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 \(m\)
- \(Enc_k\) is encryption with key \(k\)
  - \(c \leftarrow Enc_k(m)\)
- \(Dec_k\) is decryption with key \(k\)
  - \(m \leftarrow Dec_k(c)\)
- \(MAC_k\) is generation of a message authentication code \(t\) with key \(k\)
  - \(t \leftarrow MAC_k(m)\) or, alternatively, \(t \leftarrow MAC_k(c)\)
- \(<a,b>\) 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: given an $n$-bit message $m$, choose a uniformly random $n$-bit number $r$
  - $c := <r, F_k(r) \ XOR \ m>$
- Dec: given ciphertext of length $2n$ $c = <r,s>$
  - $m := F_k(r) \ XOR \ s$
Insecure against Chosen Ciphertext Attack

- Adversary is given access to \( \text{Enc}_k \) and \( \text{Dec}_k \) but is not allowed to query the actual challenge ciphertext
- Test: give a plaintext of all zeros and a plaintext of all ones as the options, can the adversary distinguish which case was encrypted?
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
Takeway

• 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