

Securing Internet Protocol Telephony

By Ron Leibfreid

In recent years, Internet Protocol (IP) Telephony has grown into a viable alternative to traditional public switched telephone network (PSTN) voice services. While most professionals in this industry are familiar with the security concerns related to traditional voice and IP security, many are not aware of how security plays a role in IP Telephony. This document addresses the security concerns specific to Voice over IP (VoIP) and the industry-recognized remedies in use today to combat them.

Security Risks

Traditional voice security problems are simple and well-understood. In the PSTN world, security problems include fraudulent use of service, privacy concerns, and loss of service. These security issues have had the same underlying technology problems and solutions for decades. The same cannot be said for IP Telephony.

IP Telephony has the same security issues as traditional telephony, including fraudulent use of service, privacy concerns, and loss of service. Even though traditional telephony has faced and solved these very same issues, placing calls and their corresponding signaling onto an IP infrastructure changes the dynamics of how these fundamental security considerations must be addressed. Many groups of technology problems must be successfully identified and addressed during the migration from traditional voice services to an IP Telephony environment.

Privacy

Privacy is a great concern to corporations looking to implement VoIP. Privacy of both the signaling and the call itself are critically important. Exposed signaling can provide eavesdroppers with calling patterns containing the information about when calls are placed, the participants involved, and the length of time that calls remain connected. Depending on other circumstances, the simple knowledge of a call's existence may provide an outsider with information that could have negative consequences. It is important to consider the need for encrypted signaling in the IP Telephony environment and the benefits that encryption provides. The adoption rate of encryption with premises-based enterprise solutions has been faster than provider-based or hosted solutions. Verizon Business has been instrumental in helping to develop the standards and best practices that are appropriate for extra-enterprise communication.

Actual call privacy is at risk as well. Many corporations may agree that it is not good security practice to conduct sensitive conversations on a mobile phone network, yet few have identified VoIP transport as being potentially insecure. While few offerings provide encryption of VoIP calls, this is a necessary option for addressing communication of sensitive information in an enterprise. Unencrypted voice conversations can be captured and later re-assembled into audible ".wav" files using freely available tools.

Availability

Availability is perhaps the most critical requirement for voice services. IP Telephony poses many challenges to ensuring availability that do not exist in a traditional voice environment. First, IP networks are vulnerable. The IP hosts and the network connections that feed them are susceptible to large floods of traffic or malformed datagrams. These attacks are meant either to saturate the connections or cause hosts and network elements to stop responding. IP Telephony's reliance on the IP network means that attacks at any point in the network can have a potentially negative impact on the availability of voice services.

Services like directory look-up and voicemail are examples of traditional functional components that now sit on IP-enabled networks. Not only are these elements exposed to attacks that could render them inoperable, but they also must be able to communicate successfully with other IP hosts to access critical supporting

services, e.g., e-mail or domain name system (DNS). In addition to server and network availability, the integrity of the data being housed, served, and accessed must be intact or service disruption may occur.

IP phones must sit on IP-enabled networks as well. If left unprotected, attackers may attempt to disrupt service using malformed datagrams or floods of traffic. IP Phones also must rely on the presence of several key network services for basic functionality. DNS, Trivial File Transfer Protocol (TFTP), and, often, Dynamic Host Configuration Protocol (DHCP) are essential underlying services that must be present. The lack of a functioning DNS or DHCP could render phone services inoperable for the duration of an outage. Rogue DHCP and TFTP server insertion represents powerful tools attackers can use to alter the flow of network data. Generally, this is associated with unauthorized data collection, but also can be a source of outages. The National Institute of Standards and Technology (NIST) suggests considering static IP address assignments that eliminate reliance on DHCP. It also recommends the use of more secure file and configuration management mechanisms when they become available for use with IP Telephony devices.

Power is an obvious requirement that must be addressed when taking measures to ensure service availability. The power requirements for customer premises IP Telephony equipment is greater than the requirements for traditional phone equipment since a larger number of devices must be supplied with power in the event of a power failure. Ensuring adequate back-up power often is overlooked when migrating to IP Telephony. Failure to adequately address this need may result in service loss during a power outage.

Network availability is crucial and assuring that network devices are powered and operational is only a small part of ensuring service levels. Universally, IP Telephony must be deployed on a Quality of Service (QoS)-enabled infrastructure. The purpose of QoS is to ensure special treatment for protocols or nodes on a network. IP phones are capable of marking datagrams with Layer 2 and Layer 3 indicators that signal the network that packets will require special treatment. Safeguards must be taken to ensure that datagrams with forged QoS markings do not trick the network into granting better per-hop behavior to nonessential data.

Fraud

Fraud is a concern in any voice environment. Unsanctioned resource use must be prevented since it can tie up valuable capacity as well as increase operating expenses. User name and password information must be safeguarded on client devices, network elements, and when in transit during login.

Security Recommendations

Network Segmentation

NIST recommends that customers separate data segments from IP Telephony segments. This strict separation has many benefits. First, it is much easier to enforce filtering and security rule sets on IP Telephony hosts when they comprise a well-defined group. This is advantageous when trying to create and enforce QoS, Security, and Intrusion Detection System (IDS) policies. The second and perhaps biggest benefit to segmenting the network is that it places IP Phones in a position where they are no longer subject to direct attacks from neighboring PCs. In a flat design, IP Phones might be attacked from neighboring PCs that were either compromised or infected. A flat network also would aid an attacker who might attempt to use a compromised PC to capture voice packets. Keeping networks logically separate makes this activity more difficult for an attacker to perform and hide.

Cisco IP Phones are capable of providing network access to a PC through a jack on the phone. This permits network operators to deploy only single cabling drops to each user. Fortunately, it is possible to configure the PC to be on a different virtual LAN (VLAN) than the one on which the phone resides. It also is possible to prevent the PC that is connected to the phone from marking datagrams with forged QoS indicators.

Soft Phone Clients

Installing a Soft Phone on a PC bridges the protective barrier that a segmented network would otherwise provide. Soft Phone usage requires the commingling of IP voice and IP data traffic in the same segment, increasing the risk of many types of security breaches. There also is no guarantee that the soft phone is installed on a clean, uncompromised PC. NIST recommends that Soft Phone clients not be used. Physical IP Phones run far fewer services than PCs and are less susceptible to attacks. Verizon VoIP does not officially support any Soft Phone usage.

Firewalls

Implementing firewalls and filters between network voice and data segments also is recommended by NIST. Firewalls provide a single point of focus for security policies. These policies define which resources have access to other resources and simultaneously provide an activity log. Firewalls can be stand-alone devices or incorporated into routers, VPN devices, or an IDS.

A firewall is strongly recommended for all Verizon VoIP configurations. Verizon VoIP installs and supports Session Initiation Protocol (SIP)-aware firewalls that are optimized for VoIP. The firewall filters the VoIP signaling based on the source address and only allows SIP messages that originate from Verizon Business's proxies to reach the IP phones.

We have certified several integrated routers that include firewall functionality, as well as a number of firewalls, for use on the Verizon VoIP network.

Customer IDS

Customer networks should be monitored for suspicious activity. NIST recommends the use of IDS on IP Telephony segments to alert network administrators in the event of anomalous or suspicious activity.

Client Authentication

To help ensure that calls placed on the Verizon VoIP network are from a trusted user, Verizon VoIP clients and servers support two forms of authentication depending on the customer premises equipment (CPE).

IP phones and Mediatrix use SIP Digest Authentication. Digest authentication uses the MD5 digest hash. Enterprise gateways for PBXs use IP Security (IP Sec) authentication header (AH).

Verizon Business sets the passwords on the IP phones before they are shipped. Telnet access is disabled to the phones for security because it is not encrypted. In 2005, Verizon Business deployed a CPE Manager in our network for secure upgrades, which will be the SMARTS in-charge system. If a customer desires, we can assist with setting up a TFTP service at their premises.

Encryption

Voice payload is not currently encrypted. Verizon Business is pursuing Internet Engineering Task Force (IETF) standards solutions to secure VoIP which includes SIPS (SIP over TLS) for session signaling and Secure Real-Time Transport Protocol (RTP) for the media data.

Verizon VoIP Infrastructure Security

Physical Access

Physical Access security is where security begins. All of our data centers require secure key access and are accessible only to authorized staff. Physical security is equally essential at our customers' locations.

Network Security

The Verizon VoIP data centers use server platforms that are selected to meet the strict high capacity and throughput requirements of our VoIP infrastructure. The data center infrastructure includes best-of-breed routers, switches, and firewall gear from companies like Juniper Networks and Cisco. All network equipment is hardened and all unnecessary services are disabled or removed. Access control policies are used to deny suspicious traffic.

Core Verizon Business servers are accessed via Secure Shell. Administrators must log in to a central server to gain access to any other server on the network. Radius provides a central point of control for username authentication. Centralizing this function eases management and improves Verizon Business's ability to enforce policies.

The SIP proxy servers are protected by redundant firewalls that protect enterprise infrastructure from a wide range of attacks. SIP servers use the Sun Solaris operating system selected for robustness and security.

Verizon Business Security Advantages

Verizon Business offers a comprehensive SLA for Verizon VoIP for many metrics that are critical to IP Telephony. These include jitter, Mean Opinion Score (MOS), latency, packet delivery, and network availability. We implement QoS on the networks on which Verizon VoIP is deployed. This makes it possible to meet these stringent performance demands by prioritizing IP Telephony signaling and media flows. When Internet Dedicated Access (IDA) is used in conjunction with the service, the Denial of Service SLA also is an included assurance offered to customers.

We have years of experience providing security solutions. We operate one of the most sophisticated network-wide IDS systems in existence within the cores of our networks that incorporate Distributed Denial of Service (DDOS) detection and suppression mechanisms. The Verizon VoIP product portfolio includes Hosted IP Centrex, which is designed to leverage Verizon Business's extensive IP infrastructure and PSTN interconnects. One of the key advantages to a hosted solution is that the infrastructure components living in our network and data centers are being guarded, monitored, and protected 24x7 by the systems Verizon Business has developed and implemented.

We actively assess our security posture and make adjustments to ensure we have taken the necessary steps to safeguard critical infrastructure. We implement message digest authentication with SIP, which means that actual passwords are never sent "in the clear," and we are involved with efforts to further enhance SIP to obfuscate in-transit data. Our SIP-aware firewalls help secure the perimeter and protect vital components without disturbing the functionality of the service and its ability to interact with ancillary components.

With premises based IP PBX solutions, often it is possible to implement safeguards and encryption between the handset and the IP PBX. The IP Trunking offering can integrate existing customer IP PBX deployments that already may use these safeguards. Verizon VoIP also supports hardware configurations that interface with legacy PBX and KSU equipment. This means that IP handset end stations are absent, along with the threat vectors associated with these devices. An example of this type of configuration is IP Integrated Access.

In support of the entire Verizon VoIP product portfolio, we also actively assess and certify software builds for IP Phones, routers, switches, Analog Telephone Adapters (ATAs), and firewalls. We follow the announcements of new security advisories and make changes to address threats as they become known.

Verizon VoIP customers can leverage the efforts and expertise associated with the portfolio's various offerings. The premises-based customer still will be able to take advantage of our infrastructure hardening and monitoring and premises device security testing. Centrex and Hosted customers will have far less to secure and monitor on their own due to the fact that a large percentage of the solution is comprised of hosted components under Verizon Business protection.

We deploy our VoIP services on QoS-enabled networks only. This helps ensure that the network will be able to deliver the required performance and service levels. SLAs specific to Verizon VoIP provide customers with the peace of mind that the infrastructure will be available and will perform as expected. A related function called Call Admission Control, or CAC, is an inherent feature of our VoIP offering, preventing the number of calls from exceeding the capacity of the links that have been deployed for each customer. Allowing the number of calls to grow beyond physical capacity would degrade the quality of all calls traversing a link.

Conclusion

Securing IP Telephony requires industry collaboration and leadership and Verizon Business has been instrumental in the development of IP Telephony standards and solutions, including security specifications. We were among the first members to join VOIPSA (VoIP Security Alliance) and we continue to work toward fulfilling the organization's charter.

With this level of industry involvement, Verizon Business has been able to add security strategically to our VoIP product sets. In addition, we are in a position to help raise security awareness specific to VoIP.

Verizon Business is a strong industry leader with many years of operational VoIP experience. These qualities make us one of the leaders in carrier-grade business VoIP solutions and a valuable source for VoIP security information.

References

Kuhn, D. Richard, Walsh, Thomas J., Fries, Steffen. (2005). Security considerations for Voice over IP systems—recommendations of the National Institute of Standards and Technology. Retrieved from <http://csrc.nist.gov/publications/nistpubs/800-58/SP800-58-final.pdf>.

