White Paper – Security Challenges in VoIP Systems

Michael Hristovski

ITEC495-Q1WW

Professor Wayne Smith

July 9th, 2017



Michael Hristovski

Security Challenges in VoIP Systems

**Table of Contents**

[Abstract 4](#_Toc487394056)

[Introduction 4](#_Toc487394057)

[Analysis of Security Threats 6](#_Toc487394058)

[Potential Solutions 9](#_Toc487394059)

[Cisco VoIP Security Model (SAFE) 9](#_Toc487394060)

[Nortel VoIP Security Model 11](#_Toc487394061)

[Criteria for Evaluating Potential Solutions 12](#_Toc487394062)

[Defense of a Potential Solution 13](#_Toc487394063)

[Conclusion 14](#_Toc487394064)

# **Abstract**

Over the last decade, Voice over Internet Protocol (VoIP) has become a popular choice for homes and even more so for business environments. VoIP has provided a cost-cutting solution that has become a viable option to replace the traditional public switched telephone network (PSTN) systems. VoIP offers scalable flexibility and advanced features over traditional PSTN systems, however, these benefits also come with additional security risks because of the merging of voice and data on the same network. The implementation of a VoIP system can provide an excellent return on investment for an organization if security countermeasures are in force to protect both the VoIP system and the network infrastructure that it relies on to function.

“Voice over Internet Protocol (VoIP) transmission began in 1973 as a result of the experimental Network Voice Protocol invented for the ARPANET. However, it wasn’t until 1995 that the first Internet Phone Software – Vocaltec – appeared.”

[VoIP History, N.D.]

# **Introduction**

VoIP technology has been available for quite some time, and the current versions are not hindered by garbled or dropped calls like in previous offerings. The technical aspects of how traditional PSTN systems operate in comparison to VoIP systems plays an important role in

understanding the importance of security. In a traditional PSTN system, voice calls use a technology known as circuit-switched telephony. Within a circuit-switched system, a dedicated channel is formed and maintained throughout the entire length of the call. Circuit-switched systems rely on copper wire to carry analog voice data over the dedicated circuits (The Difference Between VoIP and PSTN Systems, 2008). In contrast, VoIP telephony networks run on a digital-based technology and utilize a technology that is known as packet-switched telephony. Within countless network packets, the data is sent to its destination whether locally or across the internet. The main concept of VoIP is that it converts conversations into normal data that travels over the IP network, because of this VoIP presents its own unique security challenges along with that of a normal data network. Security must be viewed as a planning step when implementing a new system, and not as an afterthought to configure after the system is up and running. The proper method of security with VoIP systems as with any IT infrastructure involves layering of security, only in this manner can the systems be safeguarded against multiple threats to the organization.

“Individual packets may — and almost always do — take different paths to the same place. It's not enough to simply get VoIP packets to their destination. They must arrive through a fairly narrow time window and be assembled in the correct order to be intelligible to the recipient. VoIP employs encoding schemes and compression technology to reduce the size of the voice packets so they can be transmitted more efficiently.”

[The Difference Between VoIP and PSTN Systems, 2008]



**Figure 1: (Is Your Security Layered Like Your Bean Dip?, 2015)**

# **Analysis of Security Threats**

Each component in a VoIP system offers a potential threat for hackers to exploit. The exploits relating to the VoIP system itself are often like those of a traditional public switched telephone system. In a PSTN system, placing a device on the physical line will allow the attacker to eavesdrop on the conversation. Likewise, in a VoIP system, gaining physical access to the TCP/IP network will allow an attacker to place a device that will grab packets on the network which will intercept data which can be reassembled to listen to conversations. Gateway or areas of the infrastructure that are control mechanisms are often based on Windows or Linux platforms which present a vulnerability risk for the VoIP network segment to be attacked as well (Butcher,

D., Li, X., & Guo, J.,2007). VoIP systems usually experience security concerns that fall into three categories based consequences to a user confidentiality, integrity, and availability. Confidentiality concerns involve the exposure of conversations between the parties involved, but this could also mean the exposure of call data such as the length of the call or the telephone numbers involved. Integrity concerns involve trusting the identity of the caller, recipient, messages, voicemails, or call logs. Availability concerns interrupt normal usage of the system and may remove the ability to place or receive phone calls, voicemails, or messages.

**The following table represents common security concerns and their impact on a VoIP system.**

**Figure 2: (Butcher, D., Li, X., & Guo, J., 2007)**

By understanding the types of security concerns that organizations implementing VoIP services must plan for, it reduces the chance of a threat becoming a costly incident. DOS (Denial of Service) attacks are carried out to interrupt service for a short period based on reasons such as political agendas, revenge, defamation, prevent communications, monetary loss or used in the conjuncture of a larger attack forthcoming. Eavesdropping disregards privacy within a conversation and allows an attacker to monitor calls, fax’s, or even messages, with this advantage an attacker can obtain company secrets, credit card details, personal data, or any other sensitive information. Alteration of voice streams allows for the attacker to alter part of a conversation while listening to a call between two parties, with this exploit an attacker could commit fraud, such as using someone’s voice from a previous conversation to say “yes” to sign up for some service or credit card. Toll fraud has been a problem even since the days of circuit-switched systems and allows an attacker to trick a user into placing a call to a 900 number to force them into paying an absorbent amount of fees when they connect. VoIP includes a feature where you can redirect your main phone number to a cell phone or other specific number when you are away from your main line. Exploit of the Redirection of call feature can allow an attacker to redirect the initial phone call to a specific number of their choosing and give them a way to impersonate the victim for their gain. Accounting data manipulation occurs when an exploiter seeks to manipulate or read call logs inside the database. With this information, they

can see patterns of phone calls to predict business transactions or mergers, this data can also be manipulated to erase calls from the log to commit fraud or cover up criminal activity. Caller ID impersonation can allow an attacker to spoof a specific number of their choosing and then receive or make calls impersonating another person usually for the destruction of character or for monetary gain. Unwanted calls and messages have become a serious problem for everyone in today’s electronic environment. The problem first arrived with the popularity of email and has since found its way into telemarketing techniques. Attackers often utilize VoIP systems themselves to send out bulk voice solicitations using a list of phone numbers (Butcher, D., Li, X., & Guo, J.,2007).

# **Potential Solutions**

After deciding to switch from a traditional switched-circuit system to an onsite VoIP system it is important to select a security model that will be appropriate for the organization. Two security models are covered below including both Cisco and Nortel that will provide a multi-layered security solution for the organizations VoIP system and infrastructure.

## **Cisco VoIP Security Model (SAFE)**

Cisco is known for its reputation in data networks and offers an abundance of hardware for networking infrastructures. In addition to data, Cisco has moved into the VoIP market as well.

Below are the recommended security measures according to Cisco’s VoIP security model within SAFE (Security Architecture For Enterprise).

|  |
| --- |
| **Configure Dial Plans and User Profiles****Use features on your VoIP system that allow for more security.*** **Control voice network access by using device certificates along with usernames and passwords.**
* **Restrict the type of calls allowed on the network, by device, user, time of day along with other types of criteria.**

**Protect Your Voice Systems*** **Setup a firewall and intrusion prevention system (IPS) to monitor and filter authorized and unauthorized VoIP traffic and activities.**
* **Lock voice servers physically, and logically for administration. Use a centralized administration with domain restrictions and two – factor authentication for administrative access, including to credentials, signaling data, and configuration files.**
* **Regularly install OS updates, and limit software loading on phones.**

**Use VLANs to Segment Voice Traffic and Separate it from Data Traffic****Some voice systems and switches support device discovery protocols and automatically assign IP phones to voice VLANs.****Encrypt Sensitive Voice Traffic*** **Apply encryption to segment, device, or user; encrypting indiscriminately can result in excessive network latency or introduce operational overhead and complexity.**
* **Encrypt the signaling at your internet gateway with Session Initiation Protocol (SIP) over Transport Layer Security (TLS).**
* **Encrypt the media (packets) with protocols such as SRTP.**
* **Use VPNs for network connections by remote phones, especially when HTTPS or SRTP is unavailable.**

**Implement Strict Security Policies with Users*** **Communicate your phones’ built-in security features to users.**
* **Apply strong passwords to access the voicemail inbox.**
* **Delete sensitive voicemail messages when users are finished listening to them.**
* **Immediately report anomalies, such as saved voicemail messages that are missing or forwarded to an unusual number.**
 |

**[Figure 3: How to Protect Your Voice: Tips on IP Phone Security, 2016]**

## **Nortel VoIP Security Model**

**Nortel has switched its focus from switched circuit equipment and moved into the VoIP markets.** Nortel focuses its security model basis on the following areas of focus.

|  |
| --- |
| * Device authentication involving the MAC address security on all switches.
* Deployment of separate voice and data VLAN segments.
* Switches should also include intrusion detection monitoring.
* Voice segment should be reserved for IP phone handsets if softphones must be used then the PC’s running the softphone should be placed on the data segment and communicate to the voice segment through a VoIP-enabled firewall.
* Including a dedicated set of DHCP servers for the voice network to protect against DoS attacks due to address depletion. Static IP assignment should also be implemented based upon known MAC addresses.
* Nortel advises creating a secure voice zone using a stateful firewall. This acts as an application-level gateway supporting the SIP protocol.
* Wide Area Network IP phone traffic streams are encapsulated and encrypted inside IPSec tunnels to maintain integrity and confidentiality.
* Nortel also advises that all server’s configuration should be hardened and the removal of all unnecessary software, with the addition of OS patches and hot fixes regularly.
 |

 **[Figure 4: Nortel Security Model: Butcher, D., Li, X., & Guo, J., 2007]**

# **Criteria for Evaluating Potential Solutions**

Determining a solution for security for a VoIP system involves making sure the business is operating at full potential. A security solution that allows exploits or creates slowdowns in the systems is not beneficial to the company, therefore, a successful security solution should be graded on the following criteria.

* Calls are not interrupted or dropped by added security or encryption
* Features are not hindered by the added security
* Users can understand the added security measures such as user logins, passwords, and VPNs
* The organization is still seeing a positive return on investment with the added security measures
* The solution can be modified or upgraded as future threats become known

**Defense of a Potential Solution**

Cisco’s VoIP security model (SAFE) provides an in-depth solution utilizing the defense in depth strategy to cover all areas that are vulnerable to threats of would-be attackers. The security model provides detailed information on how you can take advantage of features incorporated with the VoIP system to help protect users and information from being exploited.

“In the Cisco SAFE, security is embedded throughout the network by following a defense-in-depth approach, and to ensure the confidentiality, integrity, and availability of data, applications, endpoints, and the network itself. For enhanced visibility and control, a rich set of security technologies and capabilities are deployed in multiple layers, but under a common strategy.”

[Cisco SAFE Reference Guide - SAFE Overview, 2013]

"By integrating Cisco SPA525G2 phones, we give the client a customized solution that implements SRTP based on the configuration file in their DHCP server that is associated with the phone's MAC address"

[How to Protect Your Voice: Tips on IP Phone Security, 2016]

Cisco offers many devices offering great security features to implement into your VoIP system. There are many models or standards to ensure security in a VOIP system, some offer similar guidelines when implementing security, however, Cisco offers a trusted reputation, products, and support that are used throughout organizations worldwide.

# **Conclusion**

There is a high demand for organizations to switch to a phone solution that can offer cutting edge features that integrate into applications that are already being used throughout the organization. VoIP offers these added features with additional cost savings after the initial return on investment. As with anything that increases features and productivity there becomes an added risk to an attacker exploiting these new features. Deciding on a multi-layered security solution can ensure that the organization's investment is safeguarded and protect against any costly attacks.

**REFERENCES**

Butcher, D., Li, X., & Guo, J. (2007). Security challenge and defense in VoIP infrastructures. IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), 37(6), 1152-1162.

Cisco SAFE Reference Guide - SAFE Overview [Design Zone for Security]. (2013, October 31). Retrieved July 09, 2017, from http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Security/SAFE\_RG/SAFE\_rg/chap1.html

How to Protect Your Voice: Tips on IP Phone Security. (2016, December 20). Retrieved June 25, 2017, from http://www.cisco.com/c/en/us/solutions/small-business/resource-center/do-business-better/tips-ip-phone-security.html

Is Your Security Layered Like Your Bean Dip? (2015, September 09). Retrieved July 09, 2017, from http://blog.thinknettech.com/is-your-security-layered-like-your-bean-dip/

Rahangdale, T. G., Tijare, P. A., Sawalkar, S. N., Balhare, Z. J., & Gulhane, V. S. (2014). An overview on security analysis of Session Initiation Protocol in VoIP network. IJRAT, 2(4), 190-5.

The Difference Between VoIP and PSTN Systems. (2008, May 9). Retrieved June 24, 2017, from http://www.webopedia.com/DidYouKnow/Internet/VoIP\_POTS\_Difference\_Between.asp

VoIP History. (n.d.). Retrieved June 24, 2017, from http://www.voipinsights.com/voip\_history.html

**RESPONSE TO REVIEWERS**

Unfortunately, I was only given two reviews on this white paper, I believe I was supposed to have had the input from 4 reviewers in total. Based on the two reviews I did get feedback on there wasn’t much for criticism.

Below is the criticism I did receive and how I chose to correct these issues:

* References title was not capitalized and centered
* I fixed this by capitalizing and centering
* Only 3 of the 5 references are cited within the paper
* Went back through the paper to verify references were cited, all were cited with 2 being used for quotation text boxes

I also took it upon myself to go back through and complete the following changes to enhance the document:

* Reworded some areas to offer more of a personal input rather than information straight from a citation, these sections were based on my Turnitin.com feedback
* Made another pass through the document to proofread for grammar, spelling, and sentence structure errors.
* Removal of excess information that isn’t vital to the paper to get the size of the document to the specifications of the assignment.
* Added additional references and citations