Encrypted Storage Attacks

Travis H.
travis+security@subspacefield.org

http://www.subspacefield.org/~travis/

AHA, 27 Feb 2008

Outline

1. Non-Cryptographic Attacks
2. ECB Mode Weakness
3. CTR Mode Time Series Attack
4. Watermarking Attack

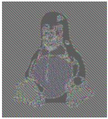
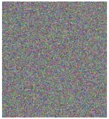
Non-Crypto Attacks

1. keylogger, jitterbug
2. side-channel attacks [1]
3. if OS is unprotected, trojan-horse the OS and/or crypto software
4. steal the key while the volume is open
5. reboot the system and quickly pull the key from memory[5]
6. can identify possible crypto keys in memory using entropy measurements

ECB Mode Weakness

- ECB (Electronic Code Book) is the simplest approach:

$$C_i = E_K(P_i)$$

- Weakness: if more than one block of plaintext encrypted under the key, same plaintext always encrypts to same ciphertext.
- plaintext ECB  optimal 
- Obviously some structure of original remains at granularity above the encryption block size

CTR Mode Time Series Attack

- CTR mode seems perfect for random-access devices:

$$C_i = P_i \bigotimes E_K(i)$$

- Time series attack: take several samples of ciphertext C_i in a given block over time
- $E_K(i)$ is constant, so we have multiple $P_i \bigotimes c$ for various times
- XOR with a constant not a strong encryption scheme!
- If distribution of P_i is non-uniform, so is C_i
- We can often deduce c by using e.g. superimposition step of Kasiski examination[2]

Background on CBC Mode

- Block devices must give random access to each disk sector
- Thus each disk sector encrypted independently
- For purposes of discussion, assume block device using CBC mode encryption:

$$C_{\mathrm{i}} = E_{\mathrm{K}}(P_{\mathrm{i}} \bigotimes C_{\mathrm{i\text{-}1}})$$

- First value ($C_{\text{-}1}$) is called initialization vector (IV)
- No place to store IVs, so just let $IV_{\mathrm{i}} = i$

Watermarking Attack

- Requires adversary be able to store data on encrypted drive (chosen plaintext)
- For two blocks i,j with known difference $IV_{\text{i}} \bigotimes IV_{\text{j}}$, adversary provides $P_{\text{i}}, P_{\text{j}}$ such that

$$P_{\text{i}} \bigotimes P_{\text{j}} = IV_{\text{i}} \bigotimes IV_{\text{j}}$$

$$P_{\text{i}} \bigotimes IV_{\text{i}} = P_{\text{j}} \bigotimes IV_{\text{j}}$$

- Thus,

$$E_{\text{K}}(P_{\text{i}} \bigotimes IV_{\text{i}}) = E_{\text{K}}(P_{\text{j}} \bigotimes IV_{\text{j}})$$

$$C_{\text{i}} = C_{\text{j}}$$

- Statistically shows your disk has adversary's data w/o breaking crypto

For Further Reading I

- Travis H.
  Security Concepts
  http://www.subspacefield.org/security/
- http://en.wikipedia.org/wiki/Kasiski_examination
- http://en.wikipedia.org/wiki/Watermarking_attack
- http://en.wikipedia.org/wiki/Block_cipher_modes_of_opera
- *Lest We Remember*, http://citp.princeton.edu/memory/