Midterm Exam
IT-S448, ITMS 448 / 548
Autumn 2014

Terminology

Understand terminology

Cryptanalyst

Code *Cipher*

Substitution *Transposition*

Steganography *Polyalphabetic Substitution*

Monoalphabetic Substitution

Block chaining

Substitution/permutation ciphers

Viruses, Worms, Trojans…

Hackers, crackers, script kiddies…

General Cipher Knowledge

A strong cipher system can protect against cryptanalysis that has much information about the cipher system. What constitutes this information?

Major causes of insecurity

- *Complexity*
- *Poor coding*
- *Technology weaknesses*
- *Configuration weaknesses*
- *Policy weaknesses*
- *Human factors*

Specific Cipher Knowledge

Be able to encode or decode a simple transposition or substitution cipher

Be able to determine keys and encode or decode a simple RSA cipher

Understand the concepts of modulus arithmetic

Know <u>key</u> values of integer powers of 2

e.g., $2^8 = ?$

$2^8 = 2^{10} / 2^2 =$ **1024** $/ 4 = 256$

$2^8 = 2^{(10-2)} = ($**1024** $/ 2) / 2 =$ **256** $= 512 / 2 = 256$

$2^{13} = ?$

$2^{13} = 2^{10} \times 2^3 =$ **1024** $\times 8 = 8192$

$2^{13} = 2^{(10+3)} = [($**1024** $\times 2) \times 2] \times 2 = 2048 \times 2 \times 2 =$

$=$ **4096** $\times 2 = 8192$

Specific Malware

Back Orifice

Architecture & Organization

How it might be used

…

Specific Malware

ARP Poisoning

How it works

What sort of attacks is it good for?

What are its limitations?

Be able to do a simple ARP poison on paper

Types of Attacks

Floods

IP Fragmentation

Spoofing

Buffer overflows

Man in the Middle

Replays

…

Smurfs

DoS and DDoS

TCP Hijacking

Be able to analyze a simple piece of pseudocode to determine if it might cause a buffer overflow

How Attacks Function

Explain how a certain attack operates

Especially taking advantage of a TCP connection setup

Given a situation, describe what type of attack it is

Simple ARP poisoning question

Secret Writing

Types of secret writing; -- taxonomy

Examples of types of secret writing

Symmetric encryption

Asymmmetric encryption

Hashing

Given a situation, show how you would accomplish achieving a certain goal

Be able to use symbolic notation

e.g., $E_k[P] = C$ $D_{Kpu}[C] =$

The four goals of secret writing

MACs

Message authentication codes - MACs

DAC

HMAC

Advantages of MACs over hashing

Information Theory

Concepts of

Side info *Unicity distance*

Per character language redundancy

One Time Pads

Why are they considered unbreakable?

Information entropy concept

General Concepts

Time to infect an unprotected networked computer.

Some accepted security truths and goals

Attacker motivation

General sources of software problems

Major sources of threats

Definitions

Computer security

Network security