Understanding Computer Security

Steve Brown
Capella University, USA

INTRODUCTION

During the last several years a great deal has been written in academic and trade journals that has focused on security. There are several different terms often used, but the following—information security (InfoSec), computer security, and information assurance—are typically meant to be the same, that is, the protection of data, although information assurance is also expanded to include aspects such as personnel, plant, and equipment. While one main theme that has been written has been to improve the effectiveness and understanding of security, apply the various security concepts learned and understand the technologies developed, it is important to recognize that computer security may take on different meanings, dependent on the context that it is being discussed.

Computer security is a very large field, and one that is often misunderstood. When we discuss computer security, are we discussing our personal computer at work or home? Are we discussing portable devices, such as mobile devices like Blackberries, PDAs, or laptops? Are we discussing security laws and regulations that might impact the safeguard of personal information, or could we be discussing, designing, and implementing, a risk-based security plan for an organization?

It is therefore difficult to discuss computer security unless it is discussed in a frame of reference. Therefore, this paper will discuss some of the issues and concerns of computer security in different frames of reference, and the importance of teaching security with that focus in mind.

BACKGROUND

The term computer security was first used as a discipline in the early 1970s. While previous studies existed before that time, they were more practical, and it was not until the 1970s that it was introduced as an educational tool. Bell and LaPadula (1973) introduced the idea of a framework of a secure computer system. This model which was abstract in nature led to the development of other security models such as the protection analysis project which was designed to detect vulnerabilities in operating system software (Bisbey & Hollingworth, 1978). The results of these earlier studies and models led to the U.S. Department of Defense (1985) publishing the Trusted Computer System Evaluation Criteria (TCSEC), which were normally known in the industry by the color of the book, for example, the orange book. This model classified systems into four broad hierarchical divisions, each of enhancing security. The orange book provided a benchmark to gauge other systems.

These earlier models started in the 1970s have led the way to many models and theories on some of the best ways to protect computer systems, and in teaching computer security, a historical perspective is very important. To begin to understand computer security, one must understand its definition. Scholars and researchers have proposed several definitions of computer security, the Alliance for Telecommunications Industry Solutions (ATIS) Committee T1A1 (2001) defines it as:

1. Measures and controls that ensure confidentiality, integrity, and availability of information-system (IS) assets including hardware, software, firmware, and information being processed, stored, and communicated. Synonym automated information systems security.
2. The application of hardware, firmware, and software security features to a computer system in order to protect against, or prevent, the unauthorized disclosure, manipulation, deletion of information, or denial of service.
3. The protection resulting from all measures to deny unauthorized access and exploitation of friendly computer systems (p. 1).

In discussing computer security, it is important that the discussion is focused in the context. In discussing data privacy it is important to discuss privacy in some context; for example, if we are discussing transporting data safely, then we might discuss encryption, if the discussion is on penalties for data disclosure, in that case, we might be discussing legislation. Therefore, it is important to look at some of the leading frames of reference surrounding computer security.

Home Computer Security

Securing a home computing environment starts with awareness. Individuals must be aware that they have very valuable pieces of information contained on their computer system that is attractive to criminals. Personal data, such as credit card numbers, passwords, and bank information, are just some of the areas where intruders seek to gain access. Individuals must also be aware that innocent looking e-mails and requests for personal information are simply phishing attempts, and that computer users should not give out personal information just for the asking. Further, people are creatures of habit, and it is quite common that the password we use for one account is the same password we use for multiple accounts. If an intruder was able to secure that password, and identify sites you have visited, which is not hard due to computer cookies, they would have access to a number of your accounts. Criminals also look at the computer itself as a resource; many hackers will use someone else's computer as a jumping off point, and conduct their illegal activities from the target host.

There are some guidelines that could help a computer user secure their system more. Carnegie Mellon (2002) University's Computer Emergency Response Team (CERT, 2002) offers some valuable training tips on securing a home computer environment, which include:

1. Install and use anti-virus programs.
2. Keep your system patched.
3. Use care when reading e-mail with attachments.
4. Install and use a firewall program.
5. Make backups of important files and folders.
6. Use strong passwords.
7. Use care when downloading and installing programs.
8. Install and use a hardware firewall.
9. Install and use a file encryption program and access controls (para 31).

In teaching home security concepts, it is important to understand that not all individuals are capable of understanding the complexities of using technology, for example, item nine, using an encryption program. It is more important to make the home computer user aware that such technologies exist, what they can be used for, and how they help to secure an environment. While users may not implement all nine items as suggested by CERT, they may implement some, thereby reducing their exposure to potentially troublesome viruses and hackers, and when they become more proficient expand on the additional countermeasures.

Wireless Security

Many individuals, who are worried about the security of their work or home computers, are less concerned when they are using their laptops and connecting to the Internet wirelessly. Again, this may come simply from a lack of awareness, and not realizing the dangers that are posed when using wireless technology. It is reported that while attackers are using sophisticated attacks to uncover information, humans are often more fooled by the simpler attacks, and at times even ignore warnings from their own security software loaded on the personal computer (Cranor, 2006).

In a typical land-based network environment, a computer has to physically be plugged into an outlet, for example, a CAT5 Ethernet outlet, but in a wireless environment, a system can connect to any wireless access point it receives a signal from. These so-called hot-spots allow wireless communications to take place. There are no national standards on these hot-spots. In some cases users are charged a fee and use specific authentication methods, and in other places, there are no charges and no authorization mechanisms in place.

In wireless security attacks, it is important to understand the importance of the seven-layer open systems interconnect (OSI) model which describes different layers and functions of computer communications, access, and the flow of data packets. The first layer is the physical layer, where security attacks usually happen, and is also the most susceptible and easiest for attackers. The most common form of attack is a rogue access point, where an attacker actually offers a signal from their own access point that allows Internet connectivity. It convinces the wireless client to use this access point, and once that client is attached to that access point, an