

Computer Security

COMP4307

COMP5327

INFS6103

Introduction

<http://www.it.usyd.edu.au/~michaelh>

What is Security?

- making the paranoid happy
- protecting the system and its resources

Importance of Security

- more and more organisations relying upon networked applications
- more and more business transactions are being conducted electronically over the Internet
- vast amount of sensitive and valuable information stored on computers

Threats

- eavesdropping
- tampering
- impersonation
- repudiation
- denial of service
- illegal access

Attacker

- someone who actually attempts to subvert a system
- may be an authorised user
- may be an outsider

Security Mechanisms

- confidentiality
- integrity
- auditing
- authentication
- authorisation

Eavesdropping

- when two parties communicate they may want their communication to be secret
- eavesdropping is when a third part "listens in"

Tampering

- when a message is sent sender usually wants it to arrive unaltered
- tampering is when the message is altered en-route

Impersonation

- when one entity attempts to gain access to resources, information, etc, by pretending to have a different identity
- attacker attempts to adopt the identity of an authorised user

Repudiation

- attacker either
 - denies carrying out an action they actually did carry out
 - claims to have taken an action they actually did not take
- attacker must be an authorised user (or impersonating one)

Denial of Service

- attacker attempts to deny access to some system service
- most common form is to overwhelm service with requests so service fails or is grossly slowed

Illegal Access

- an authorised user rarely, if ever, is granted access to all facilities of a system
- users may attempt to access resources to which they are not entitled

Defeating Attacks

- eavesdropping <- confidentiality
- tampering <- integrity
- impersonation <- authentication
- non-repudiation and denial of service <- auditing
- illegal access <- authorisation

Auditing

- record of actions
- used to defeat non-repudiation
- difficult to record everything
- parties can agree that communications will be recorded
- third party(ies) keep records

Access Control

- access control lists
- capabilities
- role based access control
- mandatory/discretionary access control
- lattice based access control

Security Policies

- managers of systems must decide what is and is not authorised
- mechanisms used to implement policy
- important to maintain a clear distinction

Service and Mechanism

- A *security service* enhances the security of the data processing and information transfers of an organisation
- Services are intended to counter attacks
- Services are implemented by one or more *mechanisms*



Trust

- A very important concept in security
- It is impossible to mechanically, or within the bounds of the system, prevent every undesirable action
- For example, an encrypted message is encrypted to stop third parties discovering its content
- What if the sender or receiver simply tell them?

Trust

- In any security system there is some part which is simply *trusted*
- That means that we *assume* it will not do anything it should not
- Which parts of a system are trusted, and why, are a very important part of the design of any security system

Trust

- When you design a security system you should make your trust assumptions clear in the documentation
- When you analyse a security system you should make certain of its trust assumptions, both from its documentation and your own analysis

So...

- Is security the final solution to our problems?
- NO!!!!
- No system is perfect

Cryptography

- Mathematicians will have you believe cryptography is infallible
 1. Cryptography **DOES NOT** equal computer security
 2. What they mean by infallible and what you mean by infallible is not necessarily the same

Theory

- In theory there is no difference between theory and practice
- In practice, there is
- That's why engineers are not the same thing as scientists

Systems vs. Machines

- Machines are (relatively) simple
- Systems
 - Are complex
 - Interact with each other
 - Have emergent properties
 - Are bug ridden

The real world

- Systems have faults
- The real world involves
 - Unforeseen problems
 - Unseen variables
 - Imperfect implementations
- Something will go wrong

25

Real attacks

- Automation
- Action at a distance
- Technique propagation
- Proaction vs. reaction

26

So...?

- Do we give up now?
- No, but the providing security is an ongoing **process**
- It's never finished
- It certainly isn't achieved by writing something that's *theoretically* correct and walking away

27

From Now

- We'll look at some of the available tools
- And processes
- And hopefully develop a healthy cynicism

28