SALARE SECURITY™

VoIP – Panacea or Time Bomb?

February 25, 2009

Agenda

1. **About Salare Security and Paul Sand**
2. **Importance of Security**
3. **VoIP the Panacea**
4. **VoIP the Time Bomb**
   a. VoIP Concerns
   b. Security Appliance Challenges
5. **Defusing the Time Bomb**
   Securing a VoIP Network
6. **Questions and Answers**

Paul Sand

- **President and CEO, Salare Security**
- **Experience at:**
  - mVerify Corporation
  - Lucent Technologies
  - AT&T
  - Bell Labs
- **Senior Member IEEE**
- **Member of:**
  - ISSA
  - IS Alliance
  - FBI InfraGard

Importance of IT Security

How Much Should We Worry?

"Cyber crime proceeds are greater than those of illegal drug sales." – US Treasury Department

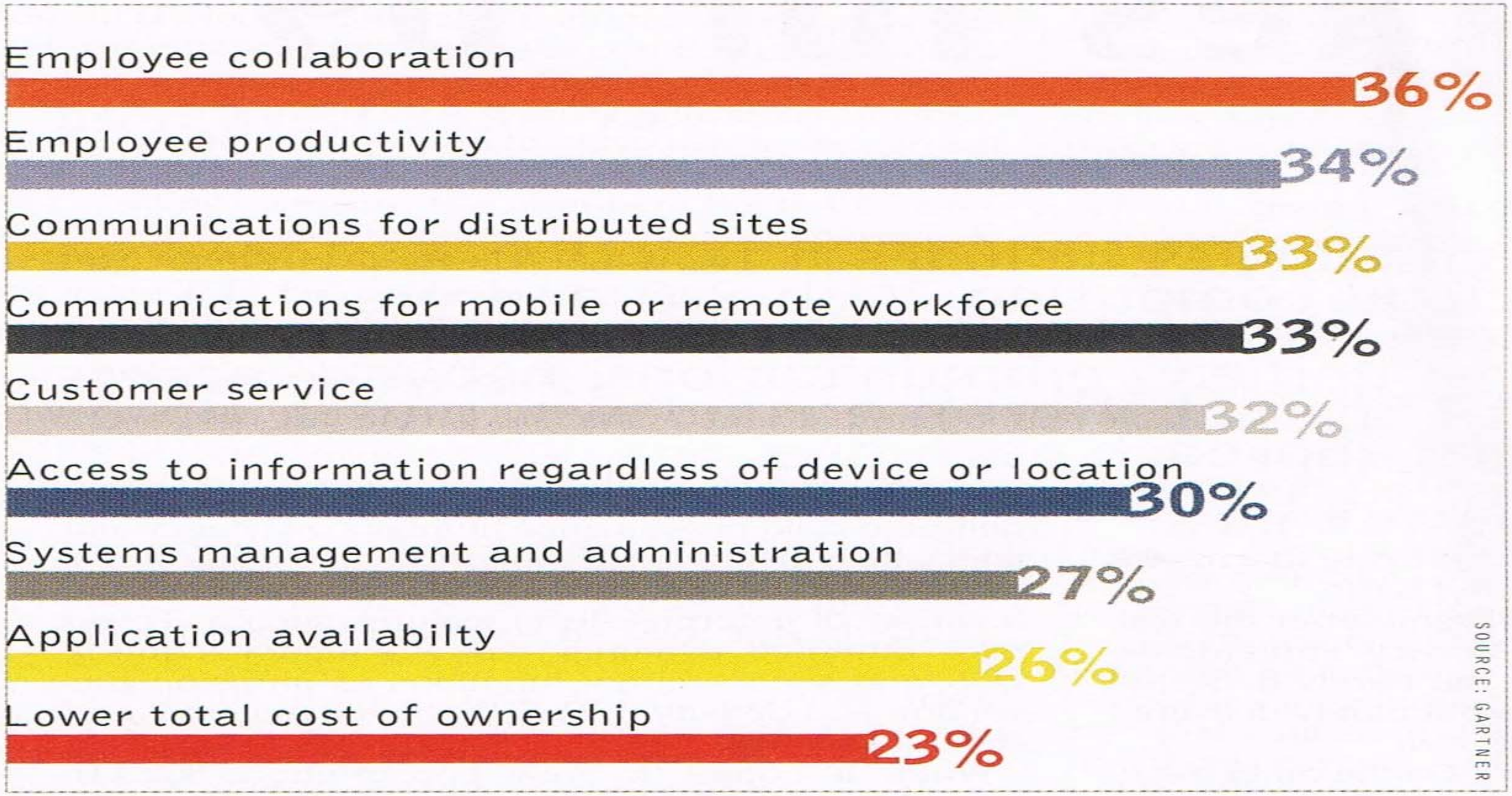
What Should We Worry About?

- Confidentiality (Privacy)
- Integrity (Trustworthiness)
- Availability (Usefulness)

VoIP the Panacea

Why unified communications?

Gartner asked IT execs in North America and Western Europe to list the three areas of their organizations that were most improved after unified communications was deployed. Employee collaboration and productivity received the most nods.



SOURCE: GARTNER

How VoIP Works

Important VoIP Protocols

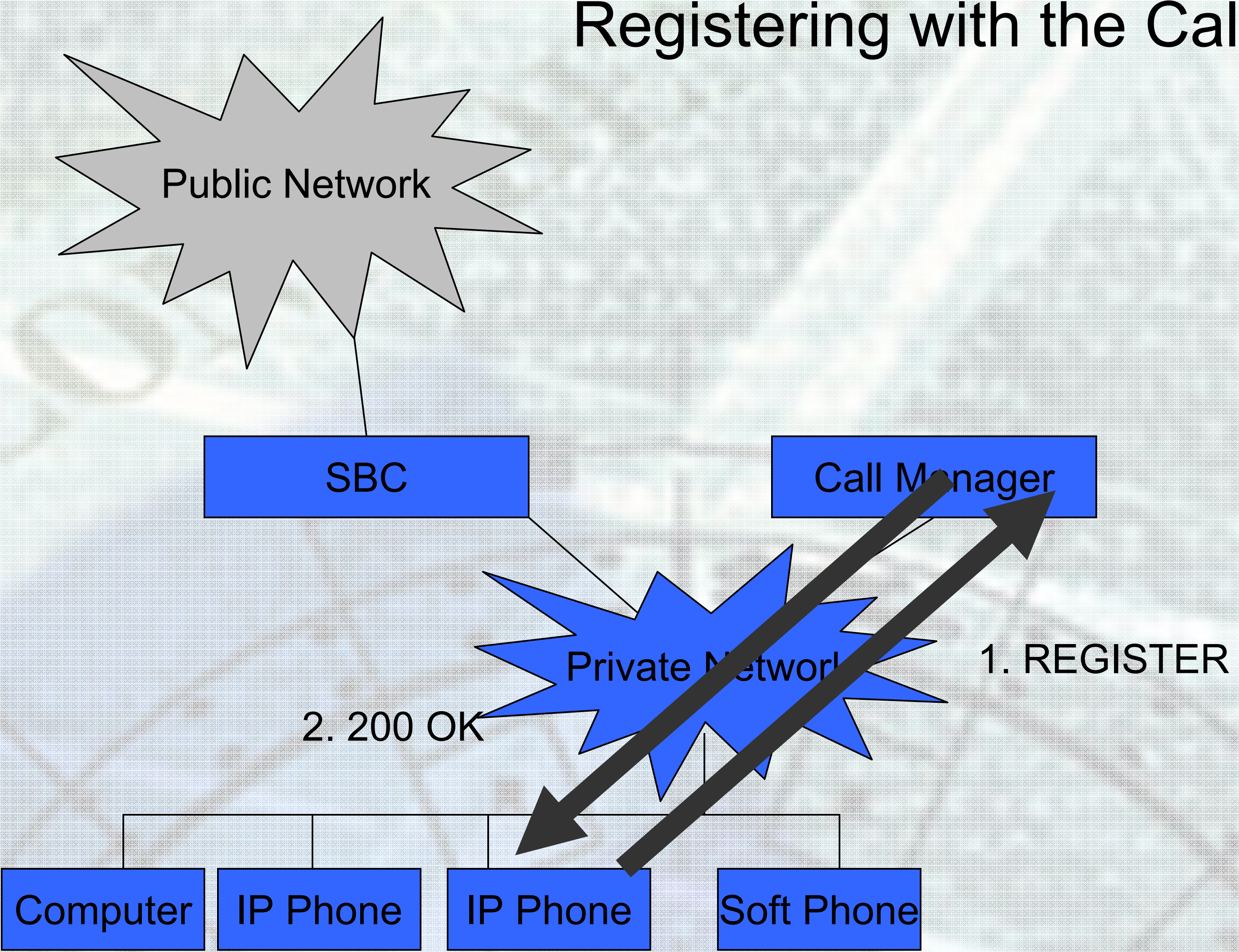
SIP (Session Initiation Protocol)

Signaling (Off-hook, Dialing)

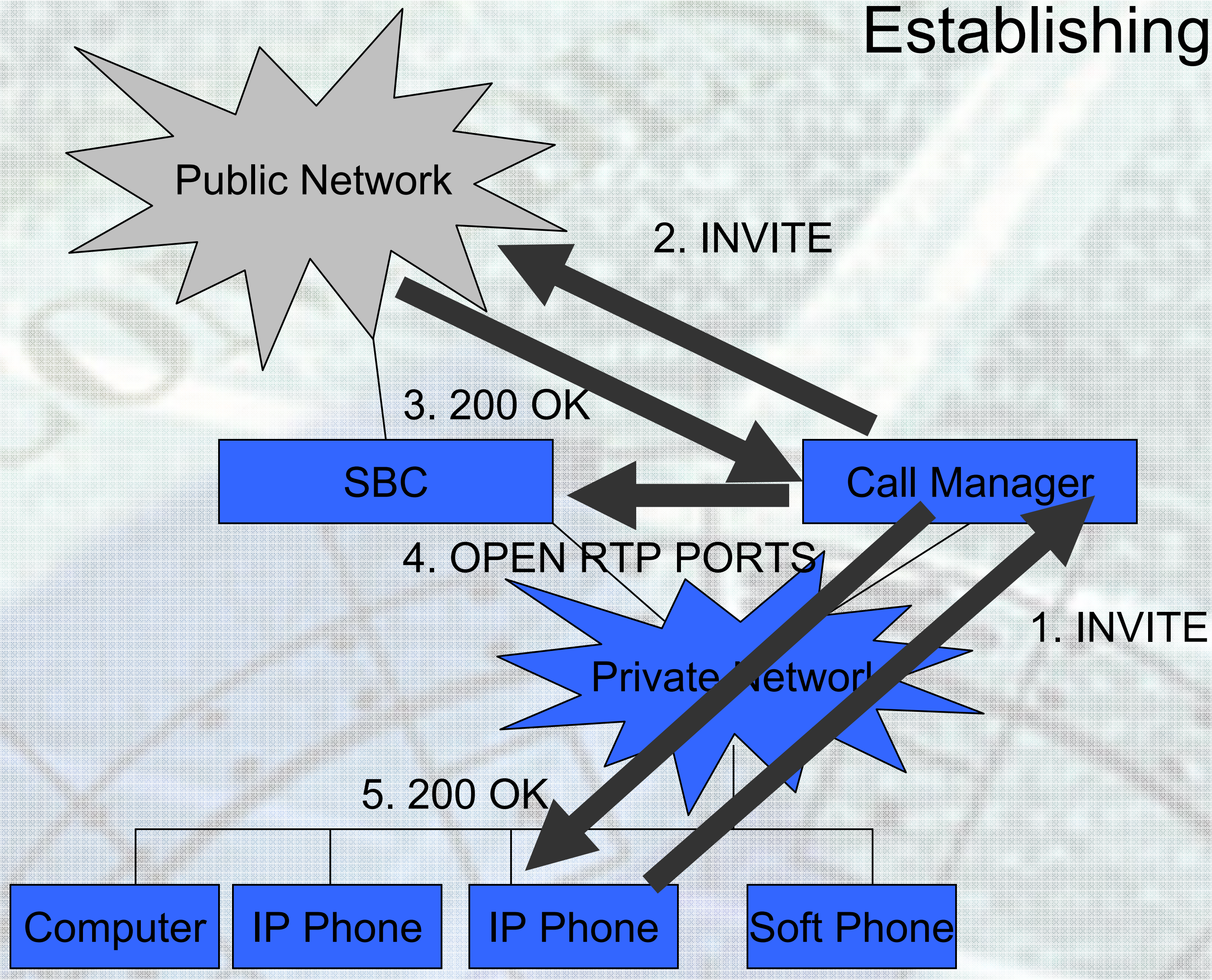
RTP (Real-Time Protocol)

Media (Speech)

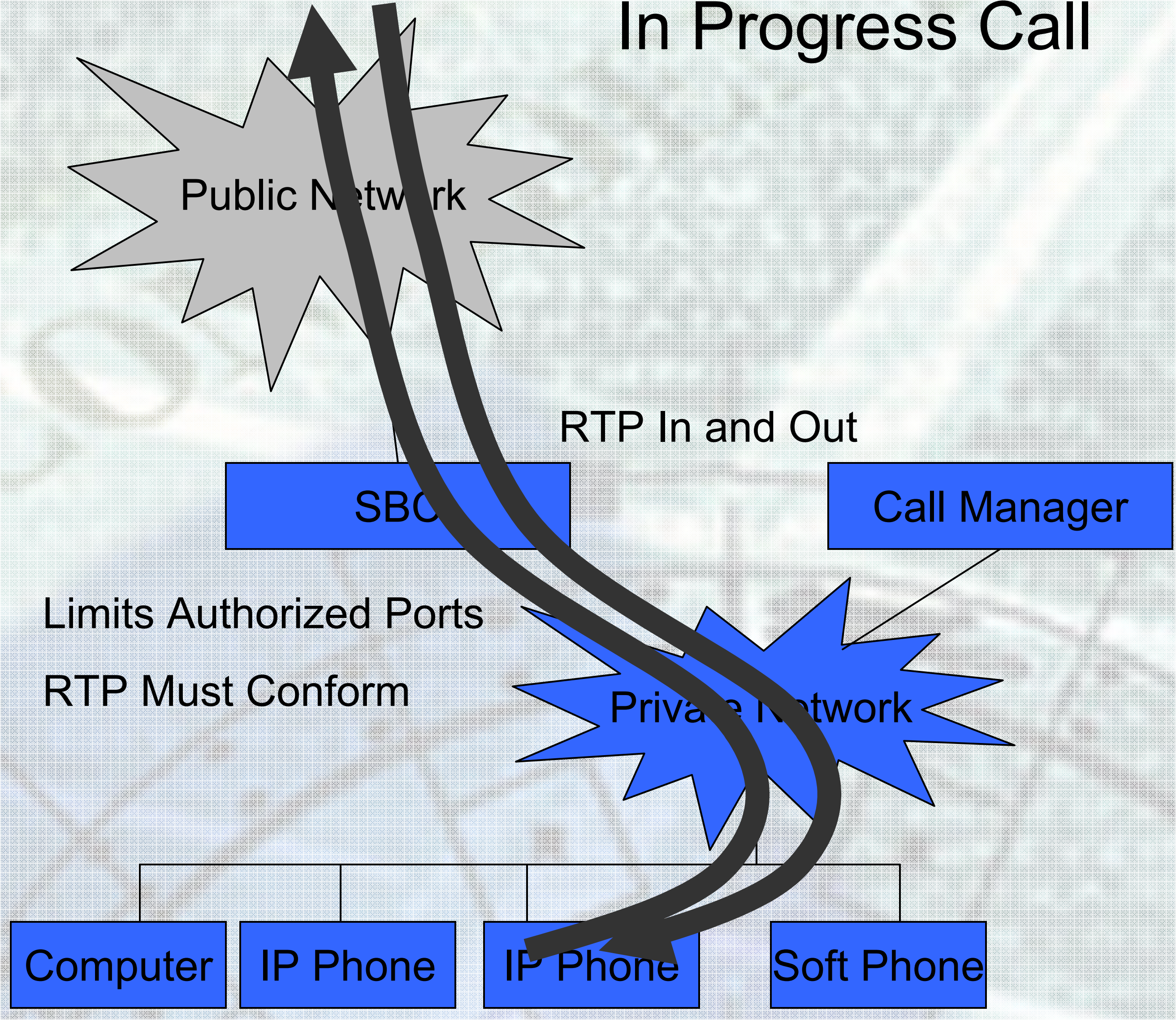
Registering with the Call Mgr



Establishing a Call

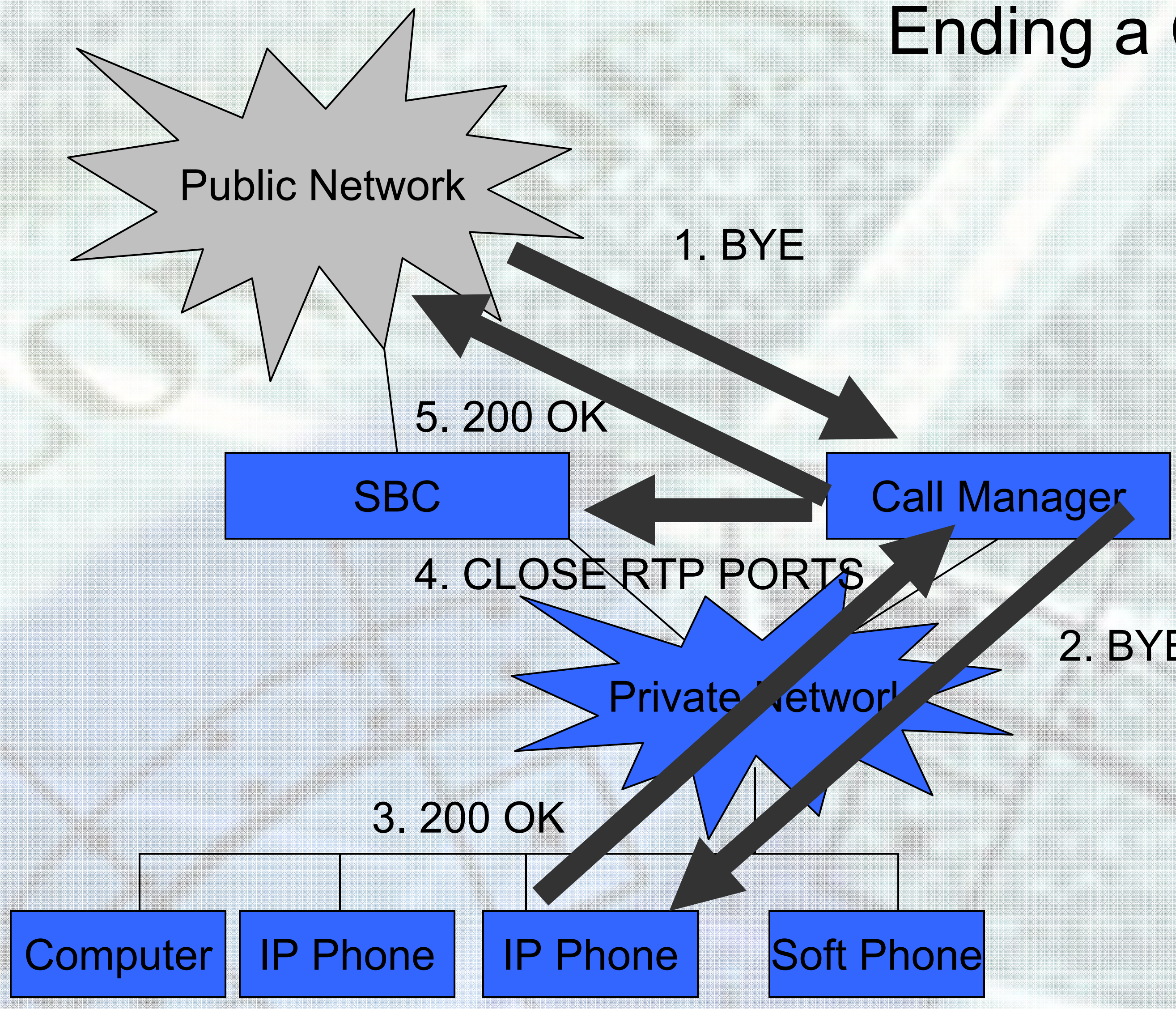


In Progress Call



Copyright 2009. Salare Security LLC.

Ending a Call



Copyright 2009. Salare Security LLC.

Voice is Different

- **Needs Low Latency**
  Time to get through network
- **Needs Low Jitter**
  Inconsistency in delivery of packets
- **Needs Privacy**
  The content must be encrypted
- **Resilient to Loss**
  Missing pieces of information not a problem
- **User Datagram Protocol (UDP) vs. Transport Control Protocol (TCP)**
  Connectionless vs. Connection Oriented

VoIP the Time bomb

“VoIP is, in essence, a time bomb, poised for a massive exploit,” says Paul Simmonds, a member of the management board of the Jericho Forum, a user group promoting new principles for secure networking.

Network World Staff, Network World, 01/02/08

Do You Trust Your Telephone?

Telespoof Demonstration

Telespoof

www.telespoof.com

Integrity: Who’s Calling?

- Caller ID
- Congressional Action
  - “…a person may not, with the intent to defraud, make a call or engage in other conduct that results in the display of false caller identification on a recipient's phone.”
  - U.S. House HR 251, the "Truth in Caller ID Act," passed June 12, 2007
  - U.S. Senate considered similar legislation (S 704)

Integrity: Who are You Calling?

- Malicious “Call Forwarding”
- Poisoning of:
  - Domain Name Server (DNS)

    Domain Names (www.cnn.com) mapped to IP addresses (157.166.224.26)
  - Address Resolution Protocol (ARP)

    IP addresses mapped to Computer’s Media Access Control (MAC) address

Integrity: Device Management

- VoIP Requires Lots of Devices Spread Over a Large Network
- Securing all of them Can be a Challenge
- The Devices are “dumb” but not “dumb enough”
  - Have Browsers
  - Can’t Host anti-Malware Software

Unmanaged VoIP Devices Demonstration

http://www.salaresecurity.com/v2o3i4p5/vd/

Is Your Telephone Ready?

Availability: Power

- The Public Switched Telephone Network has Redundant Power
- VoIP Power is not Redundant
- Remediation Add Redundant Power
  - – Uninterruptable Power Supply (UPS)
  - – Power over Ethernet (PoE)

Availability: Denial of Service (DOS)

- VoIP More Sensitive to DOS
- Types of Attacks
  - – REGISTER Flood
  - – INVITE Flood
  - – RTP Flood
- Remediation

SIP-Aware Firewall/Session Border Controller (SBC)

Can You Speak Freely?

Confidentiality: What is Said

- VoIP based on IP, so it can be:
  - Intercepted
  - Recorded
  - Monitored
  - **Discovered?**
- Remediation: Secure RTP (SRTP)
  - Media Channel
  - Point-to-Point
  - Any Type of Encryption

Confidentiality: Who calls Who

- VoIP based on IP, so it can be:
  - Intercepted
  - Recorded
  - Monitored
  - Modified
- Remediation: Secure SIP (SIPS)
  - Uses TLS Encryption
  - Hop-to-Hop so QoS is Preserved
- Remediation: Native Address Translation (NAT) Firewall

Can Secrets be Stolen?

Confidentiality: Data Loss

How to Cheat at VoIP Security, Thomas Porter, Michael Gough

“VoIP Networks simply have not existed long enough to provide real-world examples of information breaches. But they will.”

Confidentiality: Data Loss

- Data Loss through VoIP
- “Vunneling™” Exploit – tunneling data through voice or masquerading data as voice
- What Can be Stolen?
  - IP
  - Credit Card Information
  - Customer Information
  - Anything!

Vunneler™ Exploit Demo

http://www.salaresecurity.com/v2o3i4p5/V2/

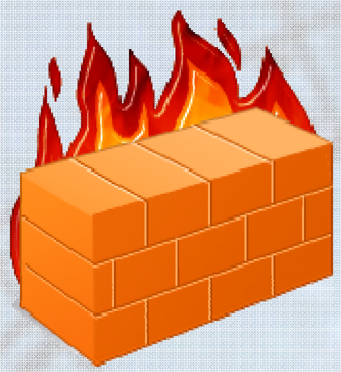
Is Voice Service Good?

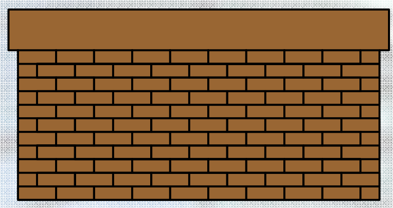
Availability

- Quality of Service (QoS)
  - Lower Jitter
  - Lower Latency
- The Network
  - Separate Physical Networks
  - Separate Virtual Networks – Virtual Local Area Networks (VLANs)

Security Appliance Challenges

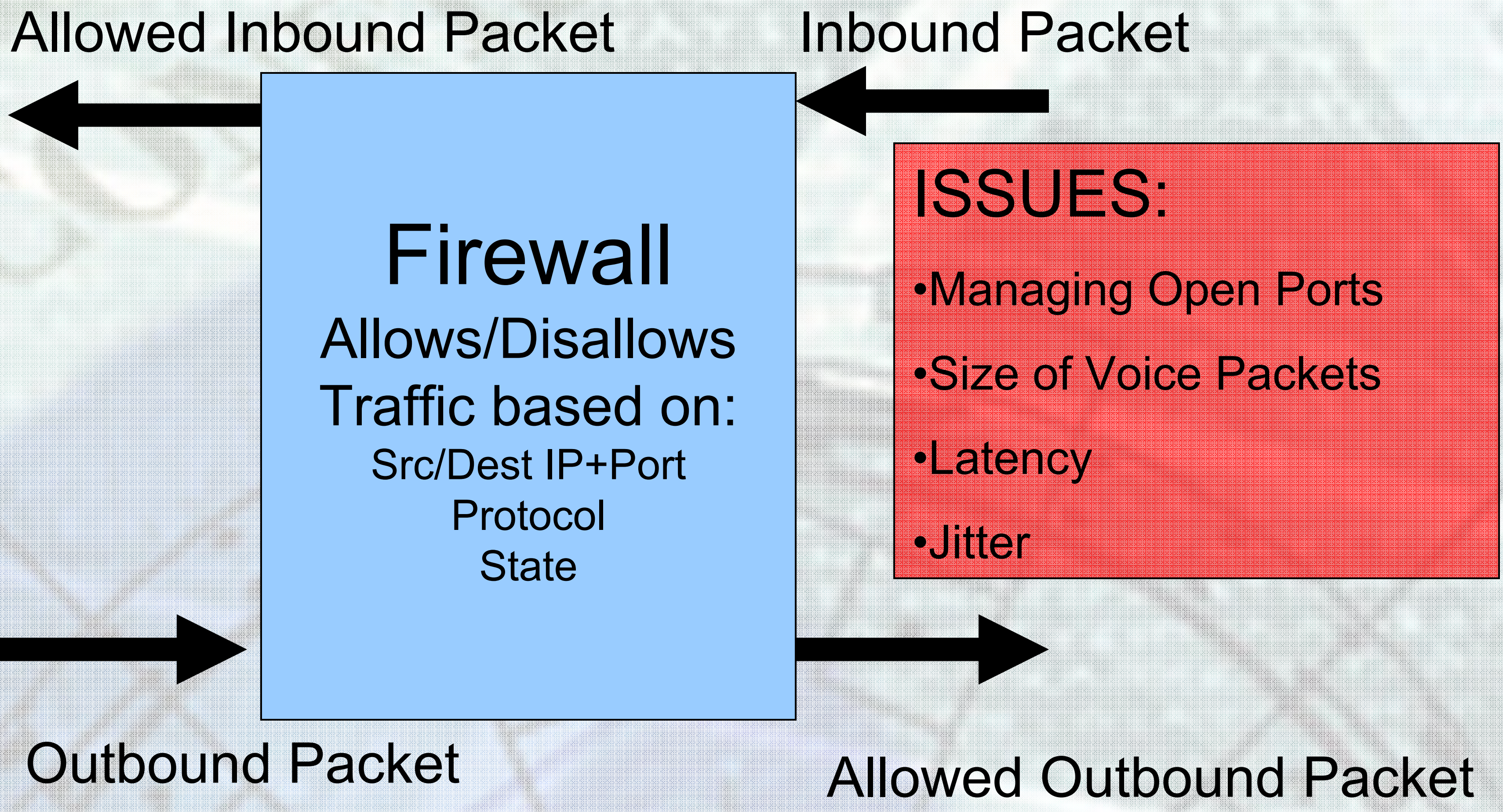
- Firewall Appliances
- Data Loss Prevention Appliances





Firewalls Challenges

Session Border Controller (SBC) = VoIP Firewall



Allowed Inbound Packet

Inbound Packet

Firewall

Allows/Disallows Traffic based on:

Src/Dest IP+Port

Protocol

State

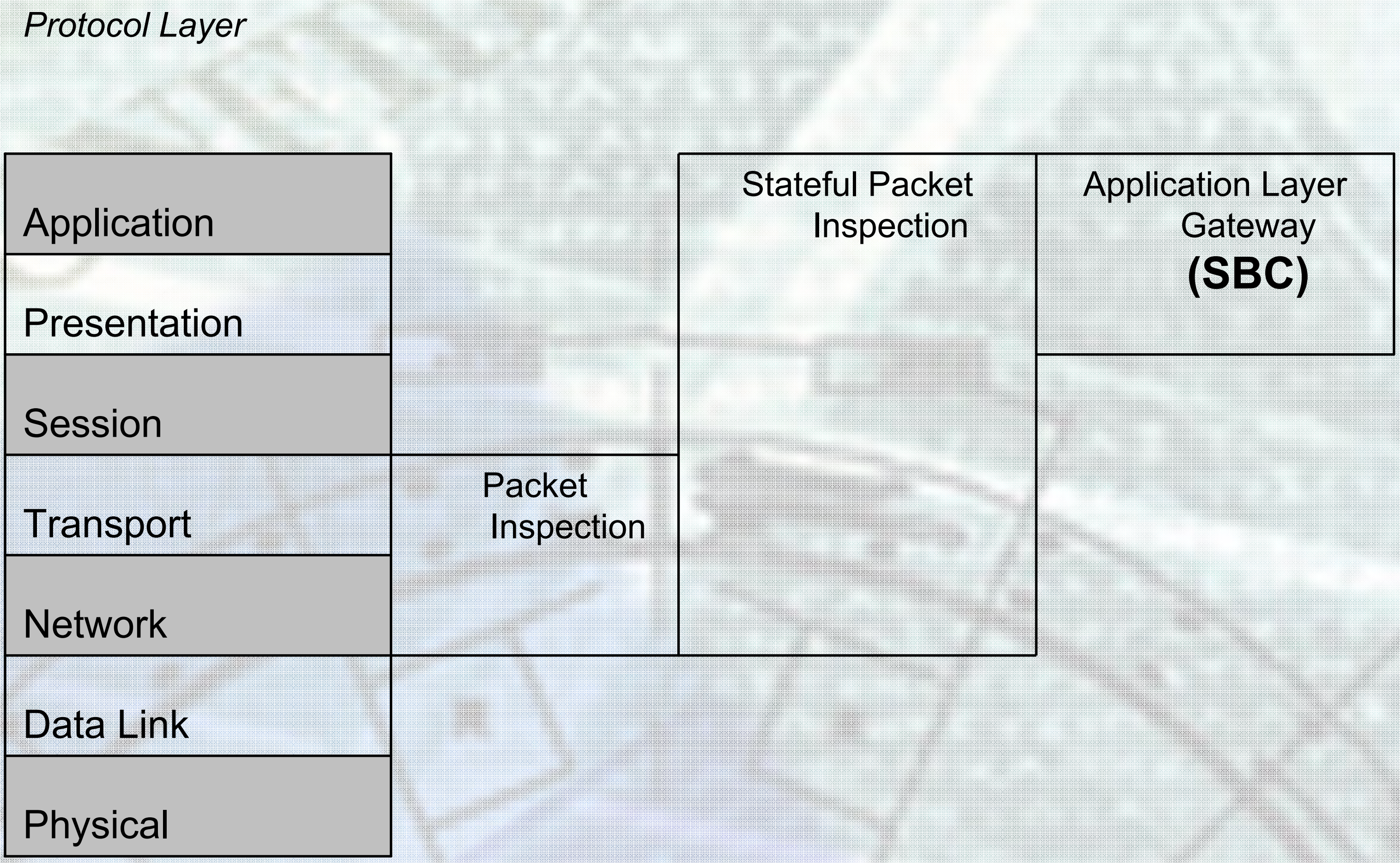
ISSUES:

- Managing Open Ports
- Size of Voice Packets
- Latency
- Jitter

Outbound Packet

Allowed Outbound Packet

Firewall Evolution



Protocol Layer

Application

Presentation

Session

Transport

Network

Data Link

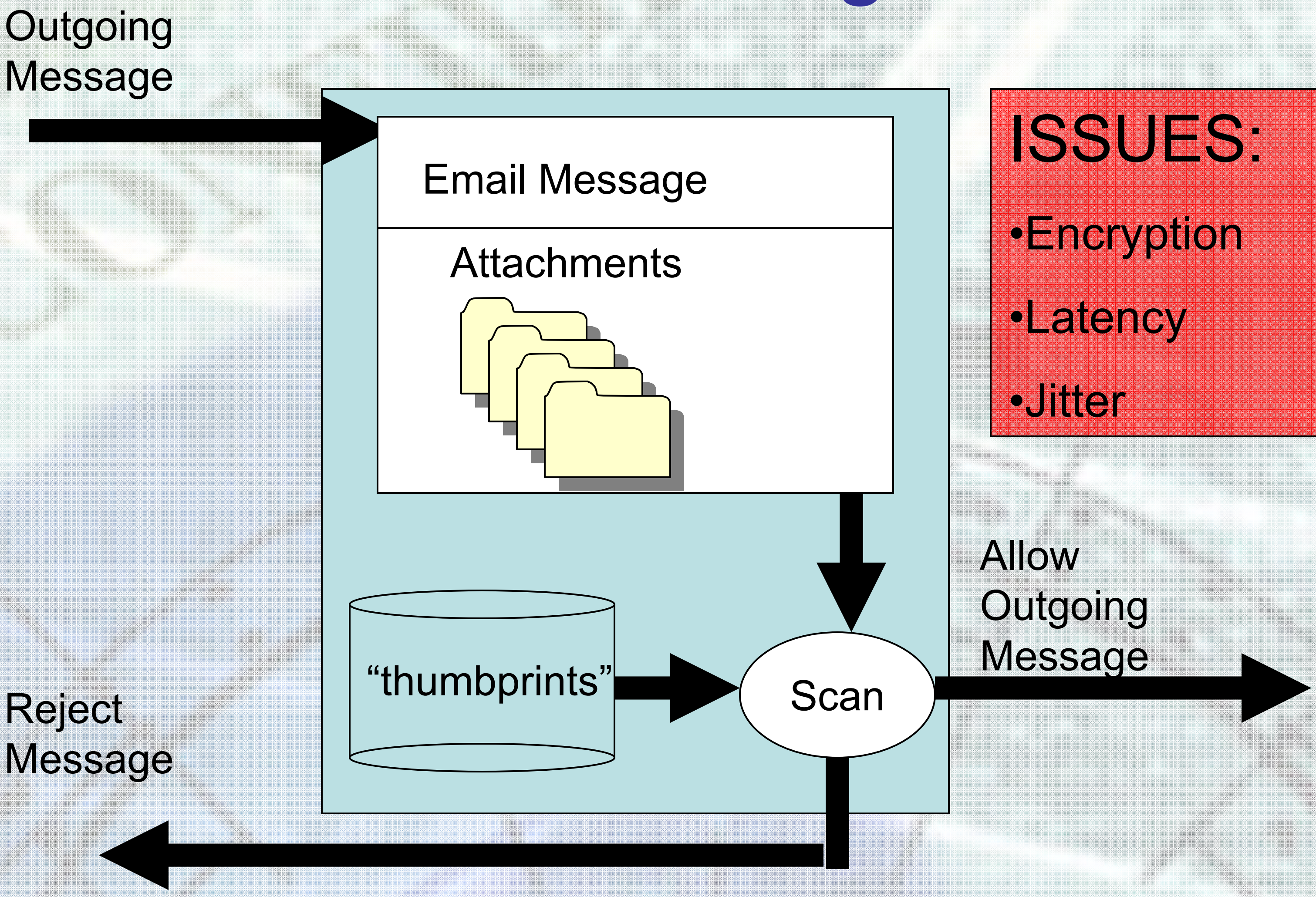
Physical

Packet Inspection

Stateful Packet Inspection

Application Layer Gateway **(SBC)**

Data Loss Prevention (DLP) Challenges

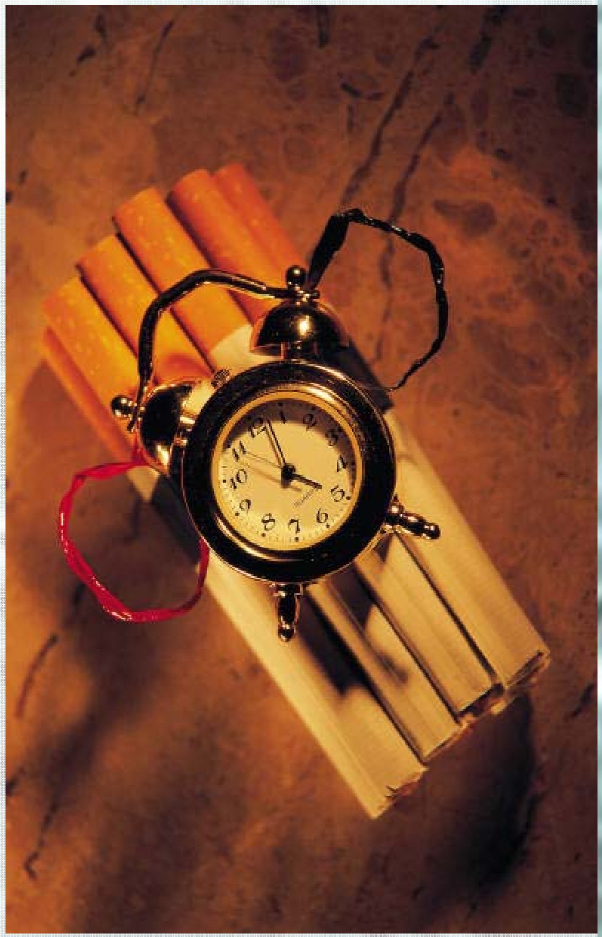


ISSUES:

- Encryption
- Latency
- Jitter

Defusing the Time Bomb

- **Redundancy**
  - Redundant Power (use PoE)
  - Redundant Proxies/DNSs/Switches
- **The Network**
  - Use VLANs
  - Use QOS Routers & Switches
- **Firewalls**
  - Use SIP-Aware Firewalls or SBCs
- **Phones**
  - Use SRTP and SIPS
  - Places Phones behind a NAT
- **Network Behavior Analysis**
  - Watch Phones for Abnormal Behavior
- **Bearer Channel**
  - Stop Malicious File Transfers with vPurity™



Panacea or Time Bomb?