Best Practices for Securing IP Telephony

Irwin Lazar, CISSP

Senior Analyst

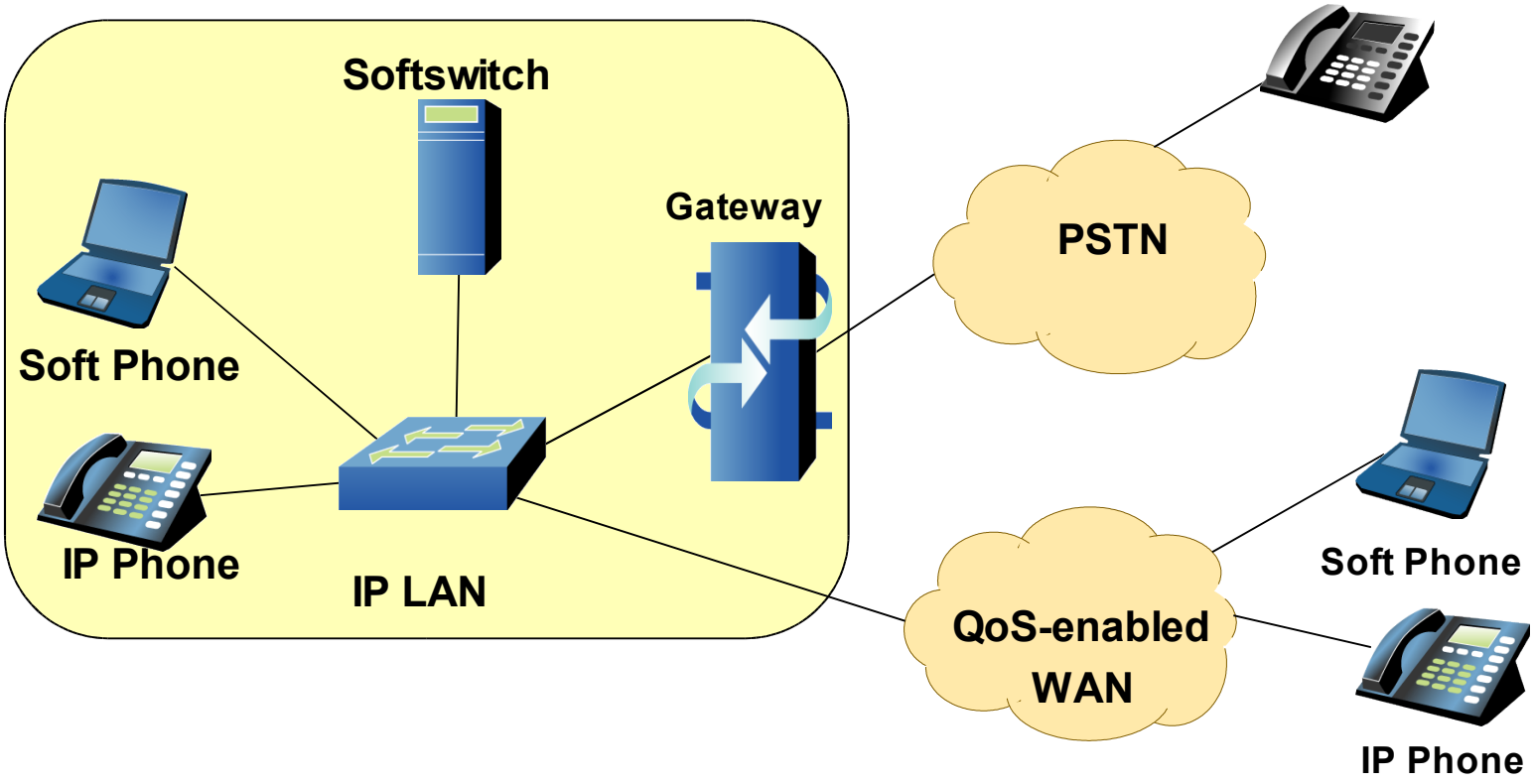
Burton Group

Agenda

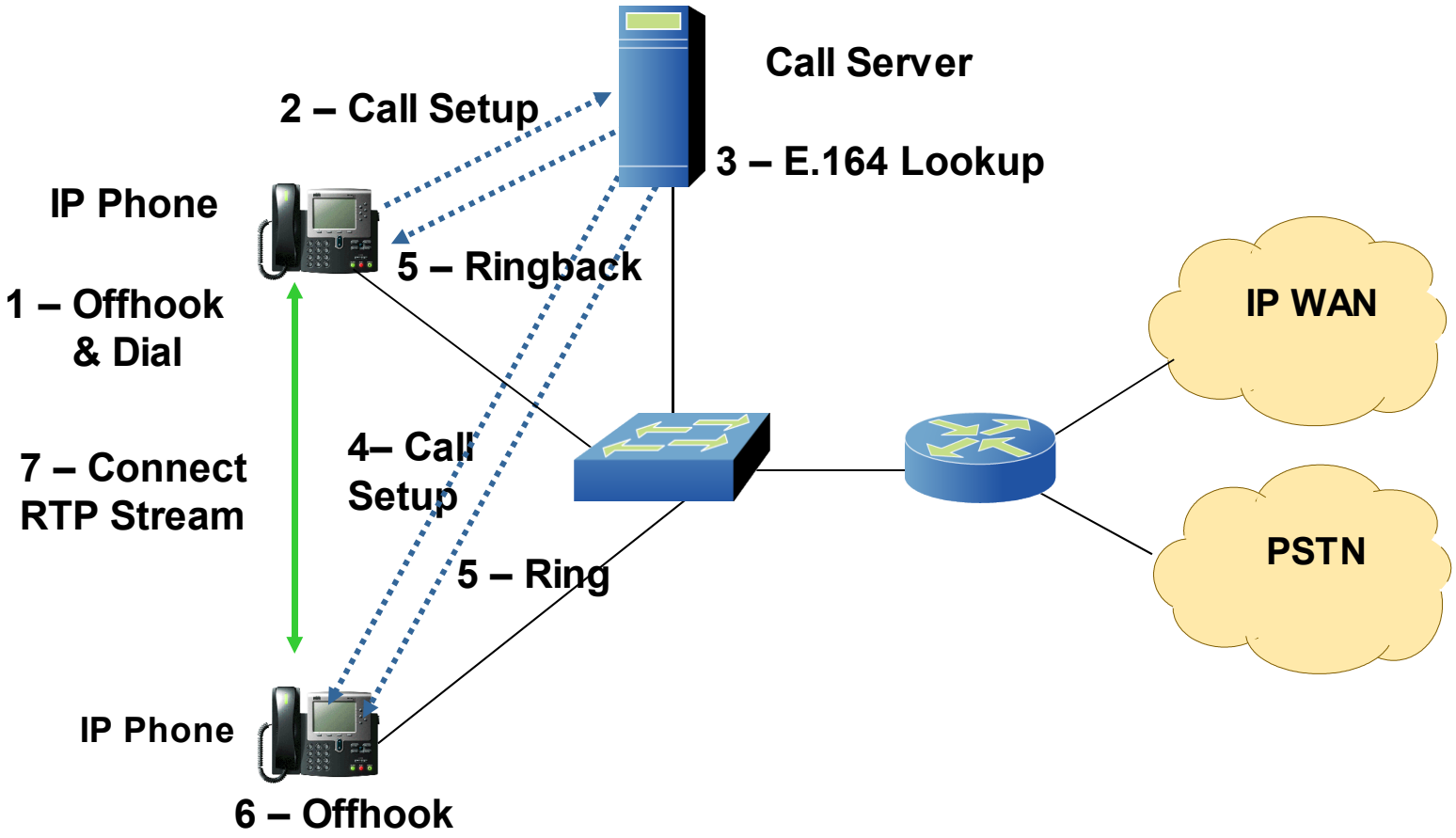
- **VoIP overview**
- **VoIP risks**
- **Mitigation strategies**
- **Recommendations**

VoIP Overview

VoIP Functional Diagram



Signaling Concepts



What Do These Diagrams Tell Us?

- **Voice & data share a common infrastructure**
  - **No different from a risk perspective**
  - **Anything that affects data will affect voice**
- **This represents a major change in the way voice services are provided**
  - **Historically functions were separate**

Hypothesis

- **Enterprises implementing VoIP have an even greater need to protect their networks than before**
  - **There is no fallback mechanism if security is compromised**
  - **Both data and voice will be effected**

Protocols to Know

Signaling protocols:

- **H.323 - used by most vendors**
  - **Cisco & Siemens use proprietary alternatives**
- **SIP - Session Initiation Protocol**
  - **Emerging "IP" based protocol**
- **H.323 relies on gateways, SIP allows direct any-to-any communications**
  - **Though in reality they are implemented the same way**

More Protocols to Know

Voice Bearer Transport Protocols

- **RTP - Real-Time Protocol**
- **RTCP - Real-Time Control Protocol**
- **UDP - User Datagram Protocol**

VoIP Risks

Specific Risks to VoIP

- **External threats**
  - **Hacks against phones, call control servers, gateways**
  - **Denial of Service (DoS) attacks**
  - **Trojans, viruses, worms**
  - **Illicit phone system usage**
  - **VoIP spam**
  - **Compromise of call data**
- **Internal Threats**
  - **Eavesdroppers**
  - **Illicit phone system usage**
  - **Compromise of call data**

A Few Possible Scenarios

- **DoS attack on inbound calling gateway**
- **Worm attack takes down call servers**
- **Worm/Virus causes excessive network congestion**
- **Unauthorized calls routed through your gateway**
- **Calls are secretly recorded**
- **Improper long distance usage**

Scared Yet?

- **Well…you should be!**
- **BUT!**
  - **You ought to be protecting against most of this stuff already**
  - **A few of these risks are already out there**
    - **Unauthorized phone use, outside hacking**
  - **Mitigation strategies are available**

IP Telephony Security

- **Mitigation Strategies**

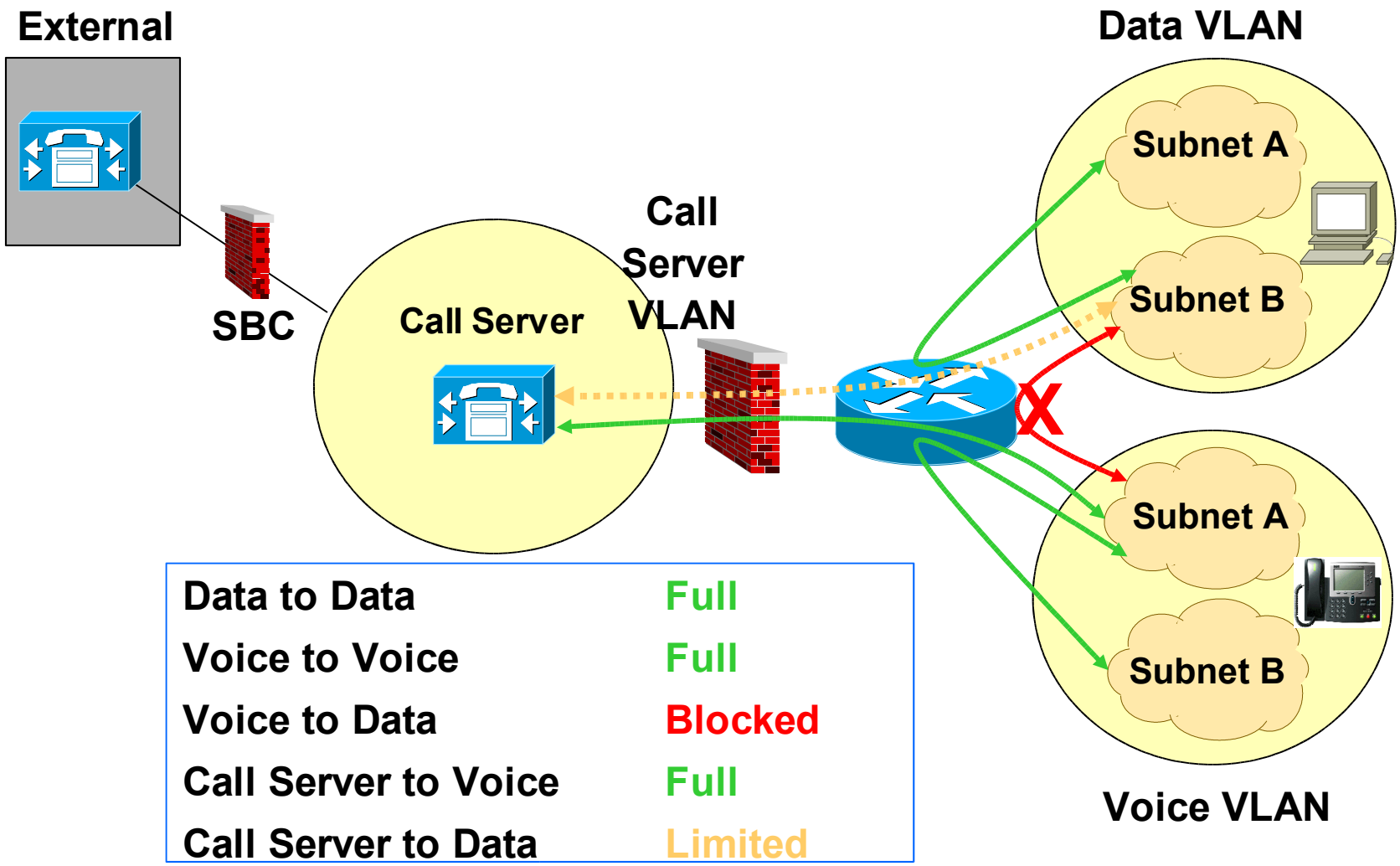
Basic Secure IP Telephony Design

- **Network security principles:**
  - **Logical separation of voice and data via VLANs wherever possible**
    - **Minimize interconnection points**
  - **VoIP-aware firewalls at interconnection points**
  - **Host-based intrusion detection & virus detection on all call management devices**
  - **Intrusion detection at network exit/entry points**

Firewall Concerns

- **Firewalls must be VoIP-aware**
  - **VoIP relies on dynamic port creation for voice traffic**
  - **Signaling protocols use well known ports**
  - **NAT may get in the way**
- **Solution: Session Border Controllers**
  - **Kagoor, Acme Packets, Jasomi, Nextone, etc.**
  - **SBCs track call establishment and dynamically handle NAT and port filtering**
  - **May also act as a calling proxy**

Security Architecture

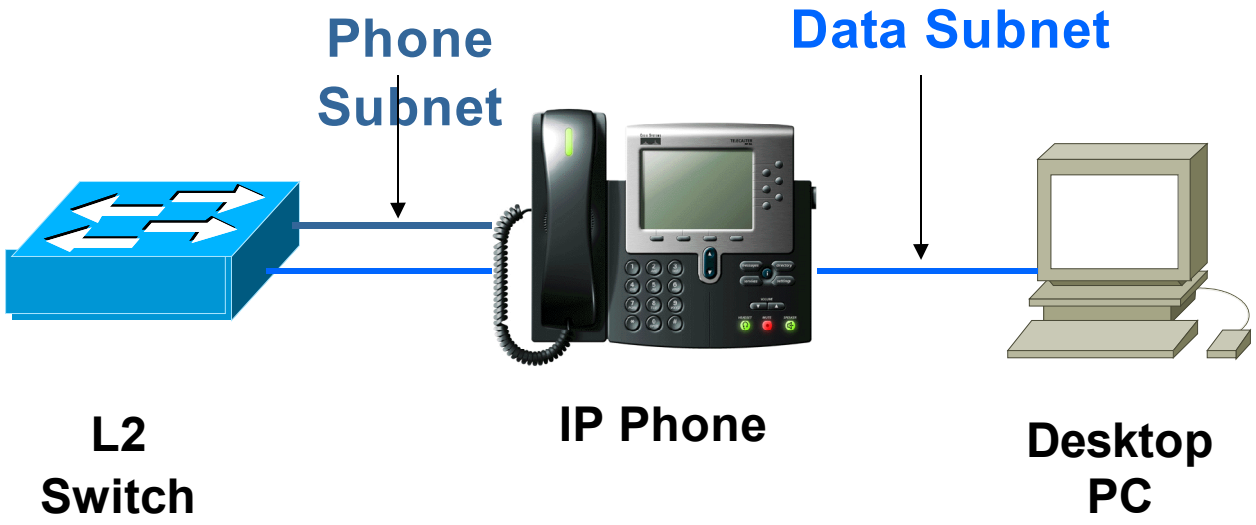


Data to Data	Full
Voice to Voice	Full
Voice to Data	Blocked
Call Server to Voice	Full
Call Server to Data	Limited

Logical Separation Issues

- **Requires Ethernet switches to support 802.1Q VLAN Trunking**
- **Two implementation methods**
  - **Ethernet switch in IP phone**
  - **Ethernet switch in closet performs separation**
- **Difficult to implement in softphone environments**

Phones at 802.1Q Trunks



Call Security Options

- **End-point security:**
  - **User authentication for hard/soft phones**
    - **802.1x - based**
  - **Phone authentication to call controller**
  - **Use of MAC address filters to prevent rogue assignment of IP addresses and transfer of configuration files**

Call Security Options (2)

- **Call data security**
  - **SSL/TLS encryption between end-points and call control servers**
    - **Negative performance impact**
  - **S/MIME signing & encryption of call data**
  - **SRTP - Secure RTP**
- **Prevent anonymous in-bound calling**
  - **Inbound calls only accepted from trusted or verifiable sources**
    - **Use of trusted certificate authority**

Call Security Options (3)

- **Protection against Denial of Service Attacks**
  - **Only an issue when there is direct connectivity of VoIP "Islands"**
  - **Use of DoS mitigation techniques or devices**
    - **E.g. Arbor Networks, Riverhead (Cisco)**

Does it Work?

- **"Breaking through IP telephony security" Network World - May 24, 2004**
  - **Mier test of Avaya & Cisco VoIP Security**
  - **Findings:**
    - **Both were secure against hacker attacks against call control infrastructure**
    - **Both were susceptible to passive probes**
    - **Avaya phones could be disrupted**
  - **Bottom line: Both systems were reasonably secure IF security architectures were fully implemented**

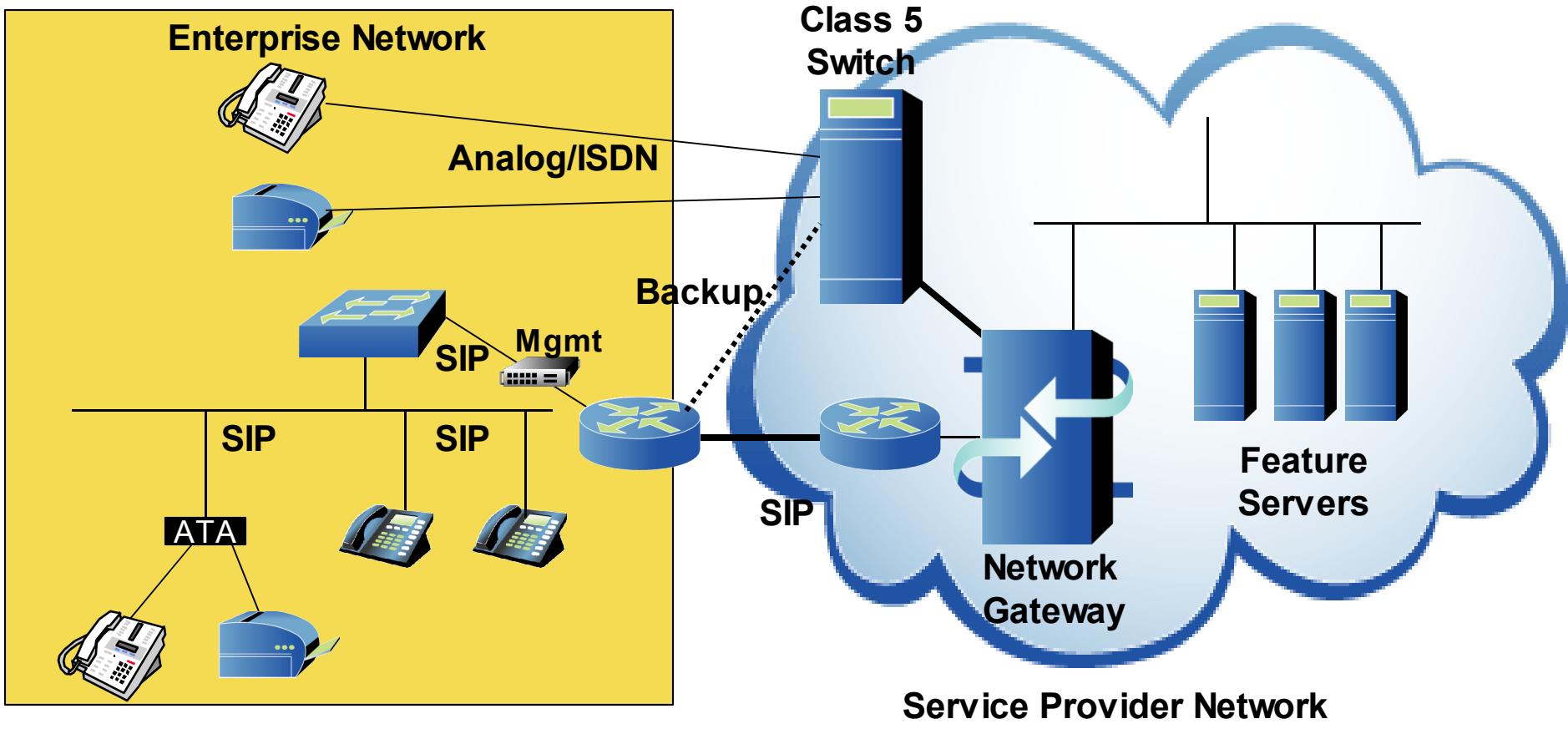
Future Developments

- **Security becoming increasingly important**
  - **Encryption more widely available (Cisco Call Manager 4.0)**
  - **Better availability of VoIP-aware security products**
- **Increasing use of softphones presents new challenges**
- **Remote users also present challenges**
  - **One solution: Zultys builds IPsec client directly into phones**
- **Growing concerns as we evolve past "Islands" of VoIP**

What About Public Services?

- **Public VoIP services are rapidly emerging**
  - **Network complexity transferred to a service provider**

Service Architecture



Service Issues

- **Security**
  - **Risks to corporate data stored on and carried by service providers**
  - **Risks of denial of service attacks on provider infrastructure**
  - **Risks to enterprise data network**
  - **Risks of data carried over the public Internet (for broadband service providers)**
  - **Eavesdropping**
  - **Reliance on service provider for security management**
  - **Are services subject to wiretapping laws?**

Recommendations

Recommendations

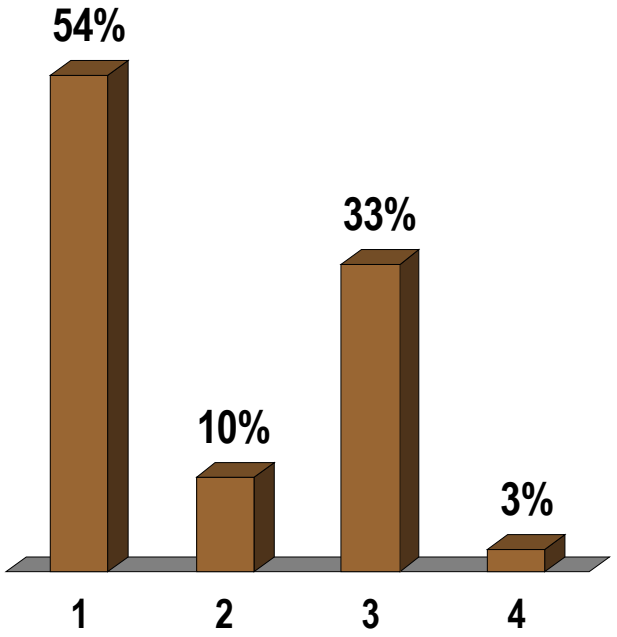
- **Conduct security assessment as part of your VoIP planning**
- **Recommended evaluation criteria:**
  - **Corporate security policies**
  - **Cost vs. Risk**
  - **Network capabilities (to support 802.1Q for example)**
  - **Firewall capabilities**
  - **Need for encryption**

Recommended Security Guidelines

- **Best practices:**
  - **Logical separate of voice and data (use VLANs in the LAN)**
  - **Firewalls/IDS at interconnection points**
  - **Host-based IDS for call control servers**
  - **Authenticate both phone and user**
  - **Implement QoS mechanisms to prioritize voice**
  - **Encrypt where necessary**
- **For users of public services**
  - **Work carefully with providers to understand security methodologies & services**

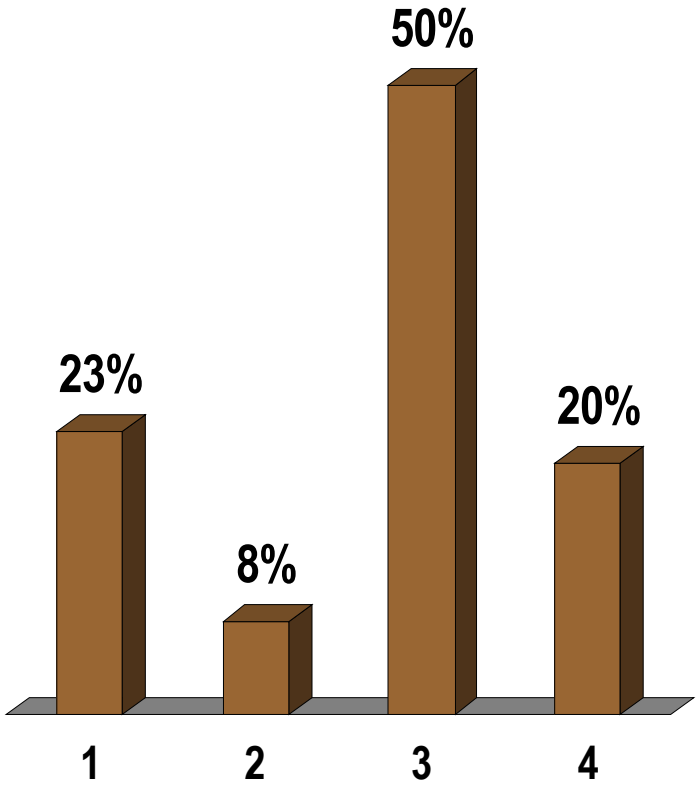
What is your primary area of concern with regard to VoIP security?

- **Hackers disrupting system**
- **Hackers misusing system**
- **Internal misuse?**
- **No concerns?**



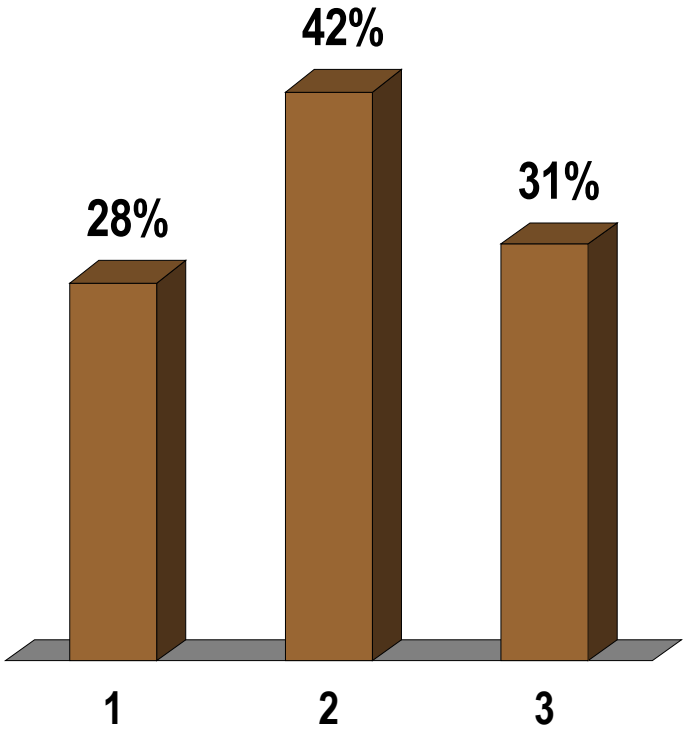
Who is responsible for VoIP security in your organization?

- Internal network security team?
- VoIP management team
- Network management team
- Nobody



Is encryption of voice a requirement?

1. **Yes**
2. **No**
3. **Not sure**



Who manages your VoIP environment?

- Outsourced private solution
- Outsource public solution
- In-sourced
- Not sure?