

# ISA 666

## Internet Security Protocols

Dr. Duminda Wijesekera  
*duminda@ise.gmu.edu*  
703-993-1578

### About the Instructor

- Dr. Duminda Wijesekera, Assistant Professor of Information & Software Engineering
  - <http://www.ise.gmu.edu/~duminda/index.html>
  - 703-993-1578
  - Office: Room 351 Science & Technology II
  - Office hours: Tuesday 3:00PM ~ 4:00P  
Thursday 6:00PM ~ 7:00PM  
or by appointment

### About the TA

- Ram Krishnan
  - rkrishna@gmu.edu
- Office hours:
  - Monday 2:00PM ~ 3:00PM
  - Tuesday 2:00PM ~ 3:00PM

### Course Description

- Comprehensive Introduction to the Security Problems in the Internet
  - What are the security issues?
  - What techniques are available?
  - The tradeoffs!
- Study Principles, Techniques and Their Applications in Building Secure Internet
  - Basic cryptography
  - Authentication, authorization
  - Digital signature

### Course Description Continued...

- Examine Existing Internet Security Techniques and Protocols
  - IPSEC/VPN
  - Firewall
  - SSL/TLS
- Advanced Internet Security Techniques
  - Intrusion Tracing
  - Steganography/Information Hiding
- Limitations of Existing Security Protocols
- Open Problems in the Internet Security

### Course Objectives

- Gain Understanding of Basic Issues, Concepts, Principles, and Techniques in Internet Security.
  - Basic security concepts
  - Cryptography
  - Authentication, authorization
  - Network security
  - Intrusion response
- Be Able to Determine Appropriate Mechanisms for Particular Security Requirement
  - Only you (or person authorized by you) can change your address record
  - Only I can give your grade in this class

## Course Outline

- Network Based Attacks
  - Passive, active attacks
  - Eavesdropping, unauthorized access, modification, deletion, forgery of confidential information
  - Denial-of-service attack
- Basic Security Concepts
  - Confidentiality, integrity, identity, anonymity, availability
  - Security policies, security mechanisms, assurance

## Course Outline (Cont'd)

- Cryptography
  - Basic number theory
  - Secret key cryptosystems
  - Public key cryptosystems
  - Hash function
  - Key management

## Course Outline (Cont'd)

- Identification and Authentication
  - Basic concepts of identification and authentication
  - Password authentication
  - Kerberos
  - Security handshake pitfalls
  - Attack on authentication and identification
    - Identity theft
    - Impersonate somebody else

## Course Outline (Cont'd)

- IPSEC/VPN
  - Security association
  - Authentication header (AH)
  - Encapsulating Security Payload (ESP)
  - Transport, tunnel modes
  - Virtual Private Network (VPN)
- IPSEC Key Management
  - ISAKMP/Oakley
- PKI

## Course Outline (Cont'd)

- Firewall
  - Packet filtering
  - Stateful inspection
  - Transparent proxy
  - Enclave
  - Firewall limitations
  - Firewalls and Virtual Private Network
- SSL/TSL

## Course Outline (Cont'd)

- Intrusion Tracing
  - IP Spoofing
  - Stepping Stones
  - Reflector
  - Zombie
- Intrusion Response
  - Blocking?
  - Rate limiting?

## Course Outline (Cont'd)

- Advanced Topics
  - Anonymity and privacy
  - Steganography/information hiding
  - Virus, worms, Trojan horse

## Prerequisites

- INFS 612 (Data Communication and Distributed Processing) or Equivalent
- INFS 601 (Operating Systems) or Equivalent
- Strong Programming
- Basic Knowledge and Skills in Discrete Mathematics

## Textbook and Handouts

- Required Textbook
  - Charlie Kaufman, Radia Perlman, and Mike Speciner, *Network Security: Private Communication in a Public World, 2nd Edition*, Prentice Hall, ISBN: 0-13-046019-2.
- Reference Book
  - William Stallings, *Network Security Essentials, 2nd Edition*, Prentice Hall.
- Research papers listed on the course website (TBA).

## On-line Resources

- WWW page:
  - <http://www.ise.gmu.edu/~duminda/classes/fall05/ise666.html>
  - For course materials, e.g., lecture slides, homework files, papers, tools, etc.
  - Will be updated frequently. So check frequently.

## Grading

- Assignments 30%, Midterm 40%, Term paper/project 30% (No final exam)
- The Final Grades Are Computed According to the Following Rules:
  - A+:  $\geq 95\%$ ; A: [90%, 95%]; A-: [85%, 90%];
  - B+: [80%, 85%]; B: [75%, 80%]; B-: [70%, 75%];
  - C+: [66%, 70%]; C: [63%, 66%]; C-: [60%, 63%];
  - D+: [56%, 60%]; D: [53%, 56%]; D-: [50%, 53%];
  - F:  $< 50\%$ .
- The Boundaries between Grades are Strict
  - Score of 84.999% would be a B+, rather than A-.

## Policies on Late Submissions

- Homework and Term Paper/Project Deadlines Will Be Hard.
- Late Homework Will Be Accepted with a 10% Penalty in Score for Each Day Past Due.
- Once a Homework Assignment is Discussed in Class, No Late Submissions Will Be Accepted.
- Late Submission of Term Paper/Project Will NOT Be Accepted

## Policies on Absences

- 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 or present term paper/project 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.

## Academic Integrity

- All University, School, and Department Policies Against Academic Dishonesty Will Be Strictly Enforced.
- University Academic Policies at
  - <http://www.gmu.edu/catalog/apolicies/#Anchor12>
- ISE Department Honor System and Code
  - <http://www.ise.gmu.edu/Honor.html>

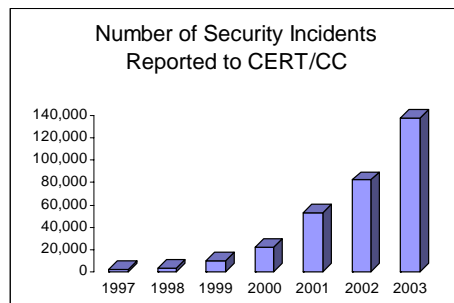
## Term Paper/Project

- Can Be:
  - Research Paper
    - Work on original research problem with **original technical contribution**
  - Survey Paper
    - Comprehensive** summary of a particular topic
  - Design of New Algorithms, Protocols or New Attacks!
    - Should justify the usefulness
  - Analysis/Evaluation of Existing Algorithms, Protocols.
    - Provide **new insights**
  - Implementation and Experimentation.
    - Better implementation of existing algorithm, protocols

## Term Paper/Project (Cont'd)

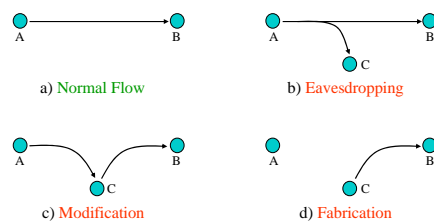
- To Be Done Individually.
- Proposal
- Presentation
- Final Report
- Suggested Topics (see course website)
- Or Pick Your Own Topic.

## Security Problems on Internet Connected Computers



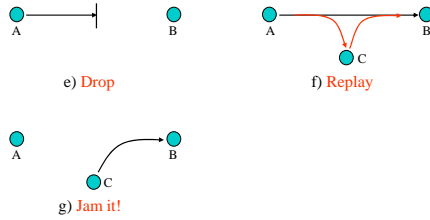
## Network Security Problems

- Start From The Basics



## Network Security Problems (Cont'd)

### • Start From The Basics



## Network Security Concepts

- Confidentiality
  - Prevent information from being exposed to unintended party
- Integrity
  - Assure that the information has not been tempered
- Identity
  - Assure that the party of concern is authentic - it is what it claims to be
- Availability
  - Assure that unused service or resource is available to legitimate users
- Anonymity
  - Assure that the identity of some party is remain anonymous
- Non-Repudiation
  - Assure that authenticated party has indeed done something and it can not deny it

## 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
- Identity
  - An employee should be able to uniquely identify and authenticate himself/herself
- Availability
  - Paychecks should be printed on time as stipulated by law
- Anonymity
  - The manager should not know who had a critical review for him
- Non-repudiation
  - Once the employee has cashed out the paycheck, he/she can't deny it

## Real-World Network Based Attacks

- Distributed Denial of Service (DDOS) Attacks
- Worm and Virus Attacks (e.g., worm sasser)
- Monitoring and Capture of Network Traffic
  - User IDs, passwords, and other information are often stolen on Internet
- Exploitation of Software Vulnerability (MS-Windows)
- Unauthorized Access to Resources
  - Disclosure, modification, and destruction of resources
- Compromised System Used as Stepping Stone
- Masquerade as Authorized User or End System
- Data driven attacks
  - Importation of malicious or infected code
- E-Mail Forgery

## Contributing Factors

- Lack of Awareness of Threats and Risks of From the Network
  - Security measures are often not considered until an Enterprise has been penetrated by malicious users
- Wide-Open Network Policies
  - Many Internet sites allow wide-open Internet access
- Vast Majority of Network Traffic is Unencrypted
  - Network traffic can be monitored and captured

## Contributing Factors (Cont'd)

- Lack of Security in TCP/IP Protocol Suite
  - Most TCP/IP protocols were not built with security in mind
  - Work is actively progressing within the Internet Engineering Task Force (IETF)
- Complexity of Management of Network Security
- Exploitation of Software (e.g., Protocol Implementation) Bugs
  - Example: Sendmail bugs
- Attacker' Skills Keep Improving

## Existing Internet Security Mechanisms

- Prevention
  - Firewall
  - Authentication, authorization
  - IPSEC/VPN
  - Access control
  - Encryption
- Detection
  - Auditing
  - Misuse detection
  - Anomaly detection
- Survivability
- Response

## Existing Internet Security Mechanisms

- Security mechanisms implement functions that help to *prevent, detect, tolerate, respond* to security attacks
- Prevention is ideal, but...
  - Detection seeks to prevent by threat of punitive action
  - Detection requires that the audit trail be protected from alteration
- If can't completely prevent attack from happening, detection is the only option
- There could be attacks we can't detect, then live with it - survivable system
- Once detect the attack, then what? Active response!!!
- Cryptography underlies (almost) all security mechanisms

## Security by Obscurity

- Security by obscurity says that if we hide the inner workings of a system it will be secure
- **It is a bad idea**
- 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

## Security by Legislation

- Security by legislation says that if we instruct our users on how to behave we can secure our systems
- **It is a bad idea**
- 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

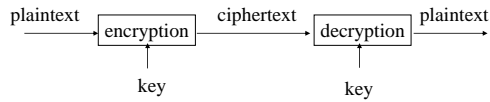
## Unique Aspects of Security Problem

- The Whole System is as Strong as Its Weakest Point
- The Root Cause of Security Problem is Not Computer, But Human Being
- Ever Changing - Moving Target
  - countermeasures by adversary
- Conflicting Requirements
  - Identity/authentication
  - Anonymity

## Cryptography

- Cryptography
  - Comes from Greek word
  - Original meaning: The art of secret writing
  - Becoming a science that relies on mathematics (number theory, algebra)
  - Process data into intelligible form, reversible, without data loss
  - Usually one-to-one (not compression)

## Encryption/Decryption



- Plaintext: a message in its original form
- Ciphertext: a message in the transformed, unrecognized form
- Encryption: the process that transforms a plaintext into a ciphertext
- Decryption: the process that transforms a ciphertext to the corresponding plaintext
- Key: the value used to control encryption/decryption.

## Cryptanalysis

- Ciphertext only:
  - Analyze only with the ciphertext
  - Example: Exhaustive search until “recognizable plaintext”
  - Smarter ways available
- Known plaintext:
  - Secret may be revealed (by spy, time), thus <ciphertext, plaintext> pair is obtained
  - Great for mono-alphabetic ciphers

## Cryptanalysis (Cont'd)

- Chosen plaintext:
  - Choose text, get encrypted
  - Useful if limited set of messages
- Chosen ciphertext:
  - Choose ciphertext
  - Get feedback from decryption, etc.

## Security of An Encryption Algorithm

- Unconditionally secure
  - It is impossible to decrypt the ciphertext
  - One-time pad (the key is as long as the plaintext)
- Computationally secure
  - The cost of breaking the cipher exceeds the value of the encrypted information
  - The time required to break the cipher exceeds the useful lifetime of the information

## Secret Keys v.s. Secret Algorithms

- Security by obscurity
  - We can achieve better security if we keep the algorithms secret
  - Hard to keep secret if used widely
  - Reverse engineering, social engineering
- Publish the algorithms
  - Security of the algorithms depends on the secrecy of the keys
  - Less unknown vulnerability if all the smart (good) people in the world are examine the algorithms

## Secret Keys v.s. Secret Algorithms (cont'd)

- Commercial world
  - Published
  - Wide review, trust
- Military
  - Keep algorithms secret
  - Avoid giving enemy good ideas
  - Military has access to the public domain knowledge anyway.
- Security of a secure protocol should be based on the secrecy of the keys, rather than based on obscurity

## Some Trivial Codes

- Caesar cipher: substitution cipher:
  - Replace each letter with the one 3 letters later
  - $A \rightarrow D, B \rightarrow E$
- Captain Midnight Secret Decoder rings:
  - shift variable by  $n$ : IBM  $\rightarrow$  HAL
  - only 26 possibilities

## Some Trivial Codes (Cont'd)

- Mono-alphabetic cipher:
  - generalization, arbitrary mapping of one letter to another
  - $26!$ , approximately  $4 \times 10^{26}$
  - statistical analysis of letter frequencies

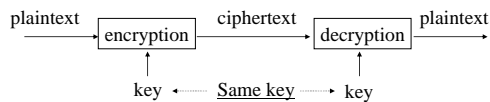
## Some Trivial Codes (cont'd)

- Poly-alphabetic Ciphers
  - A set of related mono-alphabetic substitution rules is used
  - A key determines which particular rule is chosen for a given transformation

## Types of Cryptography

- Number of keys
  - Hash functions: no key
  - Secret key cryptography: one key
  - Public key cryptography: two keys - public, private
- The way in which the plaintext is processed
  - Block cipher: divides input elements into blocks
  - Stream cipher: process one element (e.g., bit) a time

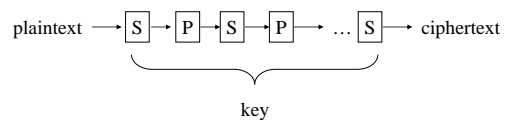
## Secret Key Cryptography



- Same key is used for encryption and decryption
- Also known as
  - Symmetric cryptography
  - Conventional cryptography

## Secret Key Cryptography (cont'd)

- Basic technique
  - Product cipher:
    - Multiple applications of interleaved substitutions and permutations



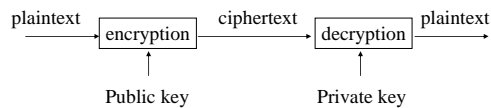
## Secret Key Cryptography (cont'd)

- Ciphertext approximately the same length as plaintext
- Examples
  - Stream Cipher: RC4
  - Block Cipher: DES, IDEA, AES

## Applications of Secret Key Cryptography

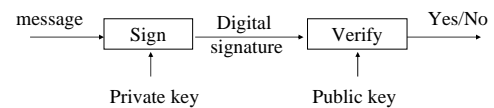
- Transmitting over an insecure channel
  - Challenge: How to share the key?
- Secure Storage on insecure media
- Authentication
  - Challenge-response
  - To prove the other party knows the secret key
  - Must be secure against chosen plaintext attack
- Integrity check
  - Message integrity code (MIC)

## Public Key Cryptography



- Invented/published in 1975
- A public/private key pair is used
  - Public key can be publicly known
  - Private key is kept secret by the owner of the key
- Much slower than secret key cryptography
- Also known as
  - Asymmetric cryptography

## Public Key Cryptography (Cont'd)



- Another mode: digital signature
  - Only the party with the private key can create a digital signature.
  - The digital signature is verifiable by anyone who knows the public key.
  - The signer cannot deny that he/she has done so.

## Applications of Public Key Cryptography

- Data transmission:
  - Alice encrypts  $m_a$  using Bob's public key  $e_b$ , Bob decrypts  $m_a$  using his private key  $d_b$ .
- Storage:
  - Can create a safety copy: using public key of trusted person.
- Authentication:
  - No need to store secrets, only need public keys.
  - Secret key cryptography: need to share secret key for every person to communicate with.

## Applications of Public Key Cryptography (Cont'd)

- Digital signatures
  - Sign hash  $H(m)$  with the private key
    - Authorship
    - Integrity
    - Non-repudiation: can't do with secret key cryptography
- Key exchange
  - Establish a common session key between two parties

## Hash Algorithms

Message of arbitrary length  $\rightarrow$  Hash  $H$   $\rightarrow$  A fixed-length short message

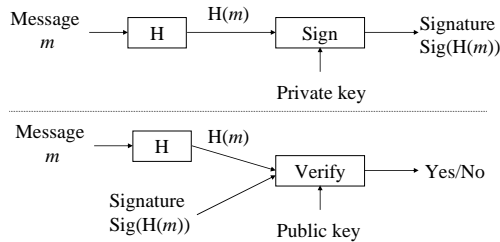
- Also known as
  - Message digests
  - One-way transformations
  - One-way functions
  - Hash functions
- Length of  $H(m)$  much shorter than length of  $m$
- Usually fixed lengths: 128 or 160 bits

## Hash Algorithms (Cont'd)

- Desirable properties of hash functions
  - **Performance**: Easy to compute  $H(m)$
  - **One-way property**: Given  $H(m)$  but not  $m$ , it's difficult to find  $m$
  - **Weak collision free**: Given  $H(m)$ , it's difficult to find  $m'$  such that  $H(m') = H(m)$ .
  - **Strong collision free**: Computationally infeasible to find  $m_1, m_2$  such that  $H(m_1) = H(m_2)$

## Applications of Hash Functions

- Primary application
  - Generate/verify digital signature



## Applications of Hash Functions (Cont'd)

- Password hashing
  - Doesn't need to know password to verify it
  - Store  $H(\text{password} + \text{salt})$  and salt, and compare it with the user-entered password
  - Salt makes dictionary attack more difficult
- Message integrity
  - Agree on a secret key  $k$
  - Compute  $H(m|k)$  and send with  $m$
  - Doesn't require encryption algorithm, so the technology is exportable