Software & Security

...Plan for next hour...

- Black hats, crime, software, the Internet, *scary* things
- Subversion, protocols, complexity of problem
- Secrecy, simple and symmetric key systems
- White hats, security guidelines, standards

“Black hats, crime & punishment”

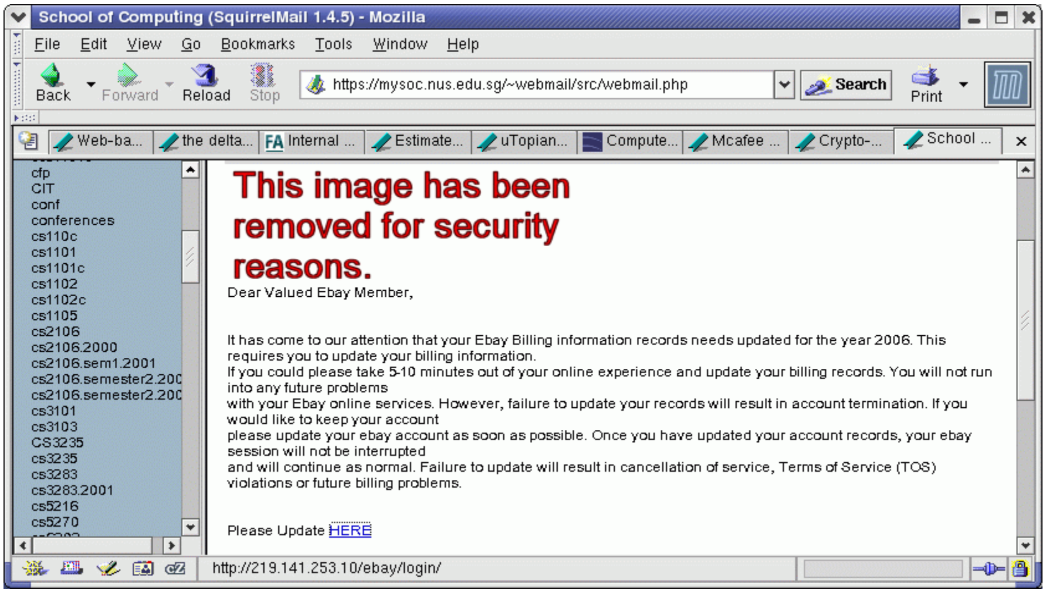
- In 2004, the FBI estimates that the level of cybercrime in the US in 2004 was about US$400 billion.

In July-August 2004, the FBI reported only 110 convictions for computer-related crimes.

- 250/500 companies admitted losses in a 2004 CSI/FBI survey ($140 million). Credit card theft reported by US credit card companies was over US$18 billion in 2004.

...increasing reliance on computer-based commerce... situation will only get worse ...

Firstly: human factors...


School of Computing (SquirrelMail 1.4.5) - Mozilla
File Edit View Go Bookmarks Tools Window Help
Back Forward Reload Stop
https://mysoc.nus.edu.sg/~webmail/src/webmail.php
Search
Print
Web-ba... the delta... Internal ... Estimate... uTopian... Compute... Mcafee ... Crypto-... School ...
cfp
CIT
conf
conferences
cs110c
cs1101
cs1101c
cs1102
cs1102c
cs1105
cs2106
cs2106.2000
cs2106.sem1.2001
cs2106.semester2.200
cs2106.semester2.200
cs3101
cs3103
CS3235
cs3235
cs3283
cs3283.2001
cs5216
cs5270
http://219.141.253.10/ebay/login/

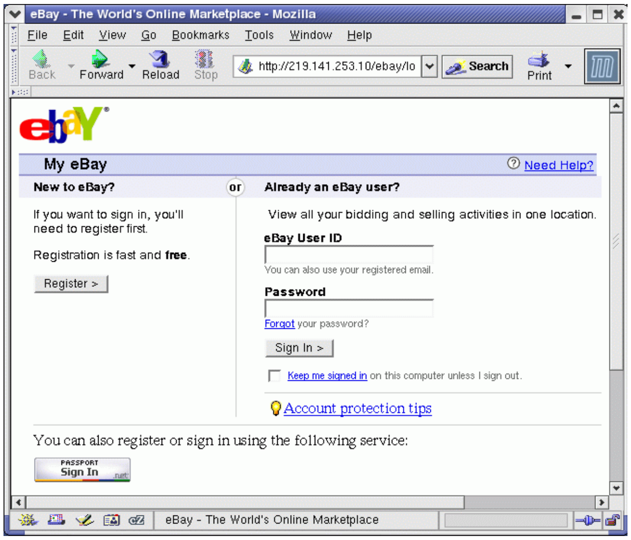
This image has been removed for security reasons.

Dear Valued Ebay Member,

It has come to our attention that your Ebay Billing information records needs updated for the year 2006. This requires you to update your billing information.
If you could please take 5-10 minutes out of your online experience and update your billing records. You will not run into any future problems
with your Ebay online services. However, failure to update your records will result in account termination. If you would like to keep your account
please update your ebay account as soon as possible. Once you have updated your account records, your ebay session will not be interrupted
and will continue as normal. Failure to update will result in cancellation of service, Terms of Service (TOS) violations or future billing problems.

Please Update HERE

Phishing...


eBay - The World's Online Marketplace - Mozilla
File Edit View Go Bookmarks Tools Window Help
Back Forward Reload Stop
http://219.141.253.10/ebay/lo
Search
Print
ebaY
eBay - The World's Online Marketplace

My eBay

Need Help?

New to eBay? or **Already an eBay user?**

If you want to sign in, you'll need to register first.

Registration is fast and **free**.

Register >

View all your bidding and selling activities in one location.

eBay User ID

You can also use your registered email.

Password

Forgot your password?

Sign In >

□ Keep me signed in on this computer unless I sign out.

Account protection tips

You can also register or sign in using the following service:

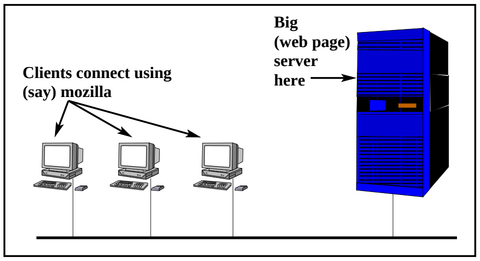
PASSPORT Sign In .net

Crimes on the Internet

- Protection rackets (Pay me or I'll kill your web server)
- Fraud (1 in 10 Asian Internet deals are fraudulent)
- Money laundering/speculation and outright theft

> Question: Why so much?
> Answer: Software complexity leaving loopholes you can drive a truck through... Systems only as strong as the weakest link...

Attack! Attack! Attack!



Consider BAD clients, who connect to web server and manage to install their own software on the server (to steal, corrupt...).

Consider BAD servers, who deliver malicious applets back to clients (to steal, corrupt...).

Commentary

- The attacks just given are very simple, and are precisely the ones exploited over and over again.

- Note that your own PCs provide many such services when connected to a network. The web server is just one example of a server.

The good news?

- The most common remote attack on software is to exploit a stack/buffer overflow flaw. Such attacks can lead to subversion of the software as just shown - the computer ends up running a program provided by the attacker, not the original software.

Good news!

The good news is that Java programs are unlikely to succumb to stack/buffer overflow attacks.

The bad news?

Java programs and applets run on computers which have operating systems and other programs which are very likely to succumb to this form of attack.

1. It is likely that someone can subvert the OS, or some other program on your computer.

2. In addition, your programs will interact with other programs possibly using a communication protocol of some sort. Without careful design, it is likely that someone can subvert the protocol.

“Subversion”
For our systems we expect...

✔ **Confidentiality** - secret things remain secret

✔ **Integrity** - meaning of data is preserved

✔ **Availability** - the system always ready

✔ **Accountability** - logs kept

But both the OS and communcations can be subverted...

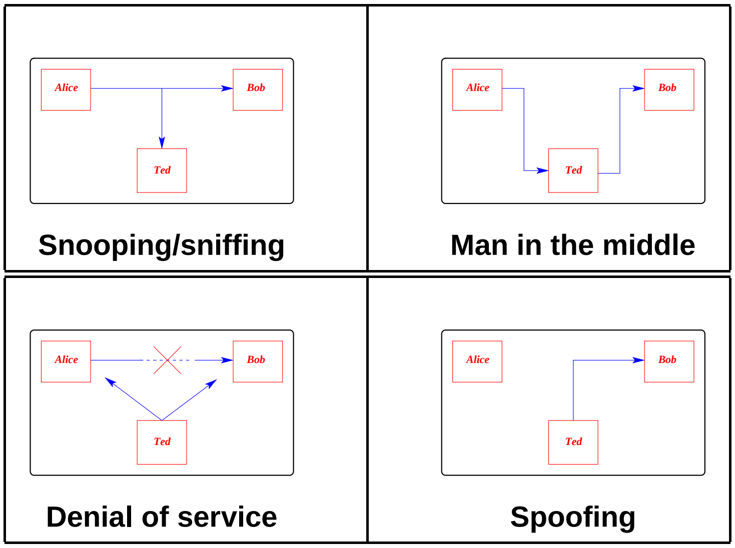
Subvert the OS?

Consider WinXP in August this year:

1. August 9, 2005 MS05-038: A remote, unauthenticated attacker may be able to execute arbitrary code...
2. August 15, 2005 MS05-039: A remote, ... (as above)
3. August 24, 2005 MS05-043: A remote, ... (as above)

3 different bugs, and delays of 1 to 4 months between discovery and the advisories.

Subvert the protocol[1]?



Snooping/sniffing

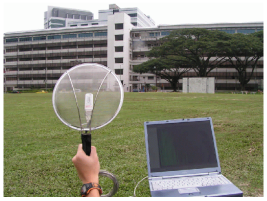
Man in the middle

Denial of service

Spoofing

[1] A protocol is the set of rules or methods by which two programs interact.

Subversion is easy...



It is easy to snoop on WiFi networks

PDAs/phones not exempt
(Ex: CommWarrior)

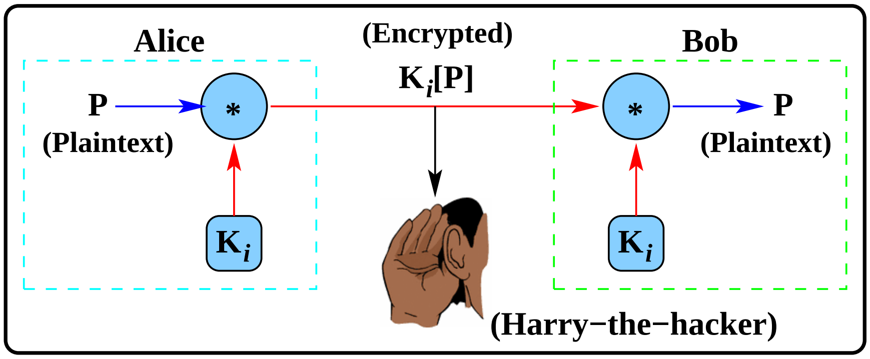
Privacy over communication links would be useful...

“Secrecy”
Messages, locks, keys (Encryption)

To ensure privacy in our messages, we can imagine taking our communications/messages and locking them up:

Note: the key has to be sent as well, and since the messages (and keys) can be recorded for reuse by a bad guy, s/he could later decrypt a previously sent message.

Messages, locks, keys (Encryption)



Alice

(Encrypted)

Bob

P

(Plaintext)

*

$K_i[P]$

*

P

(Plaintext)

K_i

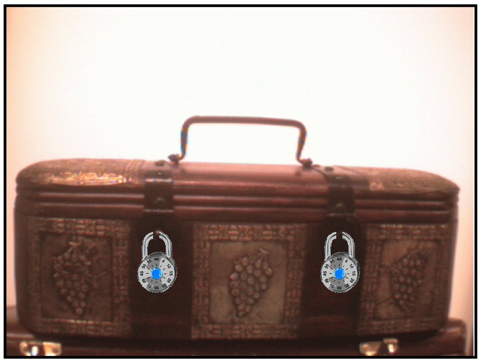
K_i

(Harry−the−hacker)

The encrypted message can be decrypted by anyone who has K_i, so we have a key distribution problem...

If we have time...

Consider this box:



Can you see a way to avoid distributing keys?

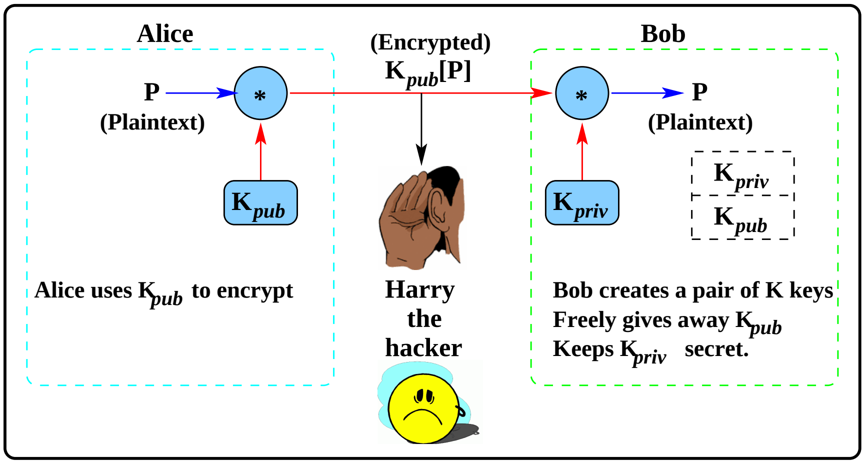
Symmetric and Asymmetric keys

- The keys we have just used are symmetric. That is, you use the same, or equivalent[2] pairs of keys to encode and decode.

- About 30 years ago, researchers discovered a way to use two different keys. If you know one of the keys, it is very difficult to find the other. The method relies on the difficulty of factoring a large composite number. These are asymmetric keys.

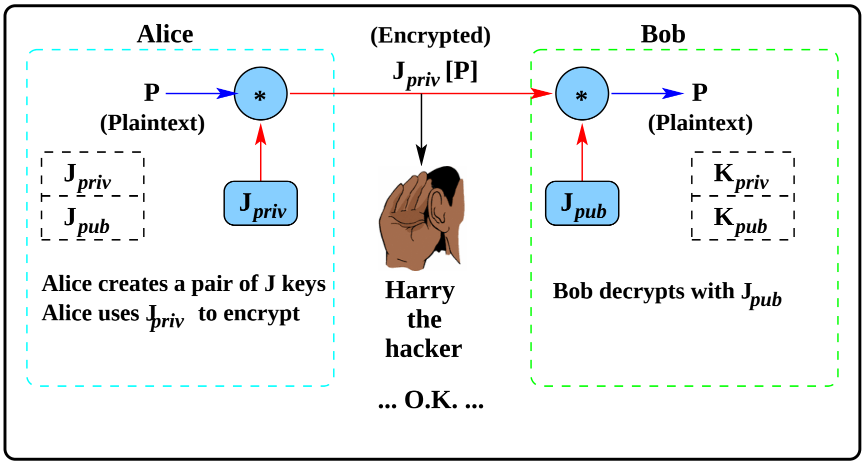
[2] If you know the encoding key you can discover the decoding key.

RSA: encryption



Alice knows that only Bob can decrypt message $K_{\text{pub}}[P]$.

RSA: authentication



Alice

(Encrypted)

Bob

P

J_{priv} [P]

P

(Plaintext)

(Plaintext)

J_{priv}

J_{pub}

J_{priv}

J_{pub}

K_{priv}

K_{pub}

Alice creates a pair of J keys

Alice uses J_{priv} to encrypt

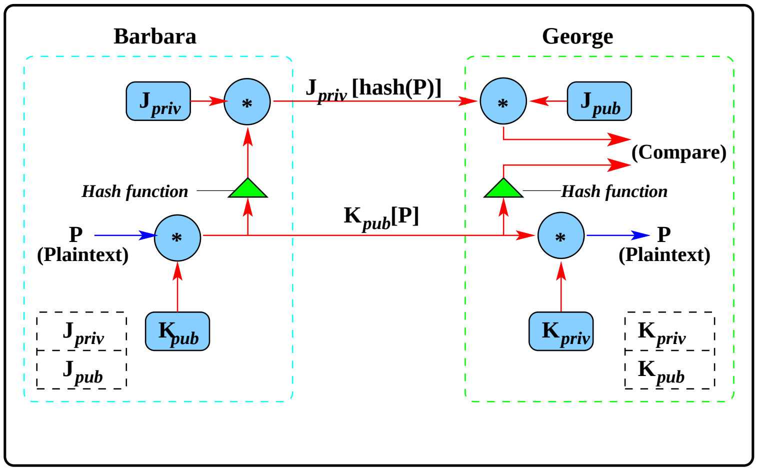
Harry the hacker

Bob decrypts with J_{pub}

... O.K. ...

Bob (and everybody) knows that only Alice could have encrypted $J_{\mathrm{priv}}[P]$.

RSA: signatures



Barbara

George

J_{priv}

J_{priv} [hash(P)]

J_{pub}

(Compare)

Hash function

Hash function

P (Plaintext)

K_{pub}[P]

P (Plaintext)

J_{priv}

J_{pub}

K_{pub}

K_{priv}

K_{priv}

K_{pub}

George knows only Barbara could encrypt $\mathrm{hash}(P)$. Only George can decrypt $K_{\mathrm{pub}}[P]$.

RSA

- Messages/plaintext represented by integers.
- Create key pairs, and encrypt and decrypt messages, with simple math ops.
- Harry the hacker can snoop, and discover the large composite $n = pq$, but to decrypt he needs to..

...factorize n. (Not impossible, just HARD).

How difficult is factorizing?

For bigger numbers than you can do in your head:

http://www.merriampark.com/factor.htm

...and if you are really good, I will give you $10,000 for:

```
2519590847565789349402718324004839857142928212620403202777
7137836043662020707595556264018525880784406918290641249515
0821892985591491761845028084891200728449926873928072877767
3597141834727026189637501497182469116507761337985909570009
7330459748808428401797429100642458691817195118746121515172
6546322822168699875491824224336372590851418654620435767984
2338718477444792073993423658482382428119816381501067481045
1660377306056201619676256133844143603833904414952634432190
1146575444541784240209246165157233507787077498171257724679
6292638635637328991215483143816789988504044536402352738195
13786365643912120103971228221207203577
```

```
25195908475657893494027183240048398571429282126204032027777137836043662020707595556264018525880784406918290641249515082189298559149176184502808489120072844992687392807287776735971418347270261896375014971824691165077613379859095700097330459748808428401797429100642458691817195118746121515172654632282216869987549182422433637259085141865462043576798423387184774447920739934236584823824281198163815010674810451660377306056201619676256133844143603833904414952634432190114657544454178424020924616515723350778707749817125772467962926386356373289912154831438167899885040445364023527381951378636564391212010397122822120720357
```

http://www.rsasecurity.com/rsalabs/node.asp?id=2093

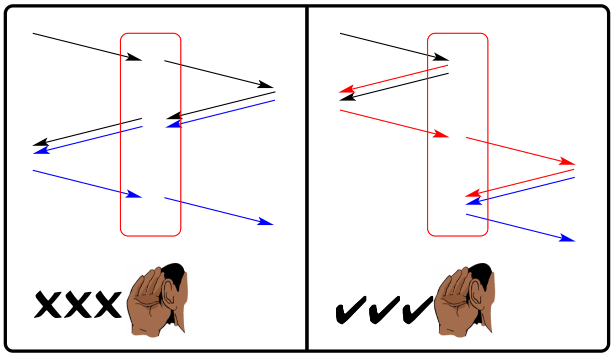
A warning

This is only the tiniest tip of the iceberg. Encryption is only one facet of security in software systems.

Any interaction between your program and another program, or the OS, must be considered dangerous.

For example consider the two-lock scheme given previously... Can it be hacked?

M'n'M



Sometimes it is difficult to see such things in even very simple protocols. A justification for automated/mathematical analysis.

“White hats”
Secure systems design principles

- **Economy of mechanism:** keep design simple
- **Fail-safe defaults:** access only by permission
- **Open design:** secret designs not effective
- **Separation of privilege:** two keys better than 1
- **Least privilege:** Use the smallest set to do job

Be aware of security at all levels of software production...

Dont..

- ✘ invent your own encryption/security schemes
- ✘ assume that since your program is perfect everything must be OK. There is no such thing as a perfect program.
- ✘ be confident about your programs.

Do...

- wear a black hat from time to time... Hack yourself!
- peer-review, audits of software, hazard analysis
- be aware that testing less useful than analysis
- good design (modularity, encapsulation, information hiding)
- use standards...

Sample standards

- UK, Germany, France, Netherlands produced Information Technology Security Evaluation Criteria (ITSEC).
- Accepted by the ISO (ISO15408).
- Many banks now require this level of certification.

ITSEC level 6 certification involves verification with independent systems, and deriving code from specification using a formal (mathematical) process.