LBSC 690: Week 12

Security and Privacy

Jimmy Lin
College of Information Studies
University of Maryland

Monday, April 23 , 2007

Contributing sources: David Evans (UVA)

Agenda

- Encryption
- Identity, privacy, and anonymity
- Security

Encryption Concepts

Plain text → Encrypt → Cipher text → Decrypt → Plain text

Insecure channel

eavesdropper eavesdropper eavesdropper

Early Forms of Encryption

Caesar Cipher

Jefferson Cipher Wheel

German Enigma Machine

Symmetric Key Encryption

Same key used both for encryption and decryption

key key

Plain text → Encrypt → Cipher text → Decrypt → Plain text

Insecure channel

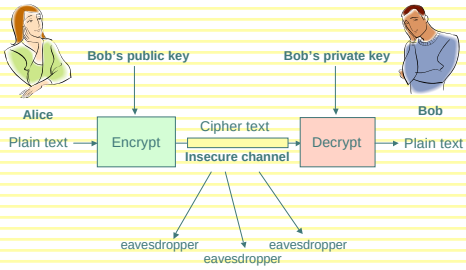
eavesdropper eavesdropper eavesdropper

Symmetric Key Encryption

- What's the fatal flaw?

Asymmetric Key Encryption

Different keys used for encryption and decryption



Asymmetric Key Encryption

- Key = a large number (> 1024 bits)
  - Public key – known by others, for encryption
  - Private key – known only by self, for decryption
- Alice and Bob don't have to exchange keys

How does encryption work?

- One-way mathematical functions
  - "trapdoor functions"
  - Large numbers are easy to multiply, but hard to factor
  - Like mixing paint: easy to do, hard to undo
- Want more security? Pick longer keys
  - Keys less than 256 bits can be cracked within a few hours by a personal computer
  - Keys greater than 1024 bits practically unbreakable

RSA in Perl

- First and most famous asymmetric key encryption algorithm

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

Digital Signatures

- Public key cryptography in reverse
- 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 key was stolen!
- Integrity: Bob can't change message
  - Doesn't know Alice's Private Key

Key Management

- Meet secretly
  - Alice and Bob meet and swap public keys
  - Not practical!

If you can arrange to meet, might as well use symmetric keys. Defeats the point of asymmetric key encryption.

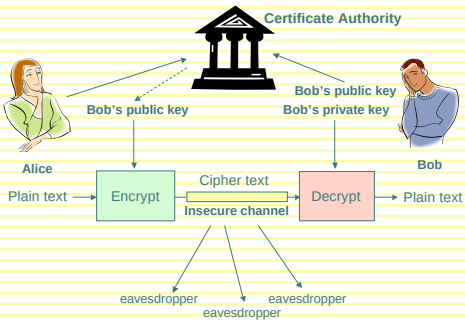
- Publish announcement
  - For example, Bob appends his public key to the end of his email

Easy for someone to pretend to be Bob!

Certificate

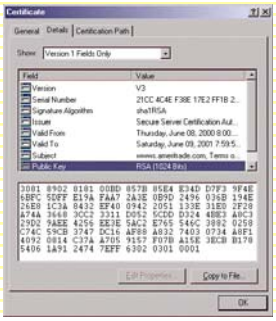
- Combination of identity and public key digitally signed by a trusted third party
  - Certificate authorities
- "Web of trust"

Certificate Authority



Certificates: Example

Certificates: In Detail



Different Types of Attacks

- Brute force
- False identity
- Social attacks
  - "Phishing"

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 the government?

Identity, Privacy, Anonymity

Or do they?

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

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
- Susceptible to social engineering

Good Passwords

- Long enough not to be guessed
  - Programs can try every combination of 4 letters
- Not in the dictionary
  - Programs can try every word in a dictionary
  - And every date, and every proper name, ...
  - And even every pair of words
- Mix upper case, lower case, numbers, etc.
- Change it often and use one for each account
- Tension between security and convenience

Is Privacy an Illusion?

Are you being watched?

- Where?
  - At home?
  - At work?
  - In a shopping mall?
  - In a parking garage?
  - In the library?
- Do they have the right?

Tracking Internet Activity

1) ISP logs
2) IP address
3) Firewalls
4) Cookies
5) Browser history
6) Spyware
7) Packet sniffing
8) Intercepting e-mails
9) Monitoring news groups
10) Monitoring chat rooms
11) Booby-trapped web sites
12) Wiretaps

The Government Knows

- The government stores a lot of information about life events:
  - Birth
  - Getting your driver license
  - Getting married
  - Getting divorced
  - Buying a house
  - Paying taxes
  - Dying

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

Businesses Know

- Business know a lot about you:
  - How you commute to work
  - What cereal you eat
  - Where you like to go for vacation
  - What hobbies you have
- And they sell each other this information

Databases

- Many organizations collect information about different facets of your life
- What happens when they start piecing the facets together?
  - Is anonymity even possible?
  - "They" are already doing this!

The Post 9/11 World

- The public (?) will choose security over privacy

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).

Etc.

- The Patriot Act gives the government broad powers

Continual Erosion of Privacy

- Slippery slope into Big Brother?
- What can you do?

Security

- Used to be simple…
- Not so in a networked environment
- Viruses and other nasty stuff
  - 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
  - Today: ??

Viruses

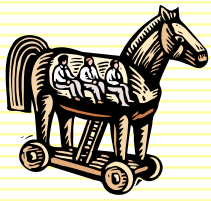
- Fragments of computer programs capable of attaching to disks or other files
  - Replicates itself repeatedly, typically without user knowledge or permission
  - Often does nothing, but sometimes actively performs malicious acts

Worms

- A self-reproducing programs that travels independently across networks
- Reproduction differences:
  - A virus is dependent upon the transfer of files between machines to spread
  - A worm can run completely independently and spread of by itself through network connections
- Famous example:
  - SQL slammer worm (January 25, 2003) claimed 75,000 victims within 10 minutes: Internet brought to a halt

Trojan Horse

- A malicious program that pretends to be a benign application
  - Examples: logs key strokes and sends somewhere; creates a "back door"
  - Usually doesn't replicate



Spyware and Adware

- Spyware: software that sits on your machine and reports information about your activity to a third party without your knowledge
  - How does spyware get onto your computer?
- Adware: software that display annoying advertisement

Denial of Service Attacks

- An attack on a computer network that causes a loss of service to users
- Typical perpetrated by flooding the host with an overwhelming number of packets
  - Consumption of resources: CPU, bandwidth, etc.

Practical Tips

- Be wary of anything free
- Always have updated anti-virus software
- Change default settings
- Choose good passwords
- Keep software patched