

Open Source Security Tools for Information Technology Professionals

School of Professional Studies (SPS)

The City University of New York (CUNY)

Aron Trauring
Adjunct Professor
CEO, Zoteca

Class 2 September 19th, 2005

Class Agenda

6:30-6:45 Article of the Week

6:45-7:45 Introduction to Internet

7:45-8:00 Break

8:00-8:30 Network Lab

8:30-9:30 Introduction to Information Security (Presentation)

Instructor

Aron Trauring – Adjunct Professor, CUNY SPS / CEO, Zoteca

Email: atrauring@zoteca.com

Personal Website: <http://aronst.org/>

Zoteca Corporate Website: <http://www.zoteca.com/>

FOSS Resources: <http://www.fourm.info/>

Introduction to Internet Infrastructure

Historical Background

Stage 1 — Ideas from MIT

- 1961 — Leonard Kleinrock — Packet Switching Theory
- 1962 — J.C.R. Licklider — “Galactic Network”
- 1965 — Lawrence Roberts & Thomas Merrill – first WAN over a phone line

Stage 2 — Defense Advanced Research Project Agency (DARPA)

- 1967 – Roberts — Paper proposing the ARPANET
- 1969 — Bob Kahn — Bolt Beranek and Newman get contract to build ARPANET
- 1969 — Kleinrock (now at UCLA) — First node
- 1969 — Engelbart at Stanford — Second node
- 1969 — First RFC — Request for Comment — standard way to propose and discuss network protocols
- Work proceeds on protocols and applications

Stage 3 — Growth of ARPANET

- 1972 — First public demonstration
- 1972 — Email introduced
- Email pushes the growth of the network

Stage 4 — The Internet is Conceived

- Open-architecture network — individual networks may be separately designed and developed
- Each network can be designed in accordance with the specific environment and user requirements of that network
- No constraints on the types of network that can be included or on their geographic scope,
- ARPANET formed first network in the Internet
- 1972 — Kahn (now at DARPA) decides to develop a new protocol for this open-architecture inter-networking

Four Principles of the Internet Protocol

1. Each distinct network would have to stand on its own and no internal changes could be required to any such network to connect it to the Internet
2. Communications would be on a best effort basis. If a packet didn't make it to the final destination, it would shortly be retransmitted from the source.
3. Black boxes would be used to connect the networks; these would later be called gateways and routers. There would be no information retained by the gateways about the individual flows of packets passing through them, thereby keeping them simple and avoiding complicated adaptation and recovery from various failure modes.
4. There would be no global control at the operations level.

Stage 5 — The Internet is Born

- 1973 — Kahn and Vincent Cerf (Stanford) develop TCP/IP
- 1974 — Three independent implementations of TCP that could inter-operate
- The Internet is not designed for just one application, but as a general infrastructure on which new applications could be conceived
- The general purpose nature of the service provided by TCP and IP that makes this possible.

Stage 6 — New Technologies Spreads Internet

- 1973 — Metcalfe Ethernet — spread of LAN and many more nodes
- 1975 — 100 nodes in the ARPANET (mostly DEC 10/20 (timesharing computers) in academic research CS departments
- mid-1970s — Low cost DEC VAX helps add many more nodes
- late '70s early '80s — ARPA funds integration of TCP/IP in Berkeley Unix
- VAX/BSD Unix leads to more rapid spread of TCP/IP to universities around the world
- 1980 — TCP/IP becomes a DOD standard
- 1983 — ARPANET fully converted to TCP/IP
- 1983 — Paul Mockapetris/ Jon Postel (USC) — invent Domain Name Server (DNS)

Stage 7 — Transition to Widespread Infrastructure

- in mid-70s alternative closed networks developed
- USENET — AT&T Unix uucp protocol
- CSNET — NSF funded network for computer scientists
- Various other government funded networks
- Commercial networks — IBM SNA, Xerox XNS, DECNet
- 1985 — NSF requires universities to open up networks to receive grants

- 1985 — NSF joins Internet Activities Board to ensure interoperability with ARPANET
- 1985 — DOE, NSF and NASA form co-ordinating committee to share networking infrastructure
- 1988 — NFS paper Al Gore read

Stage 8 — Commercial Infrastructure Begins

- NSF Acceptable Use Policy — NSF “Backbone” for Research and Academic use only
- Late Eighties — NFS encourages Commercial Backbones — PSI, UUNET, ANS
- 1988-1995 — \$200 million in NFS funding
- 1990 — ARPANET de-commissioned
- TCP/IP had supplanted or marginalized most other wide-area computer network protocols world-wide

Stage 9 — World Wide Web — Precedents

- 1960s — Doug Engelbart prototypes an "oNLine System" (NLS) which does hypertext browsing editing, email, and so on.
- 1965 — Ted Nelson coins the word Hypertext in *A File Structure for the Complex, the Changing, and the Indeterminate*
- 1967 — Andy van Dam and others build the Hypertext Editing System and FRESS
- 1969 — Piers Anthony *Macroscope* — surfing the web for information as a job!
- 1980 — Tim Berners-Lee — proposes a hypertext system of arbitrary nodes

Stage 10 — The WWW is Invented

- Applications: Email, File Transfer Protocol, News, Mailing Lists, Gopher
- New collaboration tool for researchers needed in high energy physics
- 1989 — hypertext proposal from Tim Berners-Lee at Conseil Européenne pour la Recherche Nucléaire (CERN)
- Extension of Gopher and inspired by Ted Nelson *Xanadu*
- 1990 — TBL – First hypertext browser named WorldWideWeb
- 1991 — All components working and running at CERN
- 1992 — 50 web servers around the world and several browsers
- 1993 — National Center for Supercomputing Applications (NCSA) develops MOSAIC
- 1994 — Marc Anderseen “steals” MOSAIC code and forms Netscape
- 1994 — Tim Bernays-Lee founds the W3C — WWW Consortium

Stage 11 — The Internet as the Infrastructure of Society

- Billions spent in Dot-Com era make Internet mainstream in commercial world
- 10% of Xmas sales now take place on Internet
- Over 56 million websites tracked by Netcraft
- 508 million people worldwide online (65% non-English speaking) — Gload Stats <http://www.gloadstats.com/globstats/>
- 313 billion web pages
- Tens of billions of emails sent every day

Underlying Architecture

Managing Organizations

- No one runs the Internet — Open architecture of distributed networks
- Internet Society (ISOC) — private non-profit group ISOC <http://www.isoc.org/>
- 50 organization and 16,000 individual members in over 180 countries
- Internet Architecture Board (IAB) — infrastructure issues
- Internet Engineering Task Force (IETF) — TCP/IP protocol
- Internet Assigned Number Authority (IANA) — IP Numbers overall
- Regional Internet Registries (RIRs) — AfriNIC, ARIN, LACNIC, APNIC, RIPE NCC,
- World Wide Web Consortium (W3C) — industry consortium run by MIT — web standards
- Internet Corporation For Assigned Names and Numbers (ICANN) — managing and co-ordinating DNS

Commercial Organizations

- Internet Service Providers (ISP) — sell connection to Internet to individuals and companies
- Regional Networks — provide and maintain Internet access within a geographic region
- Registrars — register domain names

Four Layers of the TCP/IP Protocol “Stack”

1. Network Interface
2. Internet Protocol
3. Transport
4. Application

Network Interface

- Physical Layer
- Physical unique address for each device
- Different transmission speeds and protocols

Basic Network Components for a LAN

- Individual device connection — NIC, 801.11x device, modem
- Physical cable or wireless base station
- Hubs
- Switch

Types of Physical Transport in LAN

- Ethernet
- 801.11x
- Bluetooth
- Fiber
- Token Ring

Types of Physical Transport in WAN

- Dial up
- Ethernet
- DSL
- Cable
- GPRS
- G3
- Satellite
- T1
- T3
- Fiber

Internet Protocol

- Logical address — no IP, no network communication
- IPv4 — 32 bits long: four octets of eight bits each — 4,294,967,296 addresses.
- Structured — A,B,C Networks
- Network — 192.168.1.0 (Subnet Mask 255.255.255.0)
- Individual computer — 192.168.1.45
- IPv6 — 128 bits — Structured (64 bits = physical layer address)

Basic IP Routing

- Routers — move traffic from one part of network to another (standardize on IP address)
- Bridge — links LANs
- Repeaters — boosts signals
- Gateway — links LANs to mid-level networks, or between larger networks
- Mid-level networks — WAN (one organization), ISP, regional networks
- NAP — Network Access Point — link to main backbones (155 megabits/second)
- Internet2 Backbones — 9.6 billion bits/second

IP Network Class

- A — 1-126 — supports 16 million hosts on each of 126 networks
- B — 128-191 — supports 65,000 hosts on each of 16,000 networks
- C — 192-223 — supports 254 hosts on each of 2 million networks
- D — 224-247 (Multicasting)
- E — 248-254 (Experimental)

Private (Inside) IP Networks

- A —10.0.0.0 through 10.255.255.255
- B —172.16.0.0 through 172.31.0.0
- C —192.168.0.0 through 192.168.255.0

IP Addresses

- 127.0.0.1 — “me, myself” — never leaves computer
- 192.168.1.124 — private (inside) network
- 64.110.168.5 — public (outside) address

Classless Inter-Domain Routing (CIDR)

- A replacement for the old process of assigning Class A, B and C addresses with a generalized network "prefix".
- Old system: network identifiers (or "prefixes") of 8, 16 or 24 bits
- CIDR: prefixes anywhere from 13 to 27 bits
- Blocks of addresses can be assigned to networks as small as 32 hosts or to those with over 500,000 hosts
- 32-bit IP address plus how many bits are used for the network prefix. For example, in the
- CIDR address 206.13.01.48/25 — first 25 bits identify the unique network; remaining bits identify the specific host (128 hosts)

Other Important IP Protocols

- NAT — Network Address Translation
- DHCP — Dynamic assignment of IP

Domain Names

- DNS — mapping between IP number and name
- TLD — Top Level Domains
- Zones
- Arbitrary number of sub-levels

Transport

- Moving Packets
- Data broken up into parts which include data and "headers"
- Routers move data from client to server and back
- Look at headers and determine most efficient route
- Sometime stay within own network
- Otherwise move through a gateway
- Reassembled at other end
- TCP — with acknowledgment
- UDP — where speed is more important

Application

- IP address + Port
- Each application has its own standard port
- Web — 80
- SSH — 22
- SMTP — 25
- Client-Server Model

Core Applications

Email

- First and most heaviest use application
- Email client for sending and receiving — Outlook, Thunderbird, Evolution, Kontact
- Data broken up into packets and sent to server
- Attachments encoded – MIME
- Sent to destination via Mail Transport Authority (MTA) server
- Received by Local Delivery Agent (LDA)
- Accessed by POP or IMAP or proprietary server

SMTP — Simple Mail Transport Protocol

- Client opens up conversation with SMTP server
- HELO
- My address
- Destination address
- Data — “Headers” + text
- End with “.”
- Next address
- QUIT
- Play with SMTP <http://email.about.com/library/misc/blspamlet.htm>

Open Source SMTP Servers

- Sendmail
- Postfix
- Exim
- Qmail
- Courier

Routing Mail

- Using destination and DNS mail is sent from MTA to MTA via SMTP
- Gateway routes it internally
- MTA hands it off to an LDA

Local Destination Authority

- Mbox format
- Maildir folder/file format
- Proprietary formats
- Procmail most widely used open source LDA
- Courier Maildrop (Maildir format)
- Who are valid email users
- Can create filters and rules

SPAM

- Headers are meaningless and can be spoofed
- Email addresses are easily harvested
- SMTP is trivial protocol
- Add it all up and you got SPAM
- Name derives from Monty Python skit

Blocking SPAM

- Don't ever respond to removal requests
- Spam filters
- ESMTP — require authentication
- POP before SMTP
- Reverse address lookup

Mail Download

- POP3 — Post Office Protocol Version 3 (download to client)
- IMAP — Internet Message Access Protocol Version 4 (mail sits on server)
- Fetchmail — downloads email from another server and deliver to a local mailbox on your system
- Proprietary

Email Servers

- PostFix
- Courier (IMAP as well)
- Exchange
- Groupwise
- Lotus

Email Lists

- Listserve
- Mailman

Newsgroups

- Open discussion bulletin boards
- News feeds optionally carried
- groupname.subgroup...
- Yahoo/Google/MSN Groups — membership forums

File Transfer Protocol

- Highly insecure
- Secure FTP
- Secure Copy
- WebDAV
- BitTorrent

Chat

- IRC
- Instant Messaging

Remote Connection

- Telnet
- SSH
- VNC

Network Lab

ifconfig

- network setup
- MAC address
- IP Address
- Network Address
- ipconfig in Windows

ping

- **I**nternet **C**ontrol **M**essage **P**rotocol (**ICMP**) - Layer 1
- Ping - Packet Internet Groper
- ICMP echo request and echo reply
- Tests: packet dropping, latency, DNS
- ping -f — flood
- ping -n — no dns
- ping -s [packet size] — large packets used in Denial Of Service

tracert

- Pings host with loop 1 to n ping TTL n
- Get information about where servers are physically located and ISP
- tracert in Windows

dig

- DNS lookup
- dig -x — reverse lookup
- dig [domain name] AXFR — domain transfer

whois

- Contact information for website from registrars
- When want to contact about some security problem
- keep information limited in your own whois

finger

- individual information
- usually not available

ps

- Shows processes running on a system
- Check if something is running that shouldn't be
- ps A — all user processes
- ps -aux — with username
- ps -aux | grep [searchterm] — search for a particular program

Sam Spade

- Windows equivalent of the basic Unix network tools

Introduction to Information Security

Vulnerability

- Software, hardware or procedural weakness
- Absence or weakness of a resource that can be exploited
- Examples: buggy service, open port, lax physical security

Threat

- Any potential danger
- Threat agent — that or whom carries out (exploits) threat
- Refers to the potential for exploiting the vulnerability
- Examples: intruder coming in through open port, Hurricane Katrina, employee error

Risk

- Likelihood of a threat agent exploiting a vulnerability
- Loss potential or probability
- More vulnerabilities increase risk

Exposure

- being open to potential losses from a threat agent exploiting a vulnerability
- Possible data stolen through break-in
- Down-time due to facility damage

Safeguard (Countermeasure)

- Software configuration, hardware or procedure that eliminates or reduces risk
- Examples: Strong password management, Anti-virus software, Employee training

The CIA Triad

- Confidentiality
- Integrity
- Availability

Confidentiality — Definition

- Prevention of unauthorized disclosure
- Data on the internal network
- Transmitted data
- Data at destination

Confidentiality — Vulnerabilities

- Network monitoring
- Shoulder surfing
- Stealing passwords
- Social engineering

Confidentiality — Countermeasures

- Encryption
- Network traffic padding
- Strict access control
- Employee training

Integrity — Definition

- Assurance of accuracy and reliability
- Prevention of unauthorized modification

Integrity — Vulnerabilities

- Virus
- Logic Bomb
- Back door
- Integrity — Techniques
- User error — accidental or malicious

Integrity — Countermeasures

- Strict access control
- Intrusion detection
- Encryption
- Restricted access
- Application checking
- Database rules

Availability — Definition

- Reliable and timely access to data and resources
- Predictable and acceptable level of performance
- Secure and quick recovery from failures

Availability — Vulnerabilities

- Device or software failure
- Environmental issues
- Denial of Service (DoS) attacks

Availability — Countermeasures

- Avoid single points of failure
- Backup and redundancy devices
- Data backups
- Intrusion detection

Organizational Security Model

- Framework for achieving CIA
- Technical and non-technical components
- Analyze risks and develop effective counter-measures

Security Goals

- Operational (daily) goals — productivity and task-oriented activities
- Examples: backup procedures, firewall rules
- Tactical goals — longer term
- Examples: network-based authentication, email-based anti-virus
- Strategic goals - longest term
- Examples: corporate VPN, off-site backup facilities
- One level depends upon the other
- Organizational requirements and risk assessment determine goals and objectives

Organizational requirements

- Function of type of organization
- Function of size
- Private business deals with customer satisfaction and competition
- Non-profit and government - serving the community
- Military and police provide community security
- Security must serve organizational requirements — not the reverse!!!

Risk Management

- Identify
- Assess
- Reduce

Risk Identification — Vulnerabilities

- Physical damage
- Equipment malfunction
- Application error
- Human error
- Misuse of data
- Inside and outside attacks

Risk Identification — Threats

- Malware — virus, auto-rooters, trojan-horse
- Vandals — script kiddies
- Crackers — malicious or for hire
- Users — employees, contractors
- Environment — fire, weather, theft
- Commercial software

Risk Assessment — Definition

- Cost/Benefit analysis
- Probability of exposure
- Dollar value of damage
- Quantitative techniques

Risk Assessment - Major Types of Exposure

- Lost data
- Stolen data
- Data tampering
- Breach of confidentiality
- Downtime

Risk Assessment — Major Cost Types

- Embarrassment — e.g. embarrassing employee emails or vandalized website
- Productivity losses — e.g. lost data, network downtime
- Lost customers — e.g. website down, go elsewhere
- Competitive risk — e.g. trade secrets revealed
- Business liability — e.g. lawsuit from stolen customer database
- Regulatory liability — e.g. HIPAA
- Countermeasures

Safeguards in the Security Model

- Policies
- Standards
- Guidelines
- Procedures

Policies

- Security program goals
- Assignment of responsibility
- Cost/benefits laid out
- Outlines enforcement
- Strategic

Standards

- Compulsory rules
- Examples: wear company badge, IT facility locked and monitored at all times
- Baseline – minimum level of security required
- Standards are developed to meet the baseline
- Government standards exist as well

Guidelines

- Recommended actions and operational guides
- Addresses grey areas of policies
- Policy: access to confidential data must be audited
- Guideline: audits should contain sufficient information to compare with prior reports

Procedures

- Detailed step-by-step actions to achieve a certain task
- Can apply to users or IT staff
- Spell out how policies, standards and guidelines are actually implemented in the operating environment
- Policy: users who access confidential data must be authenticated
- Procedure: How authentication takes place

Safeguards — Major Types

- Accountability Controls — e.g. audit logs, audit automation
- Physical and environmental controls
- Administration controls — e.g. background checks, supervision
- Access controls — e.g. authentication, biometrics
- Cryptography
- Business continuity planning — e.g. backups, off-site facilities
- Computer operations — e.g. which OS, how configured, securing workstations
- Incident handling — e.g. reporting and correction

Basic Security Tenets

- Minimalism
- Defense in Depth
- Vigilance

Minimalism (KISS)

- Safest way to avoid risk is not to introduce it in first place
- Only install what you need
- Only run what you need
- Do not have users you don't need
- Change control system or journal changes

Defense in Depth

- Multi-layered approach to defense
- Example: external firewall, host firewall, IDS, regular penetration testing

Vigilance

- Bit-rot — situation deteriorates if you do nothing
- System changes and threats change
- Check logs, audit users and groups, monitor files
- Keep patches up-to-date
- Test constantly
- Keep on your reading

Summary

- Security is expensive and time-consuming
- Constantly measure risk vs. reward
- Tools are needed both for testing and safeguarding
- FOSS lowers the costs of tools