Cryptography Part I

ECE 4156/6156 Hardware-Oriented Security and Trust

Spring 2024

Assoc. Prof. Vincent John Mooney III

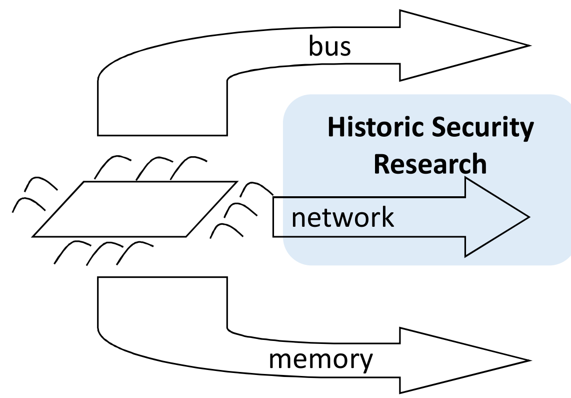
Georgia Institute of Technology

Reading Assignment

- Please read Chapter 1 of the course textbook by Katz and Lindell

Cryptography

- Cryptography is the science of keeping communication private
  - More formally, cryptography is traditionally defined as secure communication over an insecure channel



Security

- Notice that the definition of cryptography utilizes the definition of security
- A typical dictionary definition of security would say that it is freedom from danger or freedom from fear of being hurt

Secure from What Threat?

- Traditionally, in security research the perceived threats are clearly defined
- The threats of concern form an “attack surface”

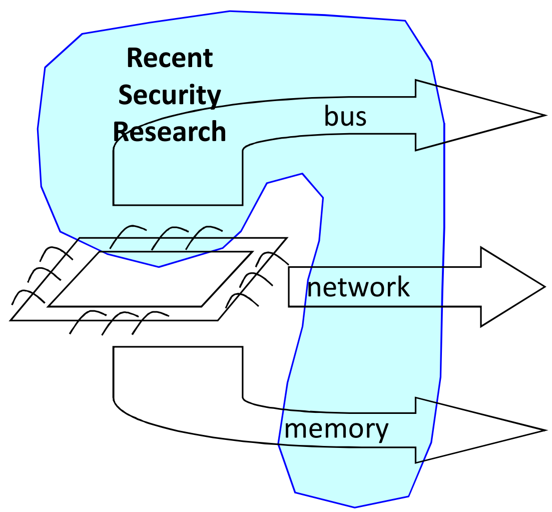
Some Interesting Historical Facts

- The capture of a version of the Enigma machine helped crack the German cryptographic codes in WWII

Terminology

- Plaintext or cleartext: the message in a language understood by both the sender (Alpha) and the receiver (Buzz)
- Encryption: the process of disguising a message such that it cannot be recognized by an adversary
- Ciphertext (also cyphertext): the encrypted message
- Decryption: the process of transforming ciphertext back into the original plaintext
- Key: information, usually a number, known to the communicating parties but not to any adversaries – a key is a *secret*

Modern Cryptography



Symmetric Keys

- A scheme which uses the same key for encryption and decryption is referred to as symmetric-key cryptography or private-key cryptography
- Note that the private key needs to be shared between the two (or more) communicating parties in a secret fashion

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
  - $m \leftarrow Dec_k(c)$
- $\langle a,b \rangle$ is a concatenation of a followed by b

Notation from Katz and Lindell (cont'd)

- *M* is a set of all possible messages, i.e., the message space
- *C* is a set of all possible ciphertexts, i.e., the ciphertext space
- *Gen* is a key generation procedure
  - The output of *Gen* is key *k*
  - *Gen* may or may not require an input

Example

1. Design Team (DT) and Fab meet in person and agree on a secret key *(SK)*

2. DT encrypts a message $m = \{m_i\}$ using the secret key *SK*, i.e., $c \leftarrow Enc_{SK}(m)$, and sends the result to the Fab

c

3. Fab decrypts the encrypted message c and obtains m, i.e., $m \leftarrow Dec_{SK}(c)$,

Kerchoffs’ Principle

- Auguste Kerchoffs
- “The cipher method must not be required to be secret, and it must be able to fall into the hands of the enemy without inconvenience.”

Formal Definitions

- Clear delineation
  - Threats
  - Security guarantees
- Mathematical analysis and comparison

Secure Encryption

- Infeasible for an attacker to recover the key
- Infeasible for an attacker to recover the entire plaintext
- Infeasible for an attacker to recover any character of the plaintext
  - Assuming none of the plaintext has been provided
- Ciphertext should leak no additional information about the plaintext
  - Need formal definition of “additional information”
  - Probability theory

Traditional Cryptanalytic Attacks

1) Ciphertext only attack
   - Cryptanalyst has the ciphertext $\{c_i\}$ of a number of messages
     - $c_1 = Enc_k(m_1)$, $c_2 = Enc_k(m_2)$, …
2) Known plaintext attack
   - Cryptanalyst has a number of plaintext, ciphertext pairs
     - $(m_i, c_i) \mid c_i = Enc_k(m_i)$
   - May also have additional ciphertext without associated plaintext
3) Chosen plaintext attack
   - Cryptanalyst can obtain ciphertext for chosen plaintext
   - Given m_i, $c_i = Enc_k(m_i)$ can be found

- Goals include decryption of specific messages and deduction of the key

Traditional Cryptanalytic Attacks (continued)

4) Chosen ciphertext attack
   - Cryptanalyst can obtain plaintext for (some) chosen ciphertext
   - Given c_i, m_i | c_i = $Enc_k(m_i)$ can be found for some (or all) cases
- The primary goal is the deduction of the key; in the case that only some plaintext can be decrypted, another goal may be decryption of specific messages not able to be decrypted via chosen ciphertext
- Note that these four traditional attacks are listed by increasing capability of the cryptanalyst, i.e., case (1) is the weakest whereas case (4) is the most capable

Clearly Defined Assumptions

- Allow checking assumptions
- Comparison of schemes
- Understanding the necessity of assumptions
- Less ambiguous claims about attackers

Problems

- Assumptions may be broken!
- Attacked may not be properly modelled!

Symmetric Keys

- A scheme which uses the same key for encryption and decryption is referred to as symmetric-key cryptography or private-key cryptography
- Note that the private key needs to be shared between the two (or more) communicating parties in a secret fashion

Data Encryption Standard (DES)

- In 1973, NIST (the National Institute of Standards and Technology – technically, however, in 1973 NIST was named the National Bureau of Standards) issued a public request for a standard cryptographic algorithm
  - High level of security dependent only on the key
  - Completely specified and easy to understand
  - Publically available
  - Usable in diverse application scenarios
  - Efficient & economical to implement in hardware
  - Validated & tested

Advanced Encryption Standard (AES)

- In 1997, NIST organized a public competition for a new cryptographic algorithm to replace DES
  - 15 algorithms were submitted from all over the world
  - The submissions were analyzed by NIST, the public, and especially by competing teams!
  - Workshops were held in 1998 and 1999, finally narrowing down to five submissions
  - Third and final workshop held in April 2000
  - In October 2000 NIST selected the algorithm of two cryptographers from Belgium, Vincent Rijmen and Joan Daemen, who names the algorithm Rijndael
  - NIST stated that all five candidates were excellent

Some Definitions

- A permutation of a list or a vector is a rearrangement of the original list or vector where no elements are duplicated nor eliminated
- A bijection is a mapping which is one-to-one and onto

Shift Cipher

- Key k is a number between 1 and 25
  - Replace each letter with the letter advanced k positions forward in the alphabet
  - Note that letter z wraps around to a
  - Of course the above assumes a 26 letter alphabet; can be modified for any known human language based on letters
- m is a message in plaintext
  - m is composed of letters m_i suitable for individual encryption steps
  - $m = \{m_i\}$
- Enc_k is encryption with key k
  - $c \leftarrow Enc_k(m)$
- Dec_k is decryption with key k
  - $m \leftarrow Dec_k(c)$

Mono-alphabetic Substitution Cipher

- Key is a permutation of the alphabet
  - Uniquely replace each letter with another letter in the alphabet
  - Note that a permutation is a bijection
- m is a message in plaintext
  - m is composed of letters m_i suitable for individual encryption steps
  - $m = \{m_i\}$
- Enc_k is encryption with key k
  - $c \leftarrow Enc_k(m)$
- Dec_k is decryption with key k
  - $m \leftarrow Dec_k(c)$

Additional Reading Assignment

- Please read Chapter 2 of the course textbook by Katz and Lindell

DEFINITION 2.5 *Encryption scheme* $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *with message space* $\mathcal{M}$ *is* perfectly indistinguishable *if for every* $\mathcal{A}$ *it holds that*

$$\Pr\left[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1\right] = \frac{1}{2}\,.$$

The following lemma states that Definition 2.5 is equivalent to Definition 2.3. We leave the proof of the lemma as Exercise 2.5.

LEMMA 2.6 *Encryption scheme* Π *is perfectly secret if and only if it is perfectly indistinguishable.*

Formally, let $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ be an encryption scheme with message space $\mathcal{M}$. Let $\mathcal{A}$ be an adversary, which is formally just a (stateful) algorithm. We define an experiment $\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi}$ as follows:

The adversarial indistinguishability experiment $\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi}$:

1. *The adversary $\mathcal{A}$ outputs a pair of messages $m_0, m_1 \in \mathcal{M}$.*
2. *A key k is generated using* Gen, *and a uniform bit $b \in \{0,1\}$ is chosen. Ciphertext $c \leftarrow \mathsf{Enc}_k(m_b)$ is computed and given to $\mathcal{A}$. We refer to c as the* challenge ciphertext.
3. *$\mathcal{A}$ outputs a bit b'.*
4. *The output of the experiment is defined to be 1 if $b' = b$, and 0 otherwise. We write $\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1$ if the output of the experiment is 1 and in this case we say that $\mathcal{A}$* succeeds.

As noted earlier, it is trivial for $\mathcal{A}$ to succeed with probability $1/2$ by outputting a random guess. Perfect indistinguishability requires that it is impossible for any $\mathcal{A}$ to do better.

DEFINITION 2.5 *Encryption scheme $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ with message space $\mathcal{M}$ is* perfectly indistinguishable *if for every $\mathcal{A}$ it holds that*

$$\Pr\left[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1\right] = \frac{1}{2}.$$

CONSTRUCTION 2.8

Fix an integer $\ell > 0$. The message space $\mathcal{M}$, key space $\mathcal{K}$, and ciphertext space $\mathcal{C}$ are all equal to $\{0,1\}^\ell$ (the set of all binary strings of length ℓ).

- Gen: the key-generation algorithm chooses a key from $\mathcal{K} = \{0,1\}^\ell$ according to the uniform distribution (i.e., each of the 2^ℓ strings in the space is chosen as the key with probability exactly $2^{-\ell}$).
- Enc: given a key $k \in \{0,1\}^\ell$ and a message $m \in \{0,1\}^\ell$, the encryption algorithm outputs the ciphertext $c := k \oplus m$.
- Dec: given a key $k \in \{0,1\}^\ell$ and a ciphertext $c \in \{0,1\}^\ell$, the decryption algorithm outputs the message $m := k \oplus c$.

The one-time pad encryption scheme.