INTERNATIONAL JOURNAL OF NETWORK MANAGEMENT
Int. J. Network Mgmt. **9**, 305–308 (1999)

Risk Management

By Judith Myerson[*]

In the first article in the series on risk management we briefly discuss frame relay network versus leased lines, network management life cycle and a risk management program. We show how coordinated denial-of-service, a new type of threat, can attack a network. Copyright © 1999 John Wiley & Sons, Ltd.

What would you do if you suddenly had 5 million users to add to your network? You start with a blueprint for a high-speed, distributed network to connect, say, five locations (see Figure 1). The blueprint shows that network linking together a frame relay network and an internet Gigabit Ethernet network to transport data, voice and video to some locations and only data to others.

Frame Relay Network Versus Leased Lines

Why frame relay network over leased lines? The availability of a frame relay network is much higher than that of leased lines, as these lines are subject to more frequent failures and outages which can extend to hours and even days. The longer the circuit distance between two or more locations, the greater the probability of an outage, given a fiber cut or other types of disruptive affecting that circuit. In contrast, frame relay minimizes or eliminates the WAN point-to-point bottleneck. Most vendors provide the feature of automatic rerouting of Permanent Virtual Connections (PVCs) around circuit failures. Another advantage of the frame relay service is that it is capable of placing multiple protocols, such as TCP/IP, SNA, NETBIOS and IPX over a network-transport protocol.

Network Management Life Cycle

From the blueprint, you choose a network management life cycle that best suits the needs and objectives of your organization. You start, for instance, with design tools[†] to optimize network topology and analyze potential and actual failures. You then proceed to use configuration management tools to store records of rack layout, cabling design and equipment location. Using the information that event-management tools generate in real time, you repeat the life cycle processes until the network topology is optimized with theoretically no or little chances of failures. The number of times you can reiterate depends on market conditions or government missions and the size of the return of reinvestments (ROIs) you can quantify.

In reality, the network of open systems is exposed to real-world risks, due to the way it is structured, especially in a global setting. You may lose your gains or savings if they are used to recoup

[†]According to Spohn[1] network management consists of three components: design management, configuration management and event management, leaving out much of risk management processes. The term *design tool* is used to describe a wide of applications that are concerned with topics such as optimization of network topology and failure analysis. The term *configuration management tool* is used to describe a wide of applications that address topics such as storing records of rack layout, cabling design, and equipment location. The term *event-management tool* is used to describe applications that are used for real time network event notification.

Judith M. Myerson was in the official capacity as the ADP Security Officer/Manager for the US Department of Navy for several years.

[*]*Correspondence to: Judith Myerson, P.O. Box 7677, Philadelphia, PA 19101-7677, USA.*

 CCC 1055–7148/99/050305–04$17.50

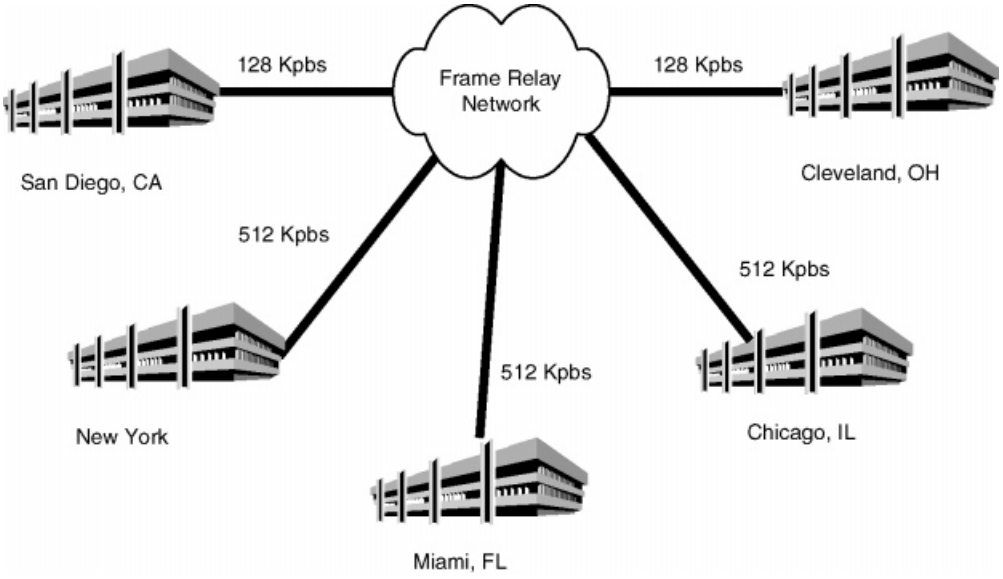

Figure 1. High-speed network scenario

losses from massive denial-of-service, widespread destruction, unauthorized modification of the systems, and unauthorized disclosure of classified data. The tools you may have used to design and deploy the network are inadequate in protecting you from losing money, savings and reputation.

The design tool, for instance, limits risk analysis to fault analysis which is used to describe the effects on demand traffic of a failure of some portion of the transport network. There are many other aspects of risk analysis, such as fault controls and safeguards. Configuration management tools restricts tangible assets to records on hardware and software configurations, excluding intangible assets (company policy, Equal Employment Opportunity program), and other types of tangible assets (personnel, software upgrades). The event-management tool is used to notify users and system administrators of real-time events—warnings, alerts and impending failures of the network. It does not address how vulnerable the network is to other types of threats.

Risk Management Program

To reduce the risks of the actual threats against the network, your organization needs a good risk management program as number one priority in network management. Although Myerson's book[2] targets risk management processes toward software engineering models, it can be applied toward network models. Myerson divides risk management into the following key components: (1) assets, (2) threats, vulnerabilities and risks, (3) safeguards, (4) economic analysis and (5) reiterative processes.

Here, we give definitions for the first two components from network perspectives. An *asset* is defined as any resource needed to plan, design, build, deploy and operate the networks. It includes tangible (software, hardware, personnel) and intangible assets (plans, organization, external factors, technical factors). A *threat* is defined any possible harm to the system, including network failures and natural disasters. A *vulnerability*, according to Russell,[3] is a point where the computer [network] system is susceptible to attack. A *risk* is the probability that a particular security threat will exploit a particular system vulnerability.

Which is the best approach? First identify the assets and then the threats? Start with the threats and then the assets? It depends on what the security policy is, and how complex and vulnerable the network system is. You may start with identifying the assets most likely to be adversely impacted by the threats that will occur in future events and then identify those threats. On the other hand, you may

be more comfortable with starting with a list of threats and then identify the assets most likely to be affected by these threats.

You can name threats as you wish, as long as you include a new type of threat in your risk assessment: coordinated denial-of-service attacks. Gone are the days of individual denial-of-service attacks. Enter the hackers who '. . . bombard target machines from thousands of different IP addresses with a very small amount of malicious packets intermixed with benign packets,' according to the navy.[4] This means a group of hackers with a single or multiple accounts coordinate to launch the attack simultaneously (see Figure 2). The today's intrusion detection tools are not sufficient to detect them, as the packets move too quickly for these tools.

To get some degree of protection from this threat, make sure you do not have routers *outside* of network firewalls, as these routers contain internal network topology information. Place the routers *inside* the firewalls. This *safeguard* partially counters the weaknesses of the vulnerabilities in the system, thus reducing the risk to a somewhat lower level.

Whatever the approach you use, it can take several vulnerabilities to launch a threat attack against the system if the risk is high. As shown in a Threat Data Sheet Example (see Figure 3), disgruntled employees can take advantage of at least four vulnerabilities to damage a frame relay network, thus stopping the system.

Economic Value Analysis

After identifying assets and threats, the next step is to perform *economic analysis*, which is concerned with relative values (rather than absolute numbers) of asset loss impacts on network projects. According to Myerson, the analysis focuses on three main areas. *Mathematical values* are used to compute the costs and other quantifiable values of implementing additional safeguards. They include impact ratings of the assets, risk prioritization rules and probability algorithms. *Savings justifications* are used to justify the costs of implementing the safeguards. The savings, for instance, are determined by comparing the expected values for each asset in the original risk analysis and the revised ones. It is

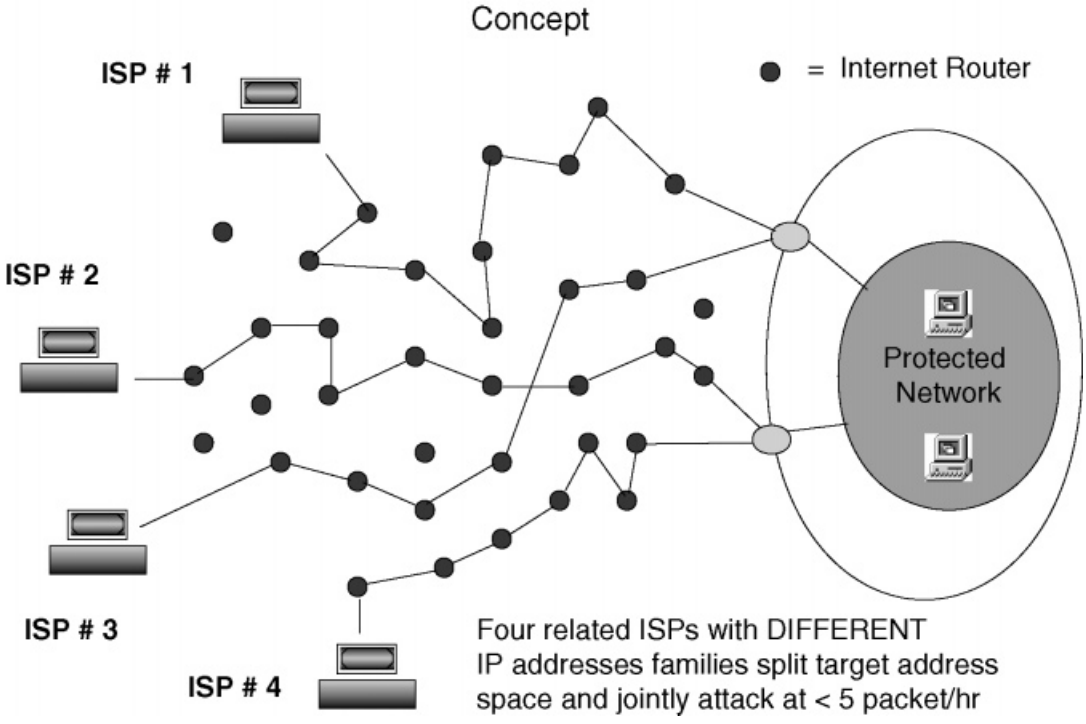

Figure 2. Synchronized reset network mapping

Threat Data Sheet

Type	Disgruntled employees
Scope	Employees who received layoff notification and who have unsatisfactory relationship with their supervisors
Average frequency	Four or six times a year
Historical Damage	Former employees returned to intentionally damage frame relay network, thus stopping the system

Vulnerabilities

1. Procedures for debriefing soon-to-be-terminated are do not exist
2. Terminated employees' access to physical facilities are not revoked
3. Background checks on employees are not adequate
4. Safeguards for protecting disgruntled employees from damaging the network are outdated
5. Training programs for supervisors on handling difficult employees are ineffective

Figure 3. Threat Data Sheet Example (after Myerson)

easier to measure *ROIs* with costs than benefits, as not all benefits can be quantified.

Reiterative Processes

Reiterative processes are used to manage new risk factors and change risk prioritization in a project and to improve continuously the quality of risk management processes. According to Myerson, conditions for continuing reiterative processes can change over a period of time or with a new set of security policies. If the impacts of changing conditions are complex, automation of reiterative processes is recommended, as it can be tedious to perform by hand. As stated before, the number of times you can reiterate depends on market conditions or government missions and the size of the return of reinvestments (ROIs) you can quantify.

Conclusion

A good risk management program is important, as fault analysis does not guarantee that the system will never be damaged, compromised or stopped. We are faced with a new type of threat: coordinated denial-of-service. As technologies evolve in response to highly competitive market conditions, new types of threats not yet addressed or known will emerge. Detailed discussions on these threats and the risk management program will be covered in future articles.

We are faced with a new type of threat: coordinated denial-of-service.

References

1. Spohn DL. *Data Network Design* (2nd edn), McGraw-Hill, New York, 1998.
2. Myerson M. *Risk Management Processes for Software Engineering Models*, Artech House Publishers, Boston, MA, 1997.
3. Russell D, Gengemi GT. *Computer Security Books*, O'Reilly & Associates, Sebastopol, CA, 1991.
4. Swoyer S. Navy warns of new hacking technique, *ent* 7 October 1998; **3**(16). ■

