Voice over IP: Απειλές, Ευπάθειες και Αντίμετρα

Παναγιώτης Νάστου
Πληροφορικός Ελεγκτής

Ενοποιημένες Επικοινωνίες

Παραδοσιακά οι επιχειρήσεις διέθεταν δύο δίκτυα για την επικοινωνία τους με τους πελάτες και προμηθευτές:

1. Το τηλεφωνικό δίκτυο αποτελούμενο από τις τηλεφωνικές συσκευές και το PBX (Private Branch Exchange) το οποίο συνδέεται στο δημόσιο τηλεφωνικό δίκτυο για την μεταφορά φωνής και
2. στο δίκτυο δεδομένων.

- Τα πρώτα χρόνια της περασμένης δεκαετίας ένας μικρός αριθμός από IT οργανισμούς στράφηκαν προς ένα ενοποιημένο δίκτυο προκειμένου να υποστηριχτούν πολλαπλοί τύποι κίνησης:
  1. Voice
  2. Data
  3. Video
- Σε αυτό το πρώιμο στάδιο της ανάπτυξης των ενοποιημένων επικοινωνιών, η φωνή θεωρήθηκε ότι θα πρέπει να αντιμετωπισθεί απλά σαν μια ακόμα εφαρμογή που θα έπρεπε να «περάσει» πάνω από ένα IP δίκτυο (IP telephony).

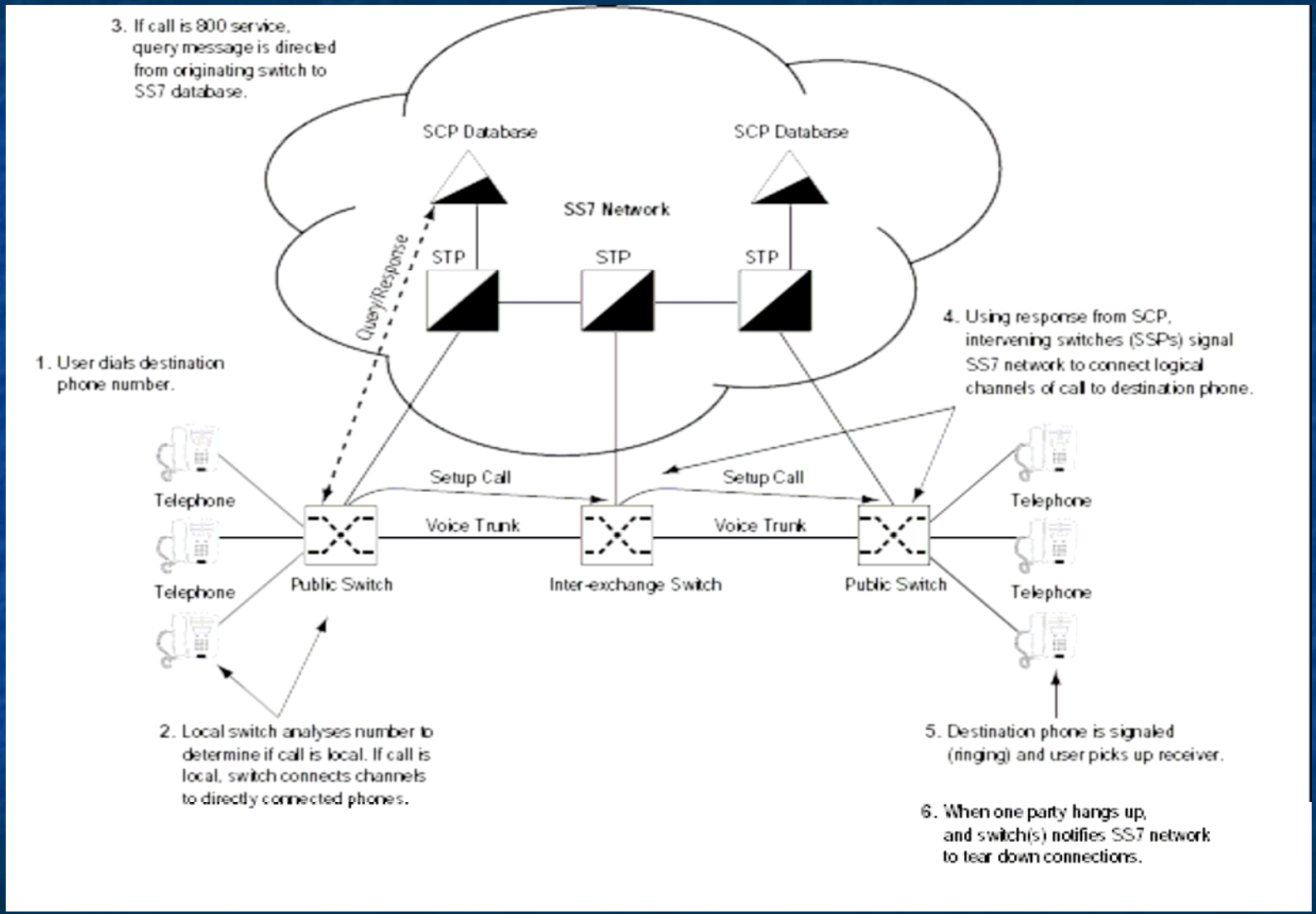
Voice over IP (1)

- Σήμερα ολοένα και περισσότερο η σύγκλιση δικτύων υλοποιείται με τη χρήση της τεχνολογίας VoIP:
  1. Μειώνοντας το κόστος μετάδοσης
  2. Βελτιώνοντας την επιχειρησιακή απόδοση
  3. Ενεργοποιώντας νέες ολοκληρωμένες εφαρμογές.
- Η σύγκλιση αυτή των δικτύων δημιουργεί ένα **μεγάλο αριθμό από τερματικά συστήματα** τα οποία δύναται να έχουν πρόσβαση στις εφαρμογές της επιχείρησης μέσω του ενοποιημένου δικτύου και κατ' επέκταση δημιουργεί εν δυνάμει κινδύνους για την ασφάλεια του δικτύου.

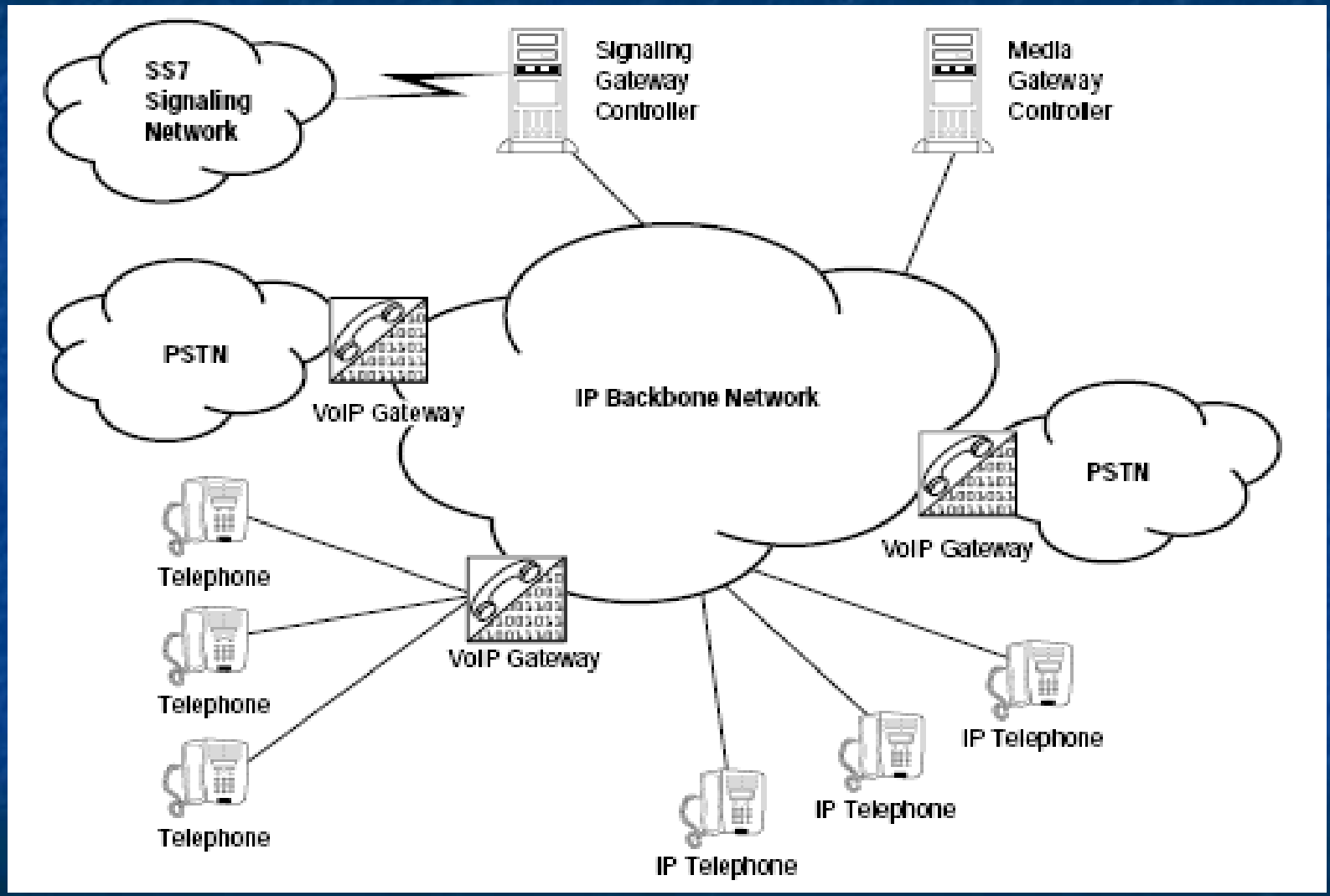
Voice over IP (2)

- Οι απειλές που προυπήρχαν στα δίκτυα δεδομένων κληρονομούνται και στα ενοποιημένα δίκτυα.
- Επίσης το γεγονός ότι κάθε χρήστης μπορεί από οποιαδήποτε συσκευή είναι κάθε φορά διαθέσιμη να έχει πρόσβαση σε πόρους με τη χρήση οποιουδήποτε τρόπου (wire, wireless, speech/text) αυξάνει τον κίνδυνο.
- Επιπρόσθετα η ύπαρξη πλέον εφαρμογών όπως VoiceMail, Call Centers και IVR στο ενοποιημένο δίκτυο εκθέτουν εσωτερική πληροφορία σε κινδύνους όπως ο κίνδυνος να κρυφακούει μη εξουσιοδοτημένο πρόσωπο ή εξαγωγή πληροφοριών από την παρακολούθηση της κίνησης πάνω στο ενοποιημένο δίκτυο.

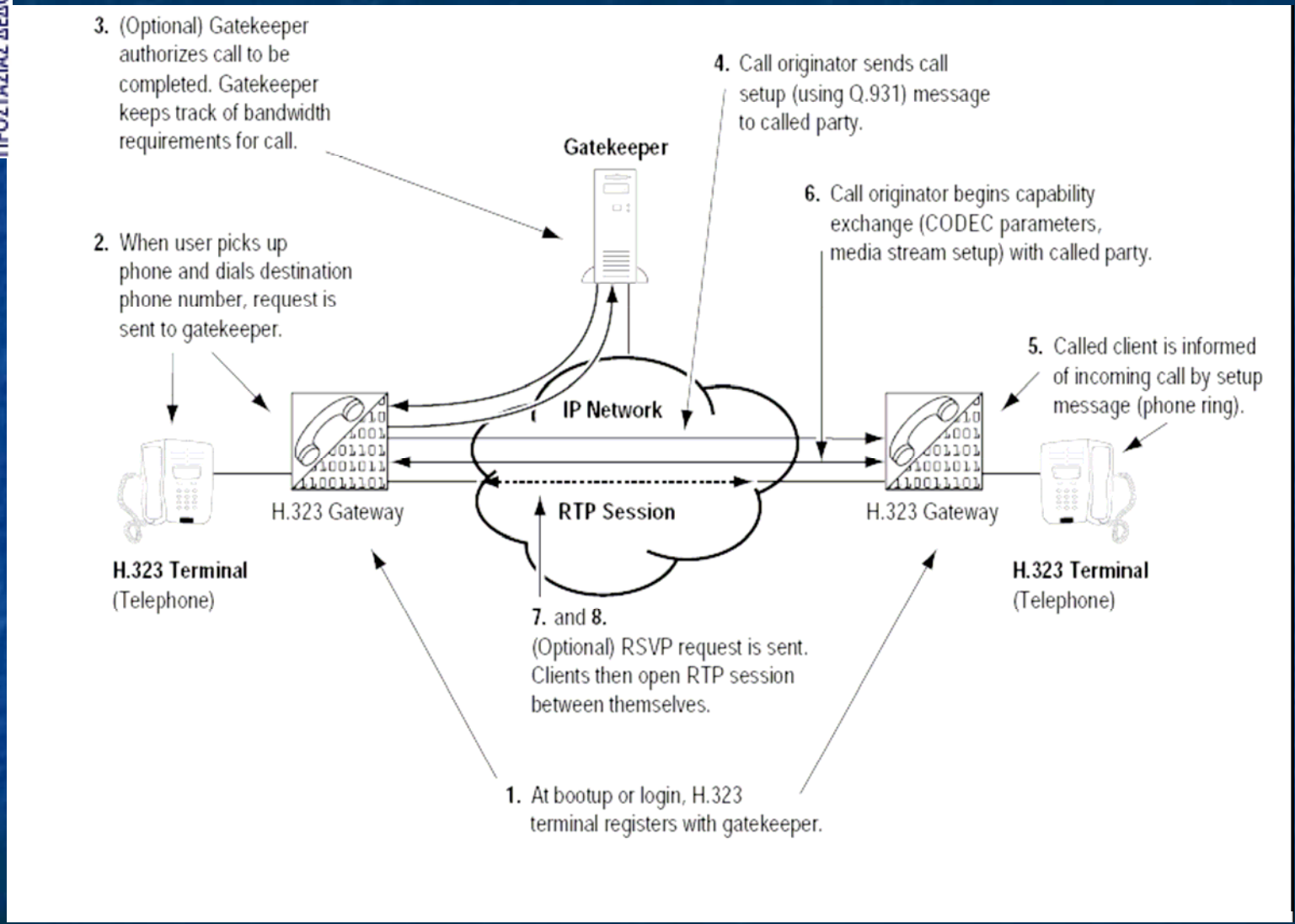
Signaling System Seven-SS7



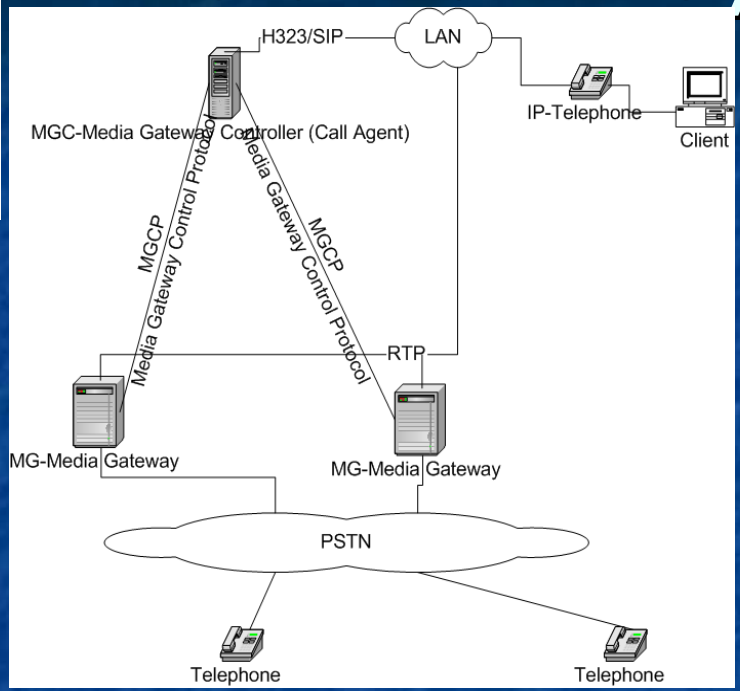
VoIP Δίκτυο

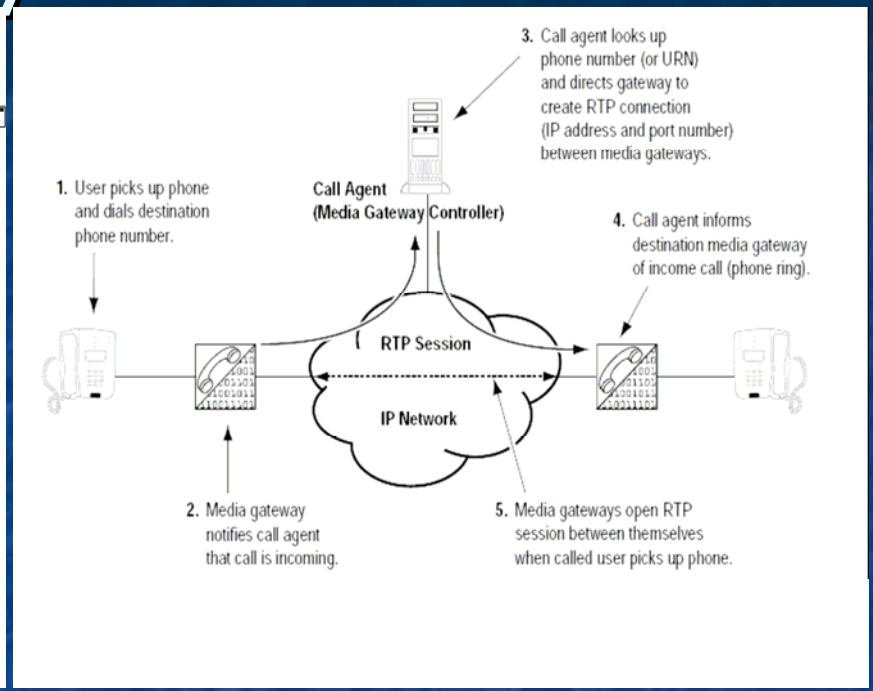

SS7
Signaling
Network
Signaling
Gateway
Controller
Media
Gateway
Controller
PSTN
VoIP Gateway
IP Backbone Network
PSTN
VoIP Gateway
Telephone
Telephone
Telephone
VoIP Gateway
IP Telephone
IP Telephone
IP Telephone

H.323


3. (Optional) Gatekeeper authorizes call to be completed. Gatekeeper keeps track of bandwidth requirements for call.
4. Call originator sends call setup (using Q.931) message to called party.
Gatekeeper
6. Call originator begins capability exchange (CODEC parameters, media stream setup) with called party.
2. When user picks up phone and dials destination phone number, request is sent to gatekeeper.
5. Called client is informed of incoming call by setup message (phone ring).
IP Network
H.323 Gateway
RTP Session
H.323 Gateway
H.323 Terminal
(Telephone)
H.323 Terminal
(Telephone)
7. and 8.
(Optional) RSVP request is sent. Clients then open RTP session between themselves.
1. At bootup or login, H.323 terminal registers with gatekeeper.

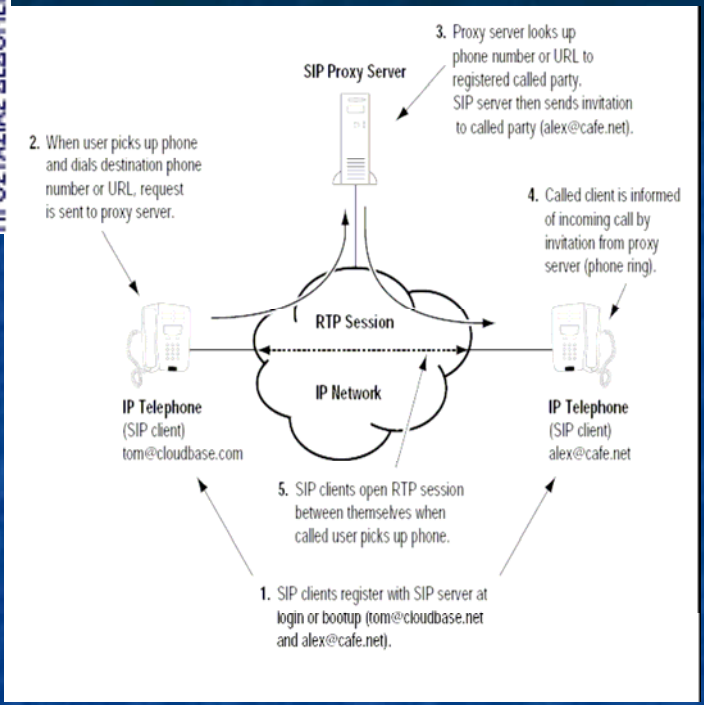
Media Gateway Control Protocol

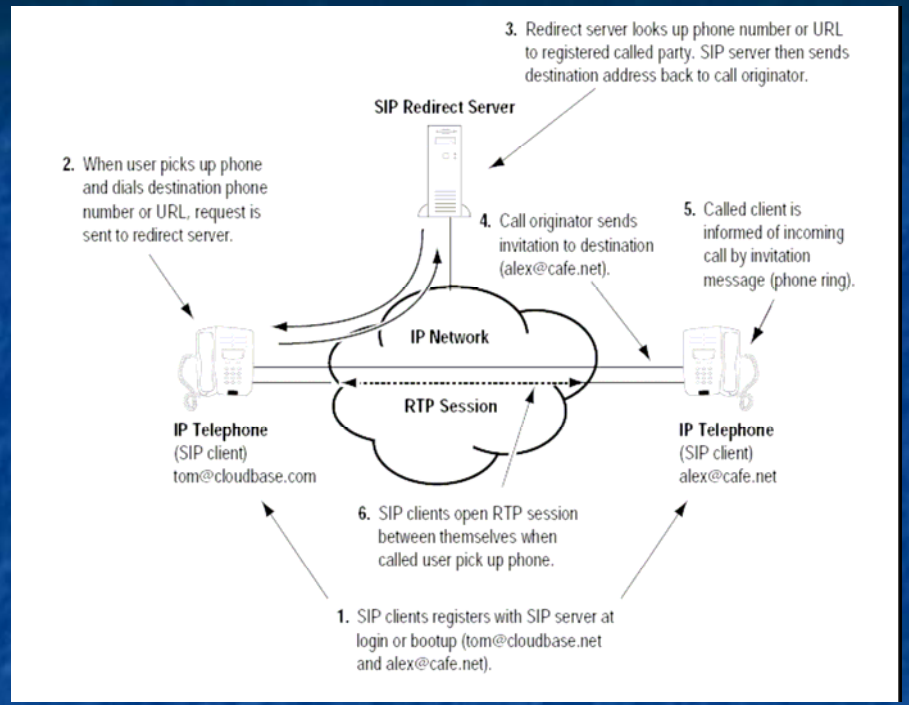




- Ο MGC εξυπηρετητής διαχειρίζεται τις κλήσεις και τις διασκέψεις.
- Ο MG απλά εκτελεί εντολές που δέχεται από τον MGC.
- Το πρωτόκολλο MGCP δεν ορίζει μηχανισμό για τον συγχρονισμό των MGCs.
- Πρόκειται για ένα πρωτόκολλο server/client με στενό δεσμό ανάμεσα στον MGC και MG.
- Τα RTP δεδομένα ανταλλάσσονται μεταξύ των εμπλεκομένων MGs.

SIP:Session Initiation Protocol





- Είναι πρωτόκολλο στο application layer αποσυνδεδεμένο από το πρωτόκολλο μεταφοράς που χρησιμοποιείται :
  1. UDP: μειώνει τις επιβαρύνσεις αυξάνοντας την ταχύτητα και την αποδοτικότητα.
  2. TCP: χρησιμοποιείται όταν πρόκειται να κάνουμε χρήση SSL/TLS για ασφαλής υπηρεσίες.
  3. Stream Control Transmission Protocol (SCTP):Παρέχει αυξημένη αντίσταση σε Dos επιθέσεις μέσω μιας μεθόδου ανταλλαγής τεσσάρων μηνυμάτων μεταξύ των σταθμών που θέλουν να επικοινωνήσουν.

Απειλές σε VoIP περιβάλλον

- Σε ένα VoIP περιβάλλον εμφανίζονται απειλές τόσο στα VoIP τηλέφωνα όσο και στους χρησιμοποιούμενους μεταγωγείς.
- Μια απειλή (Hackers, viruses, worms, Trojan Horses κλπ) εκμεταλλεύεται συγκεκριμένες αδυναμίες των συστημάτων ή πρωτοκόλλων που συνθέτουν ένα VoIP περιβάλλον με στόχο να πλήξουν την:
  1. Εμπιστευτικότητα και την ιδιωτικότητα της επικοινωνίας
  2. Ακεραιότητα των δεδομένων
  3. Διαθεσιμότητα του συστήματος
- Σε κάθε οργανισμό εμφανίζονται απειλές που σχετίζονται πιο πολύ με το επιχειρησιακό σχεδιασμό του.
- Οι περισσότεροι που ασχολούνται με την ασφάλεια των συστημάτων τις απειλές τις ταξινομούν:
  1. Σε αυτές που έχουν την βάση τους σε ευπάθειες της τεχνολογίας
  2. Και σε αυτές που έχουν την βάση τους στον ανθρώπινο παράγοντα.

Technology Based Threats

- Επιθέσεις που βασίζονται σε ευπάθειες των συστημάτων που συνθέτουν ένα VoIP περιβάλλον (routers, switches, servers, gateways κλπ).
- **Call Interception**: Με VoIP οι ευκαιρίες για παρακολούθηση μιας συνδιάλεξης πολλαπλασιάζονται καθώς μπορούμε να αξιοποιήσουμε κόμβους ενός packet δικτύου. Ευπάθειες που έχουν αξιοποιηθεί και εντοπισθεί από τον NIST:
  1. Switch Default Password.
  2. Χρήση εργαλείων για ανάλυση πρωτοκόλλων.
  3. Καταστρέφοντας την ARP cache μιας συσκευής είναι δυνατό να επιτευχθεί αναδρομολόγηση της VoIP κίνησης με αποτέλεσμα την παρακολούθηση της επικοινωνίας.
  4. Περιβάλλον Web που διαθέτουν οι περισσότερες συσκευές VoIP για την διαχείριση τους. Αρκεί η παρακολούθηση της plaintext http κίνησης.
  5. Κλέβοντας την αντιστοιχία (extension -> IP). Αναγκάζεις μια συσκευή IP να κάνει restart και παρακολουθείς την διεύθυνση που θα δώσει ο DHCP server. Άλλος τρόπος είναι με την παρεμβολή ενός rogue DHCP ή TFTP εξυπηρετητή.

Technology Based Threats

- **Denial of Service (DOS)** attack: Με την VoIP τεχνολογία το πρόβλημα είναι μεγαλύτερο καθώς είναι περισσότερο ευαίσθητη σε καθυστερήσεις και απώλειες πακέτων.
- **Toll fraud**: Αδυναμίες στην παραμετροποίηση αλλά και η χρήση των default passwords για διαχειριστικούς λόγους κάνουν το πρόβλημα έντονο και σε ένα VoIP σύστημα.
- **Pharming**: Στόχος είναι η εκμετάλλευση των αδυναμιών του μηχανισμού που μετατρέπει Web διευθύνσεις, ονόματα υπολογιστών και δικτυακών συσκευών σε διευθύνσεις διαδικτύου.

Επιθέσεις πάνω σε πρωτόκολλα

- Πειράματα που έγιναν πάνω σε διάφορες υλοποιήσεις του H323 στις ΗΠΑ, αποστολή αλλοιωμένων call setup πακέτων, έδειξαν ότι το αποτέλεσμα μπορεί να είναι κατάρρευση του συστήματος και επανεκκίνηση.
- Το γεγονός ότι το SIP πρωτόκολλο διαθέτει τα χαρακτηριστικά του http και ότι είναι σχετικά εύκολο να αλλοιώσει κανείς ένα ASCII πακέτο το κάνουν «ελκυστικό» στόχο.
  1. Registration Hijacking: Επιτιθέμενος προσποιείται ένα νόμιμο User Agent (UA).
  2. Proxy Impersonation: Ο επιτιθέμενος προσποιείται ότι είναι ένας νόμιμος proxy και με αυτόν τον τρόπο αποκτάει πρόσβαση σε όλη την κίνηση.
  3. Message Tampering.
  4. Session Tear Down: Είναι αποτέλεσμα του ότι ένα μήνυμα bye που τερματίζει ένα RTP session εκτελείται από τον παραλήπτη χωρίς προηγούμενα να γίνει authenticated ο αποστολέας.

Human based Threats

- Ένα σύστημα μπορεί να καταστεί ευάλωτο εξαιτίας του ανθρώπινου παράγοντα:
  1. Κοινωνική μηχανική.
  2. Εργαζόμενους μιας επιχείρησης που κατέχουν πληροφορία χρήσιμη στο επιτιθέμενο και επιθυμούν να την διαθέσουν.
  3. Ανεπάρκειας των τεχνικών λόγω έλλειψης εμπειρίας και εκπαίδευσης.
  4. Σφάλματα ή παραλήψεις στον σχεδιασμό του Change Control Management μπορούν να αφήσουν ευπάθειες τις οποίες μπορεί να εκμεταλλευθεί ο επιτιθέμενος.

Προστασία VoIP Network

- Ανάπτυξη και εφαρμογή πολιτικής ασφαλείας και διαδικασιών. Ενδεικτικά μια πολιτική ασφαλείας θα πρέπει να καθορίζει:
  1. Ποια ομάδα ή ποιο άτομο είναι υπεύθυνο για την εφαρμογή της πολιτικής ασφαλείας.
  2. Ρόλους και ευθύνες.
  3. Διαχείριση Κινδύνων.
  4. Ταξινόμηση της πληροφορίας.
  5. Φυσική Ασφάλεια
  6. Έλεγχος Πρόσβασης
  7. Κανόνες Συμμόρφωσης
- Αυστηρή επιτήρηση των Εξυπηρετητών, Δικτύων και συστημάτων:
  1. Κατάργηση ή διαγραφή όλων των μη απαραίτητων υπηρεσιών και δομικών στοιχείων του συστήματος.
  2. Περιορισμός πρόσβασης μόνο στις απαραίτητες υπηρεσίες που χρειάζεται ένας εργαζόμενος.
  3. Χρήση των πρόσφατων εκδόσεων λογισμικού σε κάθε σύστημα.
  4. Πιστοποίηση κάθε απόπειρας για διαχείριση και κρυπτογράφηση της απομακρυσμένης πρόσβασης για διαχείριση συστημάτων (SSH ή IPSec).
  5. Αποφυγή της χρήσης των default passwords.
  6. Υλοποίηση της VPN πρόσβασης για όσους από τους υπαλλήλους απαιτείται η απομακρυσμένη πρόσβαση σε πόρους των κεντρικών συστημάτων.

Προστασία VoIP Network

- Ενιαία Διαχείριση Δικτύου
  1. Χρήση των ήδη υπαρχόντων εργαλείων διαχείρισης δικτύου δεδομένων και για το ενοποιημένο δίκτυο.
  2. Διαχωρισμός της κίνησης διαχείρισης από την υπόλοιπη κίνηση δικτύου.
- Επιβεβαίωση ταυτότητας χρήστη:
  1. Χρήση τηλεφωνικών συσκευών που διαθέτουν user authentication.
  2. Υλοποίηση device authentication με ARP και 802.1X.
  3. Κεντρικοποιημένη διαχείριση χρηστών: χρήση Active Directory ή LDAP για authentication στις εφαρμογές και στις VoIP υπηρεσίες.
  4. Διαδικασίες για DHCP authentication.

Προστασία VoIP Network

- Ενεργητική παρακολούθηση του Δικτύου.
  1. Χρήση Host based Intrusion Detection Systems (HIDS).
  2. Χρήση Network based Intrusion Detection Systems (NIDS)
  3. Συλλογή των event και audit logs σε έναν εξυπηρετητή, συσχέτιση αυτών με την χρήση έξυπνων εργαλείων για τον εντοπισμό επιθέσεων.
  4. Penetration Testing.
- Διασφάλιση του λογικού διαχωρισμού των δικτύων.
  1. Διαχωρισμός κίνησης δεδομένων, φωνής και διαχείρισης.
  2. Virtual LANs
  3. Traffic shaping
  4. Firewalls: Αναβάθμιση των Firewalls ώστε να μπορούν να διαχειριστούν ευπάθειες των VoIP πρωτοκόλλων ή η αγορά Application Layer Gateways σχεδιασμένα για την αντιμετώπιση προβλημάτων ασφαλείας στα H323 και SIP.
  5. NAT και ιδιωτικές IP διευθύνσεις.
- Χρήση κρυπτογράφησης.