Case Study: Firewall

- This section discusses an example of applying an eight-stage risk assessment methodology to firewalls
- The reason for selecting this case study is to stimulate a discussion about the granularity of solutions
- Source
  - http://csrc.nist.gov/nissc/1996/papers/NISSC96/paper012/nissc96.pdf
  - APPLYING THE EIGHT-STAGE RISK ASSESSMENT METHODOLOGY TO FIREWALLS
  - David L. Drake, et.al.
  - Figures and quoted material are directly adopted from the paper.

Risk Assessment: Firewall

- Eight-Stage Methodology

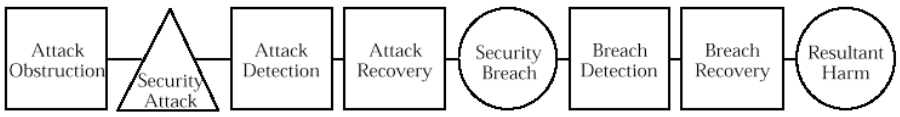

Figure 1. The Eight-Stage Model

  - squares: internal influences
  - triangle: external influence
  - circle: consequences
    - will occur if activities are insufficient

Risk Assessment: Firewall

- Data gathering:
  - "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".
  - "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".

Risk Assessment: Firewall

- Data gathering:
  - "Delineate
    - the attack scenarios that will (and will not) be defended against,
    - the likelihood of occurrence of each."
  - "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."

Risk Assessment: Firewall

- Example firewall uses amalgamation of actual system
  - firewall is a host using IP-based filtering
  - external router connected to the Internet
  - LAN supports various computer platforms
  - critical application data
    - company proprietary data
    - financial and privacy act data

Risk Assessment: Firewall

- Data flow
  - “email 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”.

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.

Risk Assessment: Firewall

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

Risk Assessment: Firewall

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

Risk Assessment: Firewall

Table 4, System Countermeasures, lists several of the countermeasures that the 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

Risk Assessment: Firewall

- Chains and Analysis
  - they demonstrate 2 chains
  - assume 80 chains for typical assessment
    - why 80 +- ?
  - 1st chain: firewall & sendmail attack
  - 2nd chain: "human error" scenario
    - can not be handled by firewall

Risk Assessment: Firewall

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**

Risk Assessment: Firewall

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**

Risk Assessment: Firewall

- False Sense of Security
  - firewalls make people happy
    - even if they don't know what it can do
    - excuse for getting lazy w.r.t. enforcing security
  - still many problems, open doors
  - even though outside users might not be able to get in, inside users still have access to all resources
- About this paper
  - seems interesting approach but unimplementable
  - seems to suffer from all problems associated with prob. risk assessment
  - scalability questionable

Risk Assessment: Firewall

- Nice quote
  - *"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