

Unified Communications Security: Latest News, Current Outlook

Attacks against VoIP and UC accelerated in 2010

- 50% increase in attacks from 2009 to 2010 from hackers targeting enterprise UC servers (source: VIPER Lab honeypots)
- Now up to 25% of all hacking attacks in the wild (open Internet) are against the voice and UC vector, up from single digits in previous years (rest of attacks are classic database and network layer attacks)
- As email, web application and classic network hacking vectors are closed, VoIP and UC are the new targets.
- An attack against VoIP takes place every 2.5 minutes during peak periods (source: VIPER Lab)
- More than 20,000 exploits and threats against VoIP and UC are now identified

Toll fraud, services theft

- More than 2,200 enterprises in US compromised by a single team of hackers in voice toll fraud attacks that stole \$55 million (source: US Federal Bureau of Investigation)
- Romanian hacking ring hit businesses with VoIP attacks stealing 11 million Euros (source: European Law Enforcement authorities)
- Thousands of examples of enterprises compromised because inadequate SIP trunk, VoIP server protection (sources: multiple, including Network World magazine, Unified Communications magazine, Comms Business Magazine, FierceVoIP, others)
- "Call walking" reconnaissance attacks, scanning attacks make up majority of VoIP attacks against enterprises, precursor to toll fraud

Worldwide Telecom Fraud Increased to \$80 Billion Annually

FRAUDSTERS

Feds bust \$55 million international hacking ring

98% OF HACKERS ALSO HIT BUSINESSES WITH DIAL THROUGH FRAUD

VoIP hackers run up \$120,000 phone bill at Perth business

Bell Canada customer billed \$207,000 after hacker breach

Cybercrime costs firms \$1 trillion globally

McAfee study says

Identity Theft Reported By 33% Of Healthcare Organizations

11 MILLION EURO LOSS IN VOIP FRAUD

PHREAKERS

THREATEN CASH STRAITS



Identity theft

- Vishing attacks utilizing VoIP against consumers, often blended with email phishing attacks
- Widespread alerts throughout 2009 and 2010 from law enforcement; organized Vishing attacks against bank customers (sources: local media, state law enforcement authorities across US)

Corporate espionage

- Vulnerable UC systems in Fortune 500 enterprises encountered multiple confirmed cases of corporate espionage: eavesdropping, UC interception, including VoIP and video
- Dozens of freely available, automated hacking tools now widespread: man-in-the-middle, voice and video jacking, VLAN hopping

VoIP quality problems

- Scanning, reconnaissance attacks, flooding, DoS are all major causes of VoIP call quality problems such as jitter and dropped calls occur daily in enterprises around the world

Compliance challenges

- Moving to VoIP, UC enables many more applications to carry data that must be kept private by law or industry requirements: payment cards, healthcare data, consumer data, student data, proprietary data
- Enterprises must encrypt communications to maintain privacy but this creates major monitoring, archiving and logging challenges (for records retention)

Security evolves

- Security concerns were #1 issue blocking VoIP and UC adoption; security requirements now defined and understood
- Proactive UC security cuts UC deployment time by an average 6 months, or about 33 percent (source: Aberdeen Group data)
- Unified Communications Proxy devices now being deployed, just as email and web proxies protected those systems a decade ago
- Privacy, Policy Enforcement, Access Control, Threat Mitigation now standard UC security components
- Siperas UC-Sec appliance is a UC proxy providing comprehensive application-layer security for UC in one, plug-and-play appliance
 - o Complements existing UC and security architecture
 - o Secures all UC to any supporting device over any network
 - o Ensures safe SIP trunks utilization without added toll fraud risk
 - o Solves compliance problems by permitting clear monitoring and archiving of encrypted traffic

Learn more at

 www.sipera.com

UNIFIED COMMUNICATIONS UNLEASHED

About Siperas Systems

Sipera Systems, the leader in real-time Unified Communications (UC) security solutions, is the choice of enterprises and service providers around the world to support their mission-critical UC deployments.

Sipera offers groundbreaking solutions that secure voice, video, messaging, collaboration, and other real-time communications in converged IP networks, boosting compliance with information security requirements and simplifying the adoption of UC. Siperas innovative *Borderless UC™* architecture delivers secure and private enterprise-class communications to any device over any network in any location.

Backed by the industry-leading research of the VIPER Lab, Siperas award-winning UC-Sec appliance provides comprehensive threat protection, policy enforcement, access control, and encryption in a single, flexible, plug-and-play device. The UC-Sec is pre-integrated with all market-leading UC vendor solutions and is the world's first UC security device to be Common Criteria certified, meeting the stringent international standard for IT security.



 www.sipera.com

 [www.twitter.com/siperasystems](https://twitter.com/siperasystems)

Sipera Systems

1900 Firman Drive, Suite 600
Richardson, TX
75081, USA

T: +1 214 206 3210

F: +1 214 206 3215

E: info@sipera.com