

# SIP Security & the Future of VoIP

Nate Klingenstein  
QUESTnet 2009  
July, 2009



## Securing SIP

- The threats
- The existing protocol's problems
- Attempted solutions
- Skype for comparison
- Next steps



# The Threat Model

- A lot like any other network application's problems
  - Denial-of-Service (DoS) attacks
  - Eavesdropping / Man in the Middle
  - Spoofing, replay, spam (SPIT)
  - Poor authentication, authorization
- Demonstrated attacks

INTERN

ARE THESE THREATS

## hypothetical?

- Security must always be pragmatic and proportional
- <http://www.loria.fr/~nassar/readme.html>
- <http://www.voipsa.org/Resources/tools.php>
- Human faces and voice recognition do provide limited authentication & protection

INTERN

# Enterprise Middleware

- Many universities and companies manage information about their members
- Directories, databases
- Applications use these data for better security, auditing, user services
- Large benefits for enterprise webapps

INTERN

## Specific Problems

- Authentication: HTTP digest, basic
  - Realm-specific
- Traffic unencrypted
- Trust between realms and proxies poor
- Disconnected from identity management infrastructure

INTERN

# Possible Solutions

- Look a lot like the solutions for other old protocols:
  - Hack security into an old protocol
  - Firewall everything
  - Accept that SIP is too difficult to secure

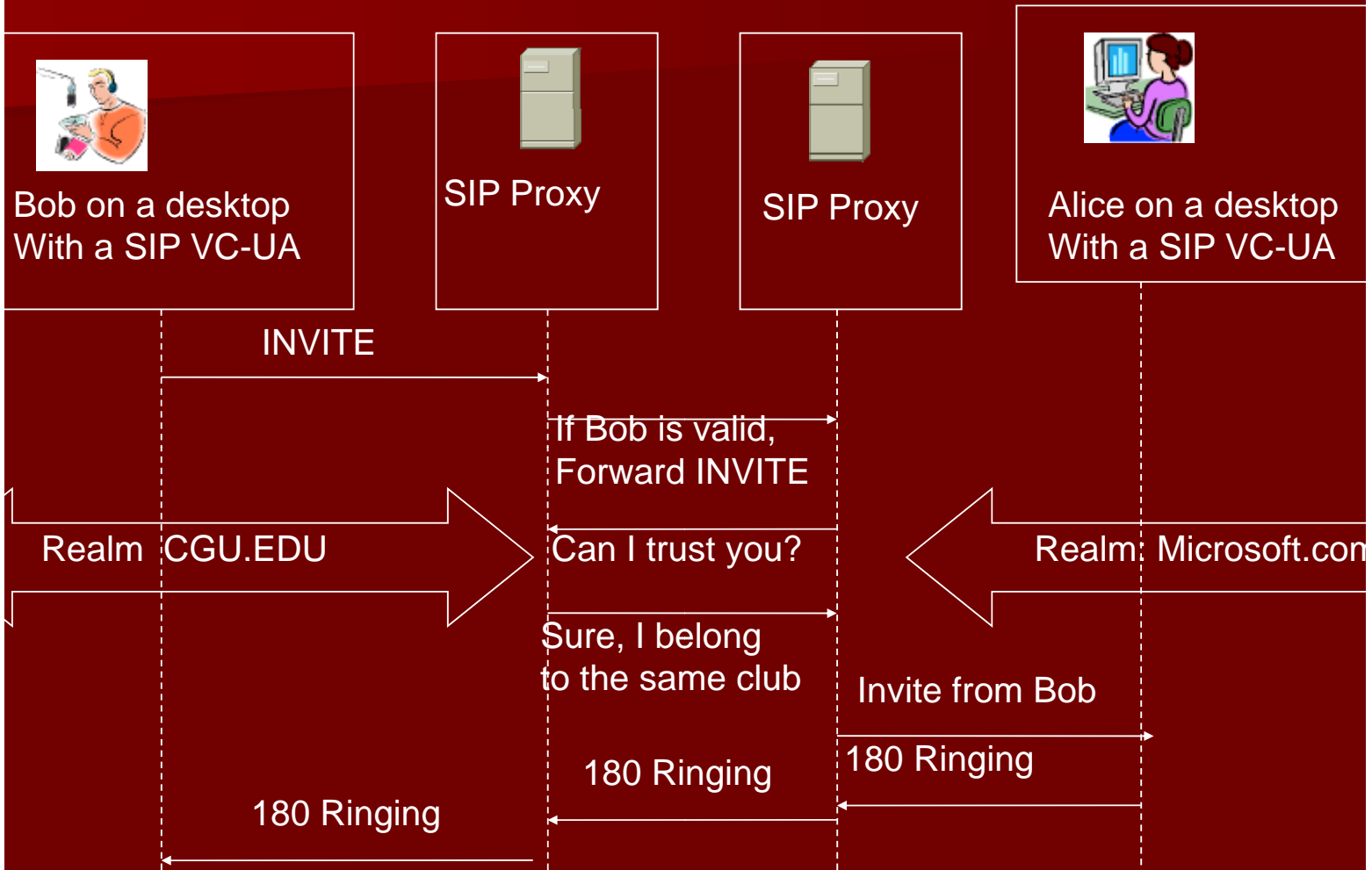
INTERNET

# Security Attempts

- Many tries with varying success
  - New RFC's, internet-drafts
  - Integration with RADIUS, TLS authentication
  - Integration with directories
  - Improved deployment practices

INTERNET

# Inter-Realm SIP



# SAML + SIP

- Attempt to fix three major problems
  - Authentication methods
  - Realm trust
  - Connection to infrastructure
- internet-drafts were written to make a SAML MIME on the invite, but failed

# Firewall Everything

- Private networks
- VPN
- IDS/IPS
- TLS/IPSec
- Dedicated hardware devices
- STUN & TURN

INTERNET

ISSUES WITH FIREWALL

## Everything

- Cross-realm trust not addressed
- Possibly multiple interfaces and/or devices with private network
- One more step towards Internet quarantine...

INTERNET

# Securing SIP

- A combination of approaches is necessary
  - Network-level protection
  - Federated trust
  - Middleware integration
- Phones and other hardware make modification more difficult



TASK FORCE

## Survey

Which VoIP Security mechanisms do[n't] you use?

IPS between VoIP network and data IP network.

IDS between VoIP network and data IP network.

NAC (network access control) such as 802.1X and RADIUS to authenticate hardware.

Phones require the use of the separate VoIP network (physical LAN, VLAN, subnets, etc.) from the data IP network.

Phones are allowed with IPSEC transport mode.

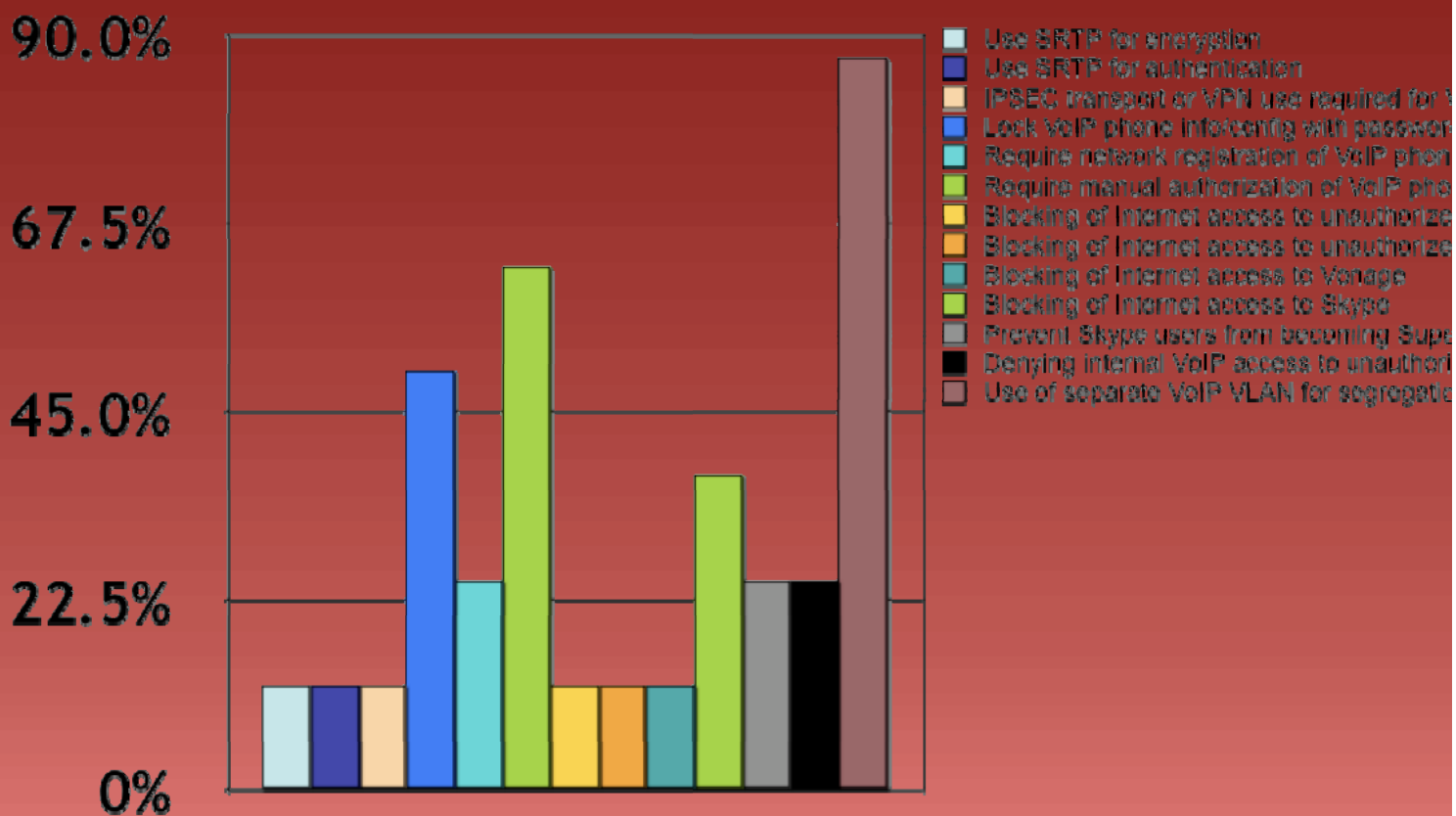
Phones are allowed with IPSEC VPNs.

NAC (network access control) such as 802.1X and RADIUS to authenticate hardware.

Allow NAT traversal via STUN or TURN Internet proxies.

Provide separate dedicated bandwidth for VoIP traffic to the Internet.

## Which VoIP Security mechanisms do you use?



# The Skype Model

- Proprietary, decentralized protocol
- RC4 encryption
- Firewall and NAT detection, agility
- Central login server, hashed
- SIP used by SkypeOut/SkypeIn with PSTN interconnections; gateways to SIP phones

# Skype?

- TLS/IPSec offer good encryption
  - Authentication over TLS (digest/PKI/SAML) is good
- Bandwidth, centralization not big problems
- The world has no central login server
  - Cross-domain trust not solved

INTERN

## Conclusions

- SIP needs a lot of attention to be secure
- Existing ideas can address some shortcomings
  - Some efforts stopped
  - No central work combining all efforts
  - Some attacks don't have cost-effective solutions

INTERN

# Questions?

- <http://www.internet2.edu/sip.edu/>
- [ndk@internet2.edu](mailto:ndk@internet2.edu)