

PF574

Pbzchgre Frphevgl

Fna Qvrtb Fgngr Havirefvgl

Fcevat 2008

Yrpgher #3

CS574

Computer Security

San Diego State University

Spring 2008

Lecture #3

Today's Structure

- Administrivia
- Questions
- Recent News
- Lectures
- Crashers

Administrivia

- Crashing
 - Depends on having add codes with me.
 - Transcripts collected at the end of class.
 - Looks like all crashers can make it
- Roll

Questions?

Recent News

- Investigating Phishers
- Money Mules
- Foiled Bank Heist

Lecture

Cryptography Basics

- Cryptography
Hidden or secret writing; the practice of keeping messages secure.
- Cryptanalysis
The practice of reading hidden/secret writing.
- Cryptology
The study of cryptography and cryptanalysis.

Cryptography Basics

- Encryption
The process of encoding (obscuring) a message.
- Decryption
The process of decoding (revealing) a message.
- Plaintext
The original message to be encrypted.
- Ciphertext
The result of encrypting the plaintext message.

Cryptography Basics

- Code
Replacing words or phrases with other words.
- Cipher
Replacing symbols with other symbols.
- Key
A means for choosing between related ciphers; alternatively, an additional input to the encryption.

Cryptography Basics

- Cryptosystem

A system for encrypting plaintext into ciphertext and decrypting ciphertext into plaintext.

- Participants

- Sender

- Receiver

- Adversary

Cryptography Basics

- Attack
An attempt by the adversary to decode the ciphertext.
- Brute Force
An attack characterized by exhaustive trials.
- Possible does not necessarily imply feasible.

Cryptography Basics

- symmetric keys

The same key is used to encrypt the plaintext as is used to decrypt the ciphertext.

- asymmetric keys

One key is used to encrypt the plaintext and a different (but related) key is used to decrypt the ciphertext.

Notation

- k_n = when multiple keys are involved, key # n
- P = plaintext
- C = ciphertext
- $E(K,T)$ = encrypt text T (normally P) with key K
- $D(K,T)$ = decrypt text T (normally C) with key K

Ciphers

Ciphers

- Caesar Cipher
 - Example of a simple substitution cipher
 - Generalized to “rotN”
 - Attack with frequency analysis
- Homophonic (substitution) ciphers
- Digram (e.g., playfair) cipher (polygram)

Ciphers

- monoalphabetic substitution cipher
A cipher that always encrypts the same plaintext symbol to effectively the same ciphertext symbol (i.e., decrypts the same ciphertext symbol to the same plaintext symbol).
- polyalphabetic substitution cipher
A cipher that encrypts the same plaintext symbol to potentially any ciphertext symbol.

Ciphers

- Some Polyalphabetic Ciphers
 - Vigenère Cipher / Tableau
 - Uses a keyword to choose rows
 - Enigma
 - A rotor cipher
 - Book (running-key) cipher

Ciphers

- Transposition Ciphers
 - Rail Fence
 - Columnar Transposition
- Product Ciphers
 - Combines two or more ciphers
 - Often iterates several weak operations
 - Aim to make ciphertext look random
 - Ideally make every bit of ciphertext depend on every bit of plaintext and key

Cipher Attacks

- Frequency Analysis
- Repetition
- Cribs
- Stereotyped Beginnings and/or Endings

Cipher Attacks

- ciphertext only attack
- known plaintext attack
- chosen plaintext attack
- adaptive chosen plaintext attack
- chosen ciphertext attack

A Perfect Cipher

- The One Time Pad (OTP)
- Requires True Randomness
- Provably Secure
- Can only use once
- Vigenère's Tableau or XOR

Aside: Steganography

- Don't mumble and say stenography!
- “Hidden Writing”
- Embed message in a larger dataset
 - bits in an image
 - typos in a document
 - etc.

What's a Good Cipher?

- Strong Algorithm
- Small Secrets (aka keys!)
- Good Implementation

Strong Algorithms

- Based on sound mathematics
 - Symmetric - algorithm review
 - Asymmetric - hard problems
- Peer reviewed (it's *hard* to devise a good algorithm)
- Secrecy in the key, not algorithm
- Large key space to resist brute-force attacks

Strong Algorithms

- Should resist known attack techniques
(a cryptographer should first study cryptanalysis)
- Ciphertext should *appear* random (to statistical tests)
 - Confusion
 - Diffusion
- Necessary \neq Sufficient

What's a Good Cipher?

Shannon's Characteristics

- Amount of secrecy need determines the amount of labor appropriate.
- Keys and algorithm should be free from complexity (i.e., allow any key, any data).
- Implementation should be simple.
- Errors enciphering should not propagate.
- Ciphertext size no larger than plaintext.

Snake Oil

Snake Oil

- “Trust Us”
- Technobabble
If you don't understand it, maybe it makes no sense.
- Secret Algorithms
Why won't they let anyone look at the algorithm?
“Assumed Information”
- Anonymous experts

Snake Oil

- “Military Grade”
No such thing.
- “Unbreakable”
- “Based on OTP”
OTP bits cannot be generated by algorithm or cipher.
- “Revolutionary”
Note difference between new cipher and new product.

Snake Oil

- Does the product let you generate your own keys?
- Are all keys probable? (Passwords and passphrases aren't equally probable.)
- Are the keys recoverable?
- Do you need their features?
(Sometimes corruption is worse than disclosure.)

Theory

Information Theory

- Measuring Information

The amount of information in a message is the minimum number of bits to encode all possible meanings.

- Entropy

$e = H(M)$; measured in $\log_2 n$ where n is # of meanings.

- Rate (bits per letter)

$r = H(M)/N$ where $N =$ length of the message

- Absolute Rate

$R = \log_2 L$ where $L =$ number of characters in the language

Information Theory

- Redundancy
 $D = R - r$
- English Language
 - absolute rate is $\log_2 26$ or ~ 4.7 bits/letter
 - (measured) entropy is ~ 1.3 bits/letter
 - redundancy is ~ 3.4 bits/letter

Information Theory

- The more redundant the language, the easier it is to cryptanalyze.
- Entropy of a cryptosystem is a measure of the size of its keyspace: $H(K) = \log_2 K$
- Perfect Secrecy
Is a cryptosystem in which the ciphertext yields no possible information about the plaintext.

Out Of Time

Lecture References

- Pfleeger, *Security in Computing*, 3rd & 4th edition
- Bishop, *Introduction to Computer Security*
- Schneier, *Applied Cryptography*
- Schneier, *Practical Cryptography*
- Schneier, *The Crypto-Gram Newsletter*, Sep. 15, 2002
- Singh, *The Code Book*
- RSA Laboratories, *RSA Crypto FAQ*
- Gutman, *Lessons Learned in Implementing and Deploying Crypto Software*
- Rothenburg, et al., *The Snake-Oil FAQ*
- *They Cryptography FAQ*

End Lecture

Reading

(For the next few classes)

- Pfleeger, Chapter 2
- Pfleeger, Chapter 12
- Snake-Oil FAQ

<http://www.interhack.net/people/cmcurtin/snake-oil-faq.html>

(Keep Reading)

Finis