

---

## Intrusion Detection

ISA 774  
George Mason University  
Spring 2006

GMU ISA 774 Spring 2006

2

---

## ISA 774 Course Objectives

- Study methodologies, techniques and tools for the monitoring of events in a computer system or a network, with the objective of preventing and detecting unwanted process activity and of recovering from malicious behavior.
- Topics include:
  - types of threats
  - host-based and network-based information sources
  - vulnerability analysis
  - denial of service
  - deploying and managing intrusion detection systems
  - passive vs. active responses
  - designing recovery solutions

GMU ISA 774 Spring 2006

3

---

*The art of war teaches us to rely not on the likelihood of the enemy's not coming, but on our own readiness to receive him; not on the chance of his not attacking, but rather on the fact that we have made our position unassailable.*

—*The Art of War, Sun Tzu*

GMU ISA 774 Spring 2006

2

---

## ISA 774 Class Members

- Instructor – Zach Tudor
  - Retired Navy Limited Duty Officer (Submarines)
  - M.Sc. IT (GMU), CISSP, CISM, PMP, CCP, IEM
  - <http://mason.gmu.edu/~ztudor/ISA774/>
- Masters Students
- PhD Students

GMU ISA 774 Spring 2006

4

## Class Introductions

---

- Your Name
- Masters, PhD, or Other
- Full Time Student, or Occupation
- Added Flavor???

GMU ISA 774 Spring 2006

5

## George Mason University Information Security Education

---

- Where does this course fit in
  - Elective requirement for each InfoSec program
- What other courses are available
  - ISA 662 Information System Security
  - ISA 765 Database and Distributed Systems Security
  - ISA 766 Internet Security Protocols
  - ISA 767 Secure Electronic Commerce
  - ISA 780 Theoretical Foundations of System Security
  - SWE 781 Secure Software Design and Programming
  - IT 862 Formal Models for Computer Security (Restricted to PhD students)
  - IT 962 Advanced Topics in Computer Security (Restricted to PhD students)
  - ECE 646 Cryptology and Computer-Network Security
  - ECE 746 Secure Telecommunication Systems

GMU ISA 774 Spring 2006

7

## George Mason University Information Security Education

---

- Degrees and Certifications
  - Masters, Doctorate, and Graduate Certificate
- Nationally recognized security labs
  - ISE Lab for Information Security Technology (LIST)
  - Center for Secure Information Systems (CSIS)
  - Lab for Attack Prevention and Detection
- GMU professors edit major InfoSec journals
  - ACM Transactions on Information Security (Sandhu)
  - International Journal of Information Security (Jajodia)

GMU ISA 774 Spring 2006

6

## Course Rules

---

- We are all here to learn
- Participation is key
  - If you have something else to do, don't do it here
- Bob Kenner's Rules for Success
  - Show up (70%)
  - Be prepared (85%)
  - Be capable (95%)
- Zach's Rule for almost everything:
  - *Semper Gumbi*

GMU ISA 774 Spring 2006

8

## Grading & Testing

- Nominally:
  - Homework assignments
    - Based on textbook and assigned reading
  - Term Paper
    - Expand on course topics
  - 2 Tests
    - Mid term and Final
- Participation !!!
- Quizzes???

GMU ISA 774 Spring 2006

9

## Terms and Terminology

- What's in a name??
- In academic study, precise use of terms is key to understanding, but ...
- Industry tends to productize concepts, technologies and methods
- For this class, the definitions in *Bace* will be our guide to terms

GMU ISA 774 Spring 2006

11

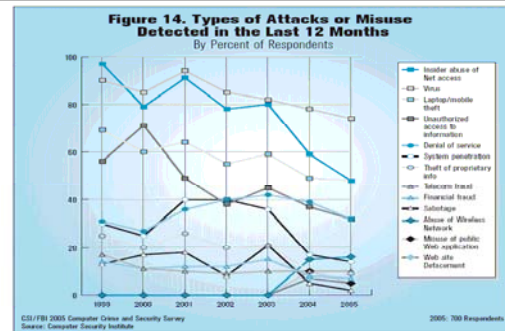
## Course Schedule

Date	Topics	Reading Assignment	Homework Assignment	Handout
Jan 24	Administrivia Introduction			
Jan 31	The History of Intrusion Detection Concepts and Lessons	<i>Bace</i> , Chapter 1 & 2		
Feb 7	Information Sources	<i>Bace</i> , Chapter 3		
Feb 14	Analysis Schemes	<i>Bace</i> , Chapter 4		
Feb 21	Responses	<i>Bace</i> , Chapter 5		
Feb 28	Vulnerability Analysis	<i>Bace</i> , Chapter 6		
Mar 7	Technical Issues	<i>Bace</i> , Chapter 7	HW 1 Due	
Mar 14	Spring Break			
Mar 21	Midterm Exam			
Mar 28	Understanding the Real World Challenge	<i>Bace</i> , Chapter 8		
Apr 4	Legal Issues	<i>Bace</i> , Chapter 9		
Apr 11	Intrusion Detection Architecture	<i>Bace</i> , Chapter 10, 11, 12		
Apr 18	Intrusion Prevention, Security Information Management		HW 2 Due	
Apr 25	Intrusion Detection for Critical Infrastructures			
May 2	Future Trends	<i>Bace</i> , Chapter 13		
May 9	Final Exam			

GMU ISA 774 Spring 2006

10

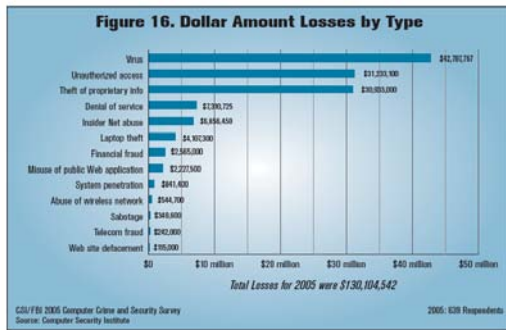
## What's the Big Deal??



GMU ISA 774 Spring 2006

12

### What's the Big Deal??



GMU ISA 774 Spring 2006

13

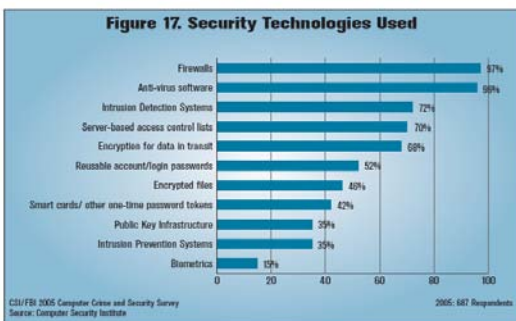
### What's the Big Deal??



GMU ISA 774 Spring 2006

15

### What's the Big Deal??



GMU ISA 774 Spring 2006

14

### What's the Big Deal??

FEDERAL COMPUTER SECURITY REPORT CARD			February 16, 2005		
GOVERNMENTWIDE GRADE 2004: D+					
	2004	2003	2004	2003	
AGENCY FOR INTERNATIONAL DEVELOPMENT	A+	C-	DEPARTMENT OF STATE	D+	F
DEPARTMENT OF TRANSPORTATION	A-	D+	DEPARTMENT OF TREASURY**	D+	D
NUCLEAR REGULATORY COMMISSION	B+	A	DEPARTMENT OF DEFENSE**	D	D
SOCIAL SECURITY ADMINISTRATION	B	B+	NATIONAL AERONAUTICS AND SPACE ADMINISTRATION	D	D-
ENVIRONMENTAL PROTECTION AGENCY	B	C	SMALL BUSINESS ADMINISTRATION	D-	C-
DEPARTMENT OF LABOR	B-	B	DEPARTMENT OF COMMERCE	F	C-
DEPARTMENT OF JUSTICE	B-	F	DEPARTMENT OF VETERANS AFFAIRS**	F	C
GENERAL SERVICES ADMINISTRATION	C+	D	DEPARTMENT OF AGRICULTURE	F	F
NATIONAL SCIENCE FOUNDATION	C+	A-	DEPARTMENT OF HEALTH AND HUMAN SERVICES	F	F
DEPARTMENT OF THE INTERIOR	C+	F	DEPARTMENT OF ENERGY	F	F
DEPARTMENT OF EDUCATION	C	C+	HOUSING AND URBAN DEVELOPMENT	F	F
OFFICE OF PERSONNEL MANAGEMENT	C-	D-	DEPARTMENT OF HOMELAND SECURITY	F	F

\* - Inspector General did not submit an independent evaluation of the agency's security management program as required by the Federal Information Security Management Act of 2002  
 \*\* - No independent evaluation from the Inspector General was submitted in 2003  
 Prepared by the Government Reform Committee, chaired by Tom Davis, based on reports required by the Federal Information Security Management Act of 2002

GMU ISA 774 Spring 2006

16

## Why are Information Systems Vulnerable to Attack?

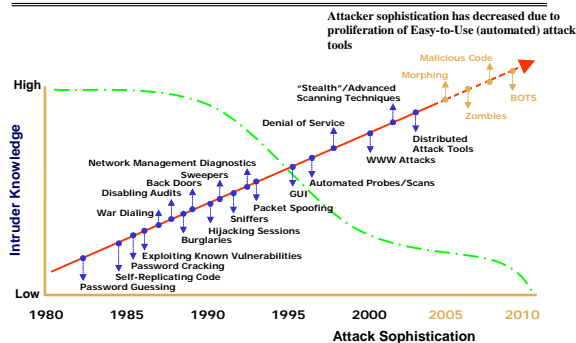
- The architecture of the Internet makes it susceptible to certain types of attacks
- Interdependent nature of Internet users
- Finite resources
- The National Research Council found in 1999 that:
  - No mechanisms or systematic design methods exist for defending against DoS
  - The ad hoc methods that were useful for defending timesharing systems from DoS are unsuitable for defending network systems

Trust in Cyberspace, Fred B. Schneider, Editor: Committee on Information Systems Trustworthiness, National Research Council (1999), <http://books.nap.edu/books/0309065585/html/index.html>

## What is Information System Security??

- Traditionally, there are three major goals of Information Security:
  - **Confidentiality**
    - The assets are accessible only by authorized parties.
  - **Integrity**
    - The assets are modified only by authorized parties, and only in authorized ways.
  - **Availability**
    - Assets are accessible to authorized parties.

## Threat Trends



## OSI Security Architecture

- ITU-T X.800 Security Architecture for OSI
- defines a systematic way of defining and providing security requirements
- For us it provides a useful, if abstract, overview of concepts of Information Security

## Security Services (X.800)

---

- **Authentication** - assurance that the communicating entity is the one claimed
- **Access Control** - prevention of the unauthorized use of a resource
- **Data Confidentiality** –protection of data from unauthorized disclosure
- **Data Integrity** - assurance that data received is as sent by an authorized entity
- **Non-Repudiation** - protection against denial by one of the parties in a communication

GMU ISA 774 Spring 2006

21

## Characteristics of Computer Intrusion

---

- A **computing system**: a collection of hardware, software, data, and people that an organization uses to do computing tasks
- Any part of the computing system can become the **target** of a computing crime.
- The **weakest point** is the most serious vulnerability.
- The **principle of easiest penetration**

GMU ISA 774 Spring 2006

23

## Status of security in computing

---

- In terms of security, computing is very close to the wild west days.
- Some computing professionals & managers do not even recognize the value of the resources they use or control, or *the need to adequately secure them*.
- In the event of a computing crime, some companies do not investigate or prosecute.

GMU ISA 774 Spring 2006

22

## Security Terminology

---

- **Assets** – hardware, software, data, people
- **Vulnerability**
  - a weakness in a system that may make it vulnerable to disruption or attack
- **Threats**
  - An event that has the potential to cause loss or harm
- **Attack**
  - A deliberate exploitation of a vulnerability
- **Exposure**
  - a form of possible loss or harm
- **Control** – a protective measure

GMU ISA 774 Spring 2006

24

## Types of Security Breaches

---

- Interruption
  - Example: DOS (Denial of Service)
- Interception
  - Peeping eyes
- Modification
  - Change of existing data
- Fabrication
  - Addition of false or spurious data

GMU ISA 774 Spring 2006

25

## Software Vulnerabilities

---

- Destroyed (deleted) software
- Stolen (pirated) software
- Altered (but still running) software
  - Trapdoor/Rootkit
  - Logic bomb
  - Information leaks
- Malicious Software
  - Trojan horse
  - Virus

GMU ISA 774 Spring 2006

27

## Computing System Vulnerabilities

---

- Hardware vulnerabilities
- Software vulnerabilities
- Data vulnerabilities
- Human vulnerabilities ?

GMU ISA 774 Spring 2006

26

## Other Exposed Assets

---

- Storage media
- Networks
- Access
- Key people

GMU ISA 774 Spring 2006

28

## People Involved in Computer Crimes

---

- Amateurs (Script Kiddies?)
- Crackers (Hackers???)
- Career Criminals
- Trusted Insiders
  - Employees
  - Developers
  - Consultants

GMU ISA 774 Spring 2006

29

## Encryption

---

- At the heart of many security methods
- Confidentiality of data
- Some protocols rely on encryption to ensure availability of resources
- Encryption does not solve all computer security problems
- Encryption *may* make our detection tasks more difficult

GMU ISA 774 Spring 2006

31

## Methods of Defense

---

- Encryption
- Software controls
- Hardware controls
- Policies
- Physical controls

GMU ISA 774 Spring 2006

30

## Software controls

---

- Internal program controls
- OS controls
- Development controls
- Software controls are usually the first aspects of computer security that come to mind.

GMU ISA 774 Spring 2006

32

## Hardware controls

---

- Smart Cards
- Secure ID
- Biometrics

GMU ISA 774 Spring 2006

33

## Physical Controls

---

- Restricted location
- Armed guards
- Environmental controls
- Fire suppression systems

GMU ISA 774 Spring 2006

35

## Policies

---

- Guidelines, rules of behavior, standards, etc to provide
- Policy controls can be simple but effective
  - Example: frequent changes of passwords
- Legal and ethical controls
  - Gradually evolving and maturing

GMU ISA 774 Spring 2006

34

## Principle of Effectiveness

---

- Controls must be used to be effective.
  - Efficient
    - Time, memory space, human activity, ...
  - Appropriate for the security need
  - Easy to use (ease of *effective* use)
  - Auditable
- The **principle of adequate protection**

GMU ISA 774 Spring 2006

36

## Overlapping Controls

---

- Several different controls may apply to one potential exposure.
  - H/w control
  - S/w control
  - Data control
- Commonly referred to as **Defense in Depth**

GMU ISA 774 Spring 2006

37

## References and Resources

---

- ITU-T Recommendation X.800 (1991): Security architecture for Open Systems Interconnection for CCITT applications, 1991. <http://www.macs.hw.ac.uk/cs/online/4nu2/21/x800.html>
- GMU CSIS Certification, Relevance to CISSP Preparation, Ron Ritchey, 2000. [http://www.isse.gmu.edu/~csis/seminars/presentations/csis\\_cissp.pdf](http://www.isse.gmu.edu/~csis/seminars/presentations/csis_cissp.pdf)
- CSI/FBI 2005 Computer Crime Survey, CSI 2005. <http://www.gocsi.com>
- Dorothy Denning, *An Intrusion-Detection Model*. IEEE Transactions On Software Engineering, Vol. Se-13, No. 2, February 1987, 222-232. <http://www.cs.georgetown.edu/~denning/infosec/ids-model.rtf>
- Tim Bass, *Traditional Intrusion Detection Model Outdated and Distracting*, [http://www.silkroad.com/papers/pdf/Traditional\\_Intrusion\\_Detection\\_Model\\_Outdated\\_and\\_Distracting.pdf](http://www.silkroad.com/papers/pdf/Traditional_Intrusion_Detection_Model_Outdated_and_Distracting.pdf)
- James P. Anderson, *Computer Security Technology Planning Study*. ESD-TR-73-51, ESD/AFSC, Hanscom AFB, Bedford, MA 01731 (Oct. 1972) [NTIS AD-758 206] <http://csrc.nist.gov/publications/history/ande72.pdf>

GMU ISA 774 Spring 2006

39

## Next Week

---

- Topics
  - History of ID
  - ID Concepts and Definitions
- Read
  - Bace, Chapter 1 & 2
  - Denning, *An Intrusion Detection Model*
  - Bass, *Traditional Intrusion Detection Model Outdated and Distracting*
  - Anderson, *Computer Security Technology Planning Study*

GMU ISA 774 Spring 2006

38