

Lecture Outline



- Internet Authentication Applications
 - X.509 (Directory Authentication Services – S/MIME)

and separately

- Ethics

- Recall Digital Certificates
 - Issued by trusted 3rd party (govt. universities, well known security companies)
 - Involves
 - public key encryption
 - Hashing (MD5 and SHA)

- One scheme has become universally accepted for formatting public key certificates: X.509 standard

- X.509 certificates are used in most network security applications – IPsec, SSL, S/MIME ...)

X.509 Certificate Format

Version
Certificate serial number
Algorithm
Issuer Name
Period of validity (not before/ not after)
Subject name (name of user to whom this certificate refers)
Subject's public key info
Issuer unique ID
Subject unique ID
Extensions
Algorithm

Certificate Revocation List

- X.509 provides a format for use in revoking a key before it expires
- Why?
- Each CRL posted to the directory is signed by the issuer
- When a user received a certificate in message, the user must determine whether the certificate has been revoked.
 - The user could check the directory each time a certificate is received
 - OR to avoid delays –
 - maintain a local cache of certificates and lists of revoked certificates

Algorithm
Issuer name
This update date
Next update date
Revoked certificate 1

....
....
....
....
Revoked certificate n

Some Potential Ethical Issues related to Computers and Information Systems

Technology Intrusion	<p>Compromise internal to firm</p> <p>Compromise external to firm</p> <p>Computer surveillance</p> <p>Employee monitoring</p> <p>Hacking</p>
Ownership Issues	<p>Moonlighting</p> <p>Proprietary rights</p> <p>Conflicts of interest</p> <p>Software copyrights – Image copyrights</p> <p>Use of company assets for personal benefit</p> <p>Theft of software and hardware</p>
Legal Issues and Social Responsibilities	<p>Embezzlement, fraud, abuse</p> <p>Accuracy and timeliness of data</p> <p>over-rated system capabilities</p>
Personnel Issues	<p>Sabotage</p> <p>Loyalties</p> <p>Outsourcing</p> <p>Access</p>

Blowing the Whistle

- Where do loyalties lie and why?
- Solutions – internal to company and external
- Internal
- External
 - [ACM Codes of Ethics and Professional Standards](#)
 - [IEEE Code of Ethics](#)
 - [AITP Standard of Conduct](#) (Association of Information Technology Professionals)

Common Themes of Codes

1. Dignity and worth of other people
2. Personal integrity and honesty
3. Responsibility for work
4. Confidentiality of information
5. Public safety, health, and welfare
6. Participation in professional societies to improve standards of the profession
7. The notion that public knowledge and access to technology is equivalent to social power

Where is the emphasis? Are you surprised?

People vs. Machines

- Emphasis on the responsibilities of professional to other people (central meaning of ethics)
- Emphasis on people rather than machines or software
- Generic – would you say?
- Why?