REDSHIFT
NETWORKS

Comprehensive Security for UC, Collaboration and CEBP Elements in Cloud and Enterprise Networks

A taxonomy of Unified Communications, Collaboration & Communication Enabled Business Process (CEBP) threats and techniques for implementing defensive measures

A RedShift Whitepaper
www.redshiftnetworks.com
December 2009

REDSHIFT
NETWORKS

REDSHIFT
NETWORKS

Executive Summary

The emergence of Unified Communications, Collaboration and CEBP technologies have caused a fundamental shift in the design of enterprise communications and cloud infrastructure. Traditional systems running on legacy networks are being replaced by IP-based systems that provide numerous benefits to an enterprise. These benefits ultimately derive from the power of open systems to deliver rich software-enabled services. They also include the practical benefits of lower cost, improved manageability and greater ease-of-use that are generated by moving applications from proprietary platforms to familiar and widely supported industry standard ones.

Unified Communication, Collaboration, & CEBP solution vendors have made great strides in tightly tying the operation of enterprise data applications together with the features of IP-telephony and other real-time communication applications to improve overall employee connectivity and business productivity. The combination of these two previously separate worlds is being called "Unified Communications" (UC) / "Collaboration", when the integration happens at the end user desktop PC or "Communication-Enabled Business Processes" (CEBP) when the integration is within an enterprise application running on dedicated servers. As a result, a new generation of highly enriched services is now feasible. These services range from simple click-to-call integration with corporate and personal directories, to a connected business process that can help solve complex logistical bottlenecks by allowing multiple partners to actively collaborate any time, using any IP-based device, on any network.

Enterprises must understand that while UC, Collaboration, and CEBP applications present great promise, they also present unique security requirements that are different from conventional data applications. The real-time nature of these communications, combined with their use of disparate open networks, means they are exposed to a wide range of complex threat vectors that are difficult to anticipate and protect against.

As vendors and service providers move to offering Unified Communications & Collaboration applications in the cloud, security takes center stage as the UCaaS cloud provider compete for enterprise customers and use 'security' as a value-add offering.

This white paper focuses on numerous threat vectors that plague these applications including Voice Denial-of-Service (VDOS & VDDOS) attacks, SPAM over Internet Telephony (SPIT) attacks, eavesdropping, spoofing, number harvesting, protocol anomaly and fuzzing attacks, call park conferencing attack, IP PBX password attack, signal and media manipulation attacks and toll fraud. The paper discusses the shortcomings in existing security solutions and presents the requirements for a comprehensive UC, Collaboration and CEBP security solution.

REDSHIFT
NETWORKS

Introduction

The emergence of Unified Communications (UC), Collaboration and Communications Enabled Business Process (CEBP) solutions has caused a fundamental shift in the way that telecommunications services are deployed in enterprises today. The convergence of Voice, Video and Data into one IP network has created a cost-effective transport mechanism that enables a rich new set of services. Voice & Video, which was previously confined to a separate legacy network, is now ubiquitous and plays an integral role in communicating among and bridging between disparate entities. These entities include multiple users and user groups both inside and outside the enterprise, as well as advanced applications that can potentially communicate "any where, any time with any device".

First, UC and other IP-based systems are quickly replacing more traditional telecom systems due to their numerous benefits such as low cost, simple manageability, compatibility with pervasive IP networks, and their easy integration with other IP-based software enabled services. The growing popularity of these systems is fundamentally the result of two factors: the cost savings inherent to the migration from legacy networks to UC networks, and the flexibility that allows new services and applications to be added to standard telephony and communication services. As a result, richer converged application services that were otherwise not possible are now feasible due to the underlying common IP-based communication platform. This fundamentally changes the communications landscape and the way users communicate with other users and applications.

Second, UC leverages the common VOIP & Video infrastructure to communicate with multiple disparate communication systems, media, devices and applications. The ability to redirect and deliver, in real-time, voice, video, email or text-based communications from a variety of systems to the device nearest to the intended recipient presents a powerful mechanism to connect anyone, anywhere, with any-device. This can significantly reduces communication delays and provide faster interaction and service delivery to the end user. A few examples of UC applications include Presence, Collaboration, IP-PBX, Interactive Voice Response (IVR) and Unified Messaging applications.

Third, in CEBP the UC logic is embedded within a business application or as part of a business flow in response to real-time events. As a result, response and resolution times can be drastically reduced and the right people with the right skill sets can be quickly engaged to solve a specific business problem. This reduction of unnecessary communication delay between the human elements necessary to solve a problem can result in both improved customer satisfaction and significant cost savings to a business. A simple example is an ERP system that can detect a sudden dip in inventory below a threshold for a specific item and immediately sets up a collaborative data-rich session with the supply-chain manager, reseller, transportation manager and customer support personnel to resolve the issue quickly.

However, significant deployments of these solutions pose several interesting challenges that need to be addressed effectively in order to gain widespread adoption. Solution providers need to preserve the high quality, reliability and security standards that public switched telephone (PSTN) network has traditionally offered even though the underlying communications

infrastructure are based on UC networks and technologies. Developing a robust architecture that adheres to these constraints is not an easy task.

It is also important to understand that most IP networks are to a greater or lesser extent open systems, and thus they may be fertile breeding grounds for a variety of malicious and illegitimate activities that can compromise the integrity of any enterprise, network or a user. A number of recent studies have concluded that nearly half of organizations planning to deploy UC believe that UC networks and applications are inherently insecure. These concerns challenge all organizations deploying or planning to deploy UC to understand and undertake effective preventive measures. One recent study from Gartner indicates "Enterprises that don't spend on IP Telephony Security today will end up spending 20% of their Security Operations Budget on it in 2011. Enterprises that are proactive in nature will only spend 5% of IP Telephony Security Budget".

REDSHIFT
NETWORKS

Unified Communications & Collaboration Security is Different

UC & Collaboration security differs from conventional data security in that the communication takes place in real-time. UC & Collaboration element characteristics include:

- High reliability requirements
  - Providing 5-9's reliability translates to:
    - 5 minutes downtime per year
    - 26 seconds downtime per month
    - 6 seconds downtime per week
  - Data networks provide only 3-9's reliability
- Stringent latency, jitter and packet loss requirements for good Quality of Service
  - Signaling
    - 2 mSec delay, no packet loss
  - Media
    - 10 mSec introduced delay
    - 100 uSec introduced jitter
    - < 0.1% packet loss
- Security requirements are very different
  - Low tolerance to false positives
  - Low tolerance to false negatives
  - Call re-attempts are not acceptable
- Complex heterogeneous network
  - Deeper interoperability requirements with disparate systems
  - Complex services spanning multiple protocols
  - Zero-touch deployment

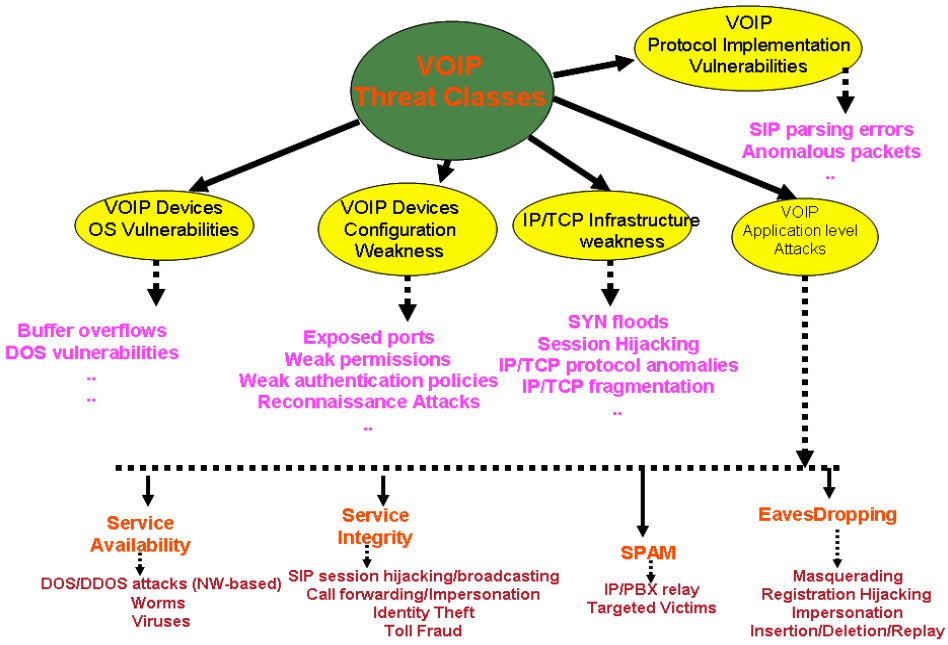
It is clear that because UC & Collaboration applications involve many new protocols, networks and devices, as well as a continued dependence on existing PSTN systems, these applications pose a formidable challenge to the security conscience network manager. They are subject to new threat vectors that can emanate from either the IP or the PSTN network. This means the underlying protection technologies designed for the individual networks are not well suited to counter many UC & Collaboration threats. The reliability and uptime requirements for these applications are very high. A typical response to a new security attack in the data world may require a human intervention resulting in a significant time delay while scope of the threat is assessed and appropriate mitigation solutions are applied. While this may be satisfactory in the data world, UC & Collaboration requires a real-time response to security threats.

Communication solutions are also highly sensitive to QoS parameters. A UC & Collaboration security solution that causes a noticeable loss in voice & video quality is unacceptable. Any interruption in the flow of packets, reassembly or jitter will impact the quality of the voice conversation. In the data world, these issues are addressed by retransmission of the lost data resulting in additional delay in end user traffic. While this may be acceptable in the data world, these kinds of errors in the VOIP & Video realm degrade the user experience to levels below

"toll quality". This is an unacceptable solution in an enterprise voice & video network where quality at least equal to currently deployed solutions is required.

Latency is another factor. Modern data security solutions employ encryption and/or deep-packet inspection methods to improve security. Both these methods introduce additional time delay and jitter to VOIP & Video packet streams, thus impacting the overall QoS.

Lastly UC & Collaboration networks will continue connect to and depend on existing PSTN networks. This hybrid network poses a new set of challenges, attack entry vectors and application threats. With a myriad of deployment solutions and architectures encompassing both VOIP/Video and traditional PSTN networks, the complexity of the threat detection and mitigation grows exponentially.



UC & Collaboration Threat Taxonomy

RedShift researchers have analyzed several thousand threats compiled from various sources, including the VOIPSA, CERT, BugTraq and vulnerability postings from several vendors. The author observes that UC & Collaboration deployment faces a variety of threats from different entry points and attack vectors ranging from exploiting weaknesses in networking layers, underlying OS, protocol implementation vulnerabilities, application layer attacks and/or device configuration weaknesses. The authors have identified five broad UC threat categories as shown in the figure. The rationale behind the categories is to group common attacks with similar entry methods and/or common vulnerability exploitation. This increased understanding of the various UC & Collaboration threat vectors helps formulate a common effective security solution for each category.

UC & Collaboration Device and OS Vulnerabilities

UC & Collaboration devices such as IP phones, Call Managers, Gateways, Registration and other Proxy servers run on an underlying operating system. If an underlying OS is compromised, this

can compromise the integrity of the affected UC & Collaboration device. Most of the UC & Collaboration devices run on traditional operating systems, e.g. Windows, Linux, RTOS's etc. that are vulnerable with numerous exploits publicly available.

A few examples in this category include:

- Several buffer overflow exploits publicly available against the Cisco IOS operating system [1]
- Denial-of-Service (DoS) exploits triggered by fragmented UDP packets for Alcatel and Avaya phone [2]

UC & Collaboration Device Configuration Weakness

Many attacks penetrate through UC & Collaboration infrastructures due to weakness in configurations, e.g. open TCP/UDP ports, open files shares with global read/write permissions or temporary folders with weak permissions etc. As a result, the services running on the UC device now become vulnerable to wide variety of attacks resulting in either a loss of service or a compromise of the UC & Collaboration device.

A few examples in this category include:

- A known Cisco SIP-based phone telnet service vulnerability that allows the telnet service to be exploited by an attacker due to weak password permissions set on the VOIP/Video device [3]
- The SNMP services offered by the devices may be vulnerable to reconnaissance attacks. Example, valuable information was gathered from an Avaya IP phone by using SNMP queries with the "public" community name [4]

IP/TCP Infrastructure Weakness

The availability of the UC services depends on the availability of the underlying IP/TCP infrastructure that it sits on top of. UC protocols rely on TCP and UDP as transport mediums and hence are also vulnerable to attacks that TCP and UDP are generally exposed to, e.g. DOS/DDOS, session hijacking, protocol anomalies, etc. which may cause an undesirable behavior on the UC services.

A few examples in this category include:

- Several publicly available tools that generate TCP and/or UDP flooding attacks
- Malformed TCP packet generators that can result in undesirable crashes

UC & Collaboration Protocol Implementation Vulnerabilities

UC protocols such as H.323 and especially SIP are relatively new standards. Both the protocol specifications and the subsequent implementations need to mature to reduce the overall threat exposure. Examples include parsing errors, NULL packets, anomalous packets, RFC violations etc.

An example in this category includes:

- Several vulnerability discoveries in vendor implementations of VOIP products that use H.323 and SIP by University of Finland's PROTOS group [5]. The PROTOS work is

publicly available to any script kiddy who can download and run the tools necessary to crash vulnerable implementations.

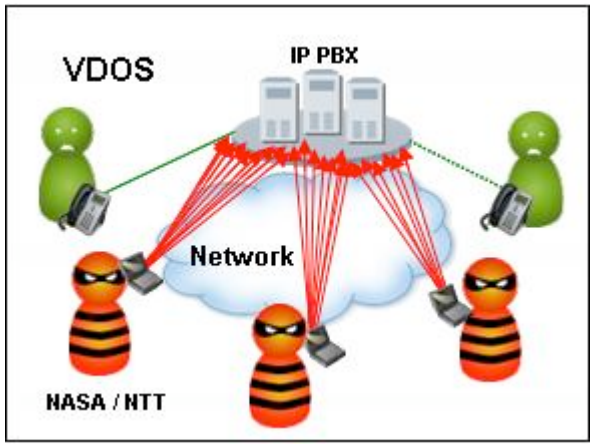
UC & Collaboration Application-Level Attacks

Finally, the UC applications themselves are subject to attacks. The authors have identified four broad attack categories after performing deep research on several hundred exploits and looking at the various entry and injection mechanisms. The categories include:

(1) Service Availability Attacks

These attacks are focused towards potentially disrupting the availability of a UC & Collaboration services. The unavailability of a critical service has a direct customer impact, lost revenues, unplanned downtimes and maintenance costs. Some examples include VDOS attacks, remote code injection, viruses or worm-based threats. The affected clients can range from end-user UC applications, phones, soft-clients, call managers, registration servers etc. Any disruption in service availability can have tremendous business impact including financial loss and loss of productivity due to the real-time nature of voice communications.

Voice Denial of Service (VDOS) Attacks



DOS attacks can be of two kinds, (1) resource starvation or (2) resource unavailable. Resource starvation usually occurs as the result of flooding attacks originating either from a single source or multiple sources. A naïve attacker can flood the destination server with several control packets hogging significant CPU bandwidth thus making the victim server totally unusable. The DDOS attack is a variant of DOS, whereby the attacker uses multiple sources to collectively generate and send excessive number of flood packets to the victim server, often with fake and randomized source addresses, so that the victim server cannot easily identify the flooding sources. The second attack type exploits a specific vulnerability (e.g. buffer overflow attack, malformed or fuzzed inputs) on one of the networking facing processes resident on the victim server thereby making it unusable, often leading to a crash or an undesirable situation.

A flood situation may also arise due to valid reasons such as a power failure or an unexpected crash of a system due to patch update etc. This can result in a sudden upsurge of normal traffic, e.g. registration requests from the endpoints.

(2) Service Integrity Attacks

These attacks are focused towards compromising the integrity of a UC & Collaboration service. The attacks are very targeted and hard to detect. The end results of these attacks can include loss of reputation, brand name, leakage of sensitive information, phishing attacks etc. Some examples include collaboration session hijacking, redirecting existing media conversations to attacker machine, classic man-in-the-middle (MITM) attacks, broadcast hijacking, identity theft, conversation alteration, protocol fuzzing and anomaly attacks, impersonation and toll fraud.

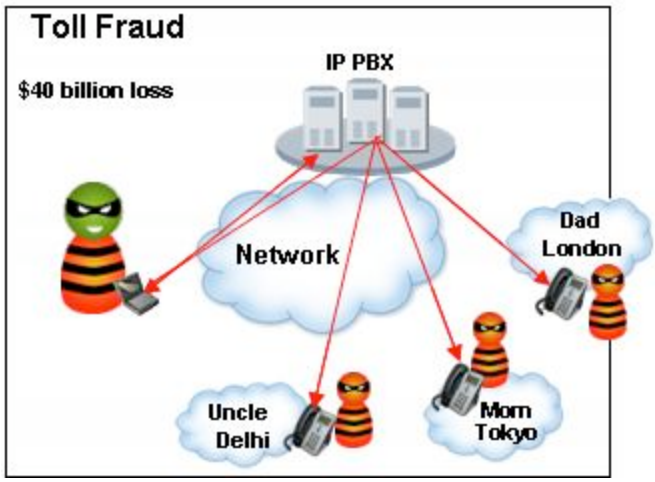
Protocol Fuzzing and Anomaly Attacks

Fuzzing is a popular black-box testing method employed by software vendors to improve robustness and performance of their code. Fuzzing involves perturbing to contents of protocol packets in order to test what the software behavior under abnormal conditions. These tests can range from input fuzzing, protocol state fuzzing or structural fuzzing and often result in a crash, denial-of-service or degradation.

There are several hundreds of such tools available on the web today that anyone can download and run it against a UC network. A few examples of open-source tools include PROTOS [5] and SiVus [6]. Commercial tools include Spirent ThreatEx [7] and CodeNomicon [8]. A malicious user can run these tools against any VOIP network in a matter of minutes resulting in a variety of risks ranging from application crash, information leaks or a denial of service.

Toll Fraud

Toll fraud happens when a hacker gains illegitimate access to a UC & Collaboration network and allows unauthorized users to makes calls to a premium rate number, e.g. repeated long distance calls to international toll numbers. UC systems are particularly vulnerable to toll fraud because they form an integral part of an enterprise's IP network, unlike PBX systems that are closely monitored and managed by separate groups. UC toll fraud attacks can lead to serious financial damage and loss of reputation in a remarkable short period of time.



In the example above, the hacker illegitimately hacks into an IP-PBX system to steal calling minutes and make free long distances calls to Dad (in London), Mom (in Tokyo) and Uncle (in Delhi). A sophisticated hacker can also sell the stolen minutes into a thriving black market. This resulting in unsuspecting users buying and making illegitimate calls and makes identification of the source of toll fraud detection much harder.

Protection from Data Threats

The beauty of converged networks is that voice over IP & Video over IP is 'just' another application running on the data network. Unfortunately from a security viewpoint, this means that it will also be affected by all the attacks that affect data networks, even if they are not deliberately targeting voice over IP and Video over IP.

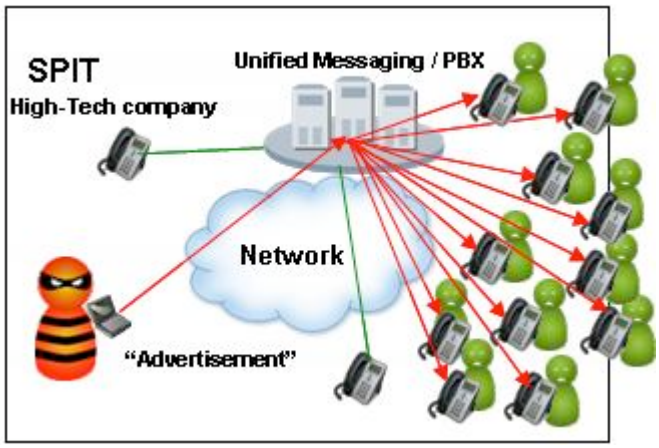
The most significant specific threat to UC is denial of service (DoS) because this can bring a data network to its knees and shut down all applications running on it - including UC. This means that affected users could be without phone service until the network is restored. Specific threats include buffer overflow exploits, malicious SQL or command injection [11] and Cross-site scripting attacks [10].

The internet security bugs that plague data applications will also affect UC users because UC is just one another application facing the internet and shares the applications potential vulnerability to malicious users.

(3) SPAM over Internet Telephony (SPIT) Attacks

SPAM over Internet Telephony (SPIT) has the potential to grow to be as big a problem as its email counterpart. With the increasing deployment of IP solutions, it is expected that SPIT will be an attractive choice for a spammer due to its low cost and pervasiveness of the internet. Conventional SPAM methods adopted by telemarketers require a human or an autodialer serially dialing phone numbers and making the voice connections. This changes drastically with IP

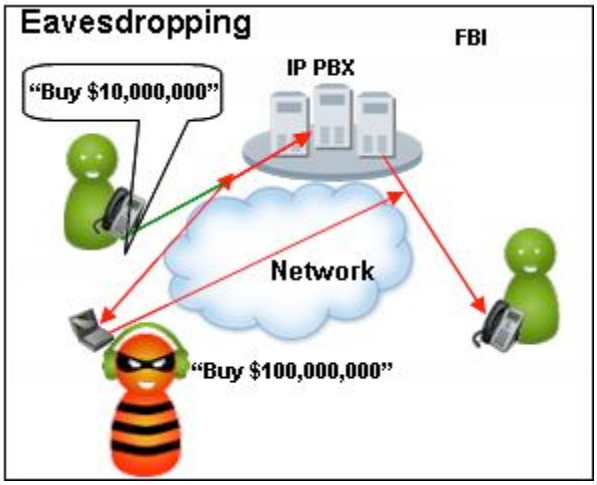
networks, as even a simple computer script can now flood corporate phone systems with many simultaneous calls without adequate protection.



The above figure shows an example where a telemarketer floods corporate VOIP phones with Viagra SPAM messages. There is a general perception that Voice SPAM will increase on a trajectory like Email SPAM. Most of the UC deployments today are confined to restricted zones with limited internet access, once they become available to open networks and to the reach of spammers, this problem will exponentially worsen.

(4) EavesDropping

These attacks allow the attacker to obtain sensitive business or personal information otherwise deemed confidential. The mechanism is the intercepting and reading of messages and conversations by unintended recipients. Once the information is collected and translated, various Man-in-the-Middle (MITM) attacks can be launched, e.g. reading, inserting, modifying the intercepted messages etc. Some examples include masquerading, registration hijacking, impersonation and replay attacks.



Eavesdropping attacks describe a method by which an attacker is able to monitor the entire signaling and/or data stream between two or more VoIP/Video endpoints, but cannot or does not alter the data itself.

Someone who hacked into a company's router could listen in to a board of directors' meeting and use the information illegitimately to buy more stocks or sell the information to another institution. The possibilities of threat risks are very large.

Call Pattern Tracking

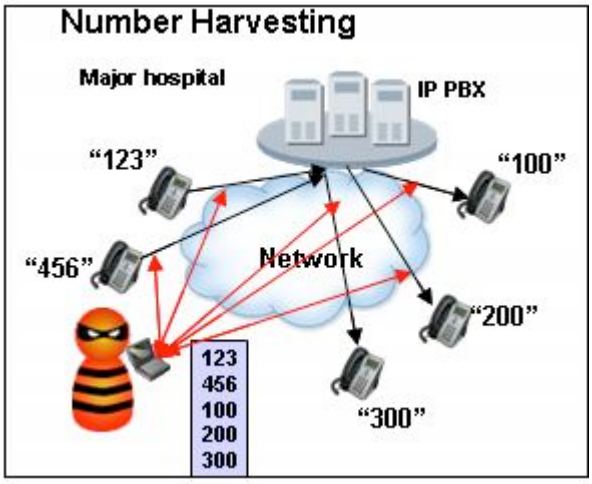
Call Pattern Tracking is the unauthorized analysis by any means of any traffic from or to any node or collection of nodes on the network. It includes monitoring and aggregation of traffic for any form of unauthorized pattern or signal analysis. Call Pattern Tracking is a technique for discovery of identity, affiliation, presence and usage. It is a general technique that enables unauthorized conduct such as theft, extortion and deceptive practices including phishing.

Traffic Capture

Traffic Capture is the unauthorized recording of traffic by any means and includes packet recording, packet logging and packet snooping for unauthorized purposes. Traffic capture is a basic method for recording a communication without the consent of all the parties.

REDSHIFT
NETWORKS

Number Harvesting



Number Harvesting is the authorized collection of IDs, which may be numbers, strings, URLs, email addresses, or other identifiers in any form which represent nodes, parties or entities on the network. Number Harvesting is an unauthorized means of capturing identity and enabling subsequent unauthorized communication, theft of information and other deceptive practices. These attacks usually run as pre-cursors used to understand UC deployments and exploit publicly known vulnerabilities against its infra-structure.

Conversation Reconstruction

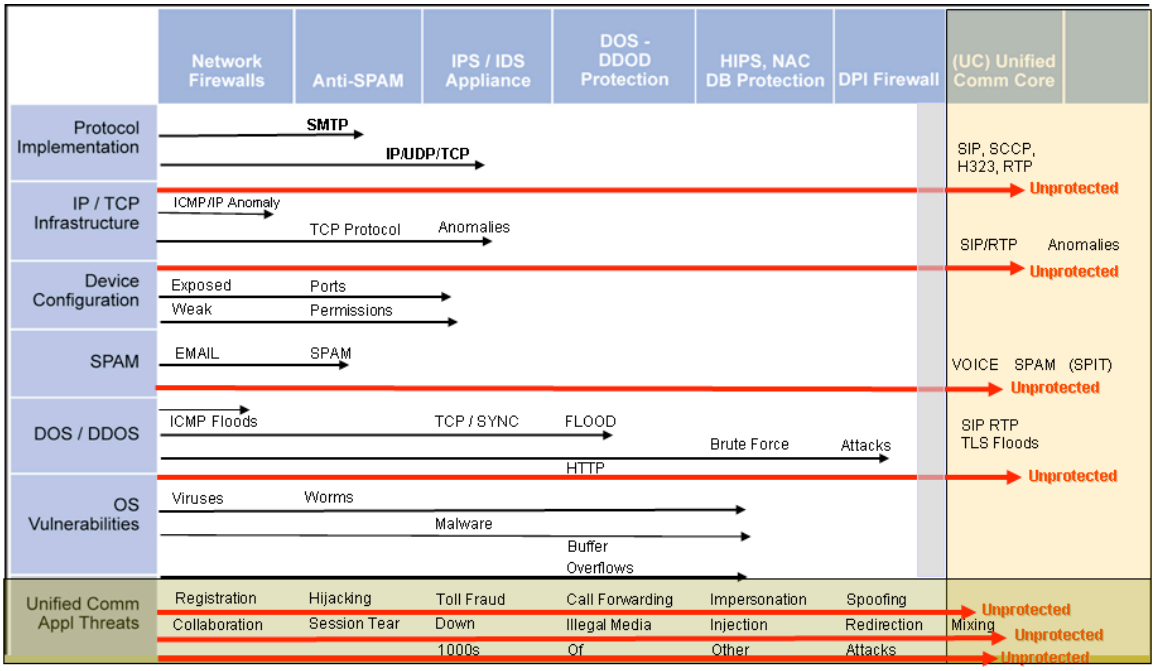
Conversation Reconstruction is any unauthorized monitoring, recording, storage, reconstruction and/or extraction of any audio or voice portion of any communication including identity, presence or status. Conversation Reconstruction is a means for collecting, duplicating or extracting information on the audio content of a conversation done without the consent of the parties engaged in the communication.

Voicemail Reconstruction

Voicemail Reconstruction is any unauthorized monitoring, recording, storage, reconstruction and/or extraction of any portion of any voice mail message without the consent of the affected party. The nature of the attack is similar to above except that the affected protocol and UC service/application is different.

REDSHIFT
NETWORKS

Drawbacks to Today's UC Security



The table maps the above mentioned threat categories against current protective solutions ranging from Network Firewalls, Anti-SPAM devices, IDS/IPS appliances, DOS/DDOS protection, Host Intrusion Prevention Systems (HIPS) and Deep packet inspection (DPI) firewalls. As shown, the far right column and the bottom row present regions that are not protected by current solutions today. The far right column indicates UC protocols such as SIP, RTP, SCCP and H.323 are totally unprotected today. The bottom row presents several hundreds of Unified Communication (UC) & Collaboration Application Layer threats, few examples (as mentioned in previous sections) include attacks such as Collaboration Hijacking, Toll Fraud and Number Harvesting.

To address complex security and deployment challenges mandated by UC networks and UC applications is a formidable challenge. Existing solutions are deficient in a number of ways:

- They cannot function in real-time

- They cannot process encrypted traffic
- They cannot do deep packet inspection (or examination) of UC protocols such as SIP, H.323, SCCP and RTP
- They cannot protect against zombie or malware attacks spreading from end-user such as click-2-call applications
- They cannot keep up and provide adequate protection for higher UC and CEBP services and features
- They have high percentage of false-positives and false-negatives which is tolerable in data applications but not for real-time applications
- Most existing protective solutions are offered as piece-meal solutions employing multiple security solutions such as firewalls, IDS/IPS, DOS appliances and other security devices that are upgraded to support UC in addition to data protection. These devices are not well suited to address complex UC & Collaboration application layer attacks
- The additional devices also result in multiple hops in the network leading to additional time delays reducing their ability to meet UC quality-of-service requirement

Comprehensive UC & Collaboration Security

A comprehensive UC & Collaboration security solution while satisfying the mandatory requirements for real-time communications such as low delays and high QoS should also provide best-of-breed security technologies that ensure that UC and CEBP security threats are pro-actively recognized, detected and remediated. The authors strongly feel that in order to meet complex security requirements for UC, Collaboration and CEBP traffic comprehensively, a solution should have the following characteristics:

- Deep packet inspection capabilities from Layer 3 up to Layer 7 UC traffic
- Advance correlation of protocol state and security events across the different layers and security modules
- Heterogeneous architecture comprising of both proactive and reactive solution elements
- One UC security solution – not a slapstick of several piecemeal solutions
- Tightly integrated with IP-PBX and other communication infrastructure elements – easy to deploy and manage
- Low latency using advanced software, hardware and system acceleration techniques
- Near-zero False-positives and False-negatives
- Comprehensively address UC and CEBP application security threats
- Easy integration with 3'rd party vendor solutions providing UC and SOA services (e.g. Microsoft, SAP, BEA, IBM)
- Provide visibility to all UC traffic
- Provide control to all UC services, Applications and Assets

Some of the finer-grain elements include:

- Protection against Voice DOS/DDOS threats
- Protection against VOIP SPAM (SPIT)
- Protection against War-dialing threats

- Protection against UC Application layer threats such as Toll Fraud, Collaboration Hijacking and Number Harvesting
- Protection against Eavesdropping threats
- Provide UC Intrusion Prevention capabilities with signatures support
- Provide full termination, stateful and deep packet inspection of UC and CEBP traffic
- Provide protection against protocol anomaly or fuzzing style of attacks
- Protection from Data Threats such as SQL injection or Cross-Site Scripting attacks
- Provide sophisticated Application Behavioral Learning
- Automatic learning and enforcement of positive behaviors
- Control and Visibility
- Not be a single point of failure in the network
- Provide complete examination of both encrypted and plain-text traffic

Conclusions

Current UC & Collaboration security solutions fall into 2 broad categories, (1) Session Border Controllers (SBC) and (2) Data Security products. The SBC sitting at the edge of the voice network provide basic VOIP protection capabilities such as Authentication, Encryption and port/ACL filtering. SBCs do not have the computing power and intelligence to perform the deep packet inspection necessary to analyze higher UC & Collaboration protocol traffic, an essential requirement for protection against UC & Collaboration layer threats.

The data security products do limited deep packet inspection and provide basic DOS/DDOS and protocol anomaly protection but are simply not geared to address the real-time challenges and increased complexity of UC networks. The QoS requirement for real-time communications (2 ms for signaling and 100 µs for media) is also a hard deployment challenge to satisfy.

In essence, a new best-of-breed product category is required to comprehensively address the UC and CEBP security while strictly adhering to the real-time deployment requirements. The device should be easy to deploy, real-time performance and posses advanced security techniques and technologies to protect UC and CEBP applications against a wide array of threat vectors and security risks.

References

[1] Cisco Call Manager Windows 2000 Workstation Service Buffer Overflow
http://www.cisco.com/warp/public/707/cisco-sa-20040129-ms03-049.shtml

[2] Miercom VOIP Security Assessment
http://www.miercom.com/?url=products/spreports

[3] Cisco IP Phone Compromise
http://www.sys-security.com/archive/papers/The_Trivial_Cisco_IP_Phones_Compromise.pdf

[4] Breaking Through IP Telephony
http://www.nwfusion.com/reviews/2004/0524voipsecurity.html

[5] PROTOS, Security Testing of Protocol Implementations

http://www.ee.oulu.fi/research/ouspg/protos/

[6] SiVUS, The VOIP Vulnerability Scanner, http://www.securityfocus.com/tools/3528

[7] Spirent ThreatEX
http://www.spirentcom.com/analysis/technology.cfm?WS=325&SS=118&wt=2

[8] CodeNomicon, Defensics VOIP Security Testing product
www.codenomicon.com

[9] SNORT™ Implementation Manual
http://www.snort.org/docs/snort_manual/2.6.1/snort_manual.pdf

[10] Cross-Site Scripting Attacks, Mookhey et al.,
http://www.blackhat.com/presentations/bh-usa-04/bh-us-04-mookhey/old/bh-us-04-mookhey_whitepaper.pdf

[11] SIP Message Tampering, The SQL Injection Code Attack, Dimitris et al.
http://www.snocer.org/Paper/camera-ready_soft_com.pdf

About RedShift Networks

Redshift Networks is the leader in the new Unified Communications & Collaboration Security market, and has developed the Unified Communications Threat Management (UCTM) platform, the industry's first complete threat management solution for Unified Communications (UC), Collaboration and Communication Enabled Business Process (CEBP) applications. Our core team has deep expertise in voice, data and security and has worked previously at leading companies such as Cisco, Avaya, Nortel, HP, SGI and NetContinum. This expertise forms the foundation of Redshift's UCTM class of products that complete security, visibility, and control of real-time voice, video and multi-media traffic. Founded in late 2006, RedShift is headquartered in Milpitas, CA. Visit www.redshiftnetworks.com.