

Assessing Cyber-Threats in the Information Environment

Stilianos Vidalis, Andy Jones, Andrew Blyth, Paula Thomas

Stilianos Vidalis

Information Security Consultant
Geo-Bureau Ltd, 47 Cowbridge Road,
Pontyclun, Rhondda Cynon Taf,
UK, CF72 9EB
e-mail: stilianos.vidalis@geobureau.co.uk
Tel: +44 (0) 845 603 10 10
Fax: +44 (0) 1443 48 23 29

Table of Contents

INTRODUCTION.....	4
TAME OVERVIEW.....	4
EXAMPLE SCENARIO.....	10
Process 1: Business Analysis.....	11
Business Goal Analysis.....	11
Business Process Analysis.....	11
Environmental Analysis	11
Process 2: Stakeholder Identification.....	12
Identify Stakeholders.....	12
Identify Stakeholder Responsibilities.....	12
Process 3: System Boundaries Identification.....	12
System Identification.....	12
Ascertain Control.....	13
Process 4: Threat Agent Identification & Selection.....	13
Threat Agent Identification.....	13
Threat Agent Selection.....	14
Process 5: Asset Identification.....	14
Asset Identification Using Staff Knowledge.....	14
Asset Selection.....	15
Process 6: Threat Agent Preference Structuring.....	16
Likelihood Analysis.....	16
Importance Analysis.....	16
Process 7: Vulnerability Identification & Selection.....	16
Vulnerability Type Structuring.....	16
Vulnerability Type Selection.....	16
Process 8: Threat Agent Attribute Calculation.....	17
Threat Agent Capability Calculation.....	17
Threat Agent Opportunity Calculation.....	17
Threat Agent Motivation Calculation.....	17
Process 10: Scenario Generation.....	17
Threat Identification.....	17
Scenario Construction.....	18
Scenario Unification.....	18
Process 13: Impact Analysis.....	18
Impact Field Identification.....	18
Tangible Impact Analysis.....	19
Intangible Impact Analysis.....	19
Process 14: Threat Statement Generation.....	19
CONCLUSION.....	21
REFERENCES.....	22

List of Figures

FIGURE 1 - TAME DIAGRAM.....	5
FIGURE 2 - PHASE 1 SCOPE OF ASSESSMENT.....	7
FIGURE 3 - PHASE 2 THREAT AGENT & VULNERABILITY ANALYSIS.....	8
FIGURE 4 - PHASE 3 SCENARIO CONSTRUCTION & SYSTEM MODELING.....	8
FIGURE 5 - PHASE 4 EVALUATION.....	9
FIGURE 6 - TAME DATA FLOWS.....	9
FIGURE 7 – STAKEHOLDER ROLES.....	12

List of Tables

TABLE 1 – THREAT AGENT LIST.....	13
TABLE 2 – ASSET LIST.....	15
TABLE 3 – THREAT AGENT PREFERENCE LIST.....	16
TABLE 4 – SUMMARY OF ATTACK SCENARIOS.....	18

Introduction

The wide development of the mobile Internet has destabilized the already fragile balance between the defenders and the attackers of computing infrastructures. That balance is very sensitive, being dependent on vulnerable computers controlling priceless information. The current risk assessment methodologies are obsolete weapons in the hands of techno phobic “grey haired” men. We should not repeat the mistakes of the 80s and go through a new “software crisis”. In today’s computing environment, organizations have been forced to allocate considerable resources for protecting their information assets. Unfortunately, worldwide statistics are indicating that things do go wrong, with catastrophic results most of the times. Computers are around for more than three decades. During that time we have learned that most risks cannot be avoided. What we should do instead is try to control them, to some extent, in a practical and cost effective manner. We argue that risk is not controlled by the assessors but by the threat agents. Having that in mind we developed a methodology called Threat Assessment Methodology for Electronic Payment Systems (TAME). TAME is a methodology for the assessment and analysis of threats and vulnerabilities within the context of security risk management and it consists of four stages. This methodology actively involves stakeholders and focuses upon a technical, socio-technical and business aspect of the system, and can form part of the wider risk assessment process.

TAME was developed during an EU framework-5 research project in order to perform the security assessment of a Micro-Payment System (MPS). After the application of the methodology to the prototype of the system, a number of issues came to surface. It was found that the methodology was too cumbersome, despite the development efforts to maintain a light and simplistic approach. This was addressed, and the outcome is the version of TAME that is presented in this paper. It was found that the “bones” of the methodology were light and accurate, but once all the activities were executed, the large number of the I/O operations was a hindrance towards the successful completion of the threat assessment. The ultimate goal of the developers of the methodology was to make the security auditor obsolete, and the specialized knowledge about threat assessment a luxury. TAME was developed with one purpose: to become a tool in the hands of any computer literate employee of any type of company.

The initial approach of TAME was to gather as much information as possible, put it on the table, and in cooperation with the stakeholders of the enterprise, filter everything and keep only data that were relevant to the scope of the assessment. The scope though was identified only after the cumbersome process of gathering the data. It was found that the above approach was time consuming and required the constant attention of the members of the enterprise. In other words, it was bringing the enterprise in a standstill until the end of the first assessment. The new approach of TAME tackles the above issues. The scope of the assessment is defined first in cooperation with the stakeholders of the enterprise, the relevant data are gathered from various sources, threat scenarios are constructed, which are then evaluated and approved by the stakeholders in order to calculate their impact towards the survivability of the enterprise.

TAME Overview

In agreement with Schneier (Schneier '01) the existing risk assessment methodologies, cannot address the needs of a modern computing system. There is still no clear distinction between a threat and a risk assessment although there have been a lot of discussions around the current methodologies. After the examination of the existing methodologies, a suitable one tailored to Electronic Payment Systems (EPS) was developed. All the examined methodologies were following the waterfall development model, which was not suitable for EPSs. These systems are generally sensitive and 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 useful for the business conducting the assessment. Furthermore, most of the examined methodologies were missing a very important factor, the factor of the business analysis for understanding the environment into which the business is operating.

Another development option was to follow the spiral development method. Yet again, even that is limiting the assessor to a specific sequence for conducting the different model stages. What we really want is the assessor

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. This can be seen in figure 1. The formal entry point of the methodology is Phase 1: Scope of Assessment. Depending on the information that is available to the auditor using the methodology, he can perform some system modelling (Phase 3: Scenario Construction and System Modelling) or he can perform some threat agent & vulnerability analysis (Phase 2). Of course, Phase 3 cannot really be executed without some inputs from Phase 2 (see later sections). Should the inputs are available though, then the auditor can move straight to Phase 3. Once information on threat agents and vulnerabilities are analysed, and relationships between them are identified, then the auditor might want to go back to Phase 1 and change the scope of the assessment. Eventually the auditor will run Phase 3, and construct the threat scenario that will be presented to the Stakeholders in Phase 4, for their evaluation. Once the stakeholders are consulted then there might be a need to change the scope of the assessment again or perform corrections to the threat agent and/or vulnerability data. After a number of cycles, the auditor will eventually execute process 14, which is part of Phase 4: Evaluation, which is the formal exit point of the methodology.

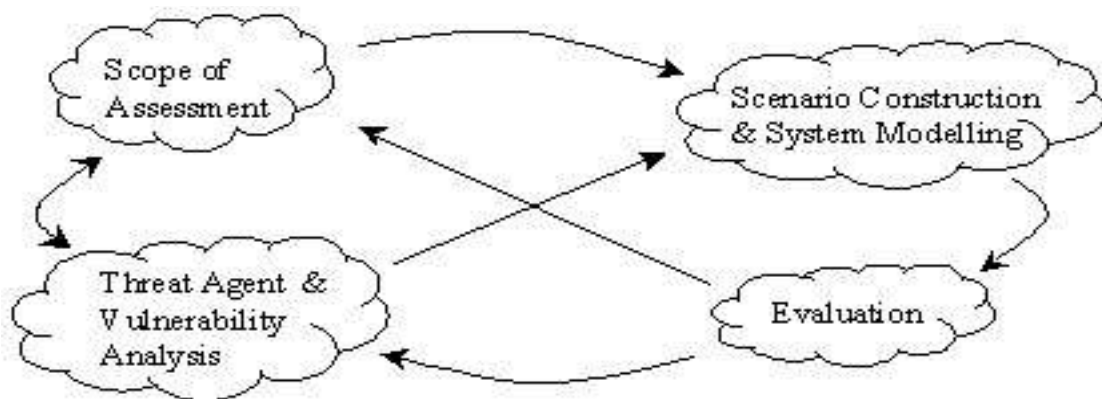


Figure 1 - TAME Diagram

According to Finne (Finne '98), a method is a set of steps used to perform a task, and a methodology is a set of tools, or research methods, translating management theory to management practice. TAME is a “third generation threat assessment methodology” that is based on the organisational analysis of the customer’s business, using business-modelling techniques. Internal and external stakeholders are actively involved through out the assessment.

Each phase contains a number of processes. Most processes are happening simultaneously (depending on the resources of the enterprise) 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. The ultimate goal of TAME is to help the security manager to decide how much security is necessary and where it should be applied. According to Hancock (Hancock '98) the above should be the only goal of a modern and effective threat assessment methodology.

The methodology examines organisational and technology issues to assemble a comprehensive picture of the threats facing a company. The four phases of the methodology contain the following processes and activities:

- Phase 1: Scope of Assessment
 - Process 1: Business Analysis,
 - Activity 1.1: Business Goals Analysis,
 - Activity 1.2: Business Processes Analysis,
 - Activity 1.3: Environmental Analysis,
 - Process 2: Stakeholder Identification,
 - Activity 2.1: Stakeholder Identification,
 - Activity 2.2: Stakeholder Responsibility Identification,
 - Process 3: System Boundaries Identification,
 - Activity 3.1: System & Boundary Identification,

- Activity 3.2: Ascertain Boundary Control,
 - Process 4: Threat Agent Identification & Selection
 - Activity 4.1: Threat Agent Identification,
 - Activity 4.3: Intention Identification
 - Activity 4.3: Threat Agent Selection
 - Process 5: Asset Identification & Selection
 - Activity 5.1: Asset Identification Using Staff Knowledge
 - Activity 5.2: Asset Identification Using Other Inputs
 - Activity 5.3: Asset Value Calculation
 - Activity 5.4: Asset Selection
- Phase 2: Threat Agent & Vulnerability Analysis
 - Process 6: Threat Agent Preference Structuring,
 - Activity 6.1: Likelihood Analysis,
 - Activity 6.2: Importance Analysis
 - Process 7: Vulnerability Identification & Selection,
 - Activity 7.1: Vulnerability Type Identification,
 - Activity 7.2: Vulnerability Type Selection,
 - Activity 7.3: Automated Vulnerability Identification,
 - Activity 7.4: Manual Vulnerability Identification,
 - Activity 7.5: Vulnerability Selection.
 - Process 8: Threat Agent Attribute Calculation,
 - Activity 8.1: Threat Agent Capability Calculation,
 - Activity 8.2: Threat Agent Opportunity Calculation,
 - Activity 8.3: Threat Agent Motivation Calculation,
 - Process 9: Vulnerability Complexity Calculation
 - Activity 9.1: Pre-analysis,
 - Activity 9.2: Structural Analysis,
 - Activity 9.3: Node Analysis,
 - Activity 9.4: Value Analysis,
 - Activity 9.5: Optimization Analysis,
- Phase 3: Scenario Construction & System Modeling
 - Process 10: Scenario Generation,
 - Activity 10.1: Threat Identification,
 - Activity 10.2: Scenario Construction,
 - Activity 10.3: Scenario Unification,
 - Process 11: System Modeling,
 - Activity 11.1: Pre-Analysis,
 - Activity 11.2: Structural Analysis,
- Phase 4: Evaluation
 - Process 12: Stakeholder Evaluation,
 - Activity 12.1: Output Identification,
 - Activity 12.2: Output Allocation,
 - Process 13: Impact Analysis,

- Activity 13.1: Impact Field Identification,
- Activity 13.2: Tangible Impact Analysis,
- Activity 13.3: Intangible Impact Analysis,
- Process 14: Threat Statement Generation

A discussion and a high-level overview of the above phases can be seen in the following pages. The numbering of the phases and of the processes is only for presentation purposes and for getting a better understanding of the data flows inside the methodology. The numbering does not declares some sort of priority in executing the phases or the processes inside those phases. Depending on the assessor, and the data available to him during the assessment, different paths might be followed in every cycle of the execution of the methodology.

In phase 1, the business area of the organization is identified and interrogated. This allow for the different stakeholders participating in the business to be identified. The information that has been gathered by this point can be used to identify the boundaries of the system. These boundaries will have to be protected from the threat agents. This need leads to another process. Threat agents that are active or inactive are being identified. These threat agents will be targeting assets. From the other processes of the methodology, the assessor has now the required information to perform the asset identification. All the information gathered from the above processes can be used as a first set of security requirements. The high level overview of phase 1, presenting its inputs and outputs, can be seen in Figure 2. Phase 1 is using information about the organization under analysis, staff knowledge and threat agent data for identifying boundaries, threat agents assets and stakeholders as well as understanding the environment that the organization is conducting business in.

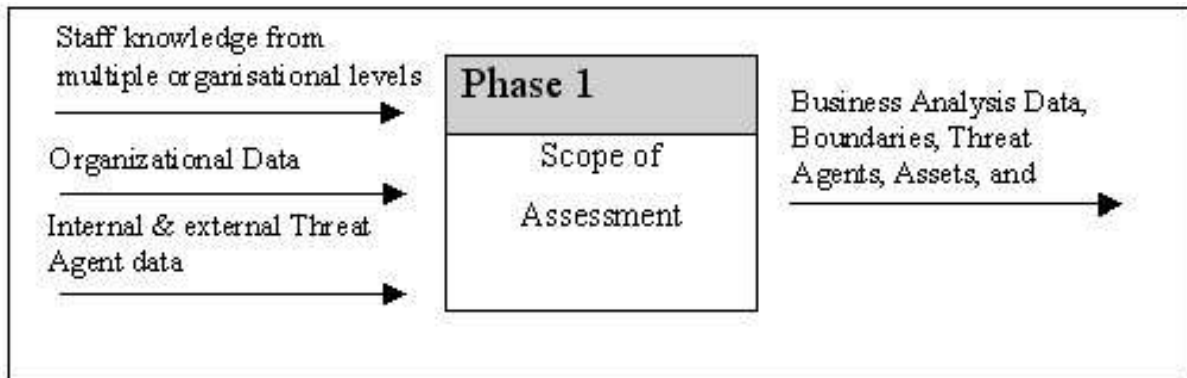


Figure 2 - Phase 1 Scope of Assessment

In phase 2, the threat agents identified in phase 1 are being examined and their attributes are analyzed. This will allow for a preference structuring according to their importance towards the organization. From all the previous phases, we have acquired enough information to perform a vulnerability identification, which will lead to the analysis of their exploitation complexity. This is taking under consideration the capabilities of the agents. The high level overview of phase 2, presenting its inputs and outputs, can be seen in figure 3.

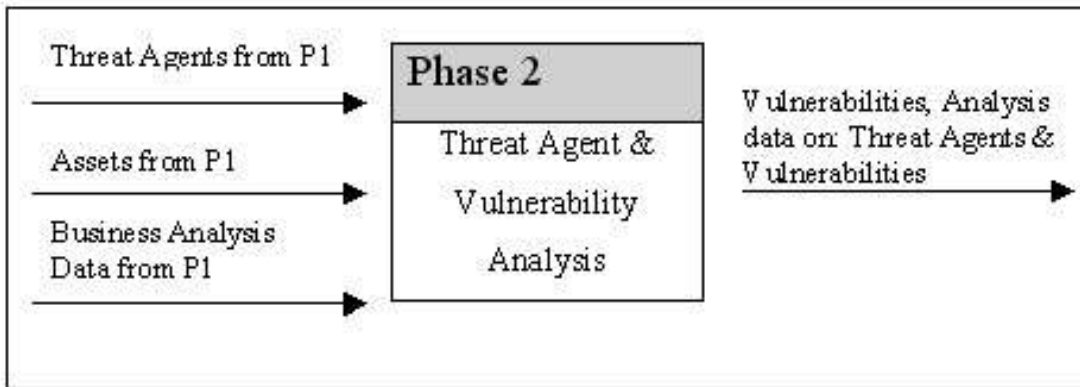


Figure 3 - Phase 2 Threat Agent & Vulnerability Analysis

In phase 3, information gathered from phase 1 & phase 2 can be used to create scenarios about threat agents (identified in phase 1, analyzed in phase 2), attacking individual assets (identified in phase 1), or processes, by exploiting one or more of their vulnerabilities (identified in phase 1, analyzed in phase 2). In this phase, for the first time in the methodology, all the three variables of a threat (threat agent, asset and vulnerability) are combined and examined as a whole. The outcome of the phase is the system models and the attack scenarios that will be used in the fourth phase. The output of this phase can be considered as a second set of security requirements that will have to be met. The high level overview of phase 3, presenting its inputs and outputs, can be seen in figure 4.

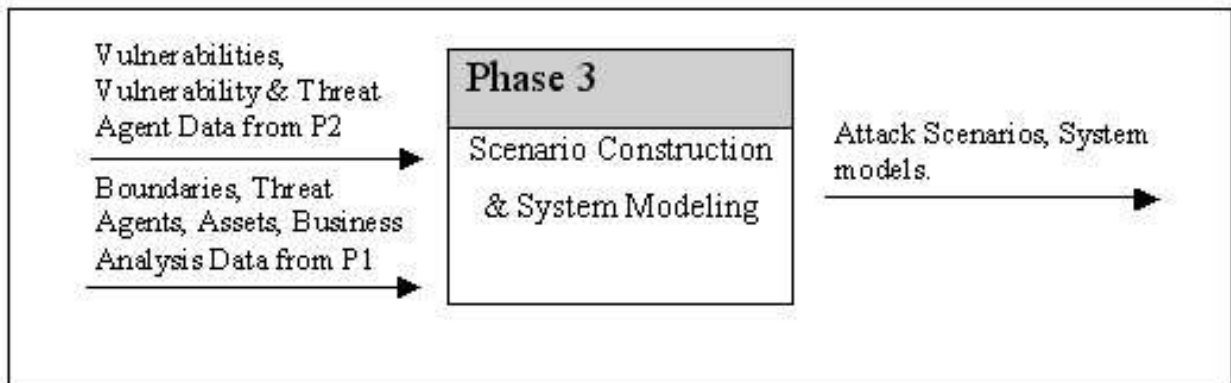


Figure 4 - Phase 3 Scenario Construction & System Modeling

In phase 4, the stakeholders are evaluating the results of each process, the impact of each threat identified in phase 3 is being calculated towards all the different levels of the business, and finally the threat statement is being generated and transferred over to the stakeholders of the business for their consideration. The high level overview of phase 4, presenting its inputs and outputs, can be seen in figure 5.

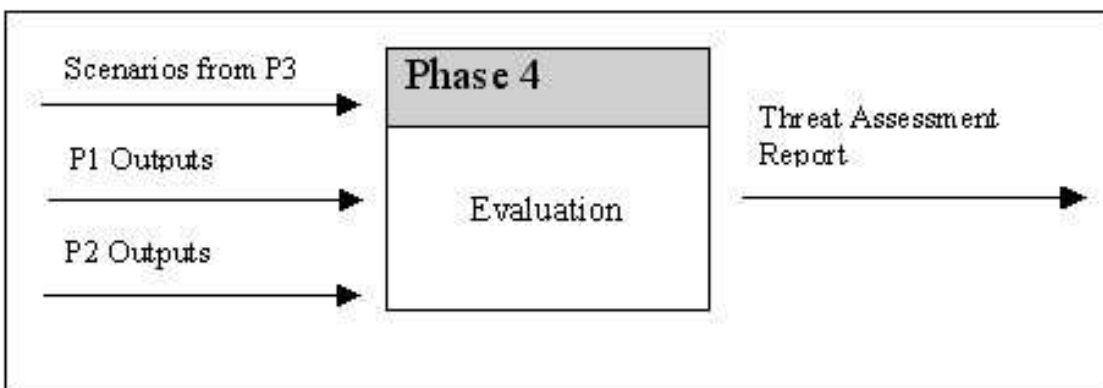


Figure 5 - Phase 4 Evaluation

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 of the methodology for getting meaningful results. Everything is dependent on the system under analysis. The simpler the system the fewer steps will have to be executed. The golden rule though is that the more steps the better the results. A high level overview of the data flows can be seen in figure 6. In the figure we can see the interactions between the different processes of TAME.

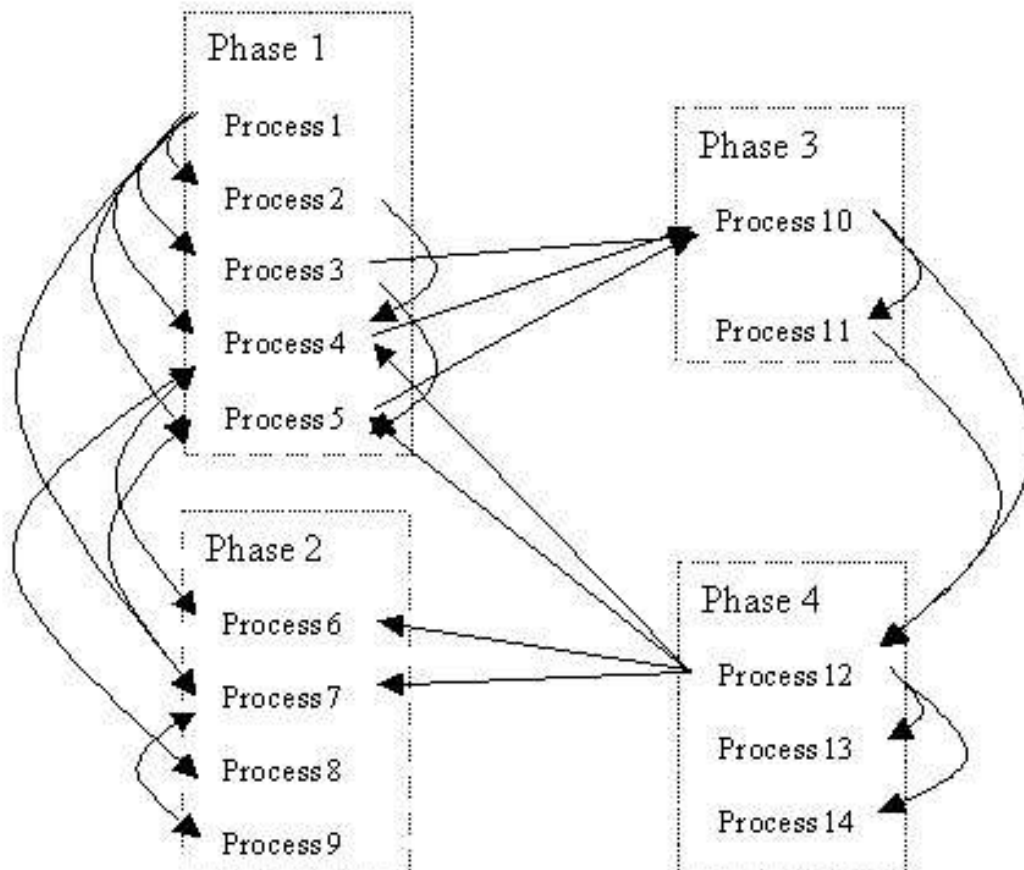


Figure 6 - TAME Data Flows

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 management will be provided with the impact of each threat that the enterprise 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. As an extension to the methodology, a module can be developed to associate each threat with one or more countermeasures based on two standards: the Common Criteria and the ISO17799. The need for been accredited is partially discussed by Eloff (Eloff '00). The need for having an assessment standard has been discussed and accepted by the EU and is one of its main goals under the eEurope 2005 initiative.

A proposed “path” for “running” TAME is the following. First determine the Scope of the Assessment where the system will be described in detail. The business environment and the business processes will get analyzed and

the stakeholders will get identified. The business analysis that is conducted in phase 1 will allow the identification of the business assets. In agreement with Nosworthy (Nosworthy '00) and Carroll (Carroll '96) the threat agent identification should be continuous. Hence, the Threat Agent Identification & Selection step is introduced in the scoping. The auditors should then conduct an analysis of the vulnerabilities and of the threat agents that the system is facing. Phase 2 is the Threat Agent & Vulnerability Analysis. After that we proceed to Phase 3, Scenario Construction & Modeling. In this phase, all the variables come together and the threats against the system are identified and evaluated. Here we construct one or more scenarios (depending on the threats that were identified and filtered) with the system under discussion, and the auditors model the system components that need further examination, using the information gathered in the Phase 1. Following that, we proceed to Phase 4. The stakeholders must evaluate the findings of the experiments and select the scenarios that will be further investigated. These scenarios will be unified and fused in one scenario. After the completion of the above steps, Process 13 will be able to estimate the impact of the identified threats to the various impact fields, and produce a statement based on the threat preference order. The methodology might be executed more than once. As the stakeholders are interacting with the experiment findings and the auditors, more information will surface and more variables will be introduced and/or excluded. The number of loops is left to the auditor. Presumably, each loop will provide the auditor with more detailed findings.

Example Scenario

KOMITIS is a unified Internet/mobile payment solution for contents and services, to be used in the so-called "Mobility Portals". A mobility portal is defined as Web/WAP information based system, which provides information or services related to mobility:

- Information related to a geographical position (which can be the position of the consumer or the one specified by him) or movement (how to go from a point to another one)
- Services like ticketing (entertainment, reservation, parking, etc.)
- Emergency services: reception of SMS signaling events (strikes or delays for travels, stock exchange conditions, etc.)
- Advertisement and advantages related to position or interest profile of the end-user.

A mobility portal has the major characteristics to address multiple terminals: fixed terminals like PC's or mobile terminals like mobile phones or PDA's. It also addresses multiple payment modes: aggregated and single payment.

The client can access the sites of on-line sellers to buy coupons, which are stored in the Core Payment System (CPS). The clients can then buy electronic/mobile contents using these coupons, which the CPS authenticates with an intermediary bank. Alternatively the client can pre-pay the bank and create an account with the system. The client can then use the CPS to buy e/m contents from online sellers, without dealing with the bank at all. The core system architecture combines an authentication layer at the CPS that connects to an aggregation engine and a single payment gateway that interfaces to an external payment system in charge of authorization and money transfers. Other important functional blocks are:

- Web back-offices: merchant back-office, consumer front-office, system/application back-office, that are all implemented as https portals,
- The system interconnection block.

The Core Payment System offers both aggregated and single payment mode, the authentication depending from the terminal capability. The KOMITIS model does not specify how the back-offices and front-offices work but only state their existence. Each implementation will use its specific interfaces. There are two specific and innovative solutions for on-line payments that will be used in the KOMITIS prototype. They represent state of the art solutions to the problem of open access aggregate payments with on-line central wallet and open access single payments. P-Wallet is a payment access solution that interfaces to multiple banking systems and to be more precise, SSL bank intermediaries. It can be used as a unique access point either for direct connections to central authorization/payment systems or to secondary access system like SSL intermediaries. P-Wallet is used for the single payments. Micro-CM is a typical third party aggregation system built for contents. It uses strong authentication through a security agent that wraps communication on http. Micro-CM is used for the aggregated payments.

Process 1: Business Analysis

Business Goal Analysis

Description: Business goals will lead bring to the surface important variables for our assessment such as key assets and key vulnerabilities. Business goals will also give an indication about threat agents, as other enterprises with common goals will have to be included in the threat agent list.

Inputs: Current knowledge of senior managers (I1.1), Current knowledge of stakeholders (I1.2), Information Security Policy Document (I1.3)

Outputs: Business Goal List (O1.1), (Successful deployment of KOMITIS system to Hellas, Achieve a threshold of 1000 users during the first six months of operation, Maintain the above threshold as a minimum number of users during the first year of operation).

Business Process Analysis

Description: By identifying critical business processes we identify more assets, and we bring to the surface more vulnerabilities.

Inputs: Current knowledge of senior managers (I1.1), Current knowledge of stakeholders (I1.2), Information Security Policy Document (I1.3), Knowledge of staff (I1.4), Organizational data (I1.5),

Outputs: Business Process List (O1.2), (Customer registration, Merchant registration, Contents management, Plafond authorization, Aggregated payment, Instant payment, Infrastructure, Human resource management, Money transfer).

Environmental Analysis

Description: 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. The environmental analysis will bring to surface more assets and help populating the threat agent table.

Inputs: Current knowledge of senior managers (I1.1), Current knowledge of stakeholders (I1.2), Current knowledge of staff (I1.4), Organizational data (I1.5)

Outputs: Omitted due to size limitations.

Process 2: Stakeholder Identification

Identify Stakeholders

Description: Each computer system will have a set of stakeholders who can be used to define its function and form.

Inputs: Information Security Policy Document (I1.3), Current knowledge of staff (I1.4), Organizational data (I1.5), Service Level Agreements (I2.1)

Outputs: Stakeholder List (O2.1) (Bank, University, TelcomA, Soft-house A, TelcomB, Soft-house B)

Identify Stakeholder Responsibilities

Inputs: Business Process List (O1.2), Information Security Policy Document (I1.3), Current knowledge of staff (I1.4), Organizational data (I1.5), Service Level Agreements (I2.1), Stakeholder List (O2.1)

Output: Responsibility List (O2.2). The following figure illustrates the roles of the different stakeholders of the system.

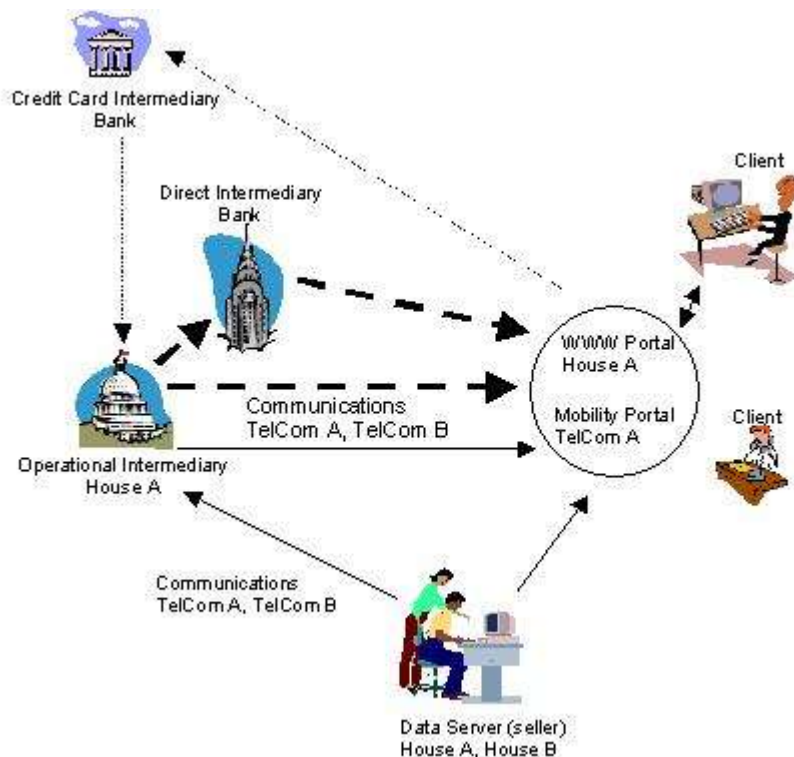


Figure 7 – Stakeholder Roles

Process 3: System Boundaries Identification

System Identification

Description: In this activity 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. These interactions will help identify more assets and vulnerabilities.

Inputs: Stakeholder List (O2.1), Current knowledge of senior managers (I1.1), Current knowledge of stakeholders (I1.2), Current knowledge of staff (I1.4), Service Level Agreements (I2.1)

Outputs: Boundary List (O3.1) (Firewall computers of the CPS, The KOMITIS gateway, the administrators/users of the system, the customers of the system).

Ascertain Control

Description: In this activity we ascertain who has control over each boundary, and what type of control it is.

Inputs: Boundary List (O3.1), Responsibility List (O2.2), Current knowledge of stakeholders (I1.2), Current knowledge of senior managers (I1.1), Current knowledge of staff (I1.4), Service Level Agreements (I2.1)

Outputs: Control List (O3.2). For presentation purposes the control list and the responsibility list have been integrated in Figure 7.

Process 4: Threat Agent Identification & Selection

Threat Agent Identification

Inputs: Threat agent catalogue (I4.1), History threat agent data (I4.2), Technical environment report (O1.3), Business environment report (O1.4), Physical environment report (O1.5), Current knowledge of senior managers (I1.1), Current knowledge of stakeholders (I1.2), Current knowledge of staff (I1.4), Stakeholder List (O2.1).

Outputs: Threat Agent List (O4.1)

Threat Agent Type	Threat Agent Description
Industrial Espionage	
TA 1	
TA 2	
TA 3	
Organised Crime	
Mafia	International – Italian and Russian based. Historically dealing with money laundering, construction, protection, debt collection, gambling, prostitution, smuggling, and small businesses. This type is not considered to be of any consequence for the trial.
Hackers and Crackers	Individuals and hacker groups will have to be identified during the lifetime of the complete system. It is pointless to analyse all the active agents in Europe. History data can be gathered from the authorities. This type is not considered to be of any consequence for the trial.
Pressure Groups	
Anti-Capitalist	Support for action in a large number of countries (Kyoto, Seattle, Geneva). Documented violent actions. The level of founding that they have is unknown. The types of targets they have been after included: city centres, world bank meetings, and the financial sector. All their actions are centred on a high level of publicity. This type is not considered to be of any consequence for the trial.

Table 1 – Threat Agent List

The companies included in the above table are involved with one or more electronic payment systems, which are competitive to the KOMITIS system. We do not suggest that the companies will actively get involved in some sort of industrial espionage. The threat is always there though and it would be catastrophic to exclude them from

the table of the possible threat agents. A complete assessment for the final system would include an in depth analysis of the above companies, of their capabilities and their actions since they were founded.

Threat Agent Selection

Description: This activity gives to the assessor the opportunity to select certain individuals or a certain threat agent category for further analysis, based on data received from the stakeholders of the enterprise, and from external threat agent sources.

Inputs: Threat Agent List (O4.1), Service Level Agreements (I2.1), Information Security Policy Document (I1.5), Current knowledge of stakeholders (I1.2)

Outputs: Threat Agent Preference List (O4.2), [TA 1, TA 2, TA 3]

Process 5: Asset Identification

Asset Identification Using Staff Knowledge

Description: This activity uses staff knowledge from all the levels of the enterprise, (staff-level, senior management, and stakeholders), to identify assets that are important for the operation of the system.

Inputs: Current knowledge of senior managers (I1.1), Current knowledge of stakeholders (I1.2), Current knowledge of staff (I1.4), Asset register (I5.1)

Output: Asset List (O5.1)

Asset Classification	Main Categories	ID Number
Hardware	I/O devices	
	Smartcard reader	0038
	Central machine	
	Appli.KOMITIS.net	0012
Software	Lillo.telcom.it	0013
	Fire.telcom.it	0014
	Routers	0045
	Application	
	SNORT	0001
	ACID	0002
	RSBAC	0003
	PostgreSQL	0004
	Rsync	0005
	SSH	0006
	BIND	0007
	APACHE	0008
	Operating System	
	DEBIAN "Woody"	0009
	SunOS 5.7	0010
	Programs	
	Xalan-Java 2	0011
Data	Sensitive	
	Customer transactions	0039
	Customer orders	0040
	www.KOMITIS.net	0046
	DNS Data	0047
	Software Banners	0048
	Operations	
	Customer registration	0015
Merchant registration	0016	
Contents management	0017	

	Plafond authorisation	0018
	Aggregated payment	0019
	Instant payment	0020
	Money transfer	0021
	Key Management	0041
	Generating Keys	0042
	Transferring Keys	0043
	Verifying Keys	0044
	Financial	
	Customer Details	0022
	Personal	
	Customer Details	0023
	Personnel	
	User Accounts	0024
Administrative	Documentation	
	KOMITIS Deliverables	0025
	Security Policy Document	0026
	Operations	
	Procedures	
	Inventory records	
	Operational procedures	
Communication		
	SSL	0049
	XML	0050
Human Resources	Computer personnel	
	House 1	0027
	System programmers	0027a
	Administrators	0027b
	House 2	0028
	Web developers	0028a
	Context administrators	0028b
	telcom A personnel	0029
	telcom B personnel	0030
	security analysts	0031
	web developers	0032
	bank clerks	0033
Physical	Environmental Systems	
	Environmental controls in secure server room in NTSys premises	0034
	Building	
	Software house A	0035
	Telcom A	0036
	Bank	0037

Table 2 – Asset List

Asset Selection

Description: This activity gives to the assessor the opportunity to select certain assets or a certain asset category for further analysis, based on data received from the stakeholders of the enterprise, and from the other activities of phase 1.

Inputs: Asset List (O5.1), Technical environment report (O1.3), Business environment report (O1.4), Physical environment report (O1.5), Current knowledge of stakeholders (I1.2), Boundary List (O3.1), Business Process List (I1.2), Business Goal List (I1.1).

Output: Asset Preference List (O5.2), [Data Operations (Customer Registration, Money Transfer), Hardware (Central Machine (Appli.KOMITIS.net, Lilo.telcom.it, Fire.telcom.it))].

Process 6: Threat Agent Preference Structuring

Likelihood Analysis

Inputs: Threat Agent Preference List (O4.2), History Threat Agent Data (I4.2), Current knowledge of senior managers (I1.1), Current knowledge of stakeholders (I1.2), Current knowledge of staff (I1.4).

Output: The activity does not produce a distinct output, but amends and updates O4.2

Threat Agent	Likelihood	Importance
Hackers and Crackers	0.5	3
TA 1	0	1
TA 2	0	1
TA 3	0	1

Table 3 – Threat Agent Preference List

Importance Analysis

Inputs: Threat Agent Preference List (O4.2), Technical Environment Report (I1.3), Business Environment Report (I1.4), Physical Environment Report (I1.5).

Output: Please refer to table 3 as for presentation purposes the two tables were integrated to one.

Process 7: Vulnerability Identification & Selection

Vulnerability Type Structuring

Description: This activity examines the scope of the assessment, the reports describing the environment into which the enterprise is functioning, to identify the different types of vulnerability categories that exist in the enterprise. These categories will then be populated by the other activities of this process.

Inputs: Default Vulnerability Type Catalogues (I7.1), Technical Environment Report (I1.3), Business Environment Report (I1.4), Physical Environment Report (I1.5).

Output: Vulnerability Type List (O7.1) was omitted due to size limitations.

Vulnerability Type Selection

Description: This activity gives the assessor the opportunity to select certain vulnerability types and the vulnerabilities included in the relevant lists for further analysis, based on data received from the stakeholders of the enterprise, and from the other activities of phase 1.

Inputs: Vulnerability Type List (O7.1), Current knowledge of stakeholders (I1.2), Technical Environment Report (I1.3), Business Environment Report (I1.4), Physical Environment Report (I1.5)

Output: Vulnerability Type Preference List (O7.2) [Masquerading, Bypasses, Active Misuse, Pest programs]

Process 8: Threat Agent Attribute Calculation

Threat Agent Capability Calculation

Description: This activity calculates the capability of each selected threat agent to exploit the selected vulnerabilities of the assets that were included in the assessment from Phase 1.

Inputs: Threat Agent Metrics (I8.1), History threat agent data (I4.2), Threat Agent Preference List (O4.2), Vulnerability List (O7.3), Vulnerability Preference List (O7.4)

Output: The activity does not produce a distinct output. It processes and amends the Threat List (O10.1).

Threat Agent Opportunity Calculation

Description: This activity calculates the opportunities that are presented to each selected threat agent for exploiting the selected vulnerabilities of the assets that were included in the assessment.

Inputs: Threat Agent Preference List (O4.2), Current knowledge of stakeholders (I1.2), Technical Environment Report (I1.3), Business Environment Report (I1.4), Physical Environment Report (I1.5), Vulnerability List (O7.3), Vulnerability Preference List (O7.4).

Output: The activity does not produce a distinct output; rather it processes and amends the Threat List (O10.1).

Threat Agent Motivation Calculation

Description: This activity calculates the motivation of each selected threat agent for exploiting the selected vulnerabilities of the assets that were included in the assessment from Phase 1.

Inputs: Current knowledge of senior managers (I1.1), Current knowledge of stakeholders (I1.2), Threat Agent Preference List (O4.2), Threat Agent List (O4.1), History threat agent data (I4.2), Threat Agent Metrics (I8.1), Vulnerability List (O7.3), Vulnerability Preference List (O7.4)

Output: The activity does not produce a distinct output; rather it processes and amends the Threat List (O10.1).

Process 10: Scenario Generation

Threat Identification

Description: This activity uses the information gathered from most of the processes we have analyzed up to this point, for producing a list containing all the interactions between the identified threat agents and the identified vulnerabilities.

Inputs: Threat Agent List (O4.1), Threat Agent Preference list (O4.2), Vulnerability List (O7.3), Vulnerability Preference List (O7.4), Asset List (O5.1), Asset Preference List (O5.2)

Output: Threat List (O10.1), (Omitted due to presentation and size limitations, results can be seen in later processes.)

Scenario Construction

Description: In this activity all the threats that were identified in the previous activity are used by the assessors in order to construct attack scenarios.

Inputs: Threat List (O10.1)

Output: Attack Scenarios List (O10.2). The attack scenarios are summarized in the following table.

Scenario	Threat Agent	Asset
Scenario A: Intelligence Gathering,	All	Disclosed
Scenario B: System Penetration	Hacker, Cracker, Script Kiddies	Disclosed
Scenario C: Denial of Service	Hacker	Disclosed
Scenario D: SSL Attack	Cracker	Disclosed
Scenario E: XML Attack	Cracker	Disclosed
Scenario F: Man in the Middle	Hacker, Cracker, Organized Crime	Disclosed
Scenario G: Bad Customer	Corporate Agent, Organized Crime, Industrial Espionage	Disclosed

Table 4 – Summary of Attack Scenarios

The following table summarizes the tools used throughout the execution of the attack scenarios.

Tool	Use
Whisker	CGI vulnerability check
Retina	Vulnerability identification
Netrecon	Vulnerability identification
Nmap	Port scanning
telnet	Remote access
ftp	Remote access
Traceroute	Network reconnaissance
Dig /	DNS interrogation
nslookup	
Whois	Network enumeration (registrar query, organizational query, domain query)
Ping (gping)	Ping sweeps
PacketX	SYN flooding
Friendly	Network reconnaissance & enumeration
Pinger	

All the attack scenarios were conducted using a test-bed consisting of the assets that were involved in the assessment.

Scenario Unification

Description: In this activity the scenarios constructed in the previous activity are being unified in one report that combines all the different perspectives from each scenario.

Inputs: Attack scenarios List (O10.2)

Output: Unified Scenario (O10.3)

Process 13: Impact Analysis

Impact Field Identification

Description: This activity uses the environmental reports from Phase 1 to identify the different business fields that a threat might affect. Taking under consideration the unified scenario, we now know the business fields that are likely to be affected by the examined threats.

Inputs: Current knowledge of stakeholders (I1.2), Technical environment report (O1.3), Business environment report (O1.4), Physical environment report (O1.5),

Output: Impact Field List (O13.1)

Tangible Impact Analysis

Description: This activity uses the threat information gathered in Phase 3, and the asset information gathered in Phase 2 to calculate the impact of the threat to the enterprise.

Inputs: Threat List (O10.1), Impact Field List (O13.1), Asset List (O5.1), Threat Agent Preference List (O4.2)

Output: The activity does not produce a distinct output; rather it processes and amends the Threat List (O10.1), by updating the impact attribute of each identified threat.

Intangible Impact Analysis

Description: This activity uses the threat information gathered in Phase 2, and the asset information gathered in Phase 1, to calculate the impact of the threats that are associated with intangible assets.

Input: Threat List (O10.1), Impact Field List (O13.1)

Output: The activity does not produce a distinct output; rather it processes and amends the Threat List (O10.1), by updating the impact attribute of each identified threat.

Process 14: Threat Statement Generation

Each attack scenario discussed in process 10 represents a threat. Briefly the threats are: intelligence gathering, system penetration, denial of service, ssl attack, xml attack, man-in-the-middle (unauthorized transactions), bad customer (sabotage). The same threat can have a variety of impacts depending on its realization. For example if there is a system penetration followed by a denial of service during the early hours of a day, but the customers do not realize it, then the impact will be a lot less severe than what it could have been. As it was discussed in process 13 the severity of the impact can be: minor, moderate, major, catastrophic, and the different fields that can be affected are: the human resources, the supply chain, the market share, the business capital, and the user trust.

The intelligence gathering is a threat that will be manifesting in a daily basis. Although it cannot be avoided it will have to be controlled, as it can be the first step towards an active more catastrophic attack. Should all the proposed countermeasures are in place, and should the details that are available to the public are not considered to be sensitive or classified, then the threat will have no impact what so ever. On the other hand, if the publicly available details contain data that can lead to personnel and to suppliers it might have a minor impact towards the human resources and towards the supply chain. For example, the information included in the web site of the system could lead to an employee and identify him as the connection between the system and the bank. A hacker can use that information to start gathering personal information that will help him identify usernames and passwords. Even worse, if the threat agent involved, falls under the organized crime category, he can start harassing the individual to part with sensitive information about the system. Back to the hacker, the suppliers of the system can also be identified from the web site. As it was mentioned before, the weakest link destroys the game. The hacker can now exploit the systems of the suppliers in order to identify holes that will allow him to attack the KOMITIS system. Here is where the system boundaries come into play. If in the future,

the enterprise start conducting business with external suppliers, then the new system boundaries must be identified and properly fortified.

The threat of the system penetration is a multi-layered one, depending on the asset that will be involved in the manifestation of the threat. If the system penetration is against any of the main hardware components of the system, and the attack is realized from the public, then even if it will have no other side-effects, the impact against the market share and the business capital will be major, and against the user trust it will be catastrophic. Furthermore if the threat agent penetrate the CPS, and get access in the financial and personal data of the customers, the impact against the market share and the user trust will be catastrophic. That is why the need for a multi-layered security is important. Just by securing the CPS with a firewall machine does not mean that the system is "hacker-proof". As it was identified in phase 1, there is a need to have very strict user permissions and in such a way that no one (not even the root) will be able to perform any modifications without authorization.

The denial of service is a threat that is directly linked with the user trust and the market share of the system. As it was discovered when analyzing other electronic payment systems, the user trust is the most important aspect of such a system. If the customer does not feel secure and confident in using the system, then it will definitely not use it. This will affect the market share of the system and in an extent the business capital. The realization of a series of manifestation of the above threat will have a catastrophic impact towards the examined fields. We do not believe that a single isolated incident will have any effect what so ever as it will be perceived as a glints of the Internet. Of course the reaction time of the system administrators is of the essence. If the system is down for anything more than a couple of minutes, that the incident will not be perceived as a glints but as a serious problem. That is why the concept of robustness is very important. If the administrators have backup equipment that they can bring on-line, that will provide the appropriate contingency.

The administration of the CPS was a real concern. According to the information gathered in phase 1, each server is hosting an SSL secured Web site dedicated to the administrators. To access these administration sites, the client must provide a valid X509 certificate. In this analysis we demonstrated how the SSL protocol can be broken and how the X509 certificates be acquired from the servers. It is essential that administrative connections are not accepted from the outside world. The only machines that should be able to remotely administer the CPS should be dedicated machines, not connected to the Internet, based on the premises of the stakeholder hosting the CPS. The discussion on the administration of the CPS and the vulnerabilities that it introduces can be seen in process 7 and 10.

As we are dealing with an on-line payment system, host integrity is the only issue between success and failure. If there is a breach in the integrity of one of the servers, and that breach is realized by the public, then we have demonstrated how catastrophic the impact will be. It is essential that certain countermeasures be deployed, no matter the costs, for ensuring that the data stored in the CPS and in the MGW are only accessible by authorized parties and in authorized ways.

It is well accepted that a system is never 100% secure. A threat agent with the proper motivation and the technical and financial capabilities can bring the KOMITIS system to a standstill. As it was proven, for causing a catastrophic impact to the system one hasn't got to break the 128bit keys that the system is using, nor to decode an XML pipe and start performing man-in-the-middle attacks. These are attacks that require a very good technical understanding of the involved principles, as well as the way in which the system is behaving and

functioning. It is very unlikely that an individual will be ever able to deploy such an attack. The problem though is that the system can be brought to its knees simply by causing a DoS, which will dissatisfy the customers and make them loose their trust towards the new on-line financial system.

CONCLUSION

Sun Tsu (Tsu '81) 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, 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. 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.

To conclude, TAME uses the assessor as an asset for better understanding the system that he/she is analyzing. 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. Traditional techniques cannot be used for modeling threats. People and professionals, who insist in doing that, should reconsider unless they want more catastrophic incidents with world wide impact to take place.

References

- (Schneier '01). Schneier, B. (2001). "Managed Security Monitoring: network security for the 21st century." Computers & Security **20**(6): 491-503.
- (Finne '98). Finne, T. (1998). "A Conceptual Framework for Information Security Management." Computers & Security **17**(4): 303-307.
- (Hancock '98). Hancock, B. (1998). "Steps to a successful creation of a corporate threat management plan." Computer Fraud & Security **1998**(7): 16-18.
- (Eloff '00). Eloff, M. M. and S. H. v. Solms (2000). "Information Security Management: a hierarchical framework for various approaches." Computers & Security **19**(3): 243-256.
- (Nosworthy '00). Nosworthy, J. D. (2000). "Implementing Information Security in the 21st Century - Do you have the balancing actors?" Computers & Security **19**(4): 337 - 347.
- (Carroll '96). Carroll, J. M. (1996). Computer Security, Butterworth-Heinemann.
- (Tsu '81). Tsu, S. and J. Clavell (1981). The Art of War, Hobber & Stoughton General.

