DoS, Fraud and More

Dr. Dorgham Sisalem
Director Strategic Architecture

Introduction

- General introduction
- VoIP is part of the Internet so expect the same security issues
- Specific SIP attacks
- General protection approaches
- Summary

Some Security Myths

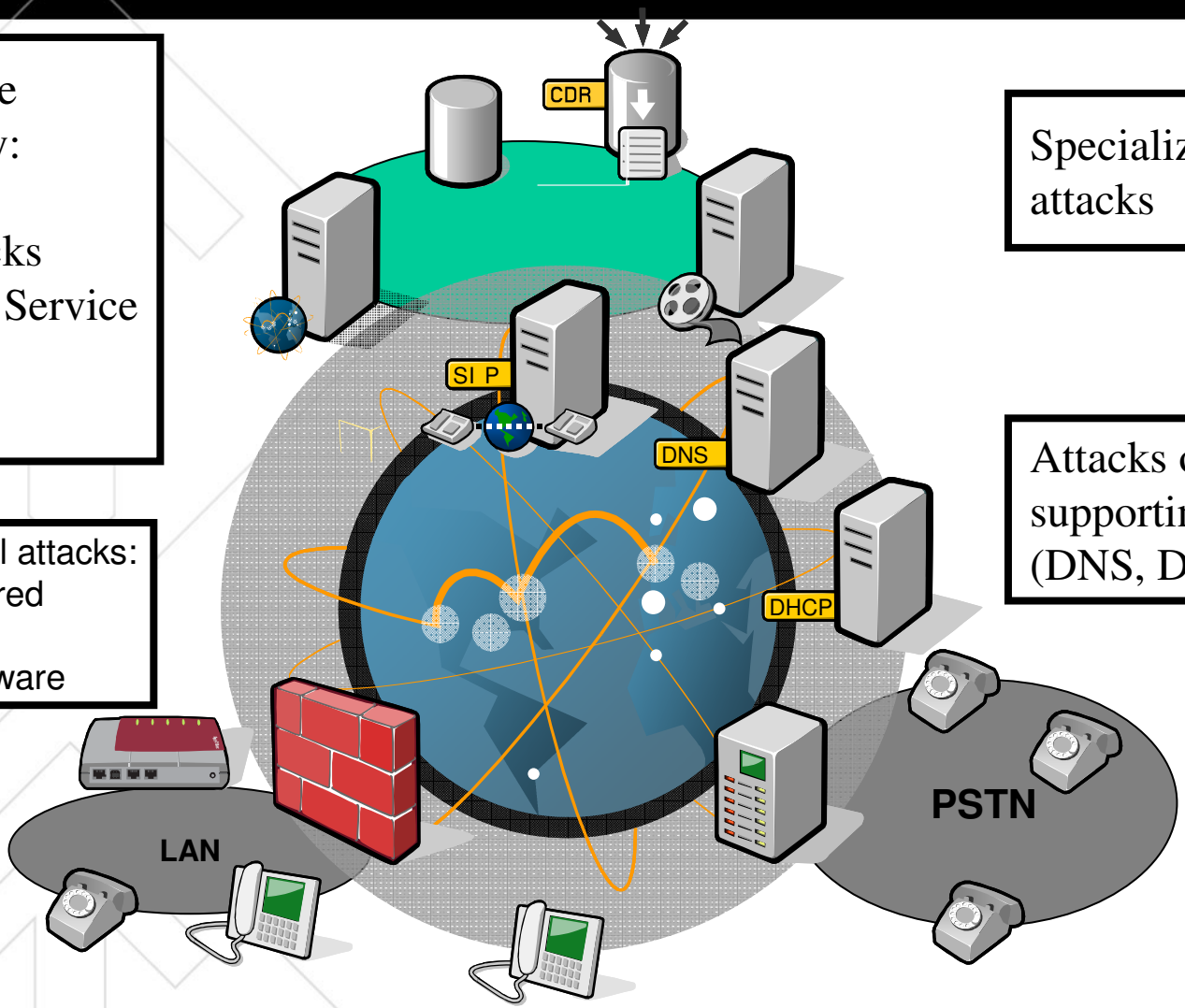
TEKELEC

- PSTN is 100% secure
  - True, as long as no one manages to get to the cables at the street corner
- Firewalls solve all security issues
  - Cutting off your Internet cable would solve them as well
- NAT is a great security feature
  - Sure, if you like complex things
- The Internet can withstand a nuclear war
  - The Internet maybe, its services probably not

What Should We Expect?

All what we know today:
- Viruses
- TCP attacks
- Denial of Service
….

Unintentional attacks:
-Mis-configured devices
- Buggy software



Specialized SIP attacks

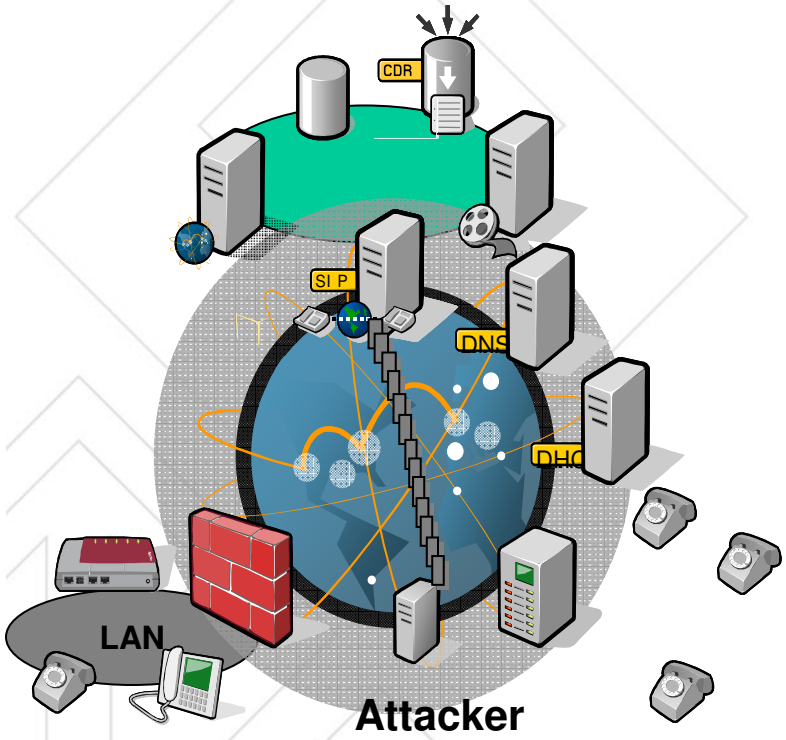
Attacks on supporting services (DNS, DHCP)

General Attacks

- Anything that applies to any device connected to the Internet applies to SIP
  - Software bugs can be misused for buffer overflow attacks
  - Bad implementation can lead to system crashes and security hole

- Anything that applies to Web and mail applies to SIP
  - Flooding attacks
  - TCP SYN attacks
  - DNS misuse
  - Cross site scripting

SIP Flooding Attacks

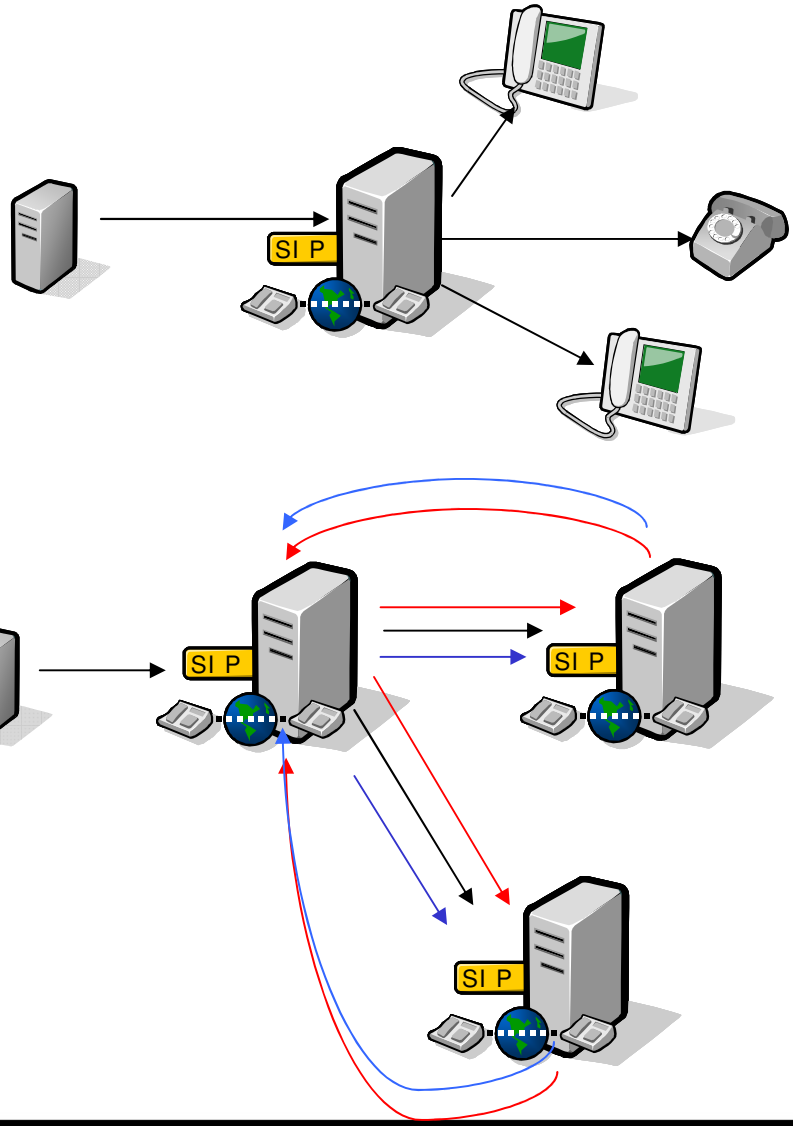


SIP Flooding Attacks

- One or more attackers send valid but useless SIP messages
  - Attack tool can be built by undergrad students with nearly no knowledge of SIP
  - Using bot-nets and similar techniques a very high load can be realized at the SIP server
    - High memory consumption
    - High CPU load
  - Difficult to detect
    - Traffic is valid
- Active research topic
  - Detect based on anomalies and similarities

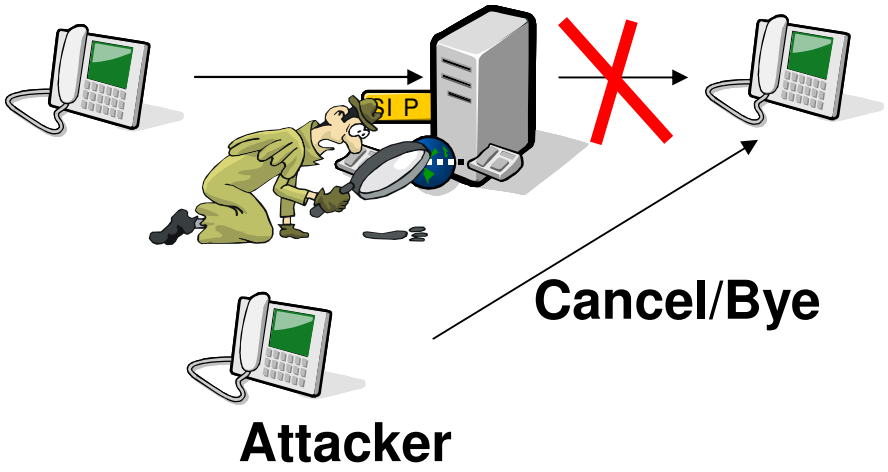
Fancy SIP Attacks

- Misuse SIP specification
  - Fork to non-existing destinations
  - Fork to malicious destinations
  - Configure loops
    - At server 1 forward calls to server 2 and 3
    - At server 2 forward calls to server 1
    - At server 3 forward calls to server 1
- Results in high memory usage
- More complex to realize and simpler to trace back



Fancy SIP Attacks

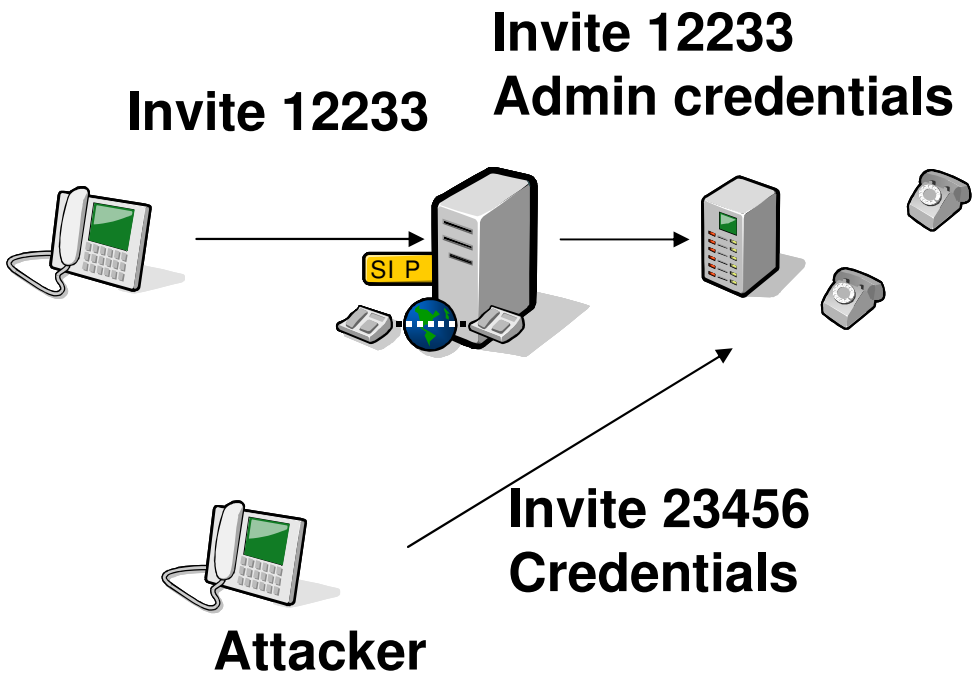
- Eavesdrop on SIP traffic and generate
  - BYE to established sessions
  - CANCEL to transaction in progress
- Could be annoying to the involved parties
  - Requires the ability to eavesdrop on the signaling traffic



Fraud with SIP

- Billing fraud
  - Guess admin passwords and credentials to get free access to PSTN

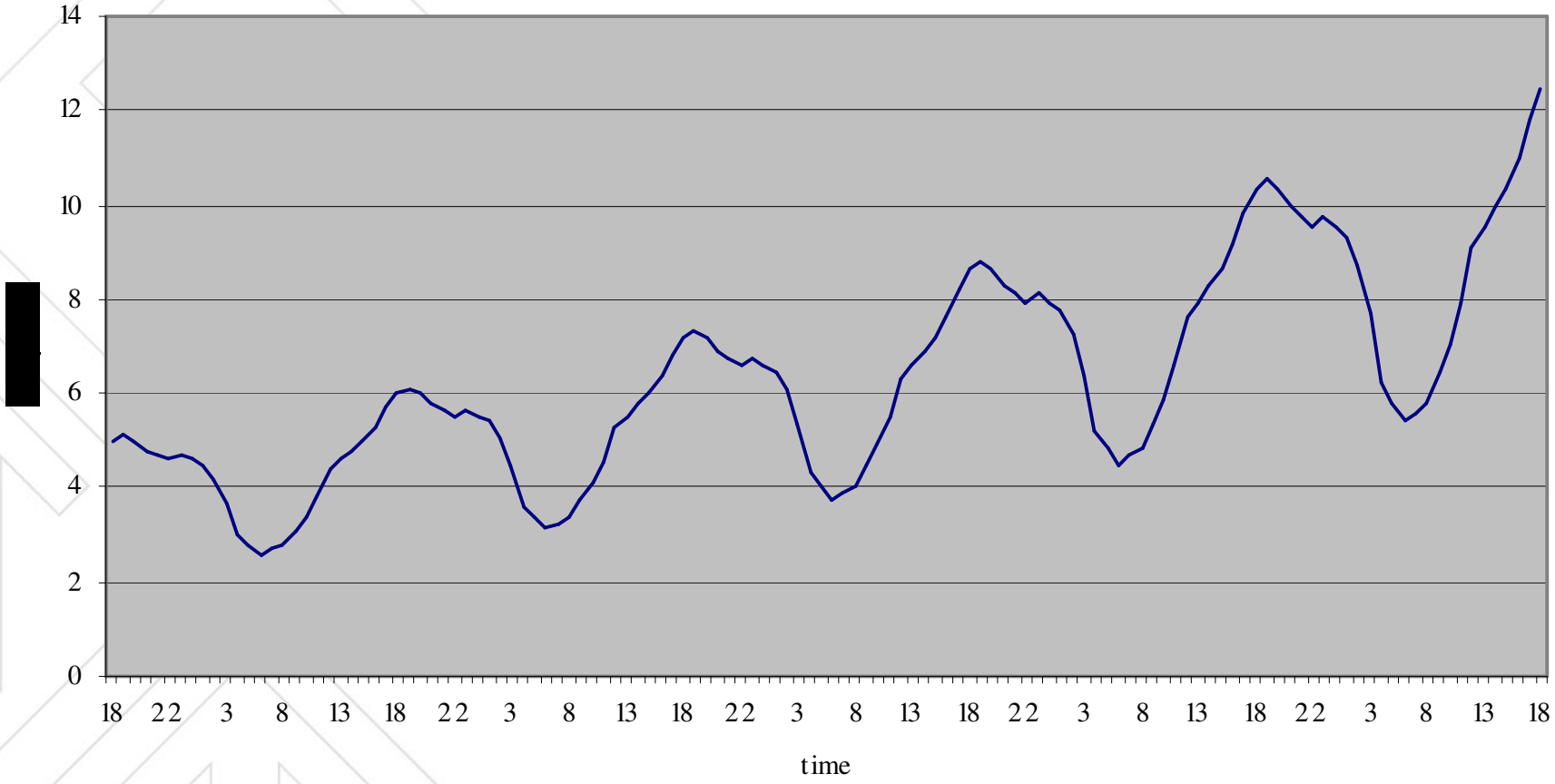
- Credit card misuse
  - Use free VoIP calls to service numbers to test credit card pins



Unintentional Attacks

- End systems generate too much useless traffic
  - Bad configuration
  - Buggy software
- Most common scenario today

Unintentional Attacks



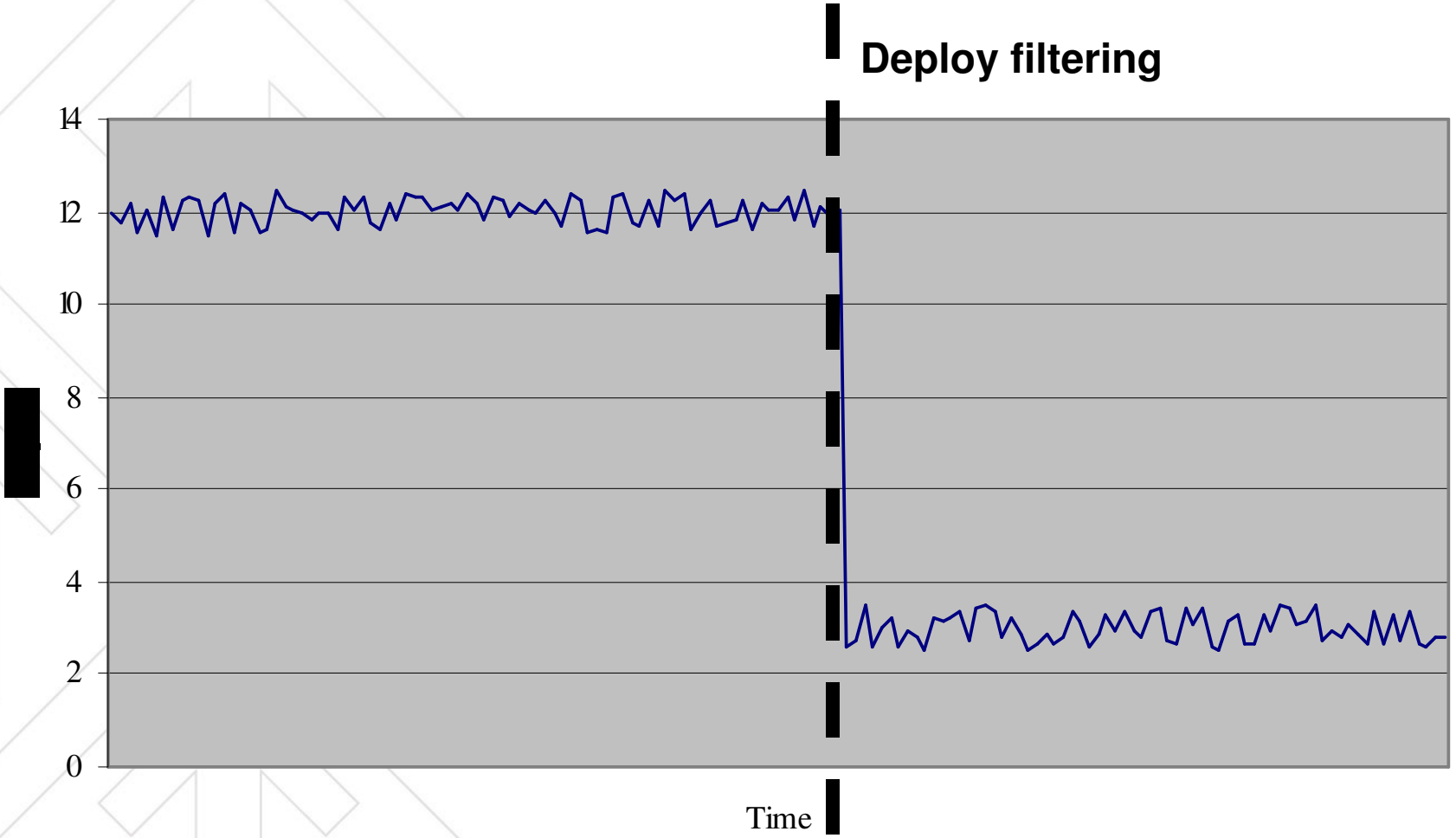
Analysis

- Good sales strategy?
- Symptoms
  - Higher load on data bases
  - Higher signaling traffic
  - No significant increase in number of calls
- General traffic analysis
  - No malicious packets
  - Unproportional high number of legal REGISTER messages
- Deep analysis
  - Certain user agents register once a second instead of once an hour
  - User agent otherwise totally RFC3261 conform

Solution

- Block all traffic from the IP addresses originating misbehaving traffic
  - Couple SIP logic with IP filtering
  - Possible but
    - Block all users with misbehaving user agents
- Block all registration traffic from the user agents
  - Simple but
    - Block all users using the same chip set (chip set indicated as the user agent and not only misbehaving user agents)
    - Block all users with misbehaving user agents
- Temporarily block registration traffic from the IP addresses generating misbehaving traffic
  - An IP address is misbehaving if it sends more than 3 REGISTER messages in less than one minute
  - If an address is misbehaving then block all REGISTER messages for 1 hour after which three REGISTER messages are allowed

Intelligent Packet Filtering



Unintentional Attack: The Mid-Night High

- To avoid improper use an ISP changes the IP address of its users every 24 hours
  - Would cause all registrations to become invalid
- Manufacturer of widely used VoIP/DSL boxes has the right approach
  - Disconnect the VoIP box every 24 hours
  - Reregister the user
- Right solution but:
  - 100000+ users registering between 3 and 4 pm is a well synchronized denial of service!!

DoS Prevention: High Level Requirements

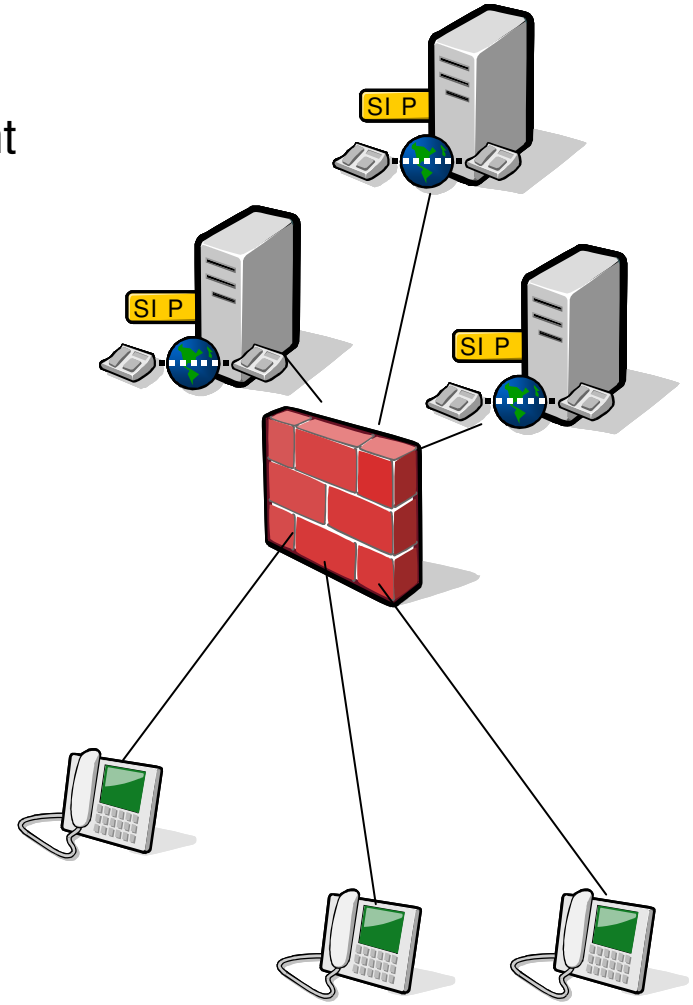
- Fast
  - Must process thousands of messages per second
  - Scale with the VoIP infrastructure
- Non-Intrusive
  - Do not add delay or SIP headers
  - Do no interfere with NAT traversal or service provisioning
- Adaptive
  - Integrate new rules and policies
  - Learn new attack signatures
- Complete
  - Analyze message and session irregularities
- Informative
  - Provide statistics and alarms in various levels of detail

Fortress and Moat

Fortress and Moat

Fortress and Moat

- Often suggested approach
  - Build an all knowing, all seeing component in front of the VoIP infrastructure
  - This component terminates sessions and starts new sessions to the proxies
  - Controls both signaling and media
  - Provide
    - Message parsing
    - Black and white lists
    - Media screening
- Adds a rather complex component in the path
  - Needs to be secured itself
  - Presents a nice target for attacks



Peace Keeping

- Use components dedicated for VoIP security that
  - Passively monitor incoming traffic
  - Check for irregularities
  - Filter out suspicious traffic
  - Deploy intrusion detection algorithms
  - Generate network statistics
- Failure of monitoring components does not lead to service failure
  - E.g., no decrease in the overall reliability of the service

Bottom Line

- SPIT, SPIM, VoIP DoS: Hype or Reality
  - Today Hype tomorrow Reality
- Reality
  - The enemy is still not the script Kiddy
  - It is those who did not spend enough time to read the RFCs and test their solutions No Script kiddies yet
  - Immature user agents
  - Mis-configured proxies and gateways
  - Inaccurate CDRs
  - Too stringent firewalls and mis-configured NATs
  - Remember:
    - DNS traffic up-to 90% mainly junk
    - Email traffic up to 95% junk

Thank you