Network Security

The Bad, The Good, and The Quiz

Technology for the Rest of Us:
What Every Librarian Should Understand about the
Technologies that Affect Us

May 26, 2004

The Ohio State University
Pfahl Hall Executive Conference Center
The Blackwell Hotel
Fisher College of Business

Peter Murray
University of Connecticut Libraries
369 Fairfield Rd, Unit 2005-A
Storrs, CT 06095-2005
Phone: +1 860-486-6771
Peter.Murray@uconn.edu
`http://www.lib.uconn.edu/`

May 27, 2004
Version 1.0.1

```
<rdf:RDF xmlns="http://web.resource.org/cc/"
    xmlns:dc="http://purl.org/dc/elements/1.1/"
    xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#">
<Work rdf:about="http://www.pandc.org/peter/presentations/ohio-tech-2004/">
   <dc:title>Network Security:  The Bad, The Good, and The Quiz</dc:title>
   <dc:description>Presentation slides, glossary, and bibliography from a seminar pre-
sented at "Technology for the Rest of Us:  What Every Librarian Should Understand
about the Technologies that Affect Us" on May 25, 2004, Ohio State University, Colum-
bus, OH.</dc:description>
   <dc:creator><Agent>
      <dc:title>Peter E. Murray</dc:title>
   </Agent></dc:creator>
   <dc:rights><Agent>
      <dc:title>Peter E. Murray</dc:title>
   </Agent></dc:rights>
   <dc:date>2004</dc:date>
   <dc:format>application/pdf</dc:format>
   <dc:type rdf:resource="http://purl.org/dc/dcmitype/Text" />
   <license rdf:resource="http://creativecommons.org/licenses/by-nc-sa/2.0/" />
</Work>

<License rdf:about="http://creativecommons.org/licenses/by-nc-sa/2.0/">
   <permits rdf:resource="http://web.resource.org/cc/Reproduction" />
   <permits rdf:resource="http://web.resource.org/cc/Distribution" />
   <requires rdf:resource="http://web.resource.org/cc/Notice" />
   <requires rdf:resource="http://web.resource.org/cc/Attribution" />
   <prohibits rdf:resource="http://web.resource.org/cc/CommercialUse" />
   <permits rdf:resource="http://web.resource.org/cc/DerivativeWorks" />
   <requires rdf:resource="http://web.resource.org/cc/ShareAlike" />
</License>

</rdf:RDF>
```

Network Security: The Bad, The Good, and The Quiz

The Bad

The Good

The Quiz

The Bad

slide 1

The Bad Guys

slide 2

Who Are They?

Not a very interesting question...

slide 3

Where Are They?

- In Russia, China, Brazil...
- In Massachusetts, South Carolina, Wyoming, Missouri...
- In Cincinnati, Toledo, Athens, Mansfield, *Cincinnati*...
- In your reading room, staff area, (wireless?) parking lot...

slide 4

Why Are They?

- Thrill seekers; hacking "gangs"
- Those seeking to launch a Distributed Denial of Service (DDoS) attack
- Those seeking "valuable" information (credit cards, identity records, etc

slide 5

What Are They Going To Do?!?

Stuff beyond your wildest dreams...

slide 6

[Distributed] Denial of Service (DDoS/DoS) Attack

"...a type of attack on a network that is designed to bring the network to its knees by flooding it with useless traffic. Many DoS attacks, such as the Ping of Death and Teardrop attacks, exploit limitations in the TCP/IP protocols. For all known DoS attacks, there are software fixes that system administrators can install to limit the damage caused by the attacks. But, like viruses, new DoS attacks are constantly being dreamed up by hackers." (DoS attack, 2002)

slide 7

E-mail Spoofing

"Forging an e-mail header to make it appear as if it came from somewhere or someone other than the actual source. The main protocol that is used when sending e-mail -- SMTP -- does not include a way to authenticate. There is an SMTP service extension (RFC 2554) that allows an SMTP client to negotiate a security level with a mail server. But if this precaution is not taken anyone with the know-how can connect to the server and use it to send spoofed messages by altering the header information." (e-mail spoofing, 2003)

slide 8

Packet Sniffer

"A program and/or device that monitors data traveling over a network. Sniffers can be used both for legitimate network management functions and for stealing information off a network. Unauthorized sniffers can be extremely dangerous to a network's security because they are virtually impossible to detect and can be inserted almost anywhere. This makes them a favorite weapon in the hacker's arsenal. On TCP/IP networks, where they sniff packets, they're often called packet sniffers." (sniffer, 2004)

slide 9

Port Scan

“The act of systematically scanning a computer's ports [in ... networks, an endpoint to a logical connection]. Since a port is a place where information goes into and out of a computer, port scanning identifies open doors to a computer. Port scanning has legitimate uses in managing networks, but port scanning also can be malicious in nature if someone is looking for a weakened access point to break into your computer.” (port scanning, 2004)

slide 10

Script Kiddie

“A person, normally someone who is not technologically sophisticated, who randomly seeks out a specific weakness over the Internet in order to gain root access to a system without really understanding what it is s/he is exploiting because the weakness was discovered by someone else. A script kiddie is not looking to target specific information or a specific company but rather uses knowledge of a vulnerability to scan the entire Internet for a victim that possesses that vulnerability.” (script kiddie, 2002)

slide 11

So what are you going to do?

- This Internet thing is just a fad -- we can ignore it.
- This Internet thing is scary -- we must disconnect from it.
- This Internet thing is useful -- we must use it wisely.

slide 12

Use a Firewall

...or, at the very least, ***Become Savvy with Router Configuration***

- *Router*: network device that join two distinct networks; or
- allow data from one network to be transmitted to the other while keeping data intended for its own network from crossing over
- *Firewall*: router with additional characteristics to examine and allow/deny access to specific types of requests
- allows quicker and a finer grain of control over the network interface

slide 13

Corollary #1: Block/Turn Off Unused "Services"

- *Service* or *Port*: An address on a machine where a particular network program is active
- Examples: HTTP (80); mail (25); daytime (7)
- How scary can the world be? Network Ports Knowedgebase **`http://www.iss.net/security_center/advice/Exploits/Ports/`**
- choice: block outbound mail except through a mail server
- choice: block inbound Microsoft Networking protocols

slide 14

Corollary #2: Know Who is On Your Network

Bad Guys on the outside, Bad Guys on the inside

- firewall with a third leg -- the *DMZ*
- place servers and a *few* administrative machines on the third leg
- authorize public ports (including wireless) with an access control device [see next/previous discussion on access control]
- Examples: Bluesocket ; cisco; others

slide 15

Patch Your System

- Windows Update (Microsoft), Software Update PrefPane (MacOS X), Redhat Network (Redhat), Packages and Ports (various *nix derivatives)
- frequency? what are your resources and tolerance of risk?

slide 16

Automatic Updates

- most major operating systems allow for automatic downloading and updating
- Windows Update Server: tie machines to a local update server where updates are downloaded, approved, and pushed to machines
- cannot be changed by end user (via domain policies); saves outbound bandwidth
- one step further...BIOS automatic startup at 6am, check in with software update and virus definition servers

slide 17

Update Virus Definitions

- don't rely on user education
- update virus definitions ***daily***
- on e-mail servers, update them ***hourly***
- get a virus scanner on your e-mail server (imbed a SPAM filter, if you like)

slide 18

Push Virus Definitions

- lock the virus definitions into a local update server
- cannot be changed by end user (locked configuration file); saves outbound bandwidth
- "Norton Corporate Edition"

slide 19

Get a Handle on Access Management

who is on your network and why?

- not necessarily what they are doing; be mindful of privacy concerns
- *Service Provisioning*: the ability to create, change and revoke individualized authorizations at a moment's notice

slide 20

Watch What You Say

Your worst enemy may be yourself.

- *Social Engineering*: You can go far with a clipboard, tie, and a purposeful stride.
- control physical access or the rest is meaningless
- the bank will never ask your for your ATM PIN; an IT professional will never ask you for your password

slide 21

Sources of Information

- key to staying safe is staying ahead
- resource are listed here for maintaining awareness

slide 22

US-CERT

- ***C***omputer ***E***mergency ***R***eadiness ***T***eam
- "Charged with protecting our nation's Internet infrastructure by coordinating defense against and response to cyber attacks."
- Partnership between the Department of Homeland Security and the public and private sectors
- Formed out of Carnegie Mellon CERT
- Newsletters at **`http://www.us-cert.gov/cas/`**

slide 23

Technical Messages

- *Technical Cyber Security Alerts:* Technical Cyber Security Alerts provide timely information about current security issues, vulnerabilities, and exploits.
- *Cyber Security Bulletins:* Cyber Security Bulletins provide bi-weekly summaries of security issues and new vulnerabilities. They also provide patches, workarounds, and other actions to help mitigate risk.

slide 24

Non-technical Messages

- *Cyber Security Alerts:* Cyber Security Alerts provide timely information about current security issues, vulnerabilities, and exploits. Cyber Security Alerts are released in conjunction with Technical Cyber Security Alerts when there is an issue that affects the general public. Cyber Security Alerts outline the steps and actions that non-technical home and corporate computer users can take to protect themselves from attack.
- *Cyber Security Tips:* Cyber Security Tips describe common security issues and offer advice for non-technical home and corporate computer users. Although each one is restricted to a single topic, complex issues may span multiple tips. Each tip builds upon the knowledge, both terminology and content, of those published prior to it.

slide 25

SANS

- Resources from SANS (SysAdmin, Audit, Network, Security) Institute
  `http://www.sans.org/newsletters/`
- ***@RISK: The Consensus Security Alert***: weekly summaries of three to eight vulnerabilities, descriptions of damage and protection/recovery strategies, and summary of the actions 15 large organizations have taken to protect their users
- ***SANS NewsBites***: weekly, high-level executive summary of the most important news articles on computer security
- ***SANS PrivacyBits***: weekly summary of news, alerts and other announcements relating to privacy in the U.S. and other countries

slide 26

Bugtraq

- at **`http://www.securityfocus.com/archive/1`**
- full disclosure, moderated mailing list for detailed discussion and announcement of computer security vulnerabilities: what they are, how to exploit them, and how to fix them
- *warning:* extremely dense, prolific, and at times incendiary, but very cutting edge

slide 27

NTBugtraq

- at **`http://www.ntbugtraq.com/`**
- same philosophy as Bugtraq, but for security exploits/bugs in Windows NT, Windows 2000, and Windows XP plus related applications

The Good

slide 28

Definitions-in-Depth: Access Management

You cannot control what you cannot define.

slide 29

Access Management Overview

slide 30

Authentication Definition

- "*Authentication* is the process where a network user establishes a right to an identity -- in essence, the right to use a name." (Lynch, 1998)
- "Authentication is the process of establishing whether or not a real-world subject is who or what its identifier says it is. Identity can be proven by: Something you know, like a password; Something you have, as with smartcards, challenge-response mechanisms, or public-key certificates; Something you are, as with positive photo identification, fingerprints, and biometrics." (I2-Authentication, 2004)

slide 31

Authorization Definition

- "*Authorization* is the process of determining whether an identity (plus a set of attributes associated with that identity) is permitted to perform some action, such as accessing a resource. Note that permission to perform an action does not guarantee that the action can be performed; for example, a common practice in cross-organizational licensing is to further limit access to a maximum number of concurrent users from among an authorized user community." (Lynch, 1998)
- "It will drive permissions for accessing networked resources, allow us to control and delegate electronic responsibilities, and serve as the basis for future administrative applications. It will allow us to convert our complex legal policies into automated systems in a easily scalable fashion." (I2-Authorization, 2004)

slide 32

Identity Management

- unique mapping of one actual individual to one network account
- no guest accounts, no open services, no exceptions
- *if you hear your campus is starting an identity management initiative, you want to be involved*
- *if your campus has not yet started an identity management project, ask why not*

slide 33

Provisioning of Services

Service Provisioning: “The process of managing attributes and accounts within the scope of a defined business process or interaction. Provisioning an account or service may involve the creation, modification, deletion, suspension, restoration of a defined set of accounts or attributes.” (Rolls, 2003)

- desire to automate management a wide variety of services: account, e-mail, file space, mainframe account, e-learning system, *ILS record, proxy server...*
- real-time (event-driven) or near-real-time (hourly batch)

slide 34

The Competing Desires

- one password per service for multiple users: easy to give out, easy to give out
- one password per service per user: administrative nightmare, privacy erroded
- one password per user for multiple services: great for the user, how do you give Elsevier all of your users' passwords (and do you want to?)

slide 35

The Competing Desires

- allow access to one community of users (the law school, a specific course) but not everyone else
- maintain user privacy
- allow finer granularity in statistics

slide 36

Tools and Techniques

Okay -- now that the problem has been layed out, how is it going to be solved?

slide 37

IP Address Recognition / Proxies / [resulting mess]

- Authentication (identification) and Authorization (all-of-none) rolled into one
- does anyone really want to keep doing this?

slide 38

LDAP

- *LDAP*: Lightweight Directory Access Protocol
- "simple" directory server
- objects and items with objects
- includes no authentication by itself, but authentication modules can be plugged in
- can be a source of authorization attributes

slide 39

PKI

- *PKI*: Public Key Infrastructure
- algorithmically based, one-way encryption scheme built into a metadata structure (X.509)
- very strong, very complicated, very "2009"
- does not preserve privacy

slide 40

Kerberos

- developed by MIT
- does authentication only

slide 41

Microsoft Active Directory (AD)

- Microsoft's "version" of Kerberos
- distributed authentication and authorization, if you play by Microsoft's rules

slide 42

Shibboleth

Provides consistent, distributed, federated, "simple" infrastructure for security, privacy and access to protected resources

- Enabling anonymous access (and thereby protecting personal privacy) by a member of the campus community to a licensed information resource available to "active members of the community."
- Ensuring anonymous access to a remote information resource where access is limited to "people associated with Course X at the origin site."
- Providing access to a restricted service using an attribute such as a person's name to determine authorization.

slide 43

It's Simple

See?

slide 44

Sources and Targets

"Authenticate Locally, Authorize Globally" *but don't tell anyone on the Shibboleth team that I said that*

- institutions (sources) provide authentication and attributes
- information providers (targets) provide authorization based on attributes
- institution, and soon the user, can control what attributes are released

slide 45

Attributes

- things known about a network identity
- "member of community"
- "employee in community"
- "student in the SAN151 class"
- "someone authorized to reach the Napster service"
- "ld83md84njfla73lsjjs9f77"
- "Peter Murray"

slide 46

Built On Trust

- targets trust that they are receiving requests from an authenticated user and are sent the appropriate attributes
- sources trust that targets will follow the contract specifications and not misuse the client attribute data

slide 47

Built Upon

- Open Source software implementation available from `http://shibboleth.internet2.edu/` for Apache and IIS
- web-based authentication scheme on the campus
- source of attributes for the user

slide 48

Other Emerging Solutions

- Microsoft .NET/Passport
- Liberty Aliance

The Quiz

slide 50

Put These Items In Chronological Order from Earliest To Most Recent

a) Amazon incorporated

b) BITNET dismantled

c) World Wide Web created

d) TCP/IP used for the first time

slide 51

The Correct Answers

d) TCP/IP used for the first time (1983)

c) World Wide Web created (1990)

a) Amazon incorporated (1994)

b) BITNET dismantled (1996)

Who Wants to be a Millionaire with Tom Sanville's Money?

slide 52

$100 -- One who uses programs to break into computers without understanding how they work is a:

a) ludite

b) script kiddie

c) tootie fruity

d) large software company in Washington state

slide 53

$250 -- Authentication is

a) a right or permission granted to an identity to access a system resource

b) gaining the right to use an identity

c) "my voice is my passcode, verify me"

d) unnecessary

slide 54

$500 -- Authorization is

a) gaining the right to use an identity

b) begging for signing authority so you can give yourself a raise

c) a right or permission granted to an identity to access a system resource

d) allowed only by secret intellegence courts

slide 55

$750 -- Which of these is not a valid Shibboleth2 attribute?

a) "member of community"

b) "community's pain-in-the-a**"

c) "student in class"

d) "1ak838kkf823820jjd7"

slide 56

$1,000 -- Identity management is

a) a good thing

b) a bad thing

c) a so-so, only if you are bored thing

d) essential to maintaining the proper alignment of the planets

slide 57

$5,000 -- Shibboleth is

a) a federated access management system

b) a flavor of ice cream

c) the name of an exciting new NBC sitcom starring Jerry Seinfeld

d) a neat word to say

slide 58

$10,000 -- US-CERT is

a) the only government-sanctioned breath mint

b) something that Ron Gilmore will tell us about this afternoon

c) the "U Suppose? Computers are an Extraordinary Research Tools Act" of 2004

d) a public-private partnership seeking to protect our national network infrastructure

slide 59

$25,000 -- Bugtraq is

a) the mess an insect makes on a car windshield at 55MPH

b) a mailing list dedicated to the open disclosure of security bugs

c) a species of bat

d) what my 2-year-old does when she sees an ant on the ground

slide 60

$50,000 -- DoS is

a) the Disk Operating System

b) a Denial of Service attack

c) the name of a grunge band

d) is it 12:15 yet?

slide 61

$100,000 -- A Packet Sniffer

a) locates unopened units of ketchup at a fast food chain

b) is someone with a serious cold and a pack of Kleenex(tm)

c) a rescue dog specializing in finding loose change

d) a program used to monitor traffic on a network

slide 62

$125,000 -- Running a Microsoft Operating Systems is bad only if

a) the rest of your colleagues are running things with a logo representing a half-eaten piece of fruit

b) one fails to install patches immediately

c) you don't own stock in Microsoft

d) you mean there are situations when it is not bad?

slide 63

$250,000 -- Social engineering is *not*:

a) a bunch of computer geeks getting together over pizza to write code

b) an attempt by some to collect knowledge to penetrate your systems

c) difficult to counteract in a naturally helpful profession

d) dangerous to the integrety of your systems

slide 64

$500,000 -- IP address recognition is a form of

a) authentication

b) authorization

c) neither

d) both

slide 65

$750,000 -- Bluesocket is a device that

a) an outdoor performance about an indian tribe

b) enables users from off campus to use an IP-restricted resource

c) authenticates and authorizes users to join a network

d) a network protocol that enables devices to talk to one another over a short distance

slide 66

$1,000,000 -- A firewall is

a) a network device that segments traffic

b) a network device that filters traffic

c) a network device that examines traffic for signs of inappropriate use

d) a network device that costs several thousand dollars, but is well worth it

e) all of the above

Appendix 1: Network Security Glossary

[With a strong focus on Authentication, Authorization, and Access Management]

Authentication (AuthN)

“Authentication is the process where a network user establishes a right to an identity -- in essence, the right to use a name.” (Lynch, 1998)

“Authentication is the process of establishing whether or not a real-world subject is who or what its identifier says it is. Identity can be proven by: Something you know, like a password; Something you have, as with smartcards, challenge-response mechanisms, or public-key certificates; Something you are, as with positive photo identification, fingerprints, and biometrics.” (*I2-Authentication*, 2004)

“The process of verifying an identity claimed by or for a system entity… An authentication process consists of two steps: 1. Identification step: Presenting an identifier to the security system. … 2. Verification step: Presenting or generating authentication information that corroborates the binding between the entity and the identifier.” (Shirey, 2000)

Authorization (AuthZ)

“Authorization is the process of determining whether an identity (plus a set of attributes associated with that identity) is permitted to perform some action, such as accessing a resource. Note that permission to perform an action does not guarantee that the action can be performed; for example, a common practice in cross-organizational licensing is to further limit access to a maximum number of concurrent users from among an authorized user community.” (Lynch, 1998)

“It will drive permissions for accessing networked resources, allow us to control and delegate electronic responsibilities, and serve as the basis for future administrative applications. It will allow us to convert our complex legal policies into automated systems in a easily scalable fashion.” (*I2-Authorization*, 2004)

“(1.) An "authorization" is a right or a permission that is granted to a system entity to access a system resource. (2.) An "authorization process" is a procedure for granting such rights. (3.) To "authorize" means to grant such a right or permission.” (Shirey, 2000)

Providing Access

Credentials: “Data that is transferred or presented to establish either a claimed identity or the authorizations of a system entity. (See: authentication information, capability, ticket.)” (Shirey, 2000)

Access Control: “Protection of system resources against unauthorized access; a process by which use of system resources is regulated according to a security policy and is permitted by only authorized entities (users, programs, processes, or other systems) according to that policy.” (Shirey, 2000)

Provisioning: "The process of managing attributes and accounts within the scope of a defined business process or interaction. Provisioning an account or service may involve the Creation, modification, deletion, suspension, restoration of a defined set of accounts or attributes." (Rolls, 2003)

Attributes: "A distinct characteristic of an object. An object's attributes are said to describe the object. Objects' attributes are often specified in terms of their physical traits, such as size, shape, weight, and color, etc., for real-world objects. Objects in cyberspace might have attributes describing size, type of encoding, network address, etc. Which attributes of an object are salient is decided by the beholder." (Rolls, 2003)

Roles

Those who seek information

Licensee institution: "organizations such as universities or public libraries that arrange for access to resources on behalf of their user communities" (Lynch, 1998)

Origin: "a site with administrative authority over users who access resources at remote providers" (Cantor, and Erdos, 2002, Section 2.2.1)

End user: "*General usage:* A system entity, usually a human individual, that makes use of system resources, primarily for application purposes as opposed to system management purposes." (Shirey, 2000)

Client: "A program that establishes connections for the purpose of sending requests."(Fielding, Gettys, Mogul, Nielsen, Masinter, Leach, and Berners-Lee, 1999)

Those who provide information

Resource operator: "publishers, web site operators, and other content providers (including libraries and universities in their roles as providers of content)" (Lynch, 1998)

Target: "An entity, or collection of entities, which is affected by a policy. For example, the "targets" of a policy to reconfigure a network device are the individual services that are updated and configured." (Westerinen, 2001)

Server: "An application program that accepts connections in order to service requests by sending back responses."(Fielding *et al.*, 1999)

Origin server: "The server on which a given resource resides or is to be created." (Fielding *et al.*, 1999)

Those in the middle

Proxy: "An intermediary program which acts as both a server and a client for the purpose of making requests on behalf of other clients. Requests are serviced internally or by passing them on, with possible translation, to other servers. A proxy MUST implement both the client and server requirements of this specification. …" (Fielding *et al.*, 1999)

Surrogate: "A gateway co-located with an origin server, or at a different point in the network, delegated the authority to operate on behalf of, and typically working in close co-operation with, one or more origin servers. Responses are typically delivered from an internal cache." (Cooper, Melve, and Tomlinson, 2001)

Firewall: "A system designed to prevent unauthorized access to or from a private network…. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria. There are several types of firewall techniques: Packet filter…, Application gateway…, Circuit-level gateway…, and Proxy server…." (*firewall*, 2003)

Privacy and Anonymity

Privacy: "The right of an entity (normally a person), acting in its own behalf, to determine the degree to which it will interact with its environment, including the degree to which the entity is willing to share information about itself with others. (See: anonymity.)" (Shirey, 2000)

Anonymous: "The condition of having a name that is unknown or concealed." (Shirey, 2000)

When Things Go Wrong

[Distributed] Denial of Service (DDoS/DoS) Attack: "…a type of attack on a network that is designed to bring the network to its knees by flooding it with useless traffic. Many DoS attacks, such as the Ping of Death and Teardrop attacks, exploit limitations in the TCP/IP protocols. For all known DoS attacks, there are software fixes that system administrators can install to limit the damage caused by the attacks. But, like viruses, new DoS attacks are constantly being dreamed up by hackers." (*DoS attack*, 2002)

E-mail Spoofing: "Forging an e-mail header to make it appear as if it came from somewhere or someone other than the actual source. The main protocol that is used when sending e-mail -- SMTP -- does not include a way to authenticate. There is an SMTP service extension (RFC 2554) that allows an SMTP client to negotiate a security level with a mail server. But if this precaution is not taken anyone with the know-how can connect to the server and use it to send spoofed messages by altering the header information." (*e-mail spoofing*, 2003)

Packet Sniffer: "A program and/or device that monitors data traveling over a network. Sniffers can be used both for legitimate network management functions and for stealing information off a network. Unauthorized sniffers can be extremely dangerous to a network's security because they are virtually impossible to detect and can be inserted almost anywhere. This makes them a favorite weapon in the hacker's arsenal. On TCP/IP networks, where they sniff packets, they're often called packet sniffers." (*sniffer*, 2004)

Port Scan: "The act of systematically scanning a computer's ports [in … networks, an endpoint to a logical connection]. Since a port is a place where information goes into and out of a computer, port scanning identifies open doors to a computer. Port scanning has legitimate uses in managing networks, but port scanning also can be malicious in nature if someone is looking for a weakened access point to break into your computer." (*port scanning*, 2004)

Script Kiddie: "A person, normally someone who is not technologically sophisticated, who randomly seeks out a specific weakness over the Internet in order to gain root access to a system without really understanding what it is s/he is exploiting because the weakness was discovered by someone else. A script kiddie is not looking to target specific information or a specific company but rather uses knowledge of a vulnerability to scan the entire Internet for a victim that possesses that vulnerability." (*script kiddie*, 2002)

Social Engineering: "…cracking techniques that rely on weaknesses in [human behavior] rather than software; the aim is to trick people into revealing passwords or other information that compromises a target system's security. Classic scams include phoning up a mark who has the required information and posing as a field service tech or a fellow employee with an urgent access problem." (*Social Engineering*, 2004)

Techniques

Network Address Translation (NAT): "…an Internet standard that enables a local-area network (LAN) to use one set of IP addresses for internal traffic and a second set of addresses for external traffic. A NAT box located where the LAN meets the Internet makes all necessary IP address translations." (*NAT*, 2002)

Packet Filtering: "Also referred to as *static* packet filtering. Controlling access to a network by analyzing the incoming and outgoing packets and letting them pass or halting them based on the IP addresses of the source and destination. Packet filtering is one technique, among many, for implementing security firewalls." (2001)

Resources Consulted

(2001) *packet filtering*. internet.com, Jun 21 2001. Accessed May 1 2004. Available from http://www.webopedia.com/TERM/P/packet_filtering.html.

(2002) *DoS attack*. internet.com, Oct 21 2002. Accessed May 2 2004. Available from http://www.webopedia.com/TERM/D/DoS_attack.html.

(2002) *script kiddie*. internet.com, Oct 21 2002. Accessed May 1 2004. Available from http://www.webopedia.com/TERM/S/script_kiddie.html.

(2002) *NAT*. internet.com, Jan 10 2002. Accessed May 1 2004. Available from http://www.webopedia.com/TERM/N/NAT.html.

(2003) *e-mail spoofing*. internet.com, Dec 11 2003. Accessed May 1 2004. Available from http://www.webopedia.com/TERM/E/e_mail_spoofing.html.

(2003) *firewall*. internet.com, Jul 24 2003. Accessed May 1 2004. Available from http://www.webopedia.com/TERM/F/firewall.html.

(2004) *Core Middleware -- Authentication*. Internet 2, Feb 26 2004. Accessed Mar 24 2004. Available from http://middleware.internet2.edu/core/authentication.html.

(2004) *Core Middleware -- Authorization*. Internet 2, 2004. Accessed Mar 24 2004. Available from http://middleware.internet2.edu/core/authorization.html.

(2004) *sniffer*. internet.com, Apr 14 2004. Accessed May 1 2004. Available from http://www.webopedia.com/TERM/s/sniffer.html.

(2004) *port scanning*. internet.com, Apr 22 2004. Accessed May 1 2004. Available from http://www.webopedia.com/TERM/p/port_scanning.html.

(2004) *Social Engineering*. hyperdictionary.com, 2004. Accessed May 1 2004. Available from http://www.hyperdictionary.com/computing/social+engineering.

Cantor, S., and Erdos, M. (2002) *Shibboleth Architecture*. v5. Internet 2, May 2 2002. Accessed April 1 2004. Available from http://shibboleth.internet2.edu/draft-internet2-shibboleth-arch-v05.html.

Cooper, I., Melve, I., and Tomlinson, G. (2001). *Internet Web Replication and Caching Taxonomy* (Report Number RFC3040). The Internet Society.

Fielding, R. T., Gettys, J., Mogul, J. C., Nielsen, H. F., Masinter, L., Leach, P. J., and Berners-Lee, T. (1999). *Hypertext Transfer Protocol -- HTTP/1.1* (Report Number RFC2616). The Internet Society.

Lynch, C. (1998). *A White Paper on Authentication and Access Management Issues in Cross-organizational Use of Networked Information Resources*. Coalition for Networked Information, Washington, DC.

Rolls, D. (2003). *Service Provisioning Markup Language (SPML) Version 1.0* (Report Number cs-pstc-spml-core-1.0.doc). OASIS.

Shirey, R. (2000). *Internet Security Glossary* (Report Number RFC2828). The Internet Society.

Westerinen, A. S., John; Strassner, John; Scherling, Mark; Quinn, Bob; Perry, Jay; Herzog, Shai; Huynh, An-Ni; Carlson, Mark; Waldbusser, Steve. (2001). *Terminology for Policy-Based Management* (Report Number RFC3198). The Internet Society.

Appendix 2: Bibliography

The 60 minute network security guide: First steps towards a secure network environment. 2002. Ft. Mead, MD: National Security Agency, sd-7. Available from **http://nsa2.www.conxion.com/support/guides/sd-7.pdf**.

Produced by the Systems and Network Attack Center (SNAC) of the U.S. National Security agency, this document summarizes actions that can be made to secure network systems. It is not specific to particular operating systems, but rather outlines general strategies and tasks that should be employed to secure systems.

Principles to guide efforts to improve computer and network security for higher education. 2003. EDUCAUSE/Internet2 Computer and Network Security Task Force, SEC0310. Available from **http://www.educause.edu/asp/doclib/abstract.asp?ID=SEC0310**.

The EDUCAUSE/Internet2 Computer and Network Security Task Force held an invitational, NSF-sponsored workshop at Columbia University in August 2002. Based on research into principles articulated by a variety of academic groups and statements by invited experts, the group proposed that higher education's efforts to improve computer and network security be guided by a set of six principles: civility and community; academic and intellectual freedom; privacy and confidentiality; equity, diversity, and access; fairness and process; ethics, integrity, and responsibility. The authors recognize that these principles are broad; each institution must ultimately determine the principles that are most relevant and valued by its own community. This set of principles is intended to serve as a starting point for campus discussions about computer and network security. The higher education community is invited to provide suggestions and changes to this document. [Supplied by author.]

Computer access, privacy, and security: Legal obligations and liabilities. 2003. EDUCAUSE. Accessed April 2 2004. Available from **http://www.educause.edu/asp/doclib/abstract.asp?ID=SEC0311**.

This presentation was provided at the NACUA Continuing Legal Education Workshop "Computers on Campus: Privacy, Security, Intellectual Property and the Internet" to describe statutory obligations, developing case law, and sample computer use policies and procedures related to computer access, privacy, and security. [Supplied by author.]

Information and computer security resources. 2004. SANS: SysAdmin, Audit, Network, Security Institute. Accessed April 7 2004. Available from **http://www.sans.org/resources/**.

SANS is widely known for its efforts in promoting and training staff on network security. It makes freely available research documents, guides, and tools for securing networks ranging from homes to global organizations. The resource center provides items such as the SANS News Browser Service, a guide to popular resources on security, the SANS/FBI Top 20

Vulnerabilities List, sample policy statements, glossaries of terms, links to free vendor white papers, and answers to many frequently asked questions.

Security resources. 2004. EDUCAUSE. Accessed April 1 2004. Available from **http://www.educause.edu/security/resources.asp**.

The Computer and Network Security Web site, developed by the EDUCAUSE/Internet2 Computer and Network Security Task Force, is intended to be a focal point of information and resources on computer and network security for the higher education community. This list of resources provides guidance, reference material, and example policies and practices for network security in the higher education environment. [Adapted from source]

[Shibboleth Introduction]. March 2004. Internet 2 Middleware Architecture Committee for Education. Accessed April 7 2004. Available from **http://shibboleth.internet2.edu/docs/shibboleth_intro.pdf**.

This two-page brochure describes the Shibboleth project and includes examples for its use and pointers to additional information.

Banerjee, Kyle. 2003. How much security does your library need? *Computers in Libraries* 23, no. 5: 12-17.

Banerjee discusses the importance of security systems in libraries. One can protect library systems quite effectively by developing good computing practices, learning the basic knowledge of library systems and employing tools like firewalls, antivirus software, and alarms. [Adapted from ABI/Inform]

Beamsley, Teresa Grose. 1999. Securing digital image assets in museums and libraries: A risk management approach. *Library Trends* 48, no. 2: 359-378.

There is an obvious need for ongoing research, evaluation, and planning if museums and archives are committed to protecting their digital image assets. A number of potential threats to the integrity of digital image information can be identified when standard practices in museums and archives are examined. Changes in the integrity of digital image information can be caused by the manner in which the source data are acquired and recorded and by modifications made to the image data file. Alterations made to contextual data can limit valid interpretation of the associated surrogate image. The destruction of the mechanisms that link contextual data to the appropriate digital image has the same effect as deleting contextual information. Loss of control over digital assets can be the result of failure or inability to establish and publicize copyright. Even if copyright is established and enforceable, failure to enforce rights has the same effect as having no rights at all. Finally, failure to detect corruption of digital information means that invalid, partial, or inappropriate information will be spread under the guise of authentic reliable information. Some institutions are already proactively applying security measures to digital image collections. Some of these security measures can have a negative impact on the integrity of the files that they are designed to protect. Systematic consideration of risk factors can inform the creation of procedures and application of se-

curity that works to guarantee the reliability and accuracy of digital image assets. [Supplied by author]

Becker, Phil. Aug. 5 2002. *Shibboleth: Identity the internet way*. Digital Identity World. Accessed April 1 2004. Available from **http://www.digitalidworld.com/article.php?id=90**.

The Internet's architectural design was not the result of any commercial efforts. Rather it was originally designed and built in research facilities and Universities. Only in the early 1990's did it gain commercial acceptance and commercial development. So it seems reasonable to ask what the research arena is doing about Digital Identity. The Internet2/Shiboleth project is their identity architecture project, and Digital ID World recently sat down with Shibboleth project leader Steve Carmody to learn more about it. [Supplied by author]

Cain, Mark. 2003. Cybertheft, network security, and the library without walls. *The Journal of Academic Librarianship* 29, no. 4: 245-248.

The author describes the security issues with proxy servers and remote user authentication, using the example of late-2002 theft of materials from JSTOR using open proxy servers on subscriber's networks.

Driscoll, Lori. 2003. *Library public access workstation authentication*. Washington, D.C.: Association of Research Libraries Office of Leadership and Management Services, ISBN: 159407609X Series ISSN: 0160-3582.

In reaction to the events of September 11, 2001, as well as several widely reported misuses of campus computer networks, computer systems administrators have re-examined network access policies. While systems administrators have moved to restrict access to information assets, librarians have worked to support barrier-free access that protects users' privacy. This survey was distributed to the 124 ARL member libraries in May 2003 to gather data on how users at public access workstations are authenticated; what is driving IT policy changes in libraries; who is involved in policy decision making; how access controls have affected services; how, with tighter campus IT security, Federal Depository libraries are meeting the information needs of the public; and other questions. [Supplied by ARL]

Ekhaml, Leticia. 2001. Protecting yourself from internet risks, threats, and crime. *Journal of Educational Media and Library Sciences* 39, no. 1: 8-14.

While the Internet poses some threats to people through potential infringement of individual's rights and invasion of privacy, certain steps can be taken by librarians, teachers, media specialists and instructional technologists to protect their users from these threats. Describes some of the ways in which these protective measures can be provided. These include watching out for people scavenging through discarded materials, software for ensuring that deleted files on floppy disks are truly erased, protecting against 'tailgating', 'spamming' and 'cloaking', preventing electronic mail addresses from becoming public knowledge, using random password generators to protect against guesswork, and the use of virus checkers to cope with the dangers of computer viruses (particularly those sent as electronic mail attachments). [Supplied by Author]

Goodwin, Bill. 2004. Companies are at risk from staff ignorance. *Computer Weekly*: 14.
Martin Smith, director of the Security Company, said, "One of the quickest and easiest ways to improve security is to raise awareness. About 80% of the organisations I speak to are doing nothing. And of the 20% that are, it is rarely adequate." [Supplied by author]

Kanabar, Dina and Vijay Kanabar. 2003. A quick guide to basic network security terms. *Computers in Libraries* 23, no. 5: 24-25.
A handy guide encapsulating the basic network security terms is presented. The list details the ways on how to protect Web servers from attackers, the different types of attacks and the risks involved in such an attack. [Supplied by author]

Robiette, Alan. 2001. Managing access to electronic information: Progress and prospects. *Serials* 14, no. 3: 301-304.
Based on a paper given at the UKSG 24th Annual Conference, April 2001 at Heriot-Watt University, Edinburgh, Scotland. Considers the various ways used to manage access to electronic information, especially for large user populations, including IP address validation and username/password methods, stressing the value of the Athens system developed for the UK academic community. Discusses the new generation of access management projects (including Shibboleth, PAPI, Akenti and Sparta), that are beginning to emerge and considers how these are likely to influence the design of access management regimes in the near future. [Supplied by author]

Williams, Robert L. 2001. *Computer and network security in small libraries: A guide for planning*. Texas State Library & Archives Commission. Accessed Apr 5 2004. Available from **http://www.tsl.state.tx.us/ld/pubs/compsecurity/**.
In a two part format, the author introduces the needs and terminology surrounding network security and then provides guidance on implementing network security in a small library environment.