Unit 4

Programs

Principles of Network Security

When computer networks were first developed, they were used on a small scale in a trusting environment. Since then, the size of computer networks has expanded exponentially into an environment fraught with malicious intent. Computer scientists and related experts have been working to secure computer networks ever since. The following are some fundamental principles of network security.

Authentication

It is often necessary to make sure that only a single person can access a computer, an email account, or a social media account. The problem then becomes: how can a computer verify that some person is who they claim to be? There are many approaches to authentication. A couple common ones are listed below.

- Username and Password

  Username and password authentication is by far the most common form of authentication. A user is assigned a username and the user makes up a secret password. Ideally, the password is hard to guess and known only to the user. If someone can provide the correct username and password, then he or she should, in theory, be the user who originally created the secret password.

  In reality, this method of authentication has three major faults that can be attributed to the laziness and error of people:

  1. People write down and share their passwords often
  2. People make easily guessable passwords
  3. People often use the same password across multiple different services

  The second problem with username, password authentication is usually solved by enforcing password complexity rules. You may have noticed that many websites force you to make a password that is of a certain length and has special characters.

  The third problem with username, password authentication is somewhat eased by forcing users to change their passwords every 3-6 months or at some regular interval.

- Biometrics

  Biometric authentication is much more advanced than username, password authentication because it relies on unique physical characteristics of the human body to identify people. This form of authentication is often more expensive and harder to implement, but the extra security is necessary in some applications. A few common forms of biometric authentication are listed below.

- Fingerprint Scanners
- Voice Recognition
- Facial Recognition
- Iris Scanners

Encryption
Think of the last time you logged into a social media website or purchased something with your credit card off the internet. You most likely assumed that when you entered your credit card or password that no one would be able to retrieve them. In reality, your password and credit card information was sent across the internet where anyone with the right tools and knowledge could have intercepted it.

To defend against this, the information must be **encrypted**, so that only the receiver can **decrypt** it, and the information will appear as garbage to anyone in the middle. We will take a simple overview of how this is done.

RSA Encryption
One of the most popular cryptosystems is the RSA (Rivest-Shamir-Adleman) cryptosystem. It is an asymmetric cryptosystem, meaning that there are two distinct keys in this cryptosystem:

A **public key**, which is made available to everyone.

A **private key**, which is secret, and only known by the person who is intended to receive and decrypt the messages.

How it works
Let's assume that I am amazon.com, and I want people to be able to securely send me their credit card information. Using the RSA cryptosystem (some very complicated math), I will generate a public key, private key pair.

I will then keep the private key to myself in secret but make the public key widely available to everyone. When someone wants to send me their credit card info, they will use the public key to "lock" (encrypt) their info. Once that information has been "locked" with the public key, only my private key can "unlock" it.

The user encrypts their message with the public key, sends it securely to me, and then I can "unlock" (decrypt) it with my private key.

Network Security Techniques

Even the most robust cryptosystems are useless if you adopt bad security practices. There are two basic practices that every internet user should adopt that will immediately make them less vulnerable in this age of identity theft, hacking, and phishing.

Using a Strong Password

This may come as common sense to most of us, but a surprising number of users still use "12345" or "password123" as their online passwords. Using common passwords is a very bad idea, as there are programs that can guess millions of commonly used passwords and crack your password in less than a few seconds.

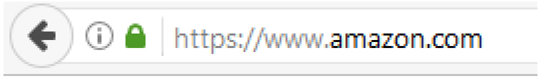
The best passwords are at least 10 characters long, and are made up of random strings of characters. Although these may be hard to remember, there is a good middle ground. Choose a password that is phonetically easy to remember, but is, in reality a seemingly random string of characters.

Example:	Weak Password:	fidothedog123
	Strong Password:	f!doTHEd0g123

It is also incredibly important that you don't use the same password for multiple sites.

Only Log into Sites that Use HTTPS

Any reputable site will use HTTPS to make its connections. Essentially, this means that site has been verified and issued a certificate by an independent third party company. The easiest way to check for this is to look at the URL in your address bar.



A green lock symbol should be visible, and the address should start with "https://" not "http://." This does not mean that websites that don't use HTTPS are bad necessarily. Just don't log in to them or input any personal information.