WILLIAM & MARY

CSCI 454/554 Computer and Network Security

Instructor: Dr. Kun Sun

WILLIAM & MARY

About Instructor

- Dr. Kun Sun, Assistant Professor of Computer Science
  - http://www.cs.wm.edu/~ksun/
  - Phone: (757) 221-3457
  - Email: ksun@wm.edu
  - Office: McGrothlin-Street Hall, #105
  - Office hours
    - 1:30pm-3:30pm TR, or by appointment

2

WILLIAM & MARY

About TA

- Shengye Wan
  - Email: swan@email.wm.edu
  - Office: : McGrothlin-Street Hall, #107-A
  - Office Hour: by appointment

3

WILLIAM & MARY

Course Objectives

- Understanding of basic issues, concepts, principles, and mechanisms in computer and network security.
  - Basic security concepts
  - Cryptography
  - Authentication
  - Kerberos
  - IPsec and Internet key management
  - SSL/TLS
  - Firewall
- Be able to determine appropriate mechanisms for protecting networked systems.

4

WILLIAM & MARY

Course Outline

- Basic Security Concepts
  - Confidentiality, integrity, availability
  - Security policies, security mechanisms, security assurance
- Cryptography
  - Basic number theory
  - Secret key cryptosystems
  - Public key cryptosystems
  - Hash function
  - Key management

5

WILLIAM & MARY

Course Outline (Cont'd)

- Identification and Authentication
  - Basic concepts of identification and authentication
  - User authentication
  - Authentication protocols

6

Course Outline (Cont'd)

- Network and Distributed Systems Security
  - Public Key Infrastructure (PKI)
  - Kerberos
  - IPsec
  - IPsec key management
  - SSL/TLS
  - Firewalls

7

Course Outline (Cont'd)

- Miscellaneous topics
  - Evaluation of secure information systems
  - Mobile security
  - Cloud security
  - Malicious software
  - Security management

8

Term Project

- Project
  - Research paper
  - Survey paper

- See the class website for detailed requirement

- You are expected to explore issues beyond what's included in lectures by yourselves

9

What's Left Out?

- Hacking
- System configuration, O.S. internals
- Political, legal, regulatory
- Financial, economics
- Social, psychological, human factors
- Morals, ethics
- Operational, business procedures, logistics

10

Prerequisites

- Programming experience in Java and C is required

- Knowledge of Algorithm and Computer Organization
  - CSCI 303 & CSCI 304

11

Textbook

- Required textbook
  - Charlie Kaufman, Radia Perlman, and Mike Speciner, *Network Security: Private Communication in a Public World, 2nd Edition*, Prentice Hall, ISBN-13: 007-6092018469, ISBN-10: 0130460192 .

12

2

On-line Resources

- Course website:
  http://www.cs.wm.edu/~ksun/csci454-s16/index.html
- For course materials, e.g., lecture slides, homework files, project, tools, etc.
  - Will be updated frequently. So check frequently.

13

Grading

- CSCI 454
  - Homework assignments 25%
  - Term project: 10%
  - Midterm exam: 30%
  - Final exam: 35%

- CSCI 554
  - Homework assignments 20%
  - Term project: 30%
  - Midterm exam: 20%
  - Final exam: 30%

Note:
1. Must use text editor (e.g. MS Word, latex) to complete your homework and project. Handwritten submissions are not accepted
2. HW and projects are submitted through Blackboard.

14

Policies on late assignments

- Homework and project deadlines will be hard.
- Late homework will be accepted with a 10% reduction in grade for each day they are late by.
- Once a homework assignment is discussed in class, submissions will no longer be accepted.

15

Policies on Absences and Makeup

- You may be excused from an exam only with a university approved condition, with proof. For example, if you cannot take an exam because of a sickness, we will need a doctor's note.
- Events such as going on a business trip or attending a brother's wedding are not an acceptable excuse for not taking an exam at its scheduled time and place.
- You will have one chance to take a makeup exam if your absence is excused. There will be no makeup for homework assignments.

16

Academic Integrity

- The university, college, and department policies against academic dishonesty will be strictly enforced.
- Honor code
  - Students are required to follow William and Mary's Honor System, as described in the student handbook.

17

Check the website for details!

18

3

CSCI 454/554 Computer and Network Security

Topic #1. Basic Security Concepts

Why This Course?

The 2013 Threat Landscape

Symantec Internet Security Threat Report 2014
http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf

20

Why This Course?

- Increased volume of security incidents
- Security threats
  - Malware: Virus, worm, spyware
  - Spam
  - Botnet
  - DDoS attacks
  - Phishing, social engineering
  - Drive-by download
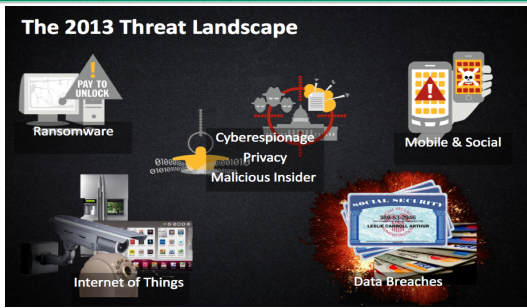 - Cross-site scripting (XSS)
  - …

21

Contributing Factors

- Lack of awareness of threats and risks of information systems
  - Security measures are often not considered until an Enterprise has been penetrated by malicious users
  - The situation is getting better, but …
- (Historical) Reluctance to invest in security mechanisms
  - The situation is improving
    - Example: Windows 95 → Windows 2000 → Windows XP → Windows Vista → Windows 7 → Windows 8
  - But there exists legacy software
- Wide-open network policies
  - Many Internet sites allow wide-open Internet access

22
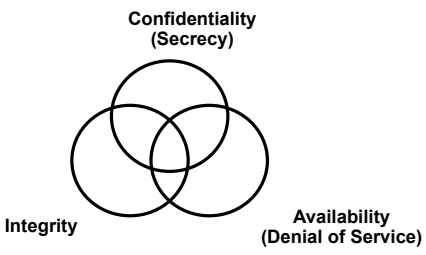
Contributing Factors (Cont'd)

- Lack of security in TCP/IP protocol suite
  - Most TCP/IP protocols not built with security in mind
  - Work is actively progressing within the Internet Engineering Task Force (IETF)
- Complexity of security management and administration
  - Security is not just encryption and authentication
- Software vulnerabilities
  - Example: buffer overflow vulnerabilities
  - We need techniques and tools to better software security
- Hacker skills keep improving
  - Cyber warfare

23

Security Objectives

Confidentiality (Secrecy)

Integrity

Availability (Denial of Service)

24

Security Objectives (CIA)

- <u>C</u>onfidentiality — Prevent/detect/deter improper disclosure of information
- <u>I</u>ntegrity — Prevent/detect/deter improper modification of information
- <u>A</u>vailability — Prevent/detect/deter improper denial of access to services provided by the system

- These objectives have different specific interpretations in different contexts

25

Commercial Example

- Confidentiality — An employee should not come to know the salary of his manager
- Integrity — An employee should not be able to modify the employee's own salary
- Availability — Paychecks should be printed on time as stipulated by law

26

Military Example

- Confidentiality — The target coordinates of a missile should not be improperly disclosed
- Integrity — The target coordinates of a missile should not be improperly modified
- Availability — When the proper command is issued the missile should fire

27

A Fourth Objective

- Securing computing resources — Prevent/detect/deter improper use of computing resources including
  - Hardware Resources
  - Software resources
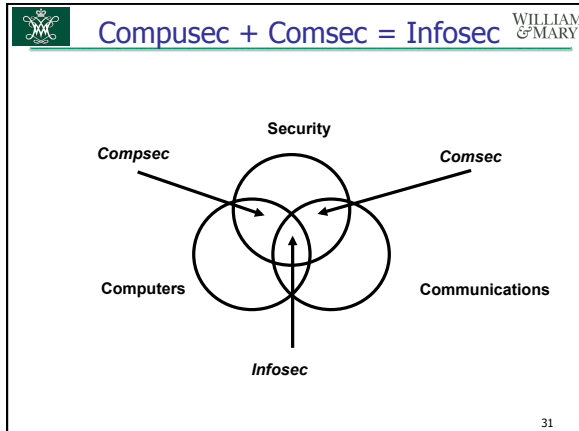 - Data resources
  - Network resources

28

Achieving Security

- Security policy — What?
- Security mechanism — How?
- Security assurance — How well?

29

Security Policy

Organizational Policy

Automated Information System Policy

30

5

Compusec + Comsec = Infosec

Security

Compsec   Comsec

Computers   Communications

Infosec

31

Security Mechanisms

- In general three types
  - Prevention
    - Example: Access control
  - Detection
    - Example: Auditing and intrusion detection
  - Tolerance
    - **Good prevention and detection both require good authentication as a foundation**

32

Security Mechanisms (Cont'd)

- Prevention is more fundamental
  - Detection seeks to prevent by threat of punitive action
  - Detection requires that the audit trail be protected from alteration
- Sometime detection is the only option, e.g.,
  - Accountability in proper use of authorized privileges
  - Modification of messages in a network
- Security functions are typically made available to users as a set of *security services*
- Cryptography underlies (almost) all security mechanisms

33

Security Services

- Security functions are typically made available to users as a set of security services through APIs or integrated interfaces
- Confidentiality: protection of any information from being exposed to unintended entities.
  - Information content.
  - Parties involved.
  - Where they are, how they communicate, how often, etc.
- Authentication: assurance that an entity of concern or the origin of a communication is authentic - it's what it claims to be or from
- Integrity: assurance that the information has not been tampered with

34

Security Services (Cont'd)

- Non-repudiation: offer of evidence that a party is indeed the sender or a receiver of certain information
- Access control: facilities to determine and enforce who is allowed access to what resources, hosts, software, network connections
- Monitor & response: facilities for monitoring security attacks, generating indications, surviving (tolerating) and recovering from attacks

35

Security Assurance

- How well your security mechanisms guarantee your security policy
- Everyone wants high assurance
- High assurance implies high cost
  - May not be possible
- Trade-off is needed

36

Security by Obscurity

- Security by obscurity
  - If we hide the inner workings of a system it will be secure
  - E.g., steganography

- Less and less applicable in the emerging world of vendor-independent open standards
- Less and less applicable in a world of widespread computer knowledge and expertise

37

Security by Legislation

- Security by legislation says that if we instruct our users on how to behave we can secure our systems
- For example
  - Users should not share passwords
  - Users should not write down passwords
  - Users should not type in their password when someone is looking over their shoulder

- User awareness and cooperation is important, but cannot be the principal focus for achieving security

38

Security Tradeoffs

Security   **Functionality**

COST

Ease of Use

39

Threat-Vulnerability-Risk

- Threats — *Possible* attacks on the system
- Vulnerabilities — Weaknesses that may be exploited to cause loss or harm
- Risk — A measure of the possibility of security breaches and severity of the ensuing damage

- Requires assessment of threats and vulnerabilities

40

Threat Model and Attack Model

- Threat model and attack model need to be clarified before any security mechanism is developed

- Threat model
  - Assumptions about potential attackers
  - Describes the attacker's capabilities
- Attack model
  - Assumptions about the attacks
  - Describe how attacks are launched

41

Risk Management

- Risk analysis
  - NIST Common Vulnerability Scoring System (CVSS)
  - Mathematical formulae and computer models can be developed, but the parameters are difficult to estimate.
- Risk reduction
  - Attack surface, Attack graph
- Risk acceptance
  - Certification
    - Technical evaluation of a system's security features with respect to how well they meet a set of specified security requirements
  - Accreditation
    - The management action of approving an automated system, perhaps with prescribed administrative safeguards, for use in a particular environment

42