A taxonomy for information security technologies

H.S. Venter[1] and J.H.P. Eloff[2]

Department of Computer Science, University of Pretoria, 0002, Pretoria, South Africa,
Tel.: +27 12 420-2361,
Fax: +27 12 362-5188
[1] Email: hventer@cs.up.ac.za
[2] Email: eloff@cs.up.ac.za

Abstract

The Internet is a public network, which is open and used by all — also for communicating private information. "But private information should be secured!", I hear you say. Yes. But where should one start looking for help when attempting to secure private information? This paper discusses a taxonomy for information security technologies, which provides information on current state-of-the-art technologies used to secure information at application, host and network level.

Keywords: access control, biometrics, remote access, passwords, cryptography, digital signatures, digital certificates, firewalls, virtual private networks, intrusion detection systems, vulnerability scanners, anti-virus scanners, security SDKs, logging, security protocols, security hardware.

1. Introduction

As the Internet took the world by storm in the mid-1990s, so did security problems. Unfortunately 'bad people', better known as hackers today [1], found ways in which they could jeopardise computer systems and the Internet for reasons such as to unlawfully obtain sensitive information or simply to cause havoc by attacking resources on the Internet.

For example, hackers developed their own software which enabled them to sniff a password being sent over the Internet. In another example, a hacker might send malicious data over the Internet so that servers connected to the Internet will not be able to handle such malicious data and will simply cause the servers to fail.

Fortunately, intensive research in computer and Internet security has proved to deliver countermeasure technologies over the past decade for the majority of these and other security problems. This paper provides a taxonomy of information security technologies available today.

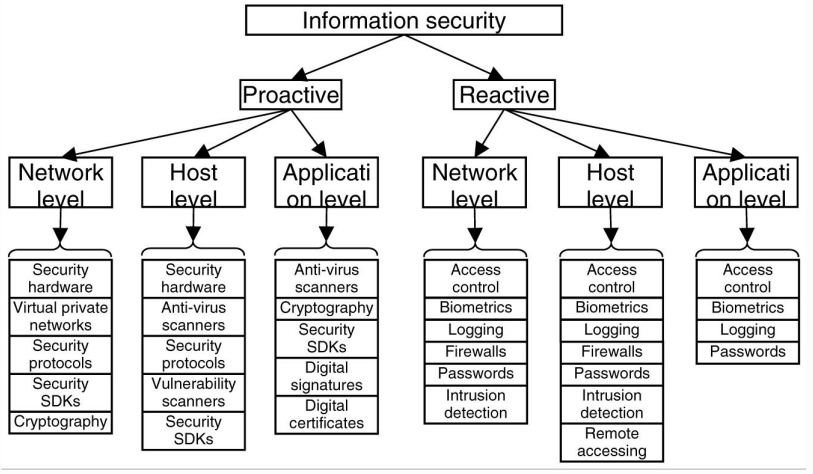
The sections that follow will give a taxonomy of the information security technologies available today, after which each technology is briefly explained.

2. A taxonomy for information security technologies

What is information security technology? *Information security* is the protection of information [2] and minimises the risk of exposing information to unauthorised parties [3]. According to Dictionary.com, *technology* is "the application of science, especially to industrial or commercial objectives" [4]. *Information security technology* thus refers to the application of all possible state-of-the-art security technologies to all possible information on the Internet [5].

Figure 1 shows a taxonomy of information security technologies. What is a taxonomy? It is

Figure 1: A taxonomy of information security technologies.



the classification of objects in an ordered list or hierarchy of terms that indicates natural relationships [6, 4]. This taxonomy is based primarily on two characteristics:

1. The specific point in time, namely proactive or reactive, when the technology interacts with data.
2. Whether the technology interacts at network, host or application level.

Proactive means that preventative measures have been taken by the specific information security technology in a bid to secure data or resources before a security breach can occur. *Reactive* means that curing measures are being taken by the specific information security technology in a bid to secure data or resources as soon as a security breach is detected. Both proactive and reactive information security technologies can apply to *network*, *host* or *application* level. Information security technologies at *network level* attempt to secure data or resources being transmitted over a system of computers interconnected by telephone wires or other means in order to share information. Information security technologies at *host level* attempt to secure data or resources that reside on a single computer. Information security technologies at *application level* attempt to secure data or resources that specifically relate to a single computer program on a host.

Figure 2: Resources covering the information security technologies.

Resource	Access control	Biometrics	Remote access	Passwords	Cryptography	Digital signatures	Digital certificates	Firewalls	Virtual private networks	Intrusion detection systems	Vulnerability scanners	Anti-virus scanners	Security SDKs	Logging	Security protocols	Security hardware
Journals																
Computers & Security [7]	✓	✓	✓	✓	✓	✓	✓	✓		✓		✓	✓	✓	✓	
Computer Fraud & Security [8]		✓		✓	✓	✓	✓			✓	✓	✓		✓		✓
Network Security [9]		✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Books																
Internet & TCP/IP Network Security [10]			✓				✓				✓				✓	
Secure Communicating Systems [11]					✓											
Computer Security Policies [12]							✓	✓	✓					✓		
Windows 2000 Security [13]	✓		✓		✓	✓	✓		✓				✓	✓	✓	✓
Hackers Beware [14]				✓							✓			✓		
Computer Security [15]	✓			✓	✓							✓		✓		
Hacking Exposed [16]			✓	✓				✓		✓	✓	✓	✓	✓		
Intrusion Detection [17]										✓	✓			✓		✓
Network Intrusion Detection [18]										✓	✓	✓			✓	
Access Denied [1]	✓	✓		✓	✓	✓			✓			✓				
Internet & Intranet Security [19]						✓		✓			✓				✓	
Secrets & Lies [20]		✓			✓						✓	✓	✓			✓
Security Architecture [3]	✓				✓		✓	✓	✓	✓	✓		✓	✓		✓
Security in Computing [21]	✓				✓	✓		✓				✓				✓
Computer Security [22]	✓			✓		✓						✓	✓			
Information Security Architecture [23]	✓	✓	✓	✓				✓	✓			✓				
Web Security [24]	✓		✓	✓		✓	✓	✓					✓	✓	✓	
Web Security [25]			✓			✓	✓					✓	✓		✓	

A comprehensive literature study was conducted to identify the state-of-the-art information security technologies available. This is indicated in Figure 2. A distinction was made between journals and books. The objective was to firstly identify which technologies are addressed by the different resources and secondly to which degree these technologies are addressed. Whenever a specific information security technology was addressed by a specific resource, it was taken into account. A tick mark shown in Figure 2 appears only when the specific technology is addressed comprehensively by a specific resource.

The information security technologies are listed in Table 1 and a brief description of each of these technologies is given in the sections that follow.

2.1 Proactive information security technologies

2.1.1 Cryptography

Cryptography, in simple terms, means 'hidden writing'. It is the science of protecting data confidentiality and integrity [16]. *Encryption* is the process of transforming or scrambling a cleartext message so that it becomes a ciphertext message. Synonyms for encryption are *encode* and *encipher*. The reverse process of

Table 1: The information security technologies.

2.1 Proactive information security technologies
2.1.1 Cryptography
2.1.2 Digital signatures
2.1.3 Digital certificates
2.1.4 Virtual private networks
2.1.5 Vulnerability scanners
2.1.6 Anti-virus scanners
2.1.7 Security protocols
2.1.8 Security hardware
2.1.9 Security SDKs
2.2 Reactive information security technologies
2.2.1 Firewalls
2.2.2 Access control
2.2.3 Passwords
2.2.4 Biometrics
2.2.5 Intrusion detection systems
2.2.6 Logging
2.2.7 Remote accessing

encryption is called *decryption*, which is the process of rearranging the ciphertext so that a ciphertext message is transformed into a cleartext message. Synonyms for decryption are *decode* and *decipher*.

Cryptography is a *proactive* information security technology because it safeguards data before a potential threat can materialise by encrypting the data. This is done to prevent an intruder from tapping a network wire and sniffing sensitive information from the network. Furthermore, cryptography is performed at various levels as indicated by the taxonomy:

- At application level: A specific application performs the encryption process before an intruder is able to intercept sensitive data.
- At network level: Hardware rather than software encryption can take place where hardware encryption modules can be placed at network level.

2.1.2 Digital signatures

A digital signature can be thought of as the equivalent of a handwritten signature with the same goal: associating a mark that is unique to an individual with a body of text [26]. In the same way as a handwritten signature, a digital signature must not be forgeable, in other words only the legitimate sender of a message should be able to create the digital signature [3]. Digital signatures are created using cryptographic algorithms.

A digital signature is a *proactive* information security technology because the digital signature is created before any dispute can arise that a specific sender of a message is not really the intended sender. Creating a digital signature thus indicates beforehand that a specific sender of a message is the sole creator of that message. Furthermore, a digital signature is performed at the following level as indicated by the taxonomy:

- At application level: The digital signature is created by a specific application before it is sent off to a specific receiver.

2.1.3 Digital certificates

Digital certificates attempt to solve the problem of *trust* on the Internet. Digital certificates are issued by *trusted third parties*, also referred to as *certificate authorities* (CAs) [25]. CAs are commercial enterprises that *vouch* for the identities of people or organisations on the Web [24]. A network of trust is thus established amongst Web users. In simple terms the concept of 'trust' or 'vouching for' can be stated as "someone I trust – the CA – trusts this other person, so I will trust him as well" [21].

A digital certificate is a *proactive* information security technology because the certificate is used to distribute the public key of a communicating party to another communicating party. In this way trust is also established before any communication between parties takes place. Furthermore, a digital certificate is performed at the following level as indicated by the taxonomy:

- At application level: A specific application, for example a Web browser, verifies that it can trust a specific party before communication commences.

2.1.4 Virtual private networks

Virtual private network (VPN) technology encrypts network traffic and therefore the

technology is closely related to cryptography. A VPN allows an organisation with multiple sites to connect these sites over a public network, i.e. the Internet, with the advantages that all data packets that travel between the sites are encrypted and secure [26]. In addition, the packets are restricted by the VPN technology to only travel between the organisation's sites. The difference in functionality between normal encryption and VPNs, however, is that the data is encrypted only when it is transmitted over a public network — the data that travels between the originating host and the VPN host is not encrypted. In addition, data will only be encrypted by the VPN if it originates from an authenticated host.

A VPN is a *proactive* information security technology because it safeguards data before it is transmitted over a public network by encrypting it so that only legitimate persons are able to read the information. Furthermore, VPNs work at the following level as indicated by the taxonomy:

- At network level: The encryption process is done between two VPN hosts sitting on the points-of-entry in a network before the encrypted data is sent over a network.

2.1.5 Vulnerability scanners

Vulnerability scanners (VSs) use signatures for the vulnerabilities they can identify. Therefore, a VS is an information security technology which is but a special case of intrusion detection [17]. Vulnerability scanning is also referred to as *interval-based* scanning, because hosts on a network are scanned at certain intervals and not continuously. When a VS has completed a scan and sampled the data into a report, it is referred to as a *snapshot*. Examples of VSs include CyberCop Scanner [27], Cisco Secure Scanner [28] (no longer on the market) and NetRecon [29].

A VS is a *proactive* information security technology because it attempts to identify vulnerabilities before the vulnerabilities can be exploited by intruders or malicious applications. Furthermore, VSs work at the following level as indicated by the taxonomy:

- At host level: A VS scans for vulnerabilities across an entire host in a bid to identify vulnerabilities in all the software applications and the hardware of the specific host.

2.1.6 Anti-virus scanners

Computer viruses have caused havoc on the Internet over the past decade. A computer virus is a piece of malicious software which has the ability to reproduce itself across the Internet, once activated [16]. Therefore, anti-virus scanners have been developed to counteract computer viruses.

Anti-virus scanners attempt to scan for viruses and functions before they can cause havoc, much in the same way as VSs in that they also 'know' what a specific virus's signature looks like. Anti-virus software is therefore also a *proactive* information security technology. Furthermore, anti-virus scanning is performed at various levels as indicated by the taxonomy:

- At application level: A specific application scans for known virus signatures in an effort to detect them before they can cause havoc. Viruses at application level tend to be 'static' viruses such as Trojan horses.
- At host level: Viruses that have the ability to reproduce themselves by using email applications, for example, can cause malicious activity almost anywhere on a host. Such viruses need to be scanned for across the entire host before they can start their malicious activity.

2.1.7 Security protocols

There are different protocols, for example Internet Protocol Security (IPSec) and Kerberos that can be classified as information security technologies. These protocols are technologies that use a standard procedure for regulating data

transmission between computers or applications to safeguard sensitive information before such information can be intercepted by intruders.

Security protocols are *proactive* information security technologies because they attempt to safeguard sensitive information using a specific security protocol before such information can be intercepted by intruders. Furthermore, security protocols work at the following level as indicated by the taxonomy:

- At application level: A security protocol, for example Kerberos, is a mutual authentication protocol which handles authentication at application level.
- At network level: A security protocol also relies on a network infrastructure to perform its security task, whether it is to encrypt data or simply to encapsulate a network packet in an effort to hide the packet's identity for security purposes.

2.1.8 Security hardware

Security hardware refers to physical hardware devices used to perform security tasks, for example hardware encryption modules or hardware routers.

Security hardware is a *proactive* information security technology because it safeguards data before a potential threat can materialise by, for example, encrypting data. This is done to prevent an intruder from changing or modifying the hardware device, since security hardware consists of physical devices that are tamper-proof. Furthermore, security hardware is implemented at various levels as indicated by the taxonomy:

- At host level: A hardware device can be attached to a specific host to perform its security function, for example a hardware key could be inserted into a specific port of a host to authenticate a specific user before the user is able to log on to the host.
- At network level: Hardware encryption modules can be placed on the network, which provides a tamper-proof solution and can be physically secured.

2.1.9 Security SDKs

Security software development kits (SDKs) are programming tools used to create security programs. The Java security manager and Microsoft .NET SDKs are examples of software that can be used to build security applications such as Web-based authentication programs.

Security SDKs are *proactive* information security technologies because they are used to develop various software security applications that safeguard data before a potential threat can materialise. Furthermore, security SDKs are used to develop security software at various levels as indicated by the taxonomy:

- At application level: A specific software application can be developed to safeguard data by encrypting data on disk, for example.
- At host level: A specific software application can be developed to authenticate a user or a process to a host.
- At network level: A specific software application can be developed to safeguard data by encrypting it before sending it over a network, for example.

2.2 Reactive information security technologies

2.2.1 Firewalls

An Internet firewall is a software tool installed on a specially configured computer that serves as a blockade, filter, or bottleneck between an organisation's internal or trusted network and the untrusted network or Internet [25]. The purpose of a firewall is to prevent unauthorised communications into or out of the organisation's internal network or host [19]. Firewalls are considered as the first line of defence in a bid to keep intruders out [10]. Personal firewalls are new to the security arena. Unlike traditional firewalls, personal firewalls

are installed on a normal workstation and attempt to only protect that specific workstation from the rest of the hosts on the network or the Internet.

Firewalls are *reactive* information security technologies because they are used to act against specific security incidents as soon as they occur. Furthermore, firewalls are implemented at various levels as indicated by the taxonomy:

- At host level: A personal firewall can be installed on a host that attempts to block or allow certain data flow to and from that specific host only.
- At network level: A network firewall can be installed on a host that is acting as the gateway to a private network. A network firewall attempts to block or allow certain data flow to and from all the hosts situated behind the network firewall.

2.2.2 Access control

The goal of access control is to ensure that a subject has sufficient rights to perform certain actions on a system [3]. A subject may be a user, a group of users, a service, or an application. Subjects have different levels of access to certain objects in a system. An object may be a file, a directory, a printer, or a process.

Access control is a *reactive* information security technology because it is used to allow or deny access to a system as soon as an access request is made. Furthermore, access control is implemented at various levels as indicated by the taxonomy:

- At application level: Access is allowed or denied to subjects on access requests to specific objects using access control lists in an application.
- At host level: Access is allowed or denied to a host when a user attempts to log on to the host.
- At network level: Access is allowed or denied to the network when a user attempts to log on to the network through a host or process.

2.2.3 Passwords

A password is a secret word, phrase, or sequence of characters that one must input to gain admittance or access to information such as a file, application, or computer system [4]. Passwords, however, should be considered as a technology on its own since the literature, as presented in Figure 2, does so.

Passwords are *reactive* information security technologies because they are used to allow or deny access to a system as soon as a person or a process wants to log on to an application, host, or network. Furthermore, passwords are implemented at various levels as indicated by the taxonomy:

- At application level: A person or process is allowed or denied access to a specific application, depending on whether the person or process provides the correct password.
- At host level: A person or process is allowed or denied access to a specific host, depending on whether the person or process provides the correct password.
- At network level: A person or process is allowed or denied access to a network, depending on whether the person or process provides the correct password.

2.2.4 Biometrics

Biometrics uses the geometry of a specific part of a human body to authenticate a person. There are many different implementations of biometrics, for example hand, fingerprint, retina and voice recognition biometrics.

Biometrics is a *reactive* information security technology because it is used to allow or deny access to a system as soon as a person wants to log on to an application, host, or network using

the geometry of a part of his/her human body. Furthermore, biometrics is implemented at various levels as indicated by the taxonomy:

- At application level: A person is allowed or denied access to a specific application, depending on whether the person provides his/her own biometric characteristic.
- At host level: A person is allowed or denied access to a specific host, depending on whether the person provides his/her own biometric characteristic.
- At network level: A person is allowed or denied access to a network, depending on whether the person provides his/her own biometric characteristic.

2.2.5 Intrusion detection systems

Intrusion detection is the process of monitoring the events that occur in a computer system or network and analysing them for signs of intrusions [17]. An *intrusion* is any set of actions that attempt to compromise the integrity, confidentiality, or availability of a resource. An *intrusion detection system* (IDS) is a software or hardware technology that automates this monitoring and analysis process [3]. Examples of IDSs are Snort [30], ISS RealSecure [31] and Cisco IDS [32].

IDSs are *reactive* information security technologies because they are used to monitor hosts on a network and to act on an intrusion as soon as it occurs. Furthermore, IDSs are implemented at various levels as indicated by the taxonomy:

- At host level: An IDS monitors a specific host to detect intrusions on that specific host. It runs on an individual host and continually reviews the host's audit log, looking for possible indications of an intrusion [14].

  At network level: An IDS node can be placed in a network which attempts to detect and react on intrusions caused by multiple hosts, for example a distributed denial-of-service attack.

2.2.6 Logging

Logging is an information security technology that attempts to gather information on certain events that take place. The goal of logging is to supply audit trails which can be traced after a security incident has taken place.

Logging is a *reactive* information security technology because it is used to trace security incidents after they have taken place. Furthermore, logging is implemented at various levels as indicated by the taxonomy:

- At application level: A specific software application monitors other software applications and records the events caused by those software applications.
- At host level: A specific software application monitors the processes that are run by the operating system and records the events caused by those processes.
- At network level: A specific hardware or software application can monitor network traffic as it moves past the network monitor at a specific point in a network.

2.2.7 Remote accessing

Remote accessing is an information security technology that allows people or processes to access remote services. Access, however, is not always controlled to remote services because it is possible to access a remote service anonymously. In this case, accessing remote services anonymously poses a threat. For example, some systems may be wrongly configured to allow anonymous connections by default, when anonymous connections should not actually be allowed according to an organisation's security policy.

Remote accessing is a *reactive* information security technology because it enables a person or process to connect to a remote service according to their access privileges.

Furthermore, remote accessing is implemented at the following level as indicated by the taxonomy:

- At host level: A specific host runs a service that enables a remote person or process to connect to it and allows access according to their specific access privileges.

3. Conclusion

The taxonomy for information security technologies discussed in this paper provides a state-of-the-art overview of the information security technologies. It is important for an organisation to know which information security technologies are available.

Furthermore, having such a taxonomy of information security technologies will also stimulate new research. For example, intrusion detection systems are not yet intelligent enough — a human still needs to interact too much in setting up and maintaining intrusion detection systems. In another example, vulnerability scanners take up too much resources and time to be effective enough since regular scans need to be conducted for such a technology to be effective.

New initiatives might also be researched, such as combining various information security technologies to form more intelligent information security technologies. For example, it might be possible in the near future to combine firewalls, intrusion detection systems and anti-virus scanner technologies to form a robust information security technology.

4. References

[1] Cronkhite, C. and McCullough, J., 2001. Access Denied. *Hackers*, McGraw-Hill/Osborne, 2001, p. 261.

[2] Maiwald, E. and Sieglein, W., 2002. Security Planning & Disaster Recovery. *Information Security Policy*, McGraw-Hill/Osborne, 2002, p. 61.

[3] King, C.M., Dalton, C.E. and Osmanoglu, T.E., 2001. Security Architecture – Design, Development & Operations. *Business and Application Drivers (Case Study)*, p. 1; *Authorisation and Access Control*, pp. 93-94; *Basic Intrusion Detection Terminology*, McGraw-Hill/Osborne, 2001, pp. 287-288.

[4] Lexico LLC, 2002. *Dictionary.com*; "technology"; "password", http://www.dictionary.com.

[5] INFOSEC 2002. Information Security & Prevention of Computer Related Crime. *What is Information Security?*, http://www.infosec.gov.hk/english/general/infosec/what_infosec.htm.

[6] Conway, S. and Sligar, C., 2002. Unlocking Knowledge Assets. *Building Taxonomies*, Microsoft Press, 2002, pp. 105-124.

[7] 2000–2002. *Computers & Security*; Elsevier Science; Vol. 19 – Vol. 21.

[8] 2000 – 2002. *Computer Fraud & Security*; Elsevier Science; Vol. 2000 – Vol. 2002.

[9] 2000 – 2002. *Network Security,* Elsevier Science; Vol. 2000 – Vol. 2002.

[10] Pabrai, U.O., Gurbani, V.K., 1996. Internet & TCP/IP Network Security – Securing Protocols and Applications. *Firewall Systems,* McGraw-Hill, 1996, pp. 163-181.

[11] Huth, M.R.A., 2001. *Secure Communicating Systems – Design, Analysis, and Implementation*; Cambridge University Press, 2001.

[12] Walker, K.M. and Cavanaugh, L.C., 1998. *Computer Security Policies and SunScreen Firewalls,* Prentice Hall, 1998.

[13] McLean, I., 2000. *Windows 2000 Security – Little Black Book*; The Coriolis Group.

[14] Cole, E., 2002. Hackers Beware – Defending Your Network from the Wiley Hacker. *Install Intrusion Detection Systems.* New Riders Publishing, 2002, pp. 238-239.

[15] Carroll, J.M., 1996. *Computer Security,* Third Edition, Butterworth-Heinemann, 1996.

[16] McClure, S., Scambray, J. and Kurtz, G., 2002. Hacking Exposed. *Cryptography*, Third Edition, McGraw-Hill/Osborne, 2002, p. 581.

[17] Bace, R.G., 2000. Intrusion Detection. *Defining Intrusion Detection*, pp. 3-4; "Vulnerability Analysis: A Special Case", ; Macmillan Technical Publishing, 2000, pp. 134-154.

[18] Northcutt, S., Novak, J. and McLachlan, D., 2001. *Network Intrusion Detection – An Analyst's Handbook*, Second Edition, New Riders Publishing, 2000.

[19] Oppliger, R., 1998. *Internet & Intranet Security*; "Access Control Mechanisms", p. 58; "Access Control", Artech House Incorporated, 1998, pp. 91-147.

[20] Schneier, B., 2000. *Secrets & Lies – Digital Security in a Networked World*; John Wiley & Sons Inc., 2000.

[21] Phleeger, C.P., 1997. *Security in Computing*; "Hash Algorithms", pp. 97-99; "Certificates", pp. 135-145; "Mandatory and Discretionary Access Control", p. 290; Prentice Hall; Second Edition, 1997.

[22] Gollmann, D., 1999. *Computer Security,* John Wiley & Sons, 1999.

[23] Tudor, J.K., 2000. *Information Security Architecture – An Integrated Approach to Security in the Organization*; Auerbach, 2000.

[24] Stein, L.D., 1998. Certifying Authorities and the Public Key Infrastructure. *Web Security – A Step-by-Step Reference Guide,* Addison Wesley, 1998, pp. 25-28.

[25] Tiwana, A., 1999. "Are Firewalls Enough?", pp. 112-135; "Securing Transactions with Digital Certificates", pp. 211-227. *Web Security*; Digital Press, 1999.

[26] Comer, D.E., 1999. Virtual Private Networks. *Computer Networks and Intranets*; Prentice Hall, 1999, p. 191.

[27] Network Associates 2002. CyberCop Monitor. *PGP Securities* http://www.pgp.com/products/cybercop-monitor/default.asp.

[28] Cisco Systems Inc., 2000. *Cisco Secure Scanner*; Version 2.0.1.2; http://www.cisco.com.

[29] Symantec 2002. *Products*; "Symantec NetRecon 3.5"; http://enterprisesecurity.symantec.com/products/products.

[30] SNORT.ORG; 2002; *Snort*; "Snort"; http://www.snort.org.

[31] Internet Security Systems 2002. *Internet Security Systems Incorporated*; "RealSecure Gigabit Network Sensor 7.0"; http://www.iss.net.

[32] Cisco Systems 2002. *Cisco Documentation*; "Cisco IDS (Formerly NetRanger) – Intrusion Detection System"; http://www.dictionary.com/search?q=technology.