Geo Bureau
Geographic Information Specialists

Ordnance Survey
Developer Partner

ESRI
AUTHORIZED DEVELOPER

TAME: A Threat Assessment Method for the METEORE System

Stilianos Vidalis[1] and Andrew Blyth[2]

Information Security Consultant
Geo-Bureau Ltd, 47 Cowbridge Road,
Pontyclun, Rhondda Cynon Taf
UK, CF37 9EB
e-mail: stilianos.vidalis@geobureau.co.uk
Tel: +44 (0) 845 603 10 10
Fax: +44 (0) 1443 48 23 29

[2]School of Computing
University of Glamorgan
Pontypridd, RCT, CF37 1DL
e-mail: ajcblyth@glam.ac.uk

Table of Contents

List of Figures

List of Tables

Abstract

The wide development of the mobile Internet technology is creating the opportunity for companies to utilise Electronic Payment Systems for the delivery of services. Due to that, organisations have been forced to allocate considerable resources for protecting their information assets. Unfortunately the opportunity still exists for systems to be exploited with catastrophic results. Modern security management methods now acknowledge that most risks cannot be completely eliminated and that they need to be managed in a cost effective manner. This paper will concentrate on the development of a method for the assessment and analysis of threat and vulnerabilities within the context of security risk management. We will discuss a methodology developed with the needs of electronic payment systems in mind, which focuses upon the technical, socio-technical and business aspects of the system.

Threat, Vulnerability, Threat Agent, Threat Impact, Security Audit,
Vulnerability Analysis, Threat Assessment

0. Introduction

The corporate world is heavily relied upon computers for more than two decades. During that time we have learned that instead of trying to avoid threats, we should try to control them in a practical and cost effective manner [1], [2], [3], [4], [5].

Until now, threat assessment was just part of risk analysis. The reasons for conducting a risk assessment are [6], [7], [8], [9]: new threats, new technology, new laws and new available safeguards. All of the existing methodologies though assume that the users have already analysed the above and are ready for using them. In other words the users must do a subjective analysis and investigation on the above aspects/terms, and bring them in contradiction with their system. According to [4], [5] there is a need for a model to be able to examine the above in an objective way for what they are and not for what they used to be. Everything is changing and evolving, so must our methodologies be able to do.

A meaningful threat assessment model cannot be part of another process any more. Threats and risks are different concepts and should be treated as such. There are a lot of factors [10], [9], [8], [7] to consider and process in order to understand and benefit from a threat assessment. This paper presents a "third generation" [4] threat assessment methodology, which is making use of all of the above and examines threats from a business impact perspective. The methodology was developed for performing the security audit of the METEORE prototype micro-payment system, which was developed by NTSys, Banca Antonveneta, COSI, Business Architects, TIM and TILab. The system was developed under the context of an IST framework-5 research program. More information on the project itself can be found at http://www.meteore2000.net.

1. Background

As it was realised, all the different methodologies [10], [9], [8], [11], [2], [1], [12], [13] were assuming that the user knew about the threats and the threat agents his system had to face. That assumption might be adequate for a risk analysis, but in today's ever-changing world a threat assessment cannot and should not make that mistake.

All of the examined methodologies and models are following the waterfall method [14]. That means that they are not flexible enough and cannot cope with the amount of changes that their "inputs" have to go thought during the lifetime of the assessment. They do not examine the sources of the threats but wrongly assume that the users are already familiar with the threat agents. Furthermore, they are using probabilities for calculating the likelihood of the threat, without examining the likelihood of the agent. Just the concept of using probabilities greatly undermines the validity of the methods. None of the methods is trying to model the system in the business environment hence various assumptions are made. These assumptions can lead to wrong estimations. Most of the models only think of the threat impact as only causing a financial loss. A threat though can have an impact on various levels and aspects of a business.

2. Proposed Methodology

After the examination of different methodologies a suitable one tailored to EPS [15], [16], [17], was developed. All the examined methodologies were following the waterfall development model [14], which was not suitable for our case. EPS are generally sensitive systems prone to changes. Because of their nature, their life span and their "internationality", a waterfall assessment model would be too monolithic and too slow. It would require a great amount of effort and time for producing results only half of which would be of any use. The reasons [11], [18], [7], for conducting a threat assessment are ever changing in our world, hence, there is a need for the model to be flexible, easy to run, and make good use of the available resources. One "way out" is to follow the spiral development method [14]. Even that though is limiting the user to a specific sequence for conducting the different model stages. What we really want is the user to be able to change his way of thinking "on-the-spot", be as much flexible as possible, and be able to change the parameters of the experiment on the fly, from any point of the experiment, without having to restart it. In development terms, we want to achieve high cohesion [19] and loose coupling[19] between the different steps of the model. The model must be able to address all the different security layers [20] of the system such as firewalls, intrusion detection systems, and security policies…

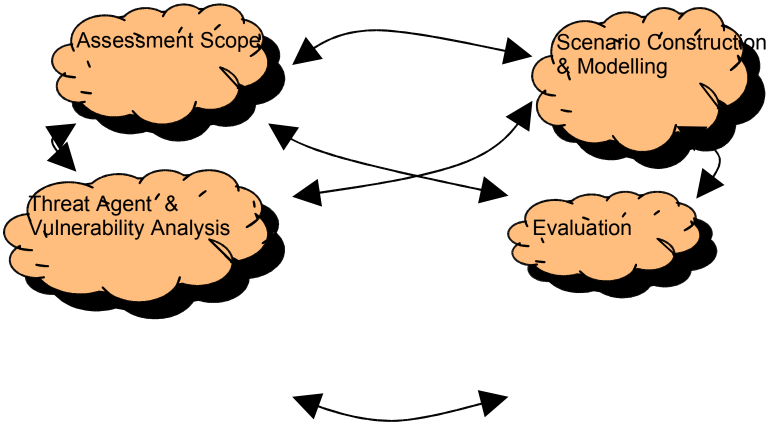

Assessment Scope
Scenario Construction & Modelling
Threat Agent & Vulnerability Analysis
Evaluation

Figure 1 – TAME

The developed methodology was named **T**hreat **A**ssessment **M**odel for **E**PS, or TAME for short, and is illustrated in figure 1. Each stage contains a number of steps. All steps are happening simultaneously and the output of one can be the input of the other and vice versa. The methodology once applied to a business should never come to an end as constant attention is needed to ensure that countermeasures remain appropriate and effective [11], [2], [4], [7], [21].

The formal entry point of the model is the Scope. It is essential to clearly define the scope and the boundaries of the experiment, in order for it to be reproducible and clearly understood by the audience. The formal exit point of the model is the evaluation. At the exit point, the user will be provided with the impact of each threat that his EPS is facing, and with a shortlist of all those threats. The criteria for the short listing are: the importance of the threat, its impact to the business after its realization, and its complexity for occurring towards the system. Each threat will be associated with one or more countermeasures based on two standards: the Common Criteria [22] and the ISO17799.

2.1 Scope

2.1.1 Business Analysis

Business Goals: In agreement to [23], [24], [1], [25], we first conduct a business analysis by identifying the business goals and the business processes. Business goals will lead us to fields that we have to examine and bring to the surface important variables for our assessment [26].

Business Processes: By identifying critical business processes we identify more assets, we bring to the surface more threats and vulnerabilities. Depending on the size of the business under discussion three to eight processes could be identified [25] . Example processes are: receipt of orders, sale of products, delivery services, invoicing, payroll, etc… A detailed description of each identified process will be produced. From that description the auditors will be able to identify more assets and include them in the relevant list. According to the Porter's model [27], the business processes can be categorized us primary activities and support activities.

Environmental Analysis: Environmental analysis is based on the five forces approach that Porter proposes as a means of examining the competitive environment at the level of the strategic business unit [27]. Three types of environments were identified: the technical, the business and the physical environment. The technical environment is concerned with the technical specifications and the technical inner-workings of the EPS. The physical environment is discussing all the physical vulnerabilities of the EPS and of the business in more general. The environmental analysis will bring to the surface more assets and will help populating the threat agent table [26].

2.1.2 Stakeholder Identification

According to [28]:

> ***Stakeholders*** *are defined as those individuals within and without the organization that have a vested interest in decisions made and faced by the organization.*

Each computer system will have a set of stakeholders who can be used to define its function and form. In [29] three distinct types of stakeholders are defined for a computer system: the management's', the user's' and the developer's' [29]. However there are other classifications of stakeholders that can also be used, depending on the type of business the company is conducting.

A list with all the identified stakeholders must be constructed. Each stakeholder will have to give his input for the other steps of this stage. Information security is not something only experts tend to. "In today's' environment all the stakeholders of a business should be part of the information security team"[3]. Stakeholders could be identified from the information security policy document of the company.

2.1.3 System Boundaries Identification

The EPS, according to the size of the business, might vary in size. Trying to describe the whole system will easily disorient the user. After the completion of the previous steps the users will need to clearly identify and define its boundaries and its interfaces. The type of interactions that the system has with its surrounding environment through the above interfaces is also important.

> *A* ***boundary*** *'B' of a system is the point where the system is receiving or sending information to processes outside the scope of its control.*

The system boundary identification will help the stakeholders and the users to place the system in an environment and to better understand the "why's" of the system as they are discussed in the modeling stage and in [30]. Peter Checkland's [31] way for conducting a system boundary identification is by drawing a rich picture of the system.

2.1.4 Threat Agent Identification & Selection

Threat Agent. The term threat agent is used to denote an individual or group that can manifest a threat. It is fundamental to identify who would want to exploit the assets of a company, and how they might use them against the company [32]. The analysis section on threat agents is not presented, as it is not totally relevant to the presentation of the methodology.

We distinguish between the threat agents to those that are hostile towards our system and to those which are not. We use the terms to express an intention towards our system. We can think of the hostile agents being: the career criminal, the hackers and the crackers, and the non-hostile as being: the amateurs and the hackers. In agreement with [13], [25], [20] the identification of threats should be continuous as new agents might be discovered/developed in the future.

2.2 Scenario Construction & Modeling

2.2.1 Scenario Generation

In this step all the parties involved in the risk analysis have to come up with a scenario involving the company using the EPS. The threat assessment will be conducted with this scenario in mind. This step is helping in describing and including the assessment variables that cannot be defined with mathematical equations. It will help to understand and categorize the threats included in the scope according to their importance towards the selected scenario [11]. The more we refine a scenario the more hidden aspects of the system will come to surface. Furthermore, because each stakeholder will construct a scenario, all the different views of the system will come to surface and it is not likely that the auditors will fail to take under consideration a hidden aspect of the system.

2.2.2 System Modeling

The system as a whole will be modeled. All its aspects, procedures, resources and transactions will be analyzed in extend. It is important to understand that we do not want to describe only the EPS. Like the ancient Greek philosophers used to say for any problem they had to face; we must go some steps backwards and see our problem (the EPS) in its surrounding environment. The more complete and detailed the model is, the more successful the other stages will be. Again, as in the previous step, more threats, assets and vulnerabilities are expected to be identified. After checking that they fall under the scope of the assessment, they will be included in the relevant lists.

There are different techniques that can be used to model a computing system [33], [34],[35],[27], [14]. The purpose of this paper is not to identify a new one, or to say which one is better. According to [30] by using traditional modeling techniques, we will be able to focus on the modeling of activities, entities and flows of the system. Traditional modeling techniques are those that are based on structured analysis and entity relationship modeling. Dr. Yu and Dr. Mylopoulos [30] are making the observation that these techniques cannot express the “why” something is the way it is in the model. There is a need for modeling the strategic relationships between the different organizational stakeholders, so that their motivations and intents (the “whys”) can be reasoned out. By using UML and FTAs in conjunction with the stakeholder identification and analysis we will be able to clearly understand the “what”, “how” and “why” of the system. Depending on the knowledge and background experience of the user any modeling technique can be used.

2.2.3 Asset Identification

The entries of the asset register, relevant to the scope under which we see the EPS, as well as the business procedures [25] involved in the transactions that we want to examine, should be included. Assets fall under the following categories [36] [11], [37], [6], [25], [13], [38]: Software, Hardware, Data, Administrative, Communications, Human resources, and Physical. It is not necessary for the table to contain all the asset categories. The selection of the categories is depended on the scope and extent of the experiment.

The problem in this step is to assign a value to each asset and identify what is really a critical asset and what is not [32]. For the purposes of this model, we will use the following definition:

> *An exploitation of an asset ‘A’ can cause a loss of confidentiality ‘Co’, a breach of integrity ‘I’ or a loss of availability ‘Av’ [11], [39], [36]. The* ***value*** *‘V’ of each asset is the cost of restoring or repairing any of the above qualities in its previous state.*

The common factor in the above definition is the time. The value of an item is greatly dependent on the time that will be required for restoring it to its previous state. In the functions that calculate the confidentiality, the importance and the availability the value is proportional to the time. The longer will take the company to restore the integrity of the asset the greater will be the impact in the business, hence the bigger the value of the asset. The same principle applies in the function that calculates the availability. The confidentiality function is probably more important than the other two, due to its close relation to the user trust. A loss of confidentiality in an asset will greatly jeopardise the trust that is shown from the users of that asset to the asset itself and to a greater scale to the system that is using that asset [5]. The users will perceive a loss of confidentiality in a company as a loss of their trust towards that company.

According to [40], [16] user trust is what distinguishes successful EPS from unsuccessful ones. Based on case studies presented in the last two bibliographies, we see that the user trust is not easily restored. Although a company can spend a significant amount of money to restore the confidentiality of an asset in a small amount of time, it cannot do the same for restoring the user trust. That above procedure is time consuming and very slow in progress. The users will have to convince themselves that the company is trustworthy again, and then and only then they will start using the system in a “business efficient” manner. The examined EPS case studies were unsuccessful because the technology was not mature enough; hence not stable enough, to be able to maintain user trust. The asset list will have more than one instance as each stakeholder [28] will have a different opinion about the system. Following the DELPHI approach [11], all these lists will have to be combined and a main one assembled.

2.3 Threat Agent & Vulnerability Analysis

2.3.1 Vulnerability Type Identification & Selection

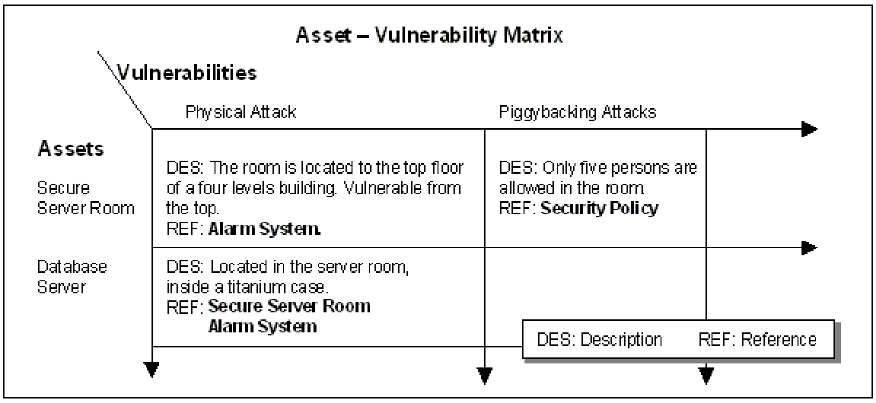
For the purposes of our methodology we will concentrate on the software vulnerabilities[41]. According to [6] these vulnerabilities arise from the technological gap that exists between what a computer system is actually capable of enforcing, and what it is expected to enforce. The vulnerability list presented in [6] is the one that will be followed. An example of its structure can be seen in table 1.

Mode	Misuse type	Countermeasures
External		
Visual spying	Observing of keystrokes on screens or keyboards. Most of the times passwords and other secrets are obtained by a simple “over the solder” observation. Observing user behavior. In advance attack methods used by advanced computer criminals, when masquerading as a legitimate user, it is important to behave like that user as well. User behavior should be put in the same level as user credentials.	**Common Criteria** User Guidance (CC 5.3.4.2) **BS7799/ISO17799** Personnel Security (BS 6.1.4)
Misrepresentation	Deceiving operators and users. Social engineering attacks are the most common type of attack. By misrepresenting people and data a computer criminal can convince legitimate users to part with corporate secrets and sensitive data.	**Common Criteria** User Guidance (CC 5.3.4.2) Specification of secrets (CC 5.2.5.3) **BS7799/ISO17799** Assets Classification & Control (BS 6.1.3) Personnel Security (BS 6.1.4)

Table 1– Vulnerability List Structure

There are so many aspects and variables involved with a system, that the output of an assessment could be so big that would render it unusable (see CRAMM) [13], [42]. Vulnerability Selection is introduced to the model in order to simplify things, and tailor the output to real user needs. From all the vulnerabilities that were identified in the above table, the stakeholders are selecting a category for further investigation. For example the stakeholders might decide to select the vulnerabilities related to the customer data, or to the broker servers of the micro-payment system. Of course the selection is optional and the stakeholders might decide to include all the categories. The final vulnerability list needs to be combined with the asset list in order to get a matrix with all the vulnerabilities for each asset. By doing that we also link countermeasures to assets.

. After listing them, the user will be able to see all the related countermeasures, which in turn are related to other assets. The result will look like the matrix in figure 2.



Assets \ Vulnerabilities	Physical Attack	Piggybacking Attacks
Secure Server Room	DES: The room is located to the top floor of a four levels building. Vulnerable from the top. REF: **Alarm System.**	DES: Only five persons are allowed in the room. REF: **Security Policy**
Database Server	DES: Located in the server room, inside a titanium case. REF: **Secure Server Room** **Alarm System**	

Figure 2 – Asset/Vulnerability Matrix

For each entry in the matrix we will need to construct a fault three. This will give us the difficulty of exploiting a vulnerability of a given asset.

2.3.2 Vulnerability Complexity Calculation

From the previous step we should have a matrix identifying most of the vulnerabilities for each asset involved in the EPS. There is a need for finding out how easy or hard it is for each vulnerability to be exploited from the aspect of complexity [43], [11]. Does a threat agent need to exploit another vulnerability in order to achieve his goal? This question can be answered through the application of fault trees as defined in the modelling stage.

For example let us consider the main Broker server of a micro-payment system. There is the physical vulnerability of a human threat agent to walk in the server room and steal it. For doing that though, he should exploit a vulnerability related to the alarm system of the room, and in extend of the building, a vulnerability related to the security guards, and a vulnerability related to the high security doors which are installed in the server room. A threat agent in the above example might not always decide to go for the “quickest way. The exploitation of a vulnerability is a combination of capabilities, motivations and opportunities. Depending on his motivations the threat agent might decide not to “reveal” himself as a high capability agent and go for another more trivial way. Furthermore, if a threat agent, after completing the information gathering stage, realizes that certain countermeasures are deployed, he might decide to alter his course of action. Hence the presented opportunity will affect the course of a vulnerability exploitation.

2.3.3 Threat Agent Preference Structuring

Each threat agent that will pass through the stakeholder validation will need to be investigated in more detail. The attributes that are getting examined here are their likelihood and their importance [28], [11], [37], [39], [43], [13]. The calculations will be based not on probabilities but on the results of the intelligence gathering for each agent. A number of resources must be interrogated as the more details we will gather the better we will be able to understand the agent. By analyzing these two attributes we will be able to structure the agents in a list with the most important one at the top. The preference structuring is based on the principles of the utility theory [44]. Once an agent has been in the list, he should not be taken out as in the future the order of the preference will most likely change.

2.3.4 Threat Agent Capabilities

In this step we will combine the threat agent list from the second step of the first stage and the vulnerability – asset matrix from the same stage to get a matrix that would present all the interactions between the two. For each interaction we will need to calculate the impact it will have on the business. According to Pfleeger [39], for a threat to be able to exploit a vulnerability, three factors must be in place: the capability factor, the motivation factor and the opportunity factor. Hence, there is a need for a multi-dimensional matrix, and more specific a three-dimensional one. In the x-axis there will be the selected vulnerabilities of the assets included in the Scope. In the y-axis there will be the threats included or identified in the Scope. In the z-axis there will be the above three factors, which are of the Boolean data type. The threats that will "qualify" to the next stage will only be the ones that exist in all three layers of the third dimension.

2.4 Evaluation

2.4.1 Stakeholder Evaluation

In this step the stakeholders of the company under discussion are reviewing the outputs of all the other stages. As with all computing systems, the developers must stay in close contact with the customer [14]. In our case the developers are the security officers conducting the assessment and the customers are the stakeholders of the company, which is paying for the assessment. Threats, assets and vulnerabilities are expected to be introduced, or excluded, not from the model, but from any further investigation. Once something is into the system, it should not be taken out. Although it might seem unimportant at the time, things are very fluid in the computing world, and it might come into play in one of the next loops of the model.

2.4.2 Scenario Selection & Conflict Resolution

Part of the Scenario Construction and Modeling stage is the Business Scenario Construction. Each stakeholder is coming up with a scenario involving the business, the system and potential threats. Depending on the number of stakeholders, the auditors might end up with a high number of possible scenarios. In the Unification stage, the stakeholders are coming together to review all the different scenarios, and unify all the concerns presented through them, in one characterizing for the business scenario. That scenario will be given to the security auditors in order to apply it to the model. It is important to understand that all the different stakeholders must participate in this step, as each one has a different view for the system and examines it under a different perspective.

2.4.3 Threat Impact Analysis

A threat impact can be towards the market share of the company, or even more important the user trust. These impacts are not easily calculated and only speculations can be made for their size. A golden rule is that any threat that could be realized from the users will have a catastrophic impact to the user trust and any threat that can be realized from the suppliers or generally the stakeholders of the company will have catastrophic results to the market share of the company. Stakeholders will only understand the threat when they realize how much of a loss is going to cost them [32].

Another classification of threat impacts is the following:

- *Minor: minor loss of a business asset, no change in business order*
- *Moderate: business disruption, moderate changes in way of conducting business*
- *Major: out of business unless countermeasures are deployed immediately*
- *Catastrophic: out of business from the moment that the threat was realized*

The impact of a threat can cause disruption in more than one field. The following impact fields were identified during the development of the model. Different types of businesses could have different types of impact fields.

- *Human Resources*
- *Supply Chain*
- *Market Share*
- *Business Capital*
- User Trust

2.4.4 Threat Statement Generation

This is the exit point of the model. No matter how many times the user will run the model, this step will always be the last one. After all the screening in the previous steps, the output of the model is a number of threats related to a vulnerability of a specific asset of a micro-payment system. In this step we produce a final list that sorts the threats according to their importance and the complexity of the vulnerability they are related to. The "primary key" is the importance and the "secondary key" is the complexity. By that we should get a list with the most "dangerous" threat at the top and the least dangerous at the bottom. Security wise the company conducting the risk assessment should start deploying countermeasures against the threats in the list, from the top to the bottom.

Because each threat is related to a threat impact, the company has a measurement on justifying the countermeasures. If the cost for a countermeasure is a fraction of the threat impact then the company can apply it with no further investigation. If on the other hand it is not, then the company might consider a different countermeasure or it might as well decide to live with the threat (which will now be a risk) and not spend a fortune on tackling it. This justification though is over the scope of this report; hence we shall not discuss it in more detail.

3. Conclusions

All companies involved in at least one level of E-Commerce must ensure that their systems are secure and do not provide threat agents with any kind of opportunities. If we want to think "European" we must act "European" and enforce the same principles over all the member nations. In E-Commerce the weakest link is not thrown out of the game, it destroys the game altogether. By using a third generation methodology such as TAME we bring all the sciences needed for a complete and meaningful threat assessment together. The methodology has the ability to:

- Explore and assess IS threats to business operations in relation to the type of business
- Determine what policies and controls should be implemented for effectively minimising the identified threats
- Promote awareness amongst all stakeholders of a system
- Evolve and react to external stimuli as they happen

The next stage for this model would be its application to various live systems for evaluation purposes and for "finely tuning" its various stages. A paper is getting prepared to cover the vulnerability tree use for modelling a system and finding out critical paths that a threat agent could follow for exploiting an asset. A third paper will cover the threat agent analysis and the attributes that are involved in the process of understanding the agents' capabilities. After the completion of the above, the foundations of the presented methodology will be solid enough to convert it to a mathematical model. This would lead to the development of a set of automated tools that will help improving its "interoperability". We have to remember that for the business world, time is money and money is a luxury that cannot be spared. The set of tools will involve a large database with threat agent and vulnerability data ready to be combined and tailored to the needs of each system. The tools will be able to take the user input (assets, threats, vulnerabilities, system modelling), calculate the assessment variables (threat agent likelihood, capabilities, vulnerability complexity…), wait for the user evaluation, recalculate the variables and present the users with the threat list.

4. Bibliography – References