Technologies for E-Commerce

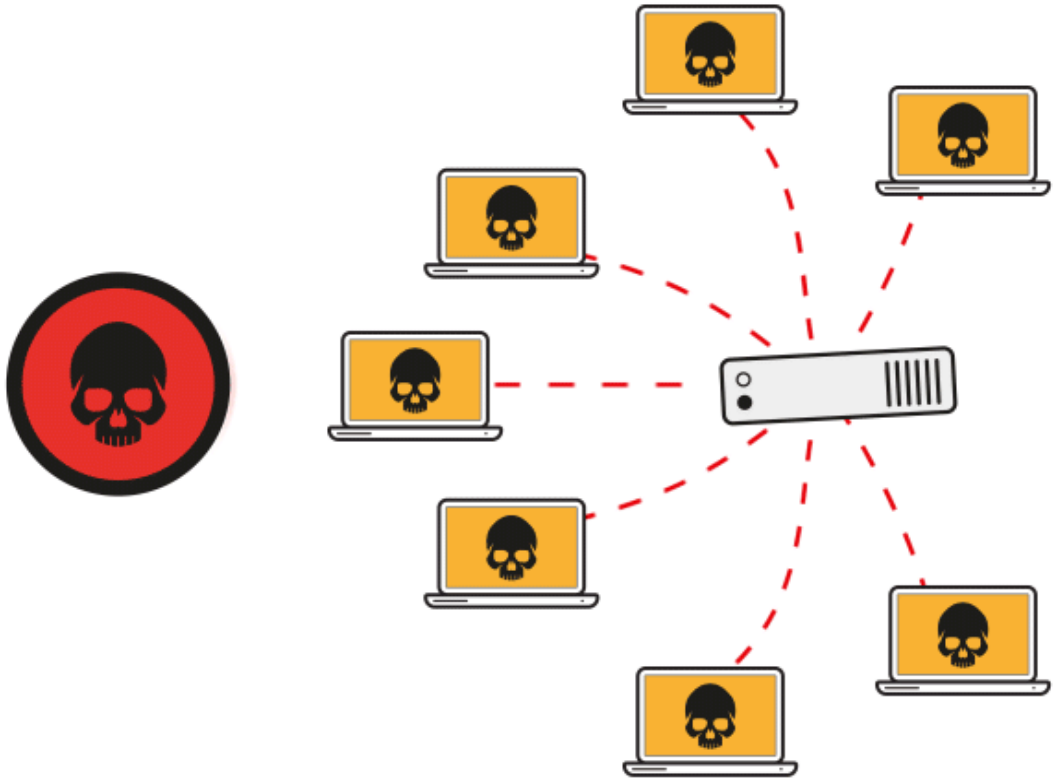
CAN302

Department of Communications and Networking

Xi'an Jiaotong-Liverpool University (XJTLU)

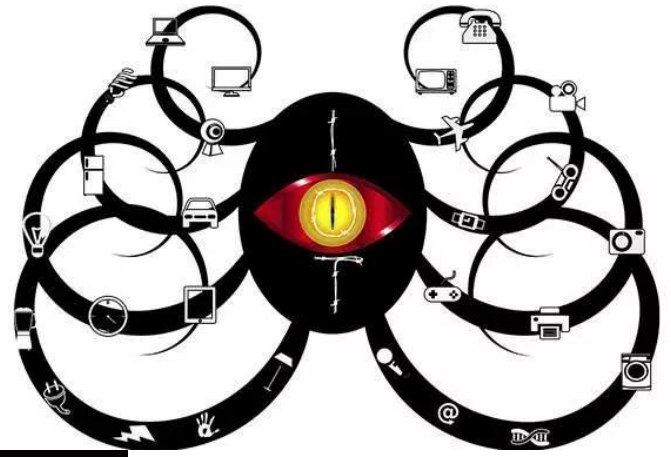
Week8 – Security in general

Attacks never sleep



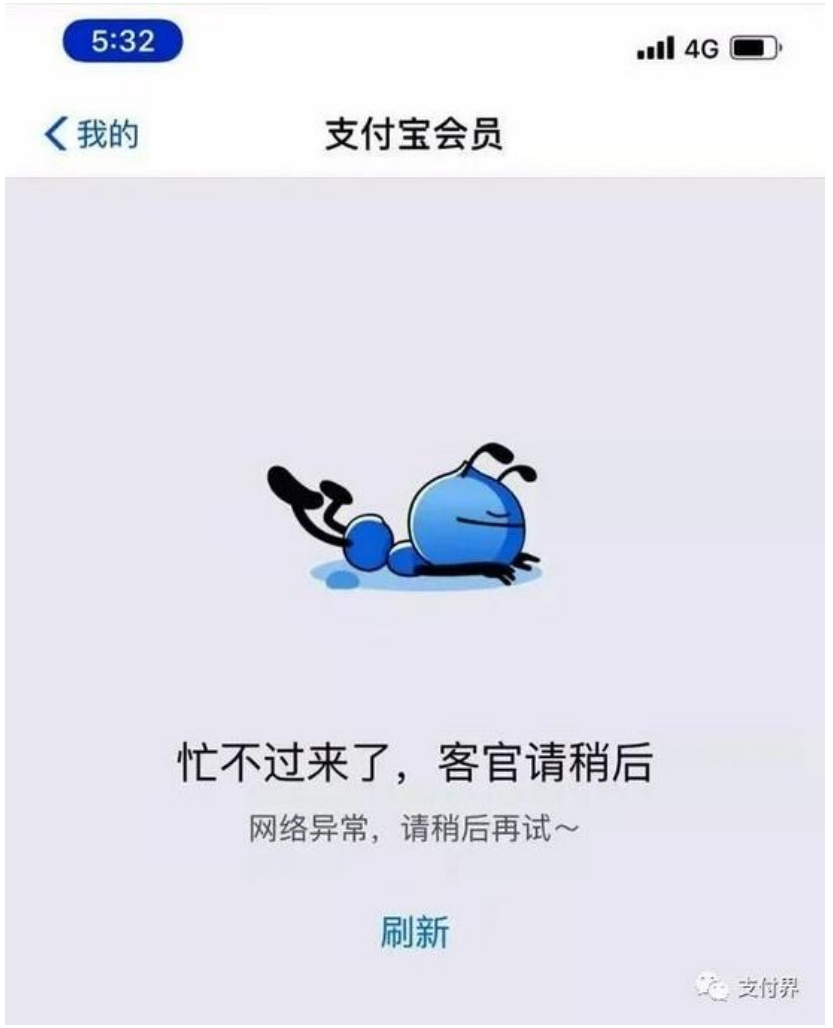
https://zhuanlan.zhihu.com/p/89428085

Attacks never sleep

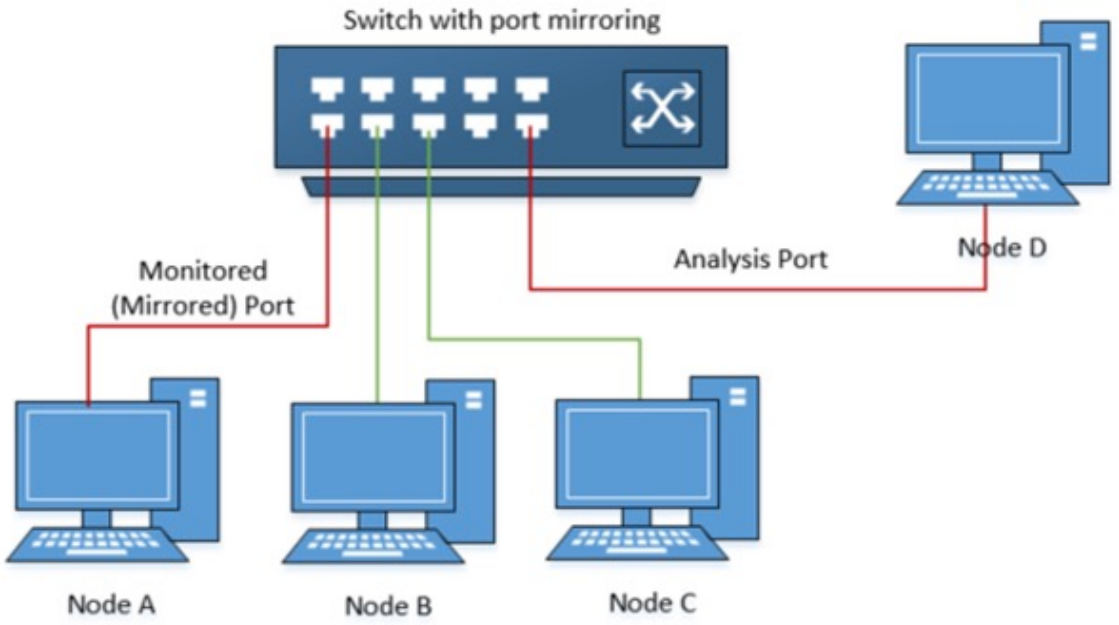


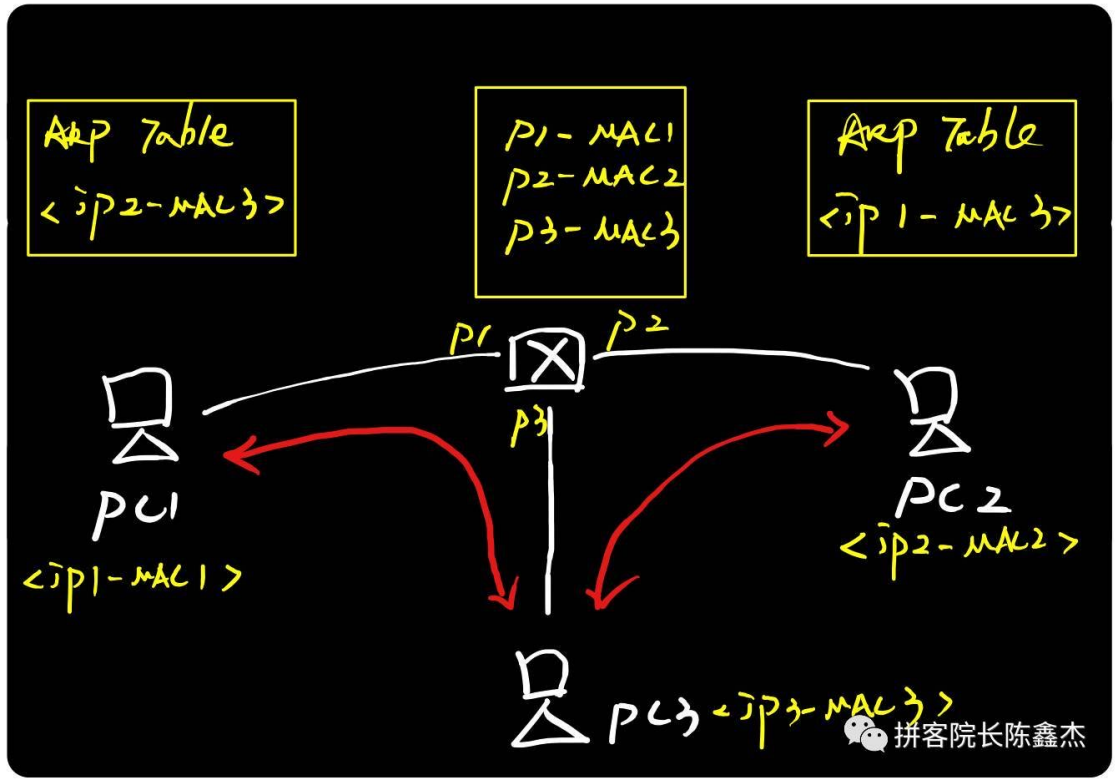
https://zhuanlan.zhihu.com/p/89428085

Or by accidences



Middle-men can SEE all packs





https://zhuanlan.zhihu.com/p/28818627
https://dun.163.com/news/p/233ea1ba40a14791a5fb8d3b6847b663

Free – Wi-Fi, “free” to SEE all your info

https://v.qq.com/x/page/b0188l0shhr.html
https://v.qq.com/x/page/g0188shm2gf.html
https://www.zhihu.com/question/41432680

Even happens to me

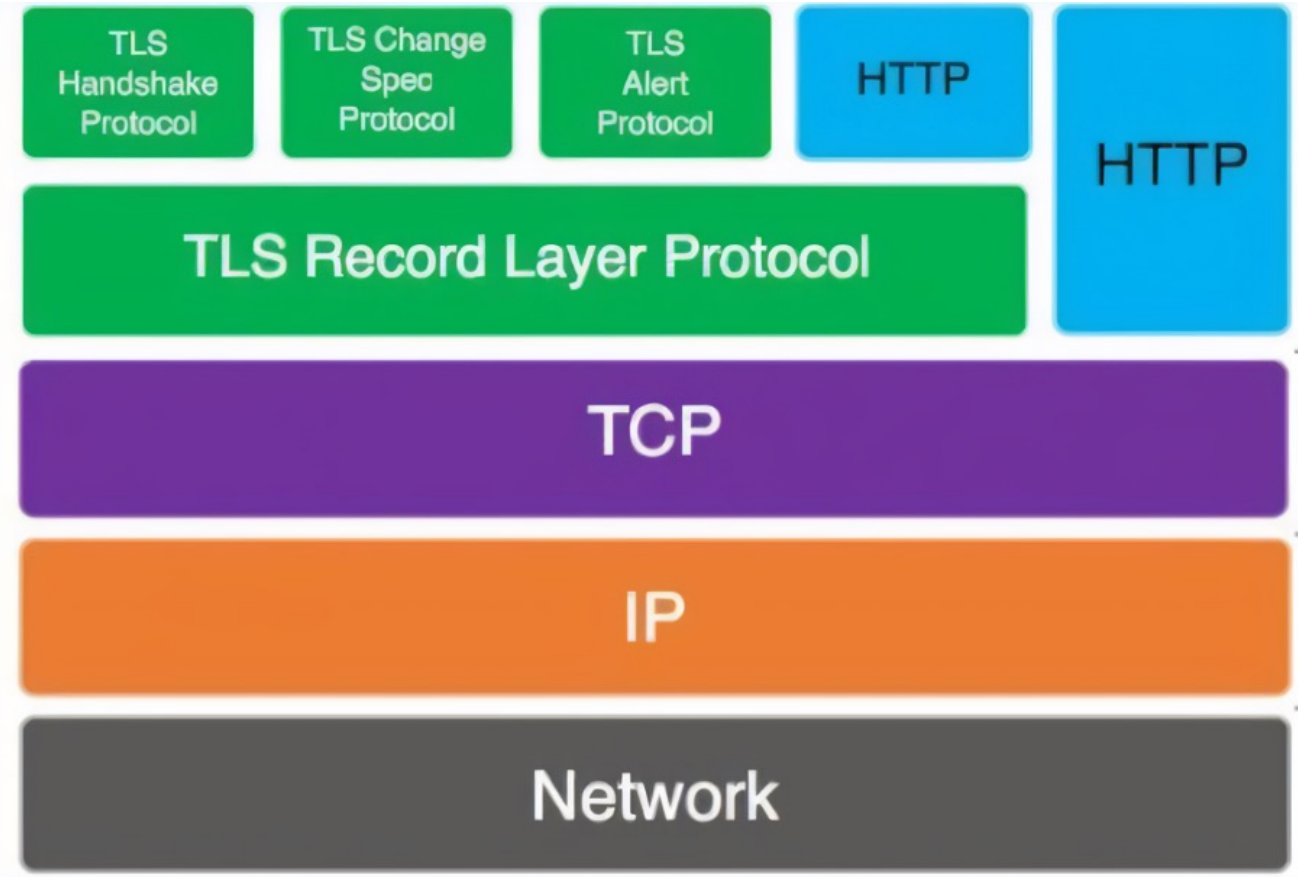
Case study: Https and Password

Http is NOT a protocol with encryption

```
1  行      HTTP/1.1  200  OK
2  头      Content-Type: text/html;charset=utf-8
3          Content-length: 2048
4          Content-encoding: gzip
5  空行
6  体      <html>
7              <head>
8              </head>
9              <body>
10                 <h1>尚硅谷</h1>
11             </body>
12         </html>
```

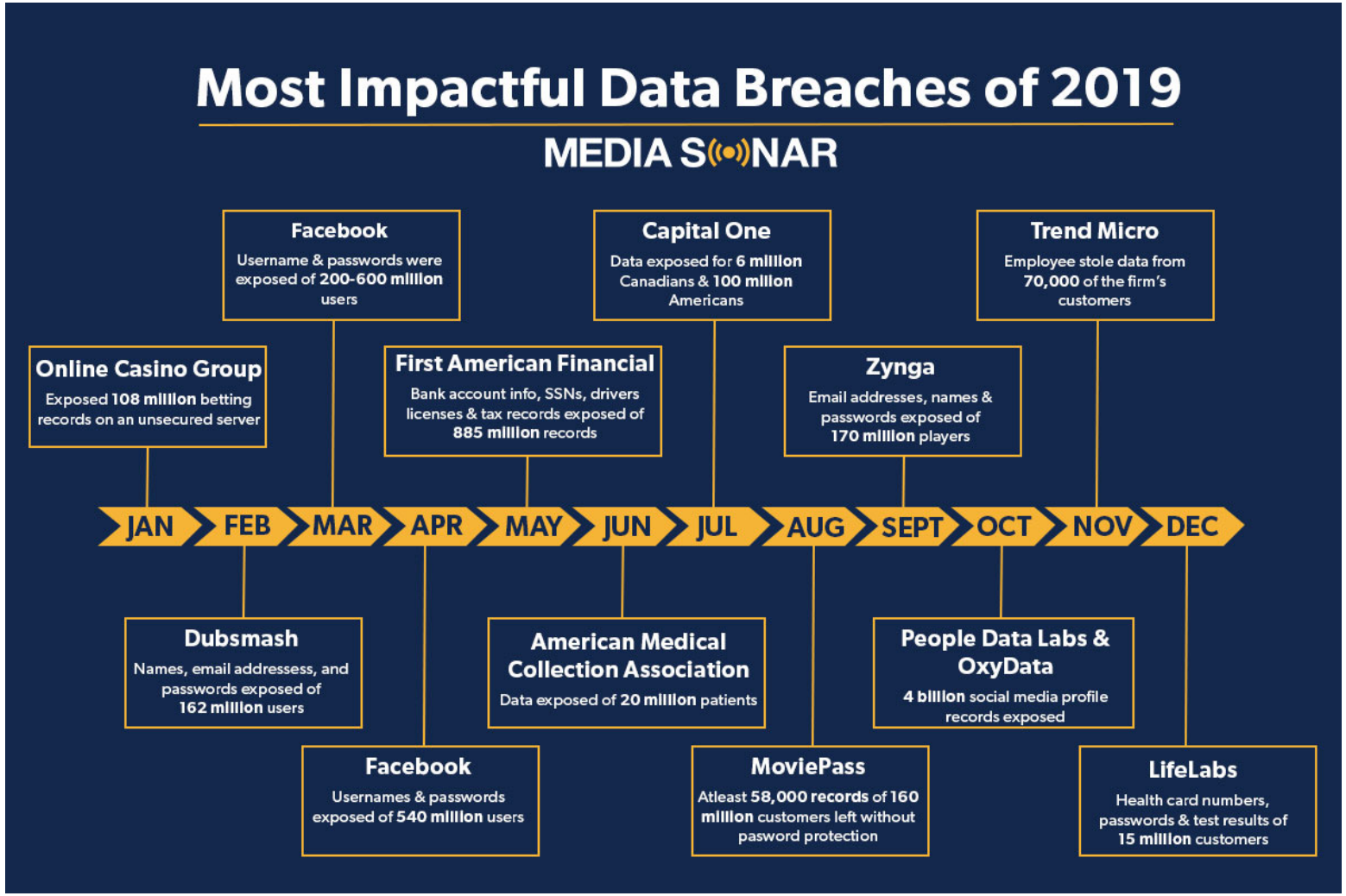
- **All message in plain text.**
- **The biggest Vulnerability is Http protocol itself!**

Https - add a lock for the Http protocol



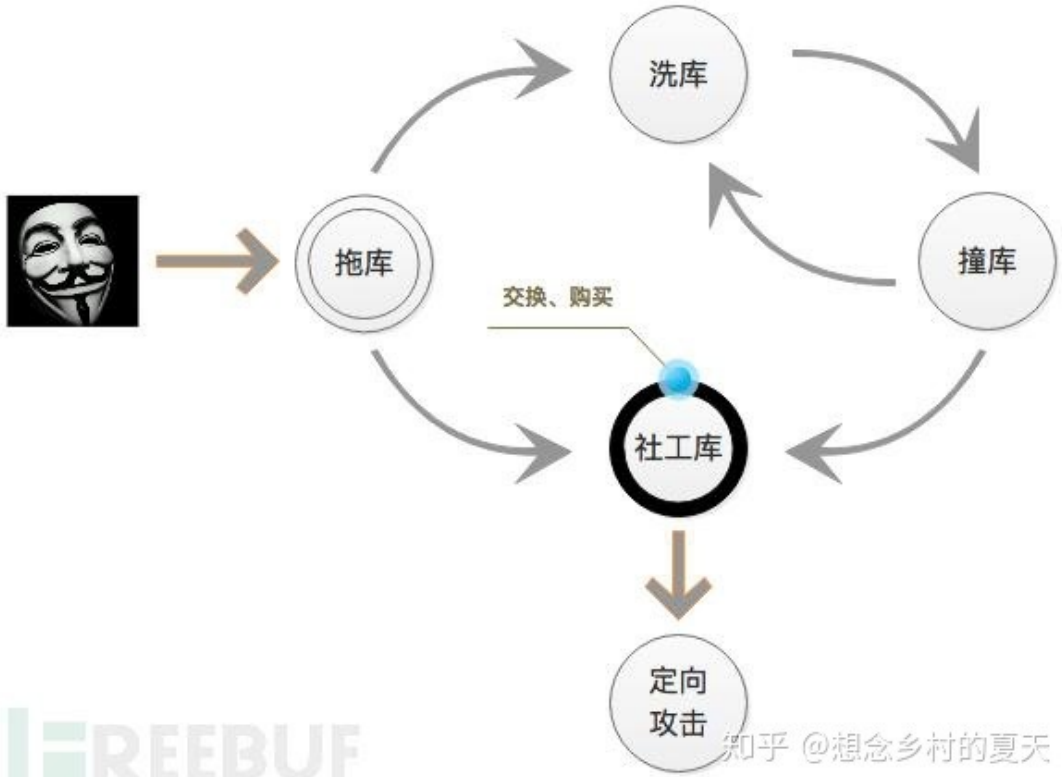
https://v.qq.com/x/page/b0188l0shhr.html
https://v.qq.com/x/page/g0188shm2gf.html
https://www.zhihu.com/question/41432680

Some many databases for username/passwd



https://www.upguard.com/blog/biggest-data-breaches

Collision attacks



https://zhuanlan.zhihu.com/p/126243422
https://www.scoopwhoop.com/most-dangerous-passwords-that-can-be-hacked/

CIA triad

The CIA Triad		
What Is the CIA?		
Confidentiality	**Integrity**	**Availability**
I send you a message, and no one else knows what that message is.	I send you a message, and you receive exactly what I sent you	I send you a message, and you receive it
What's The Purpose of the CIA?		
Data is not disclosed	Data is not tampered	Data is available
How Do You Achieve the CIA?		
e.g., Encryption	e.g., Hashing, Digital signatures	e.g., Backups, redundant systems
Opposite of CIA		
Disclosure	Alteration	Destruction

https://www.cybernewsbox.com/cia-triad/
https://digitalforensicforest.com/2017/12/14/confidentiality-integrity-availability-cia/

Risk =Threat Probability * Vulnerability Impact

- Risk is a combination of the threat probability and the impact of a vulnerability.
- In other words, risk is the probability of a threat agent successfully exploiting a vulnerability.

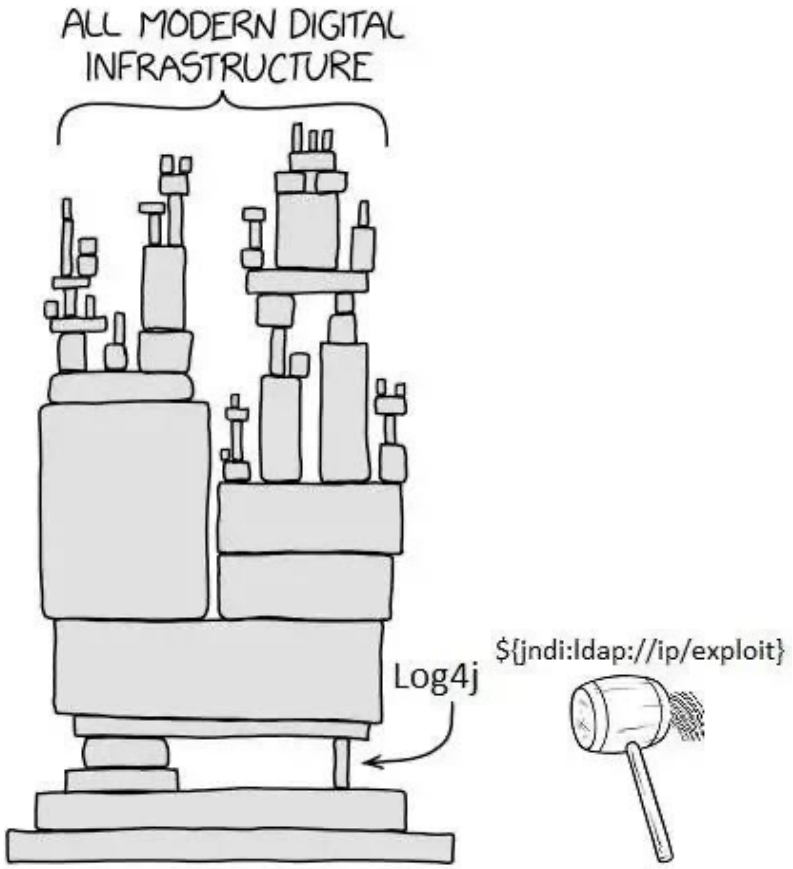
https://lifars.com/2020/07/threat-vulnerability-risk-what-is-the-difference
https://www.securingpeople.com/security-risk-assessment/threat-vulnerability-risk/

Threat

- A **threat** is any type of danger, which can damage or steal data, create a disruption or cause a harm in general.
- Common examples of threats include malware, phishing, data breaches and even rogue employees.
- Or a set of potential incidents in which a threat agent causes a threat event to an asset using a specific entry point into the system

https://zhuanlan.zhihu.com/p/22369557

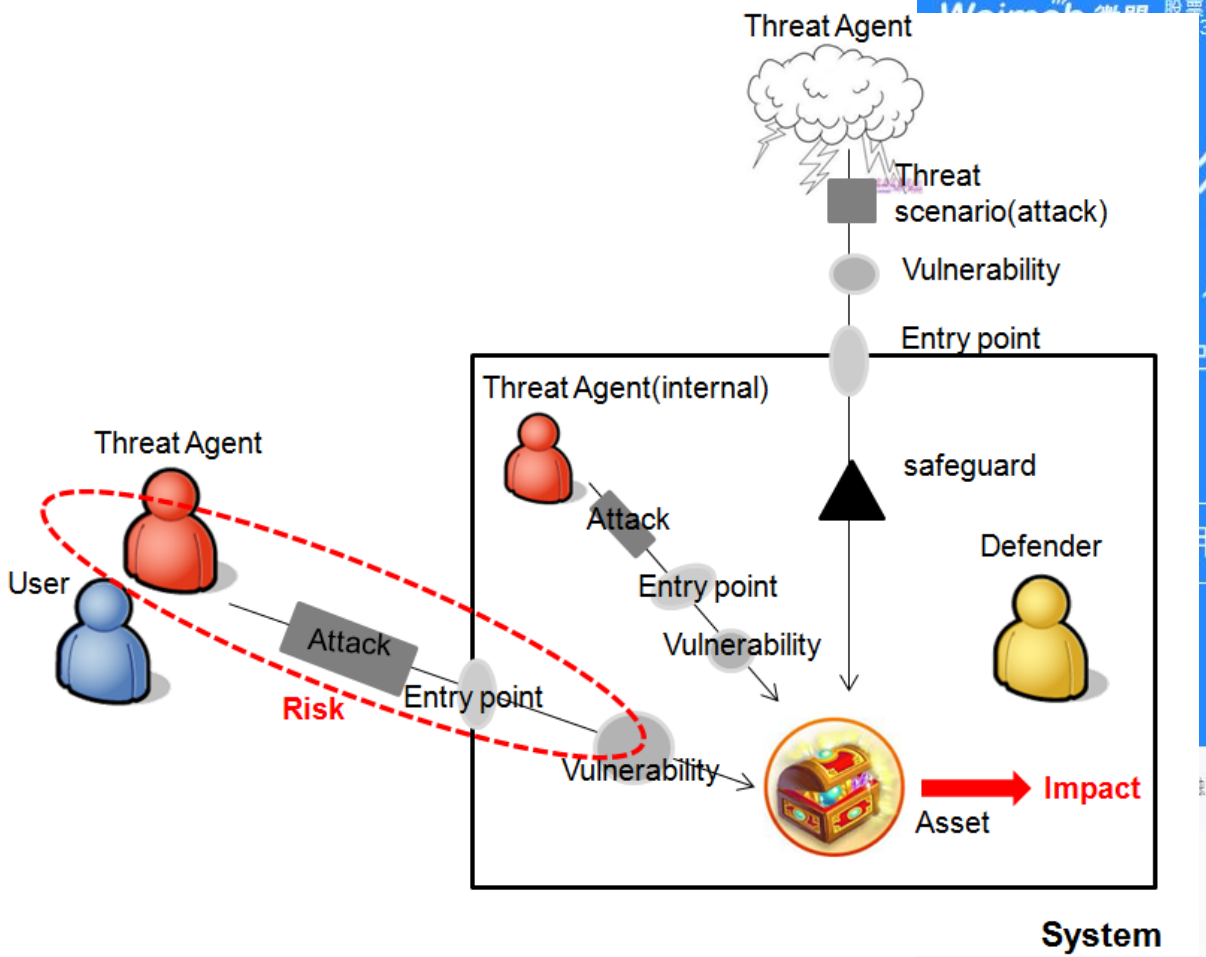
Vulnerability

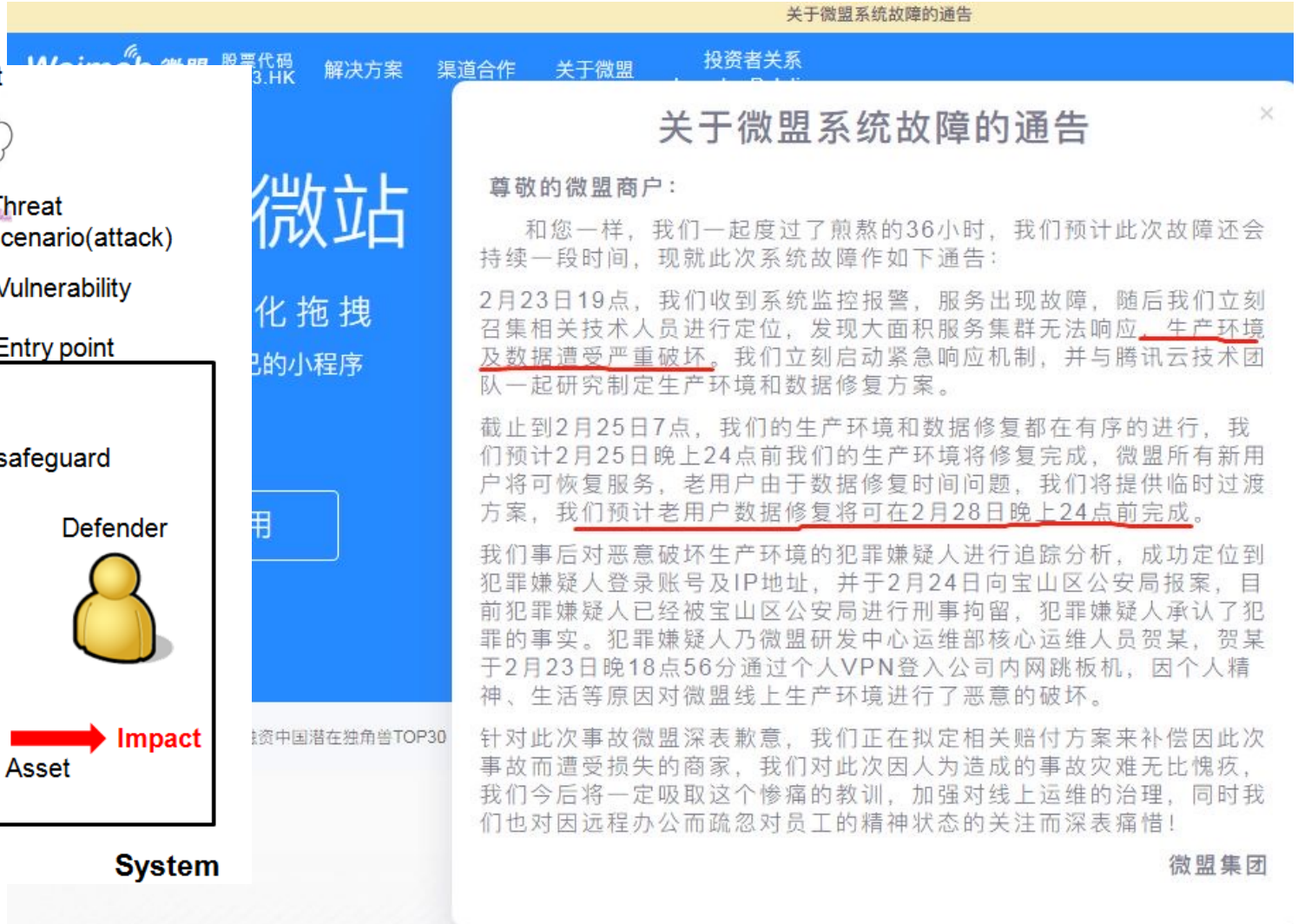


- A **vulnerability** is a weakness in hardware, software, personnel or procedures, which may be exploited by threat actors in order to achieve their goals.
- Many famous vulnerabilities, such as Log4j in 2020.
- Vulnerabilities can be marked by Common Vulnerability Scoring System or CVSS.
- It is not only hardware and software, but human being.
- A vulnerability, to which fix is not yet available, is called a zero-day vulnerability.

https://lifars.com/2020/07/threat-vulnerability-risk-what-is-the-difference
https://www.securingpeople.com/security-risk-assessment/threat-vulnerability-risk/

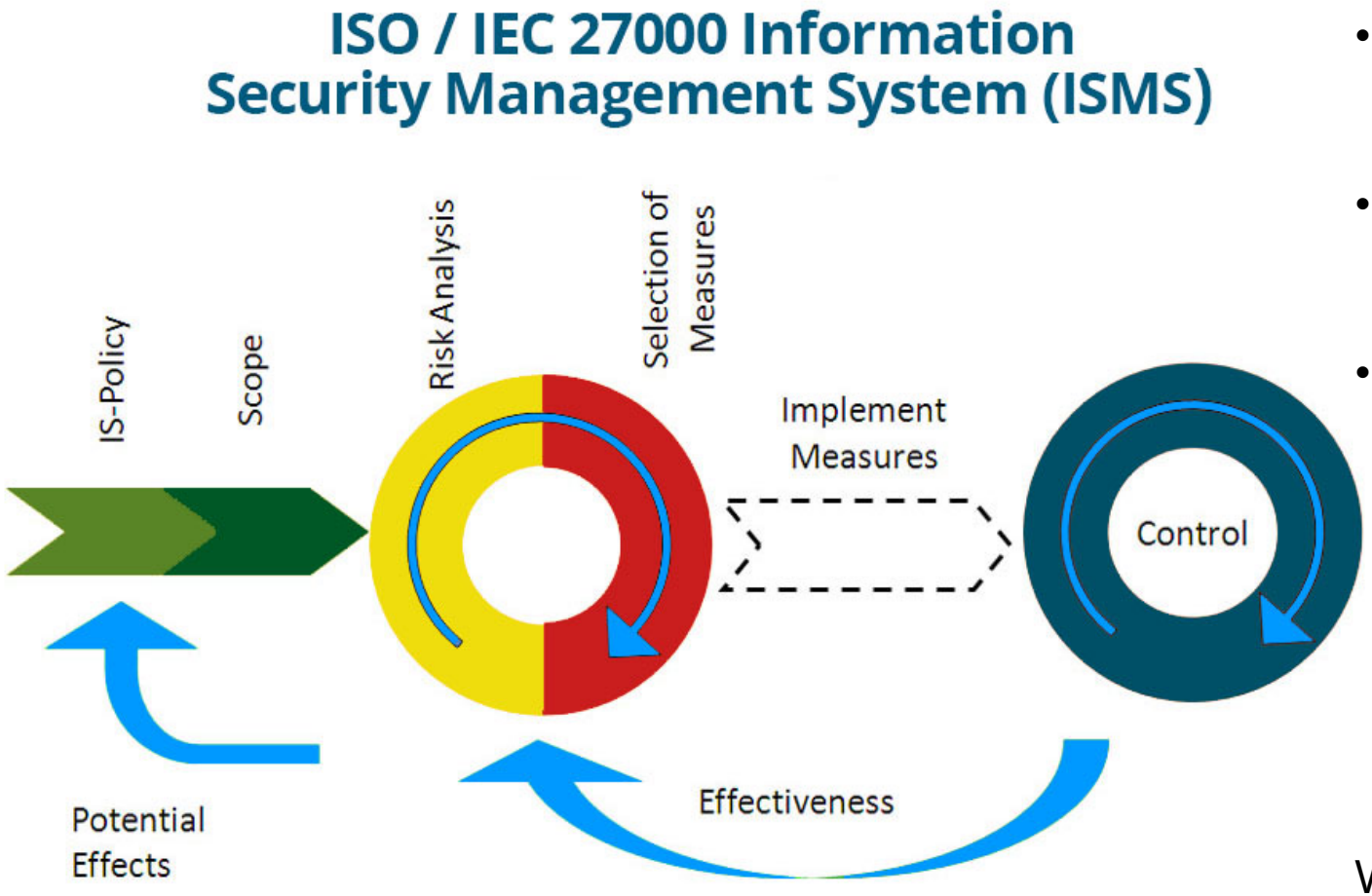
Risk is ALSO about people





- Again, risk is NOT only about program or technology.

Manage the risks



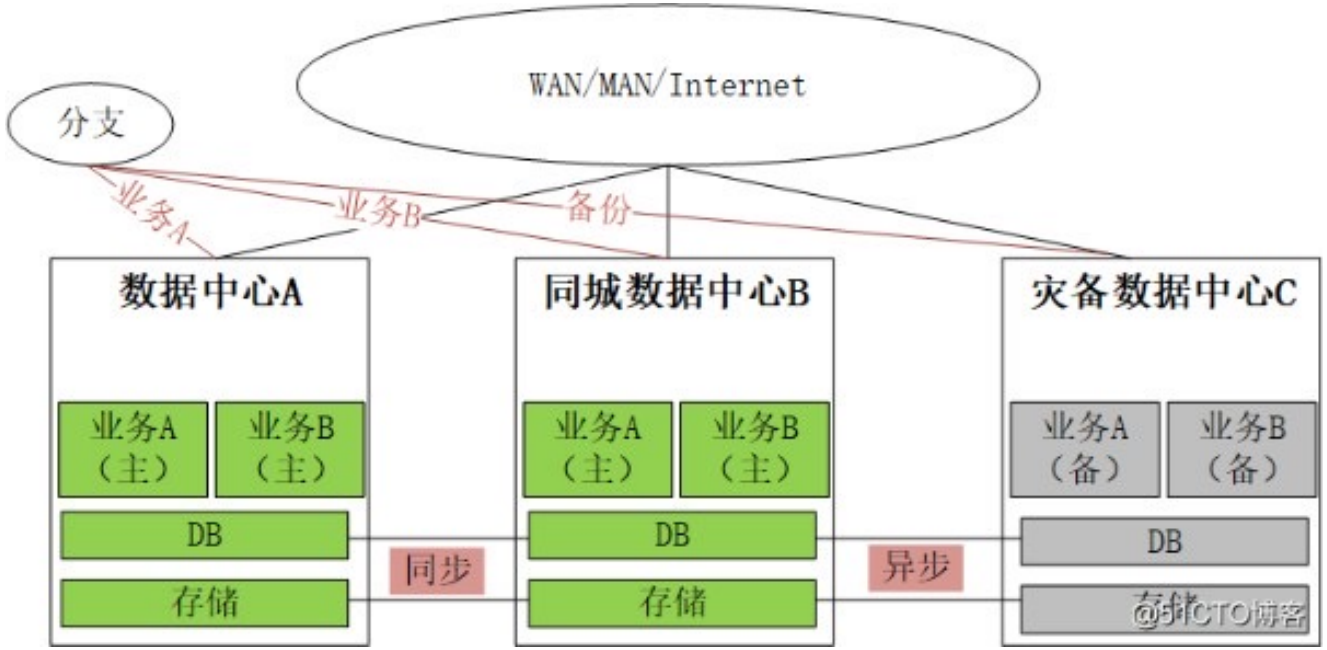
- Normally we may think security products like firewall, anti-virus software will make us safe.
- But more important thing is about people and related regulations.
- ISO27000 ensuring Integrity & Confidentiality.

  It was divided to many topics category in:
  - Physical and Environmental Security
  - Human Resource security
  - Access control

Which one of CIA is NOT covered?

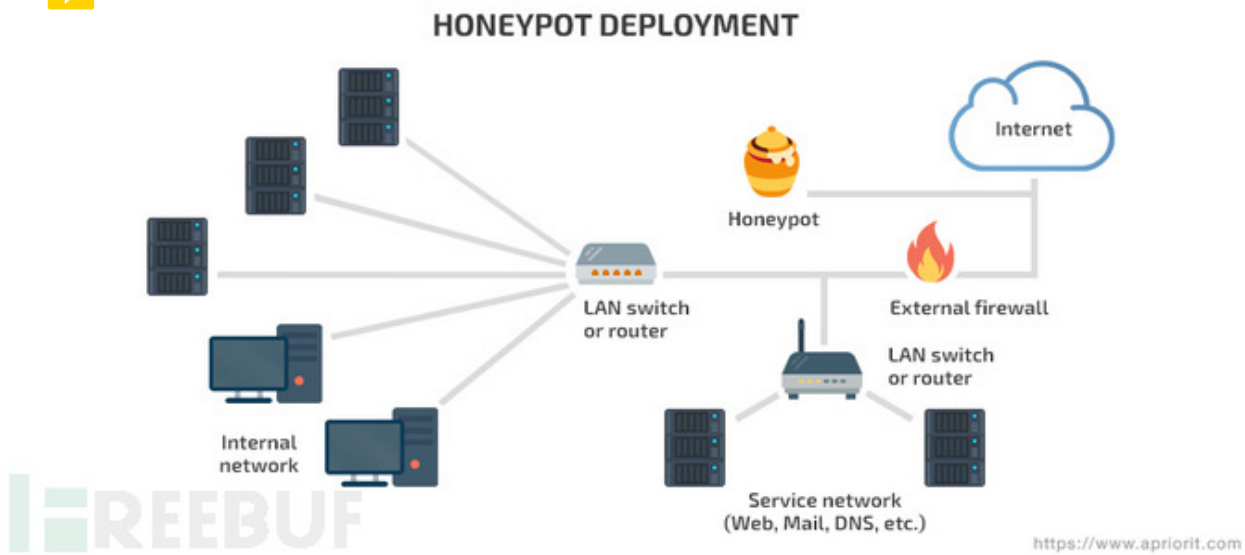
https://www.trueability.com/security/
https://www.mitre.org/capabilities/cybersecurity/overview/cybersecurity-blog/more-ancient-wisdom-for-the

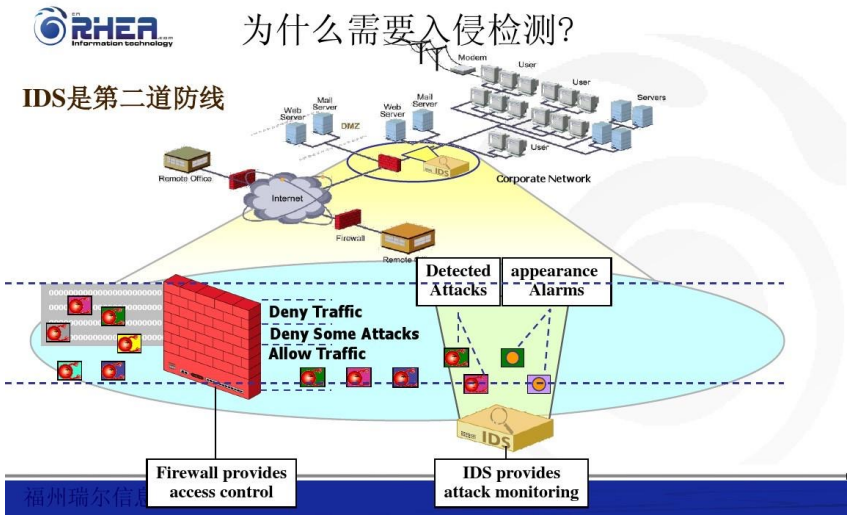
Infrastructure level

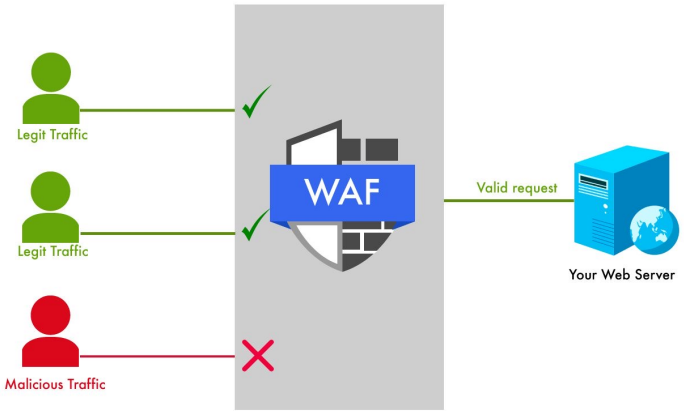


http://www.shangmayuan.com/a/e193023d83a94fb6b420b762.html

Application level







https://www.technolush.com/blog/common-web-application-threats
https://www.freebuf.com/articles/network/208895.html

Some general suggestions

- There is NO absolute security.
- Do the enough and appropriate evaluation and investment.
- Good enough lock for the asset.

- The highest risk is:

  "You think you are safe!!!"

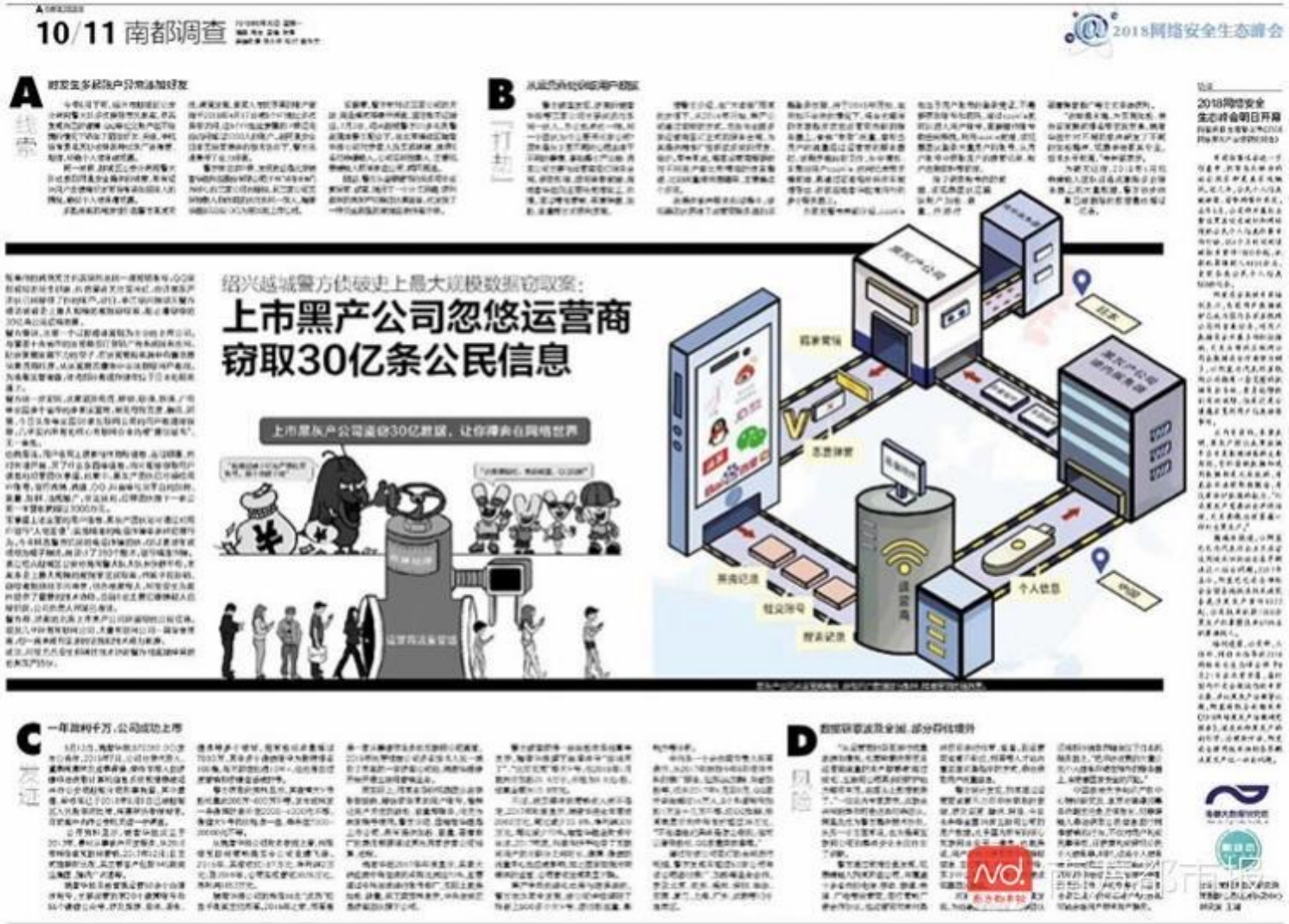
https://zhuanlan.zhihu.com/p/143757293

Some general suggestions

第一级：	一旦受到破坏会对相关公民、法人和其他组织的合法权益造成损害，但不危害国家安全、社会秩序和公共利益的一般网络；
第二级：	一旦受到破坏会对相关公民、法人和其他组织的合法权益造成严重损害，或者对社会秩序和公共利益造成危害，但不危害国家安全的一般网络；
第三级：	一旦受到破坏会对相关公民、法人和其他组织的合法权益造成特别严重损害，或者会对社会秩序和社会公共利益造成严重危害，或者对国家安全造成危害的重要网络；
第四级：	一旦受到破坏会对社会秩序和公共利益造成特别严重危害，或者对国家安全造成严重危害的特别重要网络；
第五级：	一旦受到破坏后会对国家安全造成特别严重危害的极其重要网络。

等保 划分标准

Thinks about this one


10/11 南都调查

2018网络安全生态峰会

绍兴越城警方侦破史上最大规模数据窃取案：

上市黑产公司忽悠运营商
窃取30亿条公民信息

- **Get the session key within telecom operators.**

https://baijiahao.baidu.com/s?id=1609311065725352764&wfr=spider&for=pc

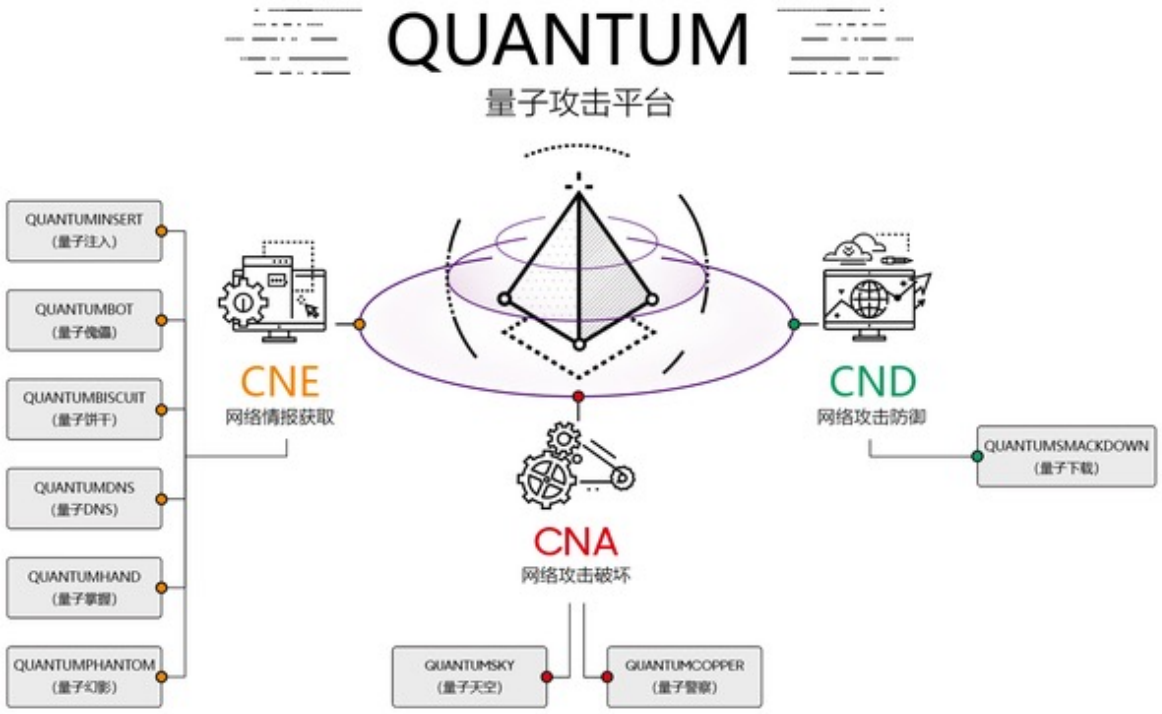
Or by nations

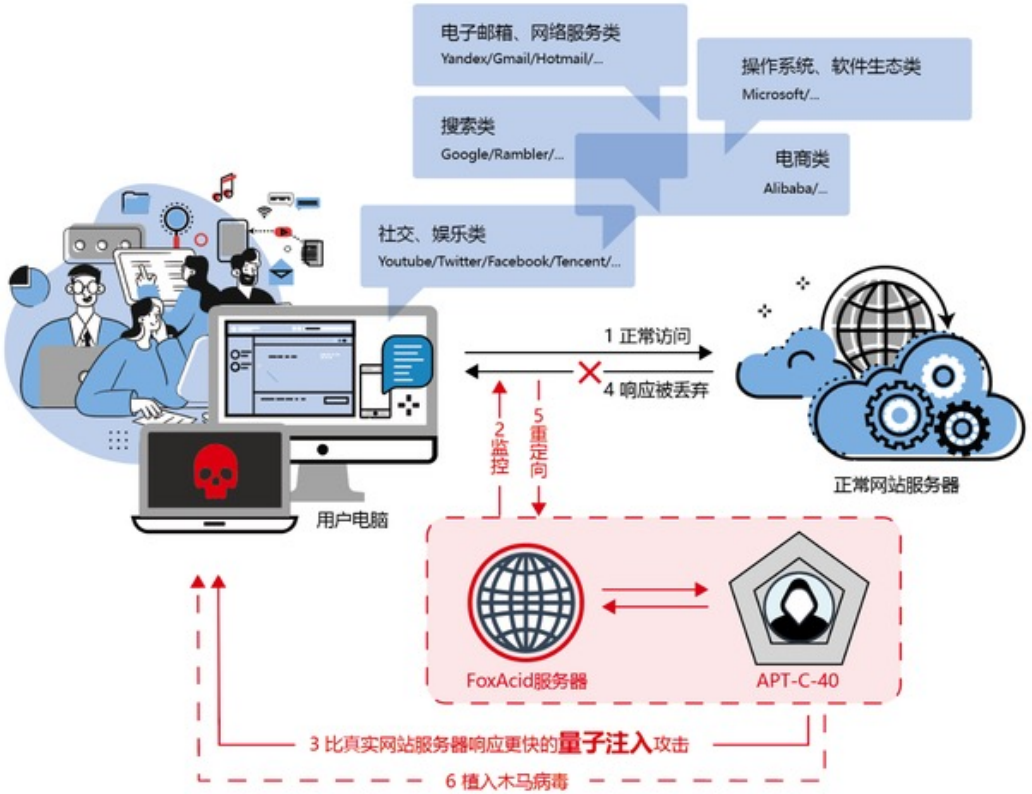
https://zhuanlan.zhihu.com/p/24037701

You may know these cases

https://www.zhihu.com/question/371511579/answer/1013863094

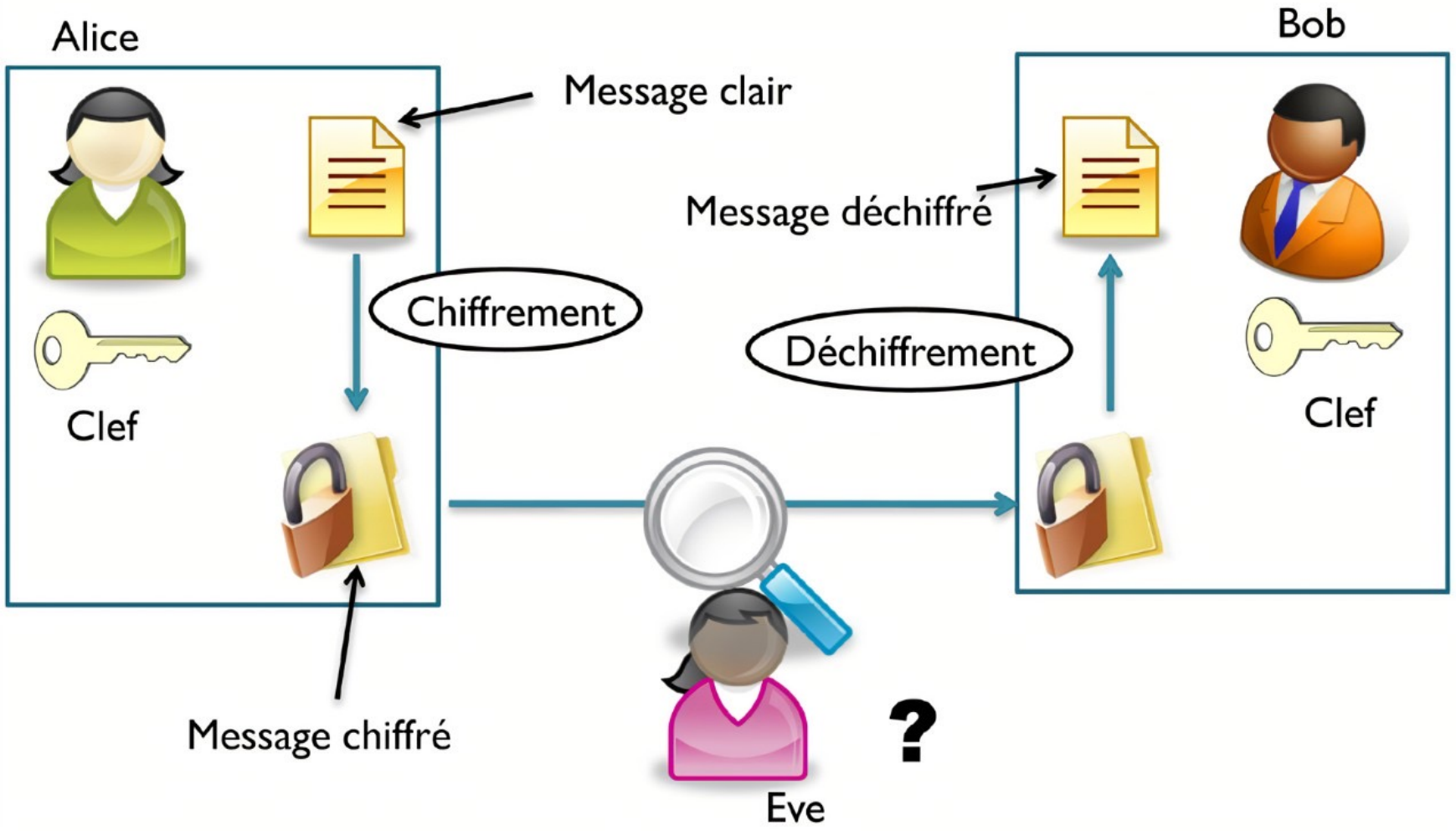
And …





https://baijiahao.baidu.com/s?id=1727991608277846854

Foreshow: Bob, Alice and Eve



To be continue …

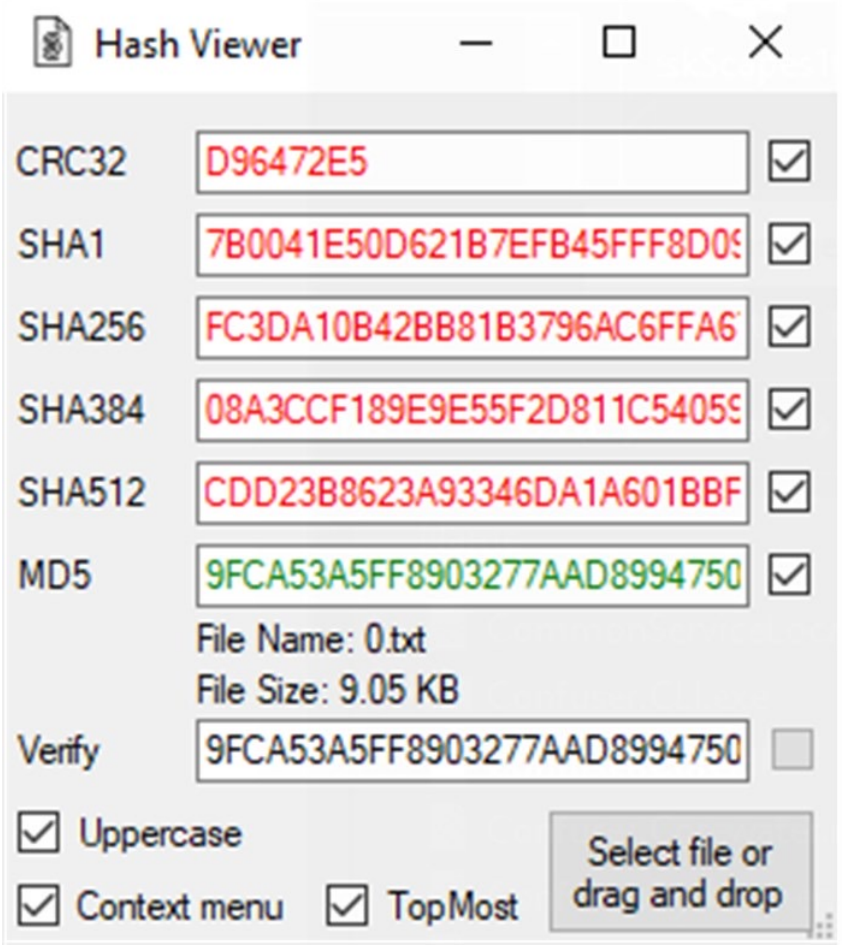
Encoding: the process of converting data from one form to another.

- The purpose of encryption is only the authorized people are allowed to read the information.
- Encryption needs encoding and decryption needs decoding.
- But, encoding like Base64 is **NOT** encryption. It is a rule everyone knows and can decode the information.

Why base64?

https://www.zhihu.com/question/36306744

Hash: message digest

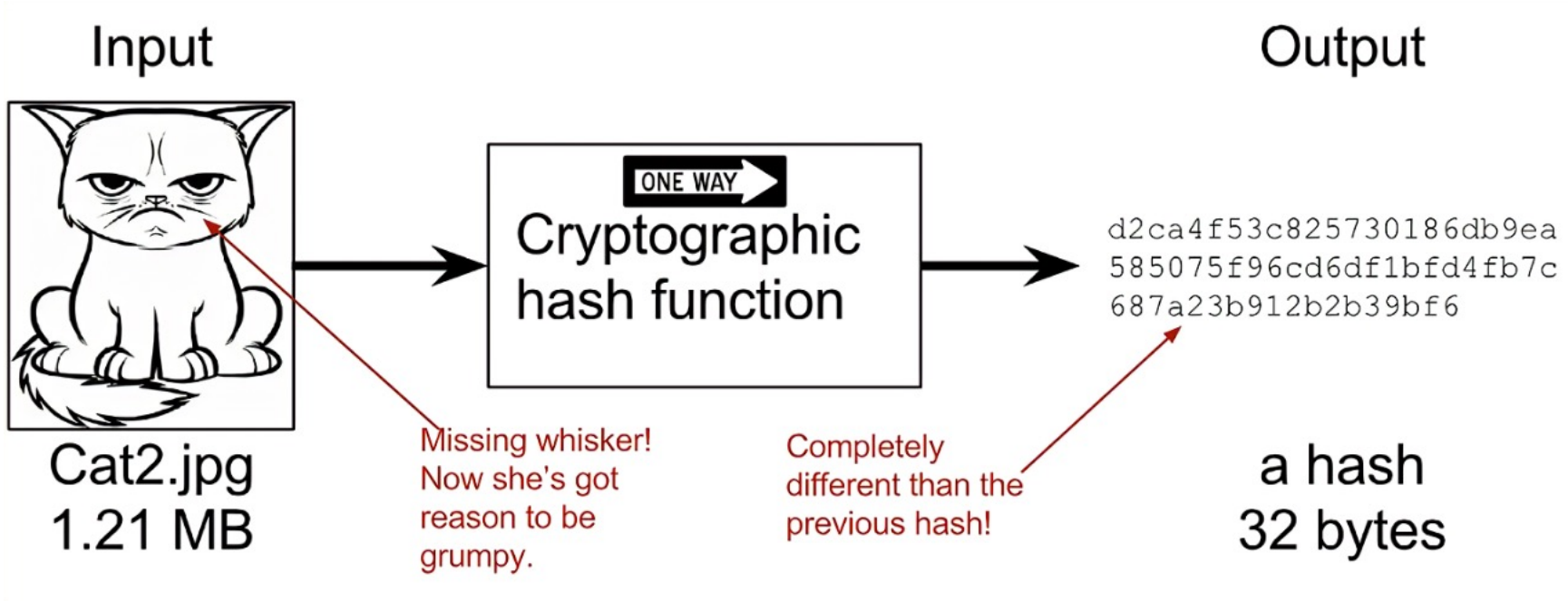


A dish of cooked meat cut into small pieces and cooked again.

Mathematical function that converts an input of arbitrary length into an output of a fixed length.

https://www.merriam-webster.com/dictionary/hash
https://www.zhihu.com/question/26762707/answer/40119521

Hash: message digest

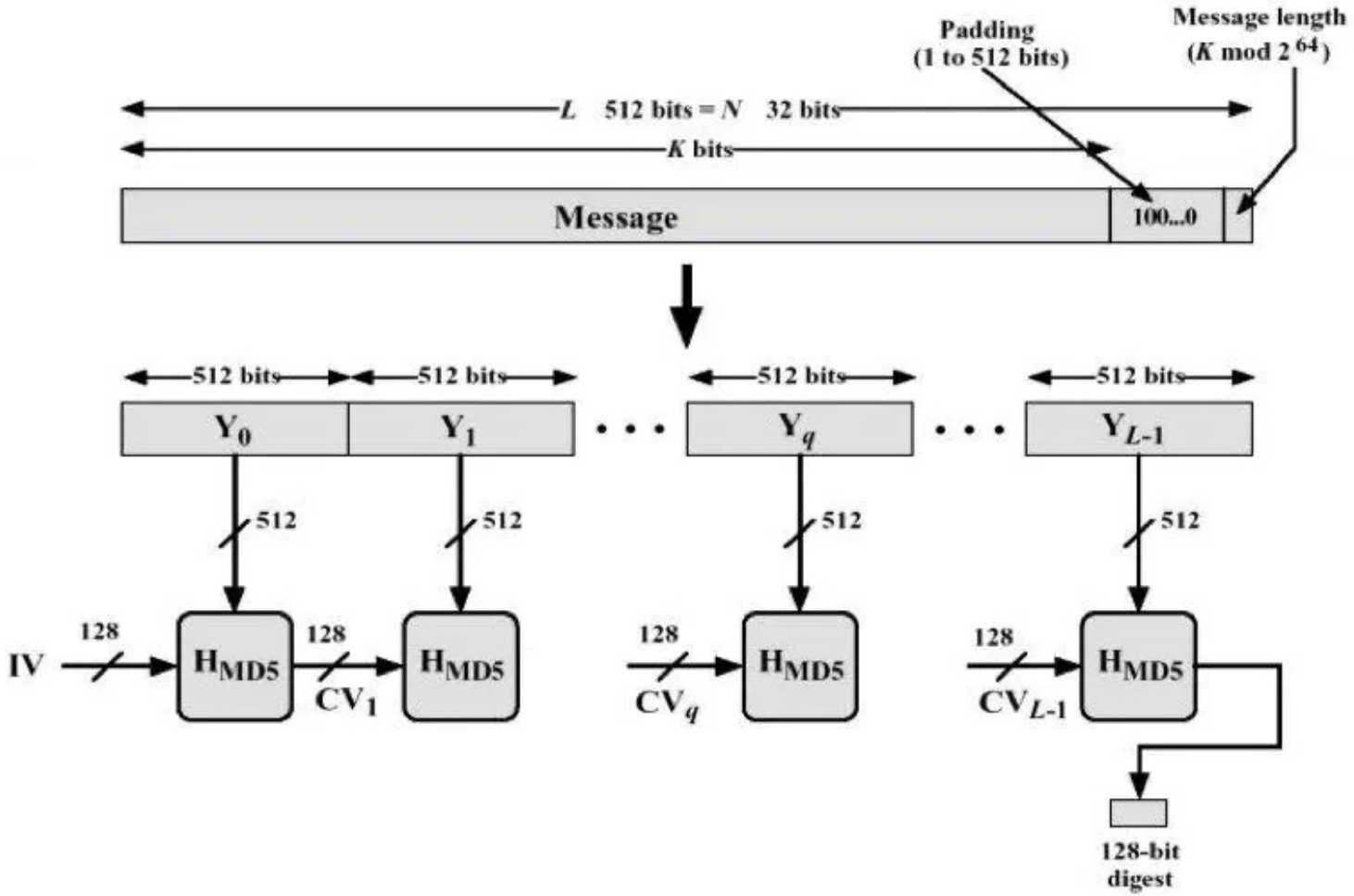


Only one way, "NO" way to decode it back

Hash: MD5

h_0	01	23	45	67
h_1	89	AB	CD	EF
h_2	FE	DC	BA	98
h_3	76	54	32	10

```
// Initialize variables - simple count in nibbles:
h0 = 0x67452301;
h1 = 0xefcdab89;
h2 = 0x98badcfe;
h3 = 0x10325476;
```



A widely used hash algorithm

https://www.jianshu.com/p/2d2debf78f69

SHA series

$$H_0^{(0)} = 67452301$$
$$H_1^{(0)} = efcdab89$$
$$H_2^{(0)} = 98badcfe$$
$$H_3^{(0)} = 10325476$$
$$H_4^{(0)} = c3d2e1f0.$$

3. For $t = 0$ to 79:

{

$T = ROTL^5(a) + f_t(b,c,d) + e + K_t + W_t$

$e = d$

$d = c$

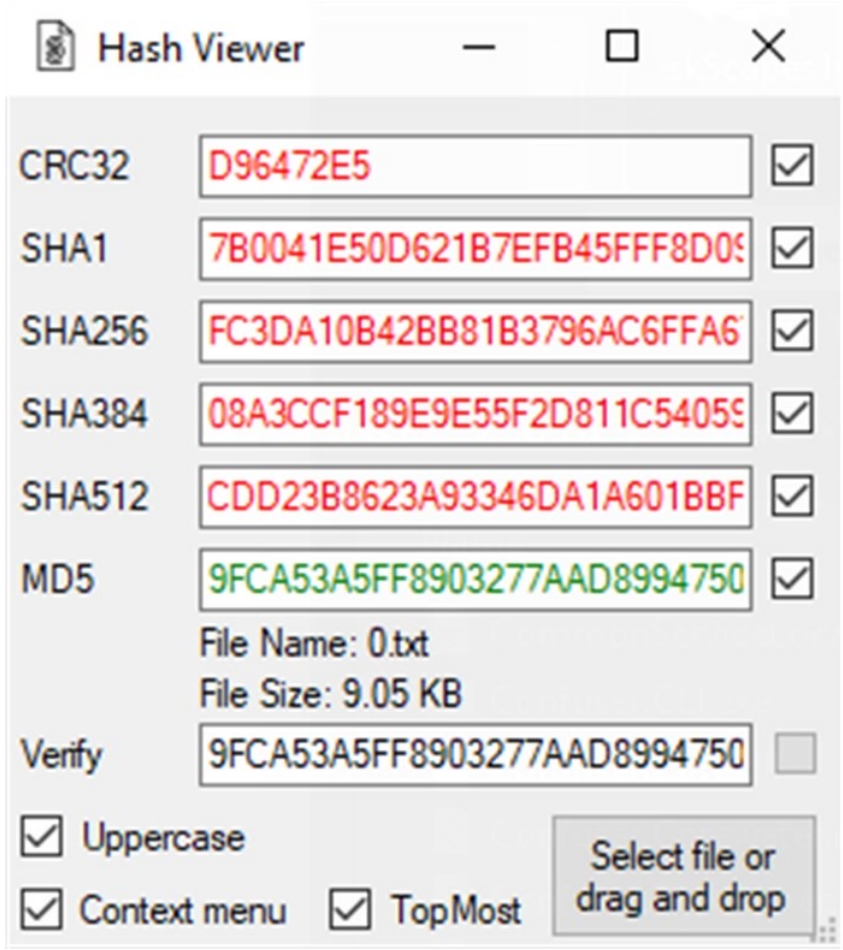
$c = ROTL^{30}(b)$

$b = a$

$a = T$

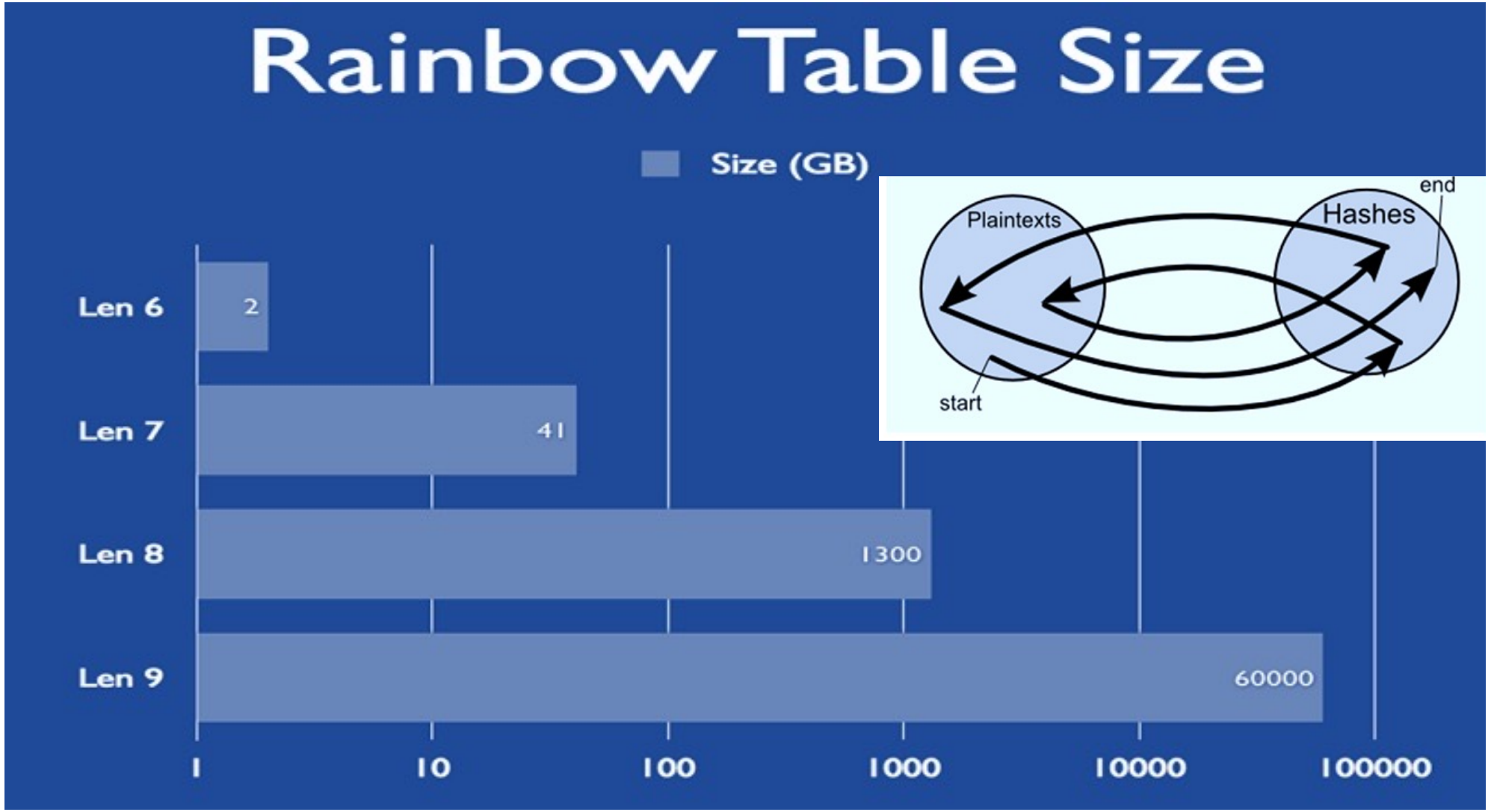
}

$$K_t = \begin{cases} 5a827999 & 0 \le t \le 19 \\ 6ed9eba1 & 20 \le t \le 39 \\ 8f1bbcdc & 40 \le t \le 59 \\ ca62c1d6 & 60 \le t \le 79. \end{cases} \quad (4.14)$$



https://www.bilibili.com/video/BV1Ua411679P

Rainbow table



https://ipwithease.com/introduction-to-rainbow-table-cyber-attack/

Hash collision attack

55

These following two different 128 byte sequences hash to the same:

MD5 Hash: 79054025255fb1a26e4bc422aef54eb4

The differences below are highlighted (bold). Sorry it's kind of hard to see.

```
d131dd02c5e6eec4693d9a0698aff95c 2fcab58712467eab4004583eb8fb7f89
55ad340609f4b30283e488832571415a 085125e8f7cdc99fd91dbdf280373c5b
d8823e3156348f5bae6dacd436c919c6 dd53e2b487da03fd02396306d248cda0
e99f33420f577ee8ce54b67080a80d1e c69821bcb6a8839396f9652b6ff72a70
```

and

```
d131dd02c5e6eec4693d9a0698aff95c 2fcab50712467eab4004583eb8fb7f89
55ad340609f4b30283e4888325f1415a 085125e8f7cdc99fd91dbd7280373c5b
d8823e3156348f5bae6dacd436c919c6 dd53e23487da03fd02396306d248cda0
e99f33420f577ee8ce54b6708028 0d1e c69821bcb6a8839396f965ab6ff72a70
```

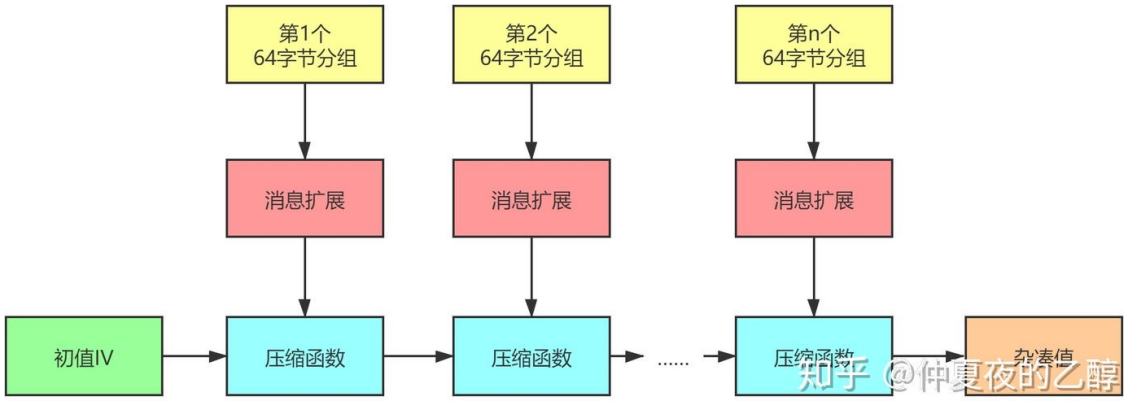
- Dr. 王小云 proved collisions can be found in MD5, SHA-1 algorithms
- She lead the design of SM-3

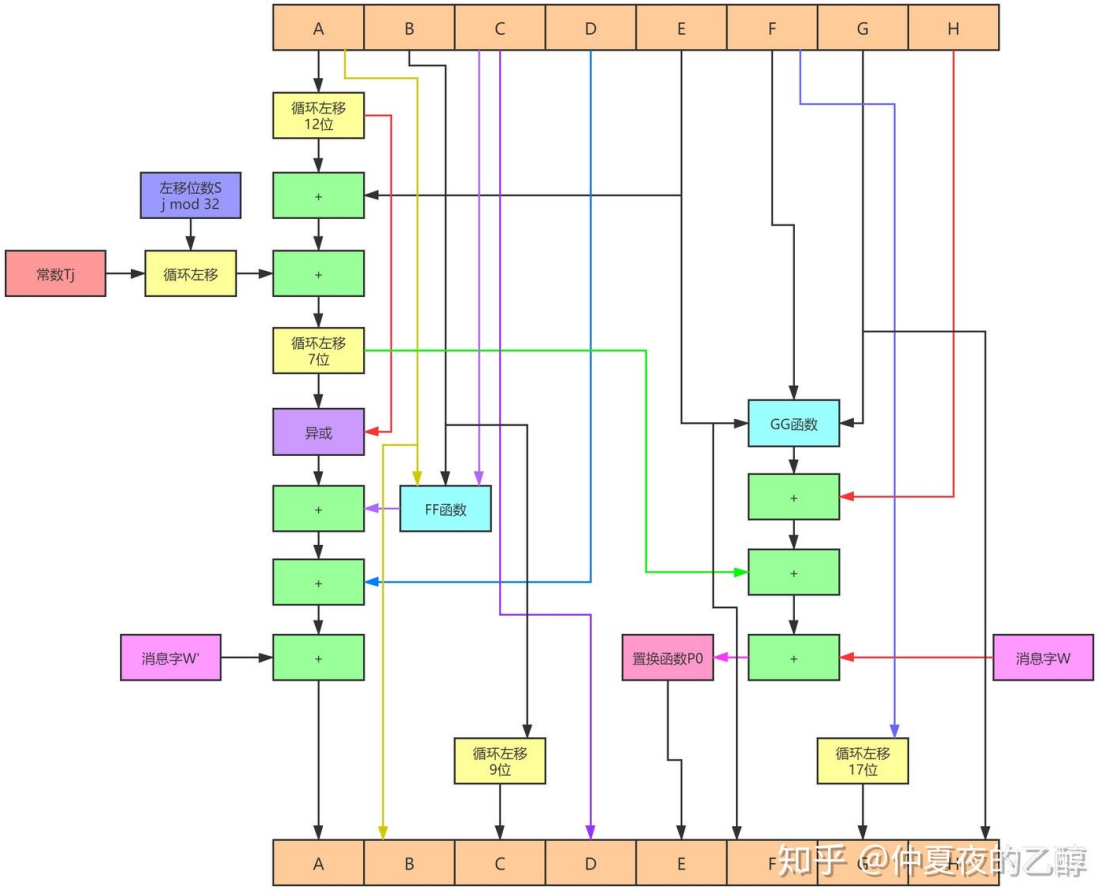
https://baike.baidu.com/item/%E7%8E%8B%E5%B0%8F%E4%BA%91/29050
https://zhuanlan.zhihu.com/p/377468857

Chinese algorithms of HASH

国家密码管理局

WWW.SCA.GOV.CN





- SM3 for HASH function

https://zhuanlan.zhihu.com/p/129692191