Software Security 415.725SC

Clark Thomborson

University of Auckland

Objectives

- Anyone who passes this class will be able to
  - give basic advice on software security, using standard terminology;
  - read technical literature on software security, demonstrating critical and appreciative comprehension; and
  - give an informative oral presentation on, and write knowledgeably about, an advanced topic in software security.

Prerequisites

- Any two of the following:
  - – 415.330 or 415.333 (compilers)
  - – 415.320 or 415.335 (algorithms)
  - – 415.313 (computer organisation)
  - – 415.314 (networks)
  - – 415.350 (CS theory)
- An interest in applying your stage-3 knowledge of CS to the study of software security.

Basic Terminology (Pfleeger 1997)

- *Vulnerability*: a weakness that might be exploited to cause loss or harm.
- An *attack* exploits a vulnerability.
- A *threat* is a possible attack.
- There are four types of threats: *Interception, Interruption, Modification, Fabrication.*

☞ Did you read this section? Do you understand these concepts? Do you think this is a complete list of threats? Could you classify *any* threatening action this way?

Threat: your system may be...

- Interrupted = lost, unavailable, unusable.
- Intercepted = available to an *unauthorised party*.
- Modified = an existing component has been changed by an unauthorised party.
- Fabricated = a new component has been inserted by an unauthorised party.

A Quick Test of Pfleeger (and you)

☞ Categorise the following attacks (taken from the content description of this course):

- – denial of service
- – privacy violations
- – playback
- – binary tampering during delivery

by type of threat and by *asset* being attacked.

- Asset types: *hardware, software, data.*

Goals of Software Security

(Pfleeger 1997)

- What are we trying to preserve?
  - *Confidentiality* (unauthorised people can’t read)
  - *Integrity* (unauthorised people can’t write)
  - *Availability* (authorised people can read and write)

☞Are these definitions appropriate? Hint: think of the Unix filesystem protection bits `drwx`. Consider non-Unix systems, too.

Vulnerabilities (Pfleeger 1997)

- Hardware is vulnerable to interruption and interception. ☞Give examples.
- Software is vulnerable to interruption, interception, and modification.
- Data is vulnerable to all four threats.

☞Is hardware vulnerable to modification or fabrication? Is software vulnerable to fabrication?

The People Involved (Pfleeger 1997)

- *Amateurs* take advantage of obviously poor security. They commit “most of the computer crimes reported to date.”
- *Crackers* use newsgroups, websites, and email to discover security flaws. They may be prosecuted severely with harsh penalties, regardless of their motive.
- *Career criminals* make a living from exploiting vulnerabilities. They might not be prosecuted even though they have caused great damage!

☞ *Authorised users* may cause *collateral damage* when trying to repair the *primary damage* from an attack.

Methods of Defense (Pfleeger 1997)

- *Encryption*: “the most powerful tool.”
- *Software controls* such as access limitations in a DBMS or an OS; and quality assurance during software development.
- *Hardware controls* such as *dongles,* that must be present to enable the software to run.
- *Policies* on appropriate use, that are enforced by *legal, ethical* or *moral* codes.
- *Physical controls* such as locks on doors and backup disks are sometimes the “easiest, most effective and least expensive” option.

Effectiveness of Controls

(Pfleeger 1997)

- Controls won’t help unless…
  - Users are aware of them, and motivated to comply;
  - Users aren’t inconvenienced by them; and
  - The controls are reviewed periodically.
- Overlapping controls can offer more protection, or they may merely add complexity, cost or inconvenience.

Pfleeger’s Taxonomy

- Concepts in computer security can be classified on the following dimensions:
  - Threat type = (interruption, interception, …)
  - Asset type = (hardware, software, …)
  - Goal of attack / vulnerability = (confidentiality, integrity, availability)
  - People involved = (amateur, hacker, …)
  - Attack or defense = (threat, control)

☞ Try to classify *reverse engineering* and *sandbox security* (as in Java).

Guidelines for the Use of University Computing Facilities and Services

- "Your responsibilities can be summarised simply as:
  - use the resources for University-related work,
  - respect other users, and
  - respect the resources. …"

☞Can you classify these Guidelines, using Pfleeger's taxonomy?

University Guidelines (cont.)

- "… Users shall use computing facilities and services only for the purpose of carrying out authorised, University-related activities.
  - This normally includes work relating to approved research and study, the administration of the University, and other delegated tasks.
  - Activities such as conducting, promoting or advertising a personal commercial, social or recreational enterprise are not permitted.
  - Activities such as transmitting or making available offensive, obscene or harassing materials are not permitted. …"

University Guidelines (cont.)

☞ Apply Pfleeger’s taxonomy:

- What class of threat is the previous portion of the Guidelines trying to control?
- What asset class?
- What goal?
- What category of people?

University Guidelines (cont.)

- “… Users shall work in a manner that does not jeopardise the security of the system and shall satisfy all reasonable demands by authorised staff to demonstrate that they are authorised to use the facilities. This includes:
  - using only their personal computer account, and not allowing any other person to use their computer account.
  - keeping their computer password secret, selecting unguessable passwords, and not attempting to discover or change any other person's password. ...”

University Guidelines (cont.)

- “… identifying themselves, upon request, to authorised staff by presentation of a valid ID card. If a user cannot produce a valid ID card then they must leave the facility if requested to do so.
- not conducting or attempting to conduct security experiments or security scans involving or using University computer or network resources without the expressed written permission of the University Computer and Network Security Officer. …”

University Guidelines (cont.)

- “… Users shall work in a manner that respects the rights of other users of the services or facilities and of people elsewhere. This includes:
  - using any facility in a considerate, ethical and lawful manner so as minimise the impact of their usage on other users of the facility. For example, users must not behave in a noisy disruptive manner, remove or deface material on notice boards or remove material (e.g. printouts) belonging to other users of the facility.
  - using any booking system in a fair and ethical manner.
  - not sending obscene, abusive, fraudulent, threatening or repetitive messages to others. …”

University Guidelines (cont.)

- "… Users shall normally use computing facilities and services as they are provided, without attempting to modify or subvert them. This includes:
  – using only those resources, facilities and data that have been made available for general access, or those which the user has been authorised to use.
  – not attempting to modify system facilities, to install viruses, to obtain illegally extra resources or to degrade the performance of any system.
  – not attempting to subvert the restrictions associated with any computer system, computer account, network service or personal computer protection software. …"

University Guidelines (cont.)

– "… running only software that has been provided by the service or facility, or has been written by themselves as part of their approved research, study or administrative activities. The installation of software is permitted when the individual has been delegated responsibility for the maintenance of the computer system in question.

– not copying, transferring or disclosing any computer software provided by the University without the written permission of the IT Director, Dean or University Librarian.

– representing themselves truthfully in all forms of electronic communication and not altering their network identity to deceive or confuse others. …"

University Guidelines (cont.)

- “… Users shall treat computing resources with care and respect. This includes:
  - leaving all food, drink, chewing gum etc. in their bags. Such material can damage equipment if dropped or spilled. Users may have only "sipper bottles" or other non-spill drink containers.
  - not tampering with the physical equipment. For example, users must not unplug connectors or connect any other equipment to the computers or network.
  - leaving all support materials (e.g. manuals, diskettes, etc.) in the facility. …”

Readings for Tomorrow

- K. Nichols, “The Age of Software Patents,” *IEEE Computer,* 7 pp., April 1999.
- Letters to the Editor in response to Nichols’ article, 2 pp., *IEEE Computer,* June 1999.
- P. Samuelson, “Encoding the Law into Digital Libraries,” *Comm. ACM,* 6 pp., April 1998.

☞Goal: a general understanding of *software patent, copyright,* and *trade secret.*