Economic Models and Approaches in Information Security for Computer Networks

Nicolas Sklavos and Panagiotis Souras
(Corresponding author: Panagiotis Souras)
Electrical & Computer Engineering Dept., University of Patras, Patras, Greece

(Received July 8, 2005; revised and accepted July 31 and Aug. 5, 2005)

Abstract

Security is one of the most important issues in computer networks. A common view of networks security is based on technical measures. Cryptographic models, firewalls and intrusion detection models are implemented in every information framework of an organization. Although deployment of such technologies may reduce security vulnerabilities and losses from security breaches, it is not clear to organizations how much they must invest in information security. In this article, common approaches of economics in information security are introduced. From the perspective of an organization, security is an investment to be estimated as cost-saving due to reduced losses from security breaches. Besides that, any new ventures that are profitable for the organization and would not be implemented without security countermeasures need to be considered. Any organization should follow a risk-management strategy according to their needs. Organizations that over-protect their information infrastructure will have spent too much on information security. Respectively, those who under-protect their information infrastructure will suffer grater losses caused by security breaches.

Keywords: Computer networks, economics, return on security information, risk management, security

1 Introduction

An information framework of any organization consists of logical and physical assets that can be grouped into five categories: information, software, hardware, humans and systems. The assets of a network system can be divided into several categories, similarly to computer systems, which can then be divided into smaller elements as shown in Table 1 [19].

Organizations, generally speaking implement an internal LAN, a demilitarized zone (DMZ) and an internet zone. Hence, regardless their size, typically are susceptible to risk due to the fact that they are connected to third party networks, typically, via internet.

Security has been defined as "the protection of information, systems and services against disasters, mistakes, and manipulation so that the likelihood and impact of security incidents is minimized" [17]. The main goals when implementing an information security system are *protection from unauthorized access, availability of information to authorized users, protection of information from integrity flaws, detection, as well as correction, of information security breaches.*

In case of unauthorized access to an organizations LAN, the unauthorized person will be capable of doing the following [5]:

- **Internet Use**: By accessing to another person's (authorized) account he achieves a high degree of anonymity. So, in case of harmful actions, targeting to other networks, all the suspicious will be pointed to the person holding the access account.
- **Picking up Communication**: The unauthorized person will be able to pick up any kind of communications within the organization's network.
- **Data Theft**: The unauthorized person will be able to read data stored within the network that are not accessible from outside.
- **Data Manipulation**: Besides the above the unauthorized person may possibly change or modify the data stored in the organization's network.

The potential decrease in Market Value due to IT security breaches is composed of both tangible and intangible assets [4]. Tangible costs are: *loss of productivity, loss of revenue, production waste it support, cost of system repair/replacement insurance.* Intangible costs are: *non-recoverable lost productivity, loss of reputation, reduction in "rand" value, loss of trading partner confidence, increased regulatory oversight, legal implications, safety costs & liabilities tariff and contractual implications.*

Table 1: Cost categories

Cost Category	Cost Elements
Equipment and Hardware	Computers (every kind), disks, tape drivers, printers, telecommunication network systems, modems.
Software	Operating Systems, Utility programs, Diagnostic programs, Application programs
Services	Commercially provided services such as teleprocessing, local batch processing, on-line processing, internet access, e-mail, voice mail, telephone, fax, packet switch of data.
Supplies	Any consumable item designed specifically for use with equipment, software, service or support service
Personnel	The salaries (compensation) and benefits for persons who perform functions such as development, support, management, operation and analysis for running the system.
Other resources	Any not included in the above categories

Considering the above one major question arises: "How much should an organization invest to ensure IT security?" The challenge is in discovering the optimal security investment that returns sufficient protection at an acceptable cost. The difficulty lies in evaluating the somewhat intangible values returned by various security options. Information security infrastructure must be diversifies defining the goals of the security infrastructure, is a critical step in thereby being able to measure how well the system performs. Different infrastructure and different implementation of that infrastructure will provide different functionality in varying environments. The task is to identify the correct combination, such that the benefit of information security is maximized, and loss (up front costs and cost due to security breaches) is minimized.

Multiple goals exist, as multiple threats and types of risk must be targeted, therefore a security system must be able to combat and respond across an array of measurable goals, or response variables. This means that the security system must be diversified such that it does not just provide good response in one area, and no response in another, but provides good response across all the response variables at hand.

In this paper, we introduce the key issues, regarding economic models, which are essential for the evaluation of an information security investment. First, we deal with networks typically deployed in an organizations LAN and the information security provided to users. In particular, we introduce basic cryptography issues of Wireless Local Area Network as well as some common type of threats related to that network. The main methods of calculating information security risk are introduced. Besides common risk quantification methods a common risk estimator known as Annual Loss Expectancy is presented.

We also present an optimization economic model delivered by Gordon & Loeb and a model delivered by Mizzi that is based upon the Cost To Break metric. The following part of this works is devoted to the ALE common framework which sets the rules for the calculation of the Return on Information Security. Another approach that is makes use of Internal Rate of Return is also given. Finally, useful conclusions are discussed based on the above economic models and approaches.

2 Networks and Security

Information technology security has emerged as an important issue in the last decade. Organizations typically employ multiple security technologies, for example, firewalls as a preventive control and Intrusion Detection Systems (IDS) as a detective control, to secure their IT systems. Assessing the value of these technologies is crucial, before the organizations make investment decisions. Whether firewalls and IDS complement or substitute each other depends critically on their qualities and the risk environment. For some organizations use of both technologies is worse than using only one of them.

Recent and future communication systems have special needs for cryptography. They must support the three basic types of cryptography: Bulk Encryption, Message Authentication and Data Integrity. Cryptography refers to a special process of computation used to protect a message. The security of a system is based upon the difficulty of the inverse computation. Generally there are three types of cryptographic systems: *Totally Secret, Public Algorithms, and Public Key Systems*. The history teaches us that the attacker's methods follow, and attempt to match any good cryptographic system design. Several technologies and protocols for wireless networks have been developed in order to meet the growing interest in mobile communications.

The Wireless Local Area Network (WLAN), typically known as IEEE 802.11, specifies an optional encryption part named Wireless Encryption Privacy (WEP). The encryption that WEP offers is either 64-bit RC4 with a 40-bit secret key or 128-bit encryption mode. The authentication function uses the same key that encryption does.

This fact imports a high level of risk for the protocol regarding security.

Possible ways of attack to the encrypted data are:

- **Calculation of the Password**: Recording of the encoded data packet may give the attacker the ability to calculate the key by WEP encryption method. This fact gives him the possibility to decode the entire encoded data packet, as well as transmit data via the network [2].
- **Dictionary Attack**: If the attacker doesn't know the password decoding of single data packets can be achieved by recording a substantial amount of encoded data packets [16].
- **Packet Modification**: Modification of specific parts of the encoded data packets can be achieved without knowing the code-key [16]. This is possible due to the fact that bits in data packets may be tipped and considering that the structure or part of the content of them is known to the attacker.
- **Packet Creation**: The attacker can create an encoded package of any size if he knows the packets encoded and unencrypted content (authentication request and authentication reply packet) [1].
- **Brute Force Attack**: The attacker may guess the password through trial and error. In some cases a few minutes are enough to guess the correct password [11].
- **Replay Attack**:Encoding of an already encoded message creates the decoded message. So the attacker records an encoded message and sends it back to the network via the base station. The base station will then re-encode the message but in fact the transmitted message will de unencrypted [16].
- **Evil Twin**: In such attack a second base station named as the original one but with greater transmitting power is installed. Because of that, most of the clients will use the second base station. In case of that base station is operated without encryption, the clients will often deactivate encoding. Hence, the attacker (known as man-in-the middle) will have access to unencrypted data, and will be able to modify them in order to deactivate any security mechanisms he wishes [20].

3 Risk Management

Risk is the possibility of something adverse happening. Risk management is the process of assessing risk, taking steps to reduce risk to an acceptable level and maintaining that level of risk. Risk management requires the analysis of risk, relative to potential benefits, consideration of alternatives, and, finally, implementation of what management determines to be the best course of action [18].

Quantification of risk can be achieved via a simple mathematical equation [12, 14]:

$$RISK = VA \times SV \times LA,$$

where VA stands for Value of the asset, SV stands for Severity of the Vulnerability, and LA stands for Likelihood of an attack.

Each risk factor is measured by a weight 1-10 (10 being the most severe or highest). Hence, by multiplying the factors we arrive at an aggregate risk value for any asset.

Another way of defining risk is given by the following equation:

$$RISK = LLE \times CLE$$
$$SecurityRisk = LSB \times CSB,$$

where LLE stands for Likelihood of Loss EventV, CLE stands for Cost of Loss Event, LSB stands for Likelihood of Security Breach, and CSB stands for Cost of Security Breach.

In a general case in which more then one loss event or breach may occur, security risk may be defined in terms of the frequency with which breaches are expected to occur (or the security breach rate):

$$SecurityRisk = SBR \times ACPB,$$

where SBR stands for Security Breach Rate and ACPB stands for Average Cost Per Breach.

3.1 Annual Loss Expectancy

One of the earliest used estimators, of loss due to security breach in the computer industry was a quantitative method for performing risk analysis known as the Annual Loss Expectancy (ALE). It was published in 1979 by the National Bureau of Standards [10]. The document sets the risk assessment standard for large data-processing centers and also proposed ALE. That metric is the product of the expected yearly rate of occurrence of the event times the expected loss resulting from each occurrence [10, 8, 15]:

$$\begin{aligned} ALE &= \text{expected rate of loss} \times \text{value of loss} \\ &= \sum_{i=1}^{n} I(O_i)F_i \end{aligned}$$

where $(O_i, \cdots, O_n)$: Set of Harmful Outcomes, $I(O_i)$: Impact of Outcome i in dollars, and F_i: Frequency of Outcome i.

The method's appeal rests in its combination of both risk components into a single number [8]. This simplicity turns out to be its primary drawback, as well. The blending of the two quantities has the disadvantage of being unable to distinguish between high-frequency, low-impact events and low frequency, high impact events. In many situations, the former may be tolerable, while the later may be catastrophic.

3.2 Summary

Risk management is an iterative process, which should lead to continuous improvement in an organization's security infrastructure. Risk management is often characterized as a lifecycle of processes, and while there are many different opinions on the varying methodologies, there are four main strategies for coping with risk:

Avoidance: If the numerator of the risk equation is small or if the probability of a threat exploiting vulnerability is low or the impact is low.

Acceptance: Often the guiding principles used when accepting risk, are in dealing with situations where the cost is significant to effect a reduction, in the overall risk. One example could be paying for an operating system upgrade for 1000 host machines, when one feels the existing systems are only slightly more vulnerable than hosts running the new operating systems. In this case, one may choose to do nothing and accept the risk of the older operating system.

Transference: In other words, assign the risk to someone else. The most common way to do this is via insurance. However, cyber insurance for issues like e-commerce loss is still immature and often provides incomplete coverage.

Mitigation: Most often, corporate security departments will choose risk mitigation-taking some actions and making some investments to measurably reduce risk in a given scenario.

4 Financial Approaches in Information Security

The cost of information security is based upon implementing infrastructures that make the organizations network "safe" from attacks. So, the benefits of such an implementation are directly related to the cost-savings that has to do with prevention of losses made by security breaches. Gordon and Loeb [6] suggested an optimization economic model for the evaluation of information security investment based upon cost and benefits.

Let total benefits of implementation of information security infrastructure be B, the total cost of that implementation C, and the different levels of information security S. The goal is to determine the point where the gain, denoted as G, related to S is maximum. From mathematical point of view that point can be found by the following analysis:

$$\begin{aligned} G(S) &= B(S - C(S)) \\ \frac{dG}{dS} &= \frac{dB}{dS} - \frac{dC}{dS} = 0. \end{aligned}$$

In other words, $\frac{dB}{dS} = \frac{dC}{dS}$ or marginal benefits are equal to marginal costs.

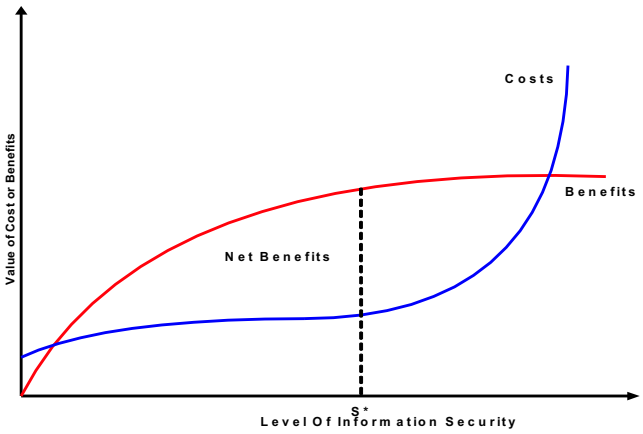


Figure 1: Benefits and costs of information security

This mathematical analysis is also illustrated in the following graph [6] of Figure 1.

Another approach [9] suggests that the total annual security expenditure of an organization is given by the following equation:

$$E_S = F + B + M,$$

where **F** stands for the annual cost to fix vulnerabilities, **B** stands for the cost of implementing defense mechanisms to protect IT from attacks, and **M** stands for the annual cost of upgrades and updates of the defense mechanisms.

Total annual loss due to security breaches is defined as:

$$L_T = L_I + A(t) + r(t),$$

where L_I stands for the instantaneous loss caused by a successful attack, **A(t)** stands for a function that describes the way that the revenue of the information assets at stake is lost over time. $A(t)$ is defined by the equation:

$$A(t) = I \times t/365,$$

where **I** stands for the value of the information assets at stake, **t** stands for the time period, in days, that the system is unavailable.

Finally, $r(t)$ stands for the cost to rebuild the system considering the man-hour labor cost, as well. The security implementation is viable if

$$E_S < L_T$$

or alternatively:

$$(F + B + M) < [L_I + A(t) + r(t)]$$

Damage can be done to defense mechanisms of the system as well as to the underlying infrastructure that hosts the information assets. The cost to repair annual damages is defined as:

$$D = D_D + D_I,$$

where D_D stands for damages to defense mechanism, D_I stands for the damages to infrastructure.

Taking account the above, the previous inequality is extended to:

$$(F + B + M) < (L_I + A(t) + r(t) + D).$$

The metric *Cost To Break* (CTB) [13] of a system is defined as the lower expected cost for anyone to discover and exploit a vulnerability in that system. Annual Cost to Break is defined by the following equation [9, 13]:

$$CTB = C_D + C_V,$$

where C_D stands for the annual cost to break into the defense mechanisms, C_V stands for the annual cost to exploit vulnerabilities in the system.

It is a common sense that the attacker is not willing to spend too much money to break or abuse a system. Thus, as long as the CTB is greater than the cost of the security implementation the information system may be considered to be safe. Of course, negligence or wrong configuration of the most expensive defense mechanism makes it worthless but generally speaking a well designed security system must satisfy the following inequality:

$$CTB > E_S$$

or

$$CTB > (F + B + M)$$

or alternatively

$$CTB < (L_I + A(t)).$$

There are cases however, where the perception of information value is greater for the attacker than the legal owner. In that case the motivation to break the system remains high even with a high CTB. The above analysis is illustrated [9] in the next Figure 2.

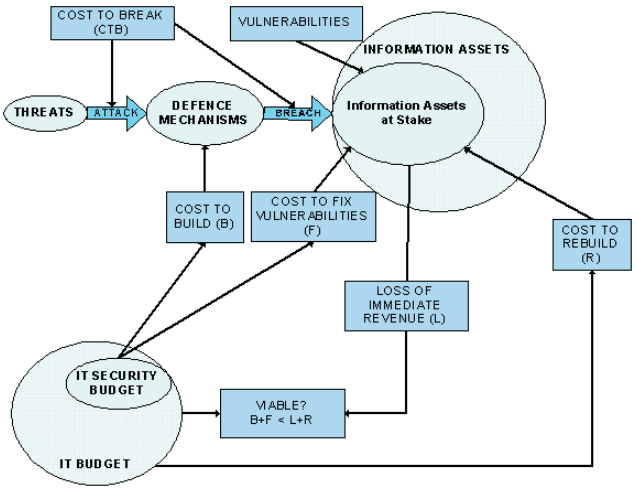


Figure 2: Viability of an information security investment

5 Return on Security Information

The **ALE** framework had seven basic elements [3]:

1) Requirements, $R = [R1, R2, R3, \cdots, Ri]$, these requirements specify the maximum expected loss of the system. For example, a requirement could be that expected loss must be less than $100,000.

2) Assets, $A = [A1, A2, A3, \cdots, Ak]$, the assets that the security system will be protecting, such as hardware, software, data.

3) Security Concerns, $C = [C1, C2, C3, \cdots, Cs]$, e.g. confidentiality, integrity, authenticity.

4) Threats, $T = [T1, T2, T3, \cdots, Tm]$, e.g. human, natural.

5) Safeguards, $S = [S1, S2, S3, \cdots, Sp]$, e.g. firewall, system admin, intrusion detection system.

6) Vulnerabilities, $V = [V1, V2, V3, \cdots, Vq]$, e.g. physical, software, hardware, administrative.

7) Outcomes, $O = [O1, O2, O3, \cdots, Or]$, e.g. combinations of A, C, T, S, V.

The framework also included three associated quantities:

1) Asset Values: $Aval = [A1val, A2val, \cdots, Akval]$.

2) Safeguard Effectiveness: $Seff = [S1eff, S2eff, \cdots, Speff]$.

3) Outcome Severity: $Osev = [O1sev, O2sev, \cdots, Orsev]$.

The framework called for an assessment of the above quantities in an iterative process [3] as diagrammed in the following Figure 3.

First step includes the identification of the security requirements, assets to be protected, security concerns, possible threats, vulnerabilities, and safeguards. Once these have been identified, an analysis phase takes place. During the analysis phase, a threat analysis is conducted in order to examine all the possible threats that are posed to the assets. Next a vulnerability analysis is conducted to identify weaknesses in the current security architecture, which may not currently exist, that might enable a successful attack against one or more of the assets. Finally scenario analysis takes place, the most important step in the analysis phase. This step requires a detailed evaluation of assets, security concerns, threats, and vulnerabilities to generate all possible scenarios whereby attacks could occur.

Once these scenarios are fully listed, a risk measurement step is conducted to measure the amount of risk (potential impact and probability) of each scenario, in order to perform the acceptability tests, where cost-benefit

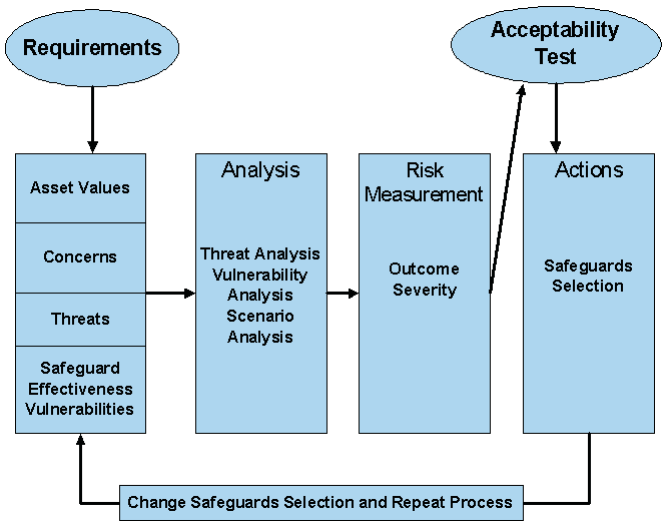


Figure 3: Common framework process diagram

analysis takes place. During cost-benefit analysis, the risk measured for a given asset and the established requirements are compared, and finally decisions on safeguards are made to close the gap, if it exists, between risk measured and the established requirements. The entire process is then repeated under the new safeguard regime, resulting in a new risk measurement for each asset. These risk measurements along with assessments of safeguard cost are then used to generate cost-benefit analysis for each safeguard.

The cost savings resulted from the above analysis, in other words the reduction in ALE is [15]:

$$S = ALE_{\text{BASELINE}} - ALE_{\text{WITH SAFEGUARDS}}.$$

The total annual benefit B is delivered by the following sum:

$$B = S + (\text{profit from new ventures}).$$

Return on security investment, also known as security ROI is defined [15] by the following equation:

$$\begin{aligned} ROI &= \frac{Benefit\ of\ Safeguards}{Cost\ of\ Safeguards} \\ &= \frac{(savings\ from\ safeguards)}{cost\ of\ safeguards} + \\ &\qquad \frac{(profit\ from\ new\ ventures)}{cost\ of\ safeguards} \\ &= \frac{ALE_{BASELINE} - ALE_{WITHSAFEGU\ ARDS}}{cost\ of\ safeguards} \\ &\qquad + \frac{(profit\ from\ new\ ventures)}{cost\ of\ safeguards}. \end{aligned}$$

The annual benefit of a security investment is considered to be received not only the first year but in all subsequent years.

Another approach [7] suggests that organizations should discard the above ROI calculation and instead make use of the Internal Rate of Return (IRR). That's because IRR incorporates discounted cash flows for investments that have different costs and benefits in different years. IRR is delivered by the solution of the following equation:

$$C_0 = \sum_{i=1}^{n} \frac{B_t - C_t}{(1 + IRR)^t}$$

where C_o is the initial cost of an investment in information security, C_t is the respective cost in year t, and B_t is the respective benefit in year t.

6 Conclusions and Outlook

When an organization designs its information security infrastructure apart from technical issues a risk-management strategy should be carried out. Although the technical aspects of information security have been the subject of much research little has been done in the area of economics concerning that implementation. Networks typically deployed in an organizations LAN generate various types of threats according to the type of the network as well as the type of information stored within the network.

Investment is a crucial issue in the implementation of any computer network infrastructure. That's because the organization should not pay more than the value of the information assets protected by the security mechanisms. Risk quantification methods have been introduced as well a model of risk estimation based upon Annual Loss Expectancy. Key issues, which are essential for the evaluation of an information security investment, are cost of implementation and benefits resulted from that implementation. So, a common model that estimates Return On Security Investment is based upon those two factors. According to other approaches, the metric used for the calculation of ROSI is Cost to Break or a common ALE framework is implemented. Although much has to be done, organizations have powerful tools at their service to calculate the ROSI of their implementation.

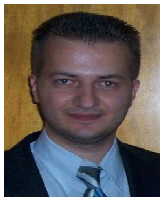
References

[1] W. A. Arbaugh, *An Inductive Chosen Plaintext Attack Against WEP/WEP2*, IEEE Document 802.11 -01/230, TGI Working Group, Orlando, May 2001.

[2] N. Borisov, I. Goldberg, and D. Wagner, "Intercepting mobile communications: the insecurity of 802.11," in *Proceedings of the 7th Annual International Conference on Mobile Computing and Networking (Mobicom'01)*, pp. 180-189, Rome, Italy, Jan. 2001.

[3] R. P. Campbell et al, "A modular approach to computer security risk management," in *AFIPS Conference Proceedings*, vol. 48, pp. 293–304, AFIPS Press, 1979.

[4] G. Crawford, "Utility case study security program implementation & cost recovery strategies," in *American Gas Association Technology Advisory Council Meeting, Security and Technology Solutions, Ernst & Young*, Apr. 2003.
[5] M. Dornseif, K. H. Schumann, and C. Klein, "Factual and legal risks regarding wireless computer networks," *Computing Research Repository (CORR)*, CS. CY/0204021, Apr. 2002.
[6] L. A. Gordon and M. P. Loeb, "Economic aspects of information security," *Security Tech Trends Notes*, vol. 110, no. 4, pp. 8–15, Fall 2001.
[7] L. A. Gordon and M. P. Loeb, "Return on information security investments: myths vs. realities," *Strategic Finance*, vol. 84, no. 5, pp. 26–31, Nov. 2002.
[8] K. J. S. Hoo, "How much is enough? A risk management approach to computer security," *Consortium for Research on Information Security and Policy (CRISP)*, working paper, 2000.
[9] A. Mizzi, "Return on information security investment. Are you spending enough? Are you spending too much?," *posted in ACM IT Security Toolbox*, Jan. 2005.
[10] National Bureau of Standards, *Guideline for Automatic Data Prossesing Risk Analysis*, FIPS PUB 65, Washington D.C., General Printinf Office, U.S, 1979.
[11] T. Nweshai, "Cracking WEP keys," in *Black Hat Briefing Conference*, Las Vegas, Nevada, July 11-12, 2001.
[12] J. Reavis, *Managing Risk and Reducing the Cost of Web Application Security*, Chief Security Officer, White paper series, Jan. 2004.
[13] S. Schrecher, "Quantitatively differentiating system security," in *First Workshop on Economics and Information Security*, pp. 176–182, May 16-17, 2002.
[14] S. E. Schechter, "Toward econometric models of the security risk from remote attacks," in *3rd Workshop on Economics and Information Security*, Las Vegas, Nevada, pp. 87–92, May 13-14, 2004.
[15] S. E. Schechter, *Computer Security Strength & Risk: A Quantitative Approach*, PhD Thesis, Harvard University, Massachusetts, June 2004.
[16] A. Stubbefield, J. Joannidid, and A. D. Rubin, *Using the Fluhrer, Mantin and Shamir Attack to break WEP*, AT&T Labs Technical report, Report number: TD 4ZPZZ, Aug. 2001.
[17] R. Summers, *Secure Computing*, McGraw Hill, 1997.
[18] M. Swanson and B. Guttman, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, National Institute of Standards and Technology, U.S. Department of Commerce, Sep. 1996.
[19] H. Wei, D. Frinke, O. Carter, and C. Ritter, "Cost-benefit analysis for network intrusion detection system," in *28th Annual Computer Security Conference*, pp. 157–164, Washington D.C, Oct. 29-31, 2001.
[20] ISS Whitepaper, "Wireless LAN security," *Internet Security Systems*, 2001.



Dr. Nicolas Sklavos received the Ph.D. Degree in Electrical & Computer Engineering, and the Diploma in Electrical & Computer Engineering, in 2004 and in 2000 respectively, both from the Electrical & Computer Engineering Dept., University of Patras, Greece. His research interests include Cryptography, Wireless Communications Security, Computer Networks and VLSI Design. He holds an award for his PhD thesis on "VLSI Designs of Wireless Communications Security Systems", from IFIP VLSI SOC 2003. He has participated to international journals and conferences organization, as Program Committee Member and Guest Editor. Dr. N. Sklavos is a member of the IEEE, the Technical Chamber of Greece, and the Greek Electrical Engineering Society. He has authored or co-authored more than 80 scientific articles, books chapters, tutorials and reports, in the areas of his research. Contact him at: nsklavos@ieee.org.

Panagioths Souras (Contact Author) received the Diploma of Electrical Engineering in 2004, from University of Patras, Greece. His research interests include Cryptography, Security and Networks. He is a referee of both international journals and conferences. P. Souras has published several technical papers in the areas of his research. Contact him at: taksou@yahoo.com.