Securing VoIP

Phil Swiderski
Security Engineer
Check Point Software Technologies, Inc.

Securing VoIP

- What is VoIP?
- Why VoIP?
- Who's using it?
- SIP, the de facto Standard
- Who should be concerned about Security?
- Why be concerned about Security?
- How to mitigate the risk.
- Questions?

What is VoIP?

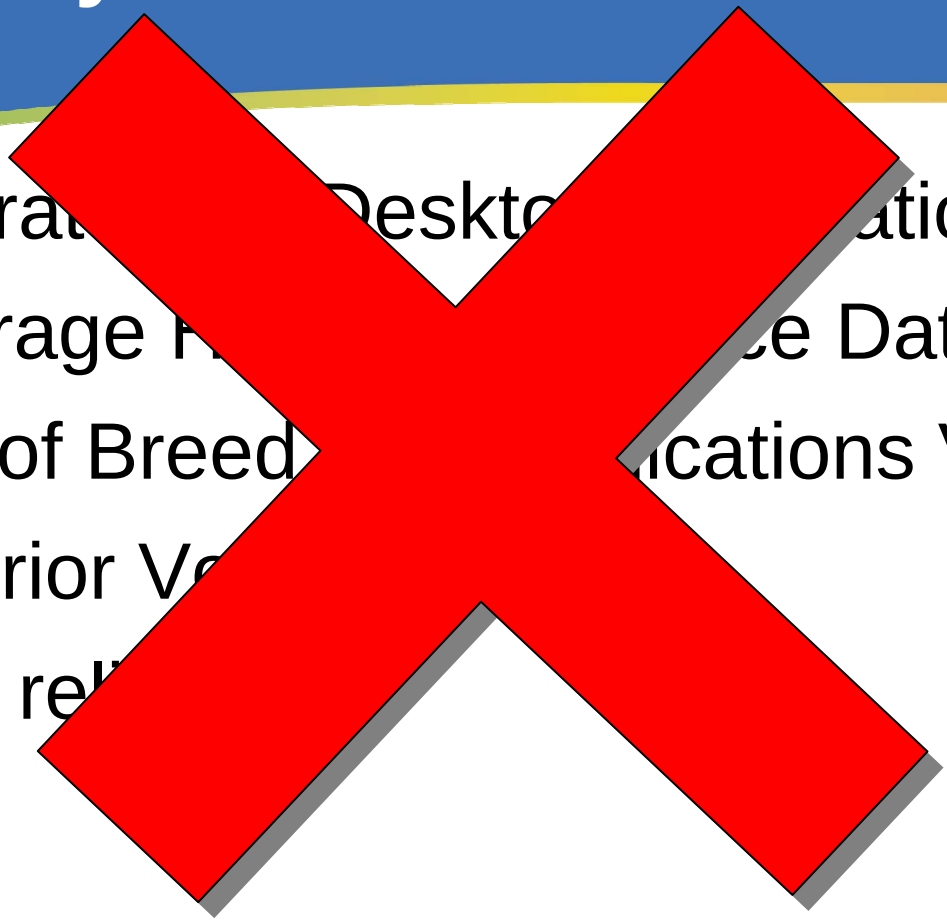
- Voice over Internet Protocol
- Voice over IP is a healthy, growing market.
- Initially used to bypass toll charges.
- Fastest growth is IP Telephony.

Why VoIP?

- Integrate with Desktop Applications
- Leverage High Performance Data Networks
- Best of Breed Communications Vendors
- Superior Voice Quality
- More reliable

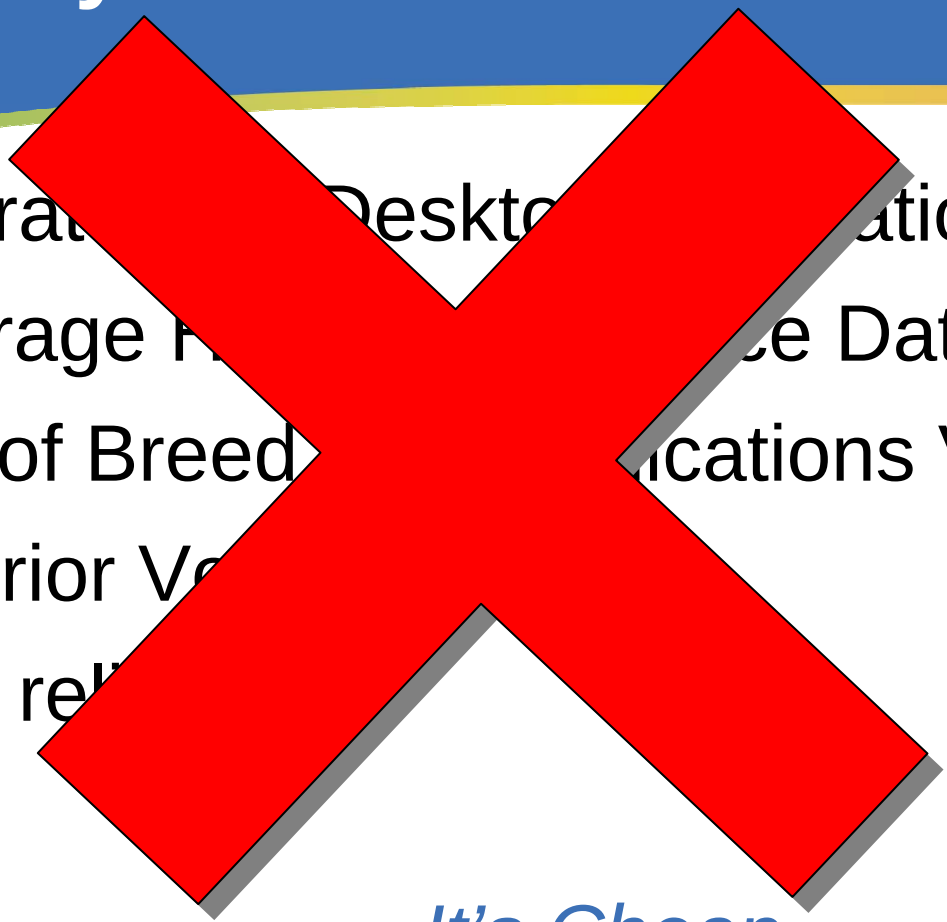
Why VoIP?

- Integrat Deskto ations
- Leverage F ce Data Networks
- Best of Breed ications Vendors
- Superior Vo
- More rel



Why VoIP?

- Integrat… Deskto… …ations
- Leverage F… …ce Data Networks
- Best of Breed … …ications Vendors
- Superior Vo…
- More rel…



It's Cheap

It's Flexible

Who is (or will be) using VoIP?

- An estimated 70 percent of U.S. companies are experimenting with voice over IP (VoIP).
- Companies in the news for their enterprise VoIP implementations include IBM, Dow Chemical, DuPont, and Merrill Lynch.
- IP telephony will be a $15 billion market by 2007, predicts IDC.
- Nineteen percent of all U.S firms, approximately 2.2 million businesses, will be using VoIP in some form by 2007, says market research firm In-Stat/MDR.
- Raymond D. Keneipp, vice president of Networks & Telecom Strategies for the Burton Group said “I think everybody has accepted the fact that we will end up with a converged [voice and data] infrastructure. It’s only a question of are you going to do it sooner or later.” (“Pack up PBX—VoIP is Here,” ZDNet Tech Update, August 12, 2002)

SIP, the de facto Standard

- Quickly replacing H.323 and proprietary protocols
- Already more wide spread
- Lightweight, Versatile, Flexible
- Easy to manage and troubleshoot
- Easy to hack

Who should be concerned about Security?

Everyone

Even if you are not using VoIP or IP Telephony

Why be concerned about VoIP Security?

VoIP is subject to well known network layer attacks

- Denial of Service
- Address Spoofing
- LAND, Ping of Death, Fragmented Packet attacks, etc…

Why be concerned about VoIP Security?

VoIP is subject to known and unknown application layer attacks

- Buffer Overflow and Injection (big problem)
- Trojans, Worms, Malware
- Spam (SPIT)
- Eavesdropping (VOMIT)
- Attack “du jour”

Why be concerned about VoIP Security?

Subject to traditional phone network attacks

(using Application Layer vulnerabilities)

- Call Hijacking
- Phreaking
- Eavesdropping
- Call Spoofing (Phishing)

Security Concerns- Network and Application Layer Attacks

- SIP is relatively untested, likely still susceptible to many attacks.
- DoS could have serious repercussions.
- Susceptible to injection attacks.
- Application layer attacks could be used to disconnect or redirect calls, or even “root” boxes.

Security Concerns- Network and Application Layer Attacks

- Many products use the same SIP Stack.
- Many products still use an underlying OS that is vulnerable to Trojans, Worms and Malware if not patch properly.
- SPIT (SPAM over IP Telephony) need I say more?
- VOMIT (still thinking SPIT is bad?)

Security Concerns- Call Hijacking

- Simply insert a spoofed redirect command (3xy redirect) during the initial call setup.
- Call is then redirected to another address without the callers knowledge.
- Could be used to glean private information using “Social Engineering” techniques.

Security Concerns- Phreaking

Fooled Billing

- Takes advantage of the separate signaling and media paths.
- Send a fake “bye” and “OK” in the signaling path while the media path remains open.
- Continue the call without additional charge.

Billing Evasion

- Find web interface on hardware phone.
- Initiate 3-party calls from web interface.

Security Concerns- Eavesdropping

Tools are freely available

- TCPDump
  - to capture the call for playback later
- Ethereal
  - to capture, analyze and save payload as “.au” file
- rpttools
  - can be used to convert to useable audio format
- VOMIT
  - Voice Over Misconfigured Internet Telephones
  - converts a tcpdump of a VoIP (using SCCP) call into a “.wav” file
  - Can be used to insert a “.wav” file into a conversation (SPIT)

Security Concerns- Call Spoofing (Phishing)

- Tools are freely available
  - Standard PC
  - Asterisk software
  - A IP Phone or Softphone
- Access is easy
  - An Internet Connection
  - A VoIP Service Provider that “supports” spoofing

Security Concerns- Call Spoofing (Phishing)

- Simply configure any ANI or “caller-id” info you want!
  Appear as the victim’s bank, credit card company, company help desk, etc.
- Ask simple “account verifying” questions (zip code, mother’s maiden name, passwords, etc.)
- You’re in! (with good “Social Engineering”)

HELP! What do I do?

- Abstinence.
- Pray.
- Implement security to reduce your risk.

Securing VoIP

- Encrypt.
- Endpoint Protection.
- Restrict usage to specific Domains (whitelist/blacklist).
- Inspect VoIP protocols going in/out.

Securing VoIP- Encrypt

- Stops (or reduce chance of) eavesdropping.
- RTP RFC's define DES as default, but not used (that I'm aware).
- Recommend IPSec, avoid SSL (for performance reasons).
- Use AES (better performance, hard to crack).

Securing VoIP- Endpoint Protection

- Firewall
- Separate VLAN for VoIP.
- Endpoint Security for Softphones.
- SIP Proxy, Gatekeepers, Call Managers, etc… should be in a physically secured space.

Securing VoIP- Restrict usage

- Establish a whitelist of domains to allow calls to/from.
- Use a device/software capable of defining VoIP Domains.
- Firewall should also be able to dynamically open/close RTP/RTCP ports.

Securing VoIP- Inspect

Strict RFC Enforcement.

- Enforce header fields.
- Check for binaries or illegal characters.
- Remove or drop inappropriate characters in address fields.
- Verify the correctness of call parameters.

Securing VoIP- Inspect

Enforce expected use of VoIP protocols.

- Implement header length restrictions.
- Limit “reinvite” messages.
- Drop or remove unknown or unapproved media types (video or IM, for example).

Securing VoIP- Inspect

Maintain & enforce the call and signaling state.

- Enforce proper call flow (set up, tear down, etc).
- Correlates IP Phone registration with users permissions to make/receive calls.
- Correlate signaling state to call state.
- Drop out of state signaling messages.

Securing VoIP

Thank You