Survivable Functional Units: Balancing an Enterprise's Mission and Technology

Lawrence R. Rogers

May 2004

CERT® Training and Education Center

Technical Note
CMU/SEI-2004-TN-004

This work is sponsored by the National Guard Bureau (NGB).

The Software Engineering Institute is a federally funded research and development center sponsored by the U.S. Department of Defense.

This work was created in the performance of Federal Government Contract Number F19628-00-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The Government of the United States has a royalty-free government-purpose license to use, duplicate, or disclose the work, in whole or in part and in any manner, and to have or permit others to do so, for government purposes pursuant to the copyright license under the clause at 252.227-7013.

For information about purchasing paper copies of SEI reports, please visit the publications portion of our Web site (http://www.sei.cmu.edu/publications/pubweb.html).

Contents

List of Figures

Abstract

Enterprises strive for success in fulfilling their mission to their customers. Information and its management are key components of their ability to succeed. Computer systems and network infrastructure components–the technologies that process this information–are playing an increasingly larger role in support of an enterprise's ability to fulfill its customers' needs. Their role has grown to a point where the slightest disruption–break-ins or even attempted break-ins–can adversely affect the enterprise's ability to manage information and therefore deliver products and services to its customers.

Although system administrators often need to focus on the details of computer systems and network infrastructure components to keep them operating smoothly, they must also be able to see the role that these technologies play in support of the enterprise's mission. This technical note describes Survivable Functional Units, a way to think about these enterprise networks. Although Survivable Functional Units have always been a part of networks, they now have a name and a more rigorous definition, and they can be linked to the mission of the enterprise in a more straightforward manner. The intended audience for this technical note is system administrators and their immediate managers, though the concepts have wider applicability.

1 Introduction

Enterprises strive for success in fulfilling their mission to their customers. Information and its management are key components of their ability to succeed. Computer systems and network infrastructure components–the technologies that process information–are playing an increasingly larger role in support of an enterprise's ability to fulfill its customers' needs. Their role has grown to a point where the slightest disruption–break-ins or even just attempted break-ins–can adversely affect the enterprise's ability to manage information and therefore deliver products and services to its customers. While system administrators often need to focus on the details of those computer systems and network infrastructure components to keep them operating smoothly, they must also be able to see the role that these technologies play in support of the enterprise's mission.

The concept of Survivable Functional Units is a way for system administrators to see more clearly the roles of the technologies they manage. The goal of Survivable Functional Units is to group computer systems and network infrastructure components based on the functions provided by their constituent elements and then think, talk, and manage the enterprise network at this group level. By operating with these abstract groupings rather than the elements that make up the groups, system administrators can more easily focus on how the mission of the enterprise is achieved through these groupings without becoming unnecessarily bogged down or overwhelmed by specifics of the constituent elements. Through this Survivable Functional Unit abstraction, the system administrator reduces the complexity of the enterprise's network so that he or she can more easily see its landscape, interrelationships and dependencies between the groups, and their contribution to the enterprise's mission.

It's a challenge for system administrators to group their computer systems and network infrastructure components into Survivable Functional Units and then view them at the group level, given the pressures of time and the demands of technology. While short-term, technology-centered achievements are satisfying, they may not support the enterprise's mission. Indeed, they may even be in opposition to that mission. System administrators need to balance the demands of technology with the enterprise's need to satisfy its critical mission objectives.

How does thinking about the enterprise network as a collection of interrelated Survivable Functional Units benefit the system administrator? Said another way, why should they bother to change their way of thinking about how they view the computer systems and network infrastructure components that they manage?

When these constituent elements are grouped together based upon the functions they provide, system administrators can more easily see how these groups serve the mission of the enterprise, which in turn helps them to focus on prioritizing their day-to-day activities. Mission-critical tasks can then receive needed attention sooner rather than later.

It is also easier for the system administrator to communicate these priorities and their constituent needs and requirements beyond the Information Technology (IT) organization because these attributes are more in tune with enterprise's mission. By communicating these needs and requirements, the system administrator and the IT organization are more likely to improve their case for investments in IT and information security-based products and services.

In short, when system administrators change their approach to one that is more clearly and obviously aimed at supporting the mission of the enterprise, their efforts are likely to succeed. The enterprise does better and system administrators do better as a result.

Successful system administrators can no longer embrace technology for technology's sake. Instead, they must now focus on the role that that technology plays in achieving the enterprise mission as embodied in goals and objectives. Technology no longer defines the business of the enterprise; rather it enables the business of the enterprise. System administrators must change their thinking about the task of system administration so that they increase their value to the business.

This technical note describes a way to think about these enterprise networks. It is intended to be an aid to system administrators so that they can more easily see the bigger picture of how technology supports the enterprise's mission and therefore enhance their value to the enterprise. The cornerstone of this thought process is the aforementioned notion of a Survivable Functional Unit. The discussion begins with the concept of a Functional Unit and then extends that by adding the concept of survivability.

2 What Is a Functional Unit?

A typical enterprise (business, government agency, university, or even a home network) has a collection of computer systems and network infrastructure components that are intended to help the enterprise achieve its mission. In most cases, these computer systems are connected by a network infrastructure made up of routers, firewalls, hubs, switches, wires, wireless access points, modems, and network interface cards (NICs). The way that an enterprise's computer systems are connected and the selection of network infrastructure components vary from enterprise to enterprise, sometimes widely.

In an arbitrary enterprise's network, it should be possible to group the computer systems and network infrastructure components into higher level, function-oriented entities. We'll call these entities *Functional Units*. A Functional Unit is defined as a collection of computer systems and network infrastructure components which, when abstracted, can be more easily and obviously linked to the goals and objectives of the enterprise, ultimately supporting the success of the enterprise's mission. From a technological perspective, a Functional Unit is an entity that consists of computer systems and network infrastructure components that deliver critical information assets,[1] through network-based services, to constituencies that are authenticated to that Functional Unit.

For example, imagine an organization that provides Web services to the Internet.[2] That organization's network probably has computer systems and network infrastructure components that can be grouped together and named the Web Development and Delivery Functional Unit (WDDFU). That Functional Unit could consist of at least the following constituent elements:

- one or more computer systems that provide access to a defined set of the enterprise's critical information assets through standard Web network-based services to the Internet constituency. This is the delivery part of the WDDFU.
- the networking infrastructure components that connect the delivery computer systems to a network, traditionally called the DMZ[3] (demilitarized zone)

[1] Critical information assets are electronic data that are especially important to achieving the enterprise mission (e.g., a product catalog).

[2] This is a simplified example that does not include an e-commerce component, which is prevalent on today's Internet.

[3] DMZ is short for demilitarized zone, a computer or small sub-network that sits between a trusted internal network, such as an enterprise private network, and an untrusted external network, such as the public Internet.

- one or more computer systems used to create the content delivered by the delivery computer systems. This is the development part of the WDDFU.
- the networking infrastructure components that connect the development computer systems to the enterprise's internal network
- the networking infrastructure components (routers, firewalls, etc.) that separate the delivery part from the development part. That is, they connect the DMZ to the enterprise's internal network.
- the networking infrastructure components that separate the delivery part from the Internet constituency. This is usually the Internet firewall or router.

By grouping these components, the system administrator can now think of them as the Web Development and Delivery Functional Unit as shown in Figure 1.

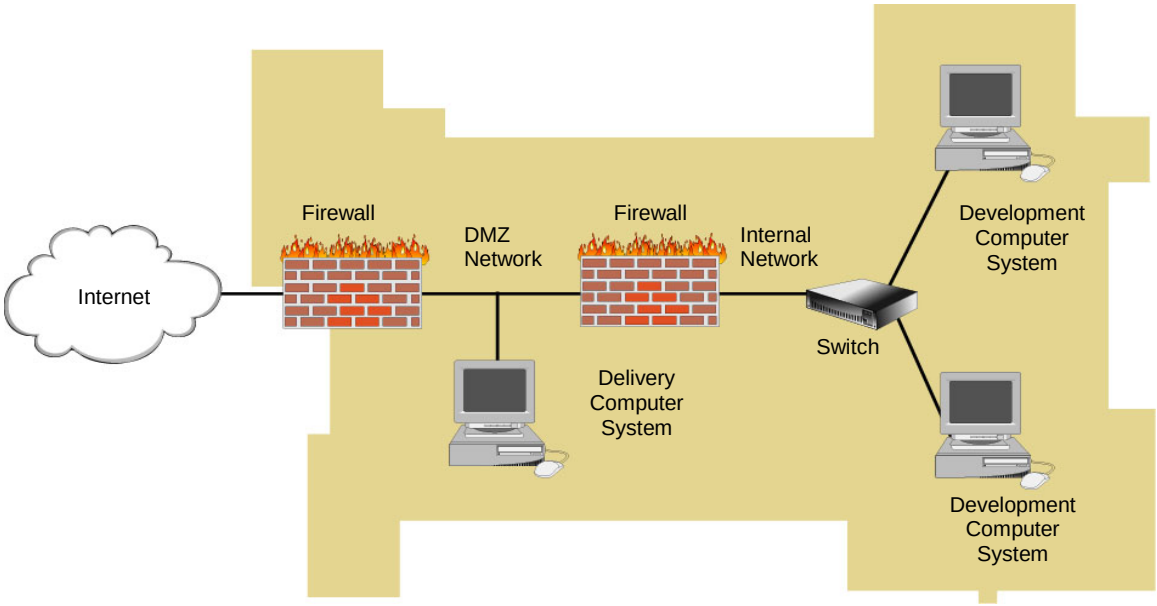

Figure 1: Web Development and Delivery Functional Unit

This Functional Unit can be thought of as a single entity that provides access to a well-defined set of the enterprise's critical information assets through Web-based services when serving the Internet constituency, and it provides access to another well-defined set of the enterprise's critical information assets through both Web- and administrative-based services when servicing the enterprise constituency. Instead of looking at the enterprise's network and seeing perhaps hundreds of computer systems and network infrastructure components, system administrators can see higher level, function-oriented building blocks that work together to achieve the enterprise's mission. Their interrelationships, relative importance, and roles in achieving the enterprise's mission help system administrators see where to concentrate their efforts when faced with competing tasks that demand their attention.

2.1 Functional Unit Authentication

One of the key attributes of every Functional Unit is that it authenticates its constituencies before providing service to them. In the example of the Web Development and Delivery Functional Unit, authentication could work as follows:

- For the Internet constituency, service could be granted if one of the following schemes is used:
  - The client's request comes from the Internet. This authentication is minimal and requires that a request simply be presented to the Functional Unit.
  - The client's request comes from the Internet where mapping the Internet Protocol (IP) address of the requesting host to its hostname and back to an IP address produces the same IP address of the requesting host. This authentication is slightly stronger than the first scheme described above and attempts to detect Domain Name Service (DNS) discrepancies, which are sometimes an indication of an attack.
  - The client's request comes from the Internet, and it uses some form of login and password. This is an even stronger authentication mechanism that attempts to require a previous interaction to register with the Web server.
  - The client's request comes from the Internet, and it uses some ancillary authentication such as a certificate. This is the strongest of the four schemes listed here.
- For the enterprise constituency, service could be granted if the following scheme is used:
  - The request comes from the enterprise network and uses a strongly authenticated and encrypted communication channel. Strong authentication reduces the likelihood of an intruder impersonating an otherwise authorized user. An encrypted channel reduces the likelihood of an intruder listening in on the network connection. Technology examples are the Secure Shell (SSH),[4] Secure Socket Layer (SSL),[5] and IP Security (IPSec).[6]

Determining whether the authentication takes place in networking infrastructure components, the computer system, or some combination of the two is the responsibility of the Functional Unit architects and builders. The point is that every Functional Unit has, and therefore must clearly define, the authentication requirements for gaining access to the critical information assets provided to constituencies of the services supplied by the Functional Unit. Clients of Functional Unit services need to know how to authenticate to that Functional Unit to gain access to the critical information assets that it provides.

---

[4] *SSH Communications Security.* http://www.ssh.com/ (2004).
[5] *Open SSL Project.* http://www.openssl.org/ (2002).
[6] *IP Security Protocol.* http://www.ietf.org/html.charters/ipsec-charter.html (2003).

2.2 Functional Unit Identification

One of the hypotheses of this technical note is that every enterprise network consists of several Functional Units even if the system administrators who maintain these networks do not recognize them. For those organizations that want to adopt the Functional Unit perspective, how would those system administrators identify the Functional Units in their enterprise? What information would they need to know to discover what Functional Units there are, what services they provide, who are the constituencies to whom these services are being provided, and what type of authentication is being used? The list below includes some artifacts that should be helpful in determining the set of Functional Units in the enterprise network:

- network traffic captures. By analyzing these traffic captures, the system administrator can determine which computer systems and network infrastructure components communicate with one another, what information they exchange with each other (protocols and perhaps authentication information), and the results of the communication attempt (an answer or request denied, which may give more information about who the constituencies truly are).

  Note that the capture's time should be long enough to capture even the occasional interactions. For example, some activities may happen only once a month or once a quarter. If the captures represent only one week's worth of data, less frequent activities may not be captured.

  The captures should also include all networks in the enterprise. For example, there should be a capture of the DMZ, any internal networks, and perhaps even a capture of the traffic beyond the Internet border router.

- logging information. The network may not contain all of the dialogue. There may be more information, including more details about denied requests, saved in log files on disk. That information can give more clues about the functional units. This kind of information must be sampled over a long enough period of time to capture occasional activities.

- a list of running programs, services available to the network or on a computer system that may not have been used, etc. This information gives a more complete picture than the network alone. Perhaps there are services that haven't been used during the span of the network capture. Again, this kind of information must be sampled over a long enough period of time to capture occasional activities.

- system administrators' testimony. The system administrators who manage these technologies may have more insight into what they do, although that information could be dated. This information may state what the various computer system and network infrastructure components used to do and not what they presently do. Therefore, this information should be thoroughly corroborated before being used.

- an inventory of the computer systems and network infrastructure components. This inventory should include the list of hardware and software that is installed at all enterprise sites or sites of interest.
- network diagrams. These are pictures that show how the computer systems and network infrastructure components are connected.
- policies and procedures that are in place. These may define some of the constituencies and the authentication schemes.

The process by which the Functional Units in an enterprise are identified is called the *Functional Unit Identification Process*. System administrators start with as many of the artifacts from the above list as can be found. They then analyze these artifacts to see communication patterns, the list of critical information assets provided through network-based connections to services, and the authentication schemes.

There are at least two ways to proceed given the artifacts: the network-traffic-first method and the network-traffic-last method. Each of these is discussed below.

In the network-traffic-first method, the fundamental assumption is that all network traffic captured by a network analysis tool (Ethereal,[7] for example) identifies all of the computer systems and network infrastructure components in the enterprise and defines all of the interactions between all of the Functional Units and their constituencies. Thus, when applying this method to all captured packets, every packet should be categorized as to the Functional Unit, the constituency, and the network service used. No packets should be ignored.[8] A complete list of computer systems and network infrastructure components will be produced as well as the topology of the networks that connect them.

For example, packets to and from a DNS server indicate the presence of a DNS Functional Unit. Further analysis of those packets may show which computer systems are the primary and secondary DNS servers. These servers are all part of the DNS Functional Unit. In addition, there may be routers or other network infrastructure components that are part of the communication path between a constituency and a computer system. These network infrastructure components are also part of the DNS Functional Unit. This same traffic also identifies the constituencies serviced by the DNS Functional Unit.

Once the constituent elements that make up the Functional Unit have been identified, the other artifacts from these constituent elements are further analyzed to identify the critical information assets, the authentication scheme, and the constituencies. Some of this information may also be gleaned from a detailed analysis of each packet's contents or perhaps all packets in a complete connection. This analysis depends on the service used, so it is challenging to define an all-encompassing, step-by-step procedure intended to identify the

[7] *Ethereal.* http://www.ethereal.com/ (2004).

[8] It is possible for an attack to occur during the packet-capture activity. This could cause the constituencies or the set of constituent elements in a Functional Unit to be defined incorrectly.

constituencies, computer systems and network infrastructure components, critical information assets, services, and authentication schemes.

Returning to our DNS example, an inspection of the DNS and any configuration files from the router network's infrastructure components should define the information assets served through the DNS protocol, the constituencies, the authentication scheme, and any other computer systems and network infrastructure components in the Functional Unit.

The network-traffic-first method does not require a list of the enterprise's technology or the topology of the computer systems and network infrastructure components. The list of computer systems and network infrastructure components and their topology, meaning a network diagram, can all be created by analyzing network traffic. This method makes fewer assumptions about the enterprise's network, choosing instead to discover the constituent pieces, how they are connected, and the services offered. The results reflect the enterprise network as it is presently constituted.

In the network-traffic-last method, the system administrator starts with a network diagram artifact and uses it in conjunction with as many of the other artifacts as are available. The system administrator then determines the set of Functional Units, their constituent elements, the critical information assets they provide, the network-based services they use, and authentication schemes. The network traffic is used as the last step to verify the results of the analysis of all of the other artifacts.

This method is based on the accuracy of the network diagram relative to the enterprise network. If the network diagram has been kept up-to-date, then it is a useful artifact for identifying all of the Functional Units and their attributes. Network traffic analysis is easier because the set of computer systems and network infrastructure components, Functional Units, critical information assets, and network-based services is known. The task becomes one of verifying the results of the analysis using network traffic. However, if the network diagram is inaccurate, then the network-traffic-first method produces results more directly.

No matter which method is used, the goal is to group computer systems and network infrastructure components together based on the functions they provide to the enterprise and then to give names to those groups. It's helpful to have an idea of what kinds of groups are likely to be found. Most enterprise networks consist of a subset of the following core groupings:

- Domain Name Service – provides DNS information
- host configuration – provides networking specifics to enterprise computer systems and network infrastructure components
- user authentication – authenticates users to the enterprise
- logging – keeps record of activities in the enterprise

- network intrusion detection – recognizes intrusion attempts through network analysis
- file service – provides files to users and servers
- file backup and restore – archives and accesses saved file archives
- electronic mail – supports email from within the enterprise, including virus and spam detection and remediation
- Web development and delivery – produces and delivers critical information assets through Web services
- remote access – makes enterprise resources available from beyond the enterprise network
- wireless access – makes enterprise resources available through wireless access
- Internet proxy – makes Internet resources available from the enterprise

The enterprise's network diagram should contain many of these groupings, as well as others that are specific to the enterprise's mission.

In the best case, each computer system and network infrastructure component should be a member of only one Functional Unit. Pragmatically, this is often not the case, primarily for economic reasons. There is usually some overlap when a network infrastructure component connects many computer systems or when a computer system provides more than one service.

Routers, firewalls, switches, and hubs are typically members of more than one Functional Unit. For firewalls and routers, this happens because these network devices contain many rules that support different access policies based upon constituency needs. For example, there could be some rules that allow DNS traffic and other rules that allow Web traffic. The former of these rules make the router or switch a member of the DNS Functional Unit, whereas the latter of these rules make it a member of the Web Development and Delivery Functional Unit.

For switches, members of different Functional Units may be connected as a matter of convenience or as a way to isolate one Functional Unit from another while still attaching each to a network. Finally for hubs, multiple Functional Units can be connected to a single network port. In all of these cases, the firewall, router, switch, or hub is a member of more than one Functional Unit, and it needs to be recognized as such.

Computer systems may be members of more than one Functional Unit. Unfortunately, some system administrators still operate more than one service on a computer system. A common example is the File Transfer Protocol (FTP) and World Wide Web (WWW) services on the same computer system. Hosting multiple services on a single computer system can create avoidable vulnerabilities that put the organization at unnecessary risk. As a side benefit, determining the allocation of elements to Functional Units can aid in this determination and possible remediation.

At the completion of the Functional Unit Identification Process, there is now an accurate network diagram that has lines drawn around the identified Functional Units. Inside these lines is the set of computer systems and network infrastructure components that cooperate to deliver critical information assets to constituencies through network-based services. In some cases, the constituent elements may be members of more than one Functional Unit.

This new network diagram is a living document that identifies all of the Functional Units in the enterprise. The Functional Unit Identification Process also creates another document that describes the attributes of each Functional Unit. Specifically, this document contains

- the names of all of the computer systems and network infrastructure components in the Functional Unit
- the information assets delivered by the Functional Unit
- the network-based services used to deliver those assets
- the constituencies serviced by the Functional Unit
- the Functional Unit authentication scheme

Figure 2 below shows a network diagram where the Functional Units have been identified.

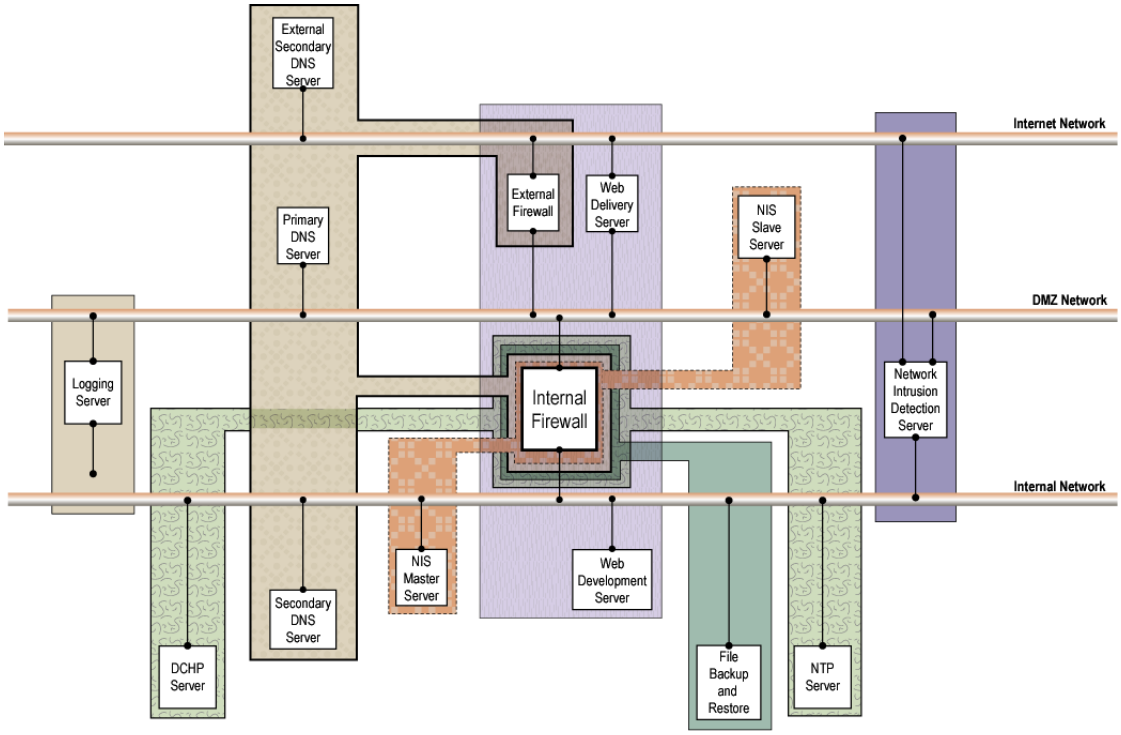

Figure 2: Functional Units

The work could end at this point with the Functional Units in the enterprise network having been identified and documented. As changes are made, the two living documents need to be

kept up-to-date as a way to help the enterprise's system administration staff balance the mission with technology. One way to accomplish this is by periodically performing the Functional Unit Identification Process. This process is analogous to a store annually taking inventory to discover what products are really on their shelves.

The next section extends the notion of a Functional Unit to include the concept of survivability.

3 What Is a Survivable Functional Unit?

When an organization chooses to manage its enterprise network as a collection of Functional Units, it first uses the Functional Unit Identification Process to identify the Functional Units that it already has in place. The next step is to transform those Functional Units into Survivable Functional Units, that is, Functional Units that can provide essential services in the presence of attacks, failures, or accidents and recover full services in a timely manner [CERT 03a]. Survivable Functional Units always provide properly authenticated access to critical information assets through network-based services, even if that access is degraded because of attacks, failures, or accidents.

Applying survivability in an operational setting is not yet well defined. There are only a few practices that can be used to design and build a more Survivable Functional Unit. Nonetheless, it is possible to at least enumerate options intended to improve the survivability of a Functional Unit.

Continuing the example of the Web Delivery and Development Functional Unit, the list below identifies a set of options to the Functional Unit that attempt to make it more survivable.

- A distributed delivery architecture uses several computer systems. These computer systems are connected to different networks that are each connected to the Internet through a different Internet Service Provider (ISP). This redundancy attempts to mitigate the risks of an attack on any one of the computer systems or ISPs.
- The Domain Name Service Functional Unit distributes the client load across the delivery computer systems. Load distribution can use a round-robin scheduling approach, for example. This scheme attempts to make the number and placement of the delivery computer systems transparent to the constituency.
- The computer systems and network infrastructure components are kept up-to-date with respect to patches. The use of timely patch applications[9] is one of the most significant actions that a system administrator can take to defend against intrusion attempts.
- The computer systems and network infrastructure components are instrumented to detect host-based anomaly intrusions. These techniques are described in the Security Knowledge in Practice (SKiP) Method from “Securing Information Assets: Security

[9] Some organizations prefer scheduled (as opposed to timely) applications of sets of patches as a more effective means to ensure availability. Patches need to be installed, and the decision about timely applications (affecting short-term availability) versus scheduled applications (accepting short-term risk) needs to be made.

Knowledge in Practice" [Rogers 02]. This early warning technology helps the system administrator recognize when computer systems and network infrastructure components are under attack.

- The client authentication scheme used is very strong. The scheme could use some combination of one-time passwords and biometric identification. This scheme attempts to reduce unauthorized access to computer systems and network infrastructure components and their service.
- All network-based administrative activity uses strongly authenticated and encrypted connections. Doing this attempts to reduce the unauthorized access and defend against inadvertent disclosure of the administrative session.
- Physical survivability issues need to be evaluated. Topics should include, but are not limited to, physical access control and authentication, uninterruptible power supplies, and heating, ventilation, and air conditioning (HVAC) requirements. Attacks on the physical plant that houses the Functional Unit must also be evaluated.

How does the organization decide how much to pay for improving the survivability of a Functional Unit? The next section provides some help in answering this question.

3.1 How Much Survivability?

Survivability has a cost, whether it is additional equipment, redundant services, or the time and effort needed to patch computer systems and network infrastructure components and maintain survivability characteristics. Once the options have been identified, the question becomes: Which options make sense and how much of each option makes a Functional Unit sufficiently survivable for the organization?

Again returning to our example of the Web Development and Delivery Functional Unit, the first item from the list of options in the previous section identifies replicated delivery computer systems as a way to improve survivability. How much replication is enough? Are 100 Web delivery computer systems matched with 100 separate ISP connections too many? Perhaps it is for most enterprises, with the possible exception of eBay®, Amazon, Microsoft®, and a handful of others. How about 50 computer systems and ISP connections? That may be too many also. Those are the easy numbers to eliminate. But what about 10 and 10, 5 and 5, or 3 and 3? These smaller numbers are not so easily dismissed for the average enterprise.

How about the other options on the list? Is patching justified? Applying patches is labor intensive and frequently produces equally vulnerable configurations after applying patches. Should valuable system-administrator time be spent applying patches? Perhaps. The same arguments can be raised for the other items on the list.

What's the answer?

All of these options attempt to reduce the likelihood that the constituent elements in the Functional Unit won't be able to deliver the critical information assets to the constituencies through network-based services. Evaluating, selecting, and prioritizing these options occurs as part of risk management. What then is the risk that an attack, failure, or accident will happen? What is the likelihood that it will compromise the Functional Unit in some way, and should that happen, what is the impact on the enterprise?

The CERT® Operationally Critical Threat, Asset, and Vulnerability Evaluation℠ (OCTAVE®) Method [CERT 03b] is one standard approach for a risk-driven, asset- and practice-based information security evaluation. OCTAVE uses the importance of assets to the enterprise's mission to help select alternatives appropriate to threats and vulnerabilities, while taking any organizational constraints into consideration. The system administrator may be part of the cross-disciplinary task force that has the responsibility of assessing the likelihood of the threat and its impact as well as considering the budget, all of which are an integral part of selecting options.

No matter how this task force is constituted, the system administrator will have the job of putting their recommendations into production. In this case, the system administrator uses the listed options to design a Web Development and Delivery Survivable Functional Unit that matches the needs and constraints of the enterprise. The resulting Survivable Functional Unit is sufficiently robust and reliable given the impact of an attack by a would-be intruder.

If an organization chooses to turn its Functional Units into Survivable Functional Units, the previously described network diagram and Functional Unit attribute documents need to be changed to reflect these improvements.

® CERT and OCTAVE are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

℠ Operationally Critical Threat, Asset, and Vulnerability Evaluation is a service mark of Carnegie Mellon University.

4 Current Work on Survivable Functional Units

The concepts of Functional Units and Survivable Functional Units are the cornerstone of the Survivability and Information Assurance (SIA) curriculum currently under development through a partnership between the Software Engineering Institute and the Community College of Allegheny County (CCAC).[10] This curriculum is described at http://sia.ccac.edu.

Briefly, the goal of the curriculum is to teach system administrators about information assurance (IA) and provide a way to integrate information assurance into their routine tasks. The intent is to produce a more survivable operational state for the enterprise network.

The curriculum contains four courses that provide the education and training necessary to integrate IA into the day-to-day tasks of today's system administrators. SIA Course 1,[11] entitled *Principles of Survivability and Information Assurance*, describes the concepts of Survivable Functional Units as one of the 10 principles of survivability and information assurance. This course expands on the concepts and methods described in this technical note.

SIA Courses 2[12] and 3,[13] entitled *Information Assurance Networking Fundamentals I and II*, examine the networking fundamentals of survivability and security for enterprise systems. These courses examine various information assurance concepts with respect to the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite, User Datagram Protocol (UDP), and the Ethernet.

SIA Course 4,[14] entitled *Sustaining, Improving, and Building Survivable Functional Units*, places the student in the role of a system administrator newly hired into an enterprise. The student analyzes the enterprise network built in the laboratory to determine the Functional Units in that network. They then manage that network using the concept of Survivable Functional Units and the SKiP Method, 2 of the 10 principles described in SIA Course 1. Students apply what they learned in SIA Courses 1, 2, and 3 to a working enterprise network.

[10] *Community College of Allegheny County*. http://www.ccac.edu.
[11] *SIA 1: Principles of Survivability and Information Assurance I*. http://sia.ccac.edu/sia1.htm.
[12] *SIA 2*: *Information Assurance Networking Fundamentals I*. http://sia.ccac.edu/sia2.htm.
[13] *SIA 3: Information Assurance Networking Fundamentals II*. http://sia.ccac.edu/sia3.htm.
[14] *SIA 4: Sustaining, Improving, and Building Functional Units*. http://sia.ccac.edu/sia4.htm.

5 The Future of Survivable Functional Units

Survivable Functional Units are a new and different way for system administrators to think about how they manage their computer systems and network infrastructure components. This section describes three areas where this concept of a Survivable Functional Unit can mature.

5.1 Adoption and Refinement

The ideas described in this technical note represent the culmination of years of system administration work by the author. The term *Survivable Functional Unit* puts a formal name on a previously nameless concept that several seasoned system and network administrators recognized as existing in the networks they've managed. In other words, Survivable Functional Units have always been a part of our networks. Now they have a name and a more rigorous definition, and they can be linked to the mission of the enterprise in a more straightforward manner.

These ideas are relatively new and, as such, they need wider adoption and refinement. The SIA Curriculum described in Section 4 was designed to educate and train system administrators and their managers in the concepts and practical applications of Survivable Functional Units. As this curriculum is licensed and used by educational institutions, Survivable Functional Units will be more widely adopted and refined.

The readers of this technical note are also encouraged to adopt and refine these concepts. Comments and suggestions should be directed to the author of this report (lrr@cert.org).

5.2 A Handbook for Survivable Functional Units

Many system administrators believe that their network is unique and that it often requires a significant level of effort to design it and keep it running smoothly. Our observation is that most enterprise networks have much in common, especially at the core Functional Unit level as previously described. Because of this level of commonality, the topologies of these core Functional Units and the set of decisions that system administrators need to make can be assembled and published in a Handbook for Survivable Functional Units.

The differences between how organizations design and build these core Functional Units are small but important enough that the handbook should show diagrams of the two to four most common architectures for each Functional Unit. As a further aid to the system administrator, the handbook should describe the conditions under which the architecture of each Functional

Unit is preferred. Finally, the handbook would list survivability options and show diagrams of the resulting Survivable Functional Units.

The rationale behind this handbook is that many system administrators have already designed and built Functional Units that successfully provide access to critical information assets through network-based services. Those designs and the thinking behind them need to be published so that other system administrators and practitioners can benefit from them. It is counter-productive and inefficient for system administrators to start anew each time they need to build or re-build functionality in their enterprise's network. The Handbook for Survivable Functional Units would give the guidance that system administrators need to design and build survivable functionality effectively.

Among the challenges in writing such a handbook is finding candidate designs of the core Functional Units and the rationale for their architecture. Potential sources include the networks of highly regulated industries (e.g., financial services and health care). Large e-commerce vendors may be another source. Encouraging them to share their designs and approaches can provide a rich set of candidate designs.

5.3 Survivable Functional Units and Vendors

Consider an analogy where a car is thought of as a Survivable Functional Unit. When you buy a car, you don't buy the front seats, the steering wheel, the chassis, etc., and then assemble them into a working (and hopefully reliable) car. Instead, you buy a complete car package with the options you want (engine size, transmission, color, and interior amenities, for example). Why then are we asked to purchase our networks a piece or a small group at a time, and then shape them to fit onto the enterprise's network "chassis"?

Given the concept of Survivable Functional Units and the Handbook for Survivable Functional Units, organizations should be asking vendors to build and sell core Survivable Functional Unit products. If there is sufficient demand, the vendors may learn what their customers want to buy and then respond by building and selling these products.

Much like a car, there should be options. For example, in the Web Delivery and Development Survivable Functional Unit, some of the options could be as follows:

- Web requests processed per unit of time: How much capacity does an organization want? This is analogous to how fast a driver wants a car to go.
- level of tolerance to distributed denial-of-service traffic: How survivable should the Functional Unit be to a specific and common type of attack? This is analogous to the crash worthiness of the front and rear bumpers, the fuel tank, side impacts, etc. While these features have government-mandated minimums, some manufactures advertise that they exceed them.

System administrators should think in Survivable Functional Units, and vendors could support that thinking by selling Survivable Functional Unit products. Even if the major vendors don’t sell these products, perhaps some leading-edge original equipment manufacturer (OEM) will be so inclined.

6 Summary

System administrators face the challenge of properly managing the computer systems and network infrastructure components in the enterprise network. This challenge is growing because the enterprise depends more and more on computer and network technology to achieve its mission, while the technology is constantly changing.

System administrators can easily lose sight of that mission when the quantity and quality of technology they must manage exceeds their capacity. The mission becomes secondary in deference to the computer and network technology originally purchased to achieve mission success.

The concept of a Survivable Functional Unit can help system administrators manage their enterprise networks. A Survivable Functional Unit is an abstraction of a collection of computer systems and network infrastructure components that (1) delivers critical information assets in the presence of attacks, failures, or accidents, through network-based services to constituencies that are authenticated to the Survivable Functional Unit, and (2) recovers those services fully in a timely manner.

By thinking of the enterprise network as a collection of cooperating Survivable Functional Units, system administrators can focus on the mission of the technology more easily and avoid becoming overwhelmed by the details of that technology. When they are more able to link the Survivable Functional Units and the services they deliver to the mission, goals, and objectives of the enterprise, they are more likely to be successful when proposing investments, prioritizing the tasks they must accomplish, and explaining the technology they manage to other parts of the enterprise.

Core Survivable Functional Units have already been built by system administrators. Their successes and the thinking behind them should be shared with others who would benefit from these experiences.

Finally, Survivable Functional Units should be the fundamental building blocks used to create tomorrow's enterprise networks. Vendors could support this effort by selling Survivable Functional Units rather than the computer systems and network infrastructure components they sell today.

References

URLs are valid as of May 2004.

[CERT 03a] CERT. *Research and Trends.* http://www.cert.org/nav/index_purple.html. (2003).

[CERT 03b] CERT. *OCTAVE.* http://www.cert.org/octave. (2003).

[Rogers 02] Rogers, Larry and Allen, Julia. "Securing Information Assets: Security Knowledge in Practice." *Crosstalk 15*, 11(November 2002). http://www.stsc.hill.af.mil/crosstalk/2002/11/rogers.html.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
(Leave Blank)	May 2004	Final

4. TITLE AND SUBTITLE	5. FUNDING NUMBERS
Survivable Functional Units: Balancing an Enterprise's Mission and Technology	F19628-00-C-0003

6. AUTHOR(S)

Lawrence R. Rogers

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213	CMU/SEI-2004-TN-004

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSORING/MONITORING AGENCY REPORT NUMBER
HQ ESC/XPK 5 Eglin Street Hanscom AFB, MA 01731-2116	

11. SUPPLEMENTARY NOTES

12A DISTRIBUTION/AVAILABILITY STATEMENT	12B DISTRIBUTION CODE
Unclassified/Unlimited, DTIC, NTIS	

13. ABSTRACT (MAXIMUM 200 WORDS)

Enterprises strive for success in fulfilling their mission to their customers. Information and its management are key components of their ability to succeed. Computer systems and network infrastructure components–the technologies that process this information–are playing an increasingly larger role in support of an enterprise's ability to fulfill its customers' needs. Their role has grown to a point where the slightest disruption–break-ins or even attempted break-ins–can adversely affect the enterprise's ability to manage information and therefore deliver products and services to its customers.

Although system administrators often need to focus on the details of computer systems and network infrastructure components to keep them operating smoothly, they must also be able to see the role that these technologies play in support of the enterprise's mission. This technical note describes Survivable Functional Units, a way to think about these enterprise networks. Although Survivable Functional Units have always been a part of networks, they now have a name and a more rigorous definition, and they can be linked to the mission of the enterprise in a more straightforward manner. The intended audience for this technical note is system administrators and their immediate managers, though the concepts have wider applicability.

14. SUBJECT TERMS	15. NUMBER OF PAGES
computer system, functional unit, information processor, network infrastructure, survivable functional unit, system administrator	26

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL