6.915 Computer and Network Security	**Fall Term, 1995**

Lecture 1 : September 7, 1995

Lecturer: Ron Rivest *Scribe: Rosario Gennaro*

6.915 is a new subject on Computer and Network Security. It's mostly intended for seniors and first-year graduate students. By going through the course outline we can see that the covered topics can be divided in three big parts. After a brief introduction on the general topic of security the first part of the course will deal with a fundamental tool that we will use during the rest of the course: *Cryptography.* We will discuss classical secret–key cryptosystems, and more recent public–key schemes. We will introduce digital signature schemes and talk about other cryptographic primitives as hash functions. We will also mention some more sophisticated cryptographic protocols like secret sharing, oblivious transfer, commitment, zero–knowledge proofs. We will then move on *Computer Security.* This area will cover topics like user's authentication, intrusion detection, access control, computer viruses, covert channels, secure operating systems, etc. We will also discuss formal models for computer security. Finally we will move on the area of *Network Security* with a special focus on Internet. We will talk about the Internet Protocol and its security issues. We will study firewalls and network protocols like Kerberos. Tentatively we will discuss specific internet features like: electronic mail, World–Wide–Web, electronic commerce, etc.

1 Security Objectives

In this class we will learn how, given a computer system we can identify and possibly solve its security problems. First of all this means that we have to define and outline what we mean by security. The computer system can be anything you may think of: a shared system, a Web server, a bank ATM, the cable–box on your TV and so on. For each case to define what security is, it actually means to specify a **security policy**, i.e., a set of desired goals. For example in a shared system only authorized users should be able to login, for a Web server accessing clients should pay a fee and so on.

Once a security policy has been specified we need to put in place **security mechanisms**, i.e., tools that make sure that the desired goals are met. For example a password scheme will (hopefully) give access to a shared system only to authorized users. A payment protocol will ensure fee payments for clients accessing a Web page.

Once the security mechanisms are put in place they need to be reviewed in order to assess possible **vulnerabilities** of the system, i.e., weakness of the system that leave it open to attacks. Hostile parties who exploit weaknesses in order to create damage are known as **threats**.

If vulnerabilities are identified, the a **safeguard** or a **countermeasure** must be designed in order to eliminate the weakness.

1.1 Goals

As we notice above there are many different goals, depending on what purpose the computer system is fulfilling. However we can group goals in three broad categories:

Confidentiality: Assets of the computer system should not be accessible by unauthorized parties.

Integrity: Assets of the computer system should not be modified by unauthorized users.

Availability: The system should be available to authorized users. A *denial of service attack* is an attack that infringes availability of the system.

Other goals may also come up: for example in a payment protocol one could require anonymity of the parties (as in with real–life cash), which does not seem to fall under any of the categories above (although confidentiality is probably the closest.)

1.2 Mechanisms

In the course of this class we will explore many possible security mechanisms. Some typical ones include in order of more sophistication:

User awareness By educating users about the security goals of the system and the possible risks, one can achieve one of the most effective security mechanism.

Physical protection Locks and keys prevent unauthorized access to buildings where computer systems reside. Shredders make snooping in the trash useless. Degaussers really delete the content of your floppy (differently than the DELETE command that usually just removes a pointer to them) and so on ...

Cryptography As we will see later in the class encryption functions can be used (in different ways) to enforce both confidentiality and integrity.

Access Control For example in UNIX access control lists specify which users can read, write, execute a given file.

Auditing By recording all the activities of the system it is possible to detect security breaches that could not be prevented.

As we can see, some mechanism aim to *prevention* while some others to *detection* of security breaches. The latter is particularly important since we are never sure to have ruled out all possible attacks. It is important then to detect is something is going wrong and take the necessary countermeasures.

1.3 Principles

In order to design effective security mechanisms we will refer to some general *security principles*. For example:

- *Principle of least privilege* : Give a user or process only privileges needed to perform task at hand. No more, no less.
- *Minimize amount of trusted components* : Identify what components of the system needs to be trusted and aim to keep those small and simple.
- *Do not aim for perfection* : It is basically impossible. Instead be prepared to detect problems, to design countermeasures and to recover from attacks.

2 Ethics

We mentioned above that user awareness is one of the most effective security mechanisms. Users in particular should be educated about the ethics of the use of computer systems. This is particularly important for students in this class. You may end up gaining knowledge that will allow you to mount unethical attacks to computer systems. This is not the purpose of this class. Please read and be bound to the Code of Ethics that we distributed in class. Thanks.

3 Handouts and Readings

There were three handouts: Course Information, Course Outline and Code of Ethics. Chapters 1 and 15 of Pfleeger cover some of the material we discussed today,