College of Information Studies

University of Maryland Hornbake Library Building College Park, MD 20742-4345

Information Security

Session 24

INST 301

Introduction to Information Science

Ownership

- Who has the right to use a system?
  - A server, the data, the Internet?
- Who establishes this policy? How?
  - What equity considerations are raised?
- Can someone else deny access?
  - Denial of service attacks
- How can denial of service be prevented?
  - Who can gain access and what can they do?

Authentication

- Used to establish identity
- Two types
  - Physical (Keys, badges, cardkeys, thumbprints)
  - Electronic (Passwords, digital signatures)
- Two-factor authentication

Good Passwords

- Long enough not to be guessed
  - Programs can try every combination of 5 letters
- Not in the dictionary
  - Programs can try every word in a dictionary
    - every proper name, every pair of words, every date, every …
- Mix upper case, lower case, numbers
- Change it often
- Reuse creates risks
  - Abuse, multiple compromise

Authentication Attacks

- Brute force
- Guessing
- “Phishing”
- Impersonation
- Theft

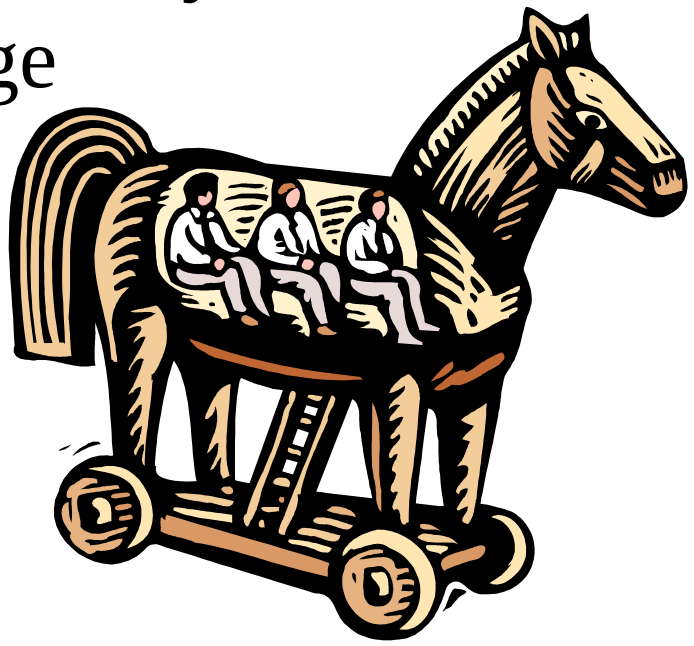
Viruses

- Platform dependent
- Typically binary
- Needs an execution path
  - Autoexecution, authorized execution, buffer overflow
- Most effective when not previously known
  - “Zero-day exploit”

Trojan Horse

- Malicious program with undesired capabilities
  - Log key strokes and sends them somewhere
  - Create a “back door” administrator logon

- Spyware: reports information about your activity without your knowledge



Access Control Issues

- Protect system administrator access
  - Greater potential for damaging acts
  - What about nefarious system administrators?

- Firewalls
  - Prevent unfamiliar packets from passing through
  - Protects against application weaknesses

Denial of Service Attacks

- Virus
- Botnet
  - Activate on command
- Worm
  - Self-replicating

Critical Infrastructure Protection

- Telecommunications
- Banking and finance
- Energy
- Transportation
- Emergency services
- Food and agriculture
- Water
- Public health
- Postal and shipping
- Defense industrial base
- Hazardous materials

SCADA: Supervisory Control and Data Acquisition

Symmetric Key Encryption

Same key used both for encryption and decryption

Alice

Bob

Asymmetric Key Encryption

Different keys used for encryption and decryption

Alice

Bob's public key

Bob's private key

Bob

Plain text → Encrypt → Cipher text → **Insecure channel** → Decrypt → Plain text

eavesdropper

eavesdropper

eavesdropper

Asymmetric Key Encryption

- Key = a large number (> 1024 bits)
  - Public key: known by all authorized encoders
  - Private key: known only by decoder
- One-way mathematical functions
  - “Trapdoor functions”
    - Like mixing paint (easy to do, hard to undo)
  - Large numbers are easy to multiply, hard to factor
- Importance of longer keys
  - Keys < 256 bits can be cracked in a few hours
  - Keys > 1024 bits presently effectively unbreakable

RSA “Public Key” Encryption

```
pri
spl
`ec                                    z;
[(p                                    >)]}
\Es                                    2/d0
<X-                                    lMlN
/ds
```

Until 1997 – Illegal to show this slide to non-US citizens!

Digital Signatures

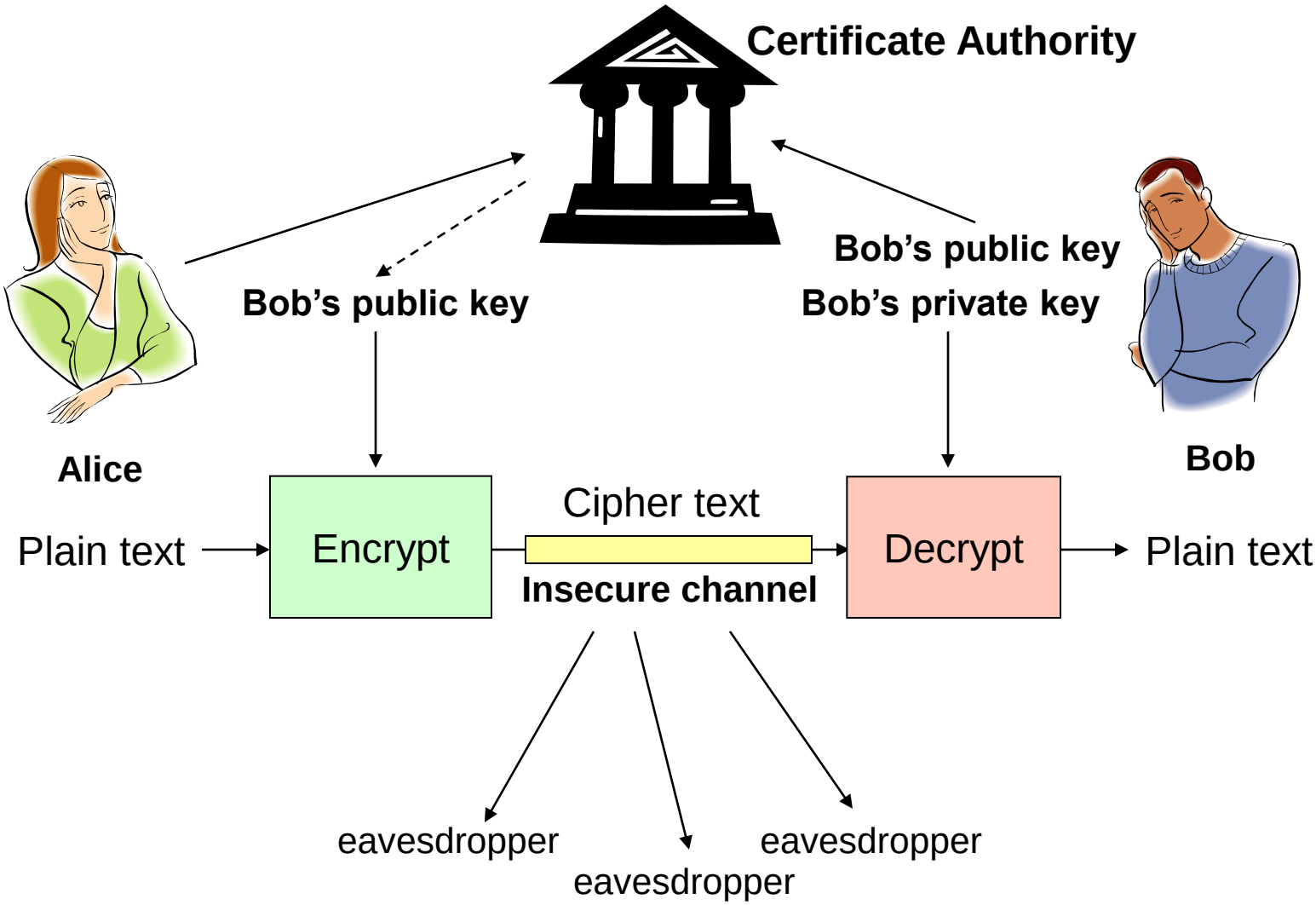
- Alice “signs” (encrypts) with her private key
  - Bob checks (decrypts) with her public key
- Bob knows it was from Alice
  - Since only Alice knows Alice’s private key
- Non-repudiation: Alice can’t deny signing message
  - Except by claiming her private key was stolen!
- Integrity: Bob can’t change message
  - Doesn’t know Alice’s Private Key

Key Management

- Pubic announcement of public key
  - e.g., append public key to the end of each email
  - But I can forge the announcement

- Establish a trusted “certificate authority”
  - Leverage “web of trust” to authenticate authority
  - Register public key with certificate authority

Certificate Authority



What Goes Wrong?

- Consider the Risks Digest articles you read
  - http://catless.ncl.ac.uk/Risks
- Focus on unexpected consequences
- Try to articulate the **root** cause
  - Not just the direct cause

Some Practical Tips

- Keep anti-virus software current
- Keep software updates current
- Change default settings
- Be wary of anything free