

LIS 385T.6 - 1.24.00

Information and Network Security

Issues & Questions

- Listserv set up - infosec-spr02@lists.cc.utexas.edu
- Class Roster – Who's here and who's not...
- Topic Paper #1 – See last slide

Introduction to NetSec - Discussion

- Where are we vulnerable? In what ways?
- What is our personal responsibility for security/privacy?
- What does the history of the Internet tell us about security and Internet technologies?
- Is digital rights management or privacy a security issue?
- How has 9/11 changed the security landscape?

Introduction to NetSec

- The 80/20 problem
- Ubiquitous vulnerability and distributed cataloguing
- Netscape SSL vulnerability/IIS-Code Red
- Proactive vs. Reactive models, tools, services
- No 100% solutions
- Standards – project idea?
- History of the Net – insights
 - Unix
 - synchronicity

Introduction to NetSec

- Information Level vs. Technical Level attacks
 - Social Engineering
 - Hoaxes
- Systems
- Automation in offense and defense
- Types of Attacks and Crimes
- Structured vs. unstructured threats – external vs. internal
- CIA Model and audit/testing

Supplemental Reading

- www.attrition.org
- www.securityfocus.com (hosts bugtraq)
- www.gocsi.com (Computer Security Institute)
- <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>
(Cybercrime Convention)
- <http://www.consumer.gov/idtheft/> (USG ID Theft site)
- <http://www.fas.org/irp/program/process/echelon.htm> (Echelon)
- <http://www.nipc.gov/> (National Infrastructure Protection Center)

TCP/IP Overview

- OSI Model and TCP/IP stack – why a model?
- <http://www.saintrochtree.com/network-advice/000027.htm>
- Messages, Packets, and Frames – Structural division
- Encapsulation – content vs. headers
- Repeaters, Bridges, Switches, and Routers
- Addressing structures – MAC, IP, others
- Protocols and RFPs

Preparation for Next Week

Readings for the week:

- ***Maximum Security***: Chapter 4
- “*Internetworking Basics*” - available at http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/introint.htm
- “*Cisco Networking Essentials*” - available at http://www.cisco.com/warp/public/779/edu/media/pdf/edu_networking_essentials_2000.pdf (BEWARE - HUGE FILE)
- “*Mike’s OSI Model Page*” – available at <http://www.csi.cc/~mike/students/networking/iso/isomodel.html>

Topic Paper 1 - Guidance

- Topic – Security Incidents or Issues
- 5-7 page research paper equivalent
- Option A – Choose a recent security incident and perform a post-mortem on it. Give me history, details, stakeholders, major players, disposition, and how it is relevant, plus any other details.
- Option B – Choose a security issue and perform an analysis of the security issues involved, based on the readings and lectures so far, plus your research. Some examples might be ID Theft, digital trade (paypal, eBay, etc.), or privacy issues.
- DUE – February 7, 2002