Introduction to Computer Security CS3235

Hugh Anderson & Sandeep Kumar

Contact information

Hugh Anderson	Sandeep Kumar
S15 #06-12	S15 #04-08
6874-6903	6874-8923
hugh@comp.nus.edu.sg	skumar@comp.nus.edu.sg

...and Spinellis...

Official SOC description

With the widespread use of computers and Internet as well as electronic commerce, computer security becomes more and more important. The objective of this module is to give students basic knowledge of computer security. This module covers the following topics: threats to computer systems, network security fundamentals, security in a layered protocol architecture, authentication in computer systems, access control, intrusion detection, security architecture and frameworks, lower layers security protocols, upper layer security protocols, electronic mail and EDI security, directory systems security, Unix systems security, security evaluation criteria.

Assessment

Assessment	**Grade**
Labs/Assignments	30%
Tutorials	4%
Tests Closed book	16%
Final Exam Open Book	50%
Total marks	**100%**

May vary the assessment in some small ways...

Assessment

Last year we had two large assignments, but this year we are going to have only a single large assignment, and some small laboratories. All of these are group activities.

Laboratory

- This year, we have a laboratory, just for this course. It is on level 2 of S15.
- The lab has a separate Internet connection, so the NUS restrictions (about use of say scanners) may be lifted, however I expect you to use this freedom wisely.
- We have a series of toys which you may use for your assignment.
- Lab times are not assigned, but we will put a booking form in the lab

Resources

- My course notes in book form (Approx $13)
- Directed readings - all available on the Internet.
- IVLE at http://ivle.nus.edu.sg/
- Web site at http://www.comp.nus.edu.sg/˜cs3235
- You may find Gollman, Liska, Pfleeger, Bishop useful

Topics - general

- History and background,
- Preliminaries
- Encoding and decoding
- Protocols used for security.

Topics - detail

Mathematical, physical, legal	(2 lectures)
Security models	(1 lecture)
Secrecy	(1 lecture)
Insecurity	(2 lectures)
Safety/control hardware/software	(2 lectures)
Assurance	(1 lecture)
Protocols	(1 lecture)
+ Case studies	

Tutorials/labs

- Start in 3rd week
- More details next week

My expectation...

- Attend classes and tutorials
- Ask if you don’t know
- Read notes, book, and the readings...
- Get interested in the subject
- ... and for PG students ... a warning!

Chapter 1

Lecture 1 - Introduction

Jump-about-introduction

...sorry sorry...

Tonight is video night...

The History of Herodotus

For Histiæus, when he was anxious to give Aristagoras orders to revolt, could find but one safe way, as the roads were guarded, of making his wishes known; which was by taking the trustiest of his slaves, shaving all the hair from off his head, and then pricking letters upon the skin, and waiting till the hair grew again. Thus accordingly he did; and as soon as ever the hair was grown, he despatched the man to Miletus, giving him no other message than this- "When thou art come to Miletus, bid Aristagoras shave thy head, and look thereon." Now the marks on the head, as I have already mentioned, were a command to revolt...

The History of Herodotus

- Histiæus ensured *confidentiality*
- Used again by Germany in the 1914-1918 war
- This is now called steganography

More history

- Cæsar encoded messages - cryptography
- Agreed protocols to ensure correct conduct of a war
- Examples taken from the world of warfare

Aspects to “computer security”

Security problems in society reoccur in computers

- Confidentiality = locks/encoding.
- Integrity = handshakes/signatures

Computer versions much faster.
In this course, security includes wider aspects.

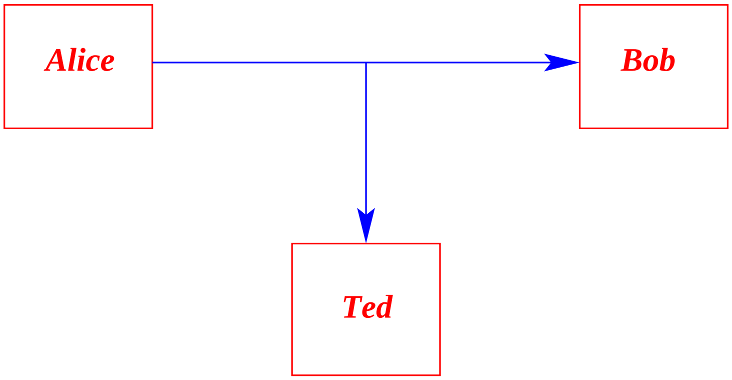
Start with some definitions

Terms: Services

Three aspects of security *services*:

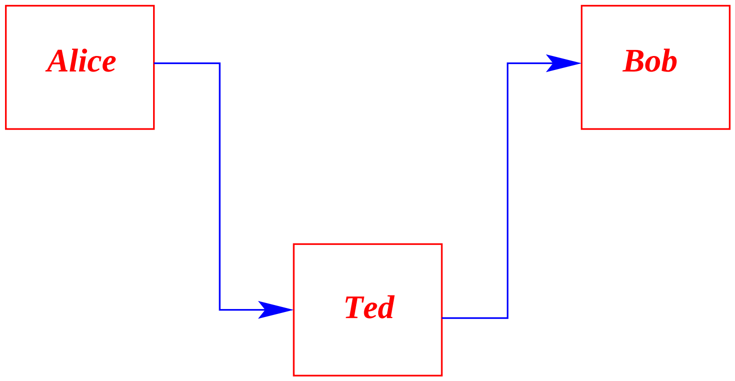
- **confidentiality**: concealing information - resources;
- **integrity**: trustworthiness of data - resources;
- **availability**: preventing denial-of-service.

Terms: Threats



Snooping

Terms: Threats



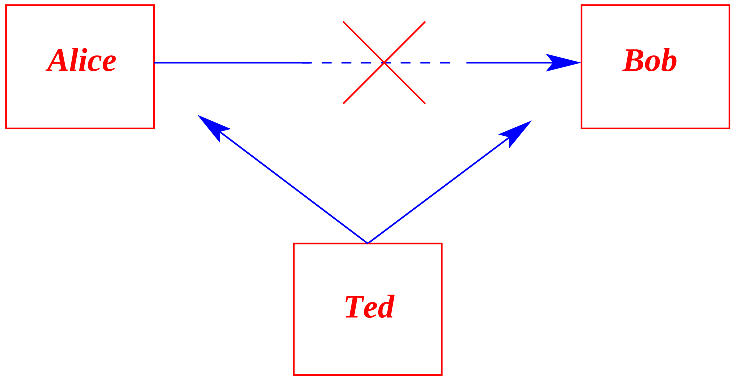
Alice

Ted

Bob

Man in the middle

Terms: Threats



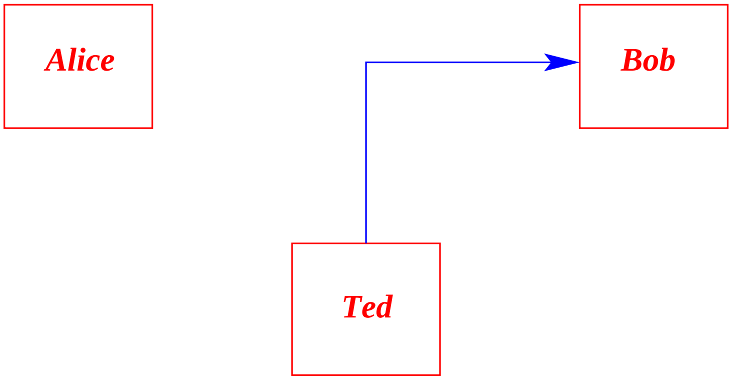
Alice

Bob

Ted

Denial of service

Terms: Threats



Spoofing

Terms: Threats

- **disclosure**: unauthorized access (snooping);
- **deception**: accept false data (man-in-the-middle);
- **disruption**: prevent correct operation (denial-of-service);
- **usurpation**: unauthorized control (spoofing).

Terms: Policy and mechanism

We differentiate between a security *policy* and a security *mechanism*:

- **policy**: what is allowed/disallowed;

- **mechanism**: ways of enforcing a policy

NUS IT policy

For example, at NUS, we have an IT policy which includes a range of clauses regarding security concerns, such as:

> ***4.2 Undermining System Integrity***
>
> *Users must not undermine the security of the IT Resources, for example, by cracking passwords or to modify or attempt to modify the files of other Users or software components of the IT Resources.*

NUS mechanisms

6.3 Use Of Security Scanning Systems

Users consent to the University's use of scanning programs for security purposes at system level for computers and systems that are connected to the University's network. This is to ensure that any computers or systems attached to the network will not become a launching pad for security attack and jeopardise the IT Resources. System level scanning includes scanning for security vulnerabilities and virus detection on email attachments. Users' files and data are excluded from the scanning.

Topic: Preliminaries

- Review some mathematical concepts. XOR, modulo, primes
- The textbook should be enough.
- *Physical* laws and procedures. Information and Entropy
- Quantum properties

Topic: Security models

These models provide formal ways of looking at computer security in an abstract manner.

1. Define a model, and

2. prove it secure

3. Ensure system complies with model

Topic: Security models

- The Bell-LaPadula model (no read-up, no write-down) provides a military viewpoint to assure *confidentiality* services.

- The Biba and Clark-Wilson models attempt to model the trustworthiness of data and programs, providing assurance for *integrity* services.

Topic: Security models

- Determine properties of the model, and
- Verify that implementations are valid.
- Basis of trusted operating systems
- Modelling for availability is tricky

Major topic: Secrecy

- Commerce relies on secure transfer of information, and
- Often just want things to be secret
- Distance between you and an attacker is shrinking
- Criminals have an access point into your living room

2000 years ago...

Replace each Roman letter in a message, with another Roman letter, obtained by rotating the alphabet some number of characters:

I CLAVDIVS

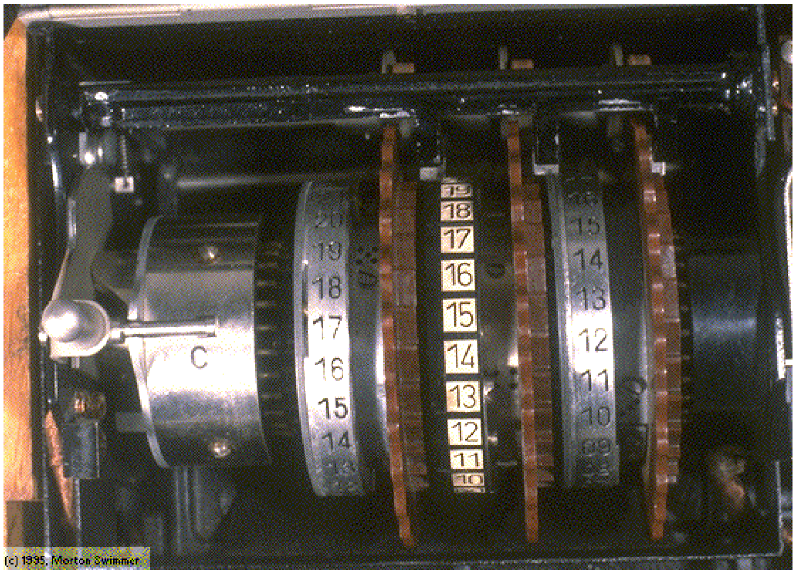
A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	V	X	Y	Z
V	X	Y	Z	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T

E YGVQZEQO

We can specify a Cæsar cipher by just noting the number of characters that the alphabet is rotated. (Keyspace?)

60 years ago...

60 years ago



Enigma machines

- Commercial device
- Used by the German military
- Belief that could not be decoded.

(video.mpg)

Enigma machines

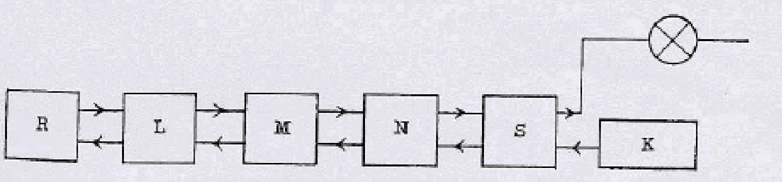
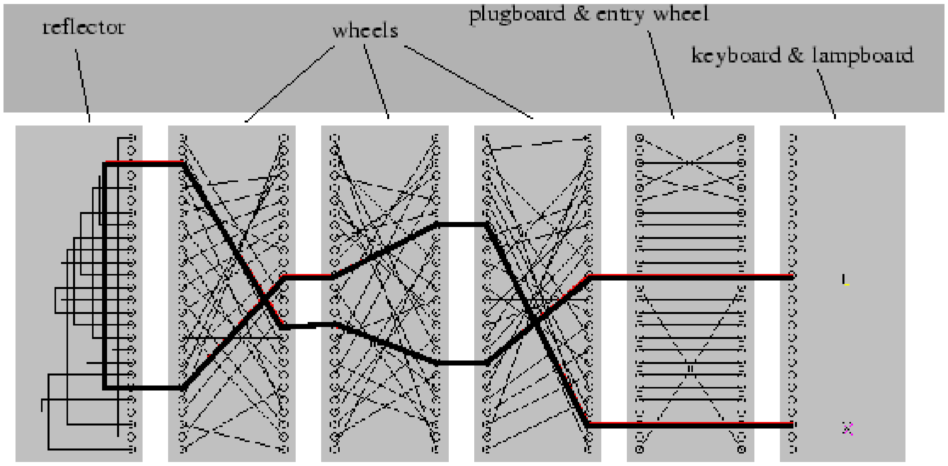


Fig. 1. Current circuit block diagram
R – reverting drum, *L*, *M*, *N* – ciphering drums, *S* – plug cables, *K* – keyboard, ⊗ – bulbs

Enigma machines



Hacking Enigma

✘ Americans captured a German submarine?

✘ Alan Turing did it all?

✘ Hard workers at Bletchley Park?

✘ My dad?

Hacking Enigma

✹ 1928: Poles intercepted a machine

✹ 1928: Maths Dept at University of Poznan: Marian Rejewski, Jerzy Rozycki, Henryk Zygalski.

✹ Decoded some messages

✹ German army using an extra level of encoding

✹ French spies uncovered the extra encoding

Hacking Enigma

- 1933-1939: the Polish Ciphers Office was able to decode messages, although slowly.
- July 1939: Poland gave Enigma copies to English
- Bletchley Park
- May 1941: English captured the U-110 submarine, complete with a genuine Enigma machine, and code books.

Hacking Enigma

- 1941-45: English could decode most German military transmissions.
- 1941-45: developed a hardware system
- Precursor to modern-day computers

(video2.mpg)

Today...sssshhhh

- Secure encrypted communications between
  - two untrusted hosts
  - over an insecure network.
- Other connections can also be forwarded
- Users must prove their identity to the remote machine

Secure-shell

- Based on public-key cryptography:
  - Encryption and decryption use separate keys
  - Not possible to derive one from other
  - RSA is one such system.
- Encodings believed to be difficult to decode, and
- Protocols of message exchange that are believed to be secure.

Topic: Insecurity

- Systems dangerously easy to subvert
- Adversary gains control over your system
- You sign a contract, and other party doesn’t.
- Investigate hacking and reducing risk

Topic: Insecurity

A locked air-conditioned room with file server:

- The lock can be picked, or the door kicked in.
- The console of the server computer may be password protected, but
    - it may be rebooted with a different disk.

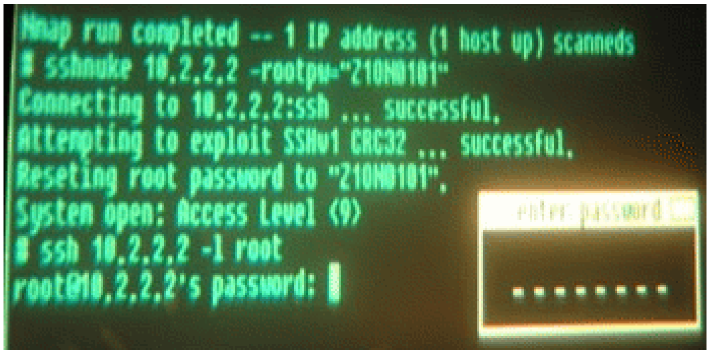
Topic: Insecurity

- The reboot process may be (BIOS) password protected, but
  - the case of the computer may be opened and the disk removed.
- And so on...

Topic: Insecurity

- Tempest - computer screen monitoring
- Paper
  - http://jya.com/emr.pdf
- Overcoming
  - http://www.cs.rice.edu/~dwallach/courses/comp527_s2000/ih98-tempest.pdf
- Monitor screens at a distance of 1km for $15.

Topic: Insecurity



```
Nmap run completed -- 1 IP address (1 host up) scanneds
# sshnuke 10.2.2.2 -rootpw="Z10N0101"
Connecting to 10.2.2.2:ssh ... successful.
Attempting to exploit SSHv1 CRC32 ... successful.
Reseting root password to "Z10N0101".
System open: Access Level (9)
# ssh 10.2.2.2 -l root
root@10.2.2.2's password:
```

Kick in doors without even using your feet: 1:43:30

Topic: Insecurity

Non-repudiation for e-commerce:

- the buyer cannot order an item and then deny the order took place;
- the seller cannot accept money or an order and then later deny that this took place.

Topic: Insecurity

- Intrusive hacking is common on the Internet.
- Farms of subservient machines:

  At first, it looked as if some students at the Flint Hill School, a prep academy in Oakton, Va., had found a lucrative alternative to an after-school job...

Topic: Insecurity

- Virusses: boot-sector hide their code in the boot sector of a disk.
  - the stoned virus for DOS, written by a student from New Zealand!
- A virus contains code that replicates, attaching itself to a program, boot sector or document. Some viruses do damage as well.

Topic: Insecurity

Worm is a program that makes copies of itself, transferring itself around. The Morris worm in 1988:

> *On the evening of 2 November 1988, someone infected the Internet with a worm program. That program exploited flaws in utility programs in systems based on BSD-derived versions of UNIX. The flaws allowed the program to break into those machines and copy itself, thus infecting those systems.*

The Morris Worm

> *This program eventually spread to thousands of machines, and disrupted normal activities and Internet connectivity for many days.*

ftp://ftp.cs.purdue.edu/pub/reports/TR823.PS.Z

The author of the worm, Robert Morris, was convicted and fined $10,050 in 1990, and is currently a professor in the Parallel and Distributed Operating Systems group at MIT, lecturing in distributed systems areas.

Topic: Protocols

Some aspects of security are determined by the way in which we do things (the protocol), rather than what is actually done.

Topic: Protocols

Summary of topics

In this section, we introduced the following topics:

- An introduction to computer security
- Some definitions

Further study

- Textbook Chapter 1
- Monitoring computer screens
  http://jya.com/emr.pdf
- Overcoming Tempest monitoring
  http://www.cs.rice.edu/~dwallach/courses/comp527_s2000/ih98-tempest.pdf
- The Morris worm
  ftp://ftp.cs.purdue.edu/pub/reports/TR823.PS.Z
- Military mathematical modelling of security
  http://80-ieeexplore.ieee.org.libproxy1.nus.edu.sg/xpl/tocresult.jsp?isNumber=13172