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

Information Management

Week 13

LBSC 690

Information Technology

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

Managing Complex Systems

- Critical system availability
  - Why can’t we live without these systems?
- Understandability
  - Why can’t we predict what systems will do?
- Nature of bugs
  - Why can’t we get rid of them?
- Auditability
  - How can we learn to do better in the future?

Agenda

- Questions
- Ownership
- Identity
- Privacy
- Integrity

Equitable Access

- Computing facilities
  - Hardware, software
- Networks
  - Speed, continuity, access points
- Information sources
  - Per-use fee vs. subscription vs. advertising
  - Language
- Skills
  - System, access strategies, information use

Ownership

- Who has the right to use a computer?
  - Who has a right to use 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?

Justifications for Limiting Use

- Parental control
  - Web browsing software, time limits
- Intellectual property protection
  - Copyright, trade secrets, privilege
- National security
  - Classified material
- Censorship

Techniques for Limiting Use

- Access control
  - Monolithic, multilevel
- Copy protection
  - Hardware, software
- Licensing
  - Shrinkwrap, shareware, GPL, creative commons
- Digital watermarks
  - Provide a basis for prosecution

Fair Use Doctrine

- Balance two desirable characteristics
  - Financial incentives to produce content
  - Desirable uses of existing information
- Safe harbor agreement
  - Book chapter, magazine article, picture, …
- Developed in an era of physical documents
  - Perfect copies/instant delivery alter the balance

Recent Copyright Laws

- Copyright Term Extension Act (CTEA)
  - Ruled constitutional (Jan 2003, Supreme Court)
- Digital Millennium Copyright Act (DMCA)
  - Prohibits circumvention of technical measures
  - Implements WIPO treaty database protection

The Pornography Debate

- Communications Decency Act (CDA)
  - Ruled unconstitutional (1997, Supreme Court)
- Child Online Protection Act (COPA)
  - Enforcement blocked (March 2007, 3rd Circuit)
- Children's Internet Protection Act (CIPA)
  - Ruled constitutional (June 2003, Supreme Court)
  - Applies only to E-Rate and LSTA funds

Filtering Technology

- Any individual approach is imperfect
- Term-based techniques
  - Recall/precision tradeoff
- Image-based techniques
- Behavior-based techniques
  - Clickstreams
- Manual whitelists and blacklists
  - Expensive, time lag

Denial of Service Attacks

- Viruses
  - Platform dependent
  - Typically binary
- Flooding
  - Worms
  - Zombies
  - Chain letters

Viruses

- Computer programs able to attach to files
- Replicates repeatedly
  - Typically without user knowledge or permission
- Sometimes performs malicious acts

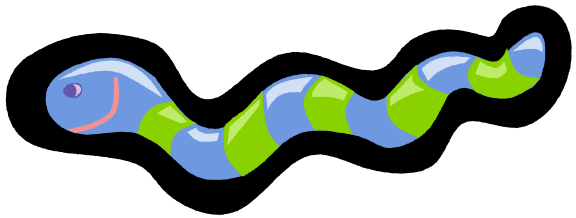
Viruses

- 1988: Less than 10 known viruses
- 1990: New virus found every day
- 1993: 10-30 new viruses per week
- 1999: 45,000 viruses and variants

Worms

- Self-reproducing program that sends itself across a network
  - Virus is dependent upon the transfer of files
  - Worm spreads itself

- SQL slammer worm (January 25, 2003) claimed 75,000 victims within 10 minutes



"On the Internet, nobody knows you're a dog."

Identity

- Establishing identity permits access control
- What is identity in cyberspace?
  - Attribution
    - When is it desirable?
  - Impersonation
    - How can it be prevented?
- Forgery is remarkably easy
  - Just set up your mailer with bogus name and email

Authentication

- Used to establish identity
- Two types
  - Physical (Keys, badges, cardkeys, thumbprints)
  - Electronic (Passwords, digital signatures)
- Protected with social structures
  - Report lost keys
  - Don’t tell anyone your password
- Use SSH to defeat password sniffers

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, pair of words, date, every …
- Mix upper case, lower case, numbers
- Change it often
- Reuse creates risks
  - Abuse, multiple compromise

Authentication Attacks

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

Access Control Issues

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

- Firewalls
  - Prevent unfamiliar packets from passing through
  - Makes it harder for hackers to hurt your system

We Already Knew a Lot About You

- Governments have information about life events
  - Birth and death
  - Marriage and divorce
  - Licenses (e.g., drivers)
  - Property and taxes

- Business exchange information about transactions
  - How you commute to work
  - What cereal you eat
  - Where you like to go for vacation
  - What hobbies you have

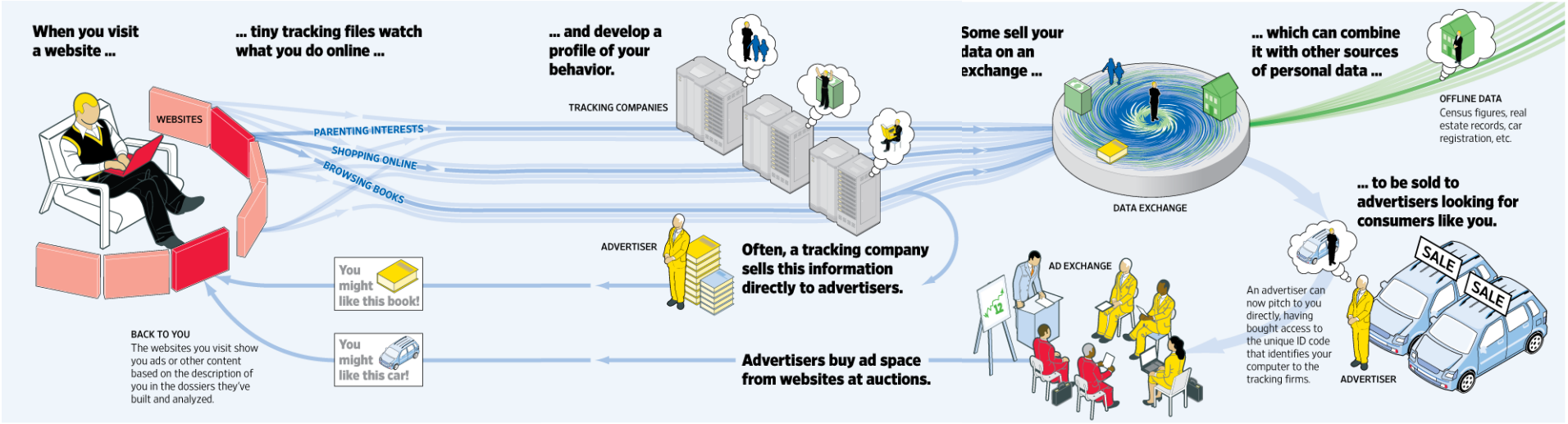
We Can See Even More Online

- Web tracking
  - Browser data, clickthrough, cookies, …
- Packet sniffers
  - Detect passwords, reconstruct packets, …
- Law enforcement
  - Carnivore (US), RIP (UK), …
- National security
  - Echelon (US), SORM (Russia), …

Tracking Internet Activity

ISP logs
IP address
Firewalls
Cookies
Browser history
Spyware
Packet sniffing
Intercepting e-mails
Monitoring news groups
Monitoring chat rooms
Spoofed web sites
Wiretaps

The Tracking Ecosystem



http://wsj.com/wtk

Privacy vs. Anonymity

Anonymity

- Serves several purposes
  - Sensitive issues on discussion groups
  - Brainstorming
  - Whistleblowers
  - Marketing (“Spam”)
- Common techniques
  - Anonymous remailers
  - Pseudonyms

Practical Obscurity

- A lot of government-collected information is public record
- Previously shielded by “practical obscurity”
  - Records were hard to access
- Not so with the Internet

Ideals in Tension

- Establishing identity permits access control
- Yet people don't want to be tracked
- How do you provide accountability?
  - People's behavior change when no one is watching

Whenever a conflict arises between privacy and accountability, people demand the former for themselves and the latter for everybody else.

The Transparent Society by David Brin

Privacy

- What privacy rights do computer users have?
  - On email?
  - When using computers at work? At school?
  - What about your home computer?
- What about data about you?
  - In government computers?
  - Collected by companies and organizations?
- Does obscurity offer any privacy?

Privacy Protection

- Privacy Act of 1974
  - Applies only to government records
- TrustE certification guidelines
  - Site-specific privacy policies
  - Federal Trade Commission enforcement
- Organizational monitoring

Symmetric Key Encryption

Same key used both for encryption and decryption

Alice

Bob

key

key

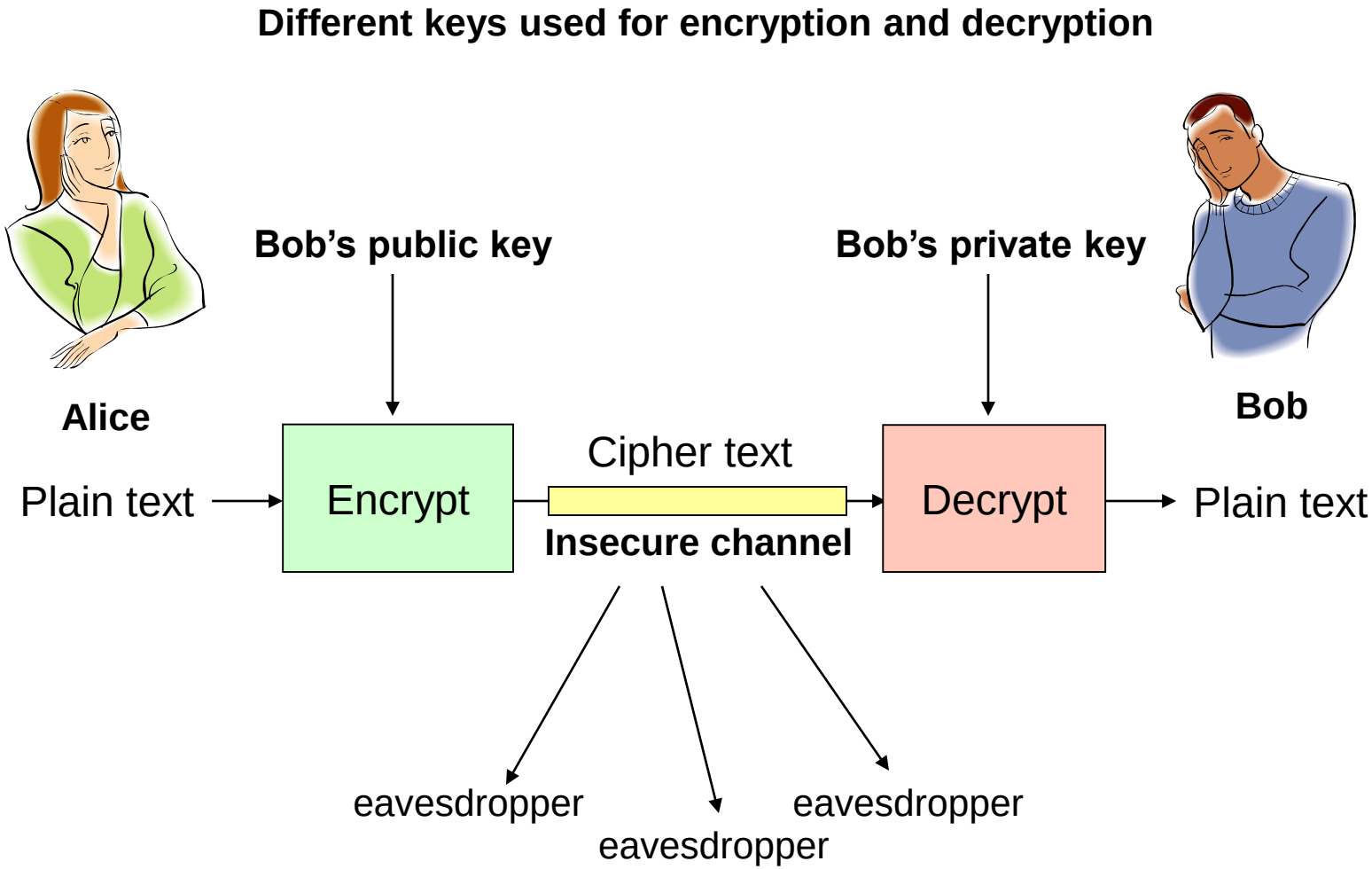
Plain text → Encrypt → Cipher text → **Insecure channel** → Decrypt → Plain text

eavesdropper

eavesdropper

eavesdropper

Asymmetric Key Encryption



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

The Dark Side of Encryption

- Encryption is a double-edged sword
  - The ability to keep secrets facilitates secure commercial transactions
  - But bad guys can use encryption to keep secrets…
- Can be cracked by "authorized parties"?
  - How should that ability controlled?

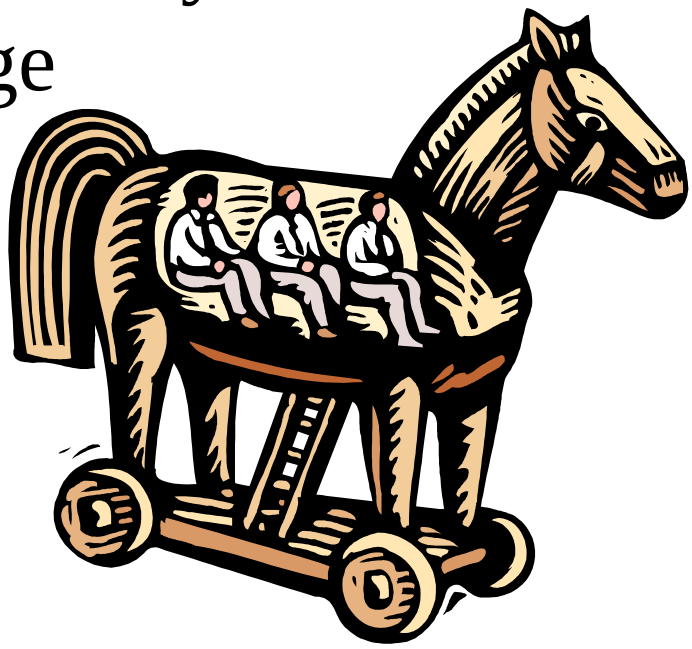
RSA “Public Key” Encryption

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

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

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
- Doesn’t (necessarily) replicate



Privacy in a Post 9/11 World

The Professional Association of Diving Instructors (PADI), which certifies about 65 percent of the nation's divers, gave the FBI a computer file containing the names of more than 2 million certified divers in May 2002.

Airlines have handed large amounts of passenger data over to the government (most voluntarily).

Surveillance Law

- USA PATRIOT Act
  - Access to business records
  - Internet traffic analysis (with a court order)
- Foreign Intelligence Surveillance Act (FISA)
  - Secret court for monitoring foreign communications
  - Special protections for citizens/permanent residents

Real-Time Local Surveillance

- Built-in features of standard software
  - Browser history, outgoing email folders, etc.
- “Parental control” logging software
  - ChatNANNY, Cyber Snoop, FamilyCAM, …
- Personal firewall software
  - ZoneAlarm, BlackIce, …

Real-Time Centralized Surveillance

- Proxy server
  - Set up a Web server and enable proxy function
  - Configure all browsers to use the proxy server
  - Store and analyze Web server log files
- Firewall
  - Can monitor all applications, not just the Web

Forensic Examination

- Scan for files in obscure locations
  - Find-by-content for text, ACDSee for pictures, …
- Examine “deleted” disk files
  - Norton DiskDoctor, …
- Decode encrypted files
  - Possible for many older schemes

Integrity

- How do you know what's there is correct?
  - Attribution is invalid if the contents can change
- Access control would be one solution
- Encryption offers an alternative

Digital Signatures

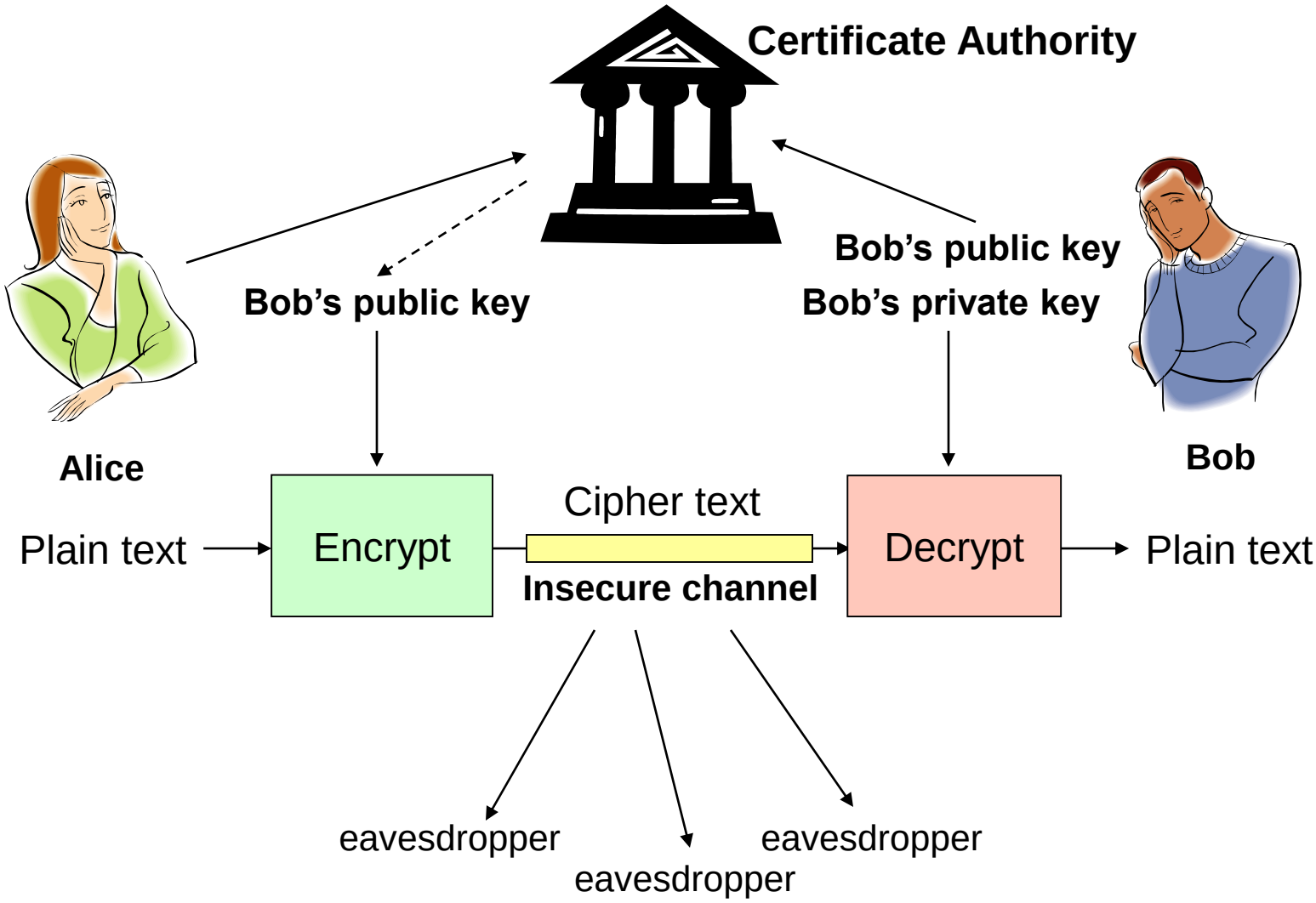
- Alice “signs” (encrypts) with her private key
  - Bob checks (decrypts) with her public key
- Bob knows it was from Alice
  - Since only Alice knows Alice’s private key
- Non-repudiation: Alice can’t deny signing message
  - Except by claiming her private key was stolen!
- Integrity: Bob can’t change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

Key Management

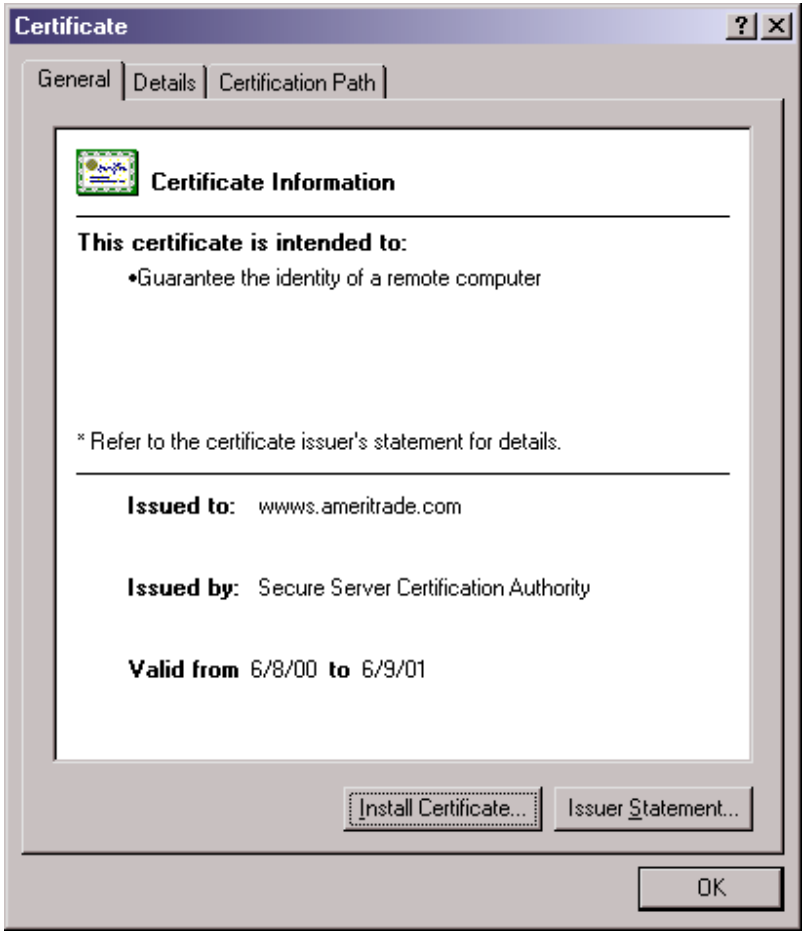
- Pubic announcement of public key
  - e.g., append public key to the end of each email
  - But I can forge the announcement

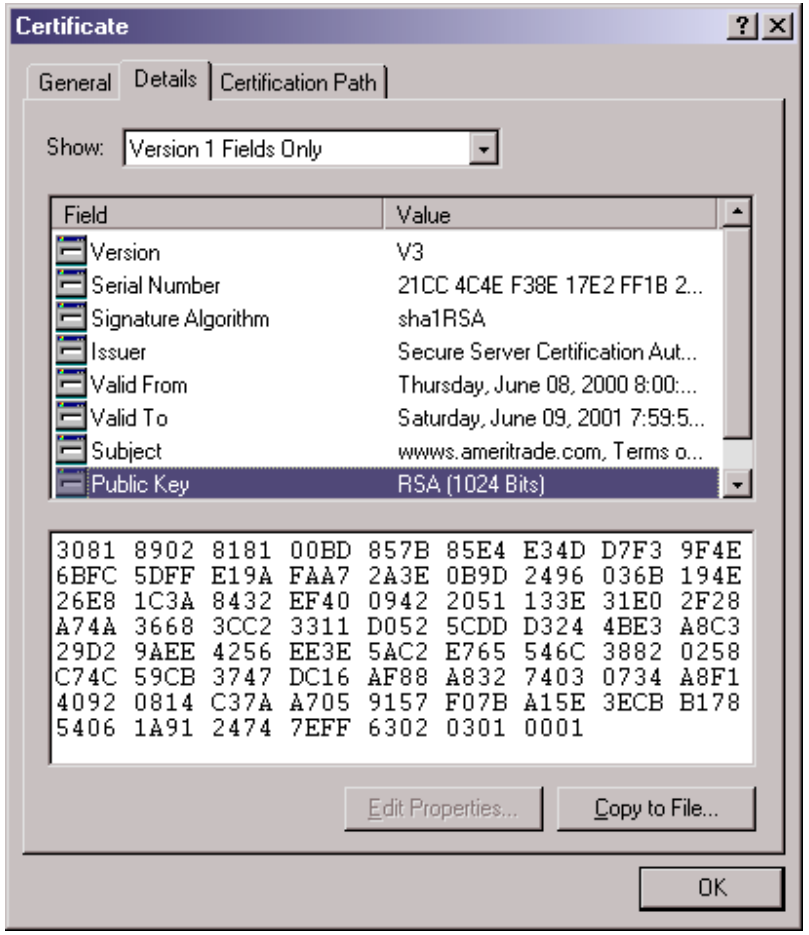
- Establish a trusted “certificate authority”
  - Leverage “web of trust” to authenticate authority
  - Register public key with certificate authority

Certificate Authority



Certificates: Example





Acceptable Use Policies

- Establish policies
- Authenticate
- Authorize
- Audit
- Supervise

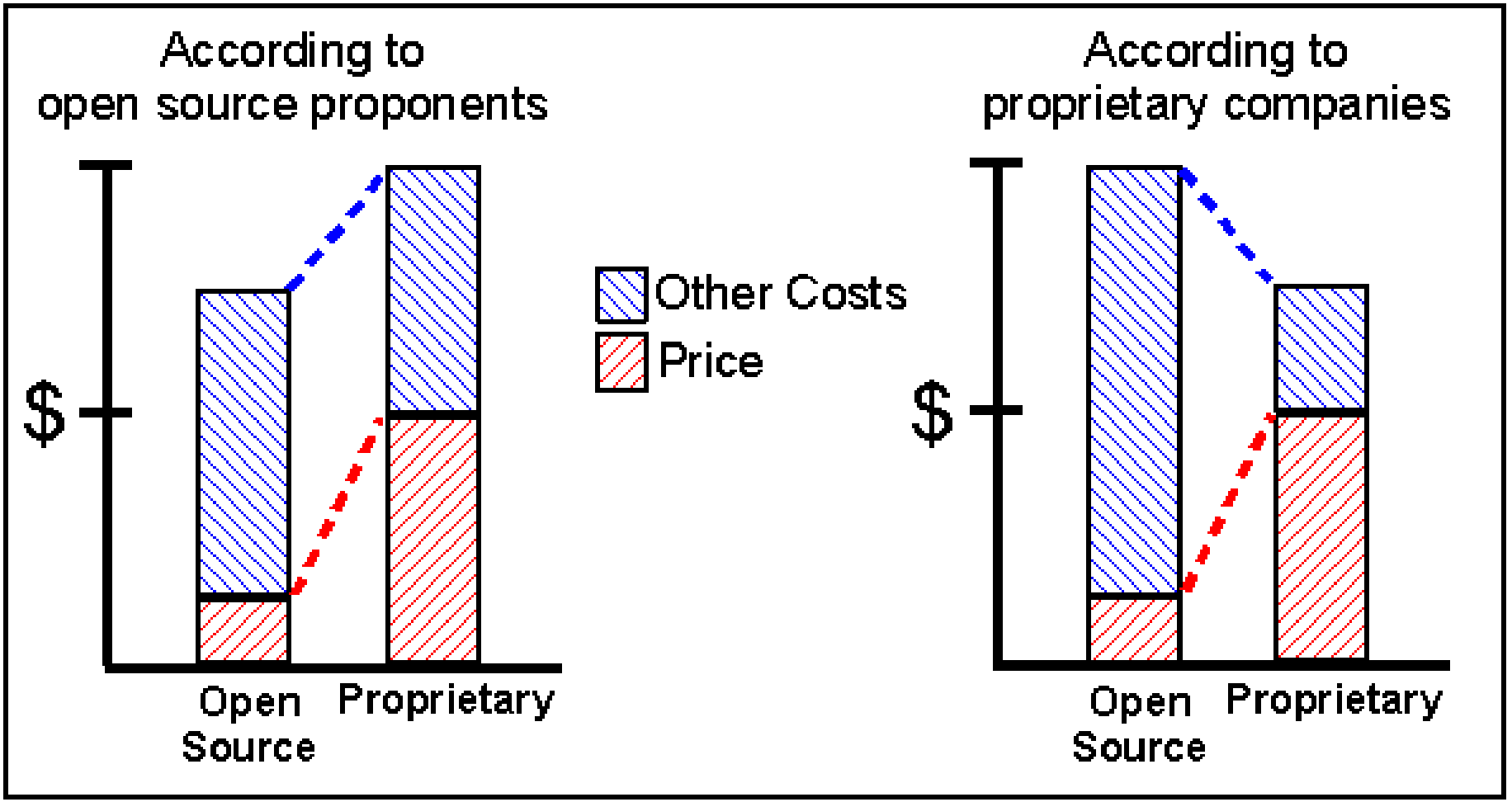
Practical Tips

- Keep anti-virus software current
- Keep software “patches” current
- Change default settings
- Be wary of anything free

Total Cost of Ownership

- Planning
- Installation
  - Facilities, hardware, software, integration, migration, disruption
- Training
  - System staff, operations staff, end users
- Operations
  - System staff, support contracts, outages, recovery, …

Total Cost of Ownership



Some Examples

	Proprietary	**Open Source**
Operating system	Windows XP	Linux
Office suite	Microsoft Office	OpenOffice
Image editor	Photoshop	GIMP
Web browser	Internet Explorer	Mozilla
Web server	IIS	Apache
Database	Oracle	MySQL

Some Opinions

- Bill Gates on Linux (March, 1999):
  - "I don't really think in the commercial market, we'll see it in any significant way."
- Microsoft SEC filing (January, 2004):
  - "The popularization of the open source movement continues to pose a significant challenge to the company's business model"

Open Source “Pros”

- More eyes ⇒ fewer bugs
- Iterative releases ⇒ rapid bug fixes
- Rich community ⇒ more ideas
  - Coders, testers, debuggers, users
- Distributed by developers ⇒ truth in advertising
- Open data formats ⇒ Easier integration
- Standardized licenses

Open Source “Cons”

- Communities require incentives
  - Much open source development is underwritten
- Developers are calling the shots
  - Can result in feature explosion
- Proliferation of “orphans”
- Diffused accountability
  - Who would you sue?
- Fragmentation
  - “Forking” may lead to competing versions
- Little control over schedule

Iron Rule of Project Management

- You can control any **two** of:
  - Capability
  - Cost
  - Schedule

- Open source software takes this to an extreme

Open Source Business Models

- Support Sellers

  Sell distribution, branding, and after-sale services.

- Loss Leader

  Give away the software to make a market for proprietary software.

- Widget Frosting

  If you're in the hardware business, giving away software doesn't hurt.

- Accessorizing

  Sell accessories:
  books, compatible hardware, complete systems with pre-installed software

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

National Cyberspace Strategy

- Response system
  - Analysis, warning, response, recovery
- Threat and vulnerability reduction
- Awareness and training program
  - Return on investment, best practices
- Securing government systems
- International cooperation

Summary

- Systems analysis
  - Required for complex multi-person tasks
- User-centered design
  - Multiple stakeholders complicate the process
- Implementation
  - Architecture, open standards, …
- Management
  - Typically the biggest cost driver

The Grand Plan