International Journal of Computer Science and Business Informatics

IJCSBI.ORG

Framework for Threat Modelling for a Power Utility: Case of Zimbabwe Power Utility Company

Samuel Musungwini, Gilbert Mahlangu,
Beauty Mugoniwa, and Samuel Simbarashe Furusa
Computer Science and Information Systems
Faculty of Science and Technology
Midlands State University
Gweru Zimbabwe

ABSTRACT

The purpose of this study was analyse threats that are inherent in the prepaid electricity meter system and to propose a framework for threat modelling. This framework can be effectively used by power utilities power utilities in particular and other prepaid meter system organisations to achieve end-to-end actionable insights on prepaid electricity metering infrastructure. The study used a qualitative case research methodology with a single unit of analysis. A purposive sampling technique was used to select suitable participants. Data was collected from power utility engineers and security experts using semi-structured interviews and focus group in order to triangulate the research findings. The findings of the study indicated that at the present moment there are very few frameworks that can be explicitly used to model threat to prepaid electricity infrastructure. This has exposed the infrastructure to various attacks such as physical bypass, cyber-attack and mechanically induced attack. We therefore recommend the adoption of an explicit framework for modelling threat in prepaid metering infrastructure.

Keywords

Threat modelling, cyber attack, electricity theft, framework, ICTs, Mobile technologies.

1. INTRODUCTION

The prepaid metering infrastructure is one of the most vital components of the electricity grid system (Hämmerli, Svendsen & Lopez, 2013), because it is the dominion of revenue collection for the power utilities. Its installation within the electricity grid system has transformed electricity from the "right to use" into a cash commodity which is one of its paramount characteristics.

This has provided significant benefits to the power utilities, which include maximising revenue collection, minimising cost associated with revenue collection, reduced consumer debt on electricity usage, supplying purchased electricity only, reduction in incorrect electricity billing, etc. (Miyogo, Ondieki, & Nashappi, 2013). With the prepaid electricity metering infrastructure, customers are now able to purchase electricity tokens from various designated points such as power utility's revenue halls and other vending kiosks (Pabla, 2008). However, the installation of prepaid electricity metering infrastructure to the consumer premises presents different threats that have left it exposed/vulnerable to attack (Tondel, Jaatun & Line, 2012).

An attack is an unwanted action that utilizes one or more vulnerabilities to which when performed, it has the paossibility of compromising the purpose of the installed infrastructure (Ucedavelez & Partner, 2012). In this case, the purpose of the prepaid electricity metering infrastructure is to ensure that consumers pay for electricity before use in order to reduce consumer debt, among other reasons. The attack on prepaid metering infrastructure which come in various forms and from different sources has seen power utilities around the world losing millions of dollars through electricity theft. This has negatively impacted revenue streams and backward operations of these utilities.

2. BACKGROUD

In Zimbabwe, a prepaid electricity metering system was launched in 2012 for both domestic and commercial consumers to replace the conventional post-paid meters and estimation billing (Megawatt Bulletin, 2012). The concept of prepayment is built around paying before using a product or service. Prepayment systems provide a disbursement for goods and services before consumption or use (Casarin & Nicollier, 2010). In the context of electricity distribution, the aspect of prepayment calls for the consumers to hold electricity credit on their accounts (Miyogo, Ondieki & Nashappi., 2013). The consumer can only use electricity as a commodity or service when the account is paid up in advance.

The power utility has managed to install more than 900 000 prepaid electricity meters for both domestic and commercial consumers by now (Sibanda, 2014), with important applications already laid out and usable. However, the installation of prepaid electricity metering system has seen the power utility being deprived of millions of dollars by the consumers who have found ways to steal from prepaid electricity meters. The power utility is losing about US$10 million a month in revenue from electricity theft (Share, 2014). Electricity theft has also seen the country experiencing more loads shedding than ever in recent months, because the power utility cannot

raise enough revenue for continuous electricity generations. The system was introduced without proper feasibility study to check the polarity of the prepaid electricity meters, hence, the consumers tampering with the system.

The power utility has reacted to electricity theft by introducing a Revenue Protection Unit (RPU) to conduct field inspections/checks, investigate and report consumers engaging in electricity thefts. Farawo & Towindo (2013) reported that the power utility now offers monetary incentives as a way to persuade consumers to provide information about electricity theft. Since it is laborious to monitor all the 900 000 and more prepaid electricity meters to be installed by means of field checks/inspection, there is need to protect the system and ensure the security of the installed infrastructure (prepaid electricity meter) so as to yield projected revenues for the investments made.

Although, electricity theft has been in existence since the 20th century, the introduction of the prepaid metering system world over which have transformed electricity into a cash commodity has seen perpetrators adopting "smart" ways or methods of stealing electricity (Sreenivasan, 2011). Some of these methods are so complicated that they cannot be easily detected by the current methods being employed by the power utilities. For example the use of infra-red programming and micro-processor programming techniques to alter electricity billing registers.

Therefore power utilities need to model threat to the prepaid electricity metering infrastructure for them to figure out appropriate ways of combating the attack. Threat modelling increases awareness of threat in order to prepare for the security of the defined system. The threat should be modelled so that all the possible attack strategies could be addressed using appropriate mitigation methods. The process of identifying and discovering vulnerabilities in an infrastructure requires awareness of the access points, threats and their exploitations in achieving an attack goal (Zhang & Xu, 2006).

3. RESEARCH PURPOSE

The purpose of this study was to propose a unique and specific framework for threat modelling that can be used by power utilities in an effective manner to achieve end-to-end actionable insights on prepaid electricity metering infrastructure. This study was guided by the following objectives:

- Evaluate and analyse various models/frameworks used in threat modelling.
- Determine the steps and processes used in threat modelling.

- Establish vulnerabilities, threats and attack strategies in prepaid metering infrastructure.
- Identify sources of threats and types of attackers in prepaid metering infrastructure.
- Provide guidance for further inquiry ito threats prevention.

4. OVERVIEW OF THREAT MODELLING

Threat modelling is a method used by many security experts and professionals to investigate security incidents and vulnerabilities in information systems and infrastructure. According to (Microsoft, 2012), the method involves identifying the infrastructure that needs protection from attack and the potential threats to that infrastructure, classifying the threats and finding mitigation strategies in a structured process. It is a practice which serves as a organised approach in creating models that define, detect and foretell threats to a given infrastructure in an organisation (Mcgrath & Lennon, 2013). It encompasses the appreciative of the complexity of the infrastructure and identifying all possible threats that may affect its purpose of deployment and use (Zhang & Xu, 2006). Threat modelling can be conducted before the deployment of the infrastructure as a preventive measure or after the deployment as a way of maintenance.

The main factors covered in threat modelling should include identification of what to be secured (system characterising), what an attacker may do (threat), weaknesses (vulnerabilities) that gives the attacker intrusion capabilities and the potential damages (Williams, 2007). The goal of threat modelling is to identify and build possible threats and vulnerabilities to the infrastructure in order to increase the security awareness of the organisation and come up with adequate mitigation strategies. To further elaborate on threat modelling, Ciampa (2009) cites that the objective of threat modelling is to understand the goal of the attacker, the attacker himself, types of attacks and the possible strategies that may be used to attack the infrastructure. The modeller should study components like who is the threat, where and how is it likely to occur and the vulnerabilities of the infrastructure. Therefore, instead of relying with continuous discovery mechanism, organisations can use threat modelling to mitigate and defeat the attack scenarios before they fully develop (Hardy, 2012).

5. PRESENT APPROACHES TO THREAT MODELLING

The capability of an organization to respond to the emerging threats to their infrastructure can be seen as a journey rather than a destination (Excellence, 2013), since attackers always aim to be ahead of the frameworks and models

currently in use. Various frameworks and models have been used to model threat to the infrastructure by different organisations. Some are simple and ease to use by non-experts in the field of security while others are complicated and require special skills and knowledge. These include, among many the Threat Logic Tree, Attack Tree-Model, Game Theoretic Model, PASTA model and Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) framework. This study only looked at the Attack Tree-Model, OCTAVE and Microsoft Security Development Lifecycle (SDL) Threat Modelling. The decision to choose these models is because ATM and Microsoft Security Development Lifecycle (SDL) Threat Modelling have been used before to model threat in Advanced Metering Infrastructure (AMI) and their concepts complement each other in threat identification and evaluation. Although OCTAVE is yet to be used in AMI and other metering infrastructure in electricity grids, its consideration was based on the fact that it focuses on balancing operational risk, security practices, and technology (Zhang & Xu, 2006), which is central to this study.

5.1 Attack Tree-Model

This one of the first modelling techniques developed by Schneier (1999). The model takes the form of a tree in demonstrating the attack whereby the attack goal is the root node while the leaf nodes represents the steps to be taken to accomplish the attack goal. It is a schematic mode of depicting how attacks can occur to the infrastructure whereby the root node represent the ultimate goal of the attack while leaf nodes represent the various ways an attacker can use to achieve the ultimate goal (Ucedavelez & Partner, 2012). The leaf nodes are decomposed until they reach a state where further decomposition is no longer possible. Leaf nodes also represent the condition(s) which must be fulfilled to accomplish successive goals or the ultimate goal of the attack. This technique has been used to define attacks against various information infrastructures and other real-world applications. The technique has gained its popularity in computer science and information systems research. It has been widely used by a number of organisations to model threats to information technology and non-information infrastructure. However, this model focused on either classifying threats or modelling the behaviour of the attacker using one specific factor which is the intrusion scenario. This has resulted in the limited scope of the attack discoveries and mitigation strategies. There is a need to extend the concepts covered in previous models to address factors like threat rating, priorities, countermeasures and protection strategies.

5.2 OCTAVE framework

OCTAVE is an approach that aims to increase the decision making process of protection and management of organizational resources (Marek & Paulina, 2006). It is intended to allow people to comprehend the security matters of the organizations and work towards improving them with least exterior assistance. It is underpinned on the philosophy and the principle of self-direct which states that people from the organization are in a better position to decide on the security of their resources. Thus, it provides a systematic and context-driven approach for the organization to manage threats to infrastructure. This technique studies, both technical and organisational issues in order to portray the security needs of an organisation using a three phase approach (Bakari, 2007) as indicated in Figure 2.

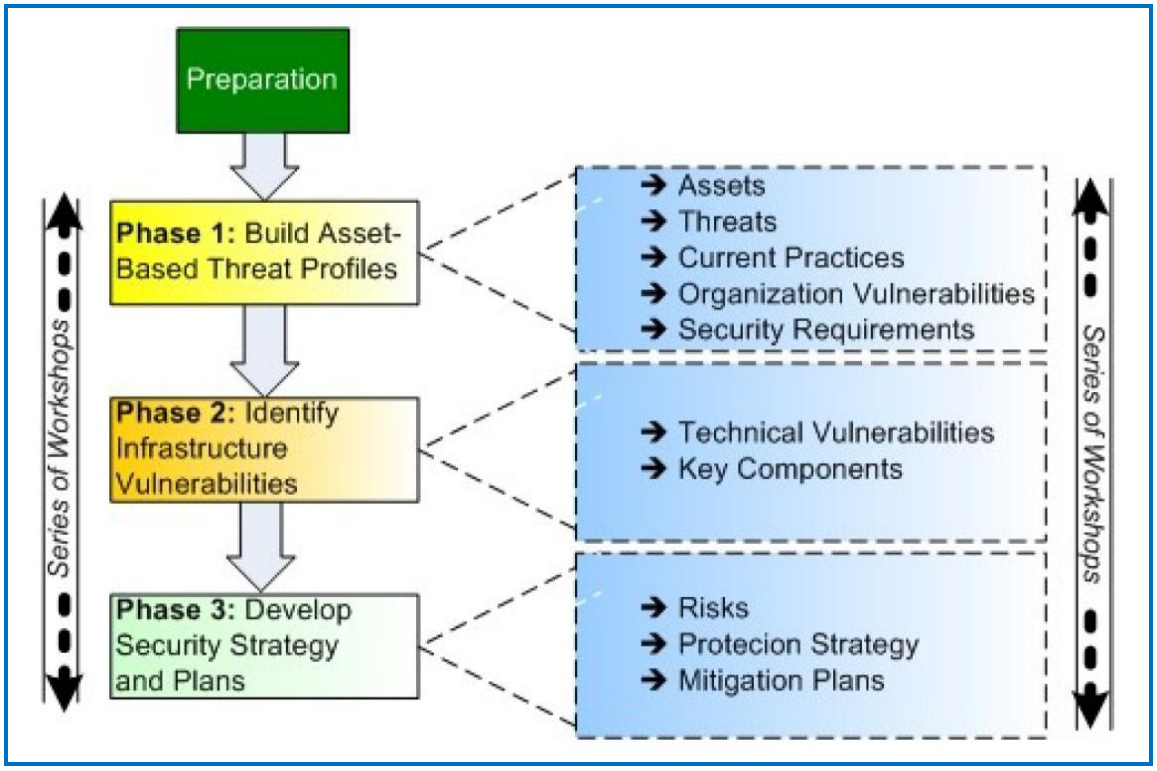

Figure 1: The OCTAVE framework

Source: Marek & Paulina, 2006

As shown in Figure 2, the major components of the OCTAVE framework are Building of Asset-Based Threat Profiles, Identifying Infrastructure Vulnerabilities and Developing Security Strategy and Plans. Within each phase, various processes and activities exist. The other factors that are covered in these three phases though not visible include information gathering, characterising the assets/infrastructure, describing threats and

current mitigation strategies/plans and establishing security requirements. The OCTAVE framework has presented the foundation and guidelines for many organizations to deal with various threats. Although the OCTAVE framework covers major factors for threat modelling, it focuses more on information infrastructure. Therefore, there is a need for an improved framework that will encompass the physical infrastructure that is deployed external to the organization such as the prepaid electricity meter.

5.3 Microsoft Security Development Lifecycle (SDL) model

This model has been used in conjunction with the ATM in modelling Threat in Advanced AMI by Tondel et al. (2012) in designing Demo Steinkjer conceptual framework. It is based on two categories which are Threat overview and Attacker strategies.

5.3.1 Threat overview

In classifying threat to the AMI, Tondel et al. (2012) used a STRIDE model which is a borrowed concept from Microsoft to aid the modeller in categorizing the threat. The model is concerned with determining the access an attacker may have to the data (spoofing) as the meter communicates with the back-end system, access to the configuration settings of the meter (information disclosure) such as billing registers and communication link in order to tamper with the billing cycle and the elevation of privileges remotely or physically.

5.3.2 Attack strategies in AMI

These can be identified through information gathering from various sources and presented together with their goals and the ways to achieve them. In order to carry out an attack, the attackers need to have knowledge of the power utility's communication grid topology and meter configurations. In addition, access is also necessary to plan the attack. Some of the attack strategies identified by Tondel et al. (2012) include:

- Manipulating power measurement (physically)
- Manipulating measurement values
- Manipulating messages from the meter
- Physical break-in
- Break-in via infra-red port

6. PROCESSES/STEPS IN THREAT MODELING

The processes and steps to be followed in the threat model differ according to the framework/model used. Although frameworks and models use different processes/steps, they all intend to achieve a common goal that is to provide guidelines in dealing with threats and attacks to the infrastructure (Bertino, Martino, Paci, & Squicciarini, 2010). Figure 3 shows a six (6) step-process model proposed by Meier et al. (2003) in their study on *"Improving Web Application Security"*.

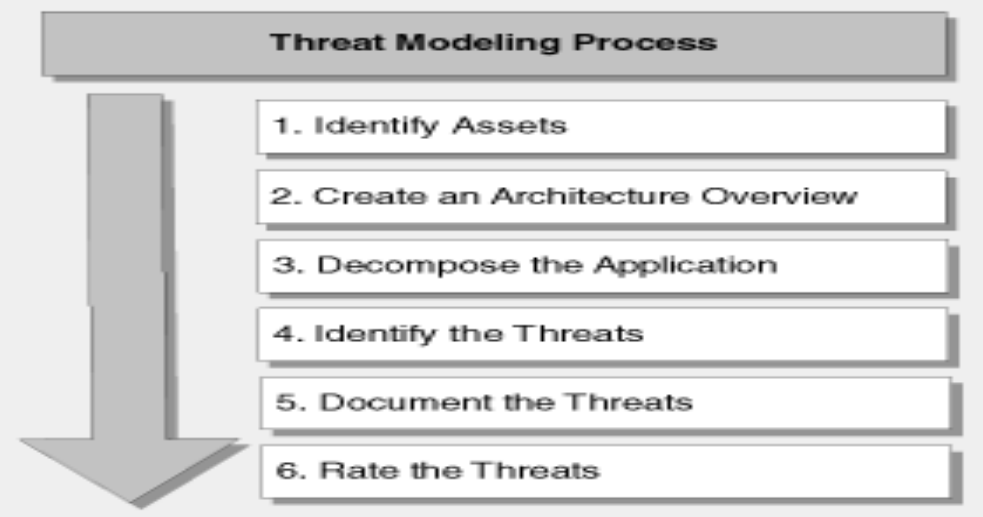

Figure 2: Process in threat modelling

Source: Meier et al. (2003)

6.1 Identify Assets

The major reason why threat and attacks exist is the availability of assets/infrastructure in the organization. Therefore the goal of the attacker is to gain access to a particular asset/infrastructure of interest and perform an attack. Asset/infrastructure identification involves the classification of critical/vital infrastructure or systems that an organization has to protect/guard against attack. Sub-processes may include describing why the asset/infrastructure needs to be protected and determining access points available for the attack to be possible (Burns, 2005).

6.2 Create an architecture overview

The goal here is to identify the key functionalities, the characteristics and the people served by the asset/infrastructure. It can be represented by Data Flow Diagrams (DFDs), tables and sequence diagrams to document the system and its subsystems. End-to-end deployment scenarios should also be specified so that threat identification in step 4 becomes easy. Therefore, the

more the modeller has knowledge about the key functionalities, characteristics and the people served by the asset/system, the easier it is to find threats and determine vulnerabilities

6.2.1 Decompose the application

In order to focus the attention of threat modelling to the areas of concern, the architecture should be divided into sub components. This is the third step that provides an illustration of the boundaries of the asset to help define the parameters of threat modelling.

6.2.2 Identify the threats.

A threat is a potential occurrence that can compromise the asset/infrastructure. For it to occur, they should be a target asset/infrastructure and a vulnerable point. In performing threat modelling, the modeller should use a systematic approach to discover all vulnerabilities of the asset/infrastructure that an attacker can be exploited to achieve the goal. They should be identified in view of the goals of an attacker, knowledge of the asset and potential vulnerabilities to the asset. It can be identified by using the attack trees, STRIDE model during a brainstorming session or just using the knowledge of the asset to list the ways in which the attacker can achieve the goals.

6.2.3 Document the threats.

A template can be created and used to document each based on certain attributes. Some of the attributes include threat description and threat target. Other attributes may include the attack techniques which may show the vulnerabilities exploited. This is the final stage of threat modelling.

6.2.4 Rate the threats.

The threat should be rated by assigning the probabilities of damage should they occur. This enables the organization to give priority to the most risk threats since it is not possible and economically viable to address all the threats. The threat should be rated in accordance to the risk they pose to the asset/infrastructure and its severity. It can be rated using the damage potential, reproducibility, exploitability, affected users and visibility.

7. METHODOLOGY

A qualitative case research methodology (Yin, 2014), with a single unit of analysis was used in this study to collect data from various sources. The

unity of analysis in this study was a power utility which has installed prepaid metering infrastructure. A purposive sampling technique was used to choose participants from the target population. The sample of this study was comprised of six (6) electrical engineers who have worked in the power utility for more than three (3) years. Data was collected from both the power utility engineers and security experts using semi-structured interviews and focus group, respectively in order to triangulate the research findings and evaluate the framework

8. FINDINGS AND DISCUSSION

8.1 Comparative analysis of available frameworks and models

This study commenced with an extensive literature review to establish the current frameworks and models used in threat modelling by various organisations. Although a number of them exist, the study found that most of the frameworks and models are directed at solving threats on IT and physical infrastructure that is located within the organisation. The frameworks and models reviewed in the literature and presented in Section 2 have limited capabilities in dealing with the threat to organisational infrastructure that is deployed in the front-end like the prepaid electricity meter. Apart from focusing on addressing threats to internal systems and infrastructures, it can be argued that the Attack-Tree Model and the Microsoft Security Development Lifecycle (SDL) model are not suitable enough for threat modelling. These approaches only assist the organization to identify ladders and routes an attacker can use to reach the goal.

8.2 Vulnerabilities, threats and attack strategies

The findings of the study have presented the landscape for the authors to understand vulnerabilities, threats and attack strategies to the prepaid electricity metering infrastructure. The prepaid metering infrastructure is highly vulnerable to attack because the attacker has unlimited physical access since they are located in consumer premises. Therefore, when an organisation is carrying out threat modelling to infrastructure it should consider the sources of threats, types of attackers, the level of access they have and the skills of the attacker. According to the findings of the study, prepaid metering infrastructure is vulnerable to three types of threats. These are:

- Threat to wiring integrity- this can be exploited through partial and wholly bypass whereby the cable can be either diverted from the service line to the load or the prepaid electricity meter is totally disconnected from the electricity grid system. Here the attacker uses a physical bypassing strategy. This is the easiest strategy that an

attacker can be used because no skill is required to exploit the threat. The attacker only needs to be brave and an understanding of the wiring integrity of the prepaid electricity meter. The attacker may use two approaches which are visible and non-visible approach. In the former the bypassing is done outside the prepaid electricity meter while in the latter bypassing takes place inside the meter. The goal is to divert the flow of electricity from the service line to the load so that electricity consumption is not measured.

- Threat to billing software embedded in the prepaid electricity meter (Cyber-attack strategy)- this threat can be exploited by using an infrared device or micro-controller programming which access the billing software through the port of the meter. Since every prepaid metering infrastructure has an infra-red port to allow the electrical engineers to carry out maintenance work, the ports permit access to any device that uses the infra-red light. The attack is non-visible and non-physical because it cannot be detected by just a mere observation and the attacker does not need to have a physical contact with the infrastructure. This strategy is usually used by intelligent people and other experts in computer programming. The goal of this strategy is to reduce the billing cycle so that few units of consumption will be recorded by the infrastructure.
- Threat to the mechanically built-up (Mechanically induced strategy) - particularly the meter disk, the magnet and other internal components. The meter disk is the most important component of the infrastructure that enables power utility record the electricity that has been consumed. This threat can be exploited by inserting metal objects to the infrastructure or exposing it to a strong magnetic object so that the disk's rotary movement is not proportional to the electricity consumed. The attack can be visible or non-visible. Any potential attacker can use this strategy since it's not complicated. The goal of this strategy is to make the disk to rotate slowly so that less electricity is recorded. The slow the movement of the disk the low electricity is recorded.

An attack-tree model shown in **Figure 3 below** has been used to model the vulnerabilities, threats and attack strategies to prepaid electricity metering infrastructure.

As shown in **Figure 3 below**, the tree starts by defining the goal of the attacker which is the root node. In this case the ultimate goal of the attacker is to defeat the electricity billing or enjoy free electricity. The nodes that follow depict the strategies that can be used to fulfil the ultimate goal. The strategies are decomposed further down so that all the possible

actions/threats that may lead to the accomplishing of the goal are known. The decomposition process will continue until the vulnerabilities are identified which make it impossible to break the tree any further.

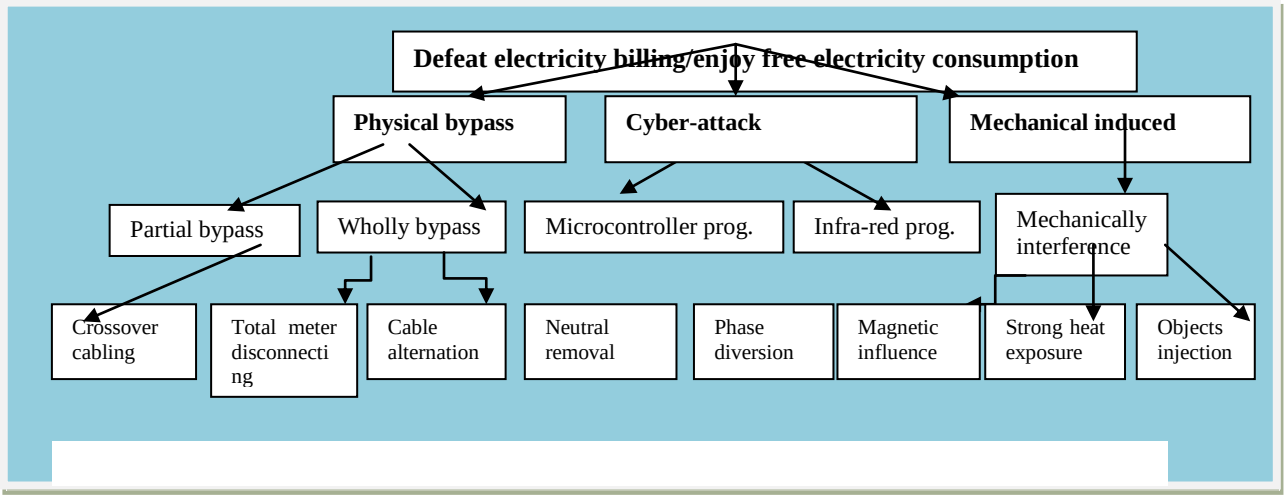

Figure 3: Outline of intrusion scenarios for prepaid electricity metering infrastructure

Source: Researcher's own construction

9. SOURCES OF THREATS AND TYPES OF ATTACKERS

Threat sources can either be internal or external

- Power utility employees (current and former)
- Technologically gifted people/experts
- Experimental people
- Financially disadvantage people

10. PROPOSED FRAMEWORK

The proposed framework presented in Figure 4 has been conceptualized to consist of three (3) phases:

- ***Phase 1: Attack detection/discovery-*** this is the initial stage of modelling a threat. The modeller should check for any information that may give clues to the attack, i.e. there is an attack that is going on. In the case of the prepaid electricity meter infrastructure, electricity purchasing reports can act as a lead, especially if the purchasing trends have dropped to low levels. Comparison of consumer and purchasing reports may also be used to guide the modeller for the perceived attack on the infrastructure. With lead

information, the modeller can consult employees and security expert on more clues. After that a security survey/field inspection can be conducted to confirm or refute the attack by looking for visible and invisible attacks. Lastly, there is a need to recognise and generate the attack patterns based on the methods used.

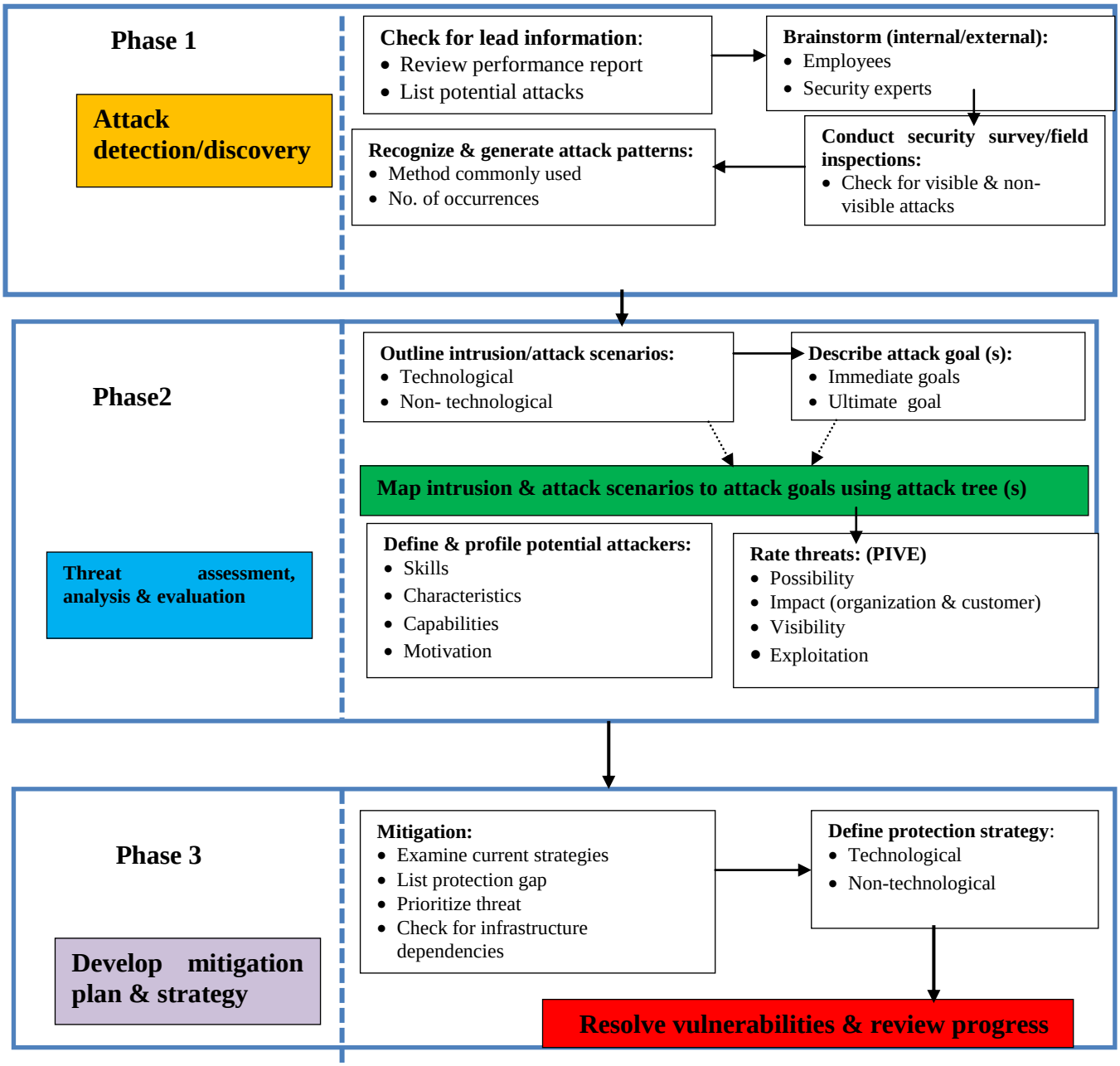

Figure 4: Proposed framework

Source: Own construction

- ***Phase 2: Threat assessment, analysis & evaluation***- this is the main phase of threat modelling. It requires an outline of the intrusion/attack scenarios based on technological and non technological conduct. For example, cyber-attack is technological while the physical by-pass and mechanically induced are both non-technological**.** The phase also requires the description and mapping of attack goals to intrusion scenarios, profiling attackers in order to understand their capabilities. Finally, the threats need to be rated using the PIVE model which has been proposed by this study.
- ***Phase 3: Develop mitigation plan & strategy***- this phase involves the examination of current protection strategies in order to identify gaps, prioritise the threat and checking for infrastructure dependencies. The modeller also needs to decide on the protection strategy based on the factors like cost befit analysis in order to decide whether to respond with technology or not. Last vulnerabilities should be resolved and a review carried out.

11. LIMITATIONS

This research was conducted at a time when the Prepaid metering system has just been rolled in Zimbabwe and as such this being a new system in a new environment, some threats are still to be discovered. Hence these researchers believed this framework to be a good starting point. In this manuscript the authors have confined the framework to ZESA the power utility organisation in Zimbabwe but in reality we believe this framework can also be extended to other organisations in Zimbabwe and beyond.

12. CONCLUSION

Threat modelling is one of the key requirements that enable organizations to minimize security risks and achieve operational excellence. When conducting threat modelling, the modeller should view the infrastructure from the position of the attacker. This will enable them to see it as an exposed system. Power utilities can use threat modelling to mitigate and defeat attack scenarios before they can cause severe damage.

13. FUTURE RESEARCH

Having proposed the framework for threat modelling to the prepaid metering infrastructure, the guidance for further inquiry may commence by looking at the strategies used to steal electricity in order to reinforce the proposed framework. The research may also proceed by establishing the

strategies used by power utilities in dealing with the attack to prepaid metering infrastructure. Furthermore, the use of mobile technologies to achieve end-to-end actionable insights and deliver operational analytics on the infrastructure may also be considered.

14. ACKNOWLEDGEMENTS

The researchers would like to acknowledge the valuable contributions to the success of this work by people from the power utility in Zimbabwe and registered electricity consumers and the framework reviewers. We would like to recognize the assistance rendered by these as their valuable input enabled us to craft this piece of work. We are indeed grateful to these participants for availing themselves for the research and providing data that enabled this study to be carried out. Otherwise this research would not have been possible. Their priceless contribution is greatly appreciated.

REFERENCES

Bakari, J. K. (2007). A Holistic Approach for Managing ICT Security in Non-Commercial Organisations: A Case Study in a Developing Country.

Bertino, E., Martino, L. D., Paci, F., & Squicciarini, A. C. (2010). Security for web services and service-oriented architectures. *Security for Web Services and Service-Oriented Architectures*, 1–226. http://doi.org/10.1007/978-3-540-87742-4

http://www.arrow.dit.ie/cgi/viewcontent.cgi?article=1012&context=engschcivcon

Burns, S. F. (2005). Threat Modeling: A Process To Ensure Application Security, (January) SANS Institute

Ciampa, M., (2009). Security and Guide to Network Security Fundamentals. 3rd edition. Boston: Cengage Learning.

Excellence, N. (2013). Deliverable D6 . 3 : Advanced Report on Smart Environments.

Hämmerli, B., Svendsen, N. K. & Lopez, J. 2013. Critical Information Infrastructures Security: 7th International Workshop, CRITIS 2012, Lillehammer, Norway, September 17-18, 2012. Revised Selected Papers, Springer Berlin Heidelberg.

Hardy, G. M. (2012) Beyond Continuous Monitoring : Threat Modeling for Real-time Response, (October) SANS Institute

Marek, P., & Paulina, J. (2006). The OCTAVE methodology as a risk analysis tool for business resources. *International Multiconference Computer Science and IT …*, 485–497. Retrieved from:http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:The+OCTAVE+methodology+as+a+risk+analysis+tool+for+business+resources#2

Mcgrath, M., & Lennon, R. (2013). Letterkenny Institute of Technology Threat Modelling for Legacy Enterprise Applications, (August).

Meier, J. D., Mackman, A., Dunner, M., Vasireddy, S., Escamilla, R., & Murukan, A. (2003). Chapter 3 – Threat Modeling, (June).

Microsoft. (2012). Introduction to Microsoft Security Development Lifecycle (SDL) Threat Modeling. Retrieved from http://www.cs.berkeley.edu/~daw/teaching/cs261-f12/hws/Introduction_to_Threat_Modeling.pdf

Miyogo, C. N., Ondieki, S., & Nashappi, G. (2013). An Assessment of the Effect of Prepaid Service Transition in Electricity Bill Payment on KP Customers , a Survey of Kenya Power , West Kenya Kisumu, *3*(9), 88–97.

Pabla A.S., (2008). Electric Power Distribution, 5th edition. New Delhi: Tata McGraw-Hill. Available at: http//www.books.google.com/books/about/Electric_Power_Distribution.html?id...

Schneier, B. (1999). Attack Trees. *Dr Dobbs Journal*, *24*(12), 21–29. Retrieved from http://www.schneier.com/paper-attacktrees-ddj-ft.html

Tøndel, A. I. , Jaatun, M. G. & Line, M. B. (2012). SecurityThreats in DemoSteinkjer_v1.pdf. *SINTEF ICT and Telenor*, 1.

Ucedavelez, T., & Partner, M. (2012). Real world threat modelling using the pasta methodology. pp.2-61. Available at: https://www.owasp.org/images/a/aa/AppSecEU2012_PASTA.pdf

Williams, L. (2007). Threat Models Software Security Touchpoints: Purpose of Threat Modeling, 1–15.

Yin, R.K. (2014) Application of case study research: Design and Methods. 5th edition. London: Sage publications.

Zhang, X., & Xu, S. (2006). TDDC03 Projects , Spring (2006): A Comparison of Attack Trees , Threat Modeling and OCTAVE.

This paper may be cited as:

Musungwini, S.,Mahlangu, G.,Mugoniwa, B., and Furusa, S. S., 2016. Framework for Threat Modelling for a Power Utility: Case of Zimbabwe Power Utility Company. *International Journal of Computer Science and Business Informatics, Vol. 16, No. 1, pp. 8-23.*