APPLYING THE EIGHT-STAGE RISK ASSESSMENT METHODOLOGY TO FIREWALLS

David L. Drake (david_drake@cpqm.saic.com)
Katherine L. Morse (katherine_morse@cpqm.saic.com)
Science Applications International Corporation
10770 Wateridge Circle
San Diego, CA 92121

ABSTRACT

The explosive growth of the Internet has brought thousands of companies exciting, new electronic contact with their customers. It has also brought them equally exciting contact with a cadre of ingenious and persistent hackers. Increasingly companies are turning to firewalls to thwart these wily hackers. While firewalls are very effective, often they are not the security panacea they are made out to be. This paper presents a risk assessment of a hypothetical firewall using the Security-Specific Eight-Stage Risk Assessment Methodology which illuminates where the security flaws lie. The example serves as guidance for assessing firewalls in general. We discuss the lessons we learned performing actual assessments which lead to recommendations for improving the security surrounding firewalls.

INTRODUCTION

In our 1994 paper [1] we identified three major flaws in existing security risk assessment methodologies. We presented our new security-specific eight-stage risk assessment which addresses these shortcomings. In this paper we show how the methodology may be applied to a firewall, a security mechanism of considerable current interest. We begin with a brief overview of the methodology. The overview is followed by a representative application of the methodology to a firewall that was drawn from our firewall evaluations. The results of the assessment lead us around to a recurring security risk and a proposal for improving firewalls to address this risk.

1. THE EIGHT-STAGE METHODOLOGY

This risk assessment of a generic, hypothetical firewall employs the Security-Specific Eight-Stage Risk Assessment Methodology [1]; henceforth referred to as the eight-stage methodology. The eight stages of the methodology are illustrated in Figure 1, The Eight-Stage Model.

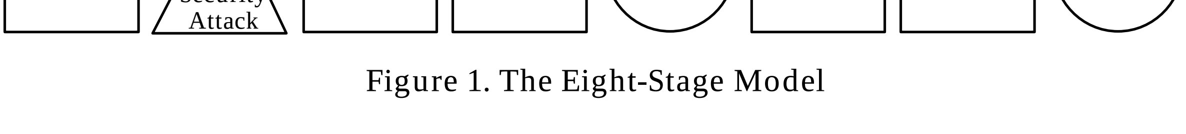

Figure 1. The Eight-Stage Model

In Figure 1, time flows from left to right. The internal influences are depicted as squares. The external influence (a security-related attack) to the system is depicted as a triangle. The consequences are depicted as circles. The objective of the security system is to prevent unwanted consequences of the security attack by employing the activities represented in the squares. The consequences, represented by circles, will occur if these activities are insufficient. One of the major principles of the model is that a system under attack has three opportunities to reduce the resultant harm: before the attack occurs, after the attack occurs but before a security breach occurs, and after a security breach occurs but before the resultant harm occurs.

When performing an assessment, we assess more than the firewall itself. We include both the automated security mechanisms of the firewall and the procedural requirements levied on the users and administrators. We refer to this without ambiguity as the "system". The eight-stage model is used to evaluate this system.

Performing an assessment using the eight-stage methodology involves two major steps:

- data gathering
- construction of eight-stage chains of security-relevant events and performing the quantitative analysis.

Both of these steps are described in the subsections below.

1.1 Gathering Data

The steps to gather the data for the assessment are:

1. Obtain the definition of the security boundary and the interfaces that will be defended by the firewall, both automatically and procedurally. The definition should be provided in the security policy.

2. Obtain the list of system assets to be protected, what constitutes a security breach, the associated harm that could befall the assets, and a quantitative loss per asset if it were compromised, modified by an unauthorized agent, or its availability were lost. This list should also be provided in the security policy.

3. Delineate the attack scenarios that will (and will not) be defended against, and the likelihood of occurrence of each. For firewall assessments, we have collected a long list of attack scenarios that cover most insider and outsider attacks.

4. Delineate each of the system's countermeasures that protect it against attack. A determination is made for each countermeasure if it is used to obstruct, detect or recover from an attack, or to detect or recover from a security breach. This distinction is used to support the quantitative assessment of each countermeasure's effectiveness.

1.2 Constructing the Chains and Performing the Analysis

The lists resulting from the data gathering phase are used to construct eight-stage event chains. One eight-stage chain is constructed for each attack scenario. In the appropriate stages, all applicable countermeasures, breaches, and are listed.

For each of the attack scenarios, the system's ability to defend against it is calculated based on the quantitative measures collected in section 1.1. There are eight data points that are collected during the data gathering phase for the eight-stage event chains: the effectiveness of the attack obstruction (CE_{AO}), the likelihood of an attack within one year (PR_A), the effectiveness of the attack detection (CE_{AD}), the effectiveness of the attack recovery (CE_{AR}), the loss in dollars if a security breach occurs (PL_B), the effectiveness of the breach detection (CE_{BD}), the effectiveness of the breach recovery (CE_{BR}), and the total value in dollars of the assets at risk in the attack scenario (PL_H). The likelihood of an attack is stated as the average number of attacks that will occur within a year. This is a departure from our 1994 paper [1] where we had assumed that the number of attacks would be less one per year. Anyone who reads the newspaper knows that this is no longer the case. All effectiveness measures are stated as probabilities ranging from 0.0 to 1.0. In our years of using this methodology, we found that the actual loss in dollars related to the security breach, PL_B, was always so low that it was not worth tracking. For example, if a hacker were breaking into a system, most security policies state that a security breach has occurred as soon as the hacker, as an unauthorized user, has somehow logged into the system. But at that point, no real dollar loss has occurred. There are exceptions, but to simplify the equations in this paper, we will assume that PL_B is always zero.

The likelihood that an attack will happen in one year and successfully result in a security breach (ER_B) is $\mathbf{PR_A \bullet (1 - (CE_{TO} + ((1 - CE_{TO}) \bullet CE_{AD} \bullet CE_{AR})))}$. The likelihood that an attack will happen and successfully result in a harm (ER_H) is $\mathbf{ER_B \bullet (1 - (CE_{BD} \bullet CE_{BR}))}$. The potential dollar loss per year (EL_T) for the one attack scenario being analyzed is $\mathbf{PL_H \bullet ER_T}$.

It is important to keep in mind that the effectiveness measure for the attack obstruction (CE_{AO}) is the combined effectiveness of all of the mechanisms being used for attack obstruction against the one attack scenario being analyzed. Additional analysis may need to be performed to determine how all of these attack obstruction mechanisms interplay. The same is true for the analysis of the effectiveness for all detection and recovery mechanisms. In cases where mechanisms have different reactions based on situations, it may be necessary to decompose the analysis into more specific attack scenarios, resulting in more eight-stage event chains to analyze. See our earlier work [1] for the underlying formulation of all calculations.

2. APPLYING THE METHODOLOGY TO AN EXAMPLE FIREWALL

The example firewall that we will use is an amalgamation of the actual systems that we have assessed. The asset values, likelihoods, and effectiveness measures used in the example are drawn from these assessments. Our example firewall is a bastion host using IP-based filtering with an external router connected to the Internet. It is used to protect company proprietary data, including financial and Privacy Act data, on a collection of LANs supporting various computing platforms. We constructed this example system because of its commonality to current firewall installations. Our example allows only the following data flows:

- e-mail in both directions
- both internal and external hosts are allowed to "ping" the firewall (for connectivity testing)
- both in-coming and out-going Domain Name Service (DNS) requests
- non-anonymous File Transfer Protocol (ftp)
- World Wide Web.

In the following subsections we proceed through an abbreviated assessment, following the steps described in subsections 1.1 and 1.2. Given the space constraints, the tables provide examples and are not exhaustive.

2.1 Gathering Data

Table 1, Security Policy, synopsizes the example firewall's security policy. While the security policy should be provided by the system owner, in all of our assessments that was not the case and developing the security policy was our first task. The table is divided into three sections: the security boundary, the automated defenses of the firewall, and procedural defenses which are the responsibility of the users and administrators.

An abbreviated list of the assets to be protected are given in Table 2, Protected Assets. Listed with each asset are the types of breaches associated with its loss, the type of the resulting harm, and the value of the resulting harm. Table 3, Attack Scenarios, lists some of the attack scenarios that will and will not be defended against by the firewall, and the likelihood of occurrence of each. The attack scenarios that will not be defended against are addressed so that a true level of vulnerability can be assessed. Impossible attack scenarios for this example, such as those using `telnet`, are excluded since the firewall completely precludes their being enacted.

Table 1. Security Policy

Security Boundary
All internal network nodes and the firewall itself
Automated Defenses
Users on the outside network and users on the inside network are prohibited from all interaction with the firewall with the exception of e-mail, ping / echo, DNS, and an extremely limited ftp capability.
E-mail is allowed to pass between the internal network and the Internet.
Users on the external network are allowed to ping the firewall.
DNS is allowed for both in-coming and out-going requests and replies.
Outbound requests for file transfers using ftp from the internal network to the Internet are permitted.
Inbound requests for file transfers using ftp from the Internet to a designated ftp site within the internal network are permitted.
Outbound requests from the internal network for WWW access to the Internet are permitted, with Java disabled.
Internal network addresses are hidden from the external network.
Procedural Defenses
Users are not allowed to modify the e-mail program.
Users are not allowed to e-mail proprietary and / or private data over the Internet.
Users are not allowed to automatically forward e-mail to the Internet.
Administrators of the firewall must securely administer the system.
Users must be wary of all data received over the Internet, independent of its source.
Users and administrators must take great care in selecting programs which support web browsers.
Proprietary or private data must never be placed in the outgoing ftp directory.

Table 2. Protected Assets

Asset	Breach*	Harm‡	Value
Firewall CPU time	A	R, T	$100 / hr.
Firewall system files	I	M	$1,000 / file
Firewall disk space	A	R	$300 / Mb
Web site on firewall	I, A	R, T	$400
Firewall password file	C, I	M	$1,000
Ftp file site	A	R, T	$2,000
Firewall e-mail service	A	R, T	$500
CPU time on non-firewall systems	A	R	$500
Privacy Act Data	C, I, A	M, P	$10,000
E-mail messages	C, I	M	$5000
Financial records	C, I, A	M, D	$50,000

*C = loss of confidentiality, I = loss of integrity, A = loss of availability

‡M = failure of mission, P = loss of personnel, R = loss of resources, D = loss of dollars, T = loss of time

Table 3. Attack Scenarios

Attack Scenario	Defended Against	Likelihood
Hacker floods firewall network ports	No	.01
Hacker peruses e-mail traffic	Via procedures	.01
Hacker forges e-mail return address	No	5.00
Hacker attempts to use the `sendmail` security holes	Yes	2.00
Hacker spoofs Internet's DNS	Yes	.01
Hacker attack on FTP	Yes	6.00
Viruses received via the WWW infect internal programs	Via procedures	3.00
User inadvertently violates security policy	Via procedures	100.00
System administrator inadvertently misconfigures firewall	Via procedures	3.00

Table 4, System Countermeasures, lists several of the countermeasures that the system provides and their types.

Table 4. System Countermeasures

System Countermeasure	Type
Packet blocking	Obstruction
Packet filtering	Obstruction
Services written with secure features	Obstruction
Security education	Obstruction
Audit log analysis	Attack & Breach Detection
Automated alarms	Attack & Breach Detection
User detection of file modification	Breach Detection
User detection of mail spoofing	Attack Detection
Statistics utility results analysis	Attack & Breach Detection
User detection of system malfunction	Breach Detection
Firewall reconfiguration	Attack & Breach Detection
Firewall shutdown	Attack & Breach Detection
Firewall reinitialization	Attack & Breach Detection
Turning off firewall services	Attack & Breach Detection

2.2 Constructing the Chains and Performing the Analysis

Since space does not permit reproducing the results of all attack scenarios, we have selected two representative samples. A typical assessment would have approximately 80 chains. The first example, Table 5, Automated Attack Scenario, illustrates an attack against which the firewall is designed to protect. The second, Table 6, Human Error Scenario, illustrates the type of human error against which the firewall cannot protect itself.

The scenarios are presented in tables, each containing an eight-stage model of the attack being enacted. The tables should be read as a time-line, progressing from stage 1 through stage 8. The stages are listed in the first column, and the instance in the second column. The third column provides the quantitative measures associated with the instance as described in section 1.2. The important results are the total effective risk, ER_T, and the loss that is associated with it, EL_T. Table 5 is the analysis of a hacker attacking a firewall protocol that is allowed, `sendmail`'s SMTP protocol, but is secured by the use of the latest version of `sendmail`. It's obstruction effectiveness is very high, but it's not guaranteed to be impenetrable. This is reflected in the bottom line by the low level of risk and effective loss.

Table 5. Automated Attack Scenario: `sendmail` attack

Stage	Instance	Effectiveness, likelihood, or potential loss level
1. Attack obstruction	Service written with secure feature: firewall's use of secure version of `sendmail`.	Effectiveness (CE_{AO}): .99
2. Attack scenario	**Hacker attempts to use the `sendmail` security holes to gain access to firewall.**	**Likelihood (PR_A): 2.0**
3. Attack detection	Audit log analysis; automated alarms	Effectiveness (CE_{AD}): .9
4. Attack recovery	Turning off firewall services; firewall shutdown	Effectiveness (CE_{AR}): .9
5. Security breach	**Hacker gains access to firewall CPU time, system files, and disk space**	**Effective risk (ER_B): .004**
6. Breach detection	Audit log analysis; automated alarms; statistics utility results analysis	Effectiveness (CE_{AD}): .9
7. Breach recovery	Turning off firewall services; firewall shutdown	Effectiveness (CE_{BR}): .9
8. Harm	**Loss of resources, time, and money.**	**Potential loss (PL_H): $9,100** **Total effective risk (ER_T): .001** **Total effective loss (EL_T): $6.57**

Table 6 addresses a very different type of scenario: human error on the part of the firewall administrator. Despite the best of intentions on the administrator's part, he or she will make approximately three misconfigurations per year that the firewall will not prevent, of which a hacker could take advantage. Note that the total effective risk is 45 times higher than in the previous scenario, and the total effective loss per year is 27 times higher.

The two examples were chosen for their illustrative capabilities. Summing the Total Effective Loss values for all eight-stage event chains results in the average dollar amount lost per year due to the attack scenarios analyzed. After approximately 80 tables, each addressing an attack scenario, it becomes clear where weaknesses exist, and where additional security measures are needed.

Table 6. Human Error Scenario: Administration of ftp Access Controls

Stage	Instance	Effectiveness, likelihood, or potential loss level
1. Attack obstruction	Security education: system administrators are educated in the importance of the security policy and the procedures to adhere to it.	Effectiveness (CE_{AO}): .9
2. Attack scenario	**System administrator inadvertently misconfigures ftp access controls.**	**Likelihood (PR_{A}): 3.00**
3. Attack detection	User detection: system administrator realizes mistake, or co-worker notices misconfiguration.	Effectiveness (CE_{AD}): .4
4. Attack recovery	Firewall reconfiguration: system administrator corrects ftp access controls.	Effectiveness (CE_{AR}): .999
5. Security breach	**Internet hacker discovers flaw, deletes files in ftp site.**	**Effective risk (ER_{B}): .18**
6. Breach detection	Audit log analysis; user detection of file modification	Effectiveness (CE_{AD}): .75
7. Breach recovery	Firewall reconfiguration: system administrator resets access controls and restores ftp files.	Effectiveness (CE_{BR}): .999
8. Harm	**Loss of ftp site resources and time to restore.**	**Potential loss (PL_{H}): $4,000** **Total effective risk (ER_{T}): .045** **Total effective loss (EL_{T}): $181**

3. LESSONS LEARNED

> *"Firewalls are the wrong approach. They don't solve the general problem, and they make it very difficult or impossible to do many things. On the other hand, if I were in charge of a corporate network, I'd never consider hooking into the Internet without one. And if I were looking for a likely financially successful security product to invest in, I'd pick firewalls."*
>
> \- Charlie Kaufman [6]

We couldn't agree more. Even when the firewall is supplemented with procedural defenses which rely on the users and administrators, the effective risk is still non-zero. At the end of each of our assessments, our customers all learned this lesson. The following are the additional lessons we learned.

3.1 A False Sense of Security

Firewalls give people the feeling that their systems on the internal network are secure, which leads to a sense of complacency. People feel they can "relax." Instead, the firewall has allowed access between the internal and external networks that users would normally feel a little less comfortable about. Ironically, internal network users should be even more concerned. The comfort provided by the firewall will tend to increase the flow of message traffic. The result is that all of the standard security precautions, e.g. running virus checkers on files that have been brought across the network, and being leery of e-mail that has been received from unknown sources, must be done with more consistency. The primary function of a firewall is to provide a buffer from external attack. Until firewall-to-firewall authentication mechanisms are in place, we still suffer the consequences of inside users having access to sensitive information and the ability to send that information externally. The opportunity for error is high and there's no way to prevent that from happening other than through training and awareness classes. Gasser highlighted this issue in 1988 [11] by stating "Fads in the computer security area can have a serious negative effect on the overall progress to achieving good security because progress stops when people think they have the answer." Firewalls are inherently a crutch. By giving us a sense of protection from the external network, they allow us to put off addressing long-standing security issues with the systems on the internal network, such as lack of comprehensive access control enforced at the enterprise level or sensitivity checks on outgoing information.

RSA Data Security, Inc. is negotiating with leading firewall and TCP/IP stack vendors to create a security standard that could eliminate a major barrier to building virtual private networks (VPNs) on the Internet [12]. Even with this in place, it means you are still extending your trust to network and assuming it is trustworthy. For example, if a hacker has penetrated the other firewall’s internal network, e.g. through a modem, and is communicating out through the other firewall, this new level of trust actually poses a threat to all systems which communicate with the firewall.

3.2 The Relationship between the Security Policy and the Firewall

Assessing this example firewall highlights the requirement that a security policy must be in place before the methodology can be applied. This requirement gives rise to two problems. The first is that many organizations, particularly commercial businesses suddenly coming to grips with the risks of being attached to the Internet for the first time, are in imminent danger. The immediacy of their need for security overrides the rational requirement for a well-reasoned, comprehensive policy. It's not even clear that many of the responsible policy-makers would know how to state their policy requirements. The second problem comes in translating between the security policy and the firewall implementation. Since the policy maker and the firewall administrator are usually different individuals, they may be unclear on the precise impact of their own decisions on each other's domains. In addition, administering a firewall requires making frequent, small changes to the configuration, effectively changing the firewall's security policy dynamically. Fortunately, a firewall, unlike many other security mechanisms, is well encapsulated. This leads us to an interesting proposal to firewall makers.

5. FUTURE DIRECTIONS

We recommend automating configuration of the firewall in conjunction with specification of the security policy. We envision a tool which presents the policy maker with potential policy statements. Statement selection would produce two outputs: 1) a human-readable description of the firewall security policy for the policy maker and the end users; 2) the associated configuration for the firewall. The tool should also provide conflict resolution. Either selection of conflicting policy statements should be automatically prevented or they should flagged as errors for the policy maker to resolve manually. In addition, direct changes to the configuration by the system administrator would be prohibited. Changes would be made through the same tool which would notify the administrator if an attempted change would violate the prescribed security policy.

Notice that we have come full circle to the fact that the biggest risk to a secure environment is still people. The proposed tool removes some of the potential for human error in the administration of a firewall.

REFERENCES

[1] "The Security-Specific Eight Stage Risk Assessment Methodology," David L. Drake and Katherine L. Morse, *Proceedings of the 17th National Computer Security Conference*, 1994. Updated and republished *in Datapro Reports on Computer Security*, McGraw-Hill, 1995.

[2] DoD 5200.28-STD, *Department of Defense Trusted Computer System Evaluation Criteria*, December 1985.

[3] FIPS PUB 31, *Guidelines for Automatic Data Processing Physical Security and Risk Management*, U.S. Department of Commerce, National Bureau of Standards, June 1974.

[4] FIPS PUB 65, *Guidelines for Automatic Data Processing Risk Analysis*, U.S. Department of Commerce, National Bureau of Standards, 1 August 1979.

[5] *Firewalls and Internet Security*, William R. Cheswick and Steven M. Bellovin, Addison-Wesley, 1994.

[6] *Network Security: Private Communication in a Public World*, Charlie Kaufman, Radia Perlman, and Mike Speciner, Prentice Hall PTR, 1995.

[7] *Computer Communications Security: Principles, Protocols and Techniques*, Warwick Ford, Prentice Hall PTR, 1994.

[8] "Addressing Threats in World Wide Web Technology," Kraig Meyer, Stuart Schaeffer, Dixie Baker, IEEE Symposium on Computer Security, 1995.

[9] "Security and the World Wide Web," David I. Dalva, Data Security Letter, Trusted Information Systems, June 1994. Available on the WWW:
`http://www.tis.com/Home/NetworkSecurity/WWW/Article.html`

[10] *E-Mail Security: How to Keep Your Electronic Messages Private*, Bruce Schneier, John Wiley & Sons, Inc., 1995.

[11] *Building a Secure Computer System*, Morrie Gasser, Van Nostrand Reinhold, 1988, pg. 12.

[12] "Group Seeks Firewall Security Standard," Nick Wingfield, *InfoWorld*, Vol. 17, Issue 41, October 9, 1995.