Global Information Assurance Certification Paper

Brett Harder
Survivability and Survivability Network Analysis (SNA)
January 23, 2002
GSEC Practical 1.2f 2nd submission

Unbound networks such as the Internet have seen a surge of crippling attacks. Examples of these attacks are the denial of service (D OS) attacks which affected large companies such as Yahoo, Amazon, eBay, CNN.com and the Melissa virus which affected thousands of networks world -wide. In a recent study, Peter Neumann [6] of SRI notes that companies and governments that have addressed incidents such as DOS attacks, web hacking, false emails, corporate espionage, corporate/customer compromise, and viruses are budgeting for prevention of these occurrences through traditional information system security products such as firewalls and encrypt ion technologies. This paper discusses methods organizations can use to reduce the damaging effect of an attack by focusing on the mission specific details of the IT infrastructure. The next sections will provide a short background on security and surviv ability and will explore the leading technique to developing survivability into the infrastructure.

Comment: The DDOS attacks / Mafia boy 2000 would be more recent & pertinent to Exodus (e.g. Yahoo, Buy.com)

Security

Security implies protection against undesirable events. The three most commonly identified properties relating to security are confidentiality, integrity, and availability.

> **Confidentiality:** Confidentiality involves protection against undesired release of information by the releaser, and protection against undesired acquisition of information by the acquirer. Confidentiality is meaningful with respect to data, but also with respect to the system itself, for example, maintaining the confidentiality of software or of the hardware implementation.
>
> **Integrity:** Integrity implies remaining in a sound, unimpaired, or otherwise desirable condition. Int egrity may have somewhat different meanings for a system, a subsystem, an application, data, hardware, communications links, and other entities.
>
> **Availability:** Availability implies that certain required resources are available when and as needed. Availa bility can be applied at many levels of abstraction, including systems, subsystems, data entities, and communications links.

Current security approaches to protect information systems focus on preventing attacks from being successful by hardening defens es with authentication, encryption, and network devices such as firewalls, network address translators, intrusion detection systems. Despite the best efforts of security practioners,

networks are still vulnerable to attack. No amount of system hardening and traditional security measures can assure 100% that a system connected to an unbound network will be invulnerable to attack [4]. Traditional security and vulnerability analysis are no longer sufficient. The traditional ways need to be supplemented with the concept of survivability.

Survivability

Survivability is defined as the ability of a system to fulfill its mission in a timely manner. ARPAnet is the precursor to the Internet and was designed as a survivable network for military purposes. Survivability was key to its design and success. It is from the ARPAnet project that the modern Internet evolved. The Internet is a fully functional survivable system by design; however, the so-called last-mile and client IT infrastructures have lacked the methodology and design for achieving a similar rate of survivability as the Internet. The next sections will examine survivability of corporate or organizational assets and will encompass the last-mile infrastructure.

Survivability stems from the growing dependence on complex, large-scale, networked systems that will be targets for hackers, misuse, and failures. In the presence of attacks, failures, or accidents, even when systems are penetrated and compromised, survivability becomes a necessity [5]. The large-scale systems depending on confidentiality, integrity, and availability (CIA) may be bookstores, music stores, power grids, payment systems, or banking systems. The need for survivability is a common requirement for effective business practices for these businesses. Potential threats include failures (usually generated internally) due to software design errors, hardware degradation, human errors, or corrupted data, hardware malfunctions, software flaws, environmental hazards, malicious and accidental (generally are externally generated events) human acts. These threats disable or distract the system from its mission. The terms attack, failure, and accident include all potentially damaging events.

For a system to survive, it must react to a damaging effect possibly before the underlying cause is identified. The distinction between a failure and an accident is less important than the actual event. It is the mission fulfillment that must survive, not any particular subsystem or system component even if significant portions of the system are damaged or destroyed [3]. Figure 1.1 defines CERTs three key system capabilities required for survival.

*Resistance - The capability to repel attacks. For example: use of firewall controls, and system hardening.
*Recognition - The capability to recognize attacks and to evaluate the extent of damage and compromise. For example: log analysis, and intrusion detection system.
*Recovery - The capability to provide essential services during attack, limit the extent of damage, and restore full services following attack. For example: designating a policy, procedure, and team to keep or recovery essential services to an adequate level.

Figure 1.1 Survivability key concepts

Survivability may be better explained with an example such a flooding attack in which the ability to provide the service is impaired. In some cases, flooding the server or network will exhaust memory, become inoperative and will not fulfill its purpose. Survivability, in this example, would focus on building in measures to allow required information to flow through the system without being denied due to the flood of SYN packets or other traffic (ICMP, etc) trying to create a denial-of-service situation. The throughput or ability to use the system may not be fully functional, but the essential services will remain working; thus, achieving survivability. If the above situation was a regional medical center and it was under a flooding attack, the flooding may reduce the medical center's ability to use email or/and use of the Internet, etc. If the concept of survivability was built into the system both the regional and parent hospital will be able to access essential information whether it be medical information, health insurance information, and other necessary administrative medical booking data such as patient allergies, to medication, patient history, and payment information. The survivability solution would include a combination of network and application development processes with the system mission being thought and built into the environment.

There have been considerable efforts in telecommunications to develop a measurable concept of survivability. Many of the telecommunications concepts are suitable to networks and information system infrastructure [5]. If we go back a few decades in business we can follow a pattern in communication. In the 1920's and 1930's business communication was primary done through the postal service.

The postal service is unreliable and does not guarantee that the message is received and no assurance of survivability is built into the system. Post can be stolen, falsified, denied, and lost. The postal solution addressed this issue with courier mail. Courier mail, although more expensive, had measures built in to assure the message was delivered such as signatures, receipts, insurance, hand

delivery, or speedy delivery. Courier mail reduced the chances of missed delivery and allowed essential mail to be delivered.

Businesses benefited with a high assura nce that business communications were delivered through more efficient mail routing and transportation such as plane, train, and bus. Signatures, and verification minimized the chance of the mail being "hijacked". This high assurance is the concept of su rvivability built in to the system.

The telecommunications since the 1940's has built in survivability through various methods such as better multiplexing technologies, underground wires, redundant nationwide backbones lines, better phones, higher capaci ty and more secure switches, lower electrical draw, better security measures and services, etc. Telecommunications has a longer history in networked communications than networked computer systems. An example of the similarity between communications and n etworked communication systems is how telecommunication companies, service providers, corporations, and others rely on bandwidth available from fiber optics. The dependence on these lines makes disruptions (from hackers, or other) and failures (equipment) from link and node critical. With the advent of fiber optics and its increasing deployment in networks, the risk of losing large volumes of data due to a span or node failure or incident has increased dramatically due to a single cable carrying massive v olumes of data.

Many businesses are dependent on a usable system. Companies such as Amazon, Ebay, Yahoo, Etrade, and others are working a non -traditional business model in the so -called new economy. CIA security concepts are critical to their success, which is additionally based on trust, service, efficiency, and survivability. One of the techniques used to measure, qualify and mitigate survivability is the Survivability Network Analysis (SNA) developed by Carnegie Mellon University. SNA is used to accomplish the following: [1]

- Analyze mission risks and tradeoffs of implementing controls
- Identify decision points with survivability impact assessment
- Provide recommendations with business justification
- Improve survivability to ensure mission c apability

Survivable Network Analysis Process

The Survivable Network Analysis method was developed by the SEI CERT Coordination Center of Carnegie Mellon University. SNA is a practical engineering process that permits systematic assessment of the surviv ability properties of proposed systems, existing systems, and modifications to existing systems. The SNA method provides a means for organizations to understand survivability in the context of their operating environments. SNA reveals the risks and leads to strategies for increasing the likelihood a survivable system.

From initial requirements to deployed systems, SNA can be tailored to any stage of development. Steps in the SNA method include system mission and architecture definition, essential capab ility definition, compromisable capability definition, and survivability analysis of architectural areas that are both essential and compromisable. SNA results are summarized in a survivability map which links recommended survivability strategies for resi stance, recognition, and recovery to the system architecture and requirements. The process is adaptable to variety of development processes and applies to infrastructure and applications [1]. SNA objectives include identification of the following:

- Survivability risks to a system or infrastructure
- Essential services must survive intrusions or incidents
- Effects of intrusions or incidents on the mission
- Mitigating strategies
- Processes, requirements, or architecture changes can improve survivability
- Changes that have the highest payoff
- Identify trade offs with software quality attributes safety, reliability, performance, and usability

SNA Methodology

Step 1: System Mission and Architecture Definition: In step 1, mission objectives and requirements for a current or proposed system are reviewed, and the structure and properties of its architecture are elicited. Step one requires input from stakeholders, owners, users, architects, developers, and administrators and identification of explicit and implicit a ssumptions such as choice of vendors, operating systems and critical dependencies on other systems.

The following is a small sample of what type of information SNA discovered for the fictional company ABCD.com. In step 1, system mission and architecture are defined. The site ABCD.com's primary function is to act as a payment brokering system for several on -line shopping websites. The mission objective is to provide flawless brokering of transactions between on -line shopping and credit card companies. A BCD.com's architecture requires extranet connectivity, certificate authentication (x.509), firewall protection (Unix based) on the front -end connectivity to the Internet and back -end firewall controls to credit companies and customers. The environment is completely Unix based.

A great analogy for SNA is an example with a military aircraft bomber. In step 1, an Air Force bomber has a mission to strategically release payload to destroy a target and to keep the pilot and crew safe. The architecture require s a large bomb bay door, ability to fly with significant damage, and redundant control systems. All systems need to be contracted through authorized vendors.

Step 2: Essential Capability Definition: In step 2, essential services (services that must be maintained during attack) and essential assets (assets whose integrity, confidentiality, availability, and other properties must be maintained during attack) are identified, based on mission objectives and consequences of failure. Function and usage scen arios characterize essential services and asset uses. These scenarios are mapped onto the architecture.

ABCD.com would be required to provide services to keep extranet customers such as the credit card companies and online stores connected at all times s o transactions can occur. Assets required for the transactions are the back -end firewall, database systems for record lookup, and application servers. Front -end systems are less essential being they are not involved in the actual transaction.

In the bom ber plane analogy, the essential capability for the bomber is to fly, navigate, and release bombs. In most cases the most essential service is to return from a mission. If the plane is under attack and hit by enemy fire and going down, it must be able to keep the pilot safe via ejection seat or other system.

Step 3: Compromisable Capability Definition: Compromisable capability is defined as the intruder capabilities based on system environment and assessment of risk. This information is used to develop intrusion scenarios. These scenarios are mapped onto the architecture as to identify corresponding components that could be penetrated and damaged by intrusion. The result is a set of representative intrusions based on the system's operating environment . Steps 1- 3 provide information to develop recommendations for architecture modifications, requirements changes, policy revisions, and operational improvements. The goal is to identify survivability strategies for backup, configuration management, and th e three "R's" (resistance, recognition, recovery) by getting input from users, management, and system administrators.

ABCD.com is vulnerable to many types of Internet based attacks such as denial of service attacks, viruses, network intrusions, and social engineering. Critical machines are the machines involved in the brokering. For example, an FTP site with client software updates is not at the same level of priority for recovery. Survivable tragedies for ABCD.com are to resist attack by hardening the servers, limit access and control Internet connectivity through a firewall. Protect all outfacing IP addresses as well as limiting internal rights in order to deter intrusion. ABCD.com needs to recognize attacks by examining network metrics, comparing me trics with established baselines, implementing intrusion detection systems, actively look into logs generated from servers, and network devices.

In the bomber example, identification of scenarios dealing with failure/recovery of components such as a rudde r, landing gear, bomb drop, etc. The plane must resist attack (stealth, speed, maneuverability). The bomber pilot must be

knowledgeable of possible problems that may occur, recognize attack via radar, be aware of ground communication and visual scope, an d be able to recover from attack by activating or using redundant systems.

Step 4: Survivability Analysis of architectural areas that are both essential and compromisable: Step 4 defines recommended mitigation strategies for resistance, recognition, an d recovery, assess architecture modifications and impacts, document findings in the survivability map and prepares the customer briefing [1].

ABCD.com's mitigation strategies may consist of the following items. Resistance: Guidelines established to check and install patches and on -going system hardening. The site will need redundant key systems in the environment. In addition, resistance to attack with multiple separate ingress / egress points. Recognition: Intrusion detection boxes will be set up at a ll ingress and egress point on the ABCD.com infrastructure. These will act as the primary recognition device. Log checking and system monitoring will enhance the effort. The recovery process will focus on bringing services back on line via adding a technical control device such as SYN defender to thwart the attack and recover bandwidth. SYN defender works by intercepting all SYN packets and mediating the connection attempts before they reach the operating system. By mediating the connection attempts, th e target host is protected from becoming flooded by the unresolved connection attempts that would cause the operating system, and the host, to stop receiving new connections. Patching the servers, router with the latest release could assist in the recover y, especially in cases where a virus is involved.

In the bomber example, the bomber would mitigate resistance by flying higher, flying at night, using tactics that draw less attention, and use features on aircraft that hide presence. Implementation of re cognition would be rear -facing cameras on the plane so the pilot can see behind or using an outside spotter for trouble. Another example is having infrared sensors to detect enemy fire. Recovery mitigation, in a worse case scenario, would be an ejection seat and recovering the pilot and crew from the sea/ground.

The success of the SNA method depends on the effectiveness of the recommendations. For each life -cycle activity, survivability goals should be addressed and methods to improve survivability shou ld be incorporated. In some cases, existing development methods can enhance survivability . The following chart (figure 1.2) diagrams activities related to life cycle development [2].

Life-Cycle Activities	Key Survivability Elements	Examples
Mission Definition	Analysis of mission criticality and consequences of failure	Estimation of cost impact of denial-of service attack
Concept of operations	Definition of system capabilities in adverse environments	Enumeration of critical mission functions that must withstand attacks
Project planning	Integration of survivability into life-cycle activities	Identification of defensive coding techniques for implementation
Requirements definition	Definition of survivability requirements from mission perspective	Definition of access requirements for critical system assets during attacks
System specification	Specification of essential service and intrusion scenarios	Definition of steps that compose critical system transactions
System architecture	Integration of survivability into architecture definition	Creation of network facilities for data replication of critical data assets
System design	Development and verification of strategies	Correctness verification of data encryption algorithms
System implementation	Application of survivability coding and implementation techniques	Definition of methods to avoid buffer overflow vulnerabilities
System testing	Treatment of intruders as users in testing and certification	Addition of intrusion usage to usage models for statistical testing
System evolution	Improvement of survivability to prevent degradation over time	Redefinition of architecture in response to changing threat environments

Figure 1.2 Survivability and life -cycle activities

SNA Benefits

The SNA process ra ises awareness of mission survivability. SNA helps avoid unpleasant surprises and reduces exposures in organization systems. The process is effective to manage survivability risks up front rather than to manage damage control later. It provides a manage ment roadmap for addressing exposures before the fact rather than consequences after the fact. SNA provides clear requirements, metrics to evaluate changes in architecture, e arly problem identification, increased stakeholder communication, and i mproved sy stem survivability.

Conclusion

Survivability requires solid knowledge of the networked infrastructure and the mission of the infrastructure must be known to develop effective survivability maps. Survivability maps need to be flexible and constantly cha nge as company or project goals change.

Critical survivability in systems and networks are extremely difficult to specify, develop, procure, operate, and maintain. They are subject to threats, laden with risks, and difficult to use effectively. Unlike traditional security measures, which often depend on central control and administration, survivability is intended to address network environments where such capabilities may not exist [4]. There is no absolute survivability; an attack or other event may compromise any system, however well defended. However survivability maps developed through SNA will allow greater prevention tactics and quicker resolution to problems as they occur due to scenarios and forethoughts of security issues and the possible out comes. SNA will become a major consideration in large networked environments, as business models are moving out of the smaller .COM configurations. Large networks supplementing established corporations are becoming mainstream thus establishing the need a nd urgency of survivability.

A major factor the SNA methodology fails to note is the major costs involved in developing a survivable system. Efforts to meet SLA's of 99999% uptime and the cost to achieve this level of service is enormous. Obviously for certain companies such as Ebay their livelihood depends on the site functioning the costs associated with survivability are justified. The increased development costs, opportunity cost in longer development cycles, and equipment costs may not be a justifi ed business expense for many in the intended SNA audience. The SNA process may be best utilized in areas where large risk of financial loss and loss in human life.

References

[1] Carnegie Mellon University. " The Survivable Netw ork Analysis Method: Assessing Survivability of Critical Systems" 2000 (January 7, 2002) <http://www.cert.org/archive/pdf/sna -tutorial.pdf>

[2] Ellison, Robert. Linger, Richard. Lipson, Ho ward. Mead, Nancy. McHugh, John.
"Life-Cycle Models for Survivable Systems" IEEE. 2000. (January 7, 2000) http://www.cert.org/archive/pdf/lifecycle -models.pdf

[3] Fisher, David. Elli son, Robert. Linger, Richard. Lipson, Howard. Longstaff, Thomas. Mead, Nancy. "Survivable Network Systems: An Emerging Discipline" 1997, revised 1999. (January 7, 2002) <http://www.sei.cmu.edu/publications/documents/97.reports/97tr013/97tr013chap01.html>

[4] Linger, Richard, Ellison, Robert. Longstaff, Thomas. Mead, Nancy. "The Survivability Imperative: Protecting Critical Systems" (January 7, 2002) <http://www.stsc.hill.af.mil/crosstalk/2000/oct/linger.asp>

[5] Moitra, Soumyo. Konda, Suresh " A Simulation Model for Managing Survivability of Networked Information Systems" *December 2000* (January 7, 2002) http://www.cert.org/research/00tr020.pdf

[6] Neumann, Peter. "Practical Architectures for Survivable Systems and Networks" SRI International 2000 (January 7, 2002) <http://www.csl.sri.com/users/neumann/survivability.html >