Exploring the human dimension of TETRA

Nico Pieter Fouché
Institute of ICT Advancement
Nelson Mandela Metropolitan University
Port Elizabeth, South Africa
s207057396@live.nmmu.ac.za

Dr. Kerry-Lynn Thomson
Institute of ICT Advancement
Nelson Mandela Metropolitan University
Port Elizabeth, South Africa
Kerry-Lynn.Thomson@nmmu.ac.za

Abstract—In order to secure communication, in the year 55 BC, Julius Caesar developed the Caesar cipher to ensure his generals on the battle field received critical information in the most secure manner possible. Today, the protection of critical information and communication is just as vital.

Police officers, fire marshals and emergency medical units require critical information to make decisions that could mean the difference between life and death. Just as in the Caesar era, the information is intended for a particular recipient and can lead to devastating consequences if intercepted or received in a malformed state. Security of these communications should be of utmost importance. One of the threats to security is Social Engineering, which is commonly deployed in computer networks. However, Social Engineering need not be limited to computer networks.

Terrestrial Trunked Radio (TETRA) is a standard intended for secure professional digital mobile radio communication, designed for use by government agencies, emergency services, transportation services and various other users in need of secure communication. TETRA is seen as a very technically secure standard, making use of authentication keys and air interface encryption amongst other techniques.

Even though TETRA is technically secure, are the TETRA users safe from Social Engineering? This paper will investigate the potential of Social Engineering on a TETRA system. Further, the various vulnerabilities and possible escalation scenarios that could occur if TETRA users are not made aware of Social Engineering will be explored.

Keywords-component; Information Security, Social Engineering, Terrestrial Trunked Radio (TETRA)

I. INTRODUCTION

The security of digital networks is of grave importance in the society we live in today. Our networks are under constant attack in attempt to gain information. Organizations have information they must protect, which is often described as its lifeblood. Different organizations have different information to protect, for example, banks have the financial information of customers. The information is the responsibility of the bank and must be protected at all times. An attacker could attempt to gain access to various levels of the bank's network to gather information and could target the least protected area of the network to acquire the information wanted. As a protector of information all possible scenarios of exploitation must be considered in order to protect against it. Computer networks are being used in almost all organizations today, so the security is under massive pressure to be kept up to date. In the context of computer networks security, it is often said that nothing is 100 percent secure and according to Mitnick, even the most technically secure computer networks (e.g. CIA, FBI, MIT) can be cracked with knowledge in human manipulation [1]. Similarly to computer networks, radio networks also have sensitive information that needs to be protected, whether it is being stored or transmitted. Further, in a radio network that is being used for public safety and security, for example, a breach in confidential information could be devastating.

II. TETRA

One communication standard that ensures the secure transmission of data over radio is the Terrestrial Trunked Radio or TETRA standard. TETRA is a digital radio network that conforms to the requirements of a Professional/Private Mobile Radio (PMR) category system. Traditional PMR networks use an analog form of communication. TETRA provides digital improvements in the form of integrated voice and data communication and the sharing of a single network by multiple users. TETRA is a digital two-way transceiver, using Time Division Multiple Access (TDMA) to allow multiple encrypted speech channels for communication and can be both point-to-point and point-to-multipoint, while allowing digital data transmission [2].

TETRA is currently in use by organizations all around the world. Germany has a nationwide adoption of TETRA for the police, fire brigade, ambulance and coastal guard under the organization

BOSNET. The United Kingdom is almost complete with the full roll out of TETRA networks for the police, fire brigade, emergency services and armed forces under the organization Airwave. Further, CONNECT is a TETRA network currently being used for transportation services in London. According to the 2010 figures compiled by TETRA association, networks using TETRA are found in 118 countries around the world. In South Africa, TETRA was used by the Eastern Cape Police for secure digital communication, and to ensure public safety and security, in the Nelson Mandela Bay Stadium during the FIFA 2010 Soccer World Cup.

TETRA is a European Telecommunications Standards Institute (ETSI) standard, which has considered previous mobile communication standards and, as was mentioned, is used extensively throughout the world. The standard allows for a wide spread adoption, creating many uses for TETRA; however this paper will focus on the aspect of public safety and security.

A. ATETRA Network

As mentioned, TETRA is a suite of standards that cover various aspects of a digital network, like air interfaces, network interfaces and the TETRA services and facilities. Figure 1 illustrates these aspects in a common TETRA network, as found in the TETRA Release 1 information from TETRAMOU, an association of TETRA specialists.

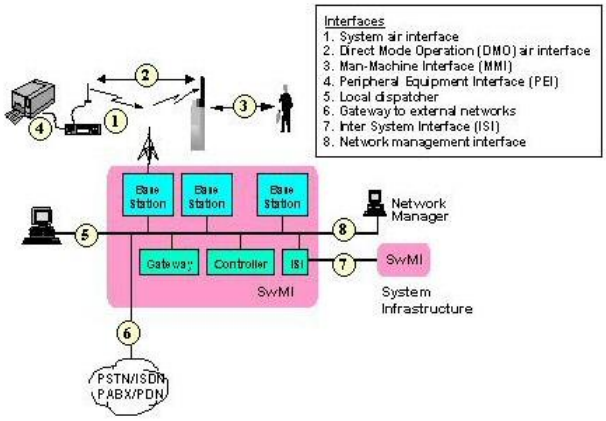

Figure 1. TETRA Network Overview [3]

The first aspect to consider is the Switching and Management Infrastructure (SwMI). SwMI is used to classify all the equipment and sub-systems in a TETRA network. The SwMI includes Base Stations (BS), Gateways, Controllers and Inter System Interface (ISI). The SwMi also has interfaces to the Network Manager, local dispatchers and external Public Switched Telephone Networks (PSTN). The ISI enables inter-operation between other SwMI's. The BS provides air interfaces between the SwMI and the TETRA terminals, although the terminal can have its own optional air interface with another terminal in Direct Mode Operation (DMO). Number 4 in Figure 1 indicates Peripheral Equipment Interface (PEI), which standardizes the connection of the radio terminal to an external device. PEI supports data transmission between applications installed on the device and the connected TETRA terminal. Local dispatchers are commonly found in a dispatcher center, indicated by the number 5 in Figure 1 [3].

Dispatchers can monitor, record, terminate, join and initiate calls to users with TETRA terminals. In addition, dispatchers can monitor the location of TETRA terminals and also make a forced call to a terminal that will not ring or notify the user of the terminal, allowing the dispatcher to listen in on the terminal. A dispatcher will typically receive an emergency call from TETRA users in an emergency and can patch them through to relevant emergency services if needed. Through the network discussed above, TETRA provides critical information for the services we depend on in society, namely the public safety and security services.

B. TETRA Adoption

Training facilities can be found all around the world, but currently the only facility found on the African continent is at the Nelson Mandela Metropolitan University. INTEGCOMM and EADS Defense & Security invested in a brand new top class infrastructure at the university, which is used for the various courses of training on campus and for The SAPS Eastern Cape TETRA Project. The mentioned project aims to equip the Eastern Cape of South Africa with the latest TETRA technology for improved secure digital communication for police officers. The facility for training is known as the TETRA Academy, which is the first and only of its kind internationally, that offers TETRA training in collaboration with a Higher Education institution.

The courses include various aspects, for example System Course, End User System Course, Dispatcher Workstation and Base Station. The courses stretch from understanding how the TETRA system works to educating dispatchers how the system operates and assisting technical staff with being responsible for commissioning and maintaining the TETRA Base Stations in the network. The above mentioned training educates students to transfer critical

information safely and securely over the TETRA network [4].

It must be noted that the TETRA training mentioned above is of a technical nature and teaches users of TETRA how to operate various equipment.

C. Security

As discussed in previously, the communications over a TETRA network are typically of a crucial nature for public safety and security. Therefore, these communications must be secured. TETRA provides security through Confidentiality, Integrity, Authentication, Availability and Accountability using Mutual Authentication, Air Interface Encryption (AIE) and End to End encryption. Mutual Authentication is a service that allows the TETRA system to control access to the network. A TETRA Subscriber Identity Module (SIM) can be used to uniquely identify terminals, providing control of which terminals may access the TETRA network. Another important service addresses the encryption of communication between the TETRA radio devices is AIE. AIE ensures that communication over the 'air', for example, from dispatcher to terminal, is encrypted. AIE supports four different TETRA Encryption Algorithms (TEAs), namely TEA1, TEA2, TEA3 and TEA4. The AIE protects all signaling and identities, including user speech and data [5].

TETRA also supports End to End encryption using a variety of encryption algorithms that are specified by the organization. TETRA provides recommended solutions for organizations in the form of International Data Encryption Algorithm (IDEA) and the newer Advanced Encryption Standard (AES) algorithm for End to End encryption. TETRA also provides a wide range of security management capabilities to control, manage and operate the individual security mechanisms in a network [5].

Therefore, TETRA is considered very technically secure as the actual data is intrinsically very well protected as it is transmitted. However, there seems to be very little research or focus on the human dimension of TETRA.

III. HUMAN DIMENSION OF SECURITY

For most organizations, the protection of information assets is of vital importance. In order to secure information assets, various controls are used. Controls are typically identified as being physical, technical or operational. Physical controls include the use of patrolling guards, security gates and locks and provide physical protection. In order to bypass physical controls the employees must provide necessary identification or keys. Physical controls allow for very little room for exploitation when implemented properly. The next category of controls identifies devices that provide technical controls for information. Technical controls usually have physical controls to protect them. A simple example is the use of a firewall to prohibit unauthorized entry via technology from remote destinations. The last category of controls considers the human dimension in daily operation, namely operational controls. Organizations can develop education, activities or policies to attempt to control the human aspect of information [6]. Mitnick proved to the US Congress that he could often obtain passwords or other pieces of sensitive information by just asking for it. Mitnick explains that he used various forms of persuasion and manipulation over telephone lines to exploit the most technically advanced security systems. Security is only as secure as the weakest link; and the human dimension is often considered the weakest link [1].

A. Social Engineering

Social Engineering is often used to exploit this human dimension. Social Engineering is a non-technical form of intrusion that relies heavily on social interaction. A person that exercises Social Engineering is considered a hacker. Like any other person, a hacker shares the human goals of money, social advancement, and self-worth [7].

Social Engineering uses the power of persuasion and manipulation to divulge sensitive information that a victim believes should be provided to the hacker. Typically, a Social Engineering victim does not realize he/she has been hacked until a good while later. The following subsections will describe some of these techniques identified by Microsoft's whitepaper [7] as can be related to Mitnick's work [1].

Intimidation

The attacker impersonates an authority figure in the relevant organization or a superior in an organization (e.g. officers of the law). Intimidation proves as an easy way to force a target to comply with the request by using mild threats.

Persuasion

Persuasion is the act of influencing a target by means of argumentation or false reasoning. This technique requires good

experience with social interaction to detect the hidden agenda of the attacker.

Ingratiation
This technique is based on a longer term attack, where the attacker forms a relationship with the victim to gain trust and encourages the victim to eventually divulge information.

Assistance
The social engineer attempts to assist the victim. The notion of assistance can build a short term relationship between the hacker and victim, resulting in information vulnerability. The hacker uses that vulnerability to divulge information.

The techniques listed above are just a few of the more common examples of the many techniques a social engineer could use to obtain unauthorized information [7].

B. Exploitation through Social Engineering

Social Engineering is a very real threat in Information Technology and there are many examples of Social Engineering attacks where information has been compromised. Below are examples of Social Engineering attacks relevant to the techniques identified in the previous sections; *intimidation, persuasion, ingratiation* and *assistance.* Consider an organization with an Information Technology (IT) Helpdesk. The IT Helpdesk is a taskforce that specializes in troubleshooting problems in computing and related software to the organization. This taskforce, perhaps unknown to the employees, has a lot of sensitive information available about the fellow employees. A hacker can intimidate the employees at the helpdesk by claiming to be a superior. The hacker can then request information by threatening the employee's occupation. A sensitive or perhaps new employee, who has been trained to be helpful and friendly, will feel obliged to provide the expected information and will then be unknowingly hacked. This is a common form of *intimidation* Social Engineering.

The mentioned IT Helpdesk can also be the target for a *persuasion* Social Engineering attack. The hacker can physically approach the helpdesk under the guise of an employee in the building. Through various clever forms of argumentation or even a sympathetic approach the hacker could persuade the helpdesk employee into resetting an account for the hacker. Alternatively, the hacker may telephone the helpdesk employee and use *persuasion* techniques to acquire information. In many cases, all the hacker requires is a name and surname which could be acquired through an easily obtained company telephone directory.

A rather difficult form of Social Engineering is the use of a long term plan, as a lot more dedication is required from the hacker. This attack is known as the *ingratiation* Social Engineering attack. Consider a hacker that applies for a janitor position at a company, forming relationships with fellow colleagues over a short period of time, for example two to three months. The hacker now has a good relationship, causing the hack to be a lot easier. A friend will assist a colleague that is having trouble with logging into the network, for example. A friend will also allow a colleague to be alone in a room while cleaning it, as the relationship includes trust, allowing the hacker to complete his hidden task of compromising the network.

When a person is assisted with a problem, they usually become thankful. A short term relationship is then formed between the two people that interacted in solving the particular problem. A hacker can pose as a person who may assist you in your problem, which in turn provides the hacker with the upper hand when attempting to hack information from the person in need. For example, a hacker could purposefully cause a network or computer issue and then contact the affected person to offer assistance in fixing the issue. When the hacker contacts the person again and asks them to download a program for his/her computer, for example, the person will be more inclined to assist the hacker.This is a form of *assistance* Social Engineering attack.

The examples described can all be related to IT environments, but the techniques used are not solely meant for hacking IT environments. The following examples will attempt to sketch scenarios in TETRA networks that could have happened during the FIFA 2010 Soccer World Cup at the Nelson Mandela Bay Stadium with the South African Police.

The dispatcher center is normally a room filled with dispatcher stations and dispatchers. Dispatchers control and monitor various calls in the network, for example an emergency call from a South African Police (SAP) officer will be immediately answered by a dispatcher and required services will be notified, be it emergency medical units or even the fire brigade. This room is filled with information about TETRA subscribers and external services. A hacker couldassume the guise as a chief technical advisor

with a legitimate looking TETRA badge and tailgate his way into the room. The hacker could then *intimidate* a dispatcher into relieving their position behind a dispatcher station, allowing the hacker to complete the hidden task.From the dispatcher workstation, the hacker could compromise many areas of the TETRA network, and consequently public safety and security. For example, the hacker could acquire the location of specific TETRA terminals or even install intelligent software code to compromise the dispatching station remotely. Control over a dispatcher's computer can be considered as the ultimate compromise in a TETRA network, as the consequent scenarios are limitless in terms of exploitation.

The FIFA 2010 Soccer World Cup generated a lot of job opportunities for various services during the tournament. The tournament required an increase in officers for public safety and security. New employees in various occupations pose as an advantageous target for Social Engineering hackers, as a slight increase in emotion is expected in the new environment. This could result in a slightly pressurized environment for the new officers, more-so as an influx of people locally and from all over the world was expected. A hacker can easily use *persuasion* Social Engineering attack on these new officers, allowing him to collect a TETRA handheld terminal that is live on the network.

A similar scenario to the IT *ingratiation* can be used for TETRA. As mentioned, during the FIFA 2010 Soccer World Cup many new employees were hired. A hacker could have easily become, for example, a janitor. Clever placement could land the hacker in the same building as the new TETRA dispatching center, allowing him unrestricted access. The hacker can also form relationships with other new employees, resulting in a considerable easier hack at the cost of a bit more time.

As mentioned previously, the FIFA 2010 Soccer World Cup welcomed an increase in various job opportunities. Similarly to the IT *assistance* Social Engineering attack, a hacker can attempt to assist one of the new SAP officers with potential technical issues on their TETRA terminal. On agreement of the newly appointed SAP officer, the hacker is allowed to inspect the terminal by possibly plugging it into a laptop for "closer inspection". TETRA terminals have a Subscriber Identity Module (SIM), which forms part of the technical security in TETRA and is physically located in the terminal. This provides authentication to the TETRA radio network and will allow the hacker to exploit the network once copied or stolen after assisting the new SAP officer with inspection of his terminal.

C. Social Engineering Awareness in TETRA

Many computer networks are considered very technically secure. These computing networks have the latest devices to ensure security, for example Cisco ASA firewall products to prohibit unauthorized remote access and hardware encryption modules for superior confidentiality inside the network. As discussed earlier, Social Engineering has been used to exploit users of computing devices. Therefore, the original target of exploiting the network has shifted from attacking technical security controls to the users of the computing network in order to bypass highly sophisticated security techniques.

Similarly, TETRA digital networks address the needs of the PMR users, providing security services such as End to End encryption, Mutual Authentication and Air Interface Encryption. TETRA is a technologically secure form of communication, with little room for technical exploitation. Further, just as hacking in the computing environment has largely shifted from technical hacking to Social Engineering; it can be argued that a TETRA environment could be subject to the same Social Engineering issues.

In computer environments, Social Engineering Training and Awareness is often used to attempt to educate users about typical Social Engineering attacks for increased security of computing networks. As has been mentioned, TETRA training and education focuses primarily on the technical aspects and usage of TETRA networks. It can be argued that, just as Social Engineering Training and Awareness is needed in a computing environment, so too does TETRA training require a focus on Social Engineering Training and Awareness.This would attempt to ensure the users of the TETRA networks are aware of potential Social Engineering attacks, which could ensure public safety and security.

IV. CONCLUSION

Even though a TETRA network is considered technically secure, it is vital for the users to be aware of potential Social Engineering attacks. Social Engineering in a TETRA network could potentially lead to confidential information being compromised and, consequently, compromise public safety and security. In order to protect the network against Social Engineering attacks, the users of the network must be educated. Therefore, a Social Engineering

Training and Awareness program should be developed and tailored specifically for TETRA users.

REFERENCES

[1] Mitnick, K. D., & Simon, W. L. (2002). *The Art of Deception: Controlling the Human Element of Security*. United States of America: Wiley Publishing, Inc.

[2] Stavroulakis, P. (2007). *Terrestrial trunked radio - TETRA: a global security tool.* Berlin: Springer.

[3] TETRA. (2011). *TETRA Release 1*. Retrieved May 1, 2011, from TETRAMOU: http://www.tetramou.com/tetramou.aspx?id=1181

[4] Nelson Mandela Metropolitan University. (2011). *TETRA ACADEMY: Educating the Workforce of a Networked Economy* [Brochure]. South Africa: Nelson Mandela Metropolitan University.

[5] TETRA. (2011). *TETRA Security*. Retrieved May 1, 2011, from TETRAMOU: http://www.tetramou.com/tetra_print.aspx?id=1184

[6] Whitman, M. E., & Mattord, H. J. (2003). *Principles of Information Security.* Canada: Thomson Course Technology.

[7] Microsoft. (2006). *How to Protect Insiders From Social Engineering Threats.* Retrieved April 14, 2011, from Microsoft Download Center: http://www.microsoft.com/downloads/en/details.aspx?FamilyID=05033E55-AA96-4D49-8F57-C47664107938&amp%3Bdisplaylang=en