Foundations of Computer Security

Lecture 41: Using Information

Dr. Bill Young
Department of Computer Sciences
University of Texas at Austin

Cryptanalysis

Attacks on an encryption algorithm are classified according to what information is available to the attacker.

Ciphertext-only: attacker has only encrypted text

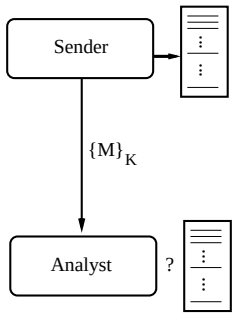
Known plaintext: attacker has some ciphertext/plaintext pairs.

Chosen plaintext: attacker can cause messages of his choosing to be encrypted.

Adaptive chosen plaintext: chosen plaintext attack adjusted according to earlier results.

Chosen ciphertext: attacker can decrypt selected ciphertext.

Breaking a Cipher



A cryptanalyst's task is extracting the correct decryption from the space of possible decryptions, given limited information.

How much can she glean from the ciphertext and the circumstances to reduce the search space?

Thought Experiment: Using Information

Question 1: Suppose you know that "xyy" encodes a string in the English alphabet (26 letters) using a substitution cipher. *How many decryptions are possible?*

Answer 1: $26^3 = 17576$

Question 2: Add the information that it's a simple substitution cipher.

Answer 2: $26 \times 25 = 650$. (Reduce search space by a factor of 27.)

Question 3: Add that you know the plaintext is an English word:

Answer 3: around 40. (Reduce original search space by a factor of 439.)

Perfect Ciphers

A *perfect cipher* would be one for which no reduction of the search space is gained from knowing:

1. the encryption algorithm, and
2. the ciphertext.

The attacker's uncertainty (the likelihood of guessing the plaintext) of the message is exactly the same *whether or not she has access to the ciphertext.*

Do you think a perfect cipher is possible?

Lessons

- The cryptanalytic task is to reduce the uncertainty in the message (plaintext) using all available information.
- A perfect cipher would be one in which no reduction of the search space is possible, even given access to the ciphertext and algorithm.

Next lecture: A Perfect Cipher