Internet Access and Information Dissemination: Selected Topics - 5
Draft... for review and comment only ... Draft
Office of Technology, State of Minnesota

[Back to Table of Contents]

26. SECURITY TECHNOLOGY

Description:
Security technology for computer systems is especially important in a distributed, networked environment such as the Internet, with limited physical and administrative controls. In the Internet environment, five major security services should be provided. These five are identified in International Standard 7498-2, which was developed to specify security for the Open System Interconnect (OSI) model of computer networks. The five security services are:

Authentication Verification of the claimed identity of a computer or network user;

Access Control Verification and enforcement of the authorized uses of a computer ne user subsequent to authentication;

Data Integrity Verification that the contents of a data item (e.g., message,file, p have not been accidentally or intentionally changed in an unauthorized manner;

Data Confidentiality Protection of the information content from unauthorized disclo

Non-repudiation Protection against denial of sending (or receiving) a data item by (or receiver).

Information Security Technologies Explained:
The following explanations describe technologies that are available - and recommended - to verify the identify of senders and users, and to secure content of messages. Requirements are also identified for users/senders and receivers to implement the technologies.

Authentication is a security service that uses a key infrastructure to verify the sender of an incoming message and also to determine if the message received is the same as the message sent. This verification, which provides for ***data integrity***, ensures nobody intercepted or altered the message, plus verifies the identify of the sender. However, authentication does not ensure that the message remained private while in transit through the network.

Encryption is a process that codes or decodes information using "keys" known to both sending and receiving parties. Encrypted information is unreadable without first being decrypted. Encryption provides ***data confidentiality***, while authentication verifies data integrity and/or that the sender and receiver are who they say they are. Authentication by itself does not provide confidentiality: for maximum protection, authenticated information also needs to be encrypted.

Different types of keys exist: the most secure is the public / private key infrastructure (PKI), used in the authentication process to verify the identity of a user or sender of information. The PKI is based on a paired set of keys - one private; the other public - that belong to an individual. The private key is secret

to all but its owner; the public key is provided by the owner to others for authentication purposes. A message can be sent with a sender identification in the form of a "digital signature". The signature is encrypted using the sender's private key and can only be decrypted by a recipient who has the sender's public key. To ensure the content of a message remains private, it can also be encrypted to prevent unauthorized access.

1. ***What is Required for Authentication?***
Authentication of a sender's identity requires those accessing a system or sending a message to be "certified". ***Certification***, provided by a "Certificate Authority", ties individuals to a paired set of keys (private and public). Authentication also requires that both senders and receivers of messages are equipped to encrypt and decrypt (using the same algorithms). Authentication of the integrity of a message requires that both sender and receiver are equipped to apply an algorithm to the message that can uniquely identify it based on its content.

Recommendations:

2. Before applying technology, management should identify business requirements for data privacy and for verifying the identity of users (or senders of information). For example, electronic funds transfers or credit card numbers should trigger higher security requirements than the routine transfer of documents.
3. Management should ensure an integrated security system is in place offering five services: authentication, access control, data integrity, data confidentiality, and non-repudiation.
4. In addition to the five services, additional security mechanisms should be incorporated as necessary to ensure network security, security from unauthorized access, and security of information being passed through the network. Examples of additional mechanisms include audits, encryption, key management, virus protection and network procedures.

Issues:

There are several issues preventing widespread adoption and use of advanced computer security technologies within the Internet. Some of these are:

1. The historic community culture: The Internet community has emphasized openness in communications, and has viewed computer security as interfering with this goal.
2. Internet management and organization: The Internet is a loosely coupled coalition of organizations and activities without a central management structure. Only minimal rules and protocols must be followed in order to connect to the Internet communication system. Few policies or practices exist to specify acceptable use or adequate security, even though policies for both have been developed. The National Performance Review (NPR) has identified a need for such policies. However, even with policies, there is no enforcement mechanism within the Internet.
3. Availability of security systems: Many individual security products exist, however, there is still a lack of integrated security systems. An example of a desirable, but non-existent, integrated security system would be a commercially supported electronic mail security mechanism that integrated a comprehensive key management support system, user authentication and authorization support services, and user message security services.

4. Interoperability: Commercial security products that solve similar security problems usually are not interoperable with other products. Internet users often must obtain additional products in order to communicate with others. Lack of interoperable products often delays users in selecting and using security products until de facto standards emerge. Eventually an architecture should be available to assist organizations in developing security systems. The National Institute of Standards and Technology (NIST) is currently working with several organizations to establish a security architecture. This architecture should enable designing an integrated security system with interchangeable and interoperable parts.
5. Costs: Since there is yet no universal market for interoperable security products, the costs of acquiring individual security products are currently high. However, costs will go down as volume and competition increase.

References:
See also:
Appendix Section: State of Minnesota References, Related Standards and Guidelines
National Institute of Standards and Technology (NIST)
International Standard 7498-2
Others exist also, such as certification, hashing algorithms and digital signature standards

27. IMPLEMENTATION AND TOOLS

Description:

This chapter, on implementation and tools, addresses server functionality, server support, content development and automated tools and services. Server functionality involves establishing the server, implementing capabilities for searching and scripting (custom program development), developing the directory structure, and setting up any additional features and functions that are needed, such as document formatting and testing, and files, such as graphics or sound. Server support is an ongoing activity that must be planned into any Internet dissemination program.

Most servers for World Wide Web have the ability to construct "fill-in-forms" for user responses and input. Fill-in forms, along with links to other agency data base, can be combined to present significant opportunities for information dissemination. Features for information searching and scripting services can also be added, but may require custom programming or system specific support. Gopher servers support functions similar to those of WWW servers. However WWW users may not be able to fully utilize Gopher, since not all WWW browsers are designed to use all Gopher commands.

Basic software that is available includes editors for WWW document formatting (using HTML - Hyper Text Markup Language), programs to convert documents from word processing to HTML formats, and browsers to support user access to the WWW. Many of these software products are available through the Internet, some as "shareware" (pay on the honor system). Other application may also be needed, such as image processing programs for graphics, audio programs, and digital video programs. Tools that are required include HTML software tools for creating WWW pages, and FTP if placing files onto a remote server.

28. USE OF TECHNICAL STANDARDS

Description:

An open systems environment allows the free flow of information within and among systems. Open systems are not proprietary, not limited to or defined by any particular brand of hardware or software.

Requirements:

---

1. Agencies are expected to implement statewide technical standards where product availability exists.

References:
See also
Appendix: State of Minnesota References: Related Standards and Guidelines

29. SYSTEM MONITORING AND PRIVACY

Description:

System monitoring refers to any processes or functions that track, report on, or monitor activities on the electronic network. It is useful to know which information and services are being used and which are not, in terms of evaluating service provided. The use of statistical tools can assist in determining which information is in most demand.

However, agencies need to be fully aware of the implications of monitoring user access, and Should know what type of information their servers are collecting, logging, or reporting. The collection and storage of all data on individuals must be limited to that necessary for the administration and management of authorized programs. (MN Statutes Section 13.05, subd. 3.)

Requirements:

---

1. Systems must be monitored to ensure that they are functioning and that problems are addressed.
2. The Minnesota Government Data Practices Act and other information laws apply.
3. Specific information on individuals that is not required to deliver a file or function must not be collected.

References:
Appendix: Legal References

IV. ACKNOWLEDGMENTS

The following Minnesota State agencies and employees have provided assistance and input in preparing this guideline:

VOLUNTEER COMMITTEE:

```
From IPO:
Anne Bentley                          IPC Member Volunteers:
Mike Bozonie                          David Arbeit        -    LMIC
Jan Bourgoin                          Bill Batcher        -    DHS
Steve Clift                           Mel Boyton          -    Commerce
Kevin Hartmann                        Joe Harte           -    MN Trade Office
Janet Hey                             Tom Klein           -    Revisor's Office
Sarah Kline-Stensvold                 Joel Oliver         -    DTED
Susan O'Neil                          Mary Welfling       -    DOT
Tom Satre
Bev Schuft
Carol Worden
```

OTHER CONTRIBUTORS:

IPO has also received feedback from Marion Matters (Legislative Reference Library) and Bill Schnellman (Intertech).

Thanks to everyone who contributed!

V. APPENDICES

WHAT IS THE INTERNET?

NOTE: An Internet specific glossary is included in the Appendices accompanying this document

---

INTERNET DEFINED:
The Internet is a high-capacity global electronic information network. Computer networks located all over the world are linked through hardware and software connections to form the Internet.

The Internet is sometimes called "The Information Super Highway", with good cause. Like a highway for automobiles, the Internet provides "routes" on which people travel. Internet routes are electronic and are accessed through computerized technology. Highways are used to move commodities as well as people. On the Internet, information and services are being "moved" electronically from place to place.

Many people actually think of the Internet as being the set of electronic tools and services that are available from their computers. For these people, the Internet is a collection of computerized services providing navigation, access to information, document downloading, electronic mail, and other electronic links that let them navigate through a world-wide network of computers.

The Internet was not originally created for the general public. As a result, most users have not found the Internet to be particularly "user-friendly". However, as more and more people have begun to use the Internet, software tools have become available to help users navigate through through the Internet. In

fact, the creation and general availability of these tools has made it possible for the Internet to become one of the fastest growing technologies in the information age.

Any discussion of the Internet warrants an explanation of these tools and user services. Some of the most common and popular Internet user services are briefly described below. (Note: technical protocols, such as TCP/IP, are not considered to be "user services" for the purposes of this document.)

SUMMARY OF INTERNET USER SERVICES:

- GOPHER

"Gopher" is Minnesota's contribution to information access. It is a distributed document delivery tool and Internet navigator created by a team of programmers at the University of Minnesota. The team developed a Campus Wide Information System (CWIS) for use by the university's students, faculty and staff. The goal was to provide practical, useful information in electronic form on the campus computer network for easy access by everyone, yet maintain its information centrally. A secondary goal was to solve deficiencies with the File Transfer Protocol, or FTP, which was the commonly used network tool at that time.

Gopher organizes information in an online menu system which is easy to navigate and browse. Through Gopher, information can be selected and viewed on-line, which FTP does not allow. Additionally Gopher can "link" to other Gophers anywhere on the Internet. Gopher is appealing because building and maintaining Gopher menus do not require extensive technical expertise. Because of its features and ease of use, Gopher has been a major contributor to the phenomenal growth in the number of Internet users online and using the network daily.

- FTP

FTP is a standard Internet application protocol for transferring electronic files. The only function it performs is transferring files between computers, which makes it unsuitable for more sophisticated information retrieval needs. The most common complaint about FTP, especially by non-computer-literate end-users, is that it does not allow "browsing" of online information. In order to see the contents of a file, transferred with FTP, it is necessary to download the file and then view the contents. If the file does not contain the desired information, the process must be repeated. If the information is not even located at that FTP site, it is necessary to log-off and begin the procedure again at other FTP sites.

Anonymous FTP sites allow anyone on the Internet access to a set of file directories and lets them download (and sometimes upload) files. It is difficult to control what is uploaded into FTP archives, or to know who is downloading files. Also, although the FTP process is rather simple, it requires a level of computer sophistication that most users do not possess. As publicly accessible services, FTP offers few advantages over Gopher or World Wide Web. Its main advantage may be to access FTP sites for documents that aren't available elsewhere.

- TELNET

Telnet is the standard Internet application protocol for connecting to a remote service. Its purpose is to allow a user at one site to interact with a system at another site as if the user's terminal is connected directly to the remote (host) computer. Both TELNET and FTP allow users to access other computers. However, TELNET allows users to run applications and use computer services on the host computer, which FTP does not. TELNET access uses the security system of the host computer, thus activities on

the remote system can be limited by the host.

Telnet was one of the first tools built by the architects of the Internet so that they could share software and research results more easily. One of the most common uses of Telnet today is to access online library card catalogs at universities and around the world.

- WWW

World Wide Web is a network navigation tool and distributed hypertext/hypermedia system all in one. Hypertext is text with pointers to other text, allowing the user to "branch-off" to another document for more information on a given topic, and then return to the same location in the original document with ease. Hypertext is a subset of hypermedia, which is any media with pointers to other media, including graphics, audio and video. The World Wide Web was a project initiated and driven by CERN, the European Laboratory for Particle Physics located in Geneva, Switzerland. The goal of the project was to build a distributed hypermedia system that would allow the exchange of information across the Internet in the form of hypertext documents.

To use the WWW, a user must have software on a local computer (the "client") which then accesses a host computer running WWW server software. In WWW terms, the client software is called a browser. The browser reads and retrieves documents from WWW servers. The browsers can access files by FTP, Gopher, and an ever-increasing range of other methods. WWW browsers and servers also deliver hypermedia documents to network users. This means that browsers are able to display images, sound, or animations in addition to text (if the client computer has the correct hardware to play the sounds or display the graphics.)

LEGAL REFERENCES:
Minnesota Government Data Practices Act (MGDPA) - MS Chapter 13
Government Information Access Council - MS 15.95, Subd 6. 1,2; Subd 7, Subd 9
Records Management Act - MS 138.163, Official Records Act - MS 15.17
Library and Historical Data - MS 13.40, Subd 2 (may apply - concepts should be considered)
Code of Ethics for Employees in the Executive Branch - MS 43A.38
Americans with Disabilities Act (federal)

INTERNET REFERENCES AND ON-LINE RESOURCES:

This section has not yet been developed. A sample of online resources is provided to demonstrate the intent of this section.

Resources Related to Internet Security:
Usenet News groups:
alt.security
comp.admin.policy
comp.security.misc

Privacy Rights Clearinghouse:
gopher://gopher.acusd.edu

World Wide Web Security Pages
http://tansu.com.au/Info/security.htm
http://www.tis/com/

ftp://coast.cs.purdue.edu/

STATE OF MINNESOTA REFERENCES FOR INTERNET INFORMATION:

MATERIALS DEVELOPED BY MINNESOTA GOVERNMENT AGENCIES
This section is under development. The intent is to provide a list of documents, policies, standards and guidelines that have been produced by Minnesota State government agencies for Internet use. This list will provide additional sources of information for agencies who want to see what others are doing.

To date, agencies with known Internet policies are:

Minnesota Department of Transportation - Draft version dated March 13, 1995 is included in Appendix section (see Table of Contents); Final version is planned for mid July 1995.

RESEARCH REPORTS DEVELOPED FOR THE STATE OF MINNESOTA
Report on the Internet, by Dana Noonan (prepared for the Information Policy Office)

RELATED STANDARDS AND GUIDELINES
This section has not been fully developed. The intent is to eventually provide a detailed list of the specific standards and guidelines that apply to Internet use. However, these materials are available and can be located in the following location:

IPO "Handbook": Creating and Managing Information Resources for Minnesota State Government Organizations - contains IRM and other information-related policies, standards and guidelines, including materials related to the Minnesota Government Data Practices Act

"A Network User's Guide to Security" by Ray Kermode of the Intertechnologies Group

Next Section