Lecture Notes on Jan/09/2023

Chapter 1:
Computer Security Introduction and Review

CYENG 351: Embedded Secure Networking

Instructor: Dr. Shayan (Sean) Taheri
Gannon University (GU)

Personal Information

- Name: Shayan (Sean) Taheri.
- Date of Birth: July/28/1991.
- Past Position: Postdoctoral Fellow at University of Florida.
- Ph.D. Degree: Electrical Engineering from the University of Central Florida.
- M.S. Degree: Computer Engineering from the Utah State University.
- University Profile: https://www.gannon.edu/FacultyProfiles.aspx?profile=taheri001

Chapter Overview

- Provide a quick introduction, a review, and a basic context to computer security for embedded systems engineers who may not have a formal background in computer science and computer security.
- Spending most of the discussion on those ideas that are most pertinent to embedded and resource-constrained systems.
- **Computer Security**
  - A rapidly evolving field; every new technology is a target for hackers, crackers, spyware, trojans, worms, and malicious viruses.
  - The threat of computer attacks dates back to the earliest days of mainframes used in the 1960s.
  - As more and more companies turned to computer technology for important tasks → Attacks on computer systems became more and more of a worry, **why?** Popularity of computer technology for important tasks.
- **Worry in Different Times**
  - Early Days of the Personal Computer → Viruses.
  - Advent of the World Wide Web + Exponential Expansion of Internet → Hackers and denial of service attacks.
  - Now → Spam, malware/spyware, email worms, and identity theft.

Chapter Overview (Cont.)

- **Critical Question:** How do we protect ourselves from this perpetual onslaught of ever-adapting attacks?
- **Answer:** Being Vigilant in Improving System Security
  - Staying one step ahead of those who would maliciously compromise the security of your system.
  - Utilizing cryptography, access control policies, security protocols, software engineering best practices, and good old common sense.
- **Remember:** Computer security is both a science and an art!

What is Security?

- **Definition of Computer Security** (in this context)
  - It is the protection of personal or confidential information and/or computer resources from individuals or organizations that would willfully destroy or use said information for malicious purposes.
- **Important Point:** The security does not need to be limited to simply the protection of resources from malicious sources - it could actually involve protection from the application itself.
- Building a secure computer system also involves designing a robust application that can deal with internal failures.
  - The concepts used is software engineering are very similar to the methods used to make an application secure.
  - No level of security is useful if the system crashes and is rendered unusable.
  - A truly secure system is not only safe from external forces, but from internal problems as well.
  - The most important point is to remember that any flaw in a system can be exploited for malicious purposes.
- What does "**Protection**" actually mean for a computer system?
  - It turns out that there are many factors that need to be considered, since any flaw in the system represents a potential vulnerability.

What is Security? (Cont.)

- **Software-Level Flaws**
  - Buffer Overflows → Potentially allow access to protected resources within the system.
  - Unintended side effects and poorly understood features → They can be gaping holes to be used for someone to break in.
  - Use of cryptography does not guarantee a secure system → If someone can simply hack into your machine and steal that data directly from the source.
- **Physical-Level Flaws**
  - A malicious individual can gain access to an otherwise protected system → Compromising the physical components of the system (i.e., this is especially important for embedded systems).
  - **Human Factor:** Social Engineering → The profession practiced by con artists, turns out to be a major factor in many computer system security breaches.
    - There is little that can be done to secure human activities, and it is a subject best left to lawyers and politicians.

What Can We Do?

- In the face of all these adversities, what can we do to make the system less vulnerable?
  - Understanding the basics of computer security from a general level.
  - Studying the specifics of **Network and Internet Security**.

Access Control and the Origins of Computer Security Theory

- **History:** Paper, "The Protection of Information and Computer Systems" (Saltzer 1976)
  - Recorded the beginning concepts of access control → Using the theory that it is better to deny access to all resources by default and instead explicitly allow access to those resources, rather than attempt to explicitly deny access rights.
  - **Reason:** It is impossible to know all the possible entities that will attempt access to the protected resources, and the methods through which they gain this access.
  - **Problem:**
    - It only takes one forgotten rule of denial to compromise the security of the entire system.
    - Strict denial to all resources guarantees that only those individuals or organizations given explicit access to the resources will be able to have access.
  - **Solution:**
    - The system is then designed so that access to specific resources can be granted to specific entities.
    - This control of resources is the fundamental idea behind computer security, and is commonly referred to as access control.

Assignment

- **Reading Assignment:**
  - Stapko, T., 2011. **Practical embedded security: building secure resource-constrained systems**. Elsevier.
    - ✓"Chapter 1: Computer Security Introduction and Review", Pages 1-3.

GANNON UNIVERSITY

Questions?