A State of the Art Security Taxonomy of Internet Security: Threats and Countermeasures

Ali Abbas[1], Abdulmotaleb El Saddik[1,2], and Ali Miri[2]

[1]Multimedia communications Research Laboratory
[2]School of Information Technology and Engineering (SITE)
University of Ottawa
800 King Edward, P.O. Box 450, Stn A,
Ottawa, Ontario, Canada, K1N 6N5
Tel: (613) 562-5800 x 6277, Fax: (613) 562-5664
samiri@site.uottawa.ca
{abed, abbas}@mcrlab.uottawa.ca

Abstract. The main objectives of the different security services and mechanisms today are to provide privacy of information to ensure that the tools used to establish a proper environment to the user are reliable and trusted. With the dramatic increase of the use of the Internet and its applications that require high level of security services, such as e-commerce transactions and on-line banking, it is quiet useful to formulate a systematic approach to analyze the security services, and countermeasures which are directly associated with each security attack. Taxonomy is one of the keys to understand the security threats that the Internet is facing today and the countermeasure approaches that should be devised in order to keep the Internet as secure as possible. In this paper, we propose a novel Internet security taxonomy. This taxonomy is based on a mapping of today's Internet security services against the corresponding security attacks and countermeasures. An assessment of the performance of the proposed taxonomy is also discussed.

1 Introduction

Today, the Internet has become the fastest growing part of the global network. However, it is the network part that draws more attention to the security related issues because of its possible design flaws and vulnerability to attacks. A successful attack on a system on the Internet can pose a major threat because it can influence the system performance and the services used by millions of users. The Internet security flaws and vulnerabilities as well as the wide range of techniques used to implement and utilize different Internet applications emphasize the complexity of connecting all those related issues together and mapping them through classification categories to produce taxonomies. Internet security countermeasures which are going to provide the essential tools to develop security defenses and improve the overall security outcomes, require a deep understanding of the methods employed by security attacks.

This paper can be seen as an attempt to provide a state of the art, yet practical approach to formalize classification categories that map the security attacks to the security services associated with the attacks and well defined countermeasures. In Section 2, we provide an overview of some related work in security taxonomies. Section 3 describes our newly proposed internet security taxonomy. Section 4 discusses the performance assessments of the proposed taxonomy. Finally, we conclude the paper in Section 5 by giving some insight into future work.

2 Related Work

In this section, we discuss several research works that classify the vulnerability of the security systems allowing us to identify different type of taxonomies. It is worth mentioning that the simplest form of taxonomies can be seen as a single list of terms. Such a simple taxonomy only lists a long range of terms without classifying the attacks or the countermeasures. Existing work can be classified by the type of taxonomy used.

Among the empirical approaches to classify security attacks and counter measures is the work presented by Neumann and Parker [4]. They designed a list of categories called the "Empirical List Taxonomy". The categories of the empirical list taxonomy has some drawbacks, for example, the abuse through inaction category, in most cases, can not be considered as an attack since a careless administrator may cause a problem not only in security but also in most of the system's aspects and utilization. Furthermore, bad administration is not an attempt to gain unauthorized use or unauthorized access into the system, which means that this approach does not clearly distinguish between a security threat and any other type of malfunctions. Beside that the empirical list has an overlap between its classes, for example; masquerading may use a technique to defeat authentication or authorization service which may cause an overlap between two different categories.

Process-based taxonomies are the second type of possible classification. One of the main approaches in defining process-based security taxonomy is the one proposed by Stallings [10]. Stallings's approach concentrated on the security threats during the transmission of data over the Internet, which can be considered as only a subset of the Internet security. This taxonomy presents a very broad framework with an unspecific and very general classification that might be considered enough for assessing the rational of the attacks.

[1] present software security faults taxonomy that come from specification, design, and/or implementation can cause security flaws, but it is a software development issue and it has to be discussed and considered within those boundaries. More specifically, software development considerations have to fall outside the classification of the security threats, unless they are imposed on the system from the outside when attackers exploit the vulnerability embedded within the software. Our taxonomy presented in the next section, will consider these issues and differentiate between software bugs and malicious programs such as viruses, time bombs, etc.

Another central works in classifying the security attacks was done by Perry [13]. The idea behind their two-dimension matrix taxonomy is to widen the scope of the classi-

fication and to form a map that matches potential attackers to potential damages. Such a map is by nature not logical, because it may difficult to associate potential attacks to specific damages. In fact this is one of the limitations of this taxonomy, because creating such a map assumes a restriction of specific kind of damage to a specific kind of attackers and vice versa. For example, it is not logical to restrict the physical destruction only to the operator, or restrict the information destruction to the operators and programmers. Generally, Perry's matrix represents an improvement over the one dimension taxonomy approaches discussed earlier because it comprises two-dimensions with respect to security attacks and damages, but still, the cells of this matrix cannot cover the whole area of security attacks.

The three-dimension matrix taxonomy presented by Landwehr [2] specifies three phases in the system life cycle where security flaws may be introduced; the development phase, the maintenance phase, and the operation phase. The development phase includes all the systematic processes from the specification up to the deployment of the system. The maintenance phase includes all the activities that can provide a mean to adjust, modify and improve the performance of the system after the initial operation. Finally, the operation phase includes the adaptation and insertion of any kind of flaws during the operation time of the system. There is obviously an overlap between the maintenance and the operational phase, but still they are distinct enough to fulfill the requirements and serve the cause of the taxonomy, that is, to be specific and provide a method to countermeasure the flaws.

Howard [12] work divides the attack into six steps that attackers should follow in order to be successful. This taxonomy differentiates between the result of an attack and the objective of the attacker. In addition to that, Howard's taxonomy summarized the vulnerability in three components where the attacker can gain some advantages: design, implementation, and configuration. Classifying the vulnerability in this way may sometimes be not practical, especially if we consider different attacks techniques that are not concerned with the design, implementation and/or configuration, such as social engineering attacks.

In the next section, we will present our newly designed security taxonomy; this will include the new classification categories of the security attacks, the matrix that map the associated security services to the attacks, and the approach used to drive the third dimension or the countermeasures to the attacks in our matrix.

3 Proposed Internet Security Classification

Based on the above discussion of existing approach we feel the need for a taxonomy which follows a less general and more specific process of categorization of the classes of the security attacks. It is important to address software flaw as one possible category but we make a clear distinction between software flaws, bugs, and viruses, just to name a few. We, therefore, specify the functionality and performance of the security services with respect to the attacks and illustrate how the security countermeasures may improve the security services in any particular area. The proposed classification consists of a list of categories, which represent the actual and potential security attacks that may target the system. The objectives and the affected areas of

the Internet security attacks are also identified, and countermeasures are introduced. The elements of the proposed list of Internet attack's categories are:

- Manual Penetrating the System and/or Individual Privacy: This category includes all methods and techniques facilitating the manual penetrating to a system such as password cracking, social engineering, and masquerading.
- Data Interception, Interruption, and Replaying: This class contains among others interception of information and/or a sequence of communication process, tampering, modifying and message deleting of data while it is in transmission.
- Biometrics and Physical Token: It includes all attacks using physical or biometrical methods and processes such as forged fingerprint or replicating the biometrics signature.
- Defeating Mechanisms and Policy: The member of this class includes all the challenges related to the authentication, authorization, and access control mechanisms and policies;
- Malicious Code: This category comprises among others malicious software, viruses, malfeasant code, bugs, coding problem;
- Distributed Communication Systems: This class contains all different types of Distributed Denial of Service (DDoS), and other attacks using network communication protocol as means such as the TCP/IP.

4 New Matrix for a State of the Art Internet Security Taxonomy

Internet security comprises the operations that protect the information and the system that is processing the information by providing some basic security services like availability, integrity, authentication, confidentiality, and non-repudiation. These services may include the prevention mechanisms against any attacks or potential security attacks. Taxonomy for security services must provide a comprehensive review of the security services and attacks in such a way that system designers will benefit in anticipating their systems flaws and vulnerabilities.

Based on a given taxonomy, the d esigner can follow all the records under any specific classified group of attacks and services to analyze the weakness and vulnerabilities to become more knowledgeable, vigilant, and confident in building a better and more secure environment. More specifically, and in order to be used the Internet security service taxonomy has to be detailed, comprehensive, and practical. The work presented in this paper is an effort in producing a comprehensive taxonomy, which can address some of the flaws and shortcomings of the previous work in the literature.

As our taxonomy tries to map the existing security attacks to that of security services; we will use the list of security services proposed by [7] as one of the axes of our two-dimensional taxonomy. NSIT security services categories include: confidentiality; Data Integrity; Authentication; Authorization and Internet Access Control; Non-repudiation; and Availability.

To produce a taxonomy requires understanding of the security mechanisms, including both the services and the attacks, and on how all of their components work.

In addition to that, one needs an understanding of how the security components are interconnected and interrelated to each other. In other words, there is a need to decompose the security system into subsystems, and try to analyze their entities, attributes of those entities, the interrelationship among them and the performance of those subsystems. Security performance of a system comes as a result of the performance of its subsystems and components. Vulnerabilities in any of the security components might be exploited by the attacker to launch his unauthorized access or use of the system.

The first step toward developing our taxonomy was to build new classification categories for Internet security attacks, as presented in the previous section. In the following, we will introduce a new matrix taxonomy of security services which relates these services to the appropriate Internet security attacks. We will also analyze each security attack, assess its impact, and link it to one or more security possible countermeasures.

Table 1 shows two dimensions of our suggested new internet security services taxonomy. One of the dimensions represents the security services. The other dimension represents the above discussed classification categories of the security attacks. The elements in the cell represent the security attack and their appropriate security counter measure.

The first cell, in the first column of the matrix, that maps confidentiality to the Manual Penetrating the System and/or Individual Privacy class (MPSIP) of attacks comprise for instance Social Engineering as security attack and Privacy and Unpredictable Password as countermeasure. The C-DIIR cell comprises Eavesdrops as security attacks and Repeated Challenge Response as countermeasure. The C-BPT cell might have Biometrics Interception as security attack and Biometrics Data Encryption as countermeasure. The C-DAMP cell comprises Extract PIN as security attack and PIN Incorporated into Base Secret as a countermeasure. The C-MP cell comprises Back Door as an attack and Eliminate Back Door as countermeasure. And the last cell in this column, C-DCP, comprises Direct Communication as attack and Observing and Restrict Connection to the System as countermeasure.

The second column in the matrix presents a Data Integrity as security service in conjunction with the Nature of Attacks. The DI-MPSIP cell comprises Passwords File Theft as security attack and Hashed Passwords File as countermeasure. The DI-DIIR cell comprises Modifying Intercepted Message as an attack and Encryption System as countermeasure. The DI-BPT comprises Forged Biometrics as security attack and Encoded Passwords as countermeasure. The DI-DAMP cell comprises Attacking Encryption Procedures as security threat and Reliable Encryption procedure as countermeasure. The DI-MP cell comprises Trojan horse as security attack and Firewall as countermeasure. Finally the DI-DCP cell comprises Source Address Forgery as security attack and TCP Synchronization as countermeasure.

Table 1. Matrix of the Internet Security Framework. The table shows security services in the x-axis, class of the security attacks in the y-axis and possible security attacks with their corresponding security counter measure (SA/SCM) in the main cells of the table.

	Confidentiality	Data Integrity	Authentication	Authorization & Internet Access Control	Non-Repudiation	Availability
Manual Penetrating the System or the Individuals Privacy	Social Engineering/ Privacy and Unpredictable Password	Passwords File Theft/ Hashed Passwords File	On-line Password Guessing/ Audit Bad Passwords	Off-line Password Search/ Forced Lengthy Trails	Account Theft/ Enrolment in Person	OS Substitution/ BIOS Password
Data Interception, Interruption and Replaying	Eavesdrops/ Repeated Challenge Response	Modifying Intercepted Message/ Encryption System	Password Sniffing/ Encrypted Password	Reply Hashed Password/ One-time Password	Sniffing a Private Key/ Public Key on Smart Card	Unauthorized Delete of Data/ Limited Access
Biometrics and Physical Token	Biometrics Interception/ Biometrics Data Encryption	Forged Biometrics/ Encoded Passwords	Replicating the Biometrics Signature/ Authenticate Biometrics Signature/	Defeating matching mechanisms / Minimizing matching score.	Biometrics Sensor Disorientation/ Check and Maintain Biometrics Sensor	Steal the Biometrics Token/ Backup Emergency Processes
Defeating Authentication Mechanisms and Policies	Extract PIN/ PIN Incorporated into Base Secret	Attacking Encryption Procedures/ Suitable Encryption Procedures	Public Key Forgeries/ Public Key Certificate	Forge Authorization Privilege/ Encrypted Access Connection	Convert Reject into Accept/ Keyed Hash Incorporating	Synchronization Flood/ Connection Management

Malicious Program	Back Door/ Eliminate Back Door	Trojan Horse/ Firewall	Trojan Login/ Change Passwords	Mutual Trust/ Fire-walls and Enforce Access Control	Buffer Overrun/ Server Encap-sulation	Time Bomb/ Firewall and or Anti-virus
Distributed and Com-munication Protocols	Direct Communi-cation Attack/ Observing and Re-strict Con-nection to the System	Source Address Forgery/ TCP Syn-chroniza-tion	IP Address Theft/ GPS Location Authenti-cation	IP Spoof-ing/ Unpre-dictable TCP Se-quencing	IP Hi-jacking/ Integrity of the Host OS	Distrib-uted Denial of Ser-vice/ Observ-ing the System Perform-ance

The third column in matrix maps authentication to the classes of the security attacks. The AUT-MPSIP cell comprises On-line Password Guessing as security attack and Audit Bad Passwords as countermeasure. The AUT-DIIR cell covers for example Password sniffing as an attack and Encrypted Password as countermeasure. The AUT-BPT comprises Replicating the Biometrics Signature as security attack and Authenticate Biometrics Signature as countermeasure. The AUT-DAMP cell comprises Public Key Forgeries as security threat and Public Key Certificate as countermeasure. The AUT-MP cell comprises Trojan Login as security attack and Change Passwords as countermeasure. Finally the AUT-DCP cell comprises IP Address Theft as security attack and GPS Location Authentication as countermeasure.

The fourth column in matrix maps authorization and internet access control to the classes of the security attacks. The AIAC-MPSIP cell comprises Off-line Password Search as security attack and Forced Lengthy Trails as countermeasure. The AIAC-DIIR cell covers for example Reply Hashed Password as an attack and One-time Password as countermeasure. The AIAC-BPT comprises Defeating matching mechanisms as security attack and Minimizing matching score as countermeasure. The AIAC-DAMP cell comprises Forge Authorization Privilege as security threat and Encrypted Access Connection as countermeasure. The AIAC-MP cell comprises Mutual Trust as security attack and Enforce Access Control as countermeasure. Finally the AIAC-DCP cell comprises IP Spoofing as security attack and Unpredictable TCP Sequencing as countermeasure.

The fifth column in matrix maps Non-repudiation as a security service to the classes of the security attacks. The NR-MPSIP cell comprises Account Theft/ as security attack and Enrolment in Person as countermeasure. The NR-DIIR cell covers for example, sniffing a Private Key as an attack and Public Key on Smart Card as countermeasure. The NR-BPT comprises Biometrics Sensor Disorientation as security attack and Check and Maintain Biometrics Sensor as countermeasure. The NR-DAMP cell comprises Convert Reject into Accept as security threat and Keyed Hash Incorporating as countermeasure. The NR-MP cell comprises Buffer Overrun as secu-

rity attack and Server Encapsulation as countermeasure. Finally the NR-DCP cell comprises IP Hijacking as security attack and Integrity of the Host OS as countermeasure.

The sixth column in matrix maps availability as security service to the classes of the security attacks. The AV-MPSIP cell comprises OS Substitution as security attack and BIOS Password as countermeasure. The AV-DIIR cell covers for example Unauthorized Delete of Data as an attack and Limited Access as countermeasure. The AV-BPT comprises Steal the Biometrics Token as security attack and Backup Emergency Processes as countermeasure. The AV-DAMP cell comprises Synchronization Flood as security threat and Connection Management as countermeasure. The AV-MP cell comprises Time Bomb as security attack and Anti-virus as countermeasure. Finally the AV-DCP cell comprises Distributed Denial of Service as security attack and observing the System Performance as countermeasure.

5 Conclusion and Future Work

The proposed taxonomy identifies different countermeasures based on the objective of the attack. For example, if the attacker succeeds to exploit communication protocol vulnerabilities such as IP address theft, then he may tamper with availability, data integrity, or any other security service. At this level of attack, all the necessary prevention countermeasures must be taken in order to stop the attacker from achieving his possible goals. To protect confidentiality, the private files and information have to be encrypted, so the attacker will fail to have a plain text of what he/she is looking for. This protection process may guard any sensitive data or information against theft, but still, there is possibility that this information will be corrupted. Therefore, to protect the integrity, we need to continuously backup such information. This extent and link connection between the attacks and the countermeasures will give the researchers a powerful tool to conduct a focused and targeted kind of research. To illustrate this further, consider the example of the cell C-PSI, which depicts the case when the confidentiality as a security service is violated by penetrating the system or the individual's privacy class of attacks. The recommendation through this taxonomy to the user or system administrator is to use the properly established authentication methods to eliminate or to reduce the risk of this attack. Under such attacks, a system can be monitored very carefully to detect any presence or attempt to retrieve the original text from the system, or any other unauthorized files transmission or malicious software. Moreover, user commands can be logged, and the resulting log is used to identify any attack on the system, and then to investigate the system's performance during and after the attack.

Every cell in the matrix (table 1) has the potential to be expanded for further research and investigation, by being used to articulate an organized and detailed record of actual and potential threats with well-defined countermeasures. Every cell can be used to map the associated security attacks to the security services designed to combat that attack. Hence, given a general goal of identifying the attacks and their class of category, researchers can use the concept and approach of our taxonomy, and utilize it to build a stronger security system.

Definitely, the research on the Internet security systems has to be expanded and formulated in more systematic approach. Internet technologies are moving very fast; as a result, new attacks and countermeasures are continuously introduced. There is always a need to update or introduce new classification categories of the Internet security attacks. In addition to that, future work may include further validation and verification of the taxonomy that we presented in this research. Such verification may be achieved by analyzing the performance of the taxonomy using newly introduced attacks and countermeasures, for example, researchers may apply new attacks which are developed based on a new emerging internet technology to our classification and identity where do they fit within our taxonomy. Another optimization of our taxonomy can be using cost functions as another dimension of the taxonomy.

References

[1] T. Aslam, I. Krsul, and E. Spafford, "Use of A Taxonomy of Security Faults", Proceedings of the 19th National Information Security Conference, 1996.

[2] C. Landwehr, A. Bull, John P. McDermott, and W. Choi , "A Taxonomy of Computer Security Flaws," ACM Computing Surveys, Vol. 26, No. 3, September 1994, Page(s): 211-254.

[3] J. Howard, T. Longstaff, "A common language for computer security incidents", Sandia National Laboratories Albuquerque Report, Report No. SAND98-8667 , New Mexico, 1998.

[4] P. Neumann and D. Parker, "A Summary of Computer Misuse Techniques," Proceedings of the 12th National Computer Security Conference, 1989, Page(s): 396 – 407.

[5] C. Irvine, T. Levin, "Toward a Taxonomy and Costing Method for Security Services", Proceedings of Computer Security Applications Conference, 1999.

[6] C. Irvine, T. Levin, February 2001 "Quality of Security Services", ACM Proceedings of the 2000 workshop on New security paradigms, ISBN:1-58113-260-3, Page(s): 91-99.

[7] National Institute of Standards and Technology (NIST), "Underlying Technical Models for Information, Technology Security", Special Publication No. 800-33, December 2001. Also available at http://csrc.nist.gov/publications/nistpubs/800-33/sp800-33.pdf

[8] Open Source Security Testing Methodology Manual Pitfalls (OSSTMM), Version 2.5, August 2003, available at http://ideahamster.org/projects/osstmm.htm.

[9] Common Criteria (CC) project report , "Common Criteria for Information Technology Security Evaluation", August 1999, available at http://www.commoncriteria.org/.

[10] W. Stallings, Network and Internetwork Security Principles and Practice, Prentice Hall, Englewood Cliffs, NJ, 1995.

[11] L. Cranor, Internet privacy, February 1999, Communications of the ACM, Volume 42, Issue 2, Page(s) 28-38.

[12] John D. Howard, "An Analysis of Security Incidents on the Internet", Ph.D. Thesis, Carnegie Mellon University, Pittsburgh, USA, 1997. Also available at http://www.cert.org/research/JHThesis/Word6/

[13] T. Perry and P. Wallich, "Can Computer Crime Be Stopped?", IEEE Spectrum, Vol. 21, No. 5.

[14] James Essinger, "Internet Trust and Security", Addison-Wesley, Great Briton 2001, Page(s): 23-43.

Biography

▲ Name: Ali Abbas
Address: 770 King Edward, CBY, B203A, Ottawa, ON,
Education & Work experience: Ph.D. Candidate Biomedical Engineering, Ottawa University
Tel: +1-613-562-5800 ext 6291
E-mail: abbas@mcrlab.uottawa.ca
Other information: Ali Abbas is a senior computer engineer, worked for different company such as CAE Electronics, Montreal, Nortel Networks, Ottawa, Mitel Networks, Kanata. He gained M.Sc. degree in Systems Science from Ottawa University, and he is a Ph.D. Candidate in Biomedical Engineering, Ottawa University.

▲ Name: Abdulmotaleb El Saddik
Address: 800 King Edward, Ottawa, ON, Canada, K1N6N5
Education & Work experience: Associate Professor
Tel: +1-613-562 5800 ext. 6277
E-mail: abed@mcrlab.uottawa.ca
Other information: Dr. El Saddik is the director of the Multimedia Communications Research Laboratory (MCRLab). He has authored and co-authored two (2) books and more than 70 publications in the areas of software engineering development of multimedia artefacts and collaborative virtual environments. He is a Senior Member of IEEE and the recent winner of the prestigious Canadian "Premier's Research Excellence Awards" (PREA).

▲ Name: Ali Miri
Address: 800 King Edward, Ottawa, ON, Canada, K1N6N5
Education & Work experience: Associate Professor
Tel: +1-613-562 5800 ext. 6111
E-mail: samiri@site.uottawa.ca
Other information: Dr. Miri is an Associate Professor at the School of Information Technology and Engineering, University of Ottawa, Canada. His research interests include security and privacy technologies and their applications in e-business and e-commerce, such as network security and the role of Public Key Cryptography.