Lecture 4

Thursday, February 2, 2017 1:59 PM

Presentation: Operation Pacifier

- What happened? FBI received tip on Tor Browser Hidden Service "Playpen"
- Developed malware to track users (hosted it in their office getting information from users)
- Tor?
  - Developed by Navy to help protect communication abroad
  - Owned by Tor Project
  - Anonymizes sender IP on the web
    - Good? Journalists to rename anonymous
    - Bad? Black market sales
  - Tor client --> Guard (only knows client and middle not destination) --> middle (knows guard, everything else but doesn't know where you're going --> exit --> destination
    - Exit node doesn't know who you are but knows where you're going
    - Destination only knows exit nodes IP (aka people who volunteer to do this are screwed)
- Surface web vs. Tor vs. Tor hidden services
  - Knows alice and bob
  - Knows alice but not bob
  - Knows both
- Zero-Day vulnerability (no one knows who you are)
- NIT aka malware - placed on user computers (IP and MAC sent to FBI)
- Why was the warrant legally questionably? Rule 41
  - Concens: privacy and 4th amendment

Example schemes:

- One-time pad
- AES(as the PRP)-CBC mode
- 1-bit encryption with OTP

Attacks on encryption

- Key recovery (extract secret key that is used to encrypt)
  - Adversary outputs secret key
  - Most difficult attack
- Recovery of plaintext
  - Adversary outputs plain text
- Indistinguishability
  - Adversary chooses messages m_0 and m_1
  - Challenger selects either message and encrypts it (choose random bit,b)
    - Then computes cipher bit
  - Challenger then sends back the ciphertext
  - Adversary has to guess which one it is.
  - (1)
    - What do we want adversary to learn and still fail at A ?
      - Known ciphertext attack (KCA)
      - Chosen plaintext attack (2) (CPA)
        - Most encryption schemes are required to prevent this attack
        - Encryption oracle
        - What prevents in his learning face to choose to look at the ciphertext of m0 and m1 and picks the correct one
        - The inputs have to vary even if the messages are the same
        - If you put in a plaintext a number of times, it cannot produce the same cipher text.
        - Note: m0 and m1 may be queried during the learning phase
          - By defining security this way
          - Rule out any deterministic encryption scheme satisfying CPA security
          - Rules out electronic codebook mode
            - How can prove this?
            - Query m1 and m0 and then ask for m1 and m0 as your
              challenges and you pick the one that returns ciphertext
            - (4)
      - Known plaintext attack (3) (KPA)
      - Chosen ciphertext attack (5) (CCA)
    - Rank (easiest for adversary/ more secure) CCA < CPA < KPA < KCA.

Why do we choose a different IV vs. choosing a different key?

- It's a way for ensuring randomization for input
- Also changing the key every time has a HIGH cost

AES-CBC mode satisfies CPA security under the assumption that AES is a good PRP
AES-CTR mode satisfied ^^^^^^^

Need to be expected to show that something is not secure based off of the scheme and a security definition (using an attack)

If AES is a secure PRP, then AES-CBC mode is IND-CPA secure
But AES-CBC mode is not IND-CCA secure

- In order to achieve this, you need integrity (preventing someone from tampering with this)

If flip a bit in ciphertext , then you can see the change that happens in the plaintext

Modify ciphertext in a way rhat you know the effect it has on the plaintext
Mallability - an encryption scheme is mallable if I can alter bits in ciphertext