Computer security: intro

6.033 Spring 2007

MASSACHUSETTS
INSTITUTE OF
TECHNOLOGY

Security Module (Ch 11)

- Introduction (section A+D+H)
  - Attaining security is difficult
  - Confidentiality
- Authentication (section C)
- Authentication of principals (section B+E)
- Authorization and Certification (section F+G)
- Ethics and Law (guest lecturer)

Security is hard

- Hackers break into Harrisburgh water system network (Feb)
- Two traffic engineers deny hacking into L.A.'s traffic system (Feb)
- TJX ID theft: 45.7M and counting ... (March)
- Companies are tuning into Web 2.0 but are simultaneously exposing their systems to next generation threats such as Cross site Scripting, Cross Site Request Forgery and Application interconnection issues due to SOA (today)

Security is hard (2006)

- RFID worm created in the lab (March)
- Bank North Phishing (April)
- Microsoft Warns Of Dangerous IE Exploit (March)
- Congress rips DHS, DOD for low cybersecurity grades (March)
- Next step in pirating: Faking a company (yesterday)

Real-world security is hard too

- A prisoner was wrongly released after a fax was received from a grocery store stating that the Kentucky Supreme Court had demanded his release: http://www.cnn.com/2007/US/04/21/wrongly.freed.ap/index.html

Security principles

- Open design:you need all the help you can get
- Economy of mechanism: fewer things to get right
- Minimize secrets: secrets don’t remain secret
- Fail-safe defaults: most users won’t change them
- Least privilege: limit the damage of an accident
- Separation of privilege: dangerous operation should require multiple principals
- Complete mediation: check every operation

A commercial, and in some respects a social doubt has been started within the last year or two, whether or not it is right to discuss so openly the security or insecurity of locks. Many well-meaning persons suppose that the discussion respecting the means for baffling the supposed safety of locks offers a premium for dishonesty, by showing others how to be dishonest. This is a fallacy. Rogues are very keen in their profession, and know already much more than we can teach them respecting their several kinds of roguery.

Rogues knew a good deal about lock-picking long before locksmiths discussed it among themselves, as they have lately done. If a lock, let it have been made in whatever country, or by whatever maker, is not so inviolable as it has hitherto been deemed to be, surely it is to the interest of honest persons to know this fact, because the dishonest are tolerably certain to apply the knowledge practically; and the spread of the knowledge is necessary to give fair play to those who might suffer by ignorance.

It cannot be too earnestly urged that an acquaintance with real facts will, in the end, be better for all parties. Some time ago, when the reading public was alarmed at being told how London milk is adulterated, timid persons deprecated the exposure, on the plea that it would give instructions in the art of adulterating milk; a vain fear, milkmen knew all about it before, whether they practiced it or not; and the exposure only taught purchasers the necessity of a little scrutiny and caution, leaving them to obey this necessity or not, as they pleased.

-- From A.C Hobbs (Charles Tomlinson, ed.), Locks and Safes: The Construction of Locks. Published by Virtue & Co., London, 1853 (revised 1868).

RC4 (or ARC4)

```
byte S[256];
procedure RC4_generate() return key-byte {
    i ← (i + 1) mod 256;
    j ← (j + S[i]) mod 256;
    swap (S[i], S[j]);
    t ← (S[i] + S[j]) mod 256;
    return S[t];
```

Initialization from a seed

```
procedure RC4_init (seed)
    for i from 0 to 255 do {
            S[i] ← i;
            K[i] ← seed[i];
    }
    j ← 0;
    for i from 0 to 255 do {
            j ← (j + S[i] + K[i]) mod 256;
            swap( S[i], S[j]);
    }
    i ← 0; j ← 0;
```