



Stealing the Words Straight From Your Mouth

Making Sense of Risk
10th February 2011

Stuart Morgan



News and VoIP Security

- “98% Of Hackers Also Hit Businesses With Dial Through Fraud”
 - Telecommunications UK Fraud Forum - Feb 2010
- “10 million minutes hijacked”
 - The Register – Sep 2010



News and VoIP Security

- “Major VoIP Fraud Gang Dismantled in Romania”
 - Softpedia News – Dec 2010



“It will never happen to me”



Talk Outline

- Introduction to Voice Over IP
- VoIP Security
- VoIP Attacks
- VoIP Defences

What Is It?

- Voice Over Internet Protocol (VoIP)
- Essentially means phone calls over the data network
 - As opposed to the PSTN



Why Be Concerned?

- A significant amount of confidential information gets discussed over the phone!
 - Credentials
 - Quotes
 - Network Infrastructure
- This data would probably get encrypted if it were being sent by email.

Summary of VoIP Attacks

- Call Fraud
 - Increased charges, negative publicity (caller ID spoofing)
- Eavesdropping
 - Confidentiality compromise, integrity compromise
- Denial Of Service
 - Availability compromise

Anatomy Of A Generic VoIP Call

- Control part
 - “Signalling”
 - Establishes connection
- Data part
 - “Media”
 - Transmits the actual voice
- Not just VoIP!

Anatomy Of A Call – Control Part

- SIP
 - Session Initialisation Protocol
- SCCP
 - Skinny Client Control Protocol
 - Cisco – Proprietary
- H.323

Anatomy Of A Call – Data Part

- RTP
 - Real-Time Transport Protocol
 - Usually RTCP (RTP Control Protocol) is used to monitor RTP
- SRTP
 - Secure Real-Time Transport Protocol
 - Uses AES (Rijndael)

Anatomy Of A Call – SIP



How does Beastie find Tux?



Different Implementations



Attacks

- Network Level Attacks
 - Capture raw SIP and RTP
 - SRTP must support the “NULL cipher”
 - Forced Downgrading
- Data Through The Phone?
 - Is it on a dedicated physical network?
 - Does the phone provide access to the data network?
 - Do you have a VoIP phone in reception, or outside?

Attacks

- Man In The Middle
 - Variety of options
 - Configuration Weaknesses (Cisco – TFTP)
 - Fake REGISTER with SIP Registrar, masquerade as someone else
- Unauthorised Voicemail Access
 - Sensitive information in voicemail messages?
 - Password policy? Usually a 4 digit PIN!

Attacks

- ENUM
 - “E.164 Number to URI Mapping”
 - Essentially a distributed phonebook, it converts phone numbers into Internet addresses
 - Uses DNS
- Call restriction circumvention
- Interactive Voice Response (IVR) Logic Flaws



Attacks

- Possible spoofing
 - Incoming calls
 - Outgoing calls
- Denial Of Service
 - Redundancy is good, but is the backup as strong as the primary
- PCI Compliance!
 - Transmission of credit card data

Attacks

- Host Attacks
 - Cisco CallManager on Windows
 - Avaya Call Manager on Linux
 - Management web applications running
- Integration Attacks
 - E-Mail, voice, fax etc all in one place
 - e.g. Cisco Unified Messaging, Avaya Unified Messaging

Defences

- Security Testing
 - Provides security assurance
 - Must have a dedicated VoIP component
 - Required for compliance

Defences

- Encryption
 - SRTP / ZRTP
 - Offers some confidentiality
 - Does not protect against most attacks
 - Beware of a false sense of security

Defences

- Intrusion Detection Systems
 - Catch some, but not all attacks
 - Not a replacement for securing your system

Conclusion

- Potentially significant risks with VoIP
- Controls may not work how you think
- VoIP systems need reviewing and testing



Questions?