VoIP Security

Security, Defined?

- Security Language:
  - Availability
    - Protect from outages and denial of service
  - Integrity
    - Don’t let someone modify messages in transit (unless authorized)
  - Confidentiality
    - Protect against eavesdropping
  - Authorization and Non-Repudiation
    - Positively identify the party you are exchanging data with, and don’t allow them to deny that they sent the data.

Threats

- Biggest impact:
  - VoIP devices are data devices; all the IP based attacks work against them (and then some).
- Voice specific:
  - Impact of lost service can be high
    - 911! (Fortunately, most of us carry out-of-band verbal communication devices aka cell phones)
  - Call Centers

Threat Impact

- Denial of Service
  - Injury
  - Loss of revenue
- Breach of Confidentiality
  - Disclosure of valuable or protected information
  - Legal Liability
- Unauthorized Use (Toll Fraud)
  - Financial Loss
    - Service through a gateway is cheap, but the cost per call is non-zero.
General Vulnerabilities

- **DNS**
  - Any DNS attack can impact VoIP
    - SRV record for SIP proxies
    - ENUM
- **ARP**
  - ARP spoofing and poisoning redirect traffic to the wrong NIC
- **DHCP**
  - Rogue DHCP servers
    - SIP proxy or file server configured via DHCP
- **DDoS (Distributed Denial of Service)**

VoIP more vulnerable?

- **Real-time traffic**
  - Less effort required to disrupt service
- **Small devices**
  - Embedded systems, small processors
    - Easier to overload
    - Less error checking
  - ITS Phones known to crash during OIT security scan
    - Less monitoring
    - Virus scans?

Sample Attacks

- **DDoS**
  - Botnet floods
    - SIP REGISTER or INVITEs at the proxy
    - RTP or RTCP at the UAs
  - Attacker sends malicious malformed packets at UAs
    - Force crash in the UA
  - Attacker sends malicious packets at SIP proxy
    - Cause crash or take control of system

Man in the Middle

- **Rogue Proxy**
  - Convince UA to register with the wrong proxy
    - Use rogue DHCP or DNS cache poison
  - Cause denial of service
  - Redirect calls
    - Banking call center
    - Send calls through eavesdropping point
Man in the Middle
- Generic man-in-the-middle attack
  - Use ARP or DNS attack
  - Reroute traffic through "black" relay for eavesdropping
  - Redirect signaling traffic
    - Denial of Service
    - Malicious Call Redirection
    - Hijack connection

Unprotected Signaling
- Unauthorized Access
  - Spoofed Caller ID
    - Too many systems rely on Caller ID as authoritative and immutable
    - Banks request that you "activate your card by calling from your home phone"
    - We tend to screen calls by looking at the Caller ID information

Tools
- Encryption
  - TLS
  - IPsec
- Authentication
  - 802.1x
- Traffic Separation
  - VLANs + packet filters
- Active Monitoring