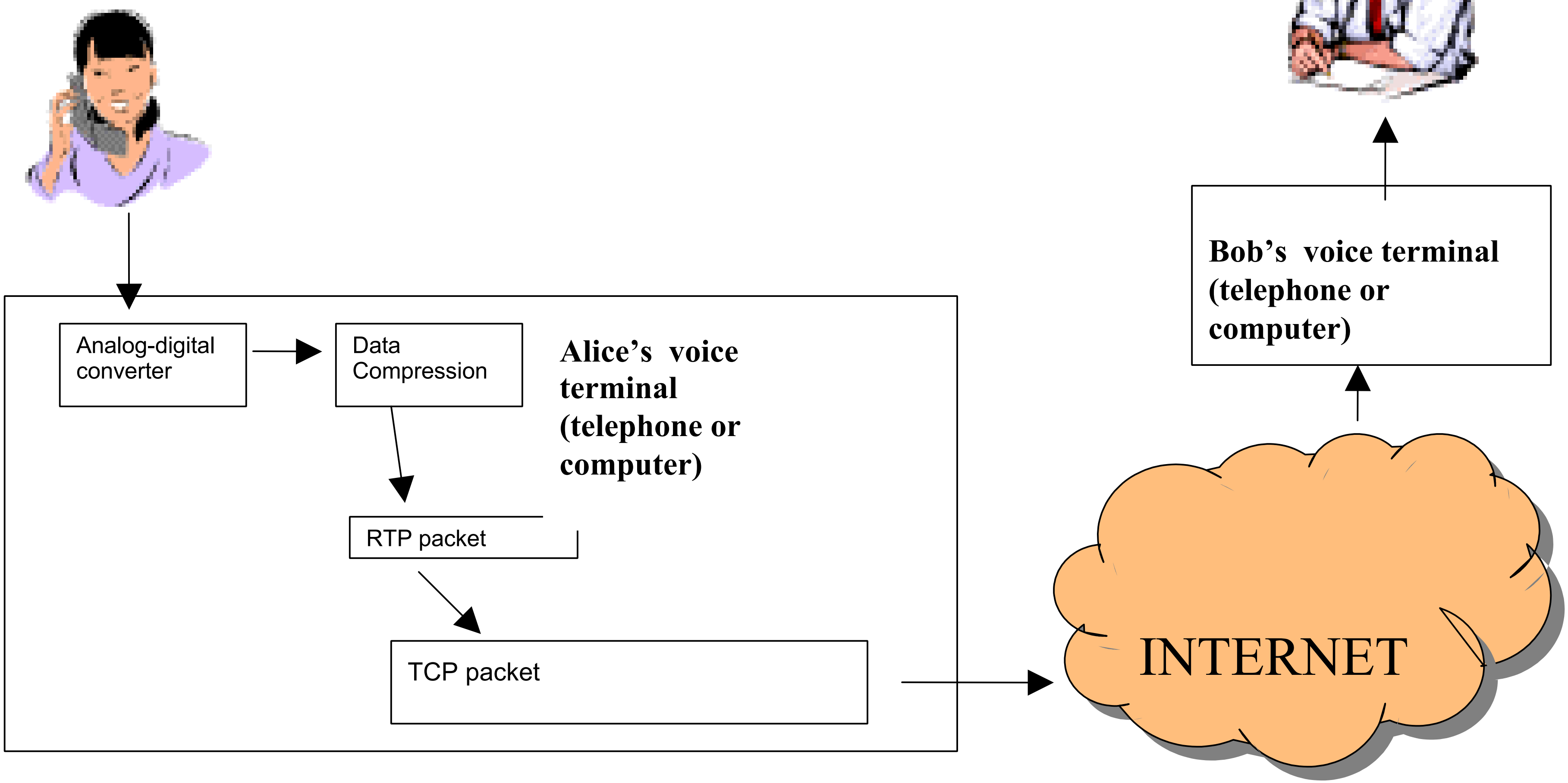
Voice Over Internet Protocol (VOIP) SECURITY

Rick Kuhn
Computer Security Division
National Institute of Standards and Technology

What is VOIP?

- Voice Over Internet Protocol
- Voice Communications over data-style r



Why use VOIP?

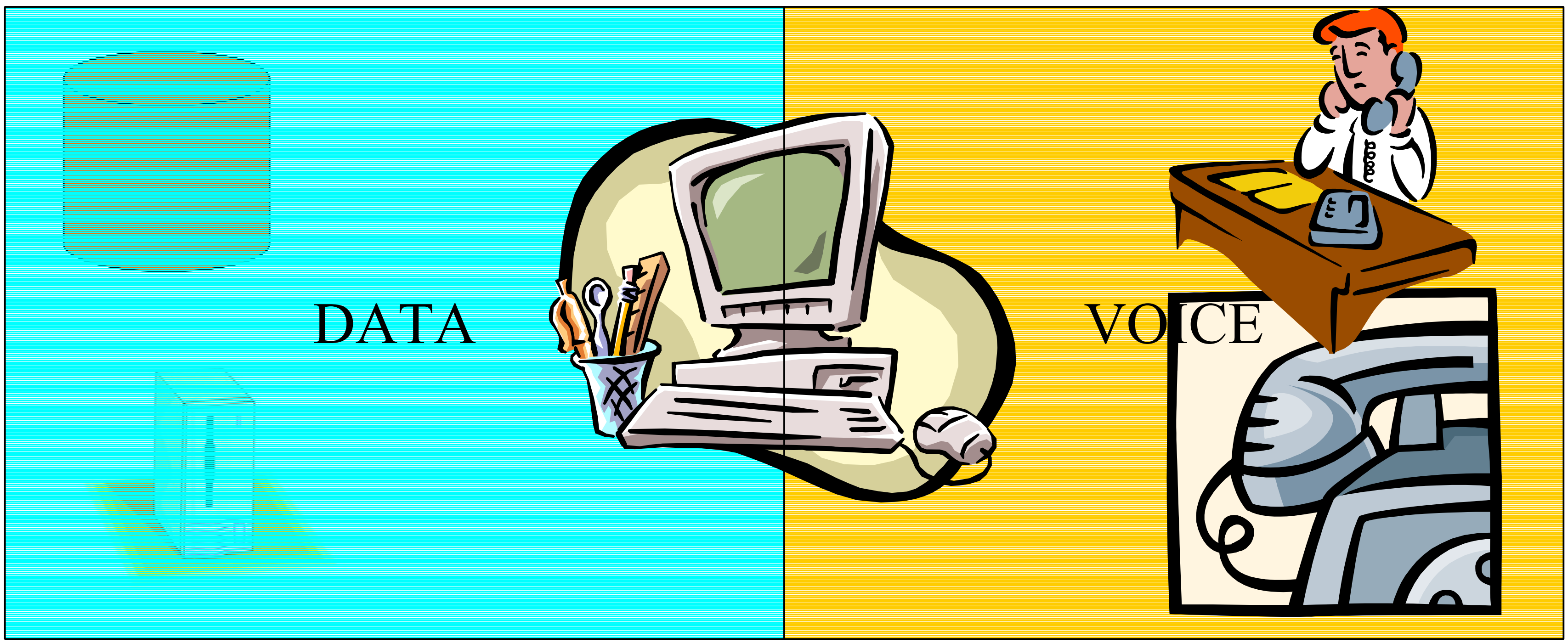
- Simpler Network Design
- More Multimedia Features
  - Full support for video-conferencing and video-phones
- Cost
  - Long distance phone call costs virtually eliminated
  - No need to support a legacy PSTN system

Who is using VOIP?

- Telecommunications companies
- Enterprises with multiple site offices.
- Home workers
- Individuals through software
  - Net2Phone
  - Microsoft’s NetMeeting

Twice the Danger

- A security breach in either the data sector or voice segment compromises the whole network, especially since PC-based phones straddle both services.



Possible Attacks

- Man in the Middle (eavesdropping and altering)
- Denial of Service (DoS)
- Compromise of Gateways
- Compromise of Endpoints
  - Impersonation

QoS and Security

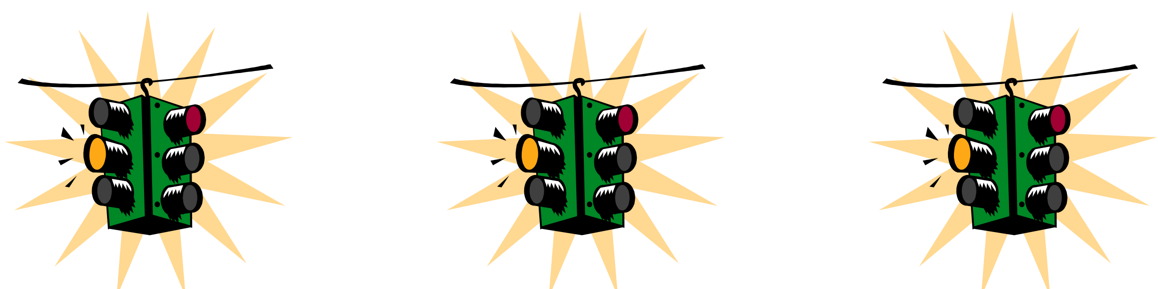
- Quality of Service (QoS) refers to the speed and clarity expected of a VOIP conversation.
- QoS makes attacks easier…
  - No longer necessary to “take down” a network, merely “slow down” the traffic.
- …and defense harder.
  - Implementing proper security measures such as firewalls and encryption introduces latency and jitter.

Latency

- The time from when words are spoken until they are heard at the other end
- Latency greater than 150 milliseconds is unacceptable in most cases

Jitter

- Non-uniform delays
- Requires buffering at the endpoints and application level reordering (more latency)
- Increased jitter makes it harder to tell when a packet is missing or just late.



Packet Loss

- VOIP is highly sensitive to packet loss
  - Loss Rates as low as 1% can garble communications
- Latency and Jitter can contribute to “virtual packet loss” as packets arriving after their deadline are as good as “lost”

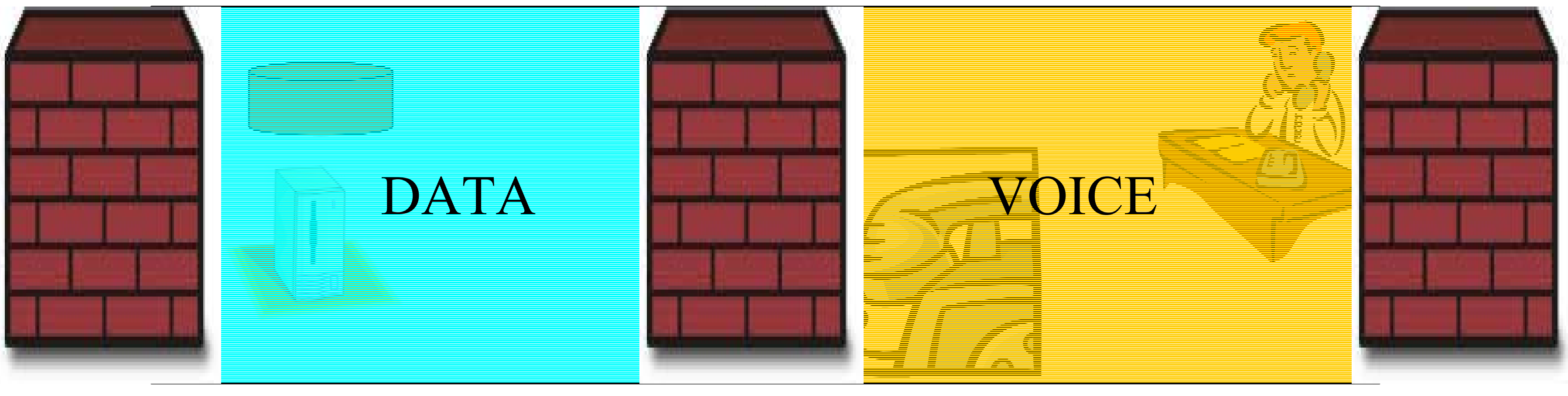
Firewalls, NAT Routers, and Encryption

The Old Stand-By's

- Cannot be Implemented in a VOIP network without special considerations
  - Standard components not built for VOIP's high rate / small packet traffic pattern.
- Degrade Quality of Service (QoS)
  - Latency, Jitter, and Packet Loss
- Obstruct the call setup process
  - Block incoming calls and interfere with the call setup process

Firewalls.

- Firewalls filter out malicious traffic based on a set of rules.
- Firewalls are needed to protect networks from outside attacks.
- Also secure the internal barrier between voice and data networks.



Firewalls and QoS

- Problem: Firewall traffic investigation adds latency to the system and heavy data traffic can introduce jitter.
- Solutions:
  - Implement firewalls with fast CPU's to handle the high rate of packet delivery.
  - Use QoS aware firewalls

IPSec

- Encryption can be used to secure voice data and avoid the firewall problems.
- IPSec is the standard encryption suite for the Internet Protocol and will be fully supported in IPv6.
- In ESP Tunnel Mode, IPSec protects both the data and the identities of the endpoints.

IPSec and QoS

- Problem: Encryption also introduces latency / jitter
  - Encryption/decryption process takes time
  - Crypto-engine schedulers do not implement QoS
- Solutions:
  - Packet compression schemes have experimentally aided performance
  - QoS-aware scheduling before and after encryption heuristically improves performance.

NAT

- Network Address Translation (NAT) is used to allow multiple terminals to share a single IP address
- allows security measures to be consolidated at the NAT router
- hides information about the structure of the internal network

Blocking Incoming Calls

- Problem: NAT and Firewalls can both block incoming calls
- Solutions:
  - Application Level Gateway
  - Firewall Control Proxy

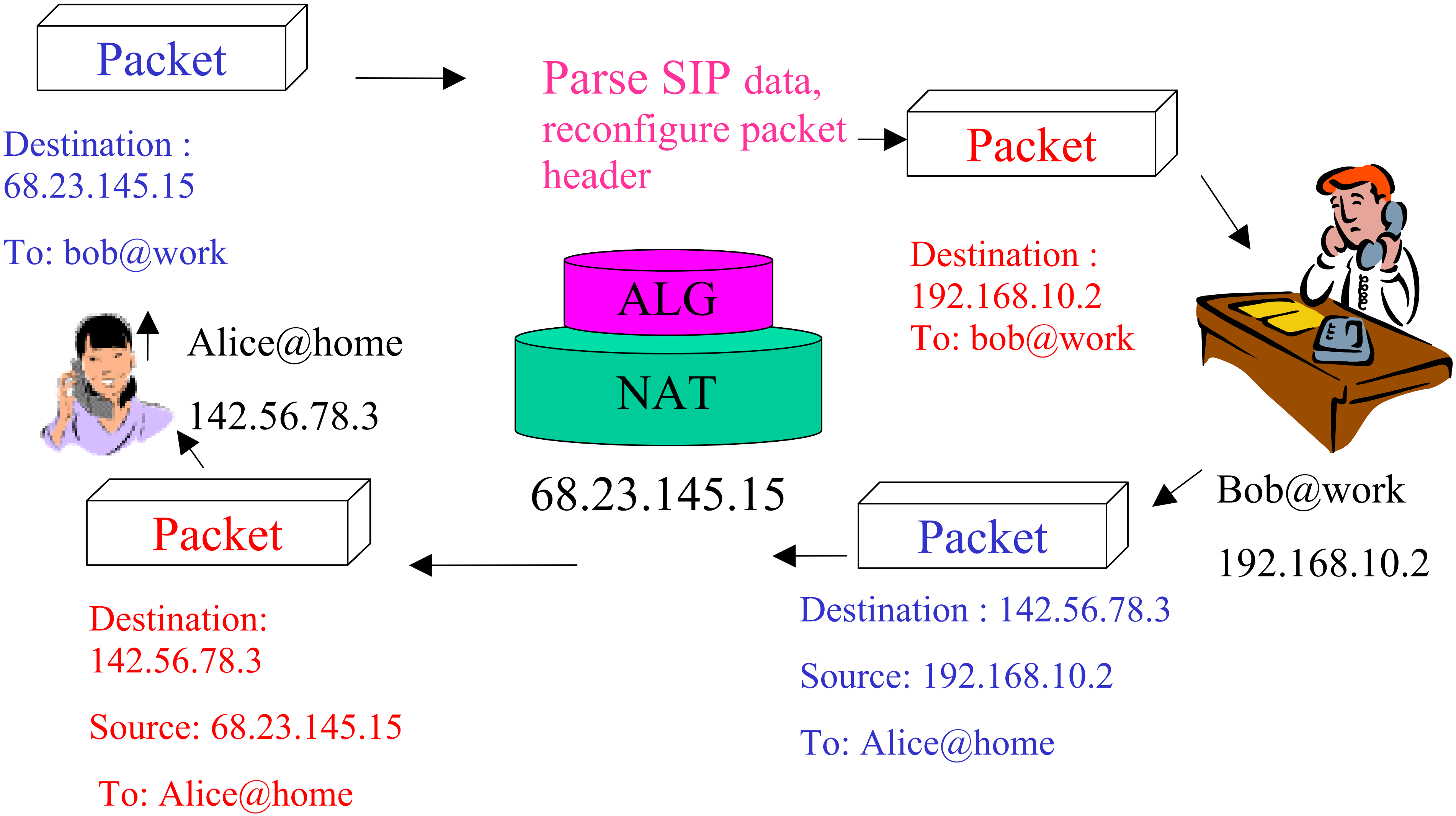
VOIP Call Setup

- Two competing protocols for VOIP call setup: H.323 and SIP.
- H.323 is a suite of several more specific protocols.
  - Uses dynamic ports and binary encoding.
- SIP is a simpler protocol running over 1 port using a three way handshake.
  - Uses a single port and text encoding.

Disrupting Call Setup

- Problem:
  - Firewalls can block the call setup ports and NAT can change the IP address/ports being used internally.
- Solutions:
  - Incorporate an ALG or FCP into the architecture that can manipulate the setup packets' data.

NAT Traversing Example



What Should You Do Now? Network tools

- Separate voice and data traffic using separate address space, virtual LANs (don't need physically separate networks)
  – Reduce risk of data sniffers
  – Can tune IDSs for voice and data separately
- ***Use firewalls designed for VOIP traffic***
- ***At the voice gateway, which interfaces with the PSTN, disallow H.323, SIP, or MGCP connections from the data network***

What Should You Do Now? Protecting voice data

- Avoid PC-based "softphones" if practical
  - Keeps voice and data separate
- Use access control, encryption, where possible
- ***Use IPSec or SSH for all remote management and auditing access***
- ***Do encryption at the router or other gateway, not the individual endpoints***

Summary

- VOIP security requires adapting traditional network security measures for a high speed, dynamic environment.
- For More Info see:

  "Security Considerations for Voice Over IP Systems" - NIST

  http://csrc.nist.gov - see "Drafts"
- "Five tips for securing a converged net"- Computerworld

  http://www.computerworld.com/securitytopics/security/story/0,10801,85844,00.html?SKC=security-85844
- ***Security in SIP Based Networks - Cisco:***

  http://www.cisco.com/warp/public/cc/techno/tyvdve/sip/prodlit/sipsc_wp.pdf
- ***IP Telephony Security in Depth - Cisco:***

  http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safip_wp.htm