Computer Security
Revision Notes
Ver 0.1

Guy Taylor

April 2011

Contents

1 Introduction

This document is a set of revision notes for the Computer Security [1] course at the Univerisy of Edinbugh.

2 Terminology

Main buzz words

Cryptography The secret writing with *ciphers*

Cryptanalysis Breaking ciphers

Cryptology Both the above

Encryption Converting *plain text* to *cipher text*

Decryption Converting *cipher text* to *plain text*

Encryption Scheme, Cipher, Cryptosystem Mechansisums for encryption and decription

What is security for

Confidentiality No agent other than the thows with permision can view the content

Integrity The data recived is in fact the data sent

Authentication I am who I say I am

Non-Repudiation Layered security. Agents with insefisient rights cannot do sertaint things.

Primitives

Plain Text The unencripted message

Plain Text The encripted message

Key The secret that needs to be know to encrypt or decrypt a message

Hash A *one-way* function. Used so help prevent realeasing the real key.

3 Malises Progams

Malware is common

3.1 Trojan *Horse*

A program that acts beinie such as a game or utility which actualy runs malisshus code while in use as the macerading program.

3.2 Virus

A program that hides within a normaly unexecutable file (eg pictures, word documents....) that when opened (including previewd by a file manager) causes the parent applicatyion to run malichious code.

3.3 Worm

A self-replication aplication. The application will try to copy itself over a network or on phisical media (ie USB drives and CDs)

3.4 Rootkit

A program that embeds itself within the Operating System. This allows it to intersept File System calls to hide itself and apply other coutermesures. These programs are hard to remove as they operate at a lower or simmilar level to Ant-virus scanners.

3.5 Loggers

Keyloggers and Screenloggers record all screen or keyboard movements. They can include filters so sensative information such as X many keys before and after a credit card (x meany numeric digits). This information is then sent back to a location to be prossesed and missued.

3.6 Web Trojan

bob

Note: The random term ”Crimeware” was used in the lecture notes with only a subsection of the above. All can be used to good or evil so all are ”crimeware” if they are used for crime ...

4 Phishing and Spoofing

TODO

References

[1] "Computer Security" "http://www.inf.ed.ac.uk/teaching/courses/cs/"