

Distributed Information System Security

Instructor: Professor Bill Bard

Course Description: This course is intended to acquaint the student with the mathematics, algorithms, and protocols constituting the cryptographic techniques that serve as the essential tools employed in securing today's networked information system environment. Emphasis is placed on examination of security threats in Internet-based distributed systems and the technologies that are being developed and implemented as countermeasures.

Syllabus:

- I. The Distributed Information System Security Problem
 - a. Basic Definitions
 - b. Risk Analysis
 - c. Physical Security
 - d. Network Infrastructure (LAN/MAN/WAN)
 - e. Security Models
 - f. Firewall Techniques

- II. Cryptographic Tools
 - a. Symmetric Key Systems (DES, IDEA, RC4, Blowfish)
 - b. Asymmetric Systems (Diffie-Hellman, RSA, ECC)
 - c. Message Digest Functions (MD5, DSA)
 - d. Key Management
 - e. Privacy Issues (Clipper/Skipjack)

- III. Authentication
 - a. Authentication Requirements
 - b. Authentication Protocols
 - c. Kerberos
 - d. X.509 Certificates
 - e. Public Key Infrastructure

- IV. Message Security
 - a. Digital Signatures (RSA, DSS)
 - b. Electronic Mail Implementations (PGP, S/MIME)
 - c. World Wide Web Transactions (SSL, SET)

- V. System Management
 - a. IPsec

- b. Intrusion Detection Systems
- c. Database Security