Security

C.W. Johnson,

University of Glasgow,
Glasgow, G12 8QQ.
Scotland.
johnson@dcs.gla.ac.uk,
http://www.dcs.gla.ac.uk/∼johnson

October 2004

CS-1Q HCI

Objectives

- Security, privacy and trust.

- Technological threats:

– Trojan horses, time bombs, eaves dropping;
– viruses, email attachments and fake attacks;
– cameras, microphones and digital retrieval.

- Technological protection:

– regular software updates and service packs;
– access control mechanism;
– cryptology;
– security and safety audits.

Objectives

- The pace may be increasing:

–http://www.microsoft.com/security/default.mspx.

Added: October 13, 2004 Microsoft released ten security bulletins (nine Windows, one Office) Tuesday. Here are links to each:

Microsoft Security Bulletin MS04-038 Critical: Cumulative Security Update for Internet Explorer (834707)

Microsoft Security Bulletin MS04-037 Critical: Vulnerability in Windows Shell Could Allow Remote Code Execution (841356)

Microsoft Security Bulletin MS04-036 Critical: Vulnerability in NNTP Could Allow Remote Code Execution (883935)

Microsoft Security Bulletin MS04-035 Critical: Vulnerability in SMTP Could Allow Remote Code Execution (885881)

Microsoft Security Bulletin MS04-034 Critical: Vulnerability in Compressed (zipped Folders Could Allow Remote Code Execution (873376)

Microsoft Security Bulletin MS04-033 Critical: Vulnerability in Microsoft Excel Could Allow Remote Code Execution (886836)

Microsoft Security Bulletin MS04-032 Critical:Security Update for Microsoft Windows (840987)

Microsoft Security Bulletin MS04-031 Important: Vulnerability in NetDDE Could Allow Remote Code Execution (841533)

Microsoft Security Bulletin MS04-030 Important: Vulnerability in WebDAV XML Message Handler Could Lead to a Denial of Service (824151)

Microsoft Security Bulletin MS04-029 Important: Vulnerability in RPC Runtime Library Could Allow Information Disclosure and Denial of Service (873350)

Objectives

- Recent threats:

– New MyDoom, Doomjuice;
– Sasser and Zindos worms;
– Blaster virus.

- Network based threats:

– spyware and DNS redirects;
– email based phising and identity theft;
– Trojan horses and software upgrades.

Security and Privacy

- Turn out your pockets
- Any personal organisers?
- Any diaries?
- Pass them to the person next to you.

Security and Privacy

- Obvious point number one:

– information has value.

- People really do ‘steal it’.

- Unlike money, difficult to retrieve.

- Unlike money, difficult to trace.

Security and Privacy

- Point number two:

– security is built on trust.

- How much do you trust:

– your colleagues?
– your staff?
– your neighbour?

Security and Privacy

- Any unusual items?

- Point number three:

– people make inferences from information.

- Breaches far worse than you think.

- reflexive-transitive closure.

Technological Threats

- Trojan horses:

– never look a gift horse in the eye...
– except if its boot-legged software;
– especially if it looks like a game.

- Time bombs and viruses:

– Friday the thirteenth, when I'm gone;
– 'hidden' files - difficult to spot.

- Donald Gene Burleson:

– leaves virus on company's commission list;
– his name disappears from payroll;
– virus erases 168,000 transactions;
– seven years probation.

Technological Threats

- Viruses (eg Blaster - August 2003):

- self replicating programs like the 'flu.

- Need some means of propagating:

- most commonly as email attachments.

- Countermeasures:

- dont open attachments by default;
- beware unknown senders;
- beware 'Your Details', 'Hello Again' etc;
- disinfect machine by OS patch.

- But beware of fake attacks.

Technological Threats

- The ‘Internet’ worm:

– Robert T. Morris, Jnr;
– introverted student;
– damage estimated at $10,000,000.

“It’s now 3.45am on Wednesday 3 November 1988. I’m tired so don’t believe everything that follows... Apparently, there is a massive attack on UNIX systems going on right now... this may be a system wide problem. Symptom: hundreds of thousands of jobs.” (Cliff Stoll, dockmaster.arpa)

- Convicted, US Fraud and Abuse Act, 1986:

– guilty of ‘stealing’ computer time;
– Computer Virus Eradication Act, 1990;
– um, not a virus - didn’t attack other programs.

Technological Threats

- Eaves dropping:

– electromagnetic radiation;
– IEC 802.11 - Gorilla networks;
– network monitoring;
– or just leaving your machine on...

- Steve Flemming and BT temporary staff:

– accessed phone numbers for 10 Downing Street;
– accessed internal lines to MI6 installations;
– accessed GCHQ and Ministry of Defence lines...
– then use fault scanning unit to monitor talk

- Virgin Atlantic and British Airways:

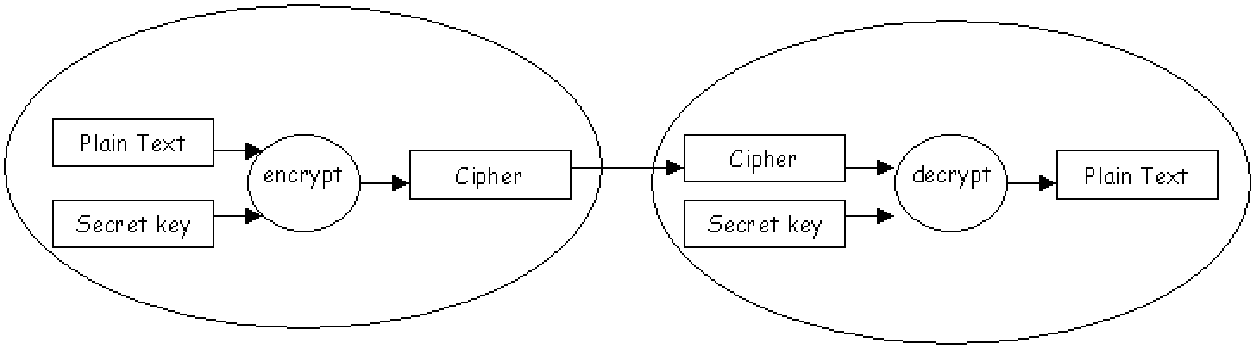
– Virgin hired one of BA's computers;
– BA 'hacked' into their helpline;
– cold-called first-class passengers;
– collated company details for advertising.

Technological Threats

- Information Retrieval.

Protection Mechanisms

- Caesar's Algorithm



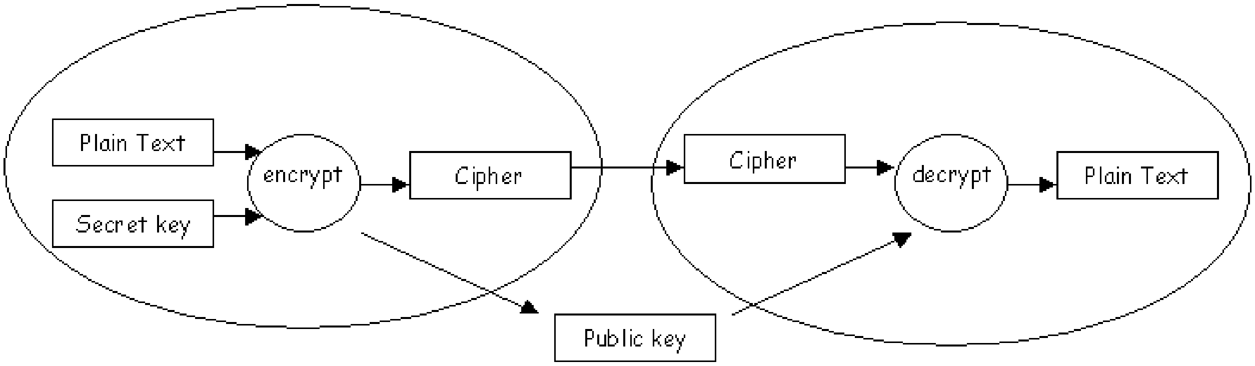
- Private key encryption:

– DES - Data Encryption Standard (IBM);
– RSA - Rivest Shamir Adelman (Netscape).

Cryptology

- Public Key encryption.

- Authentication Services.



- Digital signatures:

– you encode it and send it to me;
– I decode it using a key you sent me;
– if it makes sense then it came from you.

Access Control Mechanisms

- Access control lists:

– associate a list of people with each object;
– check person on list when they request access.

- Capabilities:

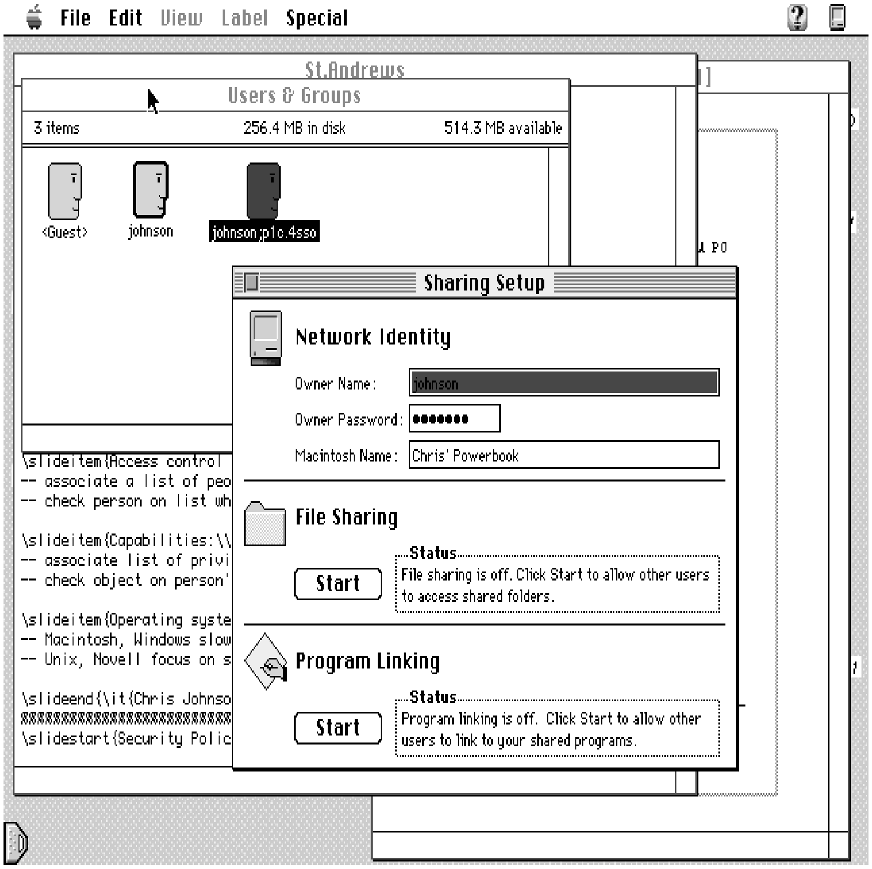
– associate list of privileges with each user;
– check object on person's list when they ask.

- Operating system support:

– Macintosh, Windows slow in catching up;
– Unix, Novell focus on security at start.

Access Control

- Associate passwords with users.



Owner Name: johnson

Owner Password: ●●●●●●●

Macintosh Name: Chris' Powerbook

Status
File sharing is off. Click Start to allow other users to access shared folders.

Status
Program linking is off. Click Start to allow other users to link to your shared programs.

```
\slideitem{Access control
-- associate a list of peo
-- check person on list wh

\slideitem{Capabilities:\\
-- associate list of privi
-- check object on person'

\slideitem{Operating syste
-- Macintosh, Windows slow
-- Unix, Novell focus on s

\slideend{\it{Chris Johnso
%%%%%%%%%%%%%%%%%%%%%%%%%%%%
\slidestart{Security Polic
```

- Don't give others your passwords.

Conclusion

- Prevention is better than the cure 8)
- No. 1: keep back-ups.
- No. 2: ONLY use authorised software.
- No. 3: restrict physical access.
- No. 4: restrict logical access.
- No. 5: keep logs and use them.
- No. 6: technology (Disinfectant, Gate keeper).