Comparison of VoIP and TETRA Regarding Security in a Safety Critical Environment

Georgios Velianitis*, Kareem Adel, Sabrina Kotrba, Bindosh Paul Manavalan
University of Applied Sciences FH Technikum Wien, Vienna, Austria.

* Corresponding author. Tel.: +43 6648273646; email: wi15m060@technikum-wien.at
Manuscript submitted March 21, 2017; accepted June 29, 2017.
doi: 10.17706/jcp.13.3.279-286

Abstract: In this document we will analyze security threats on VoIP (Voice over IP) and TETRA (Terrestrial Trunked Radio) solutions and mitigation techniques, if applicable.

Key words: Availability, safety, security, TETRA, VoIP.

1. Introduction

In our modern world we need communications to keep ourselves updated, connected and aligned with our personal lives and business. Communication is considered a Mission Critical System for Safety-Critical Industries (Port Terminals, Maritime Business, Airlines, Security, Construction etc.) and public services (Fire Fighting, Police, Ambulance etc.). The most common methods for communication in safety-critical environments are Radio Communication (UHF – Ultra High Frequency, VHF – Very High Frequency), peer-to-peer and TETRA (Terrestrial Trunked Radio), which is based on Server-client method and also enables extra features like tracking devices, private communication, applications for notifications or alarm, etc. Tetra is most commonly used for group communication using a push-to-talk feature. VoIP (Voice Over IP) communication is also used for one-to-one calls in a fast and cost efficient way. It depends on the call manager server (Private) or the VoIP server (Internet public) like MS Skype for business; on client part it could be a physical IP phone or just a desktop or web app.

Security threats on Tetra or VoIP in Safety-Critical environments are not just a cyber-security issue, they may even cause death in crisis situations. This paper will analyze the threats and vulnerabilities of both communication solutions and will compare the countermeasures focusing on confidentiality, integrity and availability.

Confidentiality means that the information cannot be accessed by unauthorized parties. The confidential information of end users includes private documentation, financial information, security information like passwords, conversion content, conversion history or patterns etc. The confidential information for network components includes operation systems, IP addresses, protocols used, address mapping, user records, etc. Leak of this information might make attackers' job easier [3].

Integrity of information means that information remains unaltered by unauthorized users. A legitimate user may perform an incorrect or unauthorized operations function and may cause delirious modification, destruction, deletion or disclosure of switch software and data. An intruder may masquerade as a legitimate user and access an operation port of the switch.

Availability refers to the notion that information and services are available for use when needed. VoIP

network is susceptible to denial of service (DoS) attacks since DoS attacks can degrade Quality of Service (QoS) quickly to unacceptable level [5]. Traditional DoS attacks against data networks are still very dangerous. However, our focus is on VoIP specific DoS attacks.

2. VoIP (Voice Over IP)

The security concerns of VoIP telephone systems are similar to those of any Internet-connected device. This means that hackers who know about these vulnerabilities can institute denial-of-service attacks, harvest customer data, record conversations and compromise voicemail messages. The quality of internet connection determines the quality of the calls. VoIP phone service also will not work if there is power outage and when the internet connection is down. The 9-1-1 or 112 service provided by VoIP phone service is also different from analog phone which is associated with a fixed address. The emergency center may not be able to determine your location based on your virtual phone number. Compromised VoIP user account or session credentials may enable an attacker to incur substantial charges from third-party services, such as long-distance or international telephone calling.

The technical details of many VoIP protocols create challenges in routing VoIP traffic through firewalls and network address translators, used to interconnect to transit networks or the Internet. Private session border controllers are often employed to enable VoIP calls to and from protected networks. Other methods to traverse NAT (Network Address Translation) devices involve assistive protocols such as STUN (Session Traversal Utilities for NAT) and Interactive Connectivity Establishment (ICE).

Many consumer VoIP solutions do not support encryption of the signaling path or the media, however, securing a VoIP phone is conceptually easier to implement than on traditional telephone circuits. A result of the lack of encryption is that it can be relatively easy to eavesdrop on VoIP calls when access to the data network is possible. Free open-source solutions, such as Wireshark, facilitate capturing VoIP conversations.

Standards for securing VoIP are available in the Secure Real-time Transport Protocol (SRTP) and the ZRTP (Z and Real-time Transport Protocol) protocol for analog telephony adapters as well as for some softphones. IPsec is available to secure point-to-point VoIP at the transport level by using opportunistic encryption.

Government and military organizations use various security measures to protect VoIP traffic, such as voice over secure IP (VoSIP), secure voice over IP (SVoIP), and secure voice over secure IP (SVoSIP). The distinction lies in whether encryption is applied on the telephone or on the network or both. Secure voice over secure IP is accomplished by encrypting VoIP with protocols such as SRTP or ZRTP. Secure voice over IP is accomplished by using Type 1 encryption on a classified network, like SIPRNet (Secret Internet Protocol Router Network). Public Secure VoIP is also available with free GNU programs and in many popular commercial VoIP programs via libraries such as ZRTP.

2.1. Confidentiality

2.1.1. Eavesdropping of phone conversation

Conventional telephone eavesdropping requires either physical access to tap a line, or penetration of a switch. With VoIP, opportunities for eavesdroppers increase dramatically because of the large number of nodes in the path between two conservation entities. If the attacker compromises any of these nodes, he can access the IP packets flowing through that node. There are many free network analyzers and packet capture tools that can convert VoIP traffic to wave files. These tools allow the attackers to save the conversation into the files and play them back on a computer. VoMIT (Voice over Misconfigured Internet Telephones) is an example of such a tool. Ethereal can also be used to record Session Initiation Protocol (SIP) packets and retrieve voice messages in wav file format [3].

2.1.2. Unauthorized access attack

Unauthorized access means that the attacker(s) can access resources on a network where they do not have the authority. Shawn Merdinger reported multiple undocumented ports and services in certain VoIP phones. There are also vulnerabilities due to implementation issues.

There are systems for call control, administration, billing and other voice telephone functions. Repositories in these systems may contain passwords, user identities, phone numbers, and private personal information. Lots of gateways and switches are shipped with default well-known passwords. If these passwords are left without changes, the attackers can easily break in. Some switches still use TELNET (Telecommunication Network) for remote access. The clear-text protocol exposes everything to anyone who can sniff the network traffic. Some of the gateways or switches might have a web server interface for remote control. The attacker might sniff the HTTP (Hypertext Transfer Protocol) traffic in local network to steal sensitive information. Attackers can also use ARP (Address Resolution Protocol) cache poisoning to forward all traffic through their machines to capture network traffic.

2.1.3. Countermeasures

Encryption of voice message packets can protect against eavesdropping. IPsec (Internet Protocol Security) can be deployed to encrypt whole packets. SRTP (Secure Real-time Transport Protocol) can provide confidentiality, message authentication and replay protection for audio and video streams.

For better protection for gateways and switches, one should use SSH (Secure Shell) instead of other clear-text protocols as remote access protocol. If web-based interface is provided, HTTPS (Hypertext Transfer Protocol Secure) should replace HTTP. In addition, all default passwords should be changed before the system is plugged into the network. An up-to-date intrusion detection system might detect ARP poisoning and other types of attacks.

2.2. Integrity

2.2.1. Caller ID (Identification) spoofing

It is the practice of causing the telephone network to indicate to the receiver of a call that the originator of the call is a station other than the true originating station. For example, a Caller ID display might display a phone number different from that of the telephone from which the call was placed. The term is commonly used to describe situations in which the motivation is considered malicious by the speaker or writer.

2.2.2. Registration hijacking

Registration hijacking refers to a situation where an attacker replaces the legitimate registration with a false one, thereby causing inbound calls to go to a nonexistent device or another SIP device, possibly including a rogue application. For example, an attacker could route the CEO's calls to their internal IP phone.

2.2.3. Proxy impersonation

Proxy impersonation occurs when an attacker tricks one of your SIP User Agents or proxies into communicating with a rogue proxy. If an attacker successfully impersonates a proxy, he has access to all SIP messages and is in complete control of the call.

2.2.4. Countermeasures

Unfortunately, there is no effective way to prevent caller ID spoofing. The best solution so far is not to trust caller ID at all. Stronger authentication schemes are the solutions to registration spoofing, proxy impersonating and call hijacking. To mitigate this type of attacks, software patching is crucial to fix any known vulnerabilities. VoIP vulnerability scanning tools like SiVuSrtp are strongly suggested.

2.3. Availability

2.3.1. VoIP signaling dos attacks

The attackers can abuse signaling protocol to conduct denial of service attacks. In most cases the attackers can create large number of call setup requests that consume the processing power of the proxy server or terminal.

2.3.2. VoIP media dos attacks

Attackers can flood gateway, IP phone and other media- processing VoIP components with large number of RTP (Real-time Transport Protocol) packets. If the target is forced to drop RTP packets, the voice quality will be degraded.

Moreover, the attacker might knock key components like gateway offline. A failure in one of these devices could bring the entire voice network to a halt. Since RTP is encapsulated in UDP (User Datagram Protocol), it is easy to crack.

2.3.3. Physical dos attacks

These attacks include power outrage and physical damage to network components. Traditional telephone operates at 48 volts supplied by the telephone line itself and can operate smoothly during a power failure. VoIP cannot operate without power supply. Besides, an attacker with physical access to any key components of VoIP network can disrupt its normal operations easily. He can plug out the power cord or network cable.

2.3.4. Countermeasures

To mitigate VoIP signaling and media DoS attacks, strong authentication is the key. VoIP components need to make sure that they are communicating with legitimate counterparts. VoIP firewall should also be implemented to monitor streams and filter out abnormal signals and RTP packets [1]. Media and signal rate limits can be set by observing normal traffic patterns. To mitigate physical DoS attacks, strict physical security schemes should be implemented with restricted areas, access control, locks, guard, etc. To guarantee continuous power supply, backup power generation system should be available.

3. Tetra (Terrestrial Trunked Radio)

The area of TETRA security is extensive; as it needs to provide different levels of security ranging from what is acceptable on commercial networks to what is acceptable on a national public safety network. The security mechanisms in the standard are covered through Authentication, Air Interface Encryption (AIE) and End to End encryption. The threats to Confidentiality, Authenticity, Integrity, Availability as well as Accountability are covered with those three mechanisms [2].

The standard based services are constantly being expanded by a sub-group of the Association - Security and Fraud Prevention Group (SFPG).

Mutual Authentication is a service required to ensure that a TETRA system can control access to it and for a radio terminal to check if a network can be trusted. In TETRA, as in most other secure systems, authentication is the basis for much of overall network security and can also be used to ensure validated billing in public access systems, and can provide the foundation for a secure distribution channel for sensitive information such as other encryption keys. The mutual authentication security mechanisms protect both Voice and Data services [4].

The TETRA standard supports four AIE TETRA Encryption Algorithms (TEAs), these being TEA1, TEA2, TEA3 and TEA4. There are differences in the intended use and the exportability of equipment containing these algorithms. For example, TEA2 is intended for use by public safety users in Schengen and related European countries only; the others have wider applications ranging from general commercial use to public safety use in regions where TEA2 is not used [6]. The main benefit of over the air encryption is that it protects all signaling and identities as well as user speech and data. This provides an excellent level of protection from traffic analysis as well as from eavesdropping. The encryption system is closely bound to

the TETRA signaling protocols and the algorithms can (if desired) be implemented as software within radio terminals and base station equipment, instead of using encryption modules, which could consume space and increase cost.

The TETRA standard also supports End to End encryption using a variety of encryption algorithms as deemed necessary by national security organizations. The TETRA Association Security and Fraud Prevention Group has extended the work carried out in the TETRA standard to define a general framework for the incorporation of End to End encryption. Recommended sample solutions have also been provided for the International Data Encryption Algorithm (IDEA) (IPR - Intellectual Property Rights owned by Ascom) and the newer Advanced Encryption Standard (AES) algorithm (IPR free), which benefits from a larger cryptographic algorithm block size. Custom and indigenous algorithms are also possible with End to End encryption, although these are not recommended for air interface encryption due to their need for integration in signaling protocols and availability of standard compliant terminals.

Besides these cores security capabilities TETRA can also support a wide range of security management capabilities such as those used to control, manage and operate the individual security mechanisms in a network. The most important of these is Encryption Key management, which is fully integrated in TETRA standard functions. Even though security functions are integrated in a network this does not automatically imply that a network is fully secure. However, what is normally achieved is that the security risks are "condensed", that is they are concentrated to specific elements in the network, which can be adequately controlled.

Further countermeasures:

- Channel coding
- Error correction
- Protocols with detection and retransmission capability
- Data recovery mechanisms
- Periodic registrations
- Fault tolerance

4. Attacks and Breaches

Pindrop Security, one of the leading providers of Caller Anti-Fraud and Authentication for Enterprise Contact Centers, estimated an increase of 45% of Call Center Fraud since 2013. Moreover, 1 in every 2,000 calls proved to be fraudulent, while fraud losses have increased 14% in the last 2 years [7].

In order to identify Fraud Risk Factors, companies are advised to implement multi-layered solutions that quickly and accurately detect fraud. They should look for solutions that offer comprehensive protection across the entire call center infrastructure, including both IVR and live agent. Call centers should understand their expected fraud exposure and average loss.

The UK has had chip card technology for many years. This has resulted in a doubling of fraud rates and more attacks originating domestically. As physical card security in the US increases, US call centers should expect to see a spike in call center fraud.

In 2015, enterprises lost an average of $0.65 to fraud per call. This means a call center that receives 40 million calls per year should expect to see somewhere between $17 million to $27 million in fraudulent transaction losses annually. Phone fraud losses have grown 14 percent since 2013, when the average loss was $0.57 per call. According to a recent survey by the Aite Group, 72% of contact center executives expect this fraud loss trend to continue on an upward trajectory, almost doubling in the next five years [8].

Voice over IP (VoIP) phones are the fraudster's first choice of devices when it comes to making fraud calls. In the past year, 16 percent of legitimate callers used a VoIP device, yet 42 percent of fraud callers did so.

This number has remained relatively steady over the past five years. In the US, VoIP calls are cheap or free, making them popular choices for fraudsters. VoIP calls are also difficult to identify. This is because it is very easy to spoof a Caller ID number with VoIP. Adding to this confusion, VoIP calls are typically routed through multiple carriers onto the PSTN network, making them hard to trace and prosecute.

The VIPROY VoIP Penetration Testing and Exploitation Kit and the Viproxy MITM Proxy and Testing Tool by Fatih Ozavci have been widely used and demonstrated in several security conferences including Black Hat (USA, Europe), Defcon, Troopers, Hack in the Box, Ruxcon and AusCERT.

The Viproy VoIP Pen-Test Kit provides penetration testing modules for VoIP networks. It is developed for security testing of VoIP and Unified Communications services. Viproy has Skinny, SIP and MSRP (Message Session Relay Protocol) libraries to develop custom security tests, as well as PoC (Proof of Concept) security testing modules.

The Viproxy MITM Proxy and Testing Tools is developed using Metasploit Framework environment. It is a standalone Metasploit module which enables users to intercept the TCP (Transmission Control Protocol)/TLS (Transport Layer Security) traffic and to execute some attacks against thick client applications, mobile applications and VoIP clients. Viproxy can be used to attack the Microsoft Lync and Skype for Business environments as demonstrated during the VoIP Wars: The Phreakers Awaken in Black Hat USA 2016 and VoIP Wars: Destroying Jar Jar Lync presentation at Black Hat Europe 2015, GSEC Hack In The Box Singapore 2015 and Ruxcon 2015 events. Viproxy also has an online rule console to manage the attacks including INVITE subject update, MESSAGE content update and sending invalid content for fuzzing.

As recently reported by the Slovenian online newspaper DNEVNIK, a student named Dejan Ornig managed to identify security-related weaknesses in the Tetra protocol, which facilitates encrypted communications and is widely used by national authorities including the Police, Intelligence and Safety Company (SOVA), Jail administration and the military. Back in 2012, Ornig started working on the Tetra implementation with his 25 colleagues. This was basically one of his school projects. In 2013, September, he identified that the protocol that is being used countryside has been misconfigured by the Slovenian authorities. It was identified that the Tetra implementation wasn't encrypting data that was being transmitted for at least 70% of the time, which obviously was leading to severely damaging consequences if allowed to run like this. Therefore, the student reported this discovery.

However, much to his surprise, the authorities didn't respond in a way that he had expected. So, Ornig decided to disclose this finding to the public in March 2015. When this was done, the authorities fixed the Tetra implementation issues, however, they started harassing the student. Ornig was charged with hacking the Government network on three different times in 2014, in February, March and December respectively.

5. Safety

Speaking to Safety supervisors in one of the busiest Terminal operators, they recommended using Tetra as it is built for emergency communication with loud speaker and immediate push-to-talk required to avoid accidents. Using Tetra base stations between Tower controllers, Quay Crane, Deck & Warf is critical for safety operations.

A VoIP application could be used between tower and RTG (Rubber Tyred Gantry) cranes as communication between RTG cabinet and Tower office suitable for private communication like VOIP phone or app.

6. Security

Resources in Security and government authorities prefer Tetra Radio Communication for its high availability and lower risk than commercial use or private use VOIP applications. To create a security attack

on Tetra communication you have to own special equipment and almost it will be a terrorist attack not a normal hacker like in VOIP case.

7. Conclusion

We recommend Tetra for safety critical environments like vessel and port terminal operations, Airports and government emergency authorities. Any place using Tetra should have a backup plan or plan B in case of unsolved attack or disaster. Backup could be using VOIP app, GSM (Global System for Mobile communications) with push to talk feature and many other applications can be used. VoIP can be used mainly in private communication with taking all security countermeasures into action to mitigate risks on Confidentiality, Integrity and Availability.

References

[1] Dowland, P. S., & Furnell, S. (2007). Advances in networks, computing and communications. *VoIP Security Threats and Vulnerabilities,* 114–122.
[2] Toikkanen, R. (2007). TETRA workshop: Understanding TETRA security. *TETRA Association.*
[3] Xin, J. (2007). Security issues and countermeasure for VoIP. *SANS Institute.*
[4] Collier, M. *The Current State of VoIP Security*. San Antonio: Secure Logix Corporation.
[5] Ma, A. (2001). *Voice over IP (VoIP).* California: Spirent Communications.
[6] Bolle, M. (2014). Overview of standard TETRA cryptographic algorithms and their rules for management and distribution*. TCCA SFPG Secretariat.*
[7] (2016). *Call Center Fraud*. (Report No. 3, 14). Pindrop Labs.
[8] Inscoe, A. (2016). *Contact Centers: The Fraud Enablement Channel*. Boston: Aite Group LLC.

Georgios Velianitis was born in Athens, Greece. He received the bachelor's degree in computer engineering from the Technological Educational Institute of Athens, Greece in 1990.

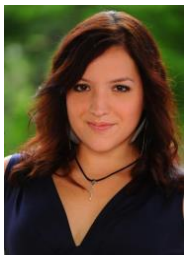
He has worked as the head of technology and security operations for Laiki Bank and as applications supervisor for Georgia-Pacific Hellas SA. He is currently employed as IT support specialist at SCA Hygiene Products GmbH in Vienna, Austria.

Currently, Velianitis is pursuing a master's degree in the University of Applied Sciences FH Technikum Wien, Vienna, Austria. His main research interests include IT service management software and business intelligence.

Kareem Adel was born in Port Said, Egypt. He received the bachelor's degree in systems & computers engineering from Al-azhar university in Cairo – 2007.

He has professional certificates in technology field like CCNA, CCNP, MCP, OCP, VCP, CEH (Certified Ethical Hacking v.7), COBIT 5 foundation and ITIL foundation. He is currently working as a IT projects & governance team leader for maersk-APM terminals in port said east port. He led and contributed in many projects as ISMS – ISO27001 implementation, IT infrastructure upgrade, advanced threat prevention implementation and build tetra infrastructure.

Eng. Kareem is currently completing his master's degree at the University of Applied Science Technikum Wien in Vienna. His diverse interests include project management, IT management, innovation management and cyber security.



Sabrina Kotrba was born in Vienna, Austria. She received the bachelor's degree in project management & IT from the University of Applied Science bfi Vienna.

She is currently working as a project manager for both internal development projects as well as customer projects on the design and implementation of safety critical communication systems in a marine environment (mainly GMDSS and port management sytems) at Frequentis AG in Vienna, Austria.

Kotrba is currently completing her master's degree at the University of Applied Science Technikum Wien in Vienna. Her diverse interests include project management, IT management, software development and business development.

Bindosh Paul Manavalan was born in Kerala, India. He received the bachelor's degree in information technology from Sikkim Manipal University, India and received the second bachelor's degree in informatics and computer engineering from Tomsk Polytechnic University, Russia.

He started his IT career as a freelancer, continued his international career with United Nations (UNCCD) and is currently working at United Nations Framework Convention on climate change (UNFCCC). He has professional certificates in technology fields like microsoft certified trainer (MCT), microsoft technology specialist(MCTS), microsoft certified IT professional, COBIT 5 foundation and ITIL foundation.

Bindosh is currently pursuing his master degree at the University of Applied Science Technikum Wien in Austria. His diverse interests include project management, IT infrastructure management, innovation management and cyber security.