Understanding and Developing a Threat Assessment Model

S Vidalis and A Blyth

School of Computing Technical Report CS-02-3

Issued: October 2002

School of Computing, University of Glamorgan, Pontypridd, CF37 1DL, Wales, UK.
www.comp.glam.ac.uk

Understanding and Developing a Threat Assessment Model

Stilianos Vidalis[1] and Andrew Blyth[2]

[1]School of Computing, University of Glamorgan,
Pontypridd, CF37 1DL, UK.

E-Mail: svidalis@glam.ac.uk

[2]School of Computing, University of Glamorgan,
Pontypridd, CF37 1DL, UK.

E-Mail: ajcblyth @glam.ac.uk

Abstract

The wide development of the mobile Internet technology is creating the opportunity for companies to extensively utilise computer systems for the delivery of services. New business models, which rely on electronic payment systems, are emerging and each one is creating a vulnerability to the Critical National Information Infrastructure (CNII). The opportunity for deploying offensive information warfare tactics against the CNII will be greatly enlarged from the introduction of such systems and the open government policy is greatly affecting the above. Organisations have been forced to allocate considerable resources for protecting their information assets. Unfortunately the opportunity still exists for both protected and unprotected 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 methodology for the assessment and analysis of threat and vulnerabilities within the context of a security risk management. We will discuss a threat and vulnerability assessment method developed with the needs of mobile computer systems in mind. This method consists of four stages: a) Assessment Scope, b) Scenario Construction & Modelling, c) Threat Agent & Vulnerability Analysis, and d) Stakeholder Evaluation. This method actively involves stakeholders and focuses upon a technical, socio-technical and business aspect of the system.

Keywords: Threat, Vulnerability, Threat Agent, Threat Impact, Vulnerability Analysis, Threat Assessment

Introduction

In today's' computing environment, organisations have been forced to allocate considerable resources for protecting their information assets. The introduction of E-Commerce have greatly destabilised the already fragile balance between the defenders and the attackers of computing systems. 54% of the online Europeans have reported they have made at least one purchase online and 27% are using online banking facilities (Hinde 2001). 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, to some extend, in a practical and cost effective manner (Pfleeger, 2000; Nosworthy, 2000; Wood, 1997; Wright, 1999; Parkin, 1998). For reference purposes the cost of security breaches at US for the year 2001 was $378 million (Hinde 2001).

The European Union has put forward a proposal (Pounder 2001), which states: "Governments have realised the extent to which their economies and their citizens are dependent on the effective working of communication networks". Furthermore it is clearly stated that all European governments must intervene to establish their national security infrastructure, and such interventions need to be harmonised amongst the state members for producing a homogeneous security barrier to both inside and outside threat agents.

The IS officers are in the very difficult point of having to protect a hill that is surrounded by the enemy (threat agents). A single breach to the defence lines could be enough for losing the battle. A threat assessment methodology will provide the means to analyse and understand the threat agents in order to anticipate their moves and ways of engagement. Furthermore, an efficient methodology will be able to pinpoint vulnerable spots to the defences and provide countermeasures for effectively shielding them from those able to exploit them.

Until now, threat assessment was just a part of risk analysis. Risk analysis is a process to assist management in defining where time and money should be spent (Nosworthy 2000). There are two types of risk analysis, the quantitative and the qualitative. The first is a mathematical approach based on probabilities and the second is a high/medium/low approach. Unfortunately the majority of threats defy all sorts of probability analysis. To overcome this problem most security professionals are using business impacts when conducting a risk analysis and not probabilities.

The reasons for conducting a risk assessment are (Neumann, 1995; Smith, 1993; Reid and Floyd, 2001; Katzke, 1988; Hancock, 1998; Brewer, 2000): new threats, new technology, new laws and new available safeguards. Most of the existing methodologies assume that the users know when and how to start a risk assessment. In other words the users, before using an existing methodology, must do a subjective analysis and investigation on the above, and bring them in contradiction with their computing system. According to (Wright, 1999; Parkin, 1998) there is a need for a model to be able to examine all those variables in an objective way for what they are and not for what they used to be. The tools and techniques that were used in the previous four decades are not sufficient for understanding the threat agents of this new electronic era we are living into.

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. This paper presents a "third generation" (Wright 1999) threat assessment methodology, which 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.

Background

As it was realised, all the different methodologies (Brewer, 2000; Katzke, 1988; Reid and Floyd, 2001; Carroll, 1996; Nosworthy, 2000; Pfleeger, 2000; Icove, Seger et al., 1995; Summers, 1977; CCTA, 1993) were assuming that the user knew about the threats and the threat agents his system had to face, and do not attempt to examine their sources. 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 (Pressman 2001) for calculating and producing results. That means that they are not flexible enough and cannot cope with the amount of changes their inputs have to go thought. 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. Most of the models 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 (Kalakota and Whinston, 1997; Daughtrey, 2001; feature, 2002; Johnson and Scholes, 1999). We not only need to consider these various levels, but we also need to examine combinations of impacts and how catastrophic they might be towards the survivability of the business. Table 1 presents a critical comparison of the examined methodologies.

	CRAMM	LAVA	ARiES	Pfleeger	Carroll	Summers	Icove
Explore & Assess IS Threats to Business Operations in relation to Type of Business							
Boundaries ID	Yes	No	No	No	No	No	No
Scenario Construction	Yes	No	No	No	No	No	No
Business Analysis	No	No	No	No	No	No	No
Threat Agent Identification & Selection	No	No	No	No	No	Yes	Yes
Threat Agent Preference structuring	Yes	No	No	No	No	No	No
Business Modelling	No	No	No	No	No	No	No
Asset ID	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Determine what Policies, Standards & Controls are worth implementing to reduce identified threats							
Impact Analysis	Yes	No	Yes	Yes	Yes	Yes	No
Vulnerability Identification	Yes	Yes	No	Yes	Yes	Yes	Yes
Vulnerability complexity calculation	No	No	No	No	No	No	No
Promote awareness & understanding amongst all stakeholders							
Stakeholder Analysis	No	No	No	No	No	No	No
Evaluation of results	Yes	Yes	No	No	No	No	Yes
Assess compliance with standards & control effectiveness							
ISO 17799	Yes	No	No	No	No	No	No
ISO 15408	No	No	No	No	No	No	No
Ability to evolve and react to external stimuli as they happen							
Top Down Approach	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Bottom Up approach	No	No	No	No	No	No	No
Threat agent capabilities analysis	No	No	No	No	No	No	Yes
Countermeasure analysis	No	No	Yes	Yes	Yes	Yes	Yes
Use of formal methods in threat calculations							
Probabilistic approach	Yes	No	Yes	Yes	Yes	Yes	No
Hierarchical approach	No	Yes	No	No	No	No	Yes

Table 1 – Critical Comparison

Model Description

After the examination of different methodologies a suitable one tailored to Electronic Payment Sytems (EPS) (O'Mahony, Peirce et al., 1997; Shirky, 2000; Manasse, 1995; Shirky, 2000), was developed. All the examined methodologies were following the waterfall development model (Pressman 2001), which was not suitable for EPS. These systems are generally sensitive systems prone to changes and 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 useful for the business conducting the assessment.

Another development option is to follow the spiral development method (Pressman 2001). Yet again, even that 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 and working "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 (Schildt 1995) and loose coupling (Schildt 1995) between the different steps of the model. Furthermore, the model must be able to address all the different security layers (feature 2002) of the system such as firewalls, intrusion detection systems, and security policies…

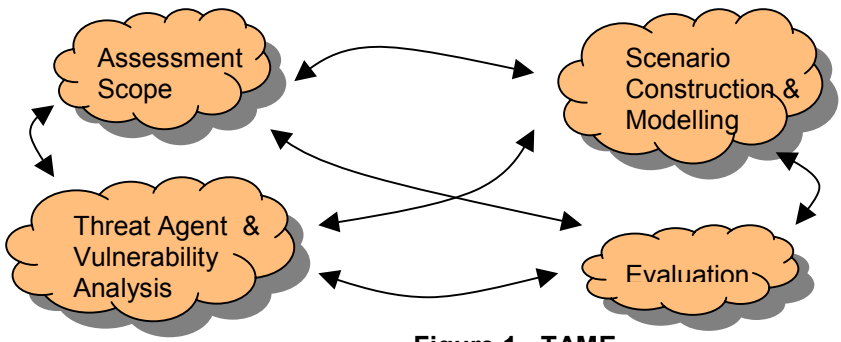

Figure 1 - TAME

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 another, or the output of one might change the input of another and vice versa. The methodology, once applied to a system should never come to an end, as constant attention is needed to ensure that countermeasures remain appropriate and effective (Carroll, 1996; Nosworthy, 2000; Wright, 1999; Smith, 1993; Barber, 2001).

Assessment Scope

- Business Analysis,
- Stakeholder Identification,
- System Boundaries Identification,
- Threat Agent Identification & Selection

Scenario Construction & Modeling

- Scenario Generation,
- System Modeling,
- Asset Identification

Threat Agent & Vulnerability Analysis

- Threat Agent Preference Structuring,
- Threat Agent Capabilities,
- Vulnerability Type Identification & Selection,
- Vulnerability Complexity Analysis

Evaluation

- Stakeholder Evaluation,
- Scenario Selection & Conflict Resolution,
- Threat Impact Analysis,
- Threat Statement Generation and Transfer

The uniqueness of TAME lies in the interactions between the different steps and in the data flows. There is not one unique path to execute the methodology. The auditor can follow whatever path he chooses so depending on the restrictions of the security audit and the restrictions of his knowledge. It is not necessary for the auditor to perform all the steps for getting a result. The golden rule though is the more steps the better the results. The formal entry point of the model is the Scope stage. As with all the experiments in the applied sciences field, it is essential to clearly define the scope and the boundaries of the experiment. The formal exit point of the model is the Evaluation stage. At the exit point, the user will be provided with the impact of each threat that his system 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 (ISO/IEC 1998) and the ISO17799.

Model Analysis

Scope

Business Analysis

Business Goals: In agreement to (Myers, 1999; Kokolakis, Demopoulos et al., 2000; Pfleeger, 2000; Nosworthy, 2000), we 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 (Forte 2000). The business goals could be obtained from the stakeholders of the company (see Stakeholder section).

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 (Nosworthy 2000) . 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 (Johnson and Scholes 1999), the business processes can be categorized us primary activities and support activities. The primary activities of the organization are grouped into five main areas: inbound logistics, operations, outbound logistics, marketing and sales, and service. Each of primary activities is linked to support activities. The support activities can be divided into four areas: Procurement, Technology Development, Human Resource Management, and Infrastructure.

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 (Johnson and Scholes 1999). Three types of environments were identified: the technical, the business and the physical environment. The environmental analysis will bring to the surface more assets and will help populating the threat agent table (Forte 2000).

Stakeholder Identification

According to (Blyth and Kovacich 2001):

> ***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 (Sutcliffe 1988) three distinct types of stakeholders are defined for a computer system: the management's', the user's' and the developer's'. 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 the internal and external stakeholders should be constructed. Each internal 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 must be part of the information security team (Wood 1997).

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 auditor. The auditors will need to clearly identify and define the boundaries of the system that will be assessed. In this step the interfaces of the system under analysis will be identified. Furthermore the type of interaction that the system has with its surrounding environment through the above interfaces is also important, as it will help identify more assets and vulnerabilities.

> *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 auditors 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 (Yu and Mylopoulos 1997).

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 (Hancock 1998). These individuals and groups can be classified as follows:

- Hostile Nations: These are people who professionally gather information and commit sabotage for governments. They are highly trained and highly funded. They are backed by

substantial scientific capabilities, directed towards specific goals, and skilful in avoiding detection. They can be very dangerous to life and property.

- Terrorism and Terrorist Groups. Terrorists are of particular interest because of the damage that they can cause against the information infrastructure such as emergency services, utilities such as water and electricity, and financial services. Terrorists are politically motivated and have their own political agenda that they use to select targets.
- The Corporation. Corporations engage in offensive IW when they actively seek intelligence about their competitors or steal their sensitive information, e.g. trade secrets. Money, market position and competitive stance are examples of some of the corporate motivations for using IW tactics. In addition, corporations have always engaged in a form of IW even before the term was first used. This type of IW is called advertising and marketing.
- Organized Crime and Criminals. Criminals target information that is of value to them, such as bank accounts, credit cards or intellectual property that can be converted into money. Criminals will often make use of insiders to help them. They may be in collusion with the insiders or use such tactics as threats, blackmail and the like.
- The Empowered Small Agent (ESA). The term empowered small agent is used to denote an individual or group who is motivated for a) ideological principles, b) political principles, c) religious principles or d) the intellectual challenge. For example Political Dissidents are people who are attempting to use information and information technology to achieve a political objective.

We distinguish between the threat agents to those that are hostile towards our system and to those which are not. We use the term “hostile” to express intention. In agreement with (Summers, 1977; Nosworthy, 2000; feature, 2002) the identification of threats should be continuous as new agents might be discovered/developed in the future. Each threat agent has a number of attributes associated with it. Two that were identified in this stage are the capability and the motivation. The capability can be affected by: software, technology, facilities, educations and training. The motivation can be political, religious, a terrorist act, or personal gain. Our belief is that the motivation will always be affected by a number of the above factors and never by a single one. Once a threat agent is identified, a number of sources must be interrogated in order to conduct an efficient intelligence gathering. The more

information we will gather, the less subjective our analysis will be. The structure of the threat agent class would look like the one presented in figure 2 underneath.

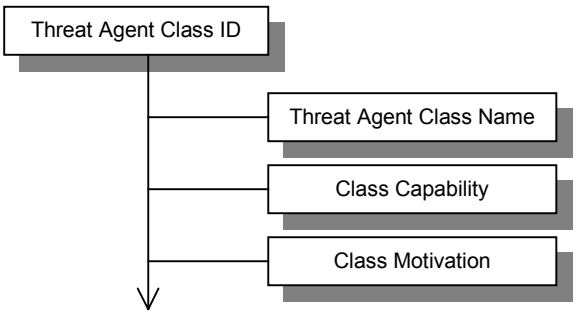

Figure 2 – Threat Agent Class Structure

Scenario Construction & Modeling

Scenario Generation

In this step all the parties involved in the threat assessment have to come up with a scenario involving the company using the EPS under discussion. The parties that will be most involved are the management of the company and the stakeholders in cooperation with the security officers. The scenario will be describing the company in the real world. 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.

This step will help to understand and categorize the threats included in the scope according to their importance towards the selected scenario (Carroll 1996). The more we refine a scenario the more hidden aspects of the system will come to surface. Furthermore, because each stakeholder will be used to construct a scenario, all the different views of the system will come to surface and it is not likely that the user will fail to take under consideration a hidden aspect of the system. The problem that was identified here is the large number of possible scenarios and it was solved by introducing a scenario selection/unification step in the evaluation stage.

System Modeling

The system as a whole will be modeled. All its aspects, procedures, resources and transactions will be analyzed in extend. 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 system) 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 (Storey, 1996; Booch, Jacobson et al., 1999; Mylopoulos and Yu, 1994; Johnson and Scholes, 1999; Pressman, 2001). The purpose of this paper is not to identify a new one, or to say which one is better. According to (Yu and Mylopoulos 1997) traditional modeling techniques, 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. We also need to model 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.

Asset Identification

The entries of the asset register, relevant to the scope under which we see the EPS, as well as the business procedures (Nosworthy 2000) involved in the transactions that we want to examine, should be included. The user identifies only the assets that he wants to examine. More assets will be identified during other steps.

Assets fall under the following categories (Kabay, 1996; Carroll, 1996; Kove, Seger et al., 1995; Neumann, 1995; Nosworthy, 2000; Summers, 1977; Casey, 2000): Software, Hardware, Data, Administrative, Communications, Human resources, and Physical. The user will populate such a table according to his system. 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 (Hancock 1998). 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' (Carroll, 1996; Pfleeger, 1997; Kabay, 1996). 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 (Parkin 1998). The users will perceive a loss of confidentiality in a company as a loss of their trust towards that company.

According to (Donal O'Mahony, Peirce et al., 1997; Shirky, 2000) user trust is what distinguishes successful EPSs 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. The 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 (D. O'Mahony, M. Peirce et al., 1997; Manasse, 1995; R. Kalakota and Whinston, 1997; Shirky 2000), 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 (Blyth and Kovacich 2001) will have a different opinion about the system. Following the DELPHI approach (Carroll 1996), all these lists will have to be combined and a main one assembled.

Threat Agent & Vulnerability Analysis

Vulnerability Type Identification & Selection

For the purposes of our methodology we will concentrate on the software vulnerabilities. According to (Neumann 1995) 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 (Neumann 1995) is the one that will be followed. An example of its structure can be seen in table 2.

Mode	Misuse type	Countermeasures
External		
Visual spying	Observing of keystrokes on screens or keyboards. 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 2– 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) (Summers, 1977; CCTA, 1993). 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 user is selecting one or more categories for further investigation. 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. The result will look like the matrix in figure 3.

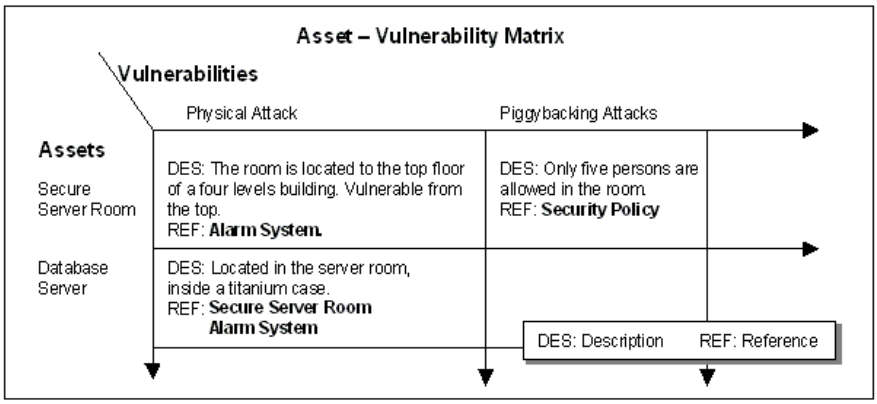

Figure 3 – Asset/Vulnerability Matrix

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.

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 (Stalling, 2000; Carroll, 1996). 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.

The vulnerability complexity calculation and the modeling of a system using vulnerability trees is the context of another paper that we are preparing for the end of this year.

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 (Blyth and Kovacich, 2001; Carroll, 1996; Kove, Seger et al., 1995; Pfleeger, 1997; Stalling, 2000; Summers, 1977). 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 could be based on the principles of the utility theory (Keeney and Raiffa 1993).

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 (Pfleeger 1997), 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. They are either true or false. The threats that will "qualify" to the next stage will only be the ones that exist in all three layers of the third dimension.

Evaluation

Stakeholder Evaluation

In this step the stakeholders are reviewing the outputs of the stages that were executed. As with all computing systems, the developers must stay in close contact with the customer (Pressman 2001). 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. It has to be clear that stakeholders have no option other to participate in this evaluation. No matter their agenda stakeholders (internal or external) must be cooperative in order to identify the vulnerabilities and achieve compliance with the security standards. If a stakeholder needs to be persuaded for taking part in a system evaluation then that stakeholder poses a major vulnerability and should be countered straight away.

Threats, assets and vulnerabilities are expected to be introduced, or excluded, not from the methodology, but from any further investigation. Once an "entity" 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.

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 this 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.

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 (Hancock 1998).

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:* Any kind of organization is depended on its employees. If the employees are demoralized, scared or not able to perform up to the managements' expectations in any way due to the manifestation of a threat, then the business will be at a loss.
- *Supply Chain:* All businesses are dependent on their supply chain. The majority of the businesses are like functions in a software program. They take something as an input, do specific operations with the input, and produce an output, which they pass over to either another function or to one of the standard output devices of a computer system. If there is a disruption in that chain, then the function is not able to operate. Exactly the same principle applies to the businesses, only in a larger scale. Once there is a disruption in the supply chain, the business will survive only if it has good continuity plans.
- *Market Share:* The market share is essential for the survivability of a business as it declares more or less its ability to sell the product that is producing. If there is a major disruption or change in the market share of the business, then it is unlikely that the business will be able to recover in a short term, if ever at all.
- *Business Capital:* The capital of the business could be impacted by the manifestation of certain threats. The result of that will be a further disruption on the ability of the business to continue offering its services.
- *User Trust:* User trust is one of the most important survivability factors for a business using a micro-payment system (Daughtrey 2001). The user trust is closely related to the market share, with one distinction. It is easier to regain market share following

marketing tricks and procedures. The user trust on the other hand is an asset that takes ages to develop and minutes to loose.

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.

Conclusions

Sun Tsu(Tsu and Clavell 1981) would be considered an IW expert should he was alive today. He had effectively described the principles of the science before even humans created the term. All modern nations have the capabilities and the motivation to proceed in such tactics (Tsu and Clavell 1981), but do they have the opportunity? 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. It is the duty of every single organisation to ensure the security of the country in which it is established, in the same way as it is the duty of every soldier to ensure the security of his platoon. If we want to think "European" we must act "European" and enforce the same principles over all the member nations. In IW 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 next stage for the proposed methodology is its application to various live systems for evaluation purposes and for "finely tuning" its various stages. Currently we are researching a method for using vulnerability trees for modelling the system that will greatly improve the decision making of possible threat agent attack paths and countermeasure selection. After the completion of the above, the foundations of our theory will be solid enough to convert it to a

mathematical model. The difficulty lies to the unique way TAME is structured. A model limits the user to a set of actions. TAME thought is doing exactly the opposite; it lets the user to decide his next step. The methodology actually uses the user as an asset for better understanding the system that he is analysing. One could say that it is a chaotic theory, which is trying to model the chaotic nature of the threat. Furthermore, because time is considered to be a constraint, most of the steps have no pre-requisites. Although it is not easy to use a UML activity diagram to model TAME, this is not a drawback but an asset itself. Traditional techniques cannot be used for modelling the threat. People and professionals, who insist in doing that, should reconsider except they want more incidents like the one on the 11th of September to take place.

Bibliography - References

Barber(2001). "Hacking Techniques." *Computer Fraud & Security* **2001**(3): 9-12.

Blyth and Kovacich(2001). Information assurance, Springer-Verlay.

Booch, Jacobson, et al. (1999). The unified modeling language users guide, Addison-Wesley.

Brewer(2000). Risk Assessment Models and Evolving Approaches, Gamma Secure Systems Ltd.

Carroll(1996). Computer Security, Butterworth-Heinemann.

Casey(2000). Digital Evidence and Computer Crime, Academic Press.

CCTA(1993). PRINCE User's guide to CRAMM, Central Computer & Telecommunications Agency.

Icove, Seger, et al. (1995). Computer Crime: A crimefighter's handbook, O'Reilly & Associates.

Daughtrey(2001). Costs of trust for e-business, Quality Progress.

Donal O'Mahony, Peirce, et al. (1997). Electronic Payment Systems, Artech House Inc.

feature (2002). "Information Security - The Great Balancing Act." *Computer Fraud & Security* **2002**(2): 12-14.

Forte(2000). "Information Security Assessment: Procedures and Methodology." *Computer Fraud & Security* **2000**(8): 9-12.

Hancock(1998). "Steps to a successful creation of a corporate threat management plan." *Computer Fraud & Security* **1998**(7): 16-18.

Hinde(2001). "Cyberthreats: Perceptions, Reality and Protection." *Computers & Security* **20**(5): 364-371.

ISO/IEC (1998). Common Criteria for Information Technology Security Evaluation, ISO/IEC.

Johnson and Scholes(1999). Exploring corporate strategy, Prentice Hall Europe.

Kabay(1996). Enterprise Security: Protecting Information Assets, McGraw-Hill.

Katzke(1988). A government perspective on risk management of automated information systems. Computer Security Risk Management Model Builders Workshop, Denver Colorado.

Keeney and Raiffa(1993). Decisions with Multiple Objectives, Cambridge University Press.

Manasse(1995). The Milllicent Protocols for Electronic Commerce. 1st USENIX workshop on electronic commerce.

Myers(1999). Managers guide to contigency planning for disasters, Willey.

Mylopoulos and Yu(1994). Using Goals, Rules and Methods to Support Reasoning in Business Process Re-Engineering. Twenty-Seventh Hawaii International Conference on System Sciences.

Neumann(1995). Computer Related risks, Addison-Wesley.

Nosworthy(2000). "A Practical Risk Analysis Approach: managing BCM risk." *Computers & Security* **19**(7): 596-614.

Nosworthy(2000). "A practical risk analysis approach`." *Computers & security* **19**: 596-614.

Parkin(1998). "The Importance of IT Security." *Computer Fraud & Security* **1998**(3): 12-15.

Pfleeger(1997). Security in Computing, Prentice Hall Int.

Pfleeger(2000). "Risky Business: what we have yet to learn about risk management." *Journal of Systems and Software* **53**(3): 265-273.

Pounder(2001). "The European Union Proposal for a Policy Towards Network and Information Security." *Computers & Security* **20**(7): 573-576.

Pressman(2001). Software engineering: A practitioner's approach, McGraw-Hill.

Kalakota and Whinston(1997). Electronic Commerce: a manager's guide, Addison Wesley.

Reid and Floyd(2001). "Extending the Risk Analysis Model to Include Market-Insurance." *Computers & Security* **20**(4): 331-339.

Kokolakis, Demopoulos, et al. (2000). "The use of business process modelling in information systems security and design." *Information Management & Computer Security* **8**(3): 107-116.

Schildt(1995). C++ The complete reference, McGraw-Hill.

Shirky(2000). The case against micro-payment, The O'reilly Network (www.oreilly.com). **2001**.

Smith(1993). Commonsence Computer Security: your practical guide to information protection, McGraw-Hill.

Stalling(2000). Network Security Essentials, Prentice Hall.

Storey(1996). Safety-critical computer systems, Addison-Wesley.

Summers(1977). Secure Computing: threats & safeguards, McGraw-Hill`.

Sutcliffe(1988). Human-Computer Interface Design, Macmillan Education.

Tah, and Carr(2001). "Towards a framework for project risk knowledge management in the construction supply chain." *Advances in Engineering Software*.

Tsu and Clavell(1981). The art of war, Hobber & Stoughton General.

Wood(1997). "Policies alone do not constiture a sufficient awareness effort." *Computer Fraud & Security* **1997**(12): 14-19.

Wright(1999). "Third Generation Risk Management Practices." *Computer Fraud & Security* **1999**(2): 9-12.

Yu and Mylopoulos(1997). "Enterprise Modeling for Business Redesign: the i* framework." *SIGGROUP Bulletin* **18**(1): 59-63.