

University of Sydney
School of Information Technologies
COMP 4307/5327 Computer Security
Semester 2 2003
Course Outline

Introduction

The growth of the Internet brings with it a growth in the amount of information being transmitted. Much of this information is private and/or sensitive. One of the important topics in data communications is information security. Unfortunately, computer communications are often insecure.

In this course we will examine the common threats in information transfer which include

- Impersonation - pretending to be another system entity.
- Eavesdropping - gaining unauthorised access to communications between other system entities.
- Tampering - altering information in passage between other system entities.
- Repudiation - denying taking an action that was taken or claiming to have taken an action that was not taken.
- Denial of service - attempting to deny other system entities access to services.

These threats are dealt with via a variety of mechanisms. The most fundamental is cryptography. We shall examine secret key, message digest and public key algorithms. Authentication systems are used to prove identity. These systems make use of various protocols based on cryptographic mechanisms. We shall look at some common systems and common flaws in authentication systems. Once the system is convinced of the identity of a user it must decide which actions that user is entitled to carry out. This is the province of access control and the course will cover the basic approaches, including Discretionary Access Control (DAC), Mandatory Access Control (MAC), Role-Based Access Control (RBAC) and Lattice based approaches. Finally we will look at some of the other mechanisms required for security, such as auditing.

Prerequisite Knowledge

Computer Science Honours & Engineering:

Completion of COMP3007 Networked Systems or equivalent knowledge

Others:

Knowledge of the Internet
Some knowledge of networks

Topic Outline:

Note that it says *topic* not *week* some topics will take more than one week's worth of lectures to complete.

1. **Introduction:** What is Security?, Threats (eavesdropping, tampering, impersonation, repudiation, denial of service, illegal access), Mechanisms (confidentiality, integrity, auditing, authentication, access control)
Cryptography: terms, outline, symmetric cryptography, asymmetric cryptography, integrity, digital signatures, authentication, hash algorithms
2. **Secret Key Cryptography:** Block encryption, transformations, substitutions, permutations, decryption
DES: overview, DES rounds, S-Boxes
IDEA: overview, comparison with DES, key expansion, IDEA rounds
Skipjack: history, overview
Uses of Secret Key Cryptography: ECB, CBC, OFB, CFB, Multiple encryption DES
3. **Hash Functions and Message Digests:** length of hash, uses, algorithms (MD2, MD4, MD5, SHS)
MD2: algorithm (padding, checksum, passes)
MD4&5: algorithm (padding, stages, digest computation)
SHS: overview, padding, stages
4. **Public Key Cryptography:** algorithms, examples, modular arithmetic (addition, multiplication, inverse, exponentiation)

RSA: generating keys, encryption and decryption

Other Algorithms: PKCS, Diffie-Hellman, El-Gamal signatures, DSS, Zero-Knowledge Signatures

5. Authentication: Password Based, Cryptographic Authentication,

Passwords: in distributed systems, on-line vs off-line guessing, storing

Cryptographic Authentication: passwords & keys, protocols, KDC's, Certification Authorities, CA's vs. KDC's, Certification Revocation, Inter-domain, groups, delegation

Authentication of People: Verification techniques, passwords, length of passwords, password distribution, smart cards, biometrics

6. Public Key Infrastructure: what is PKI, certificates, directories, cross-certification of domains in PKI, X.500 directories and X.509 certificates

7. Security Policy: What is security policy, high and low level policy, user issues

8. Security Handshake Pitfalls: protocol problems, assumptions, shared secret protocols, public key protocols, mutual authentication, reflection attacks, use of timestamps, nonces and sequence numbers, session keys, one- and two-way public key based authentication

9. Example System: Kerberos: purpose, authentication, server and ticket granting server, keys and tickets, use of AS and TGS, replicated servers

Kerberos V4: names, inter-realm authentication, key version numbers

Kerberos V5: names, realms, delegation, forwarding and proxies, ticket lifetimes, revoking tickets, multiple realms

10. Access Control: principles, subjects and objects, review of access control matrix, access control lists and capabilities

Lattice Based Access Control: information flow policies, military lattice, Bell-La Padula model, Chinese Wall lattice

Role-Based Access Control: users, roles & permissions, relation to organisational structure, role inheritance, active vs allowed roles, permission conflict, positive and negative permissions, attributes, expressing RBAC policies, managing RBAC

11. Network Security: IP security, Firewalls, Intrusion Detection

12. Security for electronic commerce: SSL, SET

Assessment

COMP4307/5327

2 assignments 40%

written exam 60%

Satisfactory performance in the examination is a requirement for a passing grade

Course Website

<http://www.it.usyd.edu.au/~michaelh>

Text

Kaufman, C., Perlman, R., & Speciner, M., .Network Security, Private Communication in a Public world, 2nd ed., Prentice Hall PTR., 2002

References

Stallings, W., .Cryptography and Network Security: Principles and Practice, 3rd ed., Prentice Hall PTR., 2003

Stallings, W., .Network Security Essentials: Applications and Standards, Prentice Hall, 2000

Kruse, W.G. & Heiser, J.G., Computer Forensics: Incident Response Essentials, Addison Wesley, 2002

M. Hitchens

michaelh@ics.mq.edu.au

July 2003