Encryption

Wednesday, 17 January 2018 8:27 PM

Introduction

- Security models are created specific to known attack patterns
- DDoS - botnets
- Computer system was designed to be open in the past, minimal security concerns

Encryption

- K sent via secure channel, C sent via public channel open to E
- Crypto.Cipher in python

Substitution Cipher

- PT/ CT: strings over a set of symbols U
- Key: bijective function from U to U
- Key space size = number of possible keys
- Key size = number of bits to represent key (log2)

Attacks

- Large number of CT, known PT attack
- Exhaustive/ brute force - takes too long, negligible probability of success
- Vulnerable to frequency analysis, not secure under CT-only attack

Permutation/ Transposition Cipher

- Multiple permutations = no effect
- Effects of multiple Substitutions/ Permutations?*

One-time Pad

- Encrypt = PT $\oplus$ K = CT
- K and PT have to be same length (might as well send PT)
- Mostly for one-time use; useless (unless key is pre-established)

Modern Ciphers

- NSA Type 1:
- RSA (public key algorithm)
- AES still considered to be secure
- Measure key space size (exhaustive search is the attack speed)
- 128-bit key size considered secure (256-bit for long-term security)
    - Speed of computers increasing rapidly (distributed computing)

Stream Ciphers

- Extend secret key to size of PT -> one-time pad
- Cryptographically secure pseudorandom sequence

Block Ciphers

- Fixed input/ output size
    - Padding of input to match block size
- Mode-of-operation to extend block cipher
    - Electronic Code Book (ECB) mode
    - CBC and CTR (stream cipher) mode

Cryptographic Pitfalls

Initial Value

- Initial Value (IV) - either RNG or counter
    - Else, pairwise XOR of PT will reveal info
    - Different IV = different secret key from generator algorithm
    - Every encryption of the same plaintext yields a different ciphertext
    - New Ciphertext = IV + Ciphertext
- Mishandling IV
    - Generating from filename/ author (metadata), Microsoft RC4 Flaw
    - BEAST attack for AES in CBC mode
    - IV cannot be predictable (not simply incremental)

Generating Random Numbers

- Pseudo RNG has to be used carefully
    - Not derived from seed in a deterministic manner
- Using Time of the Day

Design Principles

Kerckhoff's Principle	Security through Obscurity
- System should be secure if everything is known (except secret key) • Assume that attackers know the algorithms - Easier to quantify security of system	- Hide design of system to achieve security - Reliance on Obscurity - Non-secret things need not and should not be published • E.g. Presence of unpatched bugs

MIFARE Classic

- Improvement on magnetic stripe which can be read by any reader (through API call)
- Secret key used to perform encryptions
- Crypto-1 Algorithm with a 48-bit key

History

Enigma Machine

- PT and CT cannot be the same letter
- Broken by Bombe (exhaustive search)

Readings

Cipher Machines: http://ciphermachines.com/index
https://technet.microsoft.com/en-us/library/2008.06.obscurity.aspx
24C3: Mifare (Little Security, Despite Obscurity)
http://resources.infosecinstitute.com/ssl-attacks/
Imitation Game