PUNE RESEARCH TIMES ISSN 2456-0960
AN INTERNATIONAL JOURNAL OF CONTEMPORARY STUDIES VOL 2, ISSUE 1

IP CONVERGENCE NETWORKS: VULNERABILITIES/THREATS AND COUNTERMEASURES

RESHMA PATIL
Assistant Professor
Poona College of Arts, Science and Commerce,
Camp, Pune (MS) **INDIA.**

FAHEEMUDDIN AHMED
Assistant Professor
Poona College of Arts, Science and Commerce,
Camp, Pune (MS) **INDIA.**

ABSTRACT

IP Convergence network used to sent voice, video and data over the network. But this new change has brought lots of challenges for the network professional to secure the critical Assets and Data in an organization. This paper presents the vulnerabilities or threats associated with the Internet Protocol (IP) Convergence Network and possible countermeasures for the same.

Keywords: *IP Convergence Network, Vulnerabilities, Threats and Countermeasures, Wired IP Network, Wireless Networks, Voice over IP (IP Telephony), Video over IP Systems*

INTRODUCTION

IP Convergence implies the carriage of different types of traffic such as voice, video, data, and images over a single network. The integrated network is based on the Internet Protocol (IP). [2] IP Convergence has the expertise to support your network and grow it as your business grows. From Local Area Networking performance to Wide Area Network connectivity IP Convergence is your one partner for your corporate network. [7]

The nature of business conversation has changed. Face-to-face meetings have evolved into conversations with multi-modal anytime, anywhere contextual interactions. E-mail has given way to instant messaging, online presence and social media. And while globalization is expanding the reach of enterprises, restrictive travel fees are forcing them to embrace the new communication tools for doing business. With computer tablets and smart phones, nearly everyone carries always-on connectivity with them wherever they go. For a company to be competitive in this ever-changing environment, it needs to evolve its IT infrastructure to support these applications and devices and the ever-increasing user demands that dynamically

change based on which application or service is needed at any given time. The introduction of virtualization technology into the enterprise, such as desktop virtualization, pose new challenges for IT infrastructure. [1]

Components of a Converged IP Network

There are four major components of IP Converged Network

1. **Wired IP Network**

   An **IP network** is a communication **network** that uses **Internet Protocol** (**IP**) to send and receive messages between one or more computers. As one of the most commonly used global **networks**, an **IP network** is implemented in Internet **networks**, local area **networks** (LAN) and enterprise **networks**.

2. **Wireless Networks**

   Wireless networking is a method by which homes, telecommunications **networks** and enterprise (business) installations avoid the costly process of introducing cables into a building, or as a connection between various equipment locations.

3. **Voice Over IP** (IP Telephony)

   Voice over Internet Protocol (VoIP), is a technology that allows you to make **voice** calls using a broadband Internet connection instead of a regular (or analog) phone line.

4. **Video Over IP Systems (**Video Surveillance and Video Conferencing)

   Professional **video over IP** systems use some existing standard **video** codec to reduce the program material to a bit stream (e.g., an MPEG transport stream), and then to use an Internet Protocol (**IP**) network to carry that bit stream encapsulated in a stream of **IP** packets.

Vulnerabilities/Threats of IP Convergence Networks

Vulnerablites: A weakness in an information system or service that can be exploited by a threat. [9]

Threats: The potential cause of a risk. [9]

Countermeasures: A risk treatment implemented to reduce the likelihood and/or impact of a risk. [9]

Publicly available standard is used as base for protocol in Internet Protocol (IP) so detail information of the operation is available to everyone. As it is available to everyone it has lots of vulnerabilities

Vulnerabilities/Threats	**Countermeasures**
Customer can get access to the network elements by guessing administrator passwords	Passwords should use a combination of (at least three) alpha, numeric, upper and lower case, and if allowed, special characters Sufficient Length. Passwords should be at least 6 to 8 (preferably 8) characters. As a general rule, the longer the password, the more difficult it is to crack Awareness. Password policies should be formalized and well communicated to users so they are aware of acceptable password practices
Techniques like SNMP can be used to gain access about configuration details and revision levels	Network elements should be immediately updated to a security notice of network equipment vendor.
Registration Spoofing	Stronger Authentication Install software patches Use scanning tools like Sivus
Internet Service Theft	Change the default username and password of administrator Change password frequently Update security patches when vendor release it Block SNMP access Use two factor authentication to protect dial up access to console port
Proxy Impersonation	Stronger Authentication Install software patches Use scanning tools like Sivus
Call Hijacking	Stronger Authentication Install software patches Use scanning tools like Sivus

Caller ID Spoofing	Do not trust caller ID at all.
VoIP signaling and media Denial-of-Service Attack	Use strong authentication
Physical Denial-of-Service Attacks	Strict physical security schemes should be implemented with restricted areas, access control, locks, guard, etc.
Eavesdropping	Encryption of voice message packets
Virus Attack	
Lack of policies and procedures	To ensure your policies and procedures are effective a security audit is necessary

Conclusion

The vulnerable network is facing lots of challenges today. New devices brings are not in control of the IT team so increases security risk. New real-time applications, such as VoIP, video and collaboration suites push legacy networks to their limit, yet are fast becoming essential tools for organizations. New smart devices only increase the pressure on bandwidth, making it increasingly difficult for network managers to predict bandwidth consumption. This paper shows the potential vulnerabilities or threats to associated with the Internet Protocol (IP) Convergence Network and also presented possible countermeasures for the same. Implementing the countermeasures in Internet Protocol (IP) Convergence Network help organization to protect their information's assets reduce vulnerability and threats related to security.

REFERENCES

1. Ian Zahorujko, Alfred Reynolds and Bill Blair, "IP Convergence in Global Telecommunications - Voice over Internet Protocol (VoIP)", DSTO Electronics and Surveillance Research Laboratory, September 2000
2. http://www.bestpricecomputers.co.uk/glossary/ip-convergence.htm
3. http://www.excitingip.com/743/network-convergence/
4. http://searchtelecom.techtarget.com/feature/Service-provider-security-IP-convergence-requires-constant-vigilance
5. Jianqiang Xin, "Security Issues and Countermeasures for VoIP", SANS Institute 2007
6. Steven Sullivan, "Securing a Converged Network"
7. "IP Convergence", http://ipcnv.com/services/data-security/
8. "All-of-Government Risk Assessment Process: Information Security", February 2014
9. Information Systems Audit and Control Association (ISACA) (2009). Certified Information Systems Auditor (CISA) Review Manual 2009. ISACA: Rolling Meadows, IL.