Homework Solutions: Lectures 1 - 5

Lecture 1

(P&P 1.2) **Harm caused to a company by theft of computer equipment.** Monetary loss (value of equipment), data loss, monetary loss due to impaired operations.

(P&P 1.3) **Harm caused to a company by electronic espionage.** Embarrassment and loss of customers due to data loss, loss of proprietary information, loss of sensitive business strategy information (planned acquisitions, etc.).

(P&P 1.4) **Harm caused to company by compromised integrity.** Direct loss through incorrect accounts and billing, monetary loss due to impaired operations, liability from inaccurate securities filings, customer loss due to mistrust of company systems.

(P&P 1.7) **On shared memory system, who can modify system software?** Developers; root or sudoers (admin privileges). **Who can modify major applications?** Developers; root or sudoers (admin privileges). **User program?** The user (owner) and anyone with admin privileges; anyone who the owner has granted write access. **Does his seem right?** Yes, so long as defaults for access are reasonable, e.g. user files should, by default, only be accessible by the file owner.

(P&P 1.10) **Relate CIA to interruption, interception, modification, and fabrication.**
- confidentiality — interception
- integrity — modification and fabrication
- availability — interruption

(P&P 1.11) **DISCUSSION: Do you think attempting to break into a computer system without authorization should be illegal?**

(P&P 1.12) **Describe data for which confidentiality has short timeliness? Timeliness of more than a year?** Tactical military communications have short-lived intelligence value since an adversary can usually observe troop movement, etc., described in the communications. Strategic military information — weapons system development plans, sensitive deployment plans, etc. — may have intelligence value for many years.

SCADA System
- Confidentiality — need to protect proprietary information; may also want to protect information about production levels and operating status. Administrative data may include personal information requiring protection.
- Integrity — cannot allow an adversary to modify or insert data in a way that would influence the industrial process; could result in poor production quality, equipment failure, chemical leaks, and threat to human life. Administrative data could include routine financial information, which also needs to be protected from modification.

- Availability — if the system is not available, the company can't produce chemicals and loses income. If the system is poorly designed, unavailability of the SCADA system could lead to failure in the production process resulting in poor production quality, equipment failure, chemical leaks, and threat to human life. Could also delay routine processes such as billing or purchasing and receiving.

Code Snippet. If won_lottery has any value *other than* NOT_A_WINNER, it declares you to be a winner. An error in DidUserWinLottery() could result in announcing a winner erroneously.

Lecture 2

(P&P 1.14) **Describe case where full DOS is is a serious problem. Where 10% DOS is a serious problem. Could unauthorized access result in 10% DOS?** Full DOS: failure in a weapons system, nuclear plan control systems, banking. 10% DOS: real-time processes such as voice or video communication, telephone switches, etc., especially in times of crisis — could result in inability to communicate reliably; payroll processing, passport processing, weapons targeting systems, IFF, anything that requires timeliness. In all of these cases, unauthorized access could potentially result in a 10% reduction.

(P&P 1.17) **Time and temperature website. Who might want to attack it? What harm might they cause? What vulnerabilities might they exploit?** Site has no serious value, so probably just prank or script-kiddy attacks. On the other hand, the ability to modify the program could allow an attacker to gain access to other information on the site. Can't really decide who might want to attack it without knowing more about the website. An attacker could simply deface the website, or might gain access to information they are not authorized to see. If the program is something I'm just including from some other website, the attackers could exploit the fact that I don't control the code by either (1) writing the original program themselves or (2) attacking the website from which it comes.

(P&P 1.18) **Web ordering program. Who might want to attack? What harm might they cause? What vulnerabilities might they exploit?** Presumably my site processes credit card or other payment information, so an attacker would be interested in stealing customer info. They might also be interested in finding a way to make orders with reduced prices, or they might just want to shut-down my site. They could harm my reputation with customers, hurt my bottom-line but purchasing at reduced prices, or cut-off my income by bringing down the site. They would probably exploit vulnerabilities in web forms and back-end processing, or possibly poor password selection by users. Also, there could be vulnerabilities in the underlying OS that would allow attackers to gain access.

(P&P 1.19) **Vote tabulator. Who might want to attack? What harm might they cause? What vulnerabilities might they exploit?** Anyone who wants to affect the results or disrupt the election would want to attack the system. They might change the

results, or prevent the election from occurring. Most likely they would exploit vulnerabilities in the system software or voting system APIs to gain remote access.

(P&P 1.20) **Tele-surgery system. Who might want to attack? What harm might they cause? What vulnerabilities might they exploit?** Someone would have to be truly malicious to attack such a system. Other than a vendetta against the patient, I can't imagine a good reason to attack such a system. An attacker could simply monitor the system to learn personal health information; could interfere with the voice and images, or could make the system unavailable, which would degrade the ability of the remote surgeon to assist. An attacker might exploit lack of encryption or poor authentication and integrity checks.

(P&P 1.21) **DISCUSSION: find an example of a recent computer intrusion. Discuss in terms of: easiest penetration, adequate protection, effectiveness, and weakest link.**

Lecture 3

No exercises.

Lecture 4

Un-safe functions and safe alternatives.

- gets() — fgets()
- sprintf() — snprintf()
- strcat() — strncat()
- strcpy() — strncpy()
- vsprintf() — vsnprintf()

Add exit() to shellcode.

```
xor eax, eax
mov eal, 1
int 80h
```

Buffer overflow example. Overwrite the variable pass to make it non-zero.

Lecture 5

Will StackGuard help with last problem from Lecture 4? As described, no. The overwrite of pass would not be detected since local variables are below the canary.

When would a programmer legitimately want to allow execution of the stack? Nested functions (GCC extension of C) has to put small piece of code on stack.

DISCUSSION: Review some of the recent vulnerability announcements on the National Vulnerability Database (http://web.nvd.nist.gov/view/vuln/search). How many are stack-based buffer overflows? What types of buffer overflows, other than stack- based, do you see? Choose one other type of buffer overflow and research how it works in general.