Don't Just Talk
Discussions on Securing Voice-over-IP

William Emmanuel S. YU
Ateneo de Manila / Novare Technologies
Philippine Open Source Conference 2006
Agenda

- Why Bother?
- Introduction
  - Flash update on How VoIP Works?
  - Why secure VoIP? Is there a need?
- Media Path Security
  - IPSEC/VPN, SRTP
- Signaling Path
  - MIKEY, SIP on TCP with TLS, IAX
- Opportunistic Security

Copyright 2006 William E. S. Yu
Why Bother?

- VoIP Deregulated in Philippines – June 2006
- 1 Billion Internet Users in the World (16% of the World) (http://internetworldstats.com/)
  
  - VoIP will account for 75% of the world's voice traffic by 2007 (Frost and Sullivan 2001)
  
  - The Philippine Call Center industry is carrying at least 3 billion minutes a month in 2005! (DTI)
  
  - ... 6,000 vulnerabilities report in 2005 alone (http://cert.org/)
Introduction
Review: How VoIP Works?
Review: How VoIP Works?

- **Signaling Path**
  - Information regarding call setup and take down
  - SS7, CAS – used in traditional PSTN networks
  - SIP, H.323, MGCP – used in VoIP networks

- **Media Path**
  - Actual content of call
  - Analog Signal - used in traditional PSTN networks
  - RTP – used in VoIP networks

- May or may not pass through the same path!
VoIP Security Problems

- **Eaves Dropping**
  - Listen into an existing conversation
  - **Legal Intercept.** Can also be used for legitimate purposes

- **Call Hijacking**
  - Intercept a call and gain control
  - Locks other out of conversation

- **Man-in-the-Middle** Attacks
  - Sit in the middle and pass messages back and forth
  - Both parties assume call is un-compromised
Why Secure VoIP?

- Current state of **VoIP security** is no different from current state of ordinary **PSTN security**
- Security is the **responsibility of the handsets and end users**

- Different security needs:
  - **Signaling Path-only Security**
  - **Media Path-only Security**
  - **End-to-end security**
The Media Path
Media Path Intercept

- Similar to PSTN intercepts
  - Tap into the media channel
  - Wiretapping either at the exchange or last mile
  - Trunks are normally harder to tap (but possible)

- VoIP intercepts
  - Decode signaling packet
  - Determine media path details (port, codec, etc ...)
  - Intercept RTP packets and decode!
  - Even without signaling intercept, decode all intercepted RTP packets (Echelon Mode)
Security Outside VoIP

Use IPSEC/VPN technologies
Secure RTP

- Documented in RFC 3711
- Aims to secure the RTP media channel
  - Confidentiality, Authentication, Replay Protection
  - Flexibility to use multiple algorithms and selective protection (encryption or authentication or both)
- Does not answer how keys are exchanged
- An Open Source reference implementation is made available by CISCO systems
  - http://srtp.sourceforge.net/srtp/
Secure RTP
Problems with SRTP

- SRTP needs a way to send information for establishing a **security context**
  - Cryptographic Keys, Cipher Details and others
  - Key Exchange
  - Normally sent in **signaling channel**
  - If not secured SRTP is useless
- Not defined by **RFC 3711**
Problems with SRTP
The Signaling Path
Secure the Signaling
Ways to Secure

- Ensure that **signaling details** do not fall into the wrong hands
- Secure entire IP Path
  - **IPSEC** and **VPN**
  - Costly on both bandwidth and CPU!
  - IAX2 Security (not quite entire IP path)
- **Secure Signaling Path** Only
  - Special Messages in H.323/SIP messages
  - SIP INFO with SIP over TLS (non-standard)
  - SDES with SIP over TLS, MIKEY
IAX2

- **Inter-Asterisk Exchange (IAX)**
- Still an **Internet Draft**
- Currently at **Version 2** and used by the popular open source SoftPBX software, **Asterisk**

**Key Features**
- Both **signaling** and **media path** are merged into a single UDP stream
- Known for being **NAT friendly**
- Uses **challenge response** for authentication
- Can use **AES** encryption
SDES w/ SIP over TLS

- Session Description Protocol Security Descriptions for Media Streams (SDES) is defined by RFC 4568
  - Used to perform key exchange necessary for SRTP
  - Information included in SIP session
  - Channel is assumed to be secure
- SIP over TLS
  - Transaction Layer Security (TLS) is used to secure TCP SIP transactions (SIP typically uses UDP)
Multimedia Internet Keying (MIKEY)

Defined by RFC 3830

Can be used in three (3) modes:

- **Pre-shared Key Mode.** Keys are transmitted with methods outside the system. Such as fax or verbally.
- **Public Key Mode.** Uses a PKI system. However, key distribution will still be an issue.
- **Diffie-Helman Mode.** Similar to the PK Mode but uses DH for initial ephemeral key transmission.
Anything Else?
Still debatable if necessary
- Why bother? Isn't node-to-node encryption enough?
- We trust our providers!
- How about legal intercept?

Lots of problems
- Many different and incompatible systems
- Not too many standards yet
- Costly (bandwidth and processing)
End-to-End Security

- Can use **SRTP** between clients
  - Must have client support
  - Current support by a number of phones such as those by **Linksys/Sipura**
- **Key exchange** must be standardized
  - Which method? SIP INFO? SDES? MIKEY?
  - Which type? Shared Key? PK? DH?
  - For SIP INFO and DES, should TLS be used?
- Why not just encrypt everything with **IPSEC** or another form of **VPN**?
Opportunistic Encryption

- Why even bother with authentication?
- Guaranteeing confidentiality of connection might be enough
  - Isn't the voice of the other end enough?
  - Other methods to identify called and calling party
  - Saves on resources (CPU and bandwidth)
- Use opportunistic encryption
  - ZRTP
  - SRTP and MIKEY in Opportunistic DH mode
ZRTP

- Created by Phil Zimmerman (inventor of the world famous Pretty Good Privacy - PGP) and company
- No need for server side manipulation
- Just install the software in the client PC and use VoIP software of choice
- Uses SRTP to encrypt RTP
- Reference implementation called zfone
SRTP + Opportunistic MIKEY

- Uses regular SRTP to encrypt RTP
- Opportunistic MIKEY
  - Still uses Diffie-Helman Key Exchange
  - Used HMAC for “automated” mutual authentication
  - No need for fixed keys
  - Not yet ratified by the IETF
- Can now work in Opportunistic Mode
- Can be used like ZRTP
- Still an Internet Draft
Wrapping Up
Conclusion

- There is a need for **VoIP Security**!
- Unfortunately, market is **still fragmented**
  - Different vendors have different implementations
- Define **Areas of Need**
  - Authentication, Encryption or Both
  - Partial or End-to-End or IP-based
  - Opportunistic or Deterministic
  - More means sacrificing **bandwidth** and **CPU** time
- Or just leave it up to the **provider**!
- ... and Just Keep on Talking!
Thank You!

For additional information check out:

- Really good reference on All Things VoIP (http://voip-info.org)
- Asterisk Open Source SoftPBX (http://asterisk.org/)
- Academics (http://cng.ateneo.edu/cng/wyu/)
- Personal Blog (http://hip2b2.yutivo.org/)
- VoIP Stuff (http://www.microwavehouse.com.ph/)
- Zfone (http://www.philzimmermann.com/EN/zfone/)