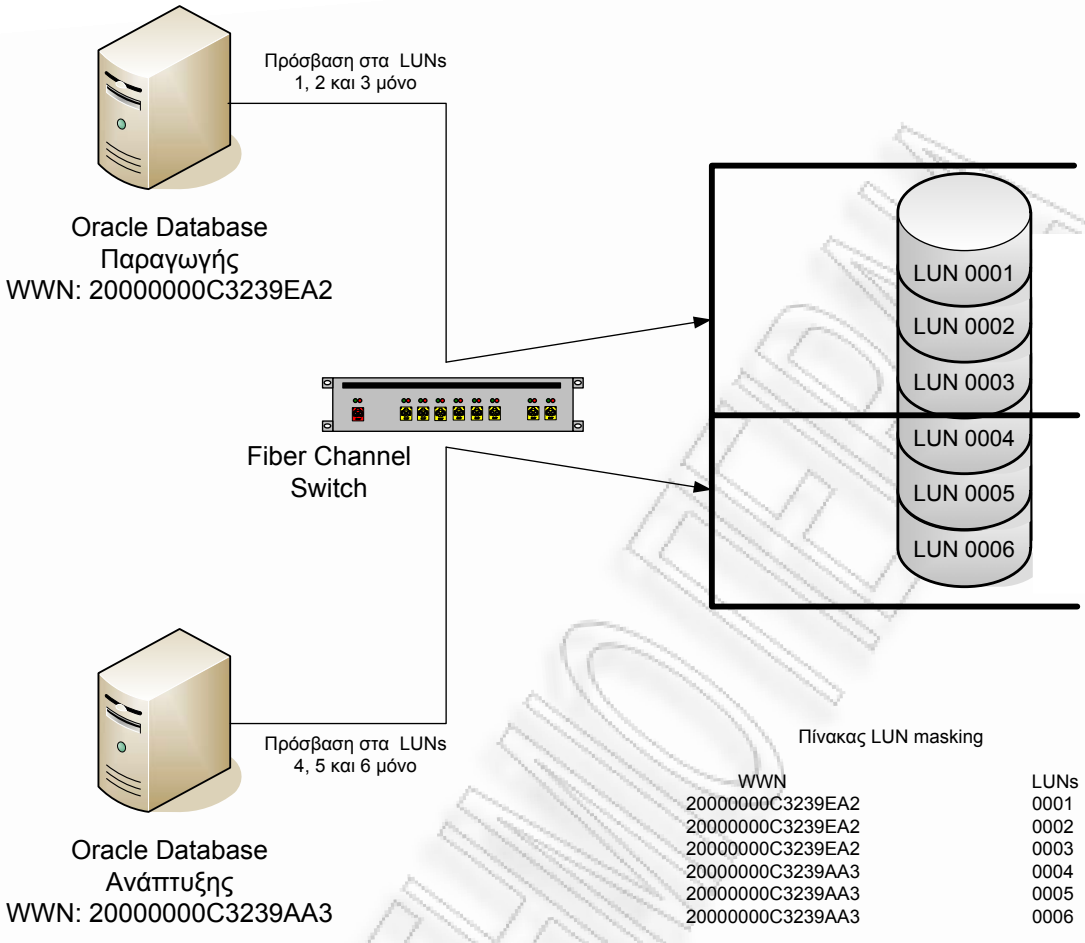
Οι λογικοί αριθμοί μονάδων (LUNs) χρησιμοποιούνται για να ταξινομήσουν σύνολα δεδομένων στους ελεγκτές δικτύων αποθήκευσης δεδομένων. Αυτή είναι μια αποδοτική μέθοδος για να διαιρεθεί και να χωριστεί ένα μεγάλο διάστημα αποθήκευσης σε λογικές μονάδες αποθήκευσης. Η ιδέα του LUN masking είναι να αποκρύπτει ορισμένα LUNs από έναν δεδομένο κόμβο του δικτύου. Συγκεκριμένα, το LUN masking είναι η διαδικασία απόκρυψης ή εμφάνισης μερών ενός δίσκου αποθήκευσης σε έναν κόμβο. Το LUN masking δημιουργεί υποσύνολα του δίσκου μέσα στην εικονική δεξαμενή του δικτύου και επιτρέπει μόνο σε οριζόμενους κεντρικούς υπολογιστές να έχουν πρόσβαση στα υποσύνολα αυτά.

Παραδείγματος χάριν, ο κεντρικός υπολογιστής Α είναι ένας κεντρικός υπολογιστής βάσεων δεδομένων που τρέχει Oracle με δεδομένα της παραγωγής μιας εταιρίας/οργανισμού, ο οποίος χρησιμοποιεί τα LUNs 1, 2 και 3. Ο κεντρικός υπολογιστής Β είναι επίσης ένας κεντρικός υπολογιστής βάσεων δεδομένων που τρέχει Oracle, αλλά με στοιχεία της ανάπτυξης της εταιρίας/οργανισμού και χρησιμοποιεί μόνο τα LUNs 4, 5, και 6. Το LUN masking είναι η μέθοδος εκείνη που θα μπορούσε να χρησιμοποιηθεί για να εξασφαλίσει ότι η Oracle βάση δεδομένων της παραγωγής και η Oracle βάση δεδομένων της ανάπτυξης δεν θα έχουν πρόσβαση

σε λάθος μονάδες αποθήκευσης. Στο σχήμα 3.2 παρουσιάζεται ένα παράδειγμα της αρχιτεκτονικής που περιγράφεται προηγουμένως. Το LUN masking αρχικά είχε ως σκοπό να είναι ένα εργαλείο τμηματοποίησης και όχι ασφάλειας, έχοντας κατά συνέπεια πολλές αδυναμίες ασφάλειας.

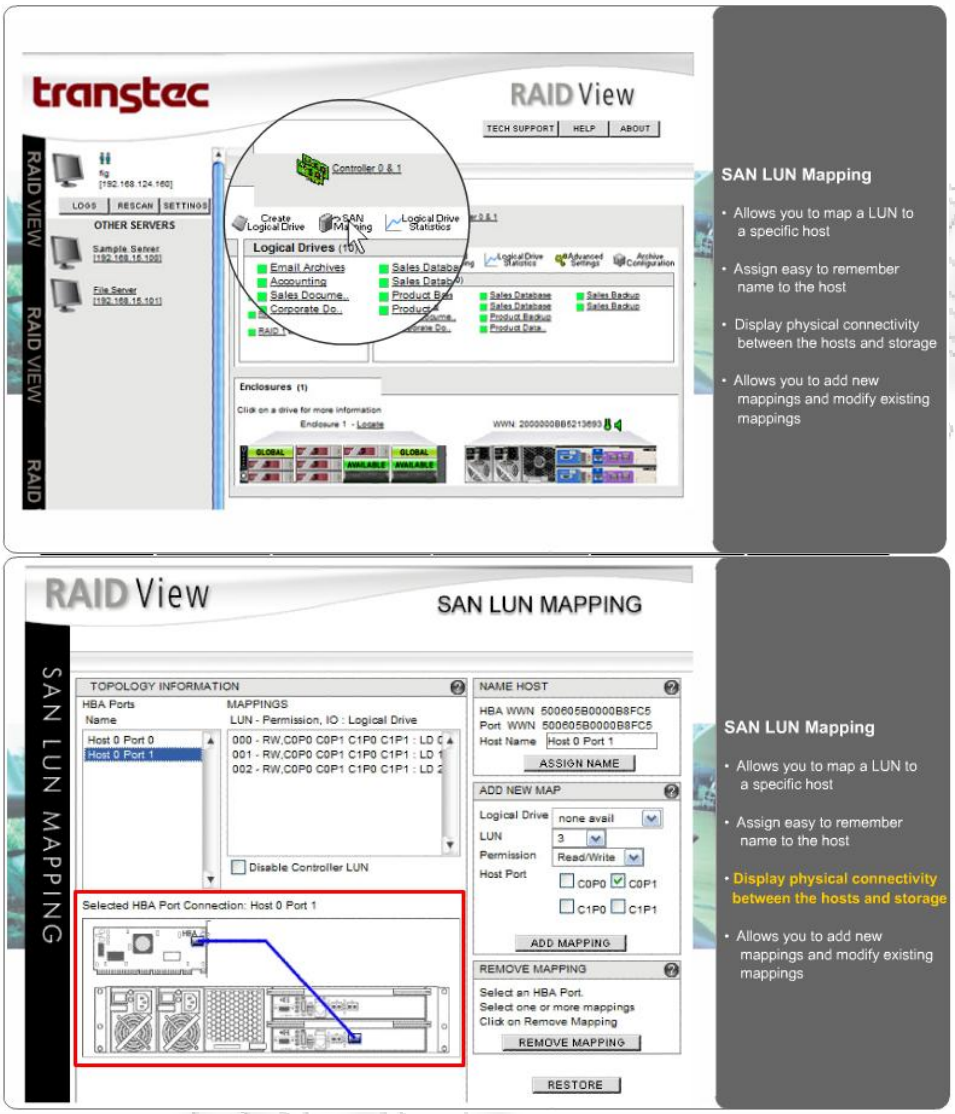
Το LUN masking στηρίζεται σε δύο τύπους WWNs: port WWN (WWPN) ή node WWN (WWNN). Σε μερικές περιπτώσεις, το LUN masking χρησιμοποιεί τη διεύθυνση ενός στόχου (24bit fabric διεύθυνση). Εάν το LUN masking χρησιμοποιεί node WWNs, τα οποία μπορεί να αλλάξουν μέσω οδηγών λογισμικού, μπορεί να υπονομευθεί εύκολα. Εάν το LUN masking χρησιμοποιεί port WWNs, τα οποία δεν μπορεί να αλλάξουν μέσω οδηγών λογισμικού, αποδεικνύεται πιο δυνατό εργαλείο ασφάλειας.

Γιατί κάποιος να χρησιμοποιεί node WWNs δεδομένου ότι η χρήση port WWNs είναι ασφαλέστερη; Ο λόγος είναι ότι τα node WWNs είναι πολύ πιο ευπροσάρμοστα και εύκολα στη χρήση σε δυναμικά περιβάλλοντα. Παραδείγματος χάριν, ένα προβληματικό HBA μπορεί να αντικατασταθεί εύκολα χωρίς σημαντικές αλλαγές διαμόρφωσης χρησιμοποιώντας node WWNs. Επιπλέον, εάν ένα δίκτυο αποθήκευσης δεδομένων χρησιμοποιεί ελεγκτές, στους οικοδεσπότες του, που δεν αλληλεπιδρούν με το λογισμικό, το οποίο χρησιμοποιείται σε πολύ δίκτυα αποθήκευσης δεδομένων, απαιτείται η χρησιμοποίηση node WWNs. Πώς γνωρίζουμε εάν χρησιμοποιούνται WWPNs ή WWNNs; Σε ένα περιβάλλον Windows που χρησιμοποιείται το λογισμικό Emulex, οι πληροφορίες μπορούν να βρεθούν στη registry. Εάν χρησιμοποιούνται WWNNs, υπάρχει μεγάλη περίπτωση κακόβουλες οντότητες να υπονομεύσουν το LUN. Εάν χρησιμοποιούνται WWPNs, η αντιγραφή WWN είναι δυσκολότερη, αλλά δυνατή.



Σχήμα 3.2 LUN Masking

Το LUN masking έχει περισσότερο έλεγχο της πρόσβασης από τον χωρισμό ζωνών. Επιπλέον, το LUN masking έχει μπορεί να πραγματοποιηθεί σε τέσσερις διαφορετικές θέσεις: στον κόμβο των clients, το switch καναλιού οπτικών ινών, τον κόμβο του δικτύου ή σε μία LUN masking εφαρμογή/συσκευή.



Σχήμα 3.3 Παράδειγμα LUN Mapping εφαρμογής

3.4.1.1. LUN masking στον κόμβο του client

Εάν το LUN masking διευθυνόταν στον κόμβο του client η χαρτογράφηση θα διευθυνόταν στο HBA επίπεδο χρησιμοποιώντας HBA λογισμικό οδήγησης, σε αυτή την περίπτωση υπάρχουν μερικά θέματα ασφαλείας. Το πρώτο που θα συζητήσουμε είναι το γεγονός ότι η πρόσβαση στο LUN masking λογισμικό που βρίσκεται στον κεντρικό υπολογιστή πραγματοποιείται χωρίς οποιαδήποτε διαδικασία αυθεντικοποίησης. Πολλά HBA λογισμικά οδήγησης παρέχουν τη δυνατότητα να

κάνουν LUN masking. Δίνεται η δυνατότητα να γίνουν οι αλλαγές στους LUN masking πίνακες χωρίς οποιαδήποτε διαδικασία αυθεντικοποίησης. Οποιοσδήποτε χρήστης που έχει πρόσβαση στον κεντρικό υπολογιστή μπορεί να έχει πρόσβαση στις LUN masking ιδιότητες και να κάνει οποιαδήποτε αλλαγή επιθυμεί. Επιπλέον, τα περισσότερα LUN masking λογισμικά έχουν επίσης τη δυνατότητα να εντοπίζουν όλα τα διαθέσιμα LUNs. Εάν ένας κακόβουλος, αναρμόδιος, ή τυχαίος χρήστης αποκτήσει πρόσβαση στο λειτουργικό σύστημα, δεν θα χρειαζόταν να γνωρίζει συγκεκριμένες πληροφορίες, αλλά θα μπορούσε απλά χρησιμοποιώντας το LUN masking λογισμικό να βρει όλα τα LUNs στο δίκτυο αποθήκευσης δεδομένων και απλά να συνδεθεί, πράγμα το οποίο είναι ιδιαίτερα επικίνδυνο σε λειτουργικά συστήματα με Windows, δεδομένου ότι τα Windows επιθυμούν να έχουν στην «ιδιοκτησία» τους κάθε LUN που μπορεί να βλέπουν. Θα έπρεπε οι εταιρίες/οργανισμοί να στηρίζονται στα Windows ή στις Unix μηχανές τους για θέματα ακεραιότητας και ασφάλειας εμπιστευτικών αρχείων των δικτύων αποθήκευσης δεδομένων τους; Εάν όχι, δεν πρέπει να κάνουν LUN masking χρησιμοποιώντας node WWNs στον κόμβο των clients.

3.4.1.2. LUN masking στο switch, στον ελεγκτή δικτύων αποθήκευσης δεδομένων ή με τη χρήση λογισμικού.

Το LUN masking μπορεί να εφαρμοστεί στον ελεγκτή δικτύων αποθήκευσης, στο switch ή μέσο ενός λογισμικού. Αν και η υπονόμευση κανόνων LUN masking που διαμορφώθηκαν στον κόμβο των clients είναι μια τετριμμένη διαδικασία, η πράξη της υπονόμευσης LUN masking όταν αυτό εφαρμόζεται στον ελεγκτή αποθήκευσης, το διακόπτη, ή μέσο λογισμικού εξαρτάται ιδιαίτερα από τον τύπο του WWN που χρησιμοποιείτε (port WWNs είτε node WWNs).

Ανακεφαλαιώνοντας, το LUN masking στηρίζεται στο WWN του HBA για την κάλυψη των ιδιοτήτων. Εάν ένας διακόπτης ή ελεγκτής δικτύων αποθήκευσης επιβάλλει την κατάτμηση LUN, τότε θα χρησιμοποιούταν το WWN του HBA ως οντότητα έγκρισης για να επιτρέψει ή να απαγορεύσει την πρόσβαση σε ένα LUN ή σε ένα σύνολο LUNs. Εάν ο διακόπτης ή ο ελεγκτής δικτύων αποθήκευσης χρησιμοποιεί ένα port WWN (pWWN) αντί node WWN (nWWN), το LUN masking είναι ασφαλέστερο.

Ας εξετάσουμε το πώς ακόμα κι αν θα μπορούσε κάποιος να αλλάξει το WWN του και αποκτούσε πρόσβαση σε ένα LUN στο οποίο κανονικά δεν έχει έγκριση πρόσβασης, πώς αποκτά πρόσβαση στα άλλα WWNs και LUNs. Η δυνατότητα απαρίθμησης και καταγραφής WWNs και LUNs στο δίκτυο αποθήκευσης δεδομένων μπορεί να γίνει, όπως προαναφέραμε, από τον οδηγό οδήγησης των συσκευών HBA αυτόματα. Πολλοί οδηγοί HBA έχουν τη δυνατότητα «να μάθουν» για το περιβάλλον τους στο δίκτυο, κατά συνέπεια έχουν πρόσβαση σε πληροφορίες από τον Name server των διακοπτών σχετικά με όλα τα WWNs και LUNs στο fabric. Επιπλέον, οι περισσότεροι drivers συσκευών HBA έχουν επίσης ένα παρόμοιο εργαλείο για να ανακαλύπτουν όλα τα LUNs, συμπεριλαμβανομένου και των LUN_IDs. Αυτό θα επέτρεπε στον επιτιθέμενο να έχει πρόσβαση σε οποιαδήποτε LUNs είχε πρόσβαση ο κόμβος του οποίου το WWN έχει υποκλέψει και αντιγράψει.

Επειδή το LUN masking στο διακόπτη, τον ελεγκτή δικτύων αποθήκευσης, ή την εφαρμογή στηρίζεται σε WWNs για τον προσδιορισμό κόμβων, το οποίο είναι μια οντότητα που μπορεί εύκολα να υποκλαπεί και να αντιγραφεί στο, το LUN masking είναι πολύ υψηλού κινδύνου μέθοδος από την άποψη έκθεσης στοιχείων. Ο συνδυασμός μιας υψηλού κινδύνου επίθεσης με την χαμηλού επιπέδου δυσκολία εκτέλεσης κάνει το LUN masking ένα στοχοθετημένο τύπο επίθεσης.

Προκειμένου να προφυλάξουμε το δίκτυό μας ενάντια στην ανατροπή μασκών LUN, πολλά θα πρέπει να γίνουν. Το πρώτο είναι η χρήση του port WWNs αντί node WWNs. Δεδομένου ότι δεν είναι δυνατό να αλλαχτεί ένα HBA port WWN, θα ήταν δυσκολότερο για έναν επιτιθέμενο να εξαπατήσει ένα port WWN από ένα node WWN και να υπονομεύσει τους LUN masking πίνακες. Εντούτοις, υπάρχουν μέθοδοι επίθεσης για να υπονομεύσουν LUN masking που χρησιμοποιεί port-based WWNs. Ένας κακόβουλος χρήστης μπορεί να αλλάξει τον node WWN του ώστε να έχει οποιαδήποτε δεκαεξαδική αξία θέλει, συμπεριλαμβανομένου του node WWN μιας άλλης οντότητας, η οποία είναι η παραδοσιακή επίθεση υποκρισίας (spoofing), ή το port WWN μιας άλλης οντότητας. Ο επιτιθέμενος μπορεί να αλλάξει το node WWN του ώστε να ταιριάζει με το port WWN του στόχου του και να παρακάμψει τους LUN masking πίνακες χρησιμοποιώντας port WWN για την κατάτμηση. Ενώ ο επιτιθέμενος δεν έχει το σωστό port WWN έχει το σωστό node WWN για να εξαπατήσει τον LUN masking πίνακα. Θα πρέπει να εξασφαλιστεί ότι η οντότητα που εκτελεί το LUN masking κάνει έλεγχο για το σωστό port WWN ενός κόμβου και

όχι το node WWN. Εάν οι οντότητες LUN masking ελέγχουν και τα δύο WWNs (node και port η ανατροπή μασκών LUN με port WWNs θα ήταν επιτυχής δεδομένου ότι το node WWN του επιτιθεμένου ταιριάζει με το port WWN του στόχου. Αυτή η επίθεση εξαπατά την οντότητα LUN με την παρουσίαση σωστής αξίας port WWN ακόμα κι αν είναι στο πεδίο του node WWN.

3.4.1.3. LUN masking – Σύνοψη επιθέσεως

Περιγραφή επίθεσης - Υπονόμευση LUN masking ιδιοτήτων και κέρδος της έκθεσης LUNs που θα έπρεπε να είναι κρυφά από συγκεκριμένους κόμβους.

Επίπεδο κινδύνου - Υψηλό. Η αναρμόδια οντότητα θα μπορούσε να αποκτήσει πρόσβαση σε ευαίσθητα στοιχεία με τετριμμένες επιθέσεις.

Δυσκολία - Χαμηλή. Οι περισσότεροι οδηγοί συσκευών HBA έχουν τη δυνατότητα να θέσουν εκτός λειτουργίας το LUN masking όταν αυτό εφαρμόζεται στον κόμβο αποθήκευσης. Εάν το LUN masking εφαρμόζεται στον ελεγκτή δικτύων αποθήκευσης, μια τυπική επίθεση WWN υποκρισίας επίσης θα υπονόμευε τους LUN masking κανόνες.

Best practice – Θα πρέπει να χρησιμοποιηθεί port-binding για να κλειδώσει το WWN ενός κόμβου στο φυσικό port του switch για να αποτρέψει τις επιθέσεις υποκρισίας WWN.

Η LUN masking ανατροπή είναι μια πολύ τετριμμένη επίθεση που έχει διάφορες τρόπους εκτέλεσης. Επιπλέον, η εμπιστοσύνη στο LUN masking για την προστασία των υποθηκευμένων δεδομένων δημιουργεί μια σημαντική έκθεση ασφάλειας για τις αρχιτεκτονικές δικτύων αποθήκευσης δεδομένων, που εξαρτώνται από την ασφάλεια.

3.5. Κονσόλες διαχείρισης δικτύων αποθήκευσης δεδομένων

Οι κονσόλες που χρησιμοποιούνται για τη διαχείριση των δικτύων αποθήκευσης δεδομένων είναι ένα ακόμα θέμα ασφάλειας προς εξέταση. Οι κονσόλες που χρησιμοποιούνται για τη διαχείριση ενός δικτύου αποθήκευσης δεδομένων είναι συνήθως μια αγνοημένη οντότητα από άποψη προστασίας και

διαχείρισης κινδύνου. Θα έπρεπε η οντότητα που ελέγχει όλα τα ευαίσθητα και κρίσιμα δεδομένα του δικτύου να προστατεύεται σε μεγαλύτερο βαθμό από το μέσο υπολογιστή γραφείου ή κεντρικό υπολογιστή σε ένα τοπικό LAN. Ενώ αυτό μπορεί για κάποιον να είναι κάτι προφανές που δεν χρειάζεται και πολλή εξήγηση, το ποσοστό επισφαλών διοικητικών κονσόλων στα δίκτυα σήμερα μακράν υπερβαίνει οποιοδήποτε αποδεκτό αριθμό. Το βασικό πρόβλημα είναι ότι οι υπεύθυνοι λειτουργίας των δικτύων δεν παίρνουν την απαραίτητη υποστήριξη προκειμένου να ασφαλίσουν τις κρίσιμες μηχανές τους σε μεγαλύτερο βαθμό από τις βασικές μηχανές τους. Όπως είναι γνωστό, δεν είναι όλοι οι κεντρικοί υπολογιστές ίσοι, μερικοί διατηρούν κρίσιμα αρχεία, όπως πηγαίο κώδικα, μερικοί έχουν πρόσβαση σε ευαίσθητα δεδομένα, όπως οι διοικητικές κονσόλες, και μερικοί δεν έχουν ευαίσθητα δεδομένα, όπως MP3 ή αρχεία βίντεο. Ενώ ο κεντρικός υπολογιστής με τα MP3 είναι πιθανών ο σημαντικότερος κεντρικός υπολογιστής για τους περισσότερους υπαλλήλους, δεν απαιτεί ένα υψηλό επίπεδο ασφάλειας. Η πρόσβαση στις κονσόλες πρέπει να περιορίζεται μόνο σε προσωπικό με υψηλό επίπεδο ασφάλειας. Υπάρχουν βασικά λάθη που κάνουν κάποιοι οργανισμοί όπως το ότι οι διοικητικές κονσόλες όχι μόνο έχουν πρόσβαση για να διαχειριστούν το δίκτυο αποθήκευσης, αλλά κάποιες φορές ενθυλακώνουν ευαίσθητες εφαρμογές όπως έχουν οι VERITAS SANPoint (www.b2net.co.uk/veritas/storage_management.html), EMC Control Center (www.emc.com/products/category/subcategory/storage-resource-management.htm) ή CA Storage Resource Manager (ca.com/products/product.aspx?ID=1541).

Ακολουθεί λίστα με τα βασικά θέματα ασφάλειας των κονσολών διαχείρισης δικτύων αποθήκευσης δεδομένων :

- Οι κονσόλες διαχείρισης βρίσκονται συχνά στο κεντρικό εσωτερικό δίκτυο ενός οργανισμού, το οποίο επιτρέπει σε οποιονδήποτε υπάλληλο, σύμβουλο και ενδεχομένως συνεργάτη του οργανισμού να έχει πρόσβαση σε αυτήν την μηχανή μέσα από το δίκτυο.

- Οι κονσόλες διαχείρισης διαμορφώνονται συχνά από τους διαχειριστές δικτύων με βάση μια βασική εταιρική πρακτική. Πολλές από τις επισφαλείς προεπιλογές, τις ελλιπείς επιλογές ασφάλειας και τα «μπαλώματα» (patches) είναι παρόμοια με αυτά του βασικού λειτουργικού συστήματος που

χρησιμοποιείται από το προσωπικό αντί αυτών που χρησιμοποιούνται για κρίσιμους κεντρικούς υπολογιστές όπως οι mail servers, οι βάσεις δεδομένων και οι file servers.

- Οι κονσόλες διαχείρισης συνήθως δεν απαιτούν two-factor επικύρωση, αλλά ένα απλό όνομα χρήστη και κωδικό πρόσβασης. Η δυνατότητα να αποκτηθεί ένας κωδικός πρόσβασης από έναν εσωτερικό έμπιστο χρήστη είναι κάτι απλό.

- Πολλές εφαρμογές διαχείρισης τρέχουν πάνω σε κονσόλες διαχείρισης που χρησιμοποιούν διαμορφώσεις παρόμοιες με αυτές λειτουργικών συστημάτων. Αυτό περιλαμβάνει την εκτέλεση επικίνδυνων υπηρεσιών και εφαρμογών που εξ ορισμού δεν είναι απαραίτητες σε μία κονσόλα διαχείρισης και πραγματικά αυξάνουν τους κινδύνους ασφάλειας των μηχανών.

Το γεγονός ότι οι κονσόλες διαχείρισης ελέγχουν την πρόσβαση και έχουν την δυνατότητα διαγραφής όλων των δεδομένων ενός δικτυού αποθήκευσης δεδομένων δημιουργεί ένα σημαντικό θέμα ασφάλειας. Αυτές οι δυνατότητες καθιστούν τις κονσόλες πρωταρχικούς στόχους για τους επιτιθεμένους.

Παραδείγματα κονσολών:

- IBM® System Storage™ Management Console

  Η IBM® System Storage™ DS6000™ κονσόλα είναι μέλος της οικογένειας των προϊόντων DS και έχει χτιστεί πάνω στην τεχνολογία 2 Gbps fibre channel και παρέχει RAID-protected αποθήκευση με προηγμένες λειτουργίες και εξελιξιμότητα. Η σειρά DS6000 είναι μια λύση αποθήκευσης που θεωρείται ότι προσφέρει υψηλή αξιοπιστία και απόδοση σε επιχειρηματικά περιβάλλοντα.

- Compaq SANworks Tape Storage Management Console

  Η SANworks Tape Storage Management Console (TSMC) είναι ένα browser based εργαλείο διαχείρισης, εγκατάστασης και τη συντήρησης των προϊόντων Direct-Attach και Fibre-Attached σε περιβάλλοντα δικτύων

αποθήκευσης δεδομένων. Η TSMC περιλαμβάνει ικανότητες διάγνωσης, προηγμένων δοκιμών και λειτουργίες διαχείρισης συστήματος με σκοπό αυτές να χρησιμοποιηθούν από τους πελάτες της Compaq και από εκπαιδευμένο προσωπικό.

4ο Κεφάλαιο

4. Ζώνες και ασφάλεια διακοπτών

Το μεγαλύτερο μέρος της ασφάλειας δικτύων επικεντρώνεται στους επιτιθεμένους εντούτοις, η ασφάλεια δικτύων αποθήκευσης δεδομένων βασίζεται στο ότι οι υπάλληλοι ή οι administrators δεν εκτελούν ενέργειες (ή έχουν τη δυνατότητα να εκτελέσουν ενέργειες) που να έχουν αρνητικές επιπτώσεις στο δίκτυο (διακοπή υπηρεσιών δικτύου ή απώλεια δεδομένων).

Οι κίνδυνοι ασφάλειας στους διακόπτες καναλιού οπτικών ινών ποικίλλουν ανάλογα με τον τύπο έκθεσης που θα προκαλέσουν, όπως έκθεση δικτυακής διαχείρισης, δεδομένων, δρομολόγησης ή ρυθμίσεων του δικτύου. Παρακάτω θα περιγράψουμε διάφορους κινδύνους σε διακόπτες καναλιού οπτικών ινών, ανεξάρτητα από τον κατασκευαστή, σχετικά με την ασφάλεια σε δίκτυα αποθήκευσης δεδομένων.

Οι περιοχές που θα εξεταστούν είναι οι ακόλουθες:

- Ζώνες
- Υπερπήδηση ζώνης
- Επιθέσεις σε διακόπτες

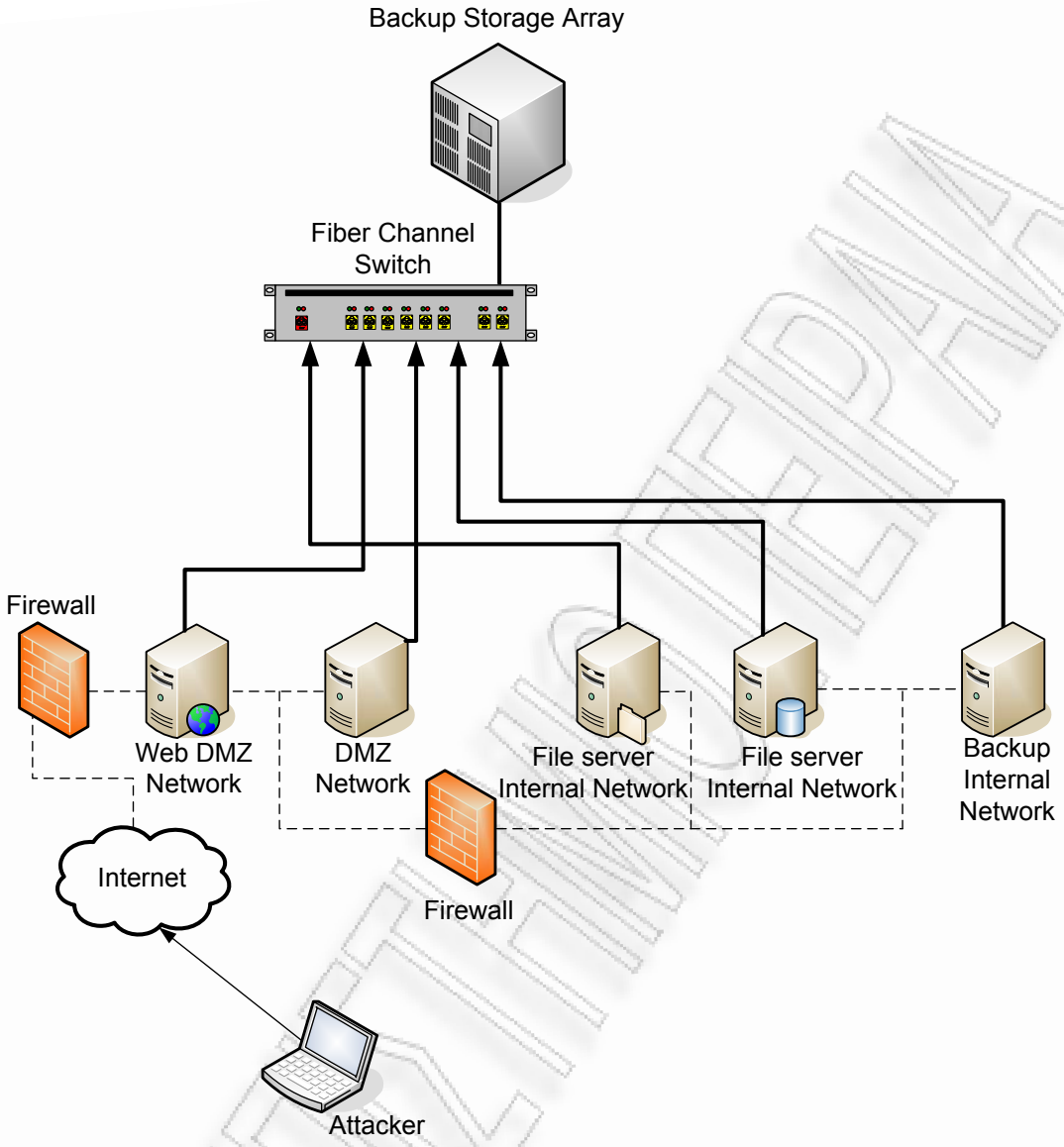
4.1. Δημιουργία ζωνών

Ζώνη είναι ο λογικός χωρισμός κόμβων που συνδέονται με έναν διακόπτη καναλιού οπτικών ινών. Οι ζώνες αρχικά προορίζονταν να χρησιμοποιηθούν ως εργαλείο διαχωρισμού μονάδων δικτύων αποθήκευσης δεδομένων. Ενώ η δημιουργία ζωνών είναι ένα άριστο εργαλείο κατάτμησης, έχει μετατραπεί σε εργαλείο ασφάλειας λόγω της έλλειψης οποιασδήποτε άλλης οντότητας που να μπορεί να παρέχει ασφάλεια. Από την στιγμή που στα δίκτυα αποθήκευσης δεδομένων

συνδέονται κόμβοι με διαφορετικά επίπεδα ασφαλείας η δημιουργία ζωνών πρέπει να χρησιμοποιηθεί για κατάτμηση αλλά και για ασφάλεια.

Το ακόλουθο παράδειγμα θα παρουσιάσει το γιατί η δημιουργία ζωνών είναι ένα καλό εργαλείο κατάτμησης αλλά όχι εργαλείο ασφάλειας. Υποθέτουμε ότι έχουμε 10 αρχεία σε έναν κεντρικό υπολογιστή, αποκαλούμενα A, B, C, D, E, P, G, H, I, και J. τα αρχεία A έως E προορίζονται για τον υπολογιστή 1, και τα αρχεία P έως J προορίζονται για τον υπολογιστή 2. Έστω ότι θέλουμε να χωρίσουμε τα 10 αρχεία σε δύο διαφορετικούς φακέλους, αποκαλούμενους φάκελος 1 και φάκελος 2. Ο υπολογιστής 1 έχει πρόσβαση μόνο στο φάκελο 1 και ο υπολογιστής 2 έχει πρόσβαση μόνο στο φάκελο 2. Τοποθετούμε τα αρχεία A έως E στο φάκελο 1 και P έως J στο φάκελο 2. Στην περίπτωση που υπήρχε ένας πραγματικός file server θα εφαρμόζαμε περιορισμούς πρόσβασης στο φάκελο 1 και 2 έτσι ώστε μόνο ο σωστός υπολογιστής να έχει πρόσβαση στον σωστό φάκελο. Με την δημιουργία ζωνών δεν δημιουργούνται τέτοιοι περιορισμοί πρόσβασης, απλά διαχωρίζονται τα αρχεία δεν υπάρχει κανένα επίπεδο ασφάλειας. Στο παράδειγμά μας ο μόνος περιορισμός είναι ότι ο «υπολογιστής 1» έχει πρόσβαση στον «φάκελο 1» και αντίστοιχα ο «υπολογιστής 2» έχει πρόσβαση στον «φάκελο 2». Η αλλαγή του host name ενός υπολογιστή είναι πολύ εύκολη στα Windows, UNIX και Macintosh, όπως και το WWN ενός HBA με τους οδηγούς οδηγήσεως. Η χρήση της κατάτμησης χωρίς κατάλληλη ασφάλεια αφήνει τα δεδομένα εύκολη λεία για μια κακόβουλη οντότητα.

Γιατί θα ήθελε ένα επιτιθέμενος να χρησιμοποιήσει το κανάλι οπτικών ινών ενός δικτύου αποθήκευσης δεδομένων για να αποκτήσει πρόσβαση αντί του κανονικού IP δικτύου. Αφού εξετάσουμε μια πορεία επίθεσης, θα δούμε ότι το δίκτυο αποθήκευσης δεδομένων μπορεί ενδεχομένως να είναι ευκολότερος στόχος επίθεσης μέσω του οπτικού καναλιού από ότι μέσω του IP δικτύου.



Σχήμα 4.1 Παράδειγμα πορειών επίθεσης δεδομένων

Πορεία μέσω IP network

1. Έκθεση του web server του DMZ.
2. Μέσω του web server, υπονόμευση του εσωτερικού firewall.
3. Μόλις υπονομευθεί το εσωτερικό firewall, εκτίθεται ο εσωτερικός file server.
4. Μόλις εκτεθεί ο file server, εκτίθενται τα δεδομένα.

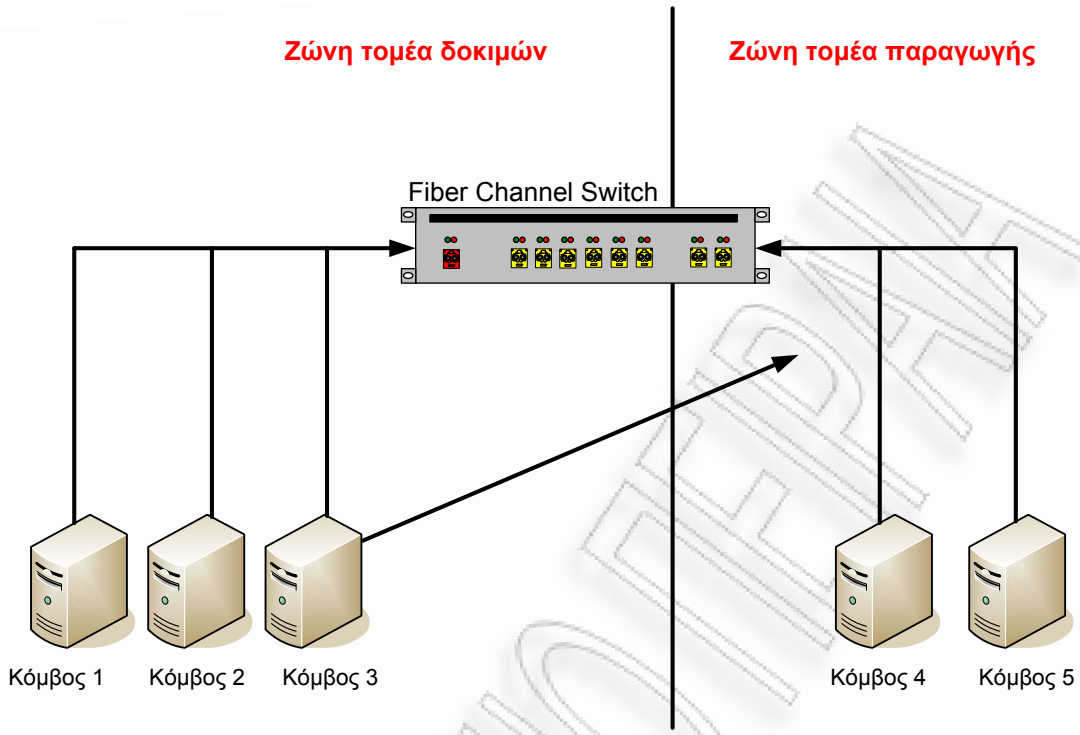
1. Έκθεση του web server.
2. Μετατροπή του WWN και πρόσβαση σε δεδομένα μέσω του storage controller.

Είναι προφανές ότι η πορεία με λιγότερη αντίσταση και το λιγότερο κόπο είναι η δεύτερη. Και οι δύο επιθέσεις στηρίζονται σε ένα επισφαλές λειτουργικό σύστημα. Αφότου εκτεθεί ο web server, μια απλή επίθεση WWN spoofing μπορεί να προκαλέσει προβλήματα προστασίας δεδομένων για ένα δίκτυο αποθήκευσης δεδομένων.

Στο παράδειγμά μας εντούτοις, αν το δίκτυο αποθήκευσης δεδομένων συνδεόταν μόνο με τον κεντρικό υπολογιστή βάσεων δεδομένων, θα ήταν απρόσιτο μέσο του DMZ δικτύου. Το παράδειγμα είναι απλά για να καταδειχθεί ότι τα δίκτυα αποθήκευσης δεδομένων δεν πρέπει να θεωρούνται αυτομάτως ασφαλή λόγω της «αφάνειάς» τους.

4.1.1. Υπερπήδηση ζωνών

Υπερπήδηση ζωνών (Zone hopping) είναι η πράξη εκείνη όπου ένας αναρμόδιος κόμβος στέλνει πλαίσια σε έναν άλλο κόμβο σε μια ζώνη που δεν έχει ή που δεν θα έπρεπε να έχει πρόσβαση. Παραδείγματος χάριν, εάν υποθέσουμε ότι έχουμε κόμβους στη ζώνη δοκιμών και κάποιους άλλους κόμβους στη ζώνη παραγωγής ενός οργανισμού, δε πρέπει ένας κόμβος από τη ζώνη δοκιμών να μπορεί να στέλνει πλαίσια σε ένα κόμβο στη ζώνη παραγωγής. Με την χρήση zone hopping επιθέσεων κάτι τέτοιο θα ήταν εφικτό.



Σχήμα 4.2 Παράδειγμα zone hopping

Η ιδέα της υπερπήδησης (hopping) ζώνης εισήχθη αρχικά, πριν από πολλά χρόνια, στη IP δικτύωση με τις VLAN hopping επιθέσεις. Τα VLANs (εικονικά LANs) είναι λογικές κατατμήσεις των δικτύων IP που συνδέονται με έναν ενιαίο διακόπτη. Παραδείγματος χάριν, εάν έχουμε ένα Cisco διακόπτη της σειράς 6500 με 100 πόρτες, θα μπορούσαμε να χωρίσουμε τις πόρτες σε 10 VLANs,. Ενώ όλες οι συσκευές συνδέονται πραγματικά με έναν φυσικό διακόπτη της Cisco, υπάρχουν ουσιαστικά 10 διαφορετικοί διακόπτες που συνδέουν όλες τις συσκευές ανεξάρτητα. Το VLAN hopping ήταν ένα πολύ μεγάλο πρόβλημα ασφαλείας επειδή πολλά δίκτυα χρησιμοποιούσαν VLANs για να χωρίσουν τα εμπιστευμένα δίκτυα τους από τα untrusted δίκτυα, όπως τα DMZ δίκτυα από τα εσωτερικά δίκτυα. Οι δυνατότητες του VLAN hopping έκαναν το εικονικό χάσμα μεταξύ των δύο δικτύων να είναι επισφαλές και ασταθές. Ενώ η Cisco έχει βελτιώσει δραστικά την τεχνολογία VLAN, οι ζώνες στους διακόπτες καναλιού οπτικών ινών έχουν ακόμα πολύ δρόμο. Όπως έχουμε επαναλάβει πρωτύτερα πολλά είδη επιθέσεων δεν είναι καινούργια, αλλά

μεταλλαγές παλαιότερων επιθέσεων. Η ιδέα του VLAN hopping μπορεί να εφαρμοστεί στα δίκτυα καναλιού οπτικών ινών με την μορφή του zone hopping.

Ο μαλακός (soft) και σκληρός (hard) χωρισμός ζωνών είναι βασισμένοι σε πληροφορίες δρομολόγησης, οι οποίες χρησιμοποιούν τη 24bit διεύθυνση του κάθε κόμβου (παρόμοια με μια διεύθυνση IP σε ένα δίκτυο IP). Η 24bit διεύθυνση προσδιορίζει έναν κόμβο στο fabric χρησιμοποιώντας το στρώμα 2, στρώμα σηματοδοσίας/διαμόρφωσης του καναλιού οπτικών ινών. Η 24bit διεύθυνση, επίσης καλούμενη ως port ID, χρησιμοποιείται για την δρομολόγηση των πλαισίων από έναν κόμβο σε ένα άλλο σε ένα δίκτυο αποθήκευσης δεδομένων. Επιπροσθέτως στο χωρισμό ζωνών, υπάρχουν δύο μέθοδοι για να δημιουργήσουν τα μέλη μιας ζώνης, η μία μέθοδος βασίζεται στο WWN (WWN-based) και η άλλη στην φυσική πόρτα (port-based). Είναι σημαντικό να σημειωθεί ότι η WWN-based ιδιότητα μέλους ζώνης δεν είναι το ίδιο πράγμα με το soft zoning καθώς και η port-based ιδιότητα μέλους ζώνης δεν είναι το ίδιο πράγμα με το hard zoning. Υπάρχει μεγάλη διαφοροποίηση μεταξύ των κατασκευαστών που συγχέει τα τέσσερα αυτά στοιχεία, αλλά είναι διαφορετικά πράγματα. Ακολουθεί ορισμός για κάθε στοιχείο:

- **Hard zoning** - Προκειμένου οι κόμβοι του δικτύου να επικοινωνήσουν ο ένας με τον άλλον και να λάβουν πληροφορίες δρομολόγησης θα πρέπει να υπάρχει έγκριση καθώς και να τους επιτραπεί η πρόσβαση ενεργά μέσω φίλτρων δρομολόγησης. Εάν δύο ή περισσότεροι κόμβοι είναι μέρος της ίδιας ζώνης ή είναι μέρος διαφορετικών ζωνών που επιτρέπεται να επικοινωνήσουν λαμβάνουν πληροφορίες δρομολόγησης προκειμένου να έχουν πρόσβαση ο έναν με τον άλλο. Εάν ένας κόμβος προσπαθούσε να επικοινωνήσει με έναν άλλο κόμβο σε μία ζώνη που δεν του επιτρεπόταν η πρόσβαση, με το hard zoning θα αποτρεπόταν η κυκλοφορία πληροφορίας μεταξύ των δύο κόμβων.

- **Soft zoning** - Προκειμένου οι κόμβοι του δικτύου να επικοινωνήσουν ο ένας με τον άλλον και να λάβουν πληροφορίες δρομολόγησης θα πρέπει να υπάρχει έγκριση, αλλά δεν γίνεται ενεργό φιλτράρισμα για να εξασφαλιστεί η εξουσιοδοτημένη δρομολόγηση. Εάν δύο ή περισσότεροι κόμβοι είναι μέρος της ίδιας ζώνης ή είναι μέρος διαφορετικών ζωνών που επιτρέπεται για να επικοινωνήσουν μεταξύ τους λαμβάνουν απευθείας της πληροφορίες δρομολόγησης προκειμένου να έχουν πρόσβαση ο ένας με τον άλλο. Εάν ένας

κόμβος σε μια ζώνη ξέρει πώς να δρομολογηθεί σε έναν άλλο κόμβο σε μια ζώνη περιορισμένης για αυτόν πρόσβασης, με soft zoning δεν θα περιοριστεί η κυκλοφορία αλλά θα περιόριζε από το να φτάσουν πληροφορίες δρομολόγησης στο αναρμόδιο μέλος ζώνης.

Επιπροσθέτως στα soft και hard zoning, υπάρχουν δύο μέθοδοι προσδιορισμού μελών μιας δεδομένης ζώνης. Παραδείγματος χάριν, μια κοινή μέθοδος για να προσδιορίσει κάποιος σε ποια περιοχή/πόλη κατοικεί είναι ο ταχυδρομικός του κώδικας . Το 17237 είναι ο ταχυδρομικός κώδικας της περιοχής του Υμηττού ενώ 17676 της περιοχής της Καλλιθέας. Μία τηλεφωνική εταιρεία μπορεί να προσδιορίσει σε ποια πόλη (ή νομό) ανήκουμε από τον ταχυδρομικό κώδικα της περιοχής μας. Αυτό το παράδειγμα σχετίζεται με τη WWN-based ζώνης, όπου τα μέλη προσδιορίζονται από το16bit WWN τους. Άλλες μέθοδοι που χρησιμοποιούνται για την κατανομή ιδιότητας μέλους ζώνης είναι ο πραγματικός φυσικός αριθμός πόρτας στο διακόπτη καναλιού οπτικών ινών. Παραδείγματος χάριν, ένας διακόπτης 16 πορτών μπορεί να έχει τέσσερις ζώνες όπου στη ζώνη Α ανήκουν οι πόρτες 1 μέχρι 4, στη ζώνη Β οι 5 μέχρι 8, στη ζώνη Γ οι 9 μέχρι 12 και στη ζώνη Δ οι 13 μέχρι 16. Ακολουθούν περιγραφές των δύο τύπων κατανομής ιδιότητας μέλους ζώνης:

- **WWN zoning** – Η συμμετοχή ενός κόμβου σε μία ζώνη βασίζεται στο WWN του συνδεδεμένου HBA του.

  Η WWN-based συμμετοχή μέλους ζώνης μπορεί να βασίζεται είτε σε node WWN (nWWN) ή port WWN (pWWN) του HBA.
- **Port zoning** - Η συμμετοχή μέλους ζώνης να βασίζεται στη φυσική πόρτα του διακόπτη καναλιού οπτικών ινών που είναι συνδεδεμένο το HBA του συγκεκριμένου κόμβου, ασχέτους WWN.

Δεδομένου ότι υπάρχουν δύο τύποι χωρισμών που μπορούν να χρησιμοποιηθούν και δύο τύποι μεθόδων κατανομής ιδιότητας μέλους ζώνης, μια zone hopping επίθεση θα είναι διαφορετική βάση του τύπου χωρισμού που χρησιμοποιείται και του τύπου ιδιότητας μέλους ζώνης που έχει χρησιμοποιηθεί. Θα αναλύσουμε πώς μία επίθεση μπορεί να ολοκληρωθεί ανάλογα με τους ακόλουθες περιπτώσεις εφαρμογής:

- Soft zoning με WWN-based δημιουργία μελών ζώνης
- Soft zoning με port-based δημιουργία μελών ζώνης
- Hard zoning με WWN-based δημιουργία μελών ζώνης
- Hard zoning με port-based δημιουργία μελών ζώνης

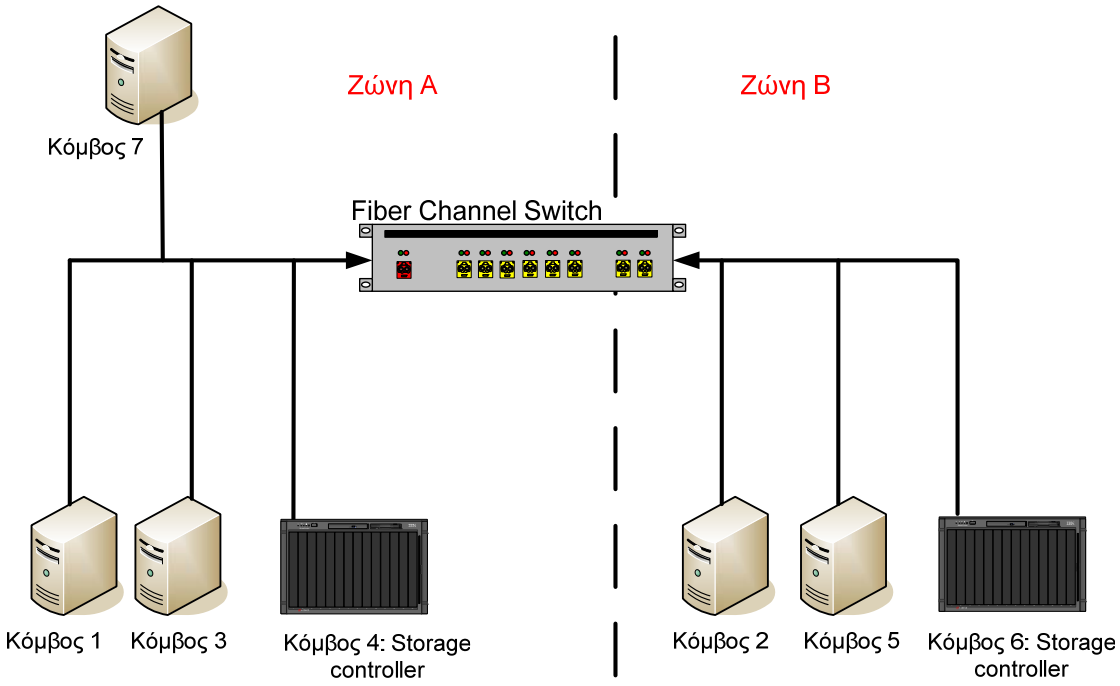
4.1.2. Soft zoning

4.1.2.1. Soft zoning σε συνδυασμό με WWN-based δημιουργία μελών ζώνης

Στη συνέχεια περιγράφονται όλες οι μέθοδοι εκτελέσεις hopping επιθέσεων όταν χρησιμοποιείται soft zoning με WWN-based μεθόδους καθορισμού ιδιότητας μέλους (node ή port WWNs). Πρέπει να σημειωθεί ότι η συντριπτική πλειοψηφία των εφαρμογών δικτύων καναλιού οπτικών ινών χρησιμοποιεί αυτόν τον τύπο διαχωρισμού και κατανομής ζωνών.

4.1.2.1.1. Επιθέσεις σε nWWN - based διαχωρισμό μελών ζώνης

Οι WWN επιθέσεις σαν στόχους έχουν τις ζώνες που είναι σχεδιασμένες με node WWN (nWWN) για να αποκτήσουν τις ιδιότητες μέλους ζώνης. Το σχήμα 4.3 παρουσιάζει ένα παράδειγμα της αρχιτεκτονική με nWWN. Το σχήμα παρουσιάζει ότι έξι κόμβοι καναλιού οπτικών ινών συνδέονται με έναν διακόπτη καναλιού οπτικών ινών. Ο κόμβος ένα, τρία, και τέσσερα είναι στη ζώνη A και κόμβοι δύο, πέντε, και έξι είναι στη ζώνη B. Ο διαχωρισμός έχει γίνει βάση του nWWN του κάθε κόμβου.



Σχήμα 4.3 Παράδειγμα αρχιτεκτονικής ζωνών δικτύων αποθήκευσης δεδομένων

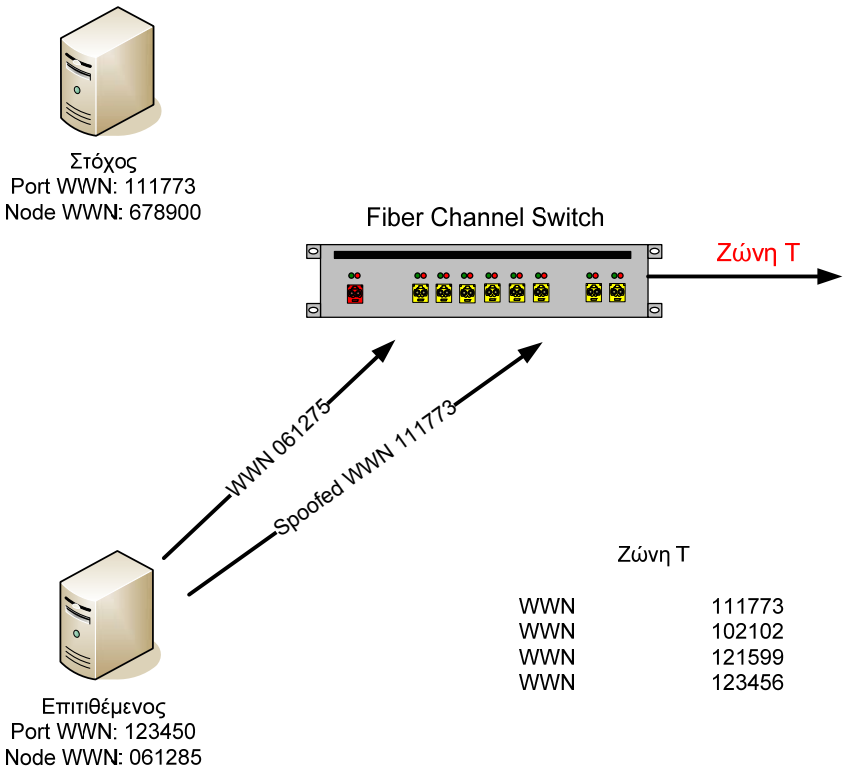
Οι κόμβοι στη ζώνη A δεν εξουσιοδοτούνται για να έχουν πρόσβαση στους κόμβους της ζώνης B. Επιπλέον, ο διακόπτης χρησιμοποιεί τα WWNs για το χωρισμό των ζωνών. Εάν ο κόμβος πέντε, που ανήκει στη ζώνη B, θέλει να επικοινωνήσει με τον ελεγκτή αποθήκευσης στη ζώνη A, θα πρέπει να εξαπατήσει ή να αλλάξει το WWN του για ώστε να είναι το nWWN ενός κόμβου της ζώνης A. Μετά από την αλλαγή του nWWN του κόμβου πέντε ώστε να ταιριάζει με το nWWN του κόμβου ένα, ο διακόπτης θα αναγνωρίσει δύο κόμβους με το ίδιο WWN που προσπαθούν να αποκτήσουν πρόσβαση στα ίδια LUNs στους ελεγκτές αποθήκευσης. Οι συσκευές δικτύων αποθήκευσης καναλιού οπτικών ινών δεν έχουν τη δυνατότητα να έχουν δύο ίδια WWNs στο ίδιο LUN συγχρόνως. Σε αυτό το σημείο, και οι δύο κόμβοι δεν έχουν πρόσβαση στο LUN. Αυτό αντιστοιχεί σε μια επιτυχημένη επίθεση άρνησης – υπηρεσιών (Denial of Service). Σε αυτή την περίπτωση ένας administrator θα προσπαθούσε να επιλύσει το πρόβλημα κάνοντας πιθανότατα επανεκκίνηση στον προβληματικό κόμβο. Με την κίνηση αυτή θα απελευθερωνόταν το LUN καθώς δεν θα υπήρχαν πια δύο κόμβοι να το διεκδικούν αλλά μόνο αυτός του επιτιθεμένου. Στο διάστημα αυτό των 5-10 λεπτών ο επιτιθέμενος έχει την δυνατότητα της ελεύθερης περιήγησης στο LUN.

Πρέπει να σημειωθεί ότι η επίθεση αυτή είναι ακόμα ευκολότερη με ορισμένες διαμορφώσεις διακοπτών. Μερικοί διακόπτες ενημερώνουν τις πληροφορίες κεντρικών υπολογιστών ονομάτων βασισμένοι στις πιο πρόσφατες πληροφορίες που παραλαμβάνουν από το δίκτυο. Παραδείγματος χάριν, εάν ένας επιτιθέμενος εξαπατήσει το WWN του και το αίτημά του είναι η τελευταία πληροφορία που θα πάρει ο διακόπτης, τότε ο διακόπτης θα πετάξει τις πληροφορίες που είχε αρχικά και θα κρατήσει τις πληροφορίες που μόλις έλαβε. Με αυτό τον τρόπο θα χορηγούσε ολικό έλεγχο των δεδομένων σε μία κακόβουλη οντότητα παρά μια επίθεση άρνησης υπηρεσιών. Ο λόγος για τον οποίο πολλοί διακόπτες υποστηρίζουν αυτό το χαρακτηριστικό γνώρισμα είναι για την ανοχή σφαλμάτων. Εάν ένα HBA αποτύχει να συνδεθεί σε έναν κόμβο, μπορεί αυτόματα να μεταπηδήσει στο επόμενο, το οποίο σημαίνει ότι ο διακόπτης καναλιού οπτικών ινών πρέπει να είναι πρόθυμος να λάβει τις νέες πληροφορίες και να ενημερώσει τον κεντρικό υπολογιστή ονομάτων του.

4.1.2.1.2. Επιθέσεις σε pWWN - based διαχωρισμό μελών ζώνης

Οι επιθέσεις WWN με τη χρήση pWWNs είναι δυσκολότερες από αυτές με nWWN, αλλά πιθανές σε ορισμένα περιβάλλοντα. Όταν οι διακόπτες χρησιμοποιούν το pWWN των κόμβων πελατών, προσδιορίζουν κάθε οντότητα που συνδέεται με ένα WWN που είναι στατικό από τη φύση του (σε αντίθεση με τα nWWNs που είναι δυναμικά δεδομένου ότι μπορούν να αλλάξουν). Όπως αναφέρεται προηγουμένως, κάθε HBA έχει δύο τύπους WWN: pWWN και nWWN. Το node WWN των HBAs μπορεί να πάρει οποιαδήποτε αξία, ενώ το port WWN ενός HBA's port δεν μπορεί να αλλαχθεί.

Εάν οι ιδιότητες μέλους ζώνης είναι βασισμένες στο pWWN του HBA ενός πελάτη και η πιστοποίηση ιδιότητας μέλους ζώνης γίνεται μόνο τη χρήση του pWWN ενός πελάτη, έχουμε μια ασφαλή μέθοδο προσδιορισμού πελατών. Υπάρχει βέβαια μέθοδος ακόμα και τα pWWNs να αντιγραφούν, όχι άμεσα αλλά έμμεσα. Στην περίπτωση που για τον προσδιορισμό μέλους ζώνης ερευνάται μόνο το pWWN, το οποίο δεν μπορεί να αλλάξει, τότε ο επιτιθέμενος μπορεί αλλάξει το nWWN του ώστε να ταιριάζει με αυτό του pWWN του στόχου του. Αφού ο έλεγχος γίνεται μόνο για pWWN και όχι και για τα δύο η επίθεση μπορεί να είναι επιτυχής.



Σχήμα 4.4 Αλλαγή του node WWN με το port WWN του στόχου.

4.1.2.2. Soft zoning σε συνδυασμό με port-based δημιουργία μελών ζώνης

Αντίθετα από την περίπτωση που χρησιμοποιούνται nWWNs για την ιδιότητα μέλους ζώνης, η χρήση φυσικών αριθμών πορτών διακόπτη FC για την ιδιότητα μέλους ζώνης έχει διάφορα πλεονεκτήματα ασφάλειας, εντούτοις, έχει και κάποιο λειτουργικό κόστος. Παραδείγματος χάριν, αντί της χρησιμοποίησης nWWNs, για το χαρακτηρισμό μιας εμπιστευμένης οντότητας, που μπορεί αρκετά εύκολα να μετατραπούν από τους τελικούς χρήστες, η χρήση των φυσικών αριθμών λιμένων ως έλεγχος ασφάλειας κάνει το hopping ζώνης ουσιαστικά αδύνατο. Παραδείγματος χάριν, στο σχήμα 4.3, έστω ότι ο κόμβος δύο, ο οποίος ανήκει στη ζώνη B, θέλει να περάσει στη ζώνη A και να επικοινωνήσει με τον κόμβο τέσσερα, ο οποίος είναι ένας εκλεκτής δικτύου αποθήκευσης. Ο πίνακας ιδιότητας μέλους ζώνης στο διακόπτη έχει καταχωρημένο ότι οι πόρτες 1, 3, 4 και 7 ανήκουν στη ζώνη A και οι πόρτες 2, 5, και

6 ανήκουν στη ζώνη Β. Αυτή η αντιστοίχηση καθιστά την επικοινωνία μεταξύ των δύο κόμβων αδύνατη.

Πολλοί κατασκευαστές διακοπτών δεν προωθούν τη χρήση του Port-based χωρισμού λόγω των αδυναμιών ασφάλειάς του. «Ποιες αδυναμίες»; Αν υποθέσουμε ότι ένας οργανισμός είχε έναν υπάλληλο που είχε πρόσβαση στο μηχανογραφικό κέντρο του, θα μπορούσε κακόβουλα ή κατά λάθος να μεταφέρει ένα patch cord από μια πόρτα σε μία άλλη. Σε αυτή την περίπτωση θα μπορούσε ένας κόμβος από μια ζώνη Α να έχει τώρα πρόσβαση σε μία ζώνη Β. Με αυτό τον τρόπο η Port-based μέθοδος χωρισμού ζώνης μπορεί να υπονομευθεί, αλλά απαιτείται φυσική πρόσβαση στο διακόπτη. Αν και αυτό μπορεί να είναι ένα μεγάλο ζήτημα σε ορισμένα κέντρα δεδομένων, οι αδυναμίες των WWN επισκιάζουν τις αδυναμίες της ασφάλειας στη φυσική υποδομή.

Κάτι ακόμα που είναι αρνητικό σε αυτή τη μέθοδο είναι το λειτουργικό κόστος διαχείρισης που έχει. Εάν το δίκτυο αποθήκευσης δεδομένων μας είναι μεταξύ 4 έως 6 διακοπτών, η port-based ιδιότητα μέλους ζώνης είναι πιθανών εύχρηστη , εντούτοις, δεδομένου ότι τα δίκτυα τέτοιου τύπου τείνουν να είναι 12 έως 14 διακόπτων, η port-based ιδιότητα μέλους ζώνης μπορεί να είναι μια πολύ δυσκίνητη διαδικασία και ένας διοικητικός εφιάλτης. Συχνά οι κεντρικοί υπολογιστές διαθέτουν δύο HBA στην περίπτωση όπου καταστραφεί το ένα. Σε αυτή την περίπτωση το λειτουργικό κόστος αλλαγής ζώνης είναι επαχθές. Συγχρόνως, η προστασία των δεδομένων και η συμμόρφωση στους κανονισμούς στηρίζονται σε αυτήν την δυσκίνητη διαδικασία. Φαίνεται ότι τα θετικά επισκιάζουν τα αρνητικά. Σε αυτό το σημείο υπεισέρχεται η διαχείριση κινδύνου.

4.1.3. Hard zoning

Αντίθετα από το soft-zoning, ο hard-zoning χωρισμός ζωνών είναι πολύ δύσκολο να υπονομευθεί. Παρομοίως με το soft-zoning, ο hard-zoning χωρισμός ζωνών διανέμει τις πληροφορίες δρομολόγησης σε όλους τους εξουσιοδοτημένους κόμβους σε μια ενιαία ζώνη ή όλους τους κόμβους που έχουν έγκριση για να έχουν πρόσβαση σε κόμβους σε άλλες ζώνες. Αντίθετα από το soft-zoning, επιβάλλει επίσης τον διαχωρισμό ζωνών με το να επιτρέπει ή όχι την δρομολόγηση ενός πλαισίου από μια ζώνη σε μία άλλη. Αντίθετα από το μαλακό χωρισμό, όπου δεν υπάρχει κανένας

περιορισμός δρομολόγησης πλαισίων μεταξύ των ζωνών, η hard-zoning μέθοδος θα ελέγξει αν ένα πλαίσιο έχει άδεια πρόσβασης σε έναν κόμβο σε μια άλλη ζώνη. Εάν ο κόμβος έχει άδεια, του χορηγείται πρόσβαση, εάν ο κόμβος δεν έχει άδεια και προσπαθεί ενδεχομένως μια επίθεση hopping ζώνης, το πλαίσιο απορρίπτεται.

Με τα οφέλη ασφάλειας του hard-zoning, είναι λογικό να αναρωτιέται κάποιος γιατί το soft-zoning χρησιμοποιείται τόσο ευρέως. Ο πρώτος λόγος είναι ότι υπάρχει παρανόηση με το είναι hard και soft zoning και τι κάνουν στην πραγματικότητα. Επιπλέον, πολλοί τελικοί χρήστες δεν γνωρίζουν το γεγονός ότι ο soft-zoning χωρισμός έχει κάποια περιορισμούς ασφάλειας. Ο κυριότερος λόγος όμως είναι επειδή πολλές εφαρμογές διαχείρισης δεν λειτουργούν καλά με διακόπτες που έχουν εφαρμόσει hard zoning για να διαχωρίσουν ζώνες. Πολλές εφαρμογές διαχείρισης δικτύων αποθήκευσης δεδομένων υποστηρίζουν μόνο τους διακόπτες που χρησιμοποιούν soft-zoning, καθιστώντας το πολύ δύσκολο για ένα administrator να χρησιμοποιεί ένα εργαλείο διαχείρισης για το δίκτυο και ένα άλλο μόνο για τους διακόπτες.

4.1.3.1. Hard zoning σε συνδυασμό με node ή port WWN-based δημιουργία μελών ζώνης

Παρομοίως με τη περίπτωση χρήσης soft-zoning με port-based ιδιότητες μέλους ζώνης, η ίδια ιδέα ισχύει και για Hard zoning. Στην περίπτωση που χρησιμοποιείται Hard zoning για τα πλεονεκτήματα ασφαλείας που έχει και εξακολουθούν να χρησιμοποιούνται nWWNs ή pWWNs για την ανάπτυξη των ζωνών, η δυνατότητα hopping στις ζώνες είναι πιθανή. Επιπλέον, η δυνατότητα hopping σε ζώνες χρησιμοποιώντας WWN επιθέσεις είναι ευκολότερη από ότι με επιθέσεις διακοπτών.

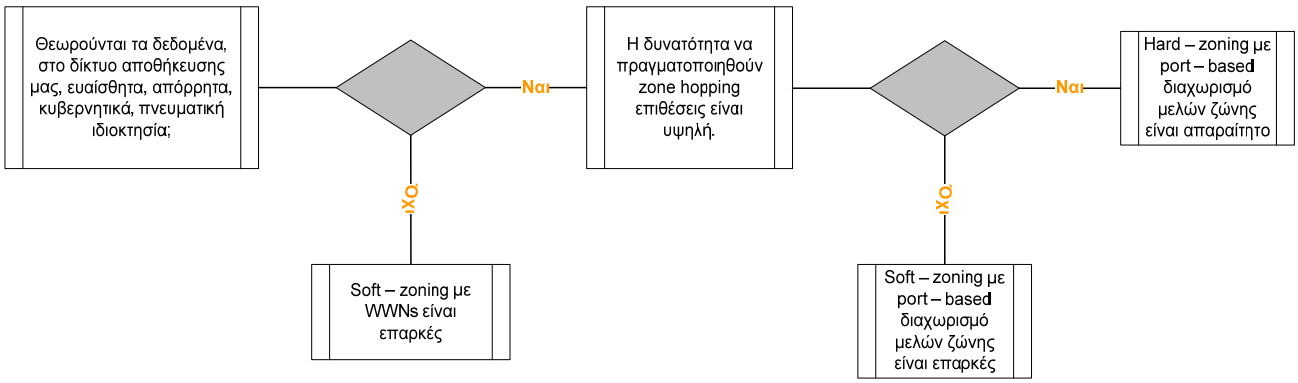
4.1.3.1. Hard zoning σε συνδυασμό με port-based δημιουργία μελών ζώνης

Η μέθοδος Hard zoning χρησιμοποιώντας τις φυσικές πόρτες διακοπτών για την ιδιότητα μέλους ζώνης είναι ασφαλέστερη εναλλακτική στο χωρισμό διακοπτών καναλιού οπτικών ινών. Όχι μόνο οποιαδήποτε επίθεση υποκρισίας WWN είναι

αδύνατη αλλά και οι route-based επιθέσεις θα ήταν επίσης αδύνατες. Η Hard zoning μέθοδος συνδυασμένη με την port-based ιδιότητα μέλους ζώνης είναι ξεκάθαρα η ασφαλέστερη μέθοδος διαμόρφωσης διακόπτη οπτικού καναλιού. Μία δεύτερη με μικρή διαφορά λύση θα ήταν ο συνδυασμός Hard zoning με port WWN, η οποία είναι ένα βήμα μακριά από τη χρήση του φυσικού αριθμού της πόρτας του διακόπτη.

Ενώ αυτή λοιπόν είναι η ασφαλέστερη εναλλακτική λύση, όπως αναφέρεται προηγουμένως, δεν είναι πανάκεια, η διαδικασία διαχείρισης κινδύνου πρέπει να πραγματοποιηθεί ώστε να παρθεί η ορθότερη λύση. Παραδείγματος χάριν, εάν το κέντρο δεδομένων μας έχει ελλιπή φυσική ασφάλεια και οι administrators είναι πολύ απρόσεκτοι τότε μπορεί η WWN - based μέθοδος διαχωρισμού ιδιότητας μέλους ζώνης να είναι ασφαλέστερη από την port – based μέθοδος διαχωρισμού ιδιότητας μέλους ζώνης.

Το σχήμα 4.5 είναι μια υψηλού επίπεδου διαδικασία που θα μπορούσε να χρησιμοποιηθεί για να καθορίσει τον τύπο διαχωρισμού που θα μπορούσε να χρησιμοποιηθεί.



Σχήμα 4.5 Εναλλακτικές zoning.

Το Zone Hopping είναι μια πολύ τετριμμένη επίθεση και μπορεί να εκτελεστεί με διάφορες μεθόδους. Επιπλέον λόγω του γεγονότος ότι το μοναδικό εργαλείο ασφάλειας που χρησιμοποιείται είναι ο διαχωρισμός ζωνών, είναι εύκολα κατανοητό ότι μία ή περισσότερες κακόβουλες οντότητες μπορούν να υποκλέψουν, καταστρέψουν ή να καταστήσουν τα δεδομένα μας μη διαθέσιμα για μια σημαντική χρονική περίοδο. Η zone hopping επίθεση θεωρείται απειλή υψηλού κινδύνου.

4.1.4. Υπερπήδηση ζωνών (WWN) – Σύνοψη επιθέσεως

Περιγραφή επίθεσης – Είσοδος ενός κόμβου σε μία ζώνη όπου δεν έχει δικαιώματα πρόσβασης

Επίπεδο κινδύνου - Υψηλό. Μια κακόβουλη οντότητα μπορεί εύκολα να εκτελέσει μια τέτοια επίθεση

Δυσκολία -Μέτρια. Για να εκτελεστεί μία Zone hopping επίθεση απαιτείται η δυνατότητα αλλαγής ενός WWN, που είναι εύκολο, και οι ζώνες να είναι διαμορφωμένες με τη χρήση nWWN.

Best practice – Τα set των ζωνών θα πρέπει να έχουν διαμορφωθεί με βάση τις φυσικές πόρτες των διακοπτών ώστε να αποφευχθούν WWN spoofing επιθέσεις. Εάν παρόλα αυτά δεν μπορούν να χρησιμοποιηθούν οι φυσικοί αριθμοί και θα πρέπει ο διαχωρισμός μελών ζώνης να βασίζεται σε WWNs, τότε θα πρέπει να χρησιμοποιούνται pWWN και όχι nWWN.

4.1.5. Υπερπήδηση ζωνών (Routing) – Σύνοψη επιθέσεως

Περιγραφή επίθεσης – Είσοδος ενός κόμβου σε μία ζώνη όπου δεν έχει δικαιώματα πρόσβασης

Επίπεδο κινδύνου - Υψηλό. Μια κακόβουλη οντότητα μπορεί εύκολα να εκτελέσει μια τέτοια επίθεση

Δυσκολία – Υψηλή. Η δρομολόγηση προς κόμβους ενός διακόπτη καναλιού οπτικών ινών απαιτεί υλικό και λογισμικό, συσκευές ανάλυσης κυκλοφορίας.

Best practice – Πρέπει να χρησιμοποιείται Hard – zoning ώστε οι πίνακες δρομολόγησης να αποστέλλονται σε κόμβους οι ο οποίοι να ανήκουν στις συγκεκριμένες ζώνες. Έτσι θα αποτρέπονται οι προσπάθειες πρόσβασης κόμβων σε άλλους κόμβους όπου δεν έχουν δικαίωμα πρόσβασης.

4.2. Επιθέσεις διακοπτών

Η παράκαμψη, διαχειριζόμενων από διακόπτες καναλιού οπτικών ινών, ελέγχων ασφαλείας είναι ένας βασικός στόχος των επιτιθέμενων. Υπάρχουν επιθέσεις που σαν στόχο έχουν τις ελλιπείς διαμορφώσεις διακοπτών, αυτές είναι οι ακόλουθες:

- Παρακολούθηση/καταγραφή διακοπτών
- Αντιγραφή E-port
- Συνοπτική δρομολόγηση
- Διαχείριση διακοπτών

4.2.1. Παρακολούθηση/καταγραφή διακοπτών

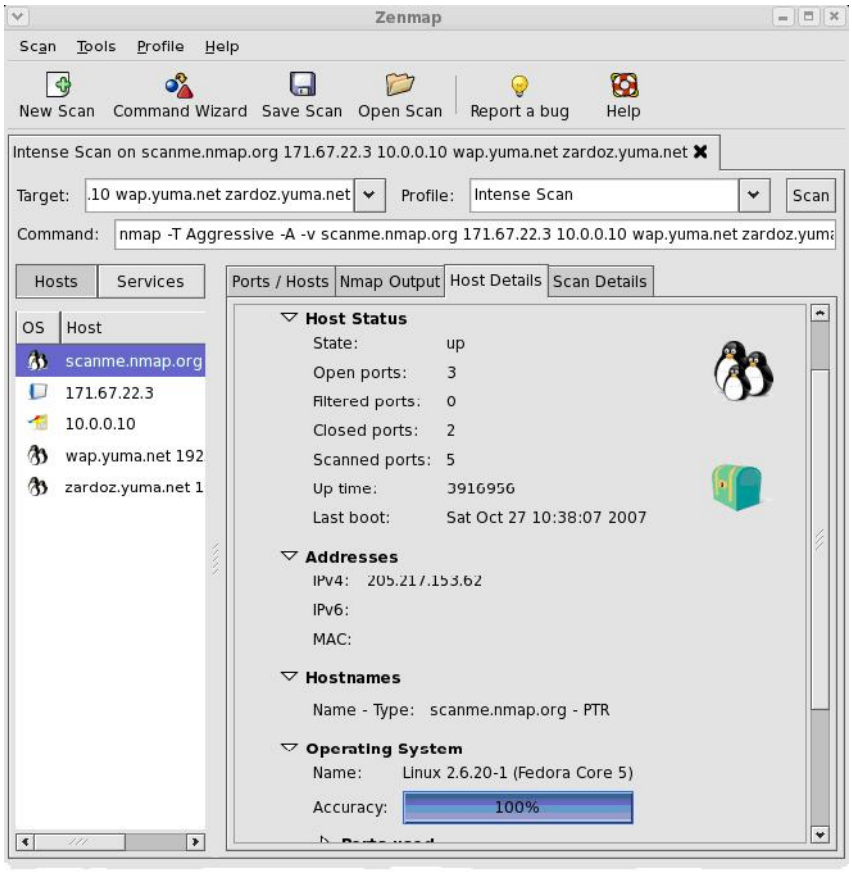
Η παρακολούθηση/καταγραφή διακοπτών απλά περιλαμβάνει τη διαδικασία εκείνη όπου μια σημαντική ποσότητα πληροφοριών του fabric υποκλέπτεται από τη IP διεπαφή διαχείρισης του διακόπτη. Δυστυχώς, από τους περισσότερους διακόπτες καναλιού οπτικών ινών, όπως ο Brocade Silkworm, δεν απαιτείται επικύρωση για να ληφθούν αυτές τις πληροφορίες.

Σχήμα 4.6 Διακόπτης Brocade

Το μόνο που απαιτείται είναι ένας browser, όπως Internet Explorer ή Firefox, και η διεύθυνση IP της Ethernet διεπαφής του FC διακόπτη. Οι Port scanners όπως το nmap είναι μια εύκολη μέθοδος για να ληφθούν όλες οι απαραίτητες πληροφορίες όπως:

- WWNs για spoofing επιθέσεις

- Ονόματα και κατανομή ζωνών για zone hopping
- Fabric γεγονότα
- Fabric τοπολογία
- Πλήρης πληροφορίες ονομάτων κεντρικών υπολογιστών



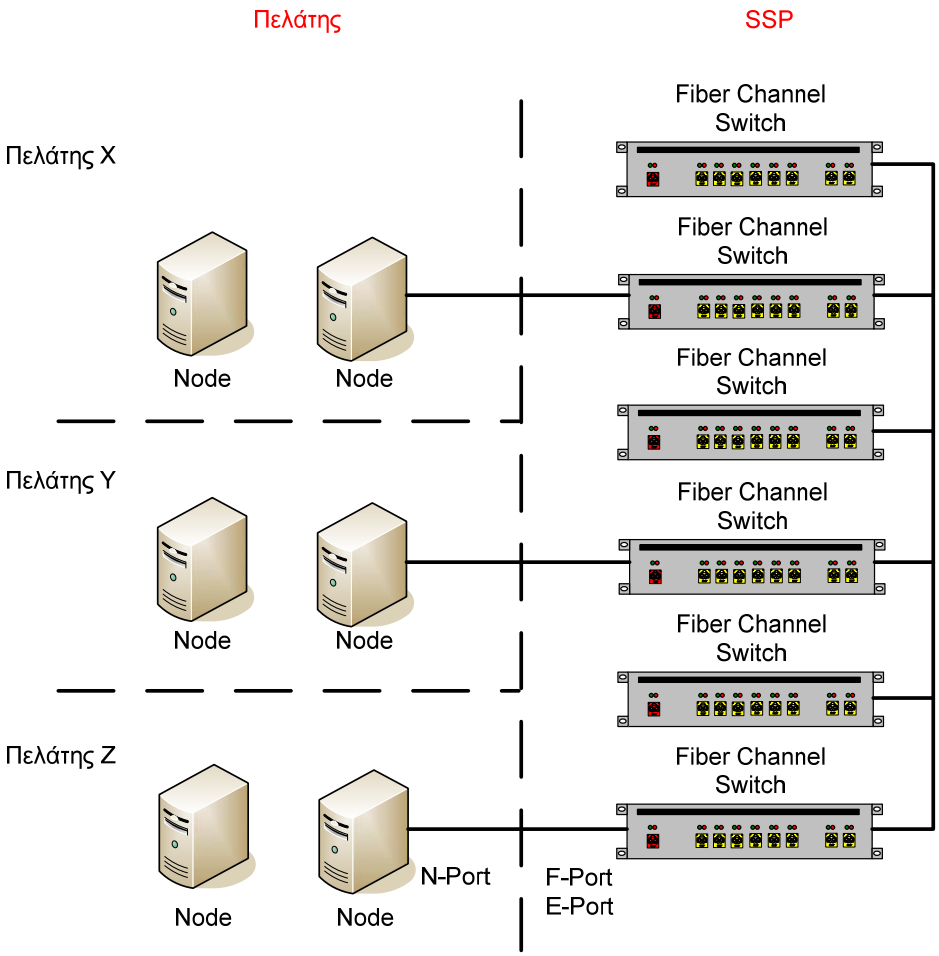
Σχήμα 4.7 Nmap Port scanner

4.2.2. Επιθέσεις αντιγραφής E-port

Η E-Port (Expansion Port) είναι ένας τύπος πόρτας που είναι διαθέσιμος σε όλους τους διακόπτες FC ώστε να έχουν τη δυνατότητα να γίνουν μέρος ενός ενιαίου fabric (παρόμοια με μια uplink port σε έναν διακόπτη Ethernet). Οι E-port συνδέσεις μεταξύ των διακοπτών επιτρέπουν την ανταλλαγή πληροφοριών μεταξύ τους. Το είδος των πληροφοριών που ανταλλάσσεται είναι συνήθως πληροφορίες δρομολόγησης, διαχωρισμού ζωνών και οι τοπολογίες κεντρικών υπολογιστών

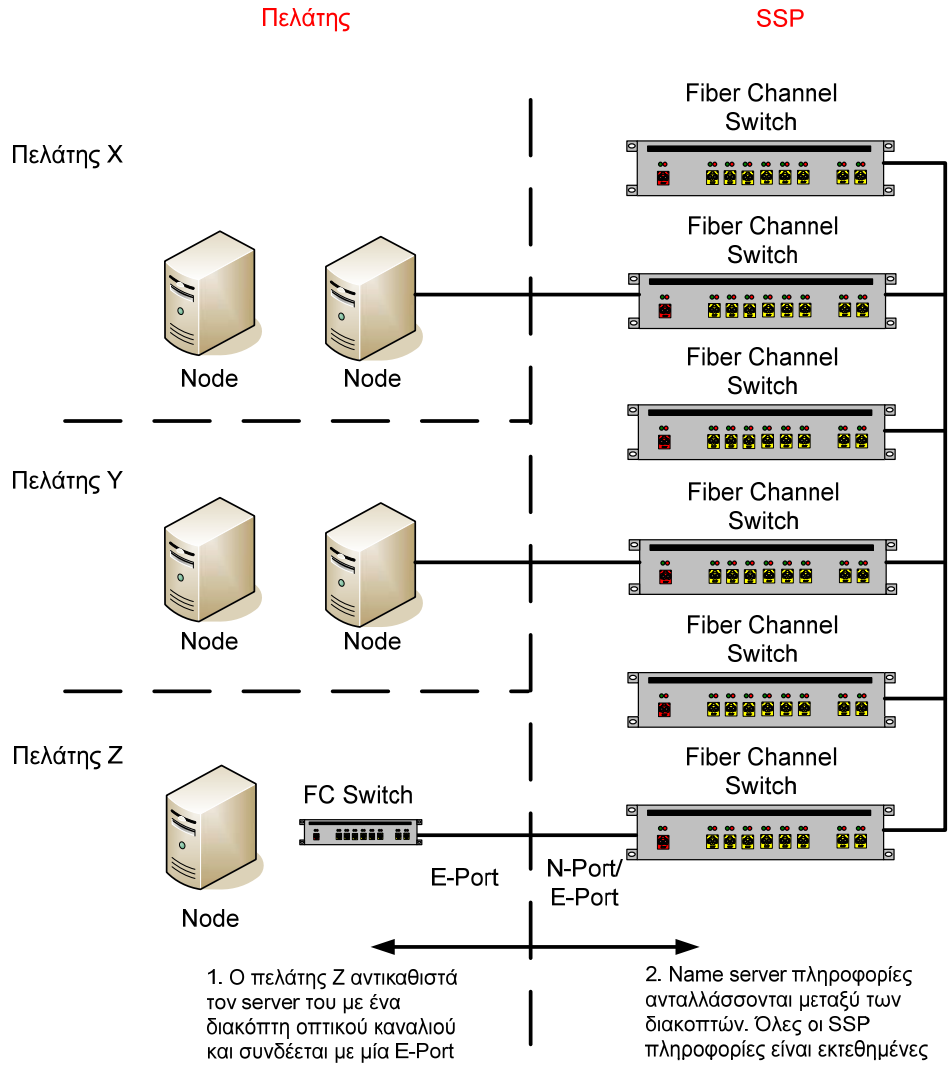
ονομάτων. Το ζήτημα με την E-port αντιγραφή είναι ότι δεν απαιτείται αυθεντικοποίηση προκειμένου δύο διακόπτες που συνδέονται με E-ports να ανταλλάξουν πληροφορίες. Στην περίπτωση των Storage Service Providers (SSPs) εάν στον κόμβο ενός πελάτη ένας κακόβουλος χρήστης συνέδεε ένα διακόπτη οπτικού καναλιού θα είχε στη διάθεσή του τις πληροφορίες δρομολόγησης, διαχωρισμού ζωνών, ολοκλήρου του δικτύου του παρόχου.

Για προστασία ενάντια στο E-port replication, πολλοί διακόπτες διαθέτουν port-type locking, port binding, και key-based αυθεντικοποίηση. Το Port-type locking στην πραγματικότητα κλειδώνει την ιδιότητα μία πόρτας, οπότε όπου δεν είναι αναγκαίο οι πόρτα ενός διακόπτη δεν θα πρέπει να μπορεί να μετατραπεί σε E-port. Το port binding χρησιμοποιείται για να «δέσει» ένα WWN σε μία συγκεκριμένη πόρτα.



Σχήμα 4.8 Αρχιτεκτονική Storage Service Provider.

Η key-based αυθεντικοποίηση χρησιμοποιείται για να αυθεντικοποιηθεί ένας διακόπτης στο fabric. Για να εισέλθει ένας διακόπτης στο δίκτυο θα πρέπει να είναι εγγεγραμμένο το δημόσιο κλειδί του, στην περίπτωση που δεν είναι εγγεγραμμένος ο διακόπτης δεν θα του δίνεται πρόσβαση.



Σχήμα 4.9 E-port replication επίθεση σε αρχιτεκτονική Storage Service Provider.

4.2.2.2. Αντιγραφή E-port - Σύνοψη επιθέσεως

Περιγραφή επιθέσεως – Υποκλοπή ευαίσθητων πληροφοριών ενός δικτύου οπτικού καναλιού από ένα μη αυθεντικοποιημένο διακόπτη μέσω ενός αυθεντικοποιημένου διακόπτη

Επίπεδο κινδύνου - Υψηλό. Μία κακόβουλη οντότητα θα μπορούσε να έχει πρόσβαση σε ολόκληρο το δίκτυο.

Δυσκολία - Μέτρια. Απαιτείται φυσική πρόσβαση και παραλείψεις στη διάρθρωση του δικτύου.

Best practice – Κλείδωμα κάθε πόρτας στην λειτουργία η οποία της έχει ανατεθεί F-port ή E-port.

4.2.3. Συνοπτική δρομολόγηση

Η συνοπτική δρομολόγηση είναι ακόμα ένα χαρακτηριστικό των διακοπτών οπτικών καναλιών το οποίο προσθέτει ένα ακόμα κίνδυνο ασφαλείας. Η συνοπτική δρομολόγηση είναι η δυνατότητα που έχει ένας διακόπτης να δρομολογεί ένα πλαίσιο από μια οντότητα σε μία άλλη έχοντας λάβει μόνο το D_ID του πλαισίου χωρίς να περιμένει να έρθει το S_ID. Αυτή η δυνατότητα αυξάνει δραματικά την απόδοση του δικτυού επιτρέπει όμως σε οποιοδήποτε κόμβο να επικοινωνήσει με οποιοδήποτε κόμβο σε οποιαδήποτε ζώνη. Αυτό ανοίγει την πόρτα σε διάφορες κατηγορίες επίθεσης, αλλά ειδικότερα στην άρνηση - υπηρεσίας και στην παραποίηση δεδομένων.

4.2.4. Διαχείριση διακοπτών

Οι περισσότεροι διακόπτες οπτικού καναλιού έχουν δύο μεθόδους διαχείρισης, είτε μέσω μιας διεπαφής γραμμής εντολών είτε μέσω μιας διεπαφής ιστού. Υπάρχουν δύο θέματα ασφαλείας με τη διαχείριση των διακοπτών. Το ένα είναι η χρήση clear-text πρωτοκόλλων, όπως Telnet για τη διεπαφή γραμμής εντολών και το HTTP για τη διεπαφή ιστού. Τα HTTP και Telnet είναι clear-text πρωτόκολλα, που σημαίνει ότι καθένας στο δίκτυο με ένα IP sniffer θα μπορούσε να υποκλέψει το όνομα χρήστη και κωδικό πρόσβασης που χρησιμοποιούνται από τον administrator. Η χρήση διακοπτών Ethernet αντί για hub δεν αποτρέπει τον επιτιθέμενο, δεδομένου ότι οι Man-in-the-Middle επιθέσεις είναι αρκετά τετριμμένες στα δίκτυα IP.

Με τη χρήση οποιουδήποτε sniffer, όπως το Ethereal, είμαστε σε θέση να αποκτήσουμε το όνομα χρήστη και τον κωδικό πρόσβασης του χρήστη και να

εκθέσουμε το διακόπτη. Ενώ μερικοί διακόπτες καναλιού οπτικών ινών έχουν τη δυνατότητα να εφαρμόσουν SSH, οι περισσότεροι έρχονται μόνο με την Telnet πρόσβαση ενεργοποιημένη. Το πλήθος των δεδομένων και λειτουργιών που μπορεί να διαχειριστεί κανείς από το διακόπτη είναι πολύ μεγάλο και απαιτείται η ανάλογη προσοχή.

Η διαχείριση ενός διακόπτη μπορεί επίσης να διεξαχθεί μέσο μιας διεπαφής ιστού (HTTP). Πρέπει να σημειωθεί ότι πολλοί διακόπτες καναλιού οπτικών ινών χρησιμοποιούν HTTP για τη διαχείριση μέσω ιστού αλλά επιτρέπουν επίσης στον τελικό χρήστη να κάνει έναρξη μιας συνόδου Telnet από ένα Java applet στη μηχανή αναζήτησης ιστού. Είτε με τον ένα είτε με τον άλλο τρόπο χρησιμοποιείται clear text επικοινωνία.

Η χρήση των clear-text πρωτοκόλλων για τη διαχείριση κάνει όλα τα ευαίσθητα και κρίσιμα δεδομένα εκτεθειμένα σε μια απλή επίθεση που έχει προσδιοριστεί εδώ και 20 έτη. Εντούτοις, το ζήτημα των clear-text πρωτοκόλλων δεν αφορά αποκλειστικά και μόνο τους διακόπτες καναλιού οπτικών ινών. Πολλές άλλες συσκευές αποθήκευσης, συμπεριλαμβανομένων των ελεγκτών αποθήκευσης και του λογισμικού διαχείρισης, χρησιμοποιούν clear-text πρωτόκολλα για την πρόσβαση.

Οι επιθέσεις διαχείρισης διακοπτών είναι πολύ απλές επιθέσεις δεδομένου ότι είτε δεν απαιτείται επικύρωση ή η επικύρωση διευθύνεται από επισφαλή πρωτόκολλα όπως Telnet ή HTTP. Δεδομένου ότι η πρόσβαση στους διακόπτες θα οδηγούσε σε έκθεση των δεδομένων, η επισφαλής διαχείριση διακοπτών είναι ένα σοβαρό πρόβλημα για τις αρχιτεκτονικές δικτύων αποθήκευσης δεδομένων.

4.2.4.1 Διαχείριση διακοπτών – Σύνοψη επιθέσεως

Περιγραφή επιθέσεως – Επίθεση στις HTTP ή Telnet διεπαφές, που είναι clear-text, και διαχείριση της συσκευής.

Επίπεδο κινδύνου – Μέτριο. Μια κακόβουλη οντότητα θα μπορούσε να αποκτήσει πρόσβαση σε πληροφορίες του δικτύου.

Επίπεδο δυσκολίας – Χαμηλό. Ο επιτιθέμενος το μόνο που χρειάζεται είναι ένας web browser για να αποκτήσει στοιχεία του δικτύου από το διακόπτη.

Best practice – Πρέπει να διασφαλιστεί ότι οι διεπαφές διαχείρισης υλικού και λογισμικού θα είναι ασφαλείς από αναρμόδιους χρήστες.

5ο Κεφάλαιο

5. Ασφάλεια δικτύων καναλιού οπτικών ινών

Όπως προκύπτει από τις αδυναμίες ασφάλειας και τις μεθόδους επιθέσεων, πρέπει να καθοριστεί το πώς θα εξασφαλιστούν τα δεδομένα του δικτύου μας.

Σε αυτό το κεφάλαιο θα αναλυθούν οι καλύτερες πρακτικές άμυνας για τις επιθέσεις σε δίκτυα αποθήκευσης δεδομένων. Στα κεφάλαια 2 μέχρι 4 αναλύθηκαν οι παρακάτω επιθέσεις:

- Session hijacking
- Man-in-the-Middle attacks
- Name server pollution
- LUN masking
- WWN spoofing
- Zone hopping (WWN)
- Zone hopping (routing)
- E-port replication
- Switch management

Όπως είδαμε τα προβλήματα ασφαλείας σε δίκτυα καναλιού οπτικών ινών δεν είναι και λίγα. Πολλά δίκτυα αυτού του τύπου σχεδιάζονται με την λανθασμένη εντύπωση ότι είναι αδιάτρητα. Στις περισσότερες περιπτώσεις ο «εχθρός» είναι κάποια εξωτερική οντότητα, στην περίπτωση των δικτύων αποθήκευσης δεδομένων υπάρχει και ο εσωτερικός κίνδυνος. Οι τυχαίες αλλαγές διαμόρφωσης, τα λάθη εφαρμογής και η ανακριβής τροποποιήσεις σε συσκευές αποθήκευσης από τους εξουσιοδοτημένους χρήστες είναι μια άλλη κρίσιμη πτυχή της ασφάλειας των δικτύων αποθήκευσης δεδομένων. Από οποία προοπτική και αν το δει κανείς, η ασφάλεια είναι επιτακτική ανάγκη.

Θα ασχοληθούμε με τις ακόλουθες περιοχές:

- Fibre Channel Layer 2
- Authentication
- Zoning and VSAN s
- Port type security
- Port security
- Switch security
- Name server queries
- Securing storage tapes with encryption

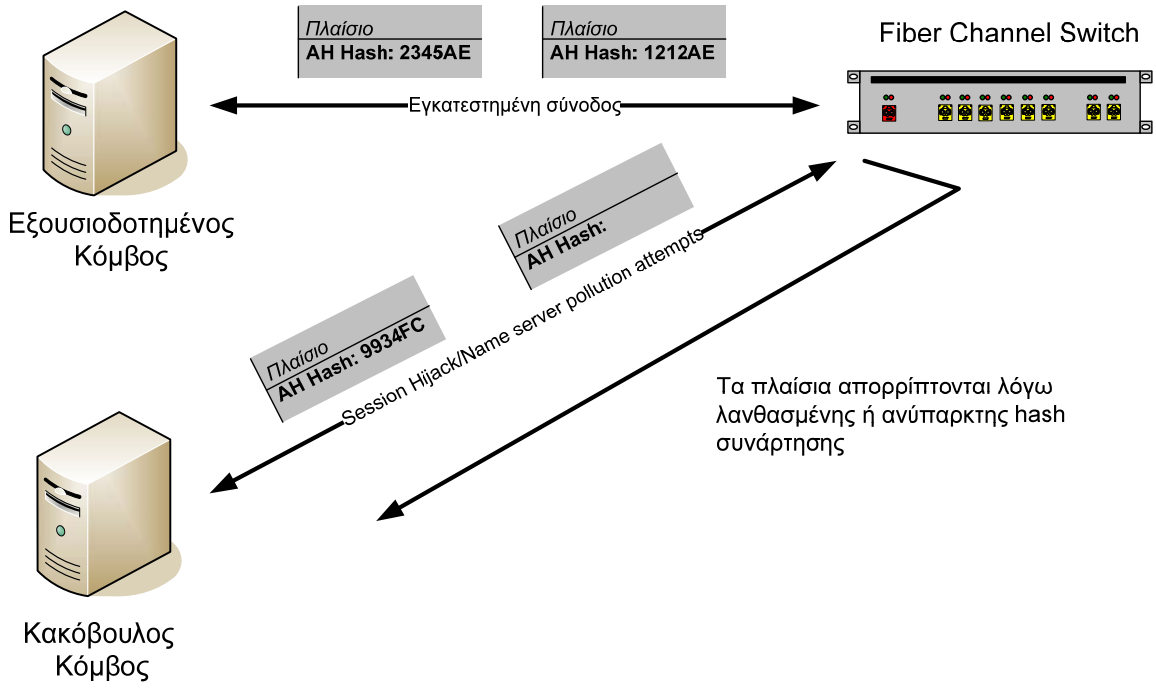
5.1. Ασφάλεια στρώματος 2 καναλιού οπτικών ινών

Το πρώτο σύνολο αμυντικών μέτρων που θα συζητήσουμε είναι για τις επιθέσεις του στρώματος 2 καναλιού οπτικών ινών. Τα πλαίσια καναλιού οπτικών ινών και συγκεκριμένα οι αριθμοί ελέγχου ακολουθίας, η ταυτότητα ακολουθιών, οι διευθύνσεις πηγής/προορισμού και οι διαδικασίες FLOGI και PLOGI, οφείλουν τις αδυναμίες τους στην έλλειψη επικύρωσης. Η έλλειψη επικύρωσης σε ένα μέσο επικοινωνίας δεν είναι καινούργιο πρόβλημα για τους αρχιτέκτονες ασφάλειας δικτύων. Τα IP δίκτυα είχαν το ίδιο πρόβλημα για πολλά έτη (και ακόμα το έχουν). Οι μέθοδοι που χρησιμοποιούνται για να αποτραπούν τέτοιου είδους επιθέσεις στα δίκτυα IP είναι η κρυπτογράφηση, ο έλεγχος ακεραιότητας και η αυθεντικοποίηση, τα οποία ισχύουν και για τα δίκτυα καναλιού οπτικών ινών. Το κανάλι οπτικών ινών μπορεί να υιοθετήσει την επικύρωση και κρυπτογράφηση μεταξύ των κόμβων και να είναι σε θέση να αποτρέψει επιθέσεις του στρώματος 2. Οι δύο μέθοδοι προστασίας ενάντια στις επιθέσεις που διευκρινίζονται στο πρωτόκολλο ασφάλειας καναλιών ινών (FC-SP) είναι οι εξής:

- Encapsulating Security Protocol (ESP):
  www.tll.org/ftp/t1I/pub/fc/sp/ 03-I49vO.pdf
- Authentication Headers (AH):
  www.t1I.org/ftp/t1I/pub/fc/sp/03-I49vO.pdf

Το Encapsulating Security Protocol (ESP) μπορεί να χρησιμοποιηθεί για να παρέχει κρυπτογράφηση ή επικύρωση στα πλαίσια καναλιού οπτικών ινών σε και από τους διακόπτες, τους κόμβους πελατών και τους ελεγκτές αποθήκευσης. Η αυθεντικοποίηση είναι ένα θέμα προς εξέταση, αλλά δεν παρέχει προστασία από τις επιθέσεις στρώματος δικτύου, εντούτοις, αποτρέπει άλλες επιθέσεις που συζητούνται παρακάτω. Για προστασία από τις επιθέσεις του στρώματος 2 καναλιού οπτικών ινών, πρέπει οι πληροφορίες συνόδου, η διαδικασία αναπροσαρμογής δρομολόγησης και οι PLOGI/FLOGI διαδικασίες να κρυπτογραφηθούν για να αποτραπεί η λήψη πληροφοριών πλαισίου από τους επιτιθεμένους ώστε να εκτελέσουν μια επίθεση.

Μια άλλη μέθοδος άμυνας ενάντια σε επιθέσεις, που δεν έχει τον αντίκτυπο απόδοσης που έχει η κρυπτογράφηση (εμπιστευτικότητα) στα πλαίσια καναλιού οπτικών ινών είναι τα Authentication Headers (AH), με τη χρήση MD5 ή SHA1 hashes συναρτήσεων. Η AH μέθοδος μπορεί να χρησιμοποιηθεί για να παρέχει ακεραιότητα σε κάθε πλαίσιο καθώς και ένα στρώμα εικονικής επικύρωσης. Η AH επιτρέπει σε ένα διακόπτη να εξασφαλίσει ότι επικοινωνεί με ένα εξουσιοδοτημένο οικοδεσπότη στο δίκτυο και όχι με έναν κακόβουλο κόμβο που έχει υποκλέψει τις πληροφορίες συνόδου ή τις port addresses. Η AH μέθοδος έχει τη δυνατότητα να δημιουργήσει μια hash συνάρτηση για κάθε πλαίσιο και να την ενσωματώσει στο πλαίσιο. Εάν γίνουν οποιεσδήποτε τροποποιήσεις σε ένα πλαίσιο ή εάν ένα άλλο πλαίσιο σταλθεί με ανακριβής hash συνάρτηση, η λαμβάνουσα οντότητα θα απορρίψει απλά το πλαίσιο και θα το ταξινομήσει ως ανακριβές. Η πειρατεία συνόδου, η επίθεση ενδιάμεσης οντότητας και η name server pollution επίθεση ως μέθοδοι είτε τροποποιούν ένα υπάρχον πλαίσιο είτε δημιουργούν ένα νέο πλαίσιο και το στέλνουν στο στόχο τους. Εάν χρησιμοποιούταν AH, όλες αυτές οι επιθέσεις θα ήταν άχρηστες, αποτρέποντας τον επιτιθέμενο από τη έκθεση των δεδομένων ή ακόμα και τη δημιουργία επιθέσεων άρνησης υπηρεσιών σε ένα δίκτυο αποθήκευσης δεδομένων. Επιπλέον, δεδομένου ότι η AH παρέχει υπηρεσίες hash για κάθε πλαίσιο, ο αντίκτυπος απόδοσης θα ήταν αρκετά μικρός δεδομένου ότι δεν υπάρχει κρυπτογράφηση.



Σχήμα 5.1 AH επικεφαλίδες

Όσο αφορά τις διαδικασίες FLOGI και PLOGI αυτό που θα έπρεπε να εφαρμοστεί από τους κατασκευαστές, πέρα από την κρυπτογράφηση η οποία θα είχε ένα αντίκτυπο στη απόδοση, είναι η χρήση μίας μεθόδου δημιουργίας τυχαίων αριθμών Seq_CNT. Κάτι τέτοιο δεν θα είχε αντίκτυπο στην απόδοση, μιας και η αλλαγή γίνεται σε μία ήδη υπάρχουσα τιμή και δεν προστίθεται κάτι επιπλέον στα πλαίσια. Εκτός από την παραγωγή ενός απρόβλεπτου και τυχαίου Seq_CNT, θα ήταν επίσης ιδανικό για την ταυτότητα ακολουθίας να μην είναι στατικός αριθμός. Η αλλαγή του Seq_ID σε μη-στατικό αριθμό θα το καθιστούσε δυσκολότερο για έναν επιτιθέμενο να προσδιορίσει τη σύνοδο στην οποία θέλει να επιτεθεί. Ένας μη-στατικός μεταβλητός αριθμός θα καθιστούσε τις διοικητικές οντότητες συνόδου του δικτύου δυσκολότερο να προβλεφθούν και επομένως δυσκολότερο να εκτεθούν.

Με τις μεθόδους ασφάλειας στρώματος 2, είτε με τη χρήση κρυπτογράφησης είτε μέσω αλλαγών σε επίπεδο πλαισίου, μπορούν να αποφευχθούν οι Session hijacking, Man-in-the-Middle, Name server pollution επιθέσεις.

5.2. Αυθεντικοποίηση

Η έλλειψη αυθεντικοποίησης είναι ένα μεγάλο πρόβλημα για τα δίκτυα αποθήκευσης δεδομένων. Το ζήτημα είναι ότι οι παράμετροι αυθεντικοποίησης, που διέθεταν τα δίκτυα αυτά, ήταν ευαίσθητες σε υποκλοπή και αντιγραφή. Αυτό δίνει σε οποιοδήποτε κόμβο την δυνατότητα να αλλάξει την ταυτότητα αυθεντικοποίησης του (WWN) και να αποκτήσει πρόσβαση σε LUNs του δικτύου. Λόγω του ότι στις οντότητες σε ένα δίκτυο αποθήκευσης δεδομένων δεν υπάρχει αυθεντικοποίηση παρά μόνο εξουσιοδότηση, ο επιτιθέμενος μπορεί να «μεταμφιεστεί» σε οποιονδήποτε επιθυμεί και να αποκτήσει πρόσβαση στο δίκτυο.

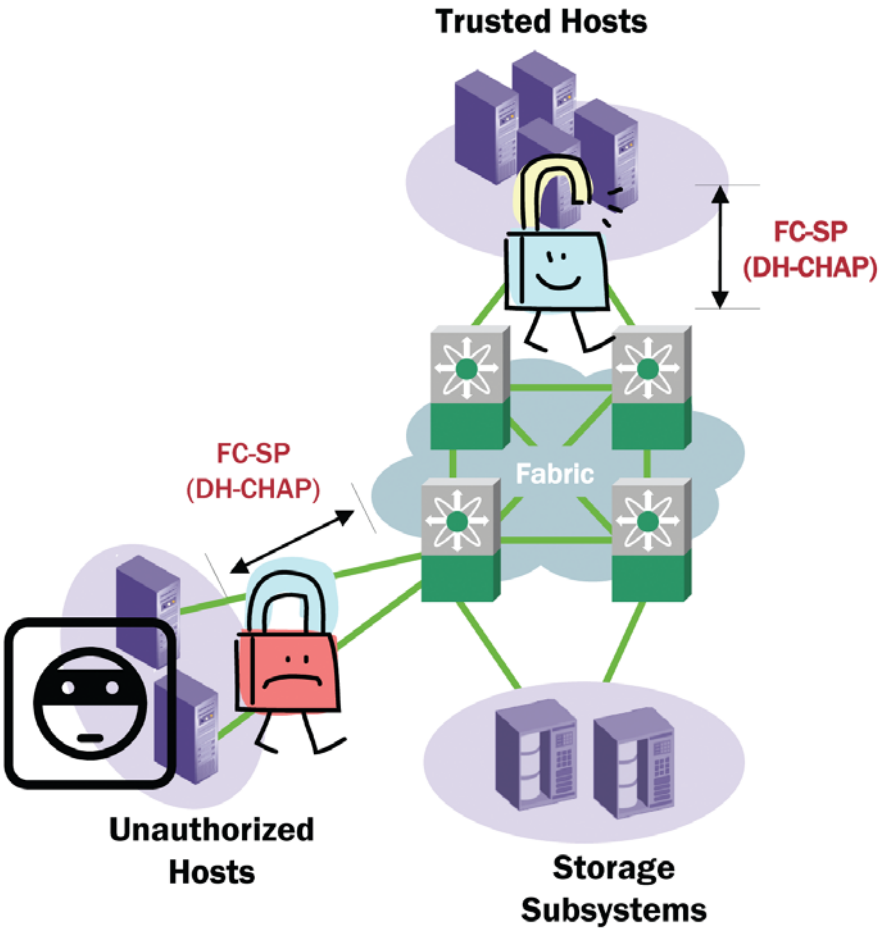
Υπάρχουν διάφορες μέθοδοι αυθεντικοποίησης αν και πολλοί κατασκευαστές δεν τις υποστηρίζουν όλες ακόμα. Παρόλα αυτά δυνατότητα να χρησιμοποιηθεί κάποιο είδος αυθεντικοποίησης είναι σημαντικό ζήτημα ασφάλειας των δικτύων αποθήκευσης δεδομένων. Παρακάτω θα αναλύσουμε τις εξής μεθόδους αυθεντικοποίησης:

- FC-SP
- DH-CHAP
- FCAP
- FCPAP
- CT authentication

5.2.1. Πρωτόκολλα ασφάλειας (FC-SP)

Τα πρωτόκολλα ασφάλειας καναλιού οπτικών ινών αναπτύχθηκαν από την *Επιτροπή T11* (www.T11.org) προκειμένου να εφαρμοστεί ασφάλεια στα δίκτυα αποθήκευσης δεδομένων. Το πρότυπο περιλαμβάνει αυθεντικοποίηση, διαμοιρασμό κλειδιών, ακεραιότητα και εμπιστευτικότητα σε κάθε πλαίσιο καναλιού οπτικών ινών. Το FC-SP αφορά μια ποικιλία διαφορετικών μεθόδων συμπεριλαμβανομένων των *Diffie-Hellman CHAP* (DH-DHCP) , *Fibre Channel Authentication Protocol*

(FCAP), *Fibre Channel Password Authentication Protocol* (FCPAP) και *Common Transport Authentication* (CT).



Σχήμα 5.2.α. DH-CHAP

5.2.2. Diffie-Hellman CHAP (DH-CHAP)

Το Diffie-Hellman CHAP μπορεί να χρησιμοποιηθεί για επικύρωση μεταξύ των διακοπτών καναλιού οπτικών ινών και είναι το πρότυπο για το πρωτόκολλο ασφάλειας καναλιού ινών (FC-SP). Το DH-CHAP επιτρέπει την επικύρωση μεταξύ των κόμβων πελατών και των διακοπτών ή των διακοπτών και των ελεγκτών αποθήκευσης. Στο DH-CHAP, είτε ένας κόμβος πελατών με HBA, είτε ένας διακόπτης είτε ένας ελεγκτής αποθήκευση μπορεί να είναι είτε ιδρυτής διαδικασίας

επικύρωσης ή αποκριτής επικύρωσης. Ανάλογα με το ποια οντότητα αρχίζει τη διαδικασία επικύρωσης καθορίζεται ποια οντότητα θα είναι ο ιδρυτής και ο αποκριτής. Το Diffie-Hellman CHAP είναι τρωτό στις χωρίς σύνδεση επιθέσεις λεξικού. Εάν χρησιμοποιηθεί DH-CHAP, απαιτούνται οι ακόλουθες διαδικασίες μεταξύ οποιουδήποτε κόμβου στο fabric:

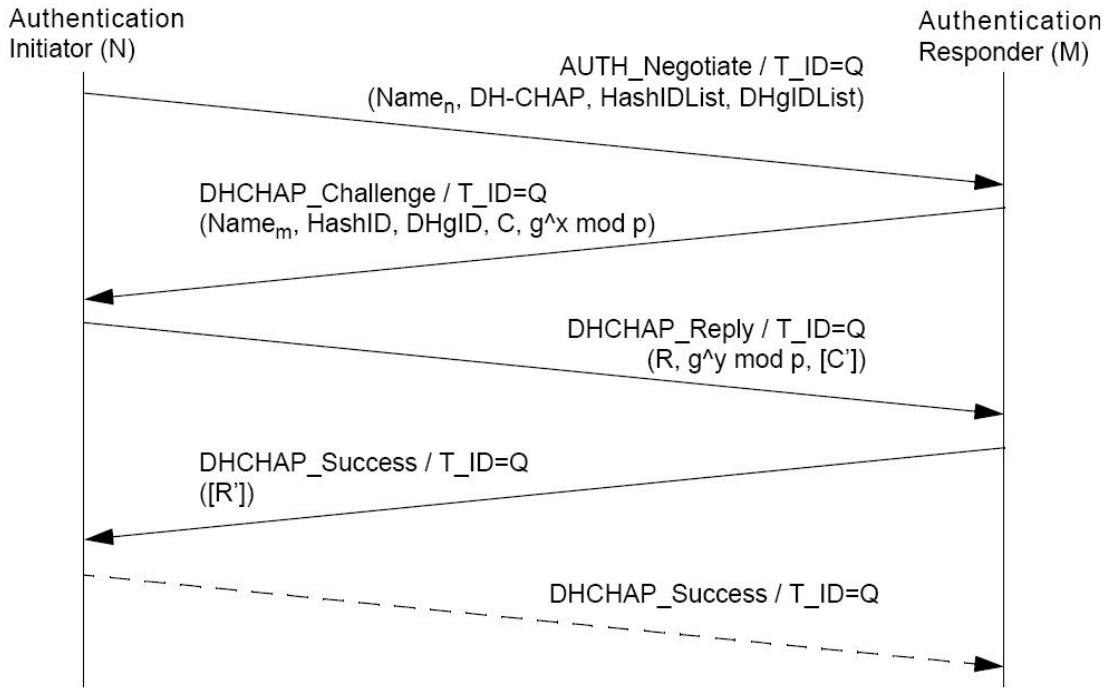
1. Ο ιδρυτής διαδικασίας επικύρωσης θα στείλει ένα Auth_Node μήνυμα στον αποκριτή επικύρωσης για διαπραγμάτευση των hash συναρτήσεων. Το Auth_Node μήνυμα περιέχει το node_name, συναρτήσεις hash (SHA1 ή MD5), και τα Diffie-Hellman προσδιοριστικά.

2. Ο αποκριτής επικύρωσης θα απαντήσει με ένα μήνυμα το οποίο περιέχει το Node_name, μία hash συνάρτηση και τις πληροφορίες της ομάδας DH.

3. Ο ιδρυτής διαδικασίας επικύρωσης θα στείλει ένα μήνυμα με την απάντηση του μηνύματος πρόκλησης και τις DH πληροφορίες. Η απάντηση θα είναι ένας συνδυασμός της πρόκλησης, ενός κοινού μυστικού και της hash συνάρτησης.

   Σημείωση: Ο ιδρυτής της διαδικασίας μπορεί επίσης να στείλει μια πρόκληση στον αποκριτή για αμοιβαία επικύρωση.

4. Εάν η απάντηση είναι σωστή, ο αποκριτής θα στείλει ένα μήνυμα επιτυχίας, το οποίο σημαίνει ότι ο ιδρυτής έχει επικυρωθεί.



Σχήμα 5.2.β. DH-CHAP πρωτόκολλο (**T11/Project 1570-D/Rev 1.2**)

Μια πρώτη πιθανή αδυναμία αυτής της μεθόδου είναι η περίπτωση της επίθεσης replay. Εάν τα διαστήματα εμφάνισης νέου μηνύματος πρόκλησης που στέλνεται από τον αποκριτή είναι μεγάλα, ενδέχεται ένας επιτιθέμενος που παρακολουθεί να συλλάβει την επαναλαμβανόμενη hash συνάρτηση από το βήμα 3 και απλά να στείλει ένα μήνυμα επανάληψης στον αποκριτή και να αποκτήσει σύνδεση. Ο αποκριτής θα το δεχόταν δεδομένου ότι περιέχει τη σωστή hash συνάρτηση. Εάν ο αποκριτής στέλνει σε μικρά διαστήματα νέο μήνυμα πρόκλησης στον πελάτη, η παλαιά hash αξία που λαμβάνεται από τον επιτιθέμενο θα ήταν άχρηστη με αποτέλεσμα την αποτροπή της επιθέσεως επανάληψης από ένα αναρμόδιο χρήστη.

Η δεύτερη αδυναμία της μεθόδου παρουσιάζεται λόγω των ανακλάσεων των CHAP μηνυμάτων που έχουμε στις περιπτώσεις πολλαπλών συνδέσεων. Στην περίπτωση όπου ο επιτιθέμενος αποστείλει ένα αίτημα για αυθεντικοποίηση σε έναν αυθεντικοποιητή θα λάβει το μήνυμα πρόκλησης, το πρόβλημα του τώρα είναι ότι δεν γνωρίζει το κοινό μυστικό ώστε να δημιουργήσει την σωστή hash συνάρτηση. Ο επιτιθέμενος τώρα μπορεί να στείλει το μήνυμα πρόκληση που έλαβε σε ένα κόμβο που προσπαθεί να αυθεντικοποιηθεί. Ο κόμβος θα απαντήσει με την hash συνάρτηση

η οποία έχει δημιουργηθεί από το αρχικό μήνυμα πρόκληση και το κοινό μυστικό. Επομένως ο επιτιθέμενος έχει τώρα στην διάθεσή του την σωστή hash και την οποία μπορεί να παρουσιάσει στον αρχικό αυθεντικοποιητή. Ο κόμβος θα πάρει την hash που περιμένει, αποτελούμενη από το μήνυμα πρόκληση και το κοινό μυστικό, και θα αυθεντικοποιήσει τον κακόβουλο κόμβο. Πρέπει βέβαια να σημειωθεί ότι το μήνυμα πρόκλησης δεν παραμένει το ίδιο για μεγάλο χρονικό διάστημα.

5.2.3. Πρωτόκολλο αυθεντικοποίησης καναλιού οπτικών ινών (FC-AP)

Το Fibre Channel Authentication Protocol είναι μια εναλλακτική μέθοδος για αυθεντικοποίηση, σε ένα δίκτυο αποθήκευσης δεδομένων, βασισμένη σε ψηφιακά πιστοποιητικά. Δύο κόμβοι καναλιού οπτικών ινών πρέπει να μοιράζονται ένα μυστικό κλειδί που θα χρησιμοποιείται για τα ψηφιακά πιστοποιητικά, έτσι θα μπορούν αμοιβαία να επικυρώσουν ο ένας τον άλλον και να επικοινωνήσουν με ασφάλεια. Εάν πρόκειται να χρησιμοποιηθεί FCAP, απαιτούνται οι ακόλουθες διαδικασίες μεταξύ οποιουδήποτε κόμβου στο δίκτυο:

1. Ένας ιδρυτής επικύρωσης θα στείλει ένα μήνυμα Auth_Node στον αποκριτή επικύρωσης για να διαπραγματευτεί τις hash συναρτήσεις. Το μήνυμα Auth_Node περιέχει το node_name, το FCAP σήμα, hash συναρτήσεις και τα χρησιμοποιήσιμα προσδιοριστικά ομάδας Diffie-Hellman.

2. Ο αποκριτής επικύρωσης θα απάντησει με ένα FCAP _Request μήνυμα, το οποίο θα περιλάβει το ψηφιακό πιστοποιητικό του αποκριτή, το επιλεγμένο hash function, την παράμετρο ομάδας DH και ένα μοναδικό αριθμό.

3. Ο ιδρυτής θα ελέγξει το πιστοποιητικό με μια Αρχή Πιστοποιητικών (CA) και θα παραγάγει έναν τυχαίο αριθμό. Μετά από την επαλήθευση, θα στείλει ένα FCAP_Acknowledge μήνυμα που περιέχει τον μοναδικό αριθμό, τον παραγμένο τυχαίο αριθμό, το ψηφιακό πιστοποιητικό του, την παράμετρο ομάδας DH και την υπογραφή του.

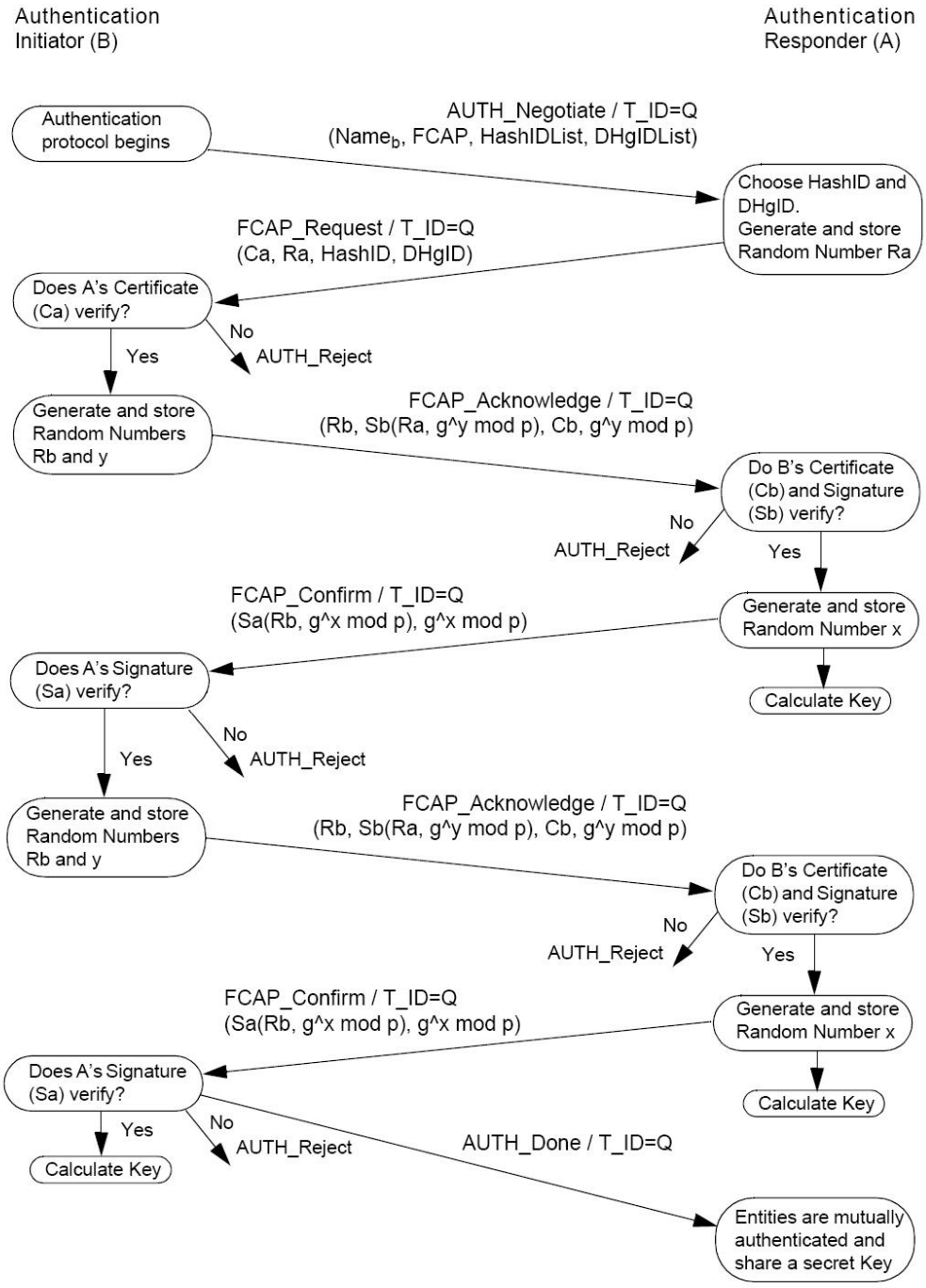
4. Ο αποκριτής θα λάβει το FCAP _Acknowledge μήνυμα και θα ελέγξει το πιστοποιητικό του ιδρυτή με την CA και την υπογραφή του με το δημόσιο κλειδί του. Θα παραγάγει έναν διαφορετικό τυχαίο αριθμό και θα στείλει ένα FCAP _Confirm μήνυμα με την υπογραφή του και την παράμετρο ομάδας DH.

5. Ο ιδρυτής θα ελέγξει την υπογραφή με το δημόσιο κλειδί του αποκριτή. Αφότου ελέγξει την υπογραφή, έχει τώρα όλες τις οντότητες για να υπολογίσει το κοινό κλειδί που χρησιμοποιείται από τον αποκριτή (αποθηκευμένο μοναδικό αριθμό, παράμετρο ομάδας DH, hash συνάρτηση). Απ' αυτή τη στιγμή και οι δύο οντότητες έχουν το κοινό κλειδί που χρησιμοποιείται για τα ψηφιακά πιστοποιητικά.

6. Ο αποκριτής θα στείλει ένα FCAP _Confirm μήνυμα με μια υπογραφή και την παράμετρο ομάδας DH.

7. Ο ιδρυτής θα λάβει το FCAP _Confirm μήνυμα και θα ελέγξει την υπογραφή με το δημόσιο κλειδί του αποκριτή, θα χρησιμοποιήσει έπειτα το αποθηκευμένο μοναδικό αριθμό, την παράμετρο ομάδας DH και την hash συνάρτησης για να εξασφαλίζει ότι ταιριάζουν με τις αρχικές.

8. Ο ιδρυτής θα στείλει έπειτα ένα μήνυμα Auth_Done. Η FCAP διαδικασία έχει ολοκληρωθεί επιτυχώς.



Σχήμα 5.3 FCAP πρωτόκολλο (**T11/Project 1570-D/Rev 1.2**)

5.2.4. Πρωτόκολλο αυθεντικοποίησης κωδικού πρόσβασης (FCPAP)

Το Fibre Channel Password Authentication Protocol (FCPAP) είναι επίσης μια εναλλακτική μέθοδος για επικύρωση σε ένα δίκτυο αποθήκευσης δεδομένων το οποίο χρησιμοποιεί SRP (Secure Remote Password Protocol) μηχανισμό. Το FCPAP

προσφέρει αμοιβαία αυθεντικοποίηση, και ανταλλαγή κλειδιών, βασισμένη σε ένα κοινό μυστικό κλειδί. Το SRP απαιτεί έναν κωδικό πρόσβασης, ένα salt και ένα verifier. Εάν πρόκειται να χρησιμοποιηθεί FCPAP, απαιτούνται οι ακόλουθες διαδικασίες μεταξύ οποιουδήποτε κόμβου στο δίκτυο:

1. Ένας ιδρυτής επικύρωσης θα στείλει ένα μήνυμα Auth_Node στον αποκριτή επικύρωσης για να διαπραγματευτεί τις συναρτήσεις hash. Το μήνυμα Auth_Node περιέχει το node_name, το σήμα FCPAP, τις hash συναρτήσεις και τα χρησιμοποιήσιμα προσδιοριστικά ομάδας Diffie-Hellman.

2. Ο αποκριτής θα επιλέξει το salt και τον verifier και θα δημιουργήσει ένα ιδιωτικό κλειδί προκειμένου να δημιουργηθεί ένα δημόσιο κλειδί. Θα απαντήσει στον ιδρυτή με ένα μήνυμα FCPAP _Init που περιέχει το όνομά του, μια μονόδρομη hash που χρησιμοποιήθηκε για να παραγάγει τον verifier, την παράμετρο ομάδας DH, το δημόσιο κλειδί και το salt.

3. Ο ιδρυτής θα λάβει το μήνυμα FCPAP _Init και θα δημιουργήσει και αυτός ένα ιδιωτικό κλειδί προκειμένου να δημιουργήσει ένα δημόσιο κλειδί. Θα πάρει και τα δύο δημόσια κλειδιά (αποκριτή και ιδρυτή) για να δημιουργήσει μια παράμετρο. Ο ιδρυτής θα δημιουργήσει έπειτα ένα άλλο ιδιωτικό κλειδί από το salt του αποκριτή και του κωδικού πρόσβασής του για να δημιουργήσει μια εκθετική αξία. Ο ιδρυτής θα πάρει έπειτα αυτήν την αξία, το δημόσιο κλειδί του και το public κλειδί του αποκριτή, και θα δημιουργήσει μία hash συνάρτηση. Ο ιδρυτής στέλνει έπειτα ένα FCPAP _Accept μήνυμα το οποίο περιέχει το δημόσιο κλειδί του και αυτή την καινούργια hash.

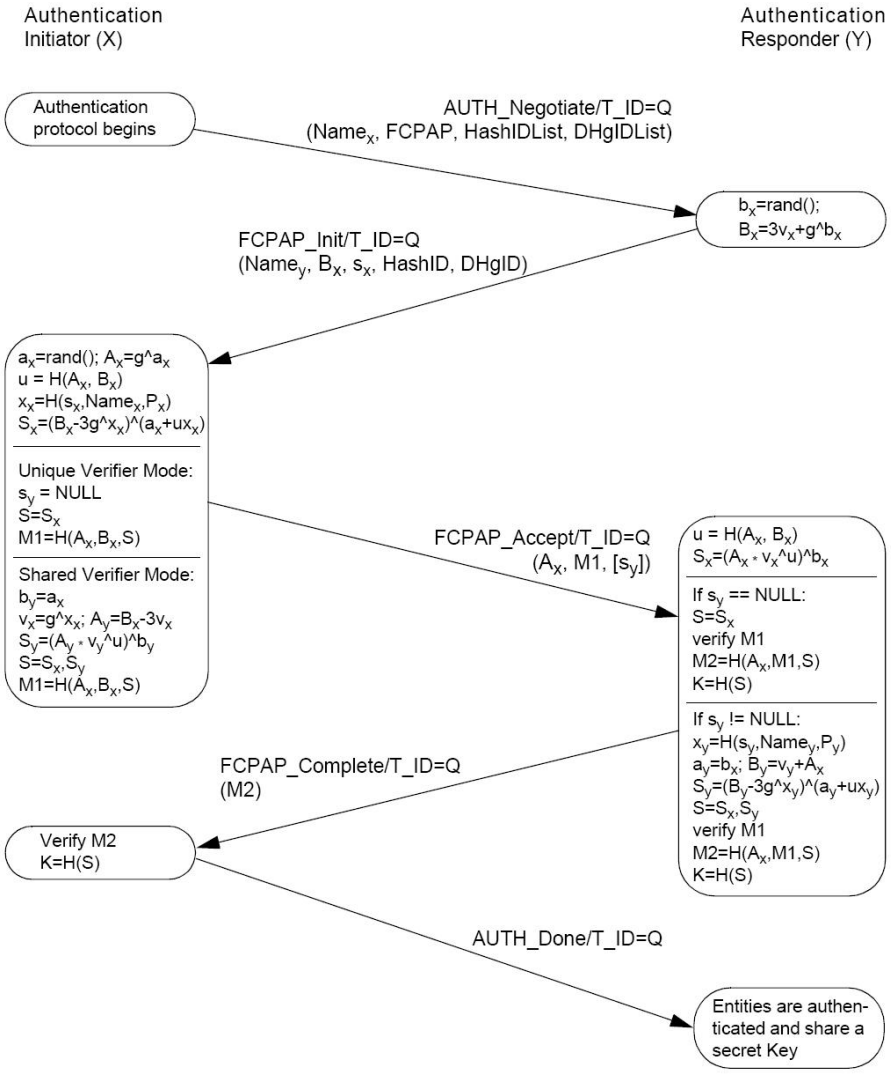
   α. Εάν το salt έχει μηδενική αξία τότε χρησιμοποιείται ο μοναδικός verifier.

   β. Εάν χρησιμοποιηθεί το salt του αποκριτή, θα χρησιμοποιηθεί ο κοινός verifier.

4. Ο αποκριτής θα λάβει ένα FCPAP _Accept μήνυμα και θα υπολογίσει την παράμετρο, την εκθετική αξία, και τη hash συνάρτηση. Εάν όλες οι

τιμές συμφωνήσουν, ο αποκριτής θα στείλει ένα FCPAP _Complete μήνυμα με τη hash που προέρχεται από το δημόσιο κλειδί του ιδρυτή, το πρώτο hash και το κλειδί συνόδου.

5. Ο ιδρυτής θα λάβει το FCPAP _Complete μήνυμα και θα υπολογίσει και αυτός το δεύτερο hash από το δημόσιο κλειδί του, το πρώτο hash, και το κλειδί συνόδου. Εάν ταιριάξουν, θα στείλει ένα μήνυμα Auth_Done στον αποκριτή που επισημαίνει ότι ολοκληρώθηκε επιτυχώς η αυθεντικοποίηση.



Σχήμα 5.4 FCPAP πρωτόκολλο (**T11/Project 1570-D/Rev 1.2**)

Το DH-CHAP φαίνεται να υιοθετείται ευρέως από τους σημαντικότερους κατασκευαστές μέχρι σήμερα. Η προτυποποίηση για την να εφαρμογή της αυθεντικοποίηση μέσα στα δίκτυα αποθήκευσης δεδομένων θα είναι κάτι πολύ σημαντικό για τον τελικό χρήστη. Επιπλέον, η διαλειτουργικότητα μεταξύ των προμηθευτών θα είναι επίσης αρκετά σημαντική προκειμένου να πραγματοποιείται σωστά η αυθεντικοποίηση.

5.2.5. Αυθεντικοποίηση Common Transport (CT)

Η Common Transport (CT) αυθεντικοποίηση μπορεί να χρησιμοποιηθεί για αυθεντικοποίηση επικοινωνίας που εκτελείται συνήθως για in-band διοικητικούς λόγους και αναπτύχθηκε από το FC-GS-4 (Fibre Channel Generic Service 4). Η επικύρωση CT παρέχει μια επικεφαλίδα ασφάλειας στα πλαίσια αίτησης καναλιού οπτικών ινών. Το αίτημα και η απάντηση χρησιμοποιούν μυστικά κλειδιά, μοναδικές hash συναρτήσεις και ψηφιακές υπογραφές για να εξασφαλίσουν την επικοινωνία. Η χρήση της επικύρωσης CT θα επιτρέψει την εξασφάλιση των διοικητικών λειτουργιών από μία in-band επικοινωνία χωρίς να χρειάζεται out-of-band τεχνολογίες, οι οποίες είναι συνήθως IP-based.

Η εφαρμογή αυθεντικοποίησης στο κανάλι οπτικών ινών θα μετριάσει το κίνδυνο από τις LUN masking, WWN spoofing, zone hopping και E-port replication επιθέσεις. Αυτό που πρέπει να κατανοήσουμε είναι ότι ακόμα και αυθεντικοποίηση αν εφαρμόζεται ένα WWN μπορεί να υποκλαπεί και να αντιγραφεί, το αντιγραμμένο αυτό WWN όμως δεν έχει την δυνατότητα, λόγω της αυθεντικοποίησης, να χορηγήσει πρόσβαση στον επιτιθέμενο, κάτι που αυτήν την περίοδο είναι απόν σε πολλές αρχιτεκτονικές δικτύων αποθήκευσης δεδομένων.

Η έλλειψη επικύρωσης σε ένα fabric ανοίγει την πόρτα σε πολλούς επιτιθεμένους. Η χρήση των αδύνατων (spoofable) προσδιοριστικών για την έγκριση και η χρήση των εργαλείων κατάτμησης που εμπιστεύονται πλήρως τα αδύνατα (spoofable) προσδιοριστικά είναι πιο τρωτά χωρίς επικύρωση. Η χρηση οποιασδήποτε από τις επιλογές επικύρωσης που περιγράψαμε θα κάνει τους οργανισμούς πιο ανθεκτικούς σε επιθέσεις όπως οι LUN masking, WWN spoofing και Zone hopping.

5.3. Διαχωρισμός Ζωνών

Ο διαχωρισμός ζωνών είναι ακόμα μια μέθοδος για προστασία των LUNs σε ένα δίκτυο αποθήκευσης δεδομένων. Γεγονός είναι ότι υπάρχουν ασφαλείς μέθοδοι διαχωρισμού σε ζώνες, αλλά χρησιμοποιούνται σπάνια και προεπιλεγμένα είναι εκτός λειτουργίας. Οι δύο τύποι ασφαλούς χωρισμού, όπως έχουν αναλυθεί, είναι αφενός ο σκληρός, που λειτουργεί με επιβολή δρομολόγησης των πλαισίων καναλιού οπτικών ινών και αφετέρου ο διαχωρισμός βάση πορτών, ο οποίος είναι κατάτμηση των κόμβων σε ένα δίκτυο με βάση το φυσικό αριθμό των πορτών τους σε έναν διακόπτη καναλιού οπτικών ινών. Η προεπιλεγμένη μέθοδος διαχωρισμού σε ζώνες που χρησιμοποιείται στους περισσότερους διακόπτες είναι Soft zoning με WWN-based ζώνες.

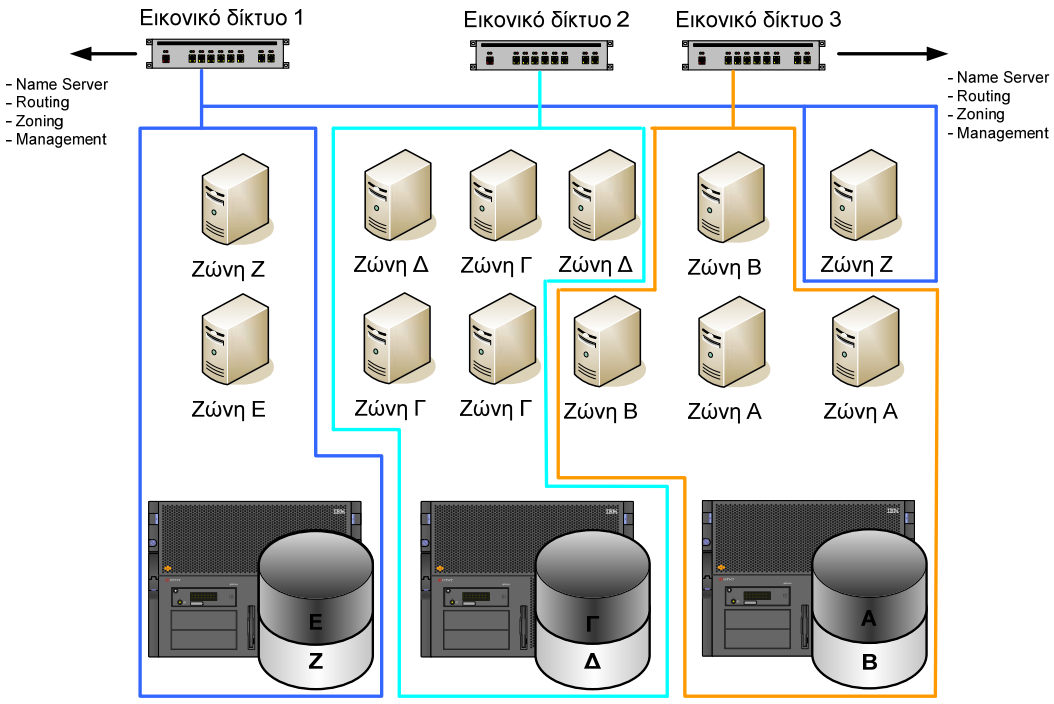
5.4. Εικονικά δίκτυα αποθήκευσης δεδομένων

Όπως αναφέραμε παραπάνω η μέθοδος hard zoning και οι port-based ζώνες βελτιώνουν εντυπωσιακά την ασφάλεια σε ένα δίκτυο αποθήκευσης δεδομένων. Ας δούμε τώρα μια άλλη μέθοδο, τα εικονικά δίκτυα αποθήκευσης δεδομένων τα οποία είναι ένα μία τεχνολογία η οποία αναπτύχθηκε και υποστηρίχθηκε από τα συστήματα της Cisco. Οι περισσότεροι διακόπτες καναλιού οπτικών ινών συμπεριλαμβανομένων των Brocade, McData, και Qlogic, χρησιμοποιούν τους παραδοσιακούς τύπους κατάτμησης. Οι διακόπτες MDS της Cisco επίσης υποστηρίζουν αυτούς τους τύπους διαχωρισμού, αλλά έχουν εισαγάγει έναν νέο τύπο κατάτμησης αποκαλούμενο ως εικονικό δίκτυο αποθήκευσης δεδομένων. Παρόμοια με τα εικονικά LANs (VLANs), υπάρχει η δυνατότητα δημιουργίας εικονικών περιοχών σε ένα δίκτυο αποθήκευσης δεδομένων. Αυτός ο τύπος κατάτμησης είναι ένα σπουδαίο εργαλείο ασφάλειας επειδή δημιουργεί δίκτυα που είναι απομονωμένα μεταξύ τους και δεν μοιράζονται πληροφορίες δρομολόγησης, υπηρεσίες ονόματος, και ιδιότητες χωρισμού. Για παράδειγμα, εάν τέσσερα υποδίκτυα έχουν δημιουργηθεί σε ένα δίκτυο αποθήκευσης δεδομένων, θα υπήρχαν τέσσερις name servers, τέσσερα fabrics και τέσσερις τοπικές ομάδες δρομολόγησης.

Το εικονικά αυτά δίκτυα μπορούν να διαμορφωθούν χρησιμοποιώντας δύο τύπους μεθόδων: Στατικά και δυναμικά. Στατικά είναι η περίπτωση όπου χρησιμοποιούνται οι φυσικοί αριθμοί των πορτών του Cisco διακόπτη κανάλιού οπτικών ινών και είναι η ασφαλέστερη μέθοδος. Η άλλη μέθοδος καλείται δυναμική ιδιότητα μέλους πορτών δικτύων αποθήκευσης δεδομένων (DPVM). Η DPVM χρησιμοποιεί τα port ή node WWN τα οποία όπως γνωρίζουμε είναι εύκολο να αντιγραφούν.

Όπως εξηγήσαμε στο παράδειγμά μας με την δημιουργία εικονικών δικτύων μέσα στο δίκτυο αποθήκευσης δεδομένων μας είναι σαν να έχουμε τέσσερα ή και παραπάνω διαφορετικά δίκτυα, πράγμα που στην περίπτωση που χρησιμοποιούμε τη στατική μέθοδο κάνει το zone hopping εξαιρετικά δύσκολο να πραγματοποιηθεί. Ενώ όμως η ασφάλεια είναι σαφώς καλύτερη, το επίπεδο πολυπλοκότητας είναι εντυπωσιακά χειρότερο. Η δυνατότητα να ρυθμιστούν, να υποστηριχθούν, και να ελεγχθούν τέσσερα ή και περισσότερα δίκτυα από ένα administrator δεν είναι ένας εύκολος στόχος.

Τα Hard zoning, port-based ζώνες και εικονικά δίκτυα μπορούν να μετριάσουν τους κινδύνους των LUN masking, WWN spoofing, Zone hopping (WWN), Zone hopping (routing).



Σχήμα 5.5 Κατάτμηση δικτύου αποθήκευσης δεδομένων.

5.5. Διαχείριση διακοπτών

Η διοικητική πρόσβαση στις συσκευές αποθήκευσης καναλιού οπτικών ινών απαιτείται να είναι ασφαλής. Η βασική μέθοδος ελέγχου ολόκληρης της υποδομή του δικτύου αποθήκευσης είναι τα διοικητικά κανάλια, τα οποία πρέπει να ασφαλιστούν από αναρμόδιους χρήστες, επιτιθεμένους, τυχαίες αλλαγές, ή τα λάθη παραμετροποίησης. Δεδομένου ότι πολλές συσκευές διοικούνται εκτός ζώνης οπτικού καναλιού με τη χρήση δικτύων IP, στα οποία η πρόσβαση είναι αρκετά εύκολη. Επιπλέον, δεδομένου ότι πολλοί από τους προεπιλεγμένους κωδικούς πρόσβασης στις συσκευές αποθήκευσης δεν αλλάζουν ποτέ, η απόκτηση ολικού ελέγχου της συσκευής αποθήκευσης μπορεί να είναι εύκολη. Τέλος, ακόμα κι αν επιλεχθεί ένας σύνθετος κωδικός πρόσβασης, πολλές συσκευές αποθήκευσης διαχειρίζονται μέσω Telnet, HTTP ή SNMP, τα οποία είναι clear text πρωτόκολλα επιτρέποντας στον επιτιθέμενο να υποκλέψει όνομα χρήστη και κωδικό πρόσβασης οποιαδήποτε στιγμή. Αυτές οι μέθοδοι διευκολύνουν έναν επιτιθέμενο να εκθέσει σε κίνδυνο τη πόρτα διαχείρισης των συσκευών αποθήκευσης και να επαναρυθμίσει το δίκτυο προκειμένου να του παρέχει πρόσβαση για να διαγράψει/καταστρέψει δεδομένα.

Μία ασφαλής μέθοδος θα ήταν αντί της χρήσης Telnet ή HTTP, να εφαρμόζαμε SSH (ασφαλές shell) για τη γραμμή εντολών και SSL (HTTPS) για τη διαχείριση μέσο γραφική διεπαφής ιστού. Τα SSH και HTTPS θα κρυπτογραφήσουν όλη την επικοινωνία αμφίδρομα από τον διοικητικό σταθμό μέχρι τη συσκευή αποθήκευσης. Εάν ένας αναρμόδιος χρήστης ή ένας επιτιθέμενος παρακολουθεί την επικοινωνία, το μόνο που θα βλέπει θα είναι κρυπτογραφημένη κυκλοφορία. Να σημειώσουμε ότι θα πρέπει να τεθούν εκτός λειτουργίας τα Telnet και HTTP αφότου ενεργοποιηθούν τα SSH και HTTPS. Σε πολλά περιβάλλοντα οι administrators εγκαθιστούν τα ασφαλέστερα πρωτόκολλα, αλλά συχνά ξεχνούν να απενεργοποιήσουν τα επισφαλή. Εκτός από τα SSH και HTTPS, θα πρέπει να εξασφαλίσουμε τη χρήση του SNMPv3 και όχι της επισφαλής clear-text έκδοσης, η οποία είναι SNMPvl. Το SNMPv3 μπορεί να χρησιμοποιηθούν με κρυπτογράφηση, πράγμα που καθιστά την υποκλοπή πολύ δύσκολη για έναν επιτιθέμενο.

Μια άλλη μέθοδος ασφαλείας διακοπτών είναι να αποτραπεί η δυνατότητα για οποιαδήποτε ανώνυμη παρακολούθηση και καταγραφή πληροφοριών του δικτύου από το διακόπτη καναλιού οπτικών ινών. Πολλοί διακόπτες καναλιού οπτικών ινών

δίνουν πληροφορίες χωρίς απαίτηση οποιουδήποτε τύπου αυθεντικοποίησης. Ένας επιτιθέμενος μπορεί να συνδεθεί με τη διοικητική IP διεπαφή ή να κάνει inband διαχείριση μέσω της σύνδεσης καναλιού οπτικών ινών για να συγκεντρώσει πληροφορίες για το δίκτυο. Όπως έχουμε αναφέρει η επιτυχία της επίθεσης οφείλεται κατά ένα μεγάλο ποσοστό στη διαδικασία παρακολούθησης και καταγραφής που πραγματοποιεί ο επιτιθέμενος. Η ιδανική μέθοδος είναι να απαιτείται αυθεντικοποίηση προτού χορηγείται οποιαδήποτε πρόσβαση είτε για λόγους πληροφόρησης είτε αλλαγών.

Το τελευταίο βήμα στην ασφάλεια διαχείρισης διακοπτών είναι η εγκατάσταση ασφαλούς διοικητικού λογισμικού για τα δίκτυα αποθήκευσης. Διοικητικές εφαρμογές αποθήκευσης από τις Veritas, Computer Associates, IBM, EMC και NetApp πρέπει να περιληφθούν στα υψηλά επίπεδα της ασφάλειας εφαρμογών. Τα θέματα ασφαλείας εφαρμογών όπως buffer overflows, format strings attacks, input/output validation, cross-site scripting, weak session identifiers, authorization bypass, hidden field manipulation, συνεχίζουν να δημιουργούν προβλήματα στους κατασκευαστές εφαρμογών. Ερευνητές ασφάλειας στοχεύουν τώρα στις διοικητικές εφαρμογές αποθήκευσης δεδομένου ότι έχουν τον έλεγχο των μεγάλου όγκου δεδομένων και είναι τρωτές σε πολλές κατηγορίες επιθέσεων.

Η ασφαλής διαχείριση διακοπτών θα μπορούσε να βοηθήσει ενάντια στις LUN masking, WWN spoofmg, Zone hopping (WWN), Switch management επιθέσεις.

5.6. Κρυπτογράφηση αποθηκευμένων δεδομένων

Η κρυπτογράφηση των "ταινιών" αποθήκευσης (data at rest) είναι μια μέθοδος εξασφάλισης ότι τα δεδομένα στο δίκτυο αποθήκευσής μας δεν είναι διαθέσιμα σε αναρμόδια μάτια. Τράπεζες και οι οργανισμοί εκτέθηκαν ανεπανόρθωτα όταν χάθηκαν μεγάλες ποσότητες δεδομένων τους. Η Τράπεζα της Αμερικής, η Ameritrade, η Iron mountain και η Citibank έπρεπε να αναγνωρίσουν την απώλεια "ταινιών" αποθήκευσης που περιείχαν ευαίσθητες πληροφορίες.:

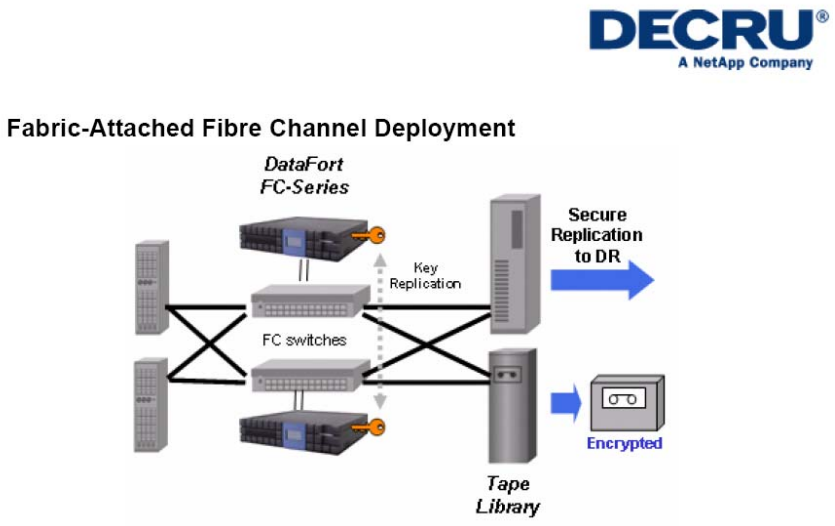
- *Citibank notifies 3.9 million customers of lost data* (MSNBC, June 7, 2005)

- *US bank staff 'sold customer details'* (Tuesday 24th May 2005)
- *Iron Mountain Admits Tape Loss, Recommends Encryption* (internetnews.com April 22, 2005)
- *Ameritrade warns clients about potential data breach* (By Todd R. Weiss , Computerworld , 04/20/2005)

Με κυβερνητικούς κανονισμούς, όπως η California Senate Bill 1386, οι οργανώσεις πρέπει να ειδοποιήσουν το κοινό εάν οποιαδήποτε προσωπική πληροφορία, όπως οι αριθμοί πιστωτικής κάρτας ή οι αριθμοί κοινωνικής ασφάλισης, έχει χαθεί, κλαπεί ή εκτεθεί. Η λύση για ένα τέτοιου είδους προβληματισμό είναι η χρήση της σε ανάπαυση (at rest) κρυπτογράφησης. Πρέπει να σημειωθεί ότι αν και η κρυπτογράφηση δεδομένων σε ανάπαυση είναι μια πολύ ορθή πρακτική ασφάλειας, δεν προστατεύει από επιθέσεις άρνησης υπηρεσιών που μπορούν να αφήσουν τα δεδομένα μη διαθέσιμα.

5.6.1 Ασφάλεια ταινιών δικτύων αποθήκευσης δεδομένων

Πολλοί προμηθευτές ασφάλειας αποθήκευσης, όπως Decru, NeoScale, Vormetric, και Kastan-Chase παρέχουν τις ευθύγραμμες συσκευές για να κρυπτογραφήσουν τα στοιχεία σε και από τις συσκευές αποθήκευσης ελεγκτών και ταινιών και για το SAN και για NAS τις υποδομές.



Σχήμα 5.6 Λύση κρυπτογράφησης από Decru

Σε ένα δίκτυο αποθήκευσης δεδομένων οι συσκευές κρυπτογράφησης θα μπαίνανε παράλληλα με τους διακόπτες καναλιού οπτικών ινών. Αντί οι διακόπτες να επικοινωνούν άμεσα με τους ελεγκτές αποθήκευσης, οι διακόπτες θα έστελναν την κυκλοφορία πρώτα στη συσκευή κρυπτογράφησης. Η συσκευή κρυπτογράφησης θα κρυπτογραφούσε τα δεδομένα και θα τα έστελνε έπειτα πίσω στο διακόπτη. Σε εκείνο το σημείο, ο διακόπτης θα έστελνε τα δεδομένα στον ελεγκτή αποθήκευσης ή τη συσκευή ταινιών όπου και θα αποθηκευτούν κρυπτογραφημένα πια. Πρέπει να σημειωθεί ότι οποιαδήποτε επίθεση και αν πετύχαινε μια κακόβουλη οντότητα τα στοιχεία που θα ελάμβανε ο επιτιθέμενος θα ήταν κρυπτογραφημένα και ως εκ τούτου άχρηστα. Η κρυπτογράφηση δεδομένων σε ανάπαυση προσθέτει μεγάλη ασφάλεια για τους οργανισμούς που διαθέτουν δίκτυα αποθήκευσης δεδομένων.

Συμπεράσματα

Με την παρούσα εργασία επιτυγχάνεται μια αναλυτική καταγραφή των πιθανών κινδύνων και επιθέσεων ασφαλείας καθώς, και των διαθέσιμων μεθόδων προστασίας των δικτύων με υποδομές οπτικών ινών. Σημαντικό, επίσης, είναι ότι πραγματοποιήθηκε μια σύγκριση και αντιστοίχηση των θεμάτων ασφαλείας μεταξύ των IP και FC πρωτοκόλλων επικοινωνιών.

Αν και τα δίκτυα οπτικών ινών είναι γενικά πιο ασφαλή από τα δίκτυα με υποδομές χαλκού υπάρχουν τρόποι με τους οποίους μία κακόβουλη οντότητα είναι ικανή να υποκλέψει οπτικά σήματα και να αποκτήσει πρόσβαση σε ευαίσθητα και εμπιστευτικά δεδομένα.

Ένα ακόμα βασικό συμπέρασμα που αποκομίσθηκε και αφορά στα ανώτερα στρώματα δικτύων οπτικού καναλιού είναι ότι πολλά είδη επιθέσεων των δικτύων αυτών δεν είναι καινούρια, αλλά μεταλλαγές παλαιότερων γνωστών επιθέσεων των IP δικτύων.

Περεταίρω έρευνα και ανάλυση θα μπορούσε να γίνει, όσο αφορά το φυσικό στρώμα, στην εξ αποστάσεως απομάστευση οπτικών σημάτων και την αντιμετώπιση της, ενώ όσο αφορά στην τεχνολογία οπτικού καναλιού ανοικτά θέματα προκύπτουν στις μεθόδους αυθεντικοποίησης και τον τρόπο εφαρμογής τους στην πράξη.

Βιβλιογραφία

1. Guide to Intrusion Detection and Prevention Systems (IDPS), Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology Gaithersburg, February 2007

2. Tapping into fibre optic cables Bernard Everett, regional sales director western and southern Europe, InfoGuard Network Security Volume 2007, Issue 5, May 2007.

3. Giant Fiber Lasers: A New Paradigm for Secure Key Distribution Jacob Scheuer, and Amnon Yariv, School of Electrical Engineering, Tel-Aviv University, Ramat-Aviv, Israel, Department of Applied Physics, California Institute of Technology, Pasadena, California, USA, 6 October 2006.

4. Fibre Optic Intrusion Detection Systems, Network Integrity Systems, Inc.2005.

5. M. Médard, D. Marquis, R.A. Barry, S.G. Finn, "Security Issues in All-Optical Networks", IEEE Network Magazine, May 1997.

6. R.L Hughes et al., "Quantum Cryptography", Contemporary Physics, vol. 36, no. 149, 1995.

7. M. Sumida, "OTDR Performance Enhancement Using a Quaternary FSK Modulated Probe and Coherent Detection", IEEE Photonics Technology Letters, vol. 7, no. 3, March 1995.

8. Attack Detection Methods for All-Optical Networks Muriel Médard, Douglas Marquis, and Stephen R. Chinn Massachusetts Institute of Technology, Lincoln Laboratory 244 Wood Street, Lexington, Massachusetts.

9. U.S. Patents 6,265,710 B1, Method and device for extracting light out of a glass fiber, Herbert Walter, Deutsche Telecoms, July 24, 2001

10. U.S. Patents 6,594,055 Securing Fiber Optic Communications against Optical Tapping Methods, Oyster Optics, Inc New York, July 15th, 2003.

11. L. B. Kish, "Totally secure classical communication utilizing Johnson (-like) noise and Kirchoff's law", Physics Letters A.

12. Secure Classical Optical Communication and Microwave Communication: Wave Implementation of the Unconditionally Secure Communicator Based on Kirchhoff's Law and Johnson-like Noise LASZLO B. KISH, Department of Electrical Engineering, Texas A&M University, College Station, TX 77843-3128, USA, October 13, 16, 2006.

13. Protection against the man in the middle attack for the Kirchhoff-Loop-Johnson(-like) -Noise chipper and expansion by voltage – based security L. B. KISH, Department of Electrical Engineering, Texas A&M University, College Station.

14. Storage Networking Protocol Fundamentals, James Long, Cisco Press, May 18, 2006

15. IBM SAN Survival Guide, August 2003

16. Using VSANs and Zoning in the Cisco MDS 9000 Family of Multilayer Fibre Channel Switches, Cisco Press

17. Data Disaster Recovery and Business Continuance Fibre Channel over IP Design Using the MDS 9000 Family of Multilayer Switches, Cisco Press

18. Brocade SAN Security Framework in a Microsoft Windows Enterprise Environment White Paper, July 2004.

19. Securing Storage: A Practical Guide to SAN and NAS Security by Himanshu Dwivedi," Addison-Wesley Professional, 2005

20. “Guide to Understanding Zoning” (Brocade publication number: 53-0000213-01).

21. “SAN Security: A Best Practices Guide” (Brocade publication number: GA-RG-250-00).

22. Extending storage infrastructure trust to the fabric edge, Emulex, September 2007.

23. Secure SAN Zoning Best Practices, 2007 Brocade Communications Systems, Inc.

24. Project Proposal For A New NCITS Standard Fibre Channel Generic Services Fourth Generation (FC-GS-4), T11/00-545v2

25. Fibre channel security protocols (FC-SP) REV 1.74 INCITS working draft proposed American National Standard for nformation Technology February 17, 2006

26. Project Proposal For A New INCITS Standard Fibre Channel Security Protocols Second Generation (FC-SP-2) 05 January 2006

27. Considerations and Best Practices for Securing Sensitive Data, Decru, February 2007.

28. Fibre Channel Industry Association http://www.fibrechannel.org

29. T11 Technical Committee http://www.t11.org

30. Storage Networking Industry Association (SNIA) http://www.snia.org