

The Security Challenge: Combating VoIP & UC Fraud

- Assess your security posture against toll fraud, premium-service fraud and related exploits
- Detect and mitigate VoIP/UC-specific threats and vulnerabilities
- Protect VoIP servers, PSTN connectivity, device authentication, and other targets

A small chain of “Mom & Pop” retail shops gets a phone bill for \$500,000, an amount 400 times its typical monthly bill.

A service provider receives interconnection charges totalling more than \$1 million for termination of long-distance phone calls from one of its partners, but there are no corresponding revenues to match these calls.

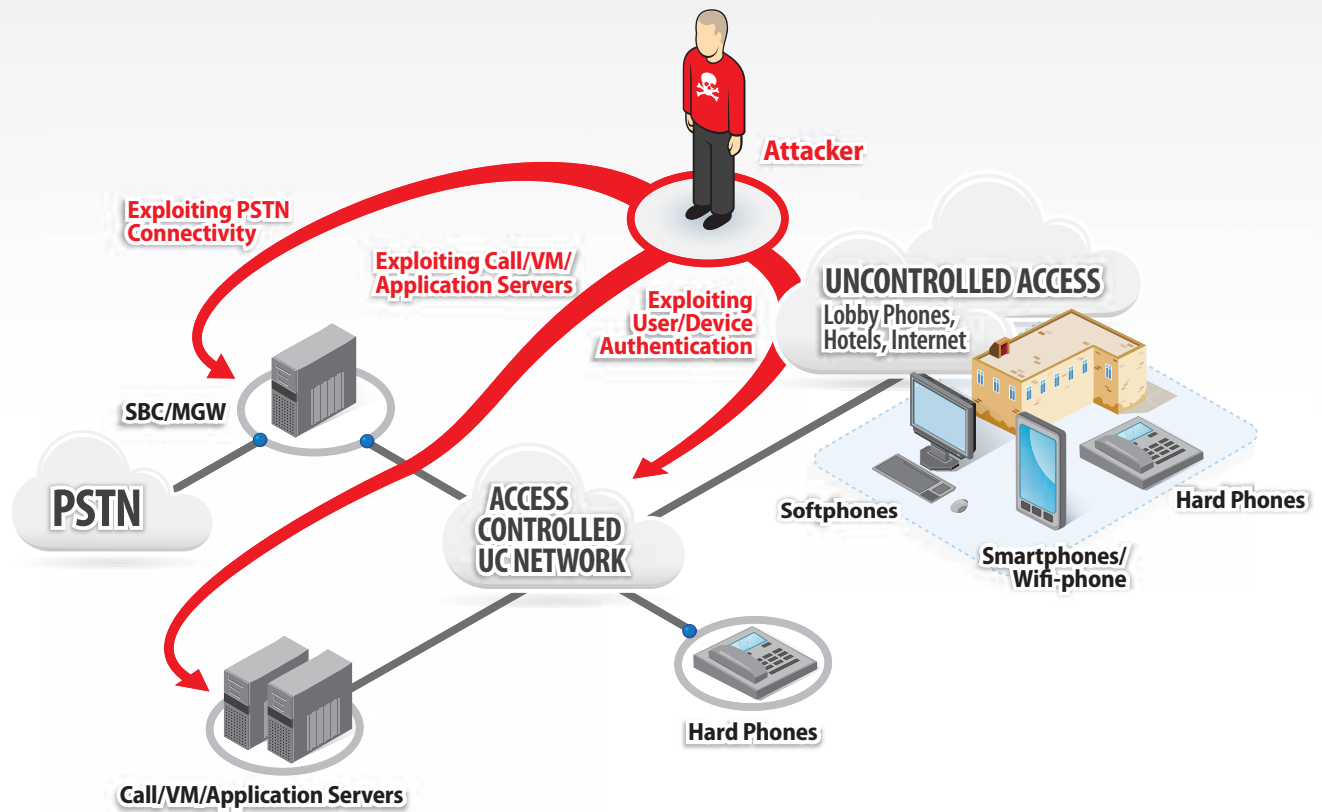
The telecom manager for a multinational enterprise discovers a spike in international calling volume and charges, but many of the calls take place during non-business hours when no one is working. Worse, the volume of calls during business hours is starting to exhaust the network capacity.

What’s going on?

Each of these scenarios illustrates how Voice-over-IP (VoIP) and Unified Communications (UC) implementations, if not deployed with adequate security, can result in toll fraud or premium-rate service fraud. Toll fraud, or long-distance fraud, is the unauthorized usage of paid long-distance communications services (such as international calling) charged to an unsuspecting entity – whether an enterprise or service provider. Closely related is premium-rate or premium-service fraud, in which a compromised phone server or services is exploited to access special services numbers that carry a per minute or per call charge. Beyond the unauthorized charges stemming from these forms of fraud, the misuse of communications services can also eat up network resources, leaving them unavailable to legitimate users.

Since 2007, the frequency and incidence of communications fraud has skyrocketed, and this issue represents one of the most pressing VoIP and UC security matters facing the industry today. Consider these facts:

- Toll fraud and attacks against VoIP and UC servers represent as much as a quarter of all attacks in the wild, according to findings from Sipera’s VIPER Lab™ research arm.
- Toll fraud and premium-rate service attacks are easy for fraudsters to initiate, exploit and monetize, because the minutes stolen are resold through various means to unsuspecting end users, according to the United States Federal Bureau of Investigation.



- Independent VoIP security researchers in later 2010 uncovered a toll fraud ring operating in Europe that stole minutes valued at more than 11 million Euros, netting more than 1 million Euros in profit themselves.
- The FBI broke up a toll fraud ring in 2009 that is estimated to have stolen more than \$55 million in long distance minutes, as hackers broke into US enterprise PBXs, took control of them, and stuck enterprises with the bill.
- The Communications Fraud Control Association estimates that compromised PBXs and premium-services fraud result in losses of around \$20 billion (in 2009).

The bottom line for any enterprise deploying VoIP or UC is that proactive security against toll fraud and premium-rate fraud must be implemented or that enterprise may become a fraud victim.

Exploiting an Enterprise VoIP/UC for toll fraud

Three areas within an enterprise VoIP/UC deployment are most vulnerable to exploitation for toll fraud or premium-rate fraud.

- **PBX/Voicemail/Application Servers:** These communications systems are particularly susceptible to security breaches due to their often weak password protection.

Furthermore, policy enforcement on these systems is limited, allowing redirects, transfers, and forwards to long distance, international toll, or premium-rate numbers without proper authorization.

- **PSTN Connectivity:** Attackers typically exploit the fact that session border controllers (SBCs) or media gateways accept calls from anywhere and route them to the service provider with limited or no authentication. Sometimes even service providers employ only weak authentication on SIP trunks, and the SBC can be bypassed.
- **User/Device Authentication:** Enterprises deploying phones over extended networks or low security networks without strong authentication – including lobby phones, guest rooms, and the Internet – are especially vulnerable to exploitation. Without strong two-factor authentication, lost or stolen phones can be easily misused. Once attackers gain access to a misplaced device or are able to guess or “brute force” weak credentials, they are ready to make calls as the authorized user. This type of attack raises further security concerns, as attackers can also exploit the user identity associated with the credentials.

Are you at risk for toll fraud?

- Do you have PSTN connectivity? Are you using SIP trunks?
- Do you have an IP-based or hybrid PBX? Do you have an IP-based voicemail system?
- How are you securing your VoIP/UC assets? Firewalls? SBCs?
- What strategy are you using to authenticate phones and phone users?
- Does your security strategy cover VoIP/UC? What priority does this get?
- Are you encrypting your VoIP/UC communications? Are you encrypting both signalling and media? Are you encrypting configuration and management protocols on phones?

- Do you collect and review logs of your systems? Do you collect call records? Is this on a per department basis? Are unusual changes flagged for investigation?
- Who maintains and tracks your calling policies? Are your VoIP users and administrators aware of security risks to your VoIP system?

These considerations are fundamental for establishing an effective security posture that reduces the risk of VoIP fraud. Siperia offers consulting services that help its customers address these and other essential security requirements.

Find Out if You're Vulnerable – Siperia VIPER Audit Services

To find out if your network deployment is vulnerable to toll fraud or other telecommunications or UC fraud, Siperia VIPER Lab, the vulnerability research and assessment arm of Siperia Systems, offers vulnerability assessment (VA) services to gauge your security posture. Ranging from security surveys to comprehensive penetration testing, VIPER Vulnerability Assessments are trusted by IT and security professionals in all types of industries to:

- Test system integrity and the security architecture of mission-critical voice, video, and data communications systems;
- Uncover and mitigate VoIP and UC security gaps and vulnerabilities that jeopardize regulatory compliance; and
- Identify and mitigate threats that hamper the adoption of UC and undermine the return on investment (ROI) on VoIP and UC.

Combating VoIP & UC fraud with Siperia UC-Sec

Toll fraud and other communications fraud cannot be properly mitigated by data security measures alone. Firewalls and data security products, for example, do not have an in-depth understanding of how communications services work and therefore cannot offer specific policies for different users based on their device, network, or business needs.

Siperia Systems' UC-Sec real-time security appliance offers comprehensive security solutions that combat VoIP and UC security threats, overcome the challenges of UC adoption, and provide the most advanced protection against toll fraud. The production-proven Siperia appliance can be deployed in the so-called "demilitarized zone" (DMZ), between virtual local area networks (VLANs), or in the core of an existing UC infrastructure. The industry's first Common Criteria-certified solution for UC security and SIP trunk termination, UC-Sec protects against a multitude of exploits that can cause toll fraud, other communications fraud, or other exploits against VoIP and UC infrastructure.

Particularly powerful against toll fraud is UC-Sec's protection of VoIP servers, PSTN connectivity, and user device authentication.

Protection against PBX/voicemail/application server exploits: Placed in front of PBX/ voicemail/application servers, UC-Sec protects against attacks by:

- Hiding the servers' network topologies and allowing access only to authorized phones via VoIP/UC-related ports (i.e., management interfaces are blocked).
- Supporting policies that forbid external calls, transfers, forwards, etc., from certain domains, users, or untrusted environments.
- Detecting a large number of calls to the same number as stealth Denial of Service (DoS), alerting administrators, and blocking the attack.
- Detecting a large number of calls from same number as Call Walking, alerting administrators, and blocking the attack.

Protection against user device authentication exploits:

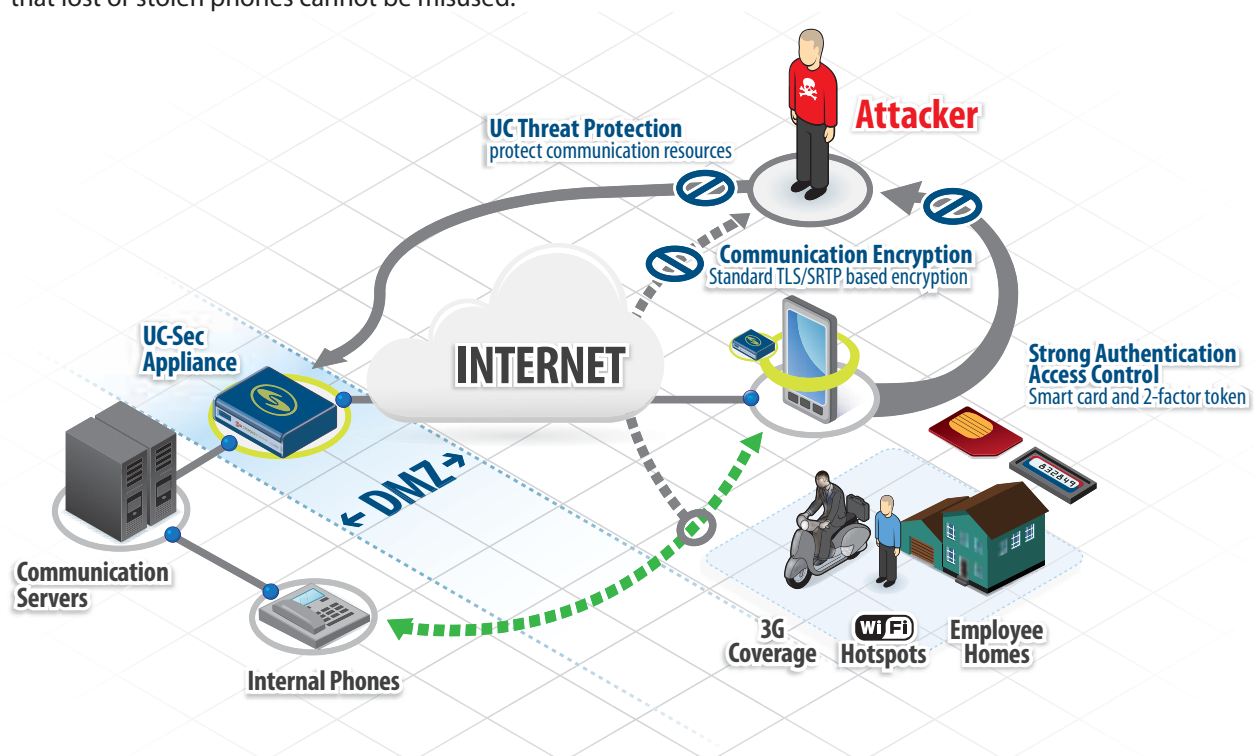
When Sipera UC-Sec is deployed between trusted/access-controlled networks and untrusted networks (such as lobby phones, hotel guest rooms, or even the Internet from user homes and hotspots), it can employ strong access control mechanisms to protect against misuse. Specifically, UC-Sec:

- Enables authentication of devices/phones with X.509 certificates.
- Integrates strong, two-factor authentication for VoIP and UC users, requiring them to key in a token-based passcode before making or receiving calls to ensure that lost or stolen phones cannot be misused.

- Enforces encryption of all credentials over transport layer security (TLS), ensuring credentials are protected in transit over unsecured/public networks.
- Enforces connection-oriented protocols and even TLS, protecting against man-in-the-middle attacks.
- Fingerprints all devices and sees any change in behavior due to spoofing. Also uses changes in device location as a trigger for re-authentication.

Protection against PSTN connectivity exploits: When Sipera UC-Sec is used as the SIP peering point to connect via an Internet Telephony Service Provider (ITSP) to Public Switched Telephone Network (PSTN), it protects against attacks by:

- Supporting policy configuration to disallow external calls, transfers, forwards, etc., from certain domains, users, or untrusted environments.
- Enabling proper authentication of call server and service provider, using X.509 certificates and TLS.
- Detecting any unusual usage as an attack and blocking it.
- Supporting the configuration of signalling rules to block certain messages, responses, error codes, and headers that are usually manipulated by attackers to route calls.
- Allowing administrators to set policy that "black lists" users and domains.



Fraud Takes a Toll on Enterprises:

- America's Most Wanted", Edwin Andres Pena, made more than a million dollars reselling minutes by hacking into the communications systems of US enterprises.
- The US Federal Bureau of Investigation reported that an estimated \$55 million worth of minutes were stolen from US enterprises by one fraud ring that resold the minutes in European countries.
- Hackers breached the VoIP PBX telephone system of a 'small Perth business' (in Australia) and made more than 11,000 international calls in 46 hours, resulting in toll charges in excess of \$120,000, according to Western Australia Police.
- Authorities in Europe in late 2010 broke up a fraud group that had hacked PBXs to place international calls and calls to premium numbers, eventually running up fraud totalling 11 million Euros.
- A small Sydney-based company discovered that hackers had broken into its telephone system and run up bills of AU\$9,000 in one week.
- In the Toronto-Hamilton area in Canada, several companies' phone systems were hacked, resulting in charges ranging from a few thousand to hundreds of thousands of dollars

CONCLUSION

Toll fraud, premium-rate fraud and other forms of telecommunications fraud are costing businesses billions of dollars. Highly motivated by the prospect of lucrative pay-offs, hackers are staging a variety of attacks, exploiting network vulnerabilities and taking advantage of unsuspecting enterprises. With the proven vulnerability assessment services of its VIPER Lab, Sipera Systems can help you determine just how secure your network and services are against toll fraud and other VoIP/UC-related attacks. Sipera's comprehensive UC-Sec security appliance proactively protects enterprises against the attacks, misuse, and service abuses they face with their VoIP/UC deployments.

UC Security in a Box

Sipera's UC-Sec appliance provides a complete application-layer security architecture in one device:

- Firewall
- Session Border Controller
- Intrusion Detection System and Intrusion Prevention System (IDS/IPS)
- Access Controller
- Authentication
- Unified Communications Proxy
- VPN / Encryption
- Policy Enforcement

... for all real-time Unified Communication applications

UNIFIED COMMUNICATIONS UNLEASHED

About Siper 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. Sipera's 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, Sipera's 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

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