As presented at NIKSUN WWSMC
July 25-27, 2011 | www.niksun.com

Self-Protecting Communications

A.S. Krishnakumar

Avaya Labs

July 27, 2011

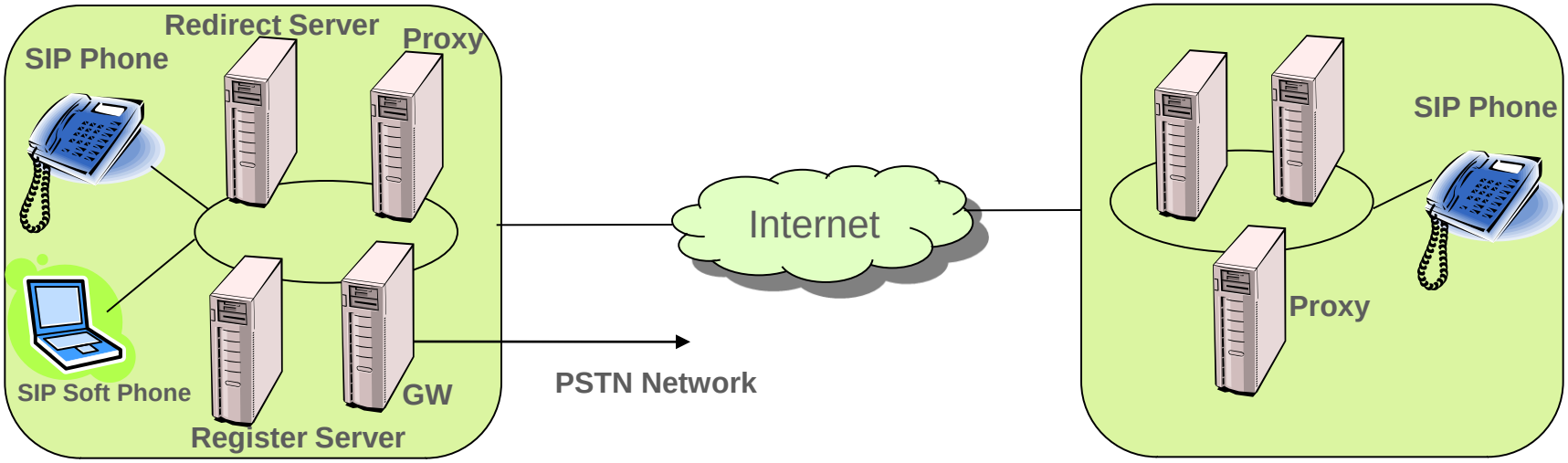
Acknowledgement

I would like to acknowledge the work of my colleague Navjot Singh in preparing this presentation.

Outline

- Overview
- Threats Against VoIP Systems
  - Non-VoIP Specific
  - VoIP-Specific
- VoIP Intrusion Detection and Mitigation System
  - Motivation
  - Components needed
- SPIT – Spam over IP Telephony
- Summary

Overview of a SIP VoIP System

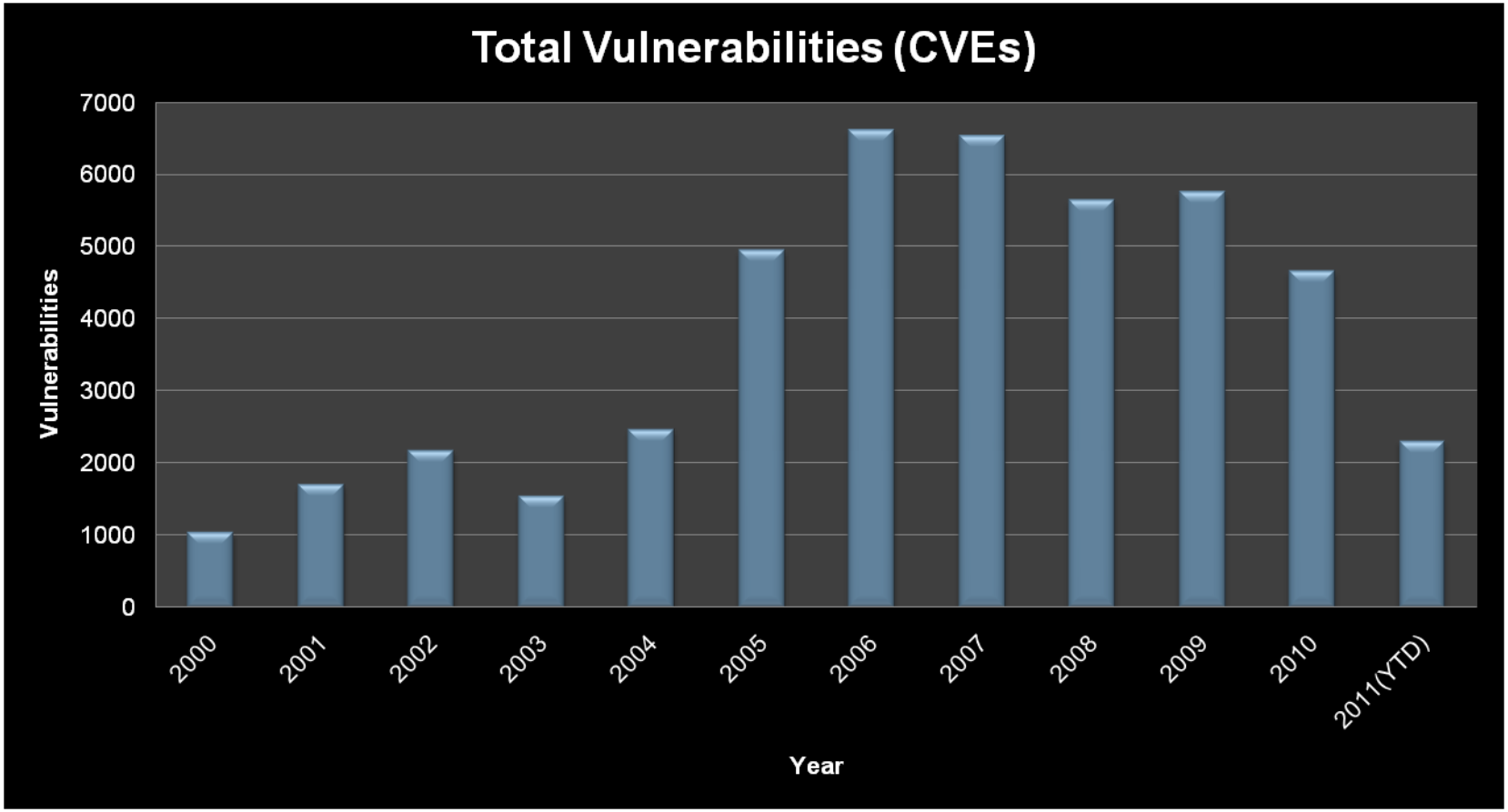


- Characteristics of VoIP Systems
  - Open environment
  - Real-time nature of service
  - Employ multiple protocols
  - Distributed nature
  - Different components may be under different administrative domains
  - Vulnerable to malicious attacks

Traditional Attacks

- ARP Spoofing/poisoning
  - Gratuitous ARP
- IP spoofing
- Malformed IP packets
  - jolt2
- Buffer overflow
  - Using unsecured functions
- Flooding attacks
  - TCP SYN
- Replay attacks
  - Capture packet and resend the packets
- Connection Hijacking
  - Predictable Initial Sequence Number
- ICMP
  - Netmask request
  - time stamp request
  - Error packet flood
- TCP
  - X-mas
  - FIN without ACK
- UDP
  - Fraggle attack
- Fragments
  - reassembly with different offset (Teardrop)
  - flood initial fragment only

Security Vulnerabilities Per Year



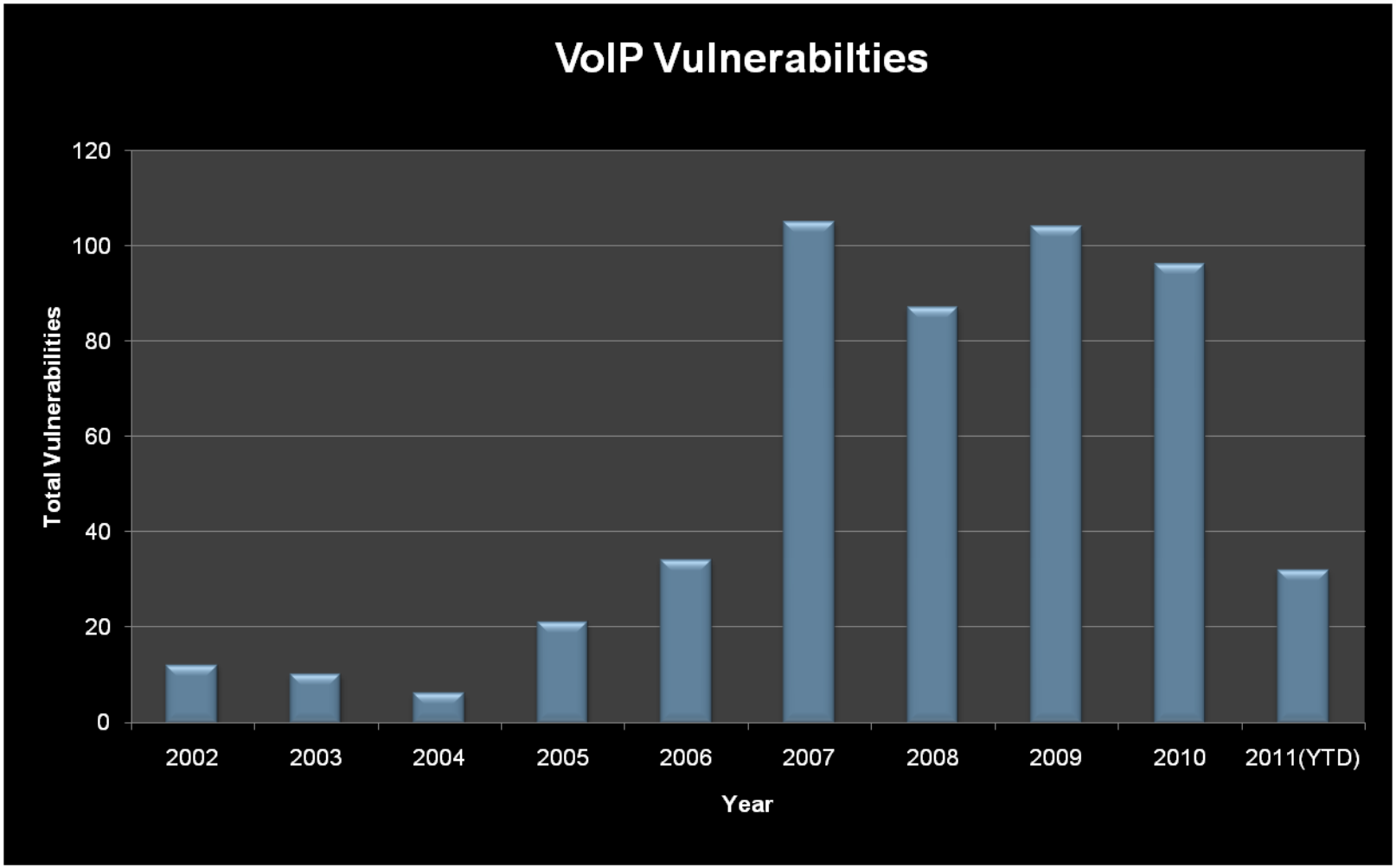
Data Collected from National Vulnerability Database

Cross-site scripting, sql injection and buffer overflow constitute major portion of the vulnerabilities discovered

VoIP Specific Attacks

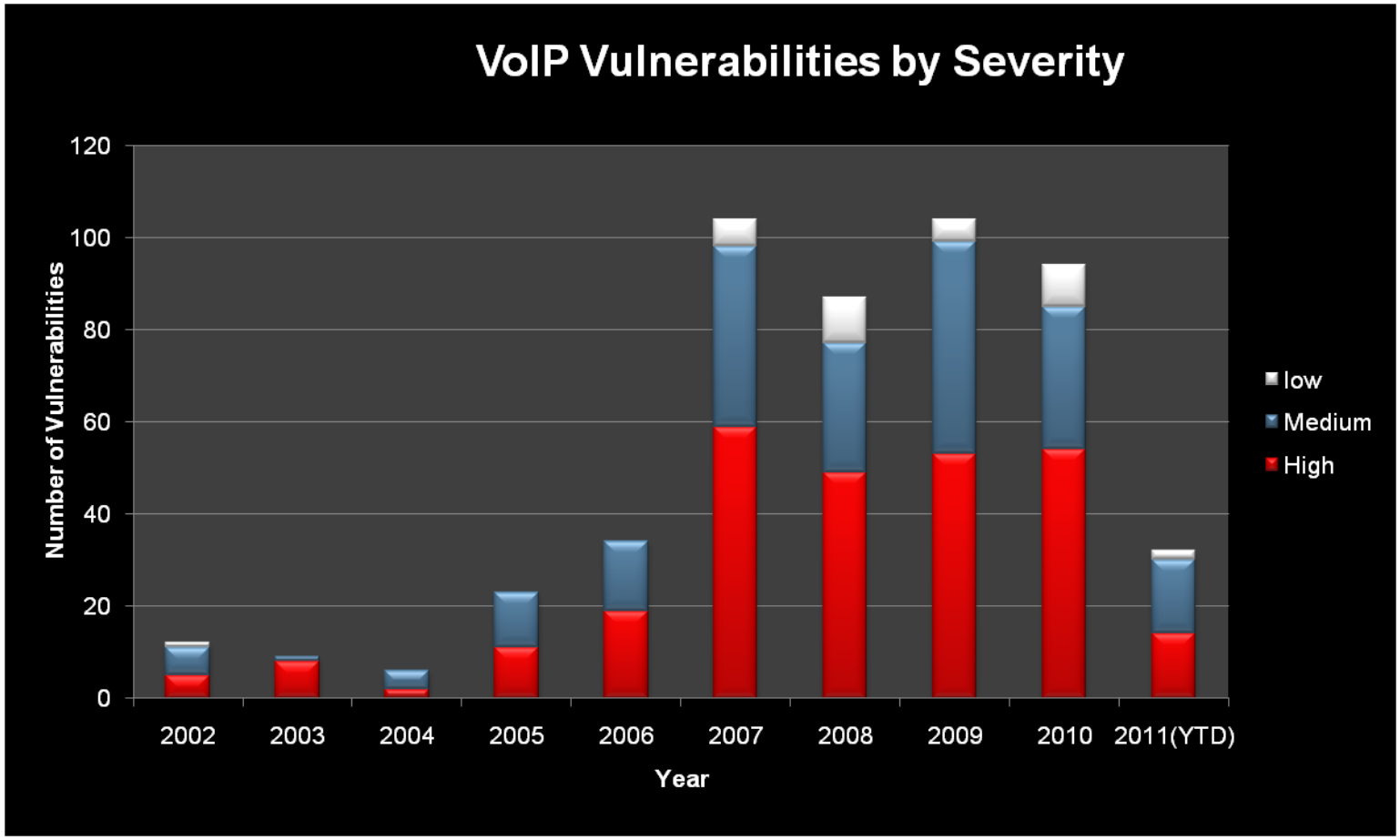
- Injecting spoofed control signaling messages
  - Fake bye
  - Fake re-invite
- Call Hijacking
  - Registration hijacking
  - Media session hijacking
- Changing call routing
  - Sniffing, DoS
- Degrading QoS
  - Packet floods
- Toll Fraud
  - Redirecting calls to avoid tolls
- SPIT/SPAM
  - Unsolicited phone calls
- Buffer Overflow
  - Due to the use of Unsafe functions
- Protocol Misuse
  - Caller ID Spoofing
- Malicious Contents
  - Transported contents may be malicious
- Fuzzing
  - Invalid SIP messages
  - Valid SIP messages
- DoS
  - Flooding
  - Resource exhaustion
  - Replay

VoIP Specific Vulnerabilities



Data Collected from National Vulnerability Database

VoIP Vulnerability by Severity

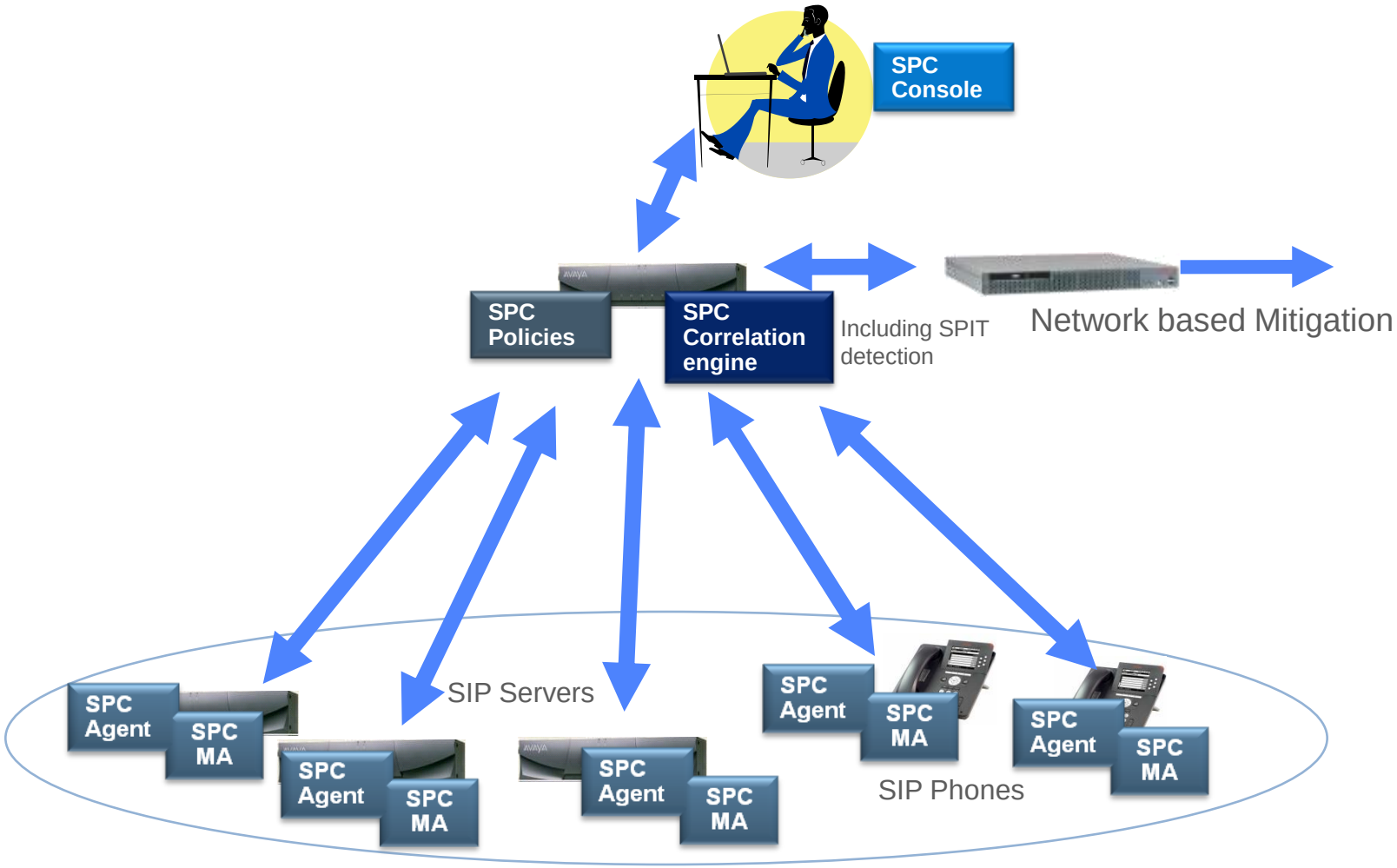


Data Collected from National Vulnerability Database

Challenges Facing VoIP Protection

- Protection at the edge alone cannot protect against attacks from inside the network
- Protocol Specific information absent at the edge firewall.
- No coordinated detection and mitigation policies
- Rogue access point can open up the network to attacks protected by the edge firewall
- The firewall at the edge can become a bottleneck due to increase in line speeds

Self-Protecting Communication Architecture



SPC Detection and Mitigation Architecture

- Detection and mitigation agents embedded in VoIP solution elements
  - Block attacks locally based on the policy
  - Communicate session information to correlation engine
- Centralized Correlation Engine
  - Correlation of events from VoIP elements
- Secure communication with correlation engine
  - Offload heavy duty processing from embedded agents and enforce global detection / mitigation policies
- Centralized management console
  - Manage policies, combined view of alert and actions
- Communication with Network Management servers
  - Attack mitigation via configuration changes to network elements

SPC Components - Detection Agent

- SPC Agent
  - Embedded in VoIP element - phone, server, gateway etc.
  - Receives events from the local mitigation agent, resource monitors, and applications etc.
  - Local correlation of events to detect attacks targeted at the end devices, e.g.
    - INVITE flood
    - Reconnaissance attacks
  - Sends events of importance to the SPC Server for global correlation
  - Receives events/policy updates from the SPC Server
  - Communicates to the SPC Server

SPC Components - Mitigation Agent

- SPC MA
  - Embedded in VoIP element - phone, server, gateway etc.
  - Receives mitigation policies from the SPC Server via SPC Agent
  - Blocks attacks based on the defined policies and sends notifications to the SPC Server
  - Sends events of importance to the SPC Agent
  - Monitors ingress/egress rates
  - Rate-limiting and logging
  - State based rule partitioning
  - This has more real-time aspects to it

SPC Components - Server

- SPC Server
  - Central repository of the SPC policies
  - View of alerts and mitigation actions via the SPC Console
  - Correlation engine for detection of topology-based attacks e.g. SPIT/SPAM, DDoS
  - Updates of policies/mitigation actions to SPC agents
  - Coordinate mitigation with network based mitigation engine
  - Notification of alerts to administrators e.g. via email, pager etc.

Spam Calls in VoIP Systems

- Spam over Internet Telephony (SPIT)
- Unsolicited and unwanted phone calls from (malicious) parties
  - Telemarketing calls
  - Harassing calls
  - Survey / polling calls
- Why is this a growing phenomenon?
  - VoIP calls are cheap to make
  - SPIT is very easy to automate
- Comparison with e-mail spam:
  - Motives and impacts are analogous
  - But, more disruptively, a VoIP spam intrudes in real-time

Challenges for Dealing with VoIP Spam

- A spam call in many ways appears like a normal (non-SPIT) call
  - Both follow the same protocols (SIP, H.323, RTP, RTCP)
  - No malformed packets
  - No exploitation of protocol vulnerabilities
  - Existing NIDS systems (Snort, SCIDIVE[1],…) do not apply
- VoIP is a real-time system
  - Before you pick up the call, can you tell if it's going to be a spam call?

[1] Y-S. Wu, S. Bagchi, S. Garg, N. Singh, T. Tsai, "SCIDIVE: A Stateful and Cross Protocol Intrusion Detection Architecture for Voice-over-IP Environments," DSN 05, pp. 401-410.

Challenges for Dealing with VoIP Spam

- VoIP system is a dynamic environment
  - Call duration, call frequency, the words you say, … can all be changing from one deployment to another
  - Different persons have different perspectives on what constitutes a SPIT call
    - Some might be interested in buying merchandise from telemarketers while they do dislike other harassing phone calls.
  - Therefore, fixed, threshold-based rules for detection are not suitable for filtering spam calls

Why Somebody might be interested in SPIT

- Telemarketers who want to sell products
  - Human telemarketers
  - Automated bots that play a message
- Malicious Hackers
  - Vishing (VoIP Phishing) attacks to get sensitive information
  - Vishing attacks for people to call expensive numbers
- Annoying Calls
  - repetitive/illegal harassing, threatening, or obscene telephone calls

Known Incidents of SPIT, Vishing etc.

- First Skype Telemarketing calls recorded in 2006
- Romanian authorities dismantled a cybercrime network dealing with VoIP Fraud (Shadow communications Inc)
  - resulted in approximately 11 million Euros in fraud
- Number of Vishing attacks related to PayPal, Bank of America, Craigslist phone verification etc.
- Number of reported cases of robocalls during elections

Few known cases of SPIT but it is expected to increase in coming years

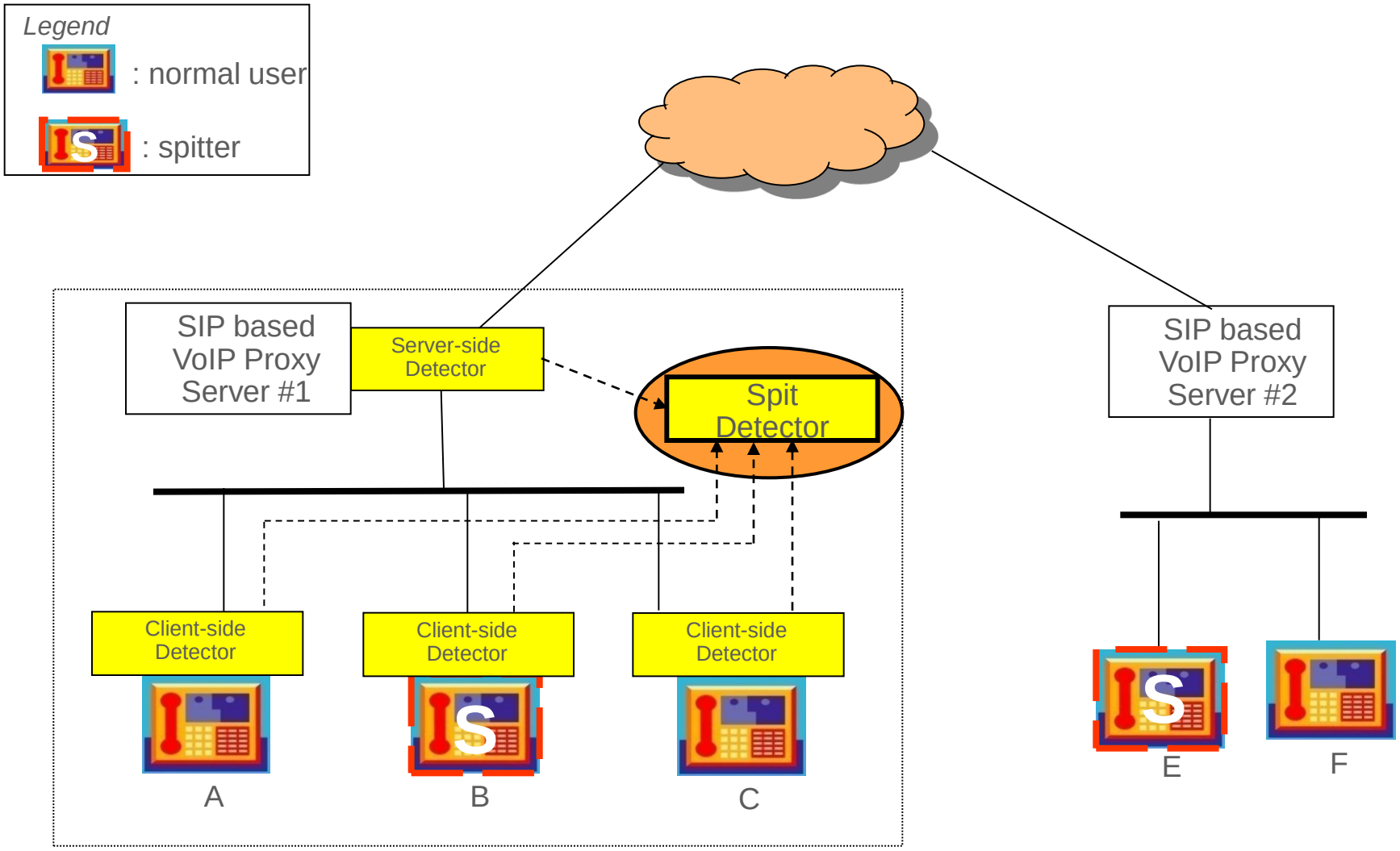
Building Blocks for Preventing SPIT

- Authentication
  - Authenticate end-user and drop unauthenticated calls or those coming from open servers
- Whitelist
  - Allow the call if the callee is on the whitelist
- Blacklist
  - Drop the call if the callee is on the blacklist
- Audio CAPTCHA
  - Challenge/response for detecting bots

Building Blocks for Preventing SPIT –Contd.

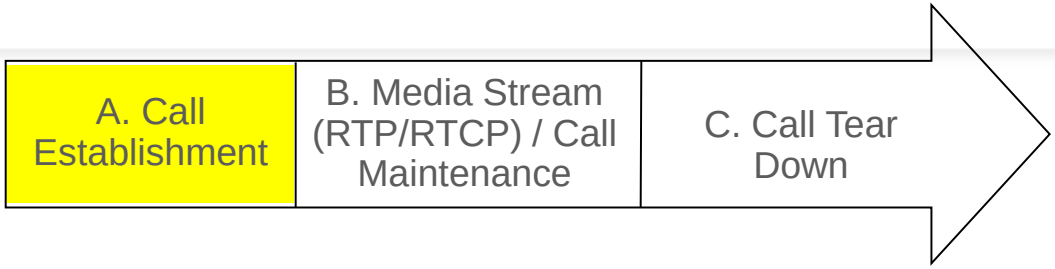
- Honeypot
  - Use extensions not assigned to user as *honeypots*
- Server side detection
  - Detect SPIT before it leaves the system
- User feedback
  - During the call or after the call to indicate SPIT
- VoIP feature analysis
  - Passive analysis to detect SPITter
- Reputation Management
  - Reputation value for the caller, callee or the call path

Semi Supervised SPIT Detection System



VoIP Call Features for Clustering

17 call features from VoIP signaling and media traffic used for clustering



1-2. From/To URI
3. Start time
4. Duration
5. # of SIP INVITE messages
6. # of SIP ACK messages
7-8. # of SIP BYE messages from caller/callee
9. Time since the last call from the originator of the current call
10-15. # of 1xx, 2xx, 3xx, 4xx, 5xx, and 6xx SIP response messages
16. Call frequency of the originator of the current call
17. Ratio of non-silence duration of the callee to the caller media streams

Only the call features in yellow are available at call establishment time.

Summary

- VoIP System and threats
- Architecture for Self-Protecting Communications
- Need for Detection and Mitigation Components on each element
- Central coordination and correlation
- SPIT Mitigation

In VoIP systems mitigation and detection components on each element with central control for defining policies and correlation yields a powerful protection framework.