1 Security Principles

1. **Know your threat model**: 谁会来攻击你，为什么要攻击你。Threat Model 指的就是对攻击者建立一个合适的模型（比如他们有多少资源，他们的动机）。*You often just need to have "good enough" defense to make attackers turn somewhere else.*
2. **Consider Human Factors**: 考虑用户习惯，别让用户太麻烦。
3. **Security is economics**: 搞 security 需要米，所以要考虑你保护的是啥。
4. **Detect if You Can't Prevent**:
   - **Deterrence**: Stop the attack before it happens.
   - **Prevention**: Stop the attack as it happens.
   - **Detection**: Learn that there was an attack (after it happened).
   - **Response**: Do something about the attack (after it happened). 对于 response，需要做的事 Mitigation and Recovery，就是比如在发现勒索软件的时候赶紧进行文件备份和转移。
5. **Defense in depth**: 多层防御，但是要考虑成本。
6. **Least Privilege**: 然鹅其实现在的操作系统做的都很遭糕。
7. **Ensure complete mediation**: You should check *every* access to *every* object. 课上提出了一个叫做 *Reference Monitor* 的概念，就是一个任何 access 操作都必须经过的结点，比如说 network firewall。用这种方法来保证每个 access 都被检查过。
8. **Separation of Responsibility**: 例子是原子弹发射，要两个人同时操作才行。
9. **Shannon's Maxim**: 你不能依赖于 Security Through Obscurity，也就是通过源代码的保密性来保护系统。想到 Kerckhoff's Principle?
10. **Use Fail-Safe Defaults**: 当系统崩溃的时候，应该让系统保持最安全的状态。比如说一些防盗门在断电的时候要自动关上。
11. **Design in Security from the Start**

TCB Design Principles:

- Unbypassable (or completeness)
- Tamper-resistant (or security)：不能改，必须保证 TCB 的完整性
- Verifiable (or correctness)：TCB 应该设计得越小越好（KISS principle: Keep It Simple, Stupid）

TOCTTOU Vulnerabilities

2 Memory Safety

2.1 x86 Calling Convention

1. Push arguments onto the stack (reverse order).
2. Push the old `EIP` onto the stack. This value becomes the `RIP`.
3. Move `EIP` to the first instruction of the function.
4. Push the old `EBP` onto the stack. This value becomes the `SFP`.
5. Move the `EBP` down to `ESP` to start a new frame.
6. Move the `ESP` down to allocate space for local vars.
7. Execute the function.
8. Move the `ESP` up to the `EBP`.
9. Pop the `SFP` and move the `EBP` to that value.
10. Pop the `RIP` and move the `EIP` to that value.
11. Remove arguments from the stack.

2.2 GDB

`finish`: 相当于 step out

`info registers`

`info frame`

`disas <function_name>`

2.3 C

```
gets -> fgets
strcpy -> strncpy / strlcpy
strlen -> strnlen / memchr
```

`size_t` 在大部分机子是 `uint32_t`

`printf("000%n", &val)`: 写入 `0x00000003` 到 `&val`

`printf("000%hn", &val)`: 写入 `0x0003` 到 `&val`

在末尾写入 `"\0"` 的函数：`gets`, `fgets`, `strcpy`

`strncpy` 要看有没有在前 n 个字符中读到 `"\0"`

```
size_t fread(void *buffer, size_t size, size_t count, FILE *stream);
```

`fread` 不加 `"\0"`

```
char *strncpy (char *destination, const char *source, size_t num);
```

返回 `destination`

```
size_t strnlen(const char *s, size_t maxlen);
```

3 Cryptography

3.1 Definitions

Confidentiality is the property that prevents adversaries from reading our private data.

Integrity is the property that prevents adversaries from tampering with our private data.

Authenticity is the property that lets us determine who created a given message.

Deniability: 可否认性，这不是我说的！

Kerckhoff's Principle

Threat Models: Ciphertext-only, Chosen-plaintext, Chosen-ciphertext, Chosen plaintext-ciphertext

chosen 啥就是 Eve 可以把选择特定的啥然后 encrypt / decrypt

IND-CPA: M_0 和 M_1 是 Eve 给的，但必须长度相同，A 来选

To break IND-CPA, Eve must learn something other than message length

$\varepsilon \leq \frac{1}{2^{80}}$ is a reasonable threshold

3.2 One-Time Pad

OTP 不是 IND-CPA secure 的

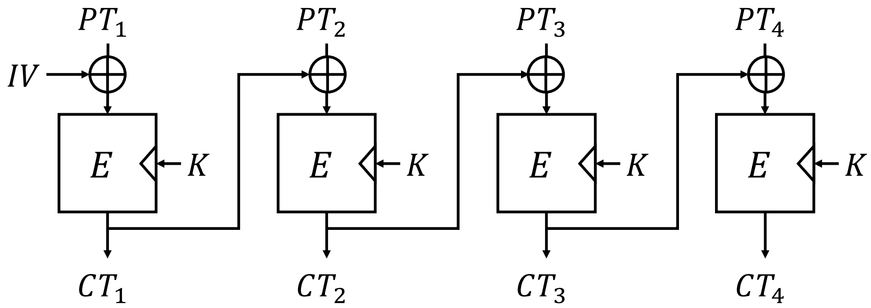
3.3 Block Ciphers

Key size (k) 128, 192, or 256 bits，一般用 256

Block size (n) 128 bits

Electronic Code Book (ECB) is deterministic

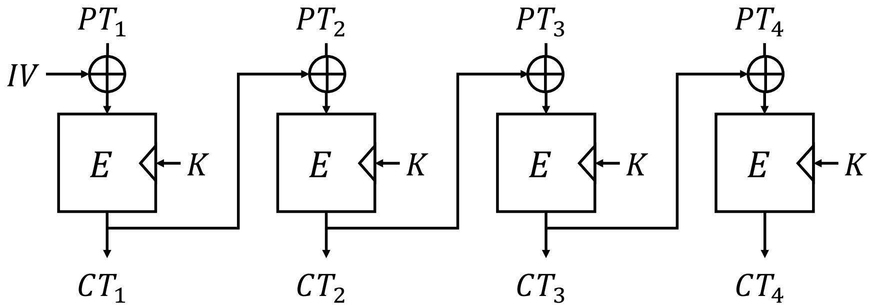
Cipher Block Chaining (CBC): Unpredictable IV



CTR Mode: Nonce unique

$C_i = E_k(\mathcal{N}\|i) \bigoplus P_i$

CFB Mode



3.4 Hash

One-way-ness ("preimage resistance"): 随便给个 y 很难找到 $H(x) = y$ ($H(x) = 1$ 不是)

Collision Resistance, birthday attack

Random / unpredictability: 改一个就会影响很大

常见的 Hash Functions:

MD5: 128 bits output, completely broken

SHA-1: 160 bits output, completely broken in 2017

SHA-2: 256, 384, or 512 bits (sometimes labeled SHA-256, SHA-384, SHA-512). Not currently broken, but some variants are vulnerable to a length extension attack. Current standard.

SHA-3 (Keccak): 256, 384, or 512 bits. Current standard.

要注意 hash provide integrity 需要在 hash 值不被改的前提下

Length extension: 给你 $\mathcal{H}(x)$ 和 x 的长度，可以构造出 $\mathcal{H}(x\|m)$（SHA-256）

3.5 MACs

Message Authentication Codes

$\text{MAC}(K, M) \to T$, generate a tag

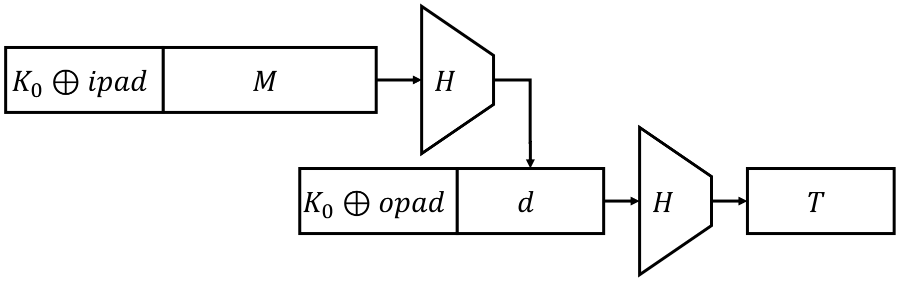
大部分 MACs 是 deterministic 的

EU-CPA: existentially unforgeable，但不要求 non-deterministic，所以不能造之前出过的数据

$\text{NMAC}(K_1, K_2, M) = \mathcal{H}(K_1\|\mathcal{H}(K_2\|M))$

用两次 hash 是为了防止 length extension

$\text{HMAC}(K, M)$: $K_1 = K_0 \bigoplus \text{ipad}, K_2 = K_0 \bigoplus \text{opad}$



K_0 是 preprocess 过的 K，太长 hash，太短 pad 0

`ipad = 0x5c * len(k_0)`

`opad = 0x36 * len(k_0)`

但 HMAC 是 deterministic 的

3.6 Authenticated Encryption

Always use encrypt-then-MAC

$\text{MAC}(K_2, \text{ENC}(K_1, M))$

MAC-then-encrypt 也是对的，但是比较难写

不能 key reuse: $K_1 \neq K_2$

Authenticated encryption with additional data (AEAD): 直接 provide both confidentiality and integrity over the plaintext and integrity over additional data

Galois Counter Mode (GCM): AEAD，但是比较难写难用，用错了之前 leak everything

3.7 PRNGs

Pseudorandom number generator, also called deterministic random bit generators (DRBGs)

3 bits of entropy = uniform, random distribution over 8 values

PRNGs are deterministic

Rollback resistance: but not required

CTR-DRBG: $\texttt{PRNG.seed}(K \| \text{IV})$

$\texttt{generate}(m) = \text{E}_k(\text{IV}\|1)\| \cdots \|\text{E}_k\left(\text{IV}\| \left\lceil \frac{m}{n} \right\rceil\right)$

HMAC-DRBG

Algorithm 1 Seed Generation for HMAC-DRBG

```
Input: Seed $s$
$K \leftarrow 0$
$V \leftarrow 0$
$K \leftarrow \text{HMAC}(K, V \| \texttt{0x00} \| s)$
$V \leftarrow \text{HMAC}(K, V)$
$K \leftarrow \text{HMAC}(K, V \| \texttt{0x01} \| s)$
$V \leftarrow \text{HMAC}(K, V)$
```

Reseed: 把 seed 中的 $K, V \leftarrow 0, 0$ 去掉

Algorithm 2 Generation for HMAC-DRBG

```
$o \leftarrow$ EmptyString
while len(output) < n do
    $V \leftarrow \text{HMAC}(K, V)$
    $o \leftarrow o \| V$
end while
$K \leftarrow \text{HMAC}(K, V \| \texttt{0x00})$
$V \leftarrow \text{HMAC}(K, V)$
return $o_{1\sim n}$
```

Assuming HMAC is secure, HMAC-DRBG is a secure, rollback-resistant PRNG

UUID: use PRNGs

3.8 Stream Ciphers

AES-CTR is a type of stream cipher

不要用同一个 key encrypt 太多 PT：如果 key 是 n bits long，最多只能 encrypt $2^{\frac{n}{2}}$ 个 blocks

3.9 DHE

DHE is an active protocol

DHE does not provide authentication

ECDH: Elliptic-curve Diffie-Hellman

3.10 Public-Key Encryption

PK: Public key

SK: Private key

3.10.1 ElGamal

Bob 生成 SK b 和 PK $B = g^b$
A 生成随机 PK r 和 PK $R = g^r$
$C = (R, M \times B^r)$
$P = C_2 \times C_1^{-b}$

3.10.2 RSA

PK: $N = pq, e$
SK: $d \equiv e^{-1} \pmod{(p-1)(q-1)}$
e 是 $(p-1)(q-1)$ 的 coprime
Enc$(e, N, M) = M^e$ mod N
Dec$(d, C) = C^d$ mod N
e is usually small (about 16 bits) and often constant $(3, 17, 65537)$
Optimal asymmetric encryption padding (OAEP): add randomness
Hybrid Encryption: 先用 asymmetric 传密钥再用 symmetric 传数据

3.11 Digital Signatures

$S = \mathcal{H}(M)^d$ mod N
Verify: check $S^e \equiv \mathcal{H}$