Crypto VII: An Attack on Encryption

Cryptographic Hardware for Embedded Systems

ECE 3894

Fall 2019
Assoc. Prof. Vincent John Mooney III
Georgia Institute of Technology
Reading Assignment

• Please read Chapter 3 of the optional course textbook by Katz and Lindell

• NOTE that you are responsible for everything that is explained in lecture!!!
Notation from Katz and Lindell

• \(\{X\}\) is a set of elements of type \(X\)
• \(m\) is a message in plaintext
  • \(m\) is composed of smaller blocks \(m_i\) suitable for individual encryption steps
  • \(m = \{m_i\}\)
• \(c_i\) is ciphertext corresponding to message block \(m_i\)
• \(c\) is ciphertext corresponding to message \(m\)
• \(\text{Enc}_k\) is encryption with key \(k\)
  • \(c \leftarrow \text{Enc}_k(m)\)
• \(\text{Dec}_k\) is decryption with key \(k\)
  • \(m \leftarrow \text{Dec}_k(c)\)
• \(\text{MAC}_k\) is generation of a message authentication code \(t\) with key \(k\)
  • \(t \leftarrow \text{Mac}_k(m)\) or, alternatively, \(t \leftarrow \text{Mac}_k(c)\)
• \(<a,b>\) is a concatenation of \(a\) followed by \(b\)
CONSTRUCTION 3.30 (page 83 in Ch. 3 of K & L)

• $F_k$ is a pseudorandom function which varies with a key $k$
  • Note: we will not cover elliptic curves in this course, but $F_k$ can be implemented by such curves (this is known as elliptic curve cryptography)

• A uniformly random $n$-bit key is selected and provided to the sender and receiver (but not to the adversary, of course)

• $Enc_k$: given an $n$-bit message $m$, choose a uniformly random $n$-bit number $r$
  • $c := <r, F_k(r) \oplus m>$

• $Dec_k$: given length $2n$ ciphertext $c = <r, s>$
  • $m := F_k(r) \oplus s = F_k^{-1}(c)$
Chosen Ciphertext Attack (CCA)

• Katz and Lindell define CCA indistinguishability in Section 3.7.1 (page 97 of their book) as follows
• Generate a uniformly random key $k$ of length $n$
• Adversary $A$ is given oracle access to $Enc_k$ and $Dec_k$ but is not allowed to query the actual challenge ciphertext
• $A$ chooses two messages $m_0$ and $m_1$
• $b \in \{0,1\}$ is chosen and is hidden from $A$
• $c \leftarrow Enc_k(m_b)$ is given to $A$
• Test: given $c$, can $A$ distinguish which case was encrypted?
• For example, consider $m_0 =$ a plaintext of all zeros and $m_1 =$ a plaintext of all ones
The Adversary Wins

• Approach:
  • take $s$ and flip the most significant bit, resulting in $s'$
  • decrypt $r, s'$
  • if the answer of decryption is a 1 followed by all zeros, the original message was all zeros
  • if the answer of decryption is a 0 followed by all ones, the original message was all ones
Takeaway

• Any encryption scheme which allows ciphertexts to “manipulated” in any controlled manner or way cannot be CCA-secure

• It is better if encryption schemes have the property that if the adversary tries to modify a given ciphertext, the results decrypts to a plaintext having no relationship to the original plaintext
  • Is enough to have no detectable relationship, i.e., which can be detected by a sequence of steps including an algorithm written in computer code