LEARN – VERIFY – PROTECT

Pure Security for VoIP › mobile › multimedia

Gaurav Saha

The Sipera Approach

- Learn

  ✓ Sipera VIPER™ lab concentrates all its efforts on Vulnerability Research to *learn* about different kinds of unique threats in SIP/IMS/UMA networks and UA

- Verify

  ✓ Sipera LAVA™ tool emulate thousands of attacks to *verify* above threats.

- Protect

  ✓ Sipera IPCS™ products combines VPN, Firewall, IPS etc functionality for VoIP systems in a single device to *protect* and enable unified communications.

Talk Outline

1. VoIP Overview
2. VoIP protocols
3. SIP Protocol Analysis
4. Weaknesses in VoIP Protocols
5. Attack Vectors
6. Conclusion
7. Demo

VoIP Overview

- What is VoIP?
  - ✓ VoIP is an IP telephony service which converts analog data signals into digital signals and carries it over internet.
- Why VoIP?
  - ✓ Cost Effective
  - ✓ Flexible and Easy implementation
  - ✓ Advance Services

VoIP Protocols

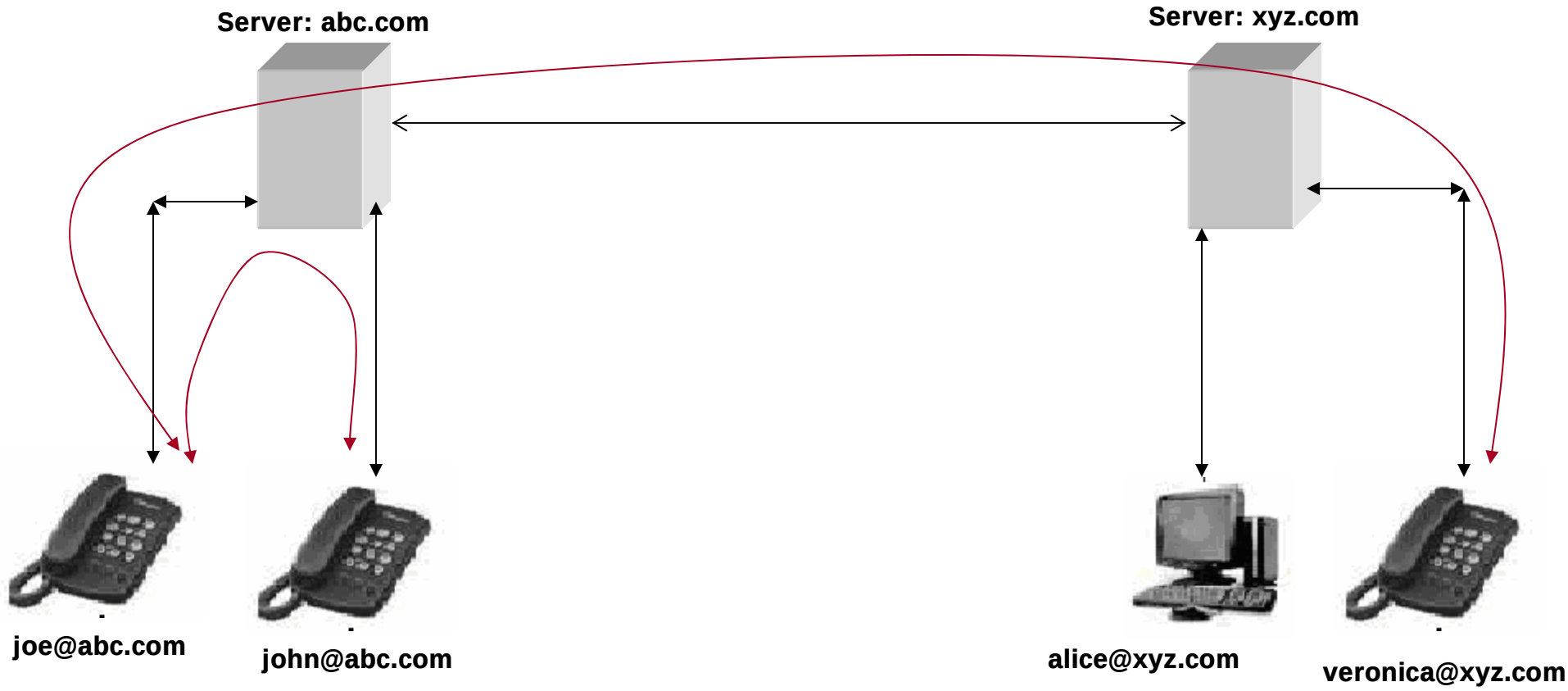
- H.323
- Session Initiation Protocol (SIP)
- Skinny Client Control Protocol (SCCP)
- Media Gateway Control Protocol (MGCP)

SIP Protocol Overview

- SIP stands for Session Initiation Protocol
  - ✓ SIP is signaling protocol
  - ✓ Plain-Text like HTTP
  - ✓ Supports encryption like HTTPS
  - ✓ Supports TLS
  - ✓ Supports encryption of VoIP Media Data

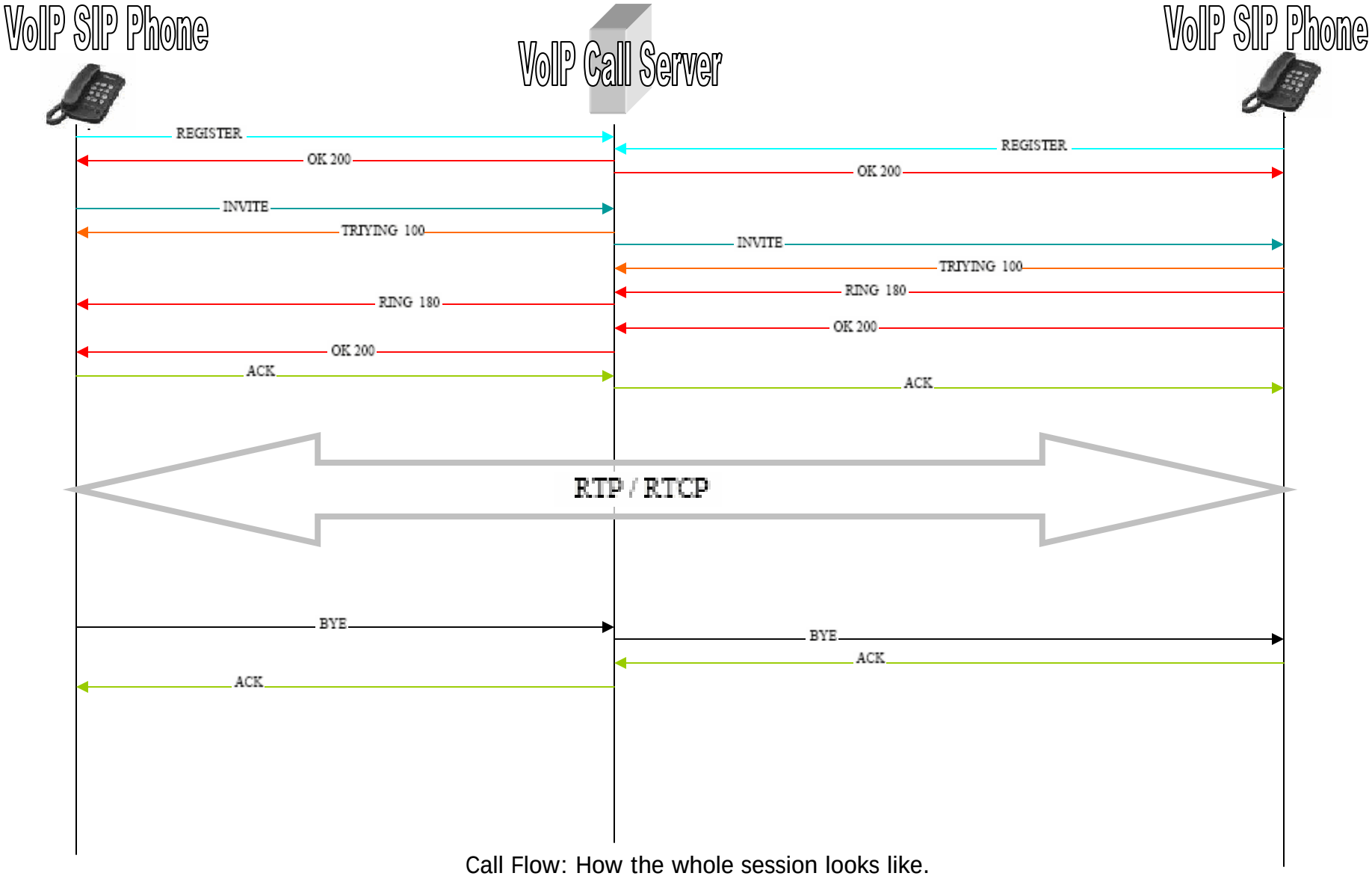
- SIP Components
  - ✓ User Agent Client (UAC)
  - ✓ User Agent Server (UAS)

SIP Architecture



How call are made between to VoIP Phones

SIP Call Flow



Call Flow: How the whole session looks like.

Weaknesses and Vulnerabilities in SIP

- UAS/UAC identity disclosure
- Username/Password cracking
- Eavesdropping
- Data Mangling
- SIP call Setup, Routing and Termination

Attack Vectors

- UAS/UAC identity disclosure
  - ✓ Similar to Banner Grabbing.
  - ✓ Users Enumeration

- Username/Password cracking
  - ✓ Call/Toll Fraud
  - ✓ Spamming

Attack Vectors

- Eavesdropping
  - ✓ Spying
  - ✓ Mass Password Discovery
- Data Mangling
  - ✓ Phishing
  - ✓ Spam Over Internet Telephony
  - ✓ QoS Degradation

Attack Vectors

- SIP call Setup, Routing and Termination
  - ✓ Fake REGISTER and INVITE
  - ✓ Active Eavesdropping
  - ✓ Fake REGISTER, BYE and CANCEL
- Denial of Service Attack (DoS)
  - ✓ Flooding (INVITE, REGISTER, SUBSCRIBE, BYE … et al)
  - ✓ Stealth DoS
  - ✓ Call Jamming
  - ✓ Distributed DoS (DDoS)

DEMONSTRATION

Witness your desk phone getting 0w|\|3d !!

Thank You ☺