Cryptanalysis

Cryptography ThreeB

Ed Crowley

Fall '08

Topics

- Cryptanalysis
- History
- Modern Cryptanalysis
- Characterization of Cryptanalysis Attacks
- Attack Types

Focus

- Cryptanalysis.

Cryptanalysis

- Science of cracking ciphers and codes, decoding secrets, violating authentication schemes, and in general, breaking cryptographic protocols.

Cryptanalysis History

- In 1920, The term "cryptanalysis" was coined by William Friedman to describe methods for breaking codes and ciphers.
  - Though, the craft of cryptanalysis is much older.
- For most classical ciphers, frequency analysis is the basic tool.
  - In natural languages, certain letters of the alphabet appear more frequently.
    - In any sample of English plaintext, "E" is likely to be the most common letter.
    - Similarly, the digraph "TH" is the most likely pair of letters.
  - Frequency analysis relies on a cipher failing to hide these statistics.

Rise of Mathematics

- As ciphers became more complex, mathematics became more important in cryptanalysis.
- This change was particularly evident during World War II.
  - Efforts to crack Axis ciphers required new levels of mathematical sophistication.
  - Automation was first applied to cryptanalysis in that era with the Polish Bomba device

Modern Cryptanalysis Context

- By most measures, modern cryptography has become much more impervious to cryptanalysis than the pen-and-paper systems of the past.
- Most attacks are against the implementation and few are against the underlying algorithm.
  - As William Hugh Murray has observed, … there are an infinite number of ways to implement an algorithm, most of them wrong.
- While we can make statements, about cryptographic strength in the abstract, we can only make statements about security in a specific application and environment context.

Modern Context

Computers have both increased the need for, and decreased the cost of, cryptography.

- Effectiveness of cryptographic algorithms now resides in complexity rather than in secrecy.
- Understand that strong security is different than strong cryptography.
- While modern algorithms are resistant to all but the most resourceful attacks, in practice they are no stronger than the systems and applications in which they are used.

Examples

- The A5/1, A5/2 and CMEA algorithms, used in mobile phone technology, can all be broken in hours, minutes or even in real-time using widely-available computing equipment.
- In 2001, Wired Equivalent Privacy (WEP), a protocol used to secure Wi-Fi wireless networks, was shown to be susceptible to a practical related-key attack.

Characterizing Cryptographic Attacks

Goal

- Gain ability to decrypt new cipher text
  - Without additional information.
  - Intermediate goal: crack message key.
- Attacks characterized by three criteria.
  1. Prerequisite knowledge and capabilities needed
  2. Additional secret information deduced
  3. Effort required

Attack Types

- Prior knowledge scenarios
  - Ciphertext Only
  - Known Plaintext
  - Chosen Plaintext
    - Adaptive Chosen Plaintext
    - Differential Cryptanalysis
  - Chosen ciphertext
    - Adaptive chosen ciphertext
- Symmetric Algorithm Attacks
  - Brute Force
  - Meet in the Middle
  - Statistical
- Hash Attacks
  - Birthday attack
- Network Attacks
  - Man in the Middle
  - Replay
- External attacks:
  - Black-bag cryptanalysis
  - Rubber-hose cryptanalysis

Cryptographic Attacks

- Ciphertext Only
  - Cryptanalyst obtains several ciphertext samples.
    - Without plaintext
  - Goal: Determine key.
    - Most difficult type of attack.
    - Requires a very large ciphertext sample.
- Known Plaintext
  - Based upon ciphertext/corresponding plaintext samples.
    - Could be partial (repeating headers)
  - Goal: determine key

Cryptographic Attacks

- Chosen Plaintext
  - Cryptanalyst can choose what plain text message he wishes to encrypt and view the results.
    - Much, much, stronger than known plain text attack.
  - Optimum type of attack.

Cryptographic Attacks

Adaptive Chosen Plaintext

- Special case of chosen-plaintext attack in which the cryptanalyst is able to choose plaintext samples dynamically, and alter his or her choices based on the results of previous encryptions.

Linear Cryptanalysis

- Specific type of chosen plaintext attack
- Succeeded in 1992 against DES
  - Took 50 days
  - Took 2^{14} operations
- Faster than brute force but not relevant …

Differential Cryptanalysis

- Differential Cryptanalysis
  - Specific type of chosen plaintext attack.
    - Looks at the difference between two text blocks
    - Makes use of the fact that after a specific number of rounds, diverse differences bring out specific intermediate results with different probabilities.
    - Based on this, and the known difference between input and output, a statistical forecast can be made about the key
  - Goal: obtain key

Cryptographic Attacks

- Chosen-ciphertext
  - Cryptanalyst may choose a piece of cipher text and attempt to obtain the corresponding plaintext.
    - Generally utilized with public-key cryptosystems
- Adaptive-chosen-ciphertext
  - Scenario in which a cryptanalyst has free use of a piece of decryption hardware, but is unable to extract the decryption key from it.

Symmetric Algorithm Attacks

- Brute Force
- Meet in the middle
- Differential cryptanalysis
- Statistical

Brute Force

- Originally meant trying every possible key until correct key is identified.
  - Advances in computing performance over time makes brute force an increasingly practical attack against fixed length keys.
  - In certain contexts, a dictionary attack can be considered a form of brute force.
  - Now, most often implemented as smart brute force attacks
- Not all cryptosystems utilize key space appropriately.
  - Those that don't are vulnerable to 'smart' brute force attacks.
    - Makes key likely to be found without searching the entire keyspace.

Symmetric Attacks

- Meet in the Middle
  - Applied to double encryption schemes by encrypting known plaintext from one end with each possible key and comparing the results in the middle.
    - Works brute force from both ends.
    - Why 2DES doesn't work
- Statistical
  - Exploiting the lack of randomness in key generation.

Hash Attacks

- Birthday attack
  - Usually applied to the probability of two different messages using the same hash function that produces a common message digest or
  - Given a message and its corresponding message digest, finding another message that when passed through the same hash function generates the same specific message digest.

Network Attacks

- Man in the Middle
  - An attacker taking advantage of the store and forward nature of a network.
  - Works by intercepting messages and forwarding modified versions of the original messages while in-between two parties attempting secure communications.
  - SSL vulnerability

Algorithm Criteria

- A good algorithm must withstand a chosen plaintext attack, otherwise it is not secure.
- If known plain text or a cipher text only attack succeeds, then algorithm should be discarded.

Side Channel Attack

Questions?

References

FM 34-40-2, Basic Cryptanalysis

http://www.umich.edu/~umich/fm-34-40-2/