Chapter 6: Understanding DSS Architecture, Networking and Security Issues

Contents

I. Introduction

IT architectures and computing infrastructures are evolving rapidly in corporations. In some companies, the IT infrastructure is being built in an ad hoc, uncoordinated, opportunistic manner. This approach is understandable given the rapid pace of technological change, but companies need much more than a "Web server here and a router there" approach to information technology architecture and networking. Managers need to take steps to design an infrastructure that 1) minimizes support costs and maximizes user productivity; 2) avoids system crashes and other performance problems; and 3) reduces infrastructure impediments that delay the deployment of new IS/IT applications, especially DSS. Networks are the critical element of the IT infrastructure that supports most Decision Support Systems.

According to Evans and Wurster in a 1997 **Harvard Business Review** article, the "rapid emergence of universal technical standards for communication, allowing everybody to communicate with everybody else at essentially zero cost, is a sea change." They note "It is easy to get lost in the technical jargon, but the important principle here is that the same technical standards underlie all the so-called Net technologies: the Internet, which connects everyone; extranets, which connect companies to one another; and intranets, which connect individuals within companies." Both managers and MIS staff need to understand the magnitude of this fundamental change in how we can communicate.

You may be asking how is the DSS architecture and IS/IT infrastructure related to networking and security issues. Part of a DSS architecture is the network design. Security issues for a DSS are impacted by architecture and network choices. These three topics are closely intertwined and are very important issues for building useful Decision Support Systems. Unless we build a DSS on a standalone computer in a secured office environment and keep the computer under the watchful eye of the manager who is using it, we will need to address DSS architecture, networking and security issues. If we want to design, develop and implement successful Decision Support Systems, then we need to understand these three fundamental technical topics.

This chapter explores the basics of DSS architecture, enterprise-wide networks and extranets, and security issues. The linkages among these issues are also explored.

I. DSS Architecture and IS/IT Infrastructure

Many academics discuss building Decision Support Systems in terms of four major components - the user interface, a database, models and analytical tools, and the DSS architecture and network (see Figure 6.1). One can label these components collectively as the overall architecture of a DSS. This traditional view of DSS components remains useful because it identifies commonalties between different types of DSS, but it provides only an initial perspective for understanding DSS architectures.

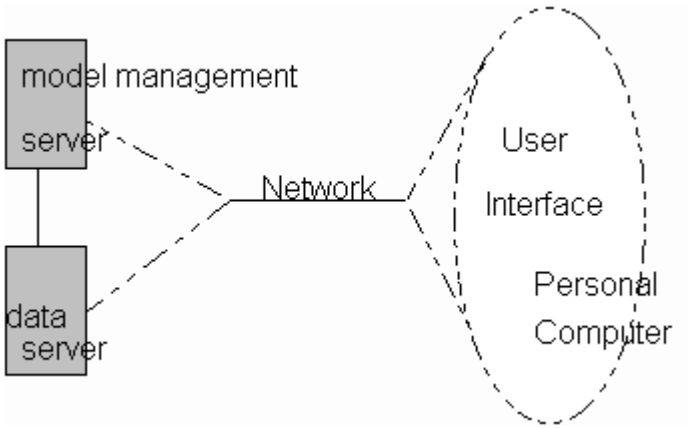

Figure 6.1. DSS components.

As noted previously, a major component in the design of a DSS is the user interface. The tools for building the user interface are sometimes termed DSS generators, query and reporting tools, and front-end development packages. DSS user interfaces can be distributed to clients in a "thick-client" architecture or delivered over a network using Web pages or Java applets in a "thin-client" architecture. A thin-client architecture where a user interacts using a web browser has many advantages, but until recently the sophistication of the user interface was limited compared to a thick-client architecture where a program resides on a DSS user's computer.

A DSS database is a collection of data organized for easy access and analysis. Large databases in enterprise-wide DSS are often called data warehouses or data marts. Document or unstructured data is stored differently than structured data. Web servers provide a powerful platform for unstructured data and documents. The architecture for a structured DSS database for a Data-Driven DSS often involves multiple servers, specialized hardware and in some cases both multidimensional and relational database software. The extraction, transformation, loading and indexing of structured DSS data is a black art, and there are as many data engineering strategies as there are data warehouses.

Mathematical and analytical models are an important part of many DSS, especially Model-Driven DSS. Model management software can be centralized on a server with a database or specific models can be distributed to client computers. Java applets and JavaScript programs provide a powerful new means of delivering models to users in a thin-client architecture.

The DSS architecture and network component refers to how hardware is organized, how software and data are distributed in the system and how components of the DSS are integrated and physically connected. A major issue today is whether DSS should only be available using thin-client technology on a company intranet or available on the Global Internet. Scalability is also an important DSS issue. Scalability refers to the ability to "scale" hardware and software to support larger or smaller volumes of data and more or fewer users. Practical scalability is the ability to increase or decrease size or capability of a DSS in cost-effective increments.

The DSS framework discussed in Chapter 1 showed the different emphases that are placed on DSS components when specific types of DSS are actually constructed. Architecture, networking and security issues vary for Data-Driven, Document-Driven DSS, Model-Driven and Suggestion DSS. Multi-participant systems like Group and Inter-Organizational DSS rely heavily on network technologies. The architecture of a Data-Driven DSS emphasizes database performance and scalability. Most Model-Driven DSS architectures store the model software on a server and distribute the user interface software to clients. Networking issues create challenges for many types of DSS but especially for a geographically distributed, multi-participant DSS. Table 6.1 identifies some of the architecture requirements for different categories of DSS.

Type	Network Needed	Components
Communications-Driven and GDSS	Always	Message storage, process support for GDSS
Data-Driven	Usually	Web-enabled data access
Document-Driven	Usually	HTML, TXT and PDF file storage and searching
Knowledge-Driven	Sometimes	AI, statistical models, Java, JavaScript, Web delivery
Model-Driven	Sometimes	Optimization, Simulation processing, Java, JavaScript
Inter-Organizational	Always	It depends on purpose

Table 6.1. DSS Framework and Architecture Issues.

An architecture for any information system is a formal definition of its elements or parts. A DSS/IS/IT architecture can be diagrammed in terms of four layers: the business process map, the systems architecture, the technical architecture, and a product delivery architecture. The business process architecture shows how tasks are completed. The systems architecture shows the software components. The technical architecture focuses on hardware, protocols and networking. The product delivery architecture focuses on outputs of the system.

II. Defining the DSS Architecture

Having a well-defined and well-communicated Decision Support System architecture provides an organization with significant benefits. An architecture helps developers work together, improves planning, increases the development teams ability to communicate system concepts to management, increases the team's ability to communicate needs to potential vendors, and increases the ability of other groups to implement systems that must work with the DSS. Technical benefits of a DSS architecture include the ability to plan systems in an effective and coordinated fashion and to evaluate technology options within a context of how they will work rather than abstractly. A DSS vision and an architecture helps communicate the future and provides a consistent goal for making individual design decisions. Achieving all these benefits requires that both information system professionals and prospective DSS users must cooperate closely in developing the architecture.

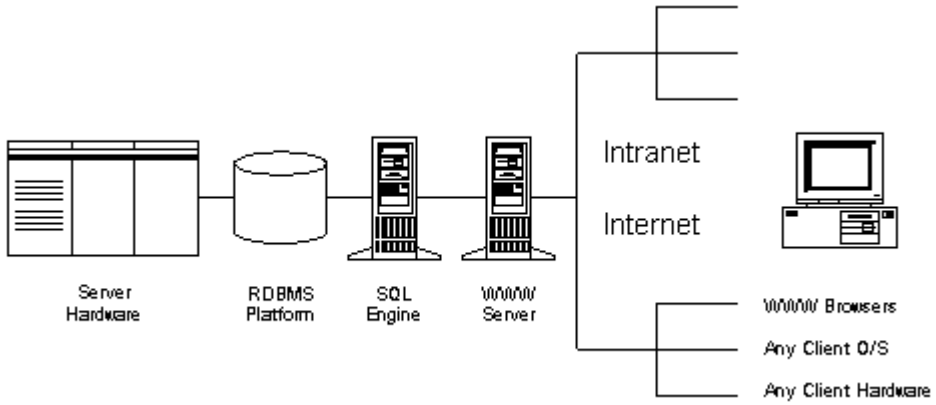

Figure 6.2 High-Level DSS Architecture

An architecture drawing provides the grand scheme of a large-scale DSS project. The overall architecture of a DSS should be diagrammed and understood before specific decisions are made. The nature of the architecture depends on the DSS. Small-scale DSS developed by individuals for their own use do not justify a major architectural planning effort, although the overall information system architecture of the organization may constrain the capabilities of desktop DSS. Enterprise-wide DSS do require careful architecture planning if they are to succeed. Figure 6.2 shows a very high-level enterprise-wide data delivery architecture. In general, much more detail about the hardware, networks, and software is needed in specifying the architecture than is shown in Figure 6.2.

According to Mallach (1994), a DSS architecture should define and specify the following components:

1. Database or databases, including any existing databases, internal or external to the organization and any databases that are created specifically for DSS use. The architecture schematic should identify who is responsible for different types of databases, including their accuracy, currency, and security.

2. Model or models, including information about their sources of data, processing, the organizational unit responsibility for maintaining them, and limits on access to them.

3. Software tools for users to access the database and the models, and software tools which system administrators can use to manage the database and the models.

4. Hardware and operating system platforms on which the databases and models reside, on which the programs run, and through which users access the DSS. Any constraints, such as a policy to standardize on products of a particular vendor or products that use a particular operating system, should be stated.

5. Networking and communication capabilities needed to connect the hardware platforms. These capabilities must support needs to connect to one or more servers and databases, needs of work group members to communicate within the group, and enterprise needs to link work groups to each other or to shared data. In many DSS situations the corporate network is used. In this case the network must be examined to make sure it meets present and future Decision Support traffic needs.

Mallach also claims potential users should be specified when a DSS architecture is designed. The specifications should state any assumptions about users' locations, jobs, levels of education, and any other factor that may affect their use of a specific Decision Support System. This information can be part of the business process map.

Bob Lambert in a paper titled "Data Warehousing Fundamentals" has a similar list of architectural issues that need to be addressed. Lambert argues "An architecture is a design completed early in a project that encompasses (but does not necessarily detail) all aspects of the finished product."

According to Lambert, a completely specified DSS architecture addresses seven major topic areas:

- A description of the problem the DSS is designed to address;
- The objectives, constraints and critical success factors for the DSS;
- Project participants and the role of each participant;
- Major system components and the interfaces, connections or communication paths among the components;
- Anticipated system enhancements, migration paths and modifications;
- An overall development and maintenance schedule and staffing plan; and
- The skills, tools and other support required to develop the Decision Support System on schedule and maintain it over the long term.

Lambert notes, "all project participants should understand and accept the architecture. The architectural design should set a common level of understanding among technical, non-technical and management participants."

Stefferud, Farber, and Dement (1982) stated that the design of a general computing architecture consists of four elements – processors, networks, services, and standards. Nolan (1983) divides an IS/IT architecture into data, applications, and communication components. Also, the capabilities of executive workstations should be determined as part of the discussion of the DSS architecture (cf., Power, 1985).

III.A Client/Server Architecture

Most DSS are built within the context of a corporate-wide client/server architecture. You might be asking, "What is a client/server architecture or what are the characteristics of a client/server architecture?" Based on Taylor (1998), client/server refers to a computational architecture that involves client processes requesting service over a network from server processes. Ravi Kalakota in the Client/Server FAQ explains client/server architectures are:

1) A combination of a client or front-end portion that interacts with the user, and a server or back-end portion that interacts with the shared resource. The client process provides the interface between the user and the rest of the application system. The server process acts as a software engine that manages shared resources such as databases, analytical processors, or printers.

2) The client and server have fundamentally different requirements for computing resources such as processor speeds, memory, disk speeds and capacities, and input/output devices.

3) Scalable. An important characteristic of client-server systems is scalability. They can be scaled horizontally or vertically. Horizontal scaling means adding or removing client workstations with only a slight performance impact. Vertical scaling means migrating to a larger and faster server machine or to multiple servers.

A common error in client/server development is to prototype an application in a small, two-tier architecture environment, and then scale up by simply adding more users to the server. This approach usually results in an ineffective system, because the server becomes overwhelmed. A three-tier architecture with a second "agent" server between the client and the server can support hundreds or thousands of users.

The Gartner group proposed terminology for describing different client/server styles or organizing schemes based on the distribution of the three components of an application: user interface, business analysis or application logic, and data management. The descriptive styles are distributed presentation, distributed function, and distributed data management. Distributed presentation is when only the user interface is processed on the client either using a Web browser or thick client interface. In a distributed function design, one part of the application processing in on the client, additional application processing is on one or more servers. Distributed function applications are the most complex type of design. In distributed data management, the entire application resides on the client and data management is located on one or more remote servers/hosts. Web-Based DSS are implemented using a distributed presentation design, but a DSS may also have distributed functions and distributed data management.

As noted, networks are a major element in the technical specification of a DSS architecture. The next section discusses this key architecture component.

IV. Networking Issues

Enterprise-wide DSS have interconnected servers, databases and workstations. In many DSS development situations an existing corporate network is used as part of the DSS architecture. In this situation the network must be examined to make sure it meets present and future DSS traffic needs. Also, the trend is toward Internet and intranet based DSS that are accessed from a browser that is connected to a Web server using the TCP/IP communications protocol.

This section summarizes a number of major issues in networking and computing communications that managers and DSS Analysts should be familiar with so they can participate in networking discussions with network technical specialists. The three major aims of this section are to:

1) Explain the basic concepts of networking,

2) Provide an explanation of what TCP/IP is and how it works,

3) Define some major networking terms.

Overview

A client/server architecture is based on having a physical network where computers act as either a server managing files and network services or as a client where users run applications and access servers. Clients rely on servers for resources like Web pages, data, files, printing and OLAP.

A network is a collection of computers connected in a way that allows them to communicate with each other and share information. To communicate the computers need an agreed upon language for communication. Networked computers are often referred to as hosts. Each host on a network must have some unique identifier that allows other hosts to communicate with it. Typical physical connections for hosts include Ethernet, token ring, serial line, and modems. Communication languages on computer networks are referred to as network protocols. A network protocol is a set of rules and formats that govern how information is sent and in what format it is sent. Some of the different network protocols used today include TCP/IP (Internet and UNIX), IPX (Novell), and Appletalk.

A number of technologies provide sharing of information, capabilities to distribute a Decision Support System, and communications connectivity. These technologies include the Internet, private Integrated Services Digital Networks (ISDN), and remote access dial-up servers. Broadband service is another form of data transmission that uses cable television coaxial and fiber optic cables. Currently, the favored technology for many new DSS is the Internet because it is inexpensive, it is low risk, and it is a mature technology.

Managers, customers and suppliers can use a dial-up or high-speed modem to connect to an Internet service provider or to their main office intranet. A major concern with using the Internet for DSS is managing security problems.

V. Sharing Resources

The fundamental purpose of computer networks is to provide access to shared resources, including storage for decision support data and information. One type of network for providing shared resources is a Local Area Network (LAN). A LAN has several primary components:

- A network interconnection and hubs (for example, copper wire, fiber optic cable, infrared, or radio).
- Network Interface Circuitry (NIC) in the individual personal computers connected to the network.
- The shared resources like a database server, each with their own NIC connected to the network.
- Software on a personal computer that uses the NIC to access the shared resources. This software is typically arranged to present the appearance to the rest of the operating system that these resources are directly connected.
- Software on the shared resource that coordinates with the software on the individual machines to provide access to the shared resources for users. This type of software is called a multi-user operating system. UNIX is a common operating system for DSS, but Windows NT is used in some architectures and for implementing some DSS packages.

The most common network design is for the server in a local area network (LAN) to be the same sort of personal computer hardware as the individual personal computers on the network. In this case, the operating system is called a "network operating system" or NOS to emphasize the difference from the single-user operating system of the personal computer. Novell Netware is an example of this approach. A NOS is an operating system that manages network resources. The NOS is like a traffic cop, controlling the exchange and flow of files, electronic mail, and print jobs. It manages multiple requests concurrently and provides the security needed in a multi-user environment.

A Local Area Network (LAN) is a communications network that serves users within a confined geographical area. It is made up of servers, workstations, a network operating system and a communications link. A Wide Area Network (WAN) is a much larger network than a LAN and all machines are not directly connected. A group of LANs are often connected and form a WAN. LANs and WANs can be directly connected to the global Internet.

VI. Connecting the Resources: TCP/IP

The Transmission Control Protocol/Internet Protocol (TCP/IP) is the most widely used set of standard networking protocols. A networking protocol enables computers to communicate with one another.

The general concept of connecting a network of dissimilar computers arose from research conducted by the Defense Advanced Research Projects Agency (DARPA). During that research, DARPA developed the TCP/IP suite of protocols to communicate among networks, and implemented an inter-network called the ARPAnet, which later evolved into the Internet. The TCP/IP suite of protocols defines formats and rules for the transmission and receipt of information independently of any given network organization or computer hardware. Although the protocols were developed for the Internet, they are also applicable to other cases where networks must be connected, including internal organizational networks called intranets. The Internet is a collection of networks and gateways that use the TCP/IP protocol suite.

Also, the Internet is a packet-switched network. A packet-switched network transmits information in small segments, called packets. If one computer transmits a lengthy file to another computer the file is divided into many packets at the origin and then reassembled at the destination. Protocols define the format of these packets, including the origin of the packet, the destination of the packet, the length of the packet, and the type of packet, as well as the way computers on the networks will receive and retransmit packets. TCP/IP routing capabilities allow forwarding of traffic from one network to another.

VII. Why TCP/IP?

The growing acceptance of TCP/IP is due to several factors. First, TCP/IP has been used since the early 1970's. Second, in the early 1980's it was distributed as a core part of Berkeley's UNIX Version 4.2 and UNIX workstations became primary servers on the Internet. TCP/IP was initially successful in the mid-80’s because it delivered a few basic services that many users needed (file transfer, electronic mail, remote logon) across a very large number of client and server systems. Several computers in a small department can use TCP/IP (along with other protocols) on a single LAN. The IP component provides routing from the department to the enterprise network, then to regional networks, and finally to the global Internet.

Third, TCP/IP is dependable. On the battlefield a communications network can be damaged, so DARPA researchers designed TCP/IP to be robust and to automatically recover from any node or phone line failure. This modular design allows the construction of very large networks with less central management. Because of its proven capabilities over Internets, its wide availability, and support for routing, it has become an accepted standard for interconnecting heterogeneous environments from multiple vendors. Fourth, when organizations use TCP/IP as their protocol stack, they can choose to use it exclusively over their own private intranet or as part of the global Internet.

VIII. TCP/IP Protocol

The objective of the Internet protocol (IP) is to get from one host to another host, with the assumption that the connection may be difficult. IP provides three capabilities: 1) a delivery service; 2) a means to fragment and reassemble data packets; and 3) routing functions to move data packets on the network.

Data might start out in Seattle with a final destination in Australia. Along the way, many computers called routers with varying capabilities will be encountered. There might be bad weather conditions that cause a particular route to be suboptimal, so the data might have to take another route. In addition, the router may not be able to transfer all the data, so the data has to be fragmented before continuing.

The TCP/IP protocol suite includes a number of protocols or rules. The Internet Protocol (IP) is a low level protocol that transports raw data over networks. The Transmission Control Protocol (TCP) sends data between programs using IP. As with all other communications protocol, TCP/IP is composed of layers.

TCP/IP assigns a unique address to every workstation in the world connected using TCP/IP. This "IP number" is a four-byte value that is created by converting each byte into a decimal number from 0 to 255 and separating the bytes with a period. For example, 208.55.100.233 is an IP number. Machines using TCP/IP also have natural language host names. A host name under TCP/IP follows the format hostname.site.domain.country. IP always uses the IP address and not the host name when it is sending information.

The Internet Protocol was developed to create a Network of Networks called the Internet. Individual machines are first connected to a LAN. TCP/IP shares the LAN with other uses, for example a Novell file server or a Windows for Workgroups peer-to-peer system. One hardware device provides the TCP/IP connection between the LAN and the rest of the Internet world. To insure that all types of systems from all vendors can communicate, TCP/IP is standardized on the LAN. TCP/IP and the Internet are not as secure as some alternative systems, but the system is available worldwide and it is inexpensive. So managers and MIS professionals need to ask how do we maintain security on networks using TCP/IP.

IX. Improving Security for Decision Support Systems

Security is a very important issue associated with building, managing and using DSS. Reports of computer crime are increasing at a rate of more than 150% a year. Viruses and worms attack computers from email message attachments. Hackers disrupt Web sites. Customer and credit card data have been stolen from Web servers. Company and customer data is valuable to competitors and thefts by unhappy employees and hackers of company data do occur. Security **IS** important.

Improving security for decision support applications involves addressing a number of issues. First, managers and MIS staff must determine security needs. Managers should ask

what are the current security problems. This task is often called security evaluation. Based on the diagnosis in the evaluation stage we need to implement the required security measures and fix any problems. These two tasks occur in what has been called the implementation stage. Once appropriate security is in place one must monitor the system and any new security problems need to be fixed. This is the feedback stage. Finally, managers and MIS Staff need to stay informed about new security problems and methods for breaking into information systems. Both managers and MIS staff need to assume shared and equal responsibility for the security of Decision Support Systems.

So let's examine the stages involved with implementing security for Information Systems and especially Decision Support Systems. The four major stages are evaluating security needs (evaluation), remedying problems and implementing solutions (implementation), observing and monitoring the operation of the system (feedback), and finally staying informed on security issues (cf., Jones, 1998).

X. Evaluation: Evaluating Security Needs

Before implementing any form of security you need to decide how important security is for your company and identify any security problems your company has that need attention. This section examines these two steps, looks at some of the possible threats and introduces some ways to evaluate security problems.

Information systems and especially DSS can be made very secure if enough effort is expended. However a very secure system is usually too inconvenient for managers to use. According to Jones (1998), when implementing a security plan both System Administrators and managers must weigh the following costs and factors:

- the importance of the computer/system, its availability and the data stored on it,
- the amount of effort required to make and keep the system secure, and
- how the security features will affect the users of the system.

A computer containing the plans for Intel's next computer chip or sensitive financial data should be carefully secured. On the other hand it doesn't make sense to spend hundreds of thousands of dollars securing a computer used for email by business students. A system can be made as secure as is necessary but in doing so you might lose all ability to make effective use of the machine. Managers and Systems Administrators must balance the needs for convenience against the need for security.

To implement security on a system you should first identify the possible threats to the system. There are three major types of threats to a computer system: physical threats, unauthorized access, and denial of service. Physical threats include fire, theft of equipment, and vandalism. Unauthorized access is the feared hacker or a former employee breaking into a company's computers or Web Site. Denial of service means people are unable to use a system because of a security breach.

A company needs a Computer Security Policy (CSP) to ensure the safe, organized and fair use of IS/IT resources. A Computer Security Policy is a document that sets out rules and principles that affect the way an organization approaches security problems. A company should specify security policy for specific DSS.

Not all attacks on computer systems rely on expert knowledge of computer hardware and software. The quickest way of denying service is to steal or destroy the physical hardware. Mechanisms should be in place to prevent access to the physical hardware of a system. Network cables are also a security risk. The simplest way to disable a computer network is to take a shovel and dig up a few of the cables used for a computer network. This problem may occur by design or accident.

Logical security threats are caused by problems with computer software. These problems are caused either by misuse, by hardware incompatibilities, by people, by mistakes in programs, or by program interactions with other programs. MIS professionals need to evaluate the possibilities of technical problems,

To break into a Decision Support System a hacker will generally go through a number of stages. The first stage is information gathering. During this phase a hacker is trying to gather as much information about your site as possible, for example, what are the user's names, their phone numbers, office locations, what machines are there. Second, using the information gathered about a DSS or OLTP a hacker tries to get a login account. It usually doesn't matter whose account. At this stage the hacker is just interested in getting onto the machine.

Third, a hacker tries to get administrator privileges for the system. Hackers exploit bugs in programs or badly configured systems. Finally, a hacker makes changes to gain access and control of the system. Social engineering is one of the most used methods for gaining access and it generally requires very little computer knowledge. The most common form of social engineering is for a hacker to impersonate an employee, usually a computer support employee, and obtain passwords or other security related information over the phone. Hackers also sift through the trash of an organization looking for passwords or other information. Some hackers actually get a job on the site; a janitor is a good bet. A lot of hackers consider people to be the weak link in security.

Passwords are the first line of defense in the security of a computer system. They are also usually the single biggest security hole. The main reason is that users perform actions with passwords that compromise their security including:

- write their password on a bit of paper and then leave it laying around,
- type their passwords in very slowly while someone is watching over their shoulder,
- choose really dumb passwords like password or their first name, and
- log into their accounts across the Internet.

These actions make it easy for hackers to obtain passwords and by pass this important first line of defense.

If a person has managed to crack someone's password and break into their account the next step they will want to take is obtain an account with more access. The Systems Administrator is responsible for first setting up the file permissions correctly and then maintaining them.

The advent of networks, especially global networks such as the Internet has drastically increased the likelihood that a network accessible DSS will be attacked. No longer do you have to worry about just people on your site. You also have to worry about all of the people on the Internet.

XI. Implementation: Remedying problems and implementing solutions

Having decided on the appropriate level of security for your site and identified the security problems at your site you now have to fix the problems and implement your security policy. This section examines tools and methods that can be used to improve security with passwords, the file system and the network.

Improving password security

There are a number of schemes Managers and Systems Administrators can use to help make passwords more secure including: user education, shadow passwords, proactive password programs, password generators, password aging, regular password cracking, and one-time passwords.

User education

Users do not want other people breaking into their accounts. If the users of a system are educated in the dangers of using bad passwords most will choose good passwords. How you perform user education will depend on your users. Different users respond to different methods. System administrators must always remember that it is important not to alienate users.

Firewalls

The Internet creates access for hackers, spies and saboteurs who would like nothing more than to break into your DSS. By connecting to the Internet you basically open the doors for them. A firewall is a concept designed to shut those doors. Basically a firewall is a collection of hardware and software that forces all in-coming and out-going Internet data to go through one gate. Everything going in and out, but especially in, of that gate is evaluated. If it doesn't fulfill a certain criteria it is shut out.

Having a firewall results in the following four advantages: protects vulnerable or strategic services, concentrates security on the most important systems, enhances privacy, and provides logging and statistics on network use.

Another measure is to have a secure server and use encryption. A Web address (the Uniform Resource Locator) for a secure server is displayed in a web browser's location field beginning with "https" rather than "http" when one enters a secure area. Most browsers also show either a closed lock or a solid key symbol in the status bar at the bottom of the screen. Companies should have a secure server for DSS applications.

XII. Feedback: Observing Operations and Maintaining Security Solutions

Once your system has been secured the job is **not** over. Managers and System Administrators must observe what people are doing with the Decision Support System and whether or not someone may have compromised the security of the DSS. Ongoing maintenance of security solutions is important. An operating system can have "security holes" that are discovered and solutions need to be implemented.

XIII. Staying Informed

Managers must also stay informed about security needs and issues. The Web is the best source of current, timely Internet security and computer security information. Some useful Web hyperlinks include:

CERT Coordination Center at http://www.cert.org. CERT is a security watch-dog and reporting group.

Sun Security site at http://java.sun.com/security focuses on UNIX and Sun Solaris security issues.

Purdue University security hotlist at http://www.cs.purdue.edu/coast/coast.html.

World Wide Web Security FAQ by Lincoln D. Stein, lstein@cshl.org, version 2.0.1, March 24, 2000 is at http://www.w3.org/Security/Faq/ .

Email lists also provide alerts for System Administrators. MIS professionals with security responsibilities need to try to keep middle-level and senior managers informed about possible security problems.

XIV. Conclusions

It is absolutely essential that a Decision Support System have an appropriate architecture, network design and level of security. Managers need to realize that the more widely accessible a DSS, the more security problems that can occur. Managers also need to

recognize that the greater the importance of DSS data, the greater the level of security that is needed. By connecting to the Internet it is no longer a case of "if" a system will be broken into but rather "when". Despite the risks, it is my opinion that we have no choice but to use the Internet for building Inter-Organizational DSS and Web-Based DSS.

A well-defined DSS architecture has many benefits. Developing a DSS should therefore include adequate attention to the many architecture issues. Networks provide the magic of high-speed data transmission that many of us have come to depend upon. So we need to understand the basics of how networks function. Security is not some specialist's responsibility. We all need to learn about security issues; security for DSS data and systems is a shared responsibility. Managers need to remember that passwords are the first line of defense against unauthorized use of a DSS. Also, DSS users themselves often weaken the defense provided by passwords. There are a number of strategies that can be used to increase the effectiveness of passwords, but the most important is user education. Educate DSS users and remind them regularly of the importance of passwords.

Security is also related to the management of networked servers. The file system structure and file permissions are the fences of multi-user operating systems like UNIX and Windows NT. If used properly permissions or rights to access files and directories and data can keep users in their own restricted areas on a server. The system administrator needs to monitor and maintain the rights and permissions granted DSS users. Finally, the network is especially important to protect. We have become very dependent on the public Internet and we need to be vigilant in our use of it. Attacks on a company's network must be anticipated and prevented when possible.

The Internet is more than a physical network connecting millions of computers that can continuously exchange information. The Internet allows us to transfer information around the world quickly. The Internet is also an information resource. And the Internet is a community of 400+ million individuals. These real people chose to interact, discuss, and share information online. Some small cadre of Internet users are anti-social and they can disrupt our computing systems.

The future of distributed DSS capabilities is only limited by a company's technology infrastructure. Technology for DSS is expanding and improving rapidly. Networking technologies will become better, faster and cheaper. Future technology will provide much higher speeds for video teleconferencing. Communications links will become wireless increasing speeds to greater than 500 Mbps. Such wireless communication links include satellite transmissions. The price for video teleconferencing will decline. The Internet has proven it can connect managers globally. The security issues associated with the Internet are being addressed proactively and the Internet is now an integral part of distributing DSS capabilities to users.

Architecture, network and security issues must be examined together during the planning for a new Decision Support System. Once a DSS is implemented, network and security monitoring must then become an ongoing activity.

XV. Audit Questions

1. Is the firm's IS/IT architecture and organization of IT resources evolving appropriately?
2. Does your company have a network? If so, what type of network?
3. Does your company connect its internal LAN to the global Internet? Is the internal network secure?
4. Does your company have a Decision Support Systems Security Policy?

Questions for Review

1. What is a DSS architecture?
2. What factors have lead to the increase in networks? What problems can networks cause companies?
3. What is a network operating system (NOS)?
4. Give examples of possible security problems related to passwords, file permissions, and using the global Internet for a DSS.
5. Outline the steps you would take to break into a DSS. How can managers make it more difficult for you to break in to a specific DSS?
6. What steps should be followed in managing IS/IT security?
7. Who should be concerned about IS/IT security issues?
8. What are the benefits of a defining a DSS architecture?

Questions for Discussion

1. What role should managers play in developing a DSS architecture?
2. How would you respond to the comment that a Client/Server architecture is not feasible in your company?
3. What are the benefits of establishing a DSS Security Policy?
4. Construct a high-level architecture diagram for a Data-Driven DSS for a small firm with 5 sales offices located in major U.S. cities and a headquarters in a small rural town.
5. What type of network and DSS architecture would you recommend for a small company located within a single building? The company has installed 25 microcomputers that are used to track production, maintain customer sales information, and create the company catalog of products and other materials for mailings. The company wants to use groupware and build a Data-Driven DSS.

An Internet Exercise

Find an example of a DSS architecture at a Web site. Check Sun, IBM or Cisco Systems. What is the URL and title of the paper? Is the paper written for managers?

XVI. Case Study - First Security Bank

Reevaluating the IS/IT Architecture

The following material is excerpted from a detailed Case Study found at URL http://www.microsoft.com/backofficeserver/bizsol/FirstSecurity.htm.

First Security Bank is the oldest multiple-state bank holding company in the United States. It has grown to become the second largest financial services organization in the Western US, with assets of approximately $22 billion. Headquartered in Salt Lake City, First Security operates hundreds of full-service banking offices throughout Utah, Idaho, New Mexico, Oregon, Nevada, Wyoming, and California.

To improve its competitive position in a dynamic industry, First Security relies on the productivity and efficiency gains afforded by information technology. The company seeks technology solutions that fulfill three core IT objectives:

1. Speed to market, which means delivering new products to banking customers faster than they can obtain them elsewhere.

2. Integration, which means all systems sharing information across applications and platforms.

3. High-quality customer service, which means providing services that customers recognize as having added value.

First Security's latest effort to stay at the forefront of technology addressed these IT mandates. The company is using Microsoft BackOffice Server at its 26 main bank locations and its 324 branch offices. The integrated BackOffice Server solution provides First Security with a consistent, scalable means of deploying and managing Microsoft Windows NT® Server operating system-based file and print services, Microsoft SNA Server connectivity for host communications, Microsoft Systems Management Server client distribution services, and a Microsoft SQL Server™-based banking application on each server.

"Microsoft BackOffice Server has played a key role in our deployment of a standard, powerful, and reliable enterprise solution in each of our campus and branch locations," says Al Pino, president of First Security Information Technology, Inc. "BackOffice Server has lowered the cost and time required to deploy our enterprise banking applications. In addition, the single point of administration and the consolidation of multiple applications on a single server will lower our technology costs into the future."

Reinventing the Infrastructure

In June 1996, First Security formed senior executive committees to begin ironing out core product and technology direction for the corporation. To achieve reduction of cost, the committees chose the Microsoft BackOffice Server product as the foundation for the company's enterprise-wide implementation. With that decision made, the company formed a rollout project for the Microsoft Windows® operating system and created a proof of concept team. Relying heavily on consultants from Microsoft and Novell, First Security employees set about proving that the products chosen would function well in a lab environment. By early 1997, a pilot project involving 50 users had demonstrated sufficient success that the company moved to the next step. In a large group conference, participants organized an architecture team for phase one development.

The Rollout Project

Phase one encompassed the deployment of BackOffice-based servers at all campus sites and business financial centers—everything except branches and the teller line of business. Started in March 1998 and completed the following November, the rollout involved approximately 5,500 client systems. Each server running BackOffice Server today supports approximately 1,000 users at each campus site.

Phase two of First Security's Windows rollout project encompasses the branch and teller line. … First Security contracted with a third-party provider to perform the actual hardware and software deployment at branches, which required only about an hour and a half on site per server. First Security was able to put file services, print services, and data application services all on one server, so they effectively halved the server hardware at the branches.

Benefits

When all phases of First Security's rollout are complete, IT managers at the company predict that users will experience greater uptime, more efficient software updates in a more timely manner, and a more reliable, stable networking and client operating environment.

Managers at First Security believe that "In this new environment, users can share information globally, or at a workgroup level, and be assured that it's readily accessible".

First Security also plans to use the system lockdown feature in Windows NT to stabilize client workstations, minimize downtime, and assure a more secure environment.

Questions for Discussion:

1. What are the elements of the First Security IS/IT system?
2. What process was used to evaluate the old system and develop a new infrastructure? How was the new distributed, client-server infrastructure implemented?
3. What are the benefits of the new infrastructure? Will the new infrastructure support DSS applications?

XVII. References

Evans, Philip B. and Thomas S. Wurster. "Strategy and the New Economics of Information." **Harvard Business Review**, September-October, 1997.

Frisch, A. **Essential System Administration**. Sebastopol, CA: O'Reilly & Associates, Inc., 1995.

Holsapple, C. W. and A. B. Whinston**. Decision Support Systems: A Knowledge Based Approach**. Minneapolis, MN.: West Publishing, Inc., 1996.

Hunt, C. **TCP/IP Network Administration**. Sebastopol, CA: O'Reilly & Associates, Inc., 1992.

Lambert, R. "Data Warehousing Fundamentals: What You Need to Know to Succeed". **Data Management Review**, March 1996.

Mallach, E. G. **Understanding Decision Support and Expert Systems**. Burr Ridge, IL: Richard D. Irwin, Inc., 1994.

Martin, E., D. DeHayes, J. Hofer, and W. Perkins. **Managing Information Technology: What Managers Need to Know**. New York: Macmillan Publishing Co., 1994.

McElreath, J. "Data Warehouses: An Architectural Perspective." **Perspectives**, October, 1995, see http://www.csc.com .

Nemeth, E., G. Snyder, S. Seebass, and T. Hein. **UNIX System Administration Handbook** (2nd edition). Upper Saddle River, NJ: Prentice-Hall PTR, 1995.

Nolan, R. L. "Building the company's computer architecture strategic plan." Stage by Stage (Nolan, Norton & Company) 2 (Winter): 1983: 1-7.

Power, D.J. and Hevner, A.R. Executive Workstations: Issues and Requirements. **Information and Management**, April 1985, 8(4), 213-220.

Sprague, R.H. and E.D. Carlson. **Building Effective Decision Support Systems**. Englewood Cliffs, NJ: Prentice-Hall, 1982.

Sprague, R. and B. McNurlin, **Information Systems Management in Practice**. Englewood Cliffs, NJ: Prentice-Hall, 1993.

Stefferud, E., D. Farber, and R. Dement. "SUMURU: A network configuration for the future." Mini-Micro Systems 15 (May): 1982 311-312.

Taylor, Lloyd ed. (1998), Client/Server Frequently Asked Questions, periodic posting to the Usenet newsgroup comp.client-server, URL: http://www.abs.net/~lloyd/csfaq.txt

Turban, E. **Decision Support and Expert Systems: Management Support Systems**. (Fourth Edition) Englewood Cliffs, NJ.: Prentice Hall, Inc, 1995.

XVIII. Web Resources

A Beginner's Guide to URLs at URL http://www.ncsa.uiuc.edu/demoweb/url-primer.html

Cisco Systems website http://www.cisco.com

Gaffin, A. with Jorg Heitkotter "EFF's (Extended) Guide to the Internet", September 1994, http://alabanza.com/kabacoff/Inter-Links/

Jones, D., "A University Course on Systems Administration", Department Math and Computing, Central Queensland University, The Study Guide, 1997-1999 at URL: http://www.infocom.cqu.edu.au/Units/aut98/85321/Study_Material/Text_Book .

Intranet FAQ at http://www.intrack.com/ intranet/ifaq.shtml

Leiner, Barry M., Vinton G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts, Stephen Wolff. "A Brief History of the Internet", http://www.isoc.org/internet/history/brief.html .

NetworkMagazine.Com at URL http://www.networkmagazine.com/ .

Novell TCP/IP Transport Supervisor's Guide, 1998 is available on the Web at URL http://occam.sjf.novell.com:8080/nw312.english/tcpipenu

Segal, B. "A Short History of Internet Protocols at CERN", 1997 at URL http://wwwcn.cern.ch/pdp/ns/ben/TCPHIST.html

SunWorld Columns http://www.sunworld.com/common/swol-backissues-columns.html

UNIX Guru Universe http://www.ugu.com

U.S. Department of Justice Computer Crime http://www.usdoj.gov/criminal/cybercrime/

World Wide Web Consortium at URL http://www.w3.org

World Wide Web FAQ http://www.boutell.com/faq/