

Technologies for E- Commerce

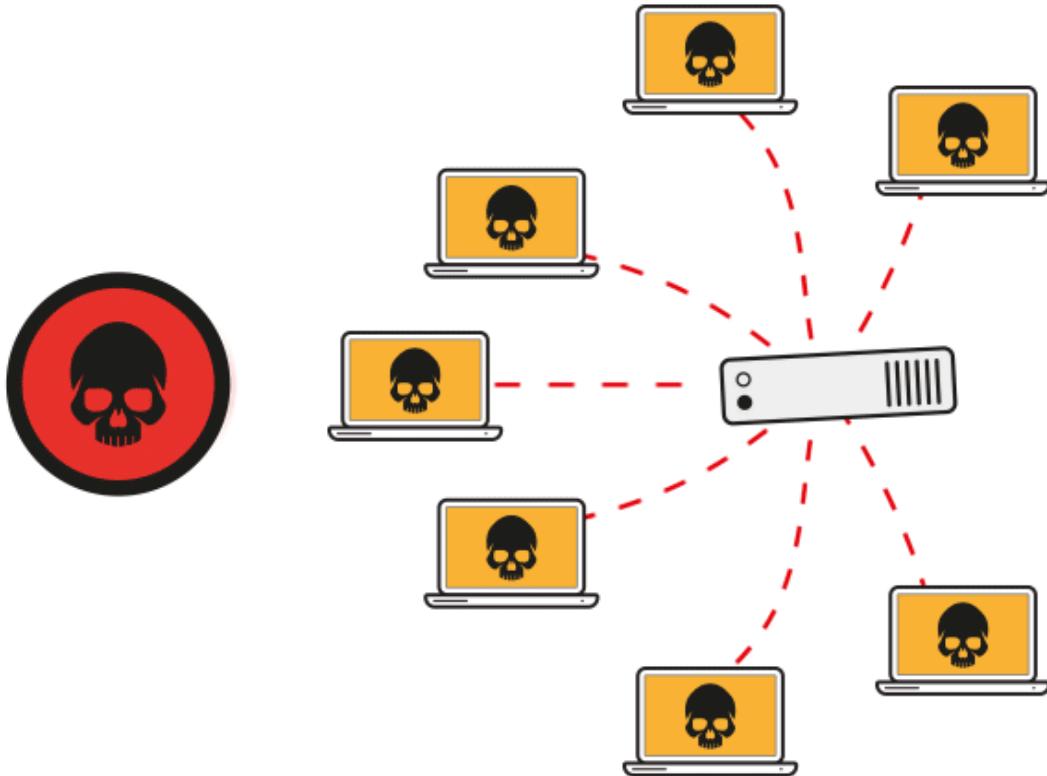
CAN302

**Department of Communications and Networking
Xi'an Jiaotong-Liverpool University (XJTLU)**

Week8 – Security in general

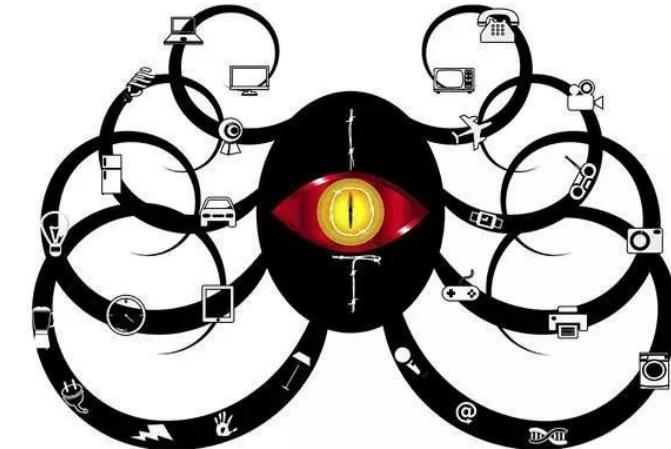


Attacks never sleep



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

Attacks never sleep



briankrebs @briankrebs

Follow

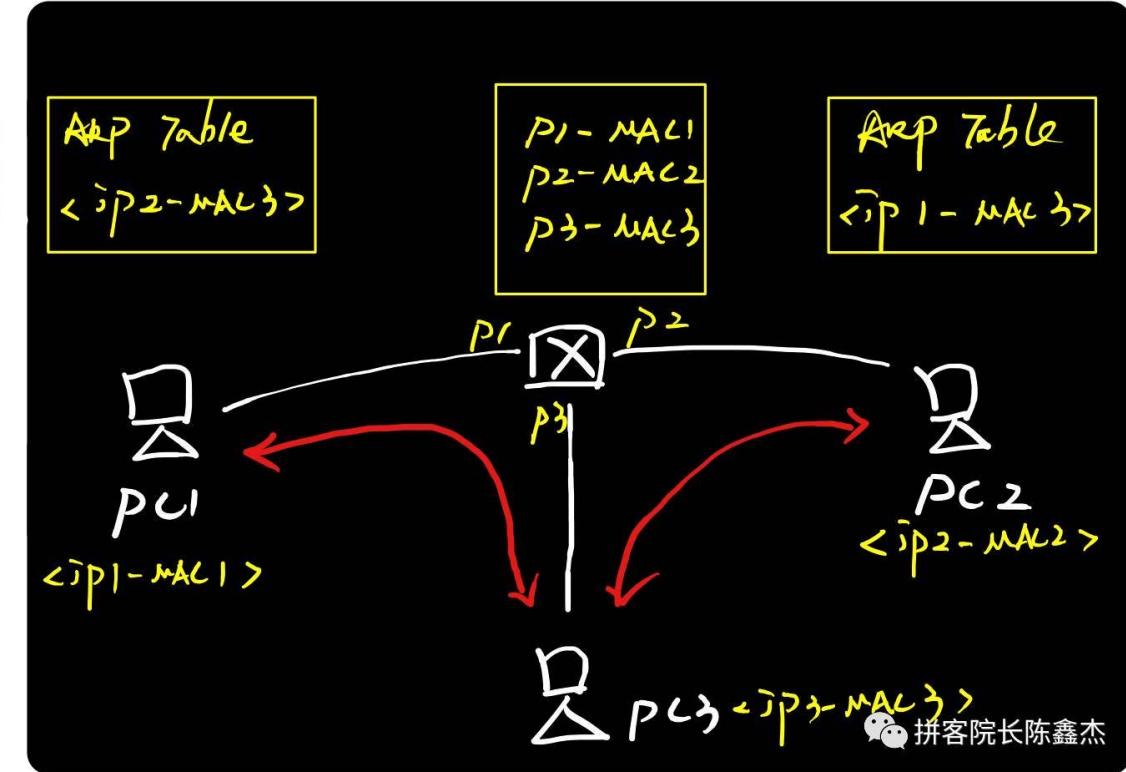
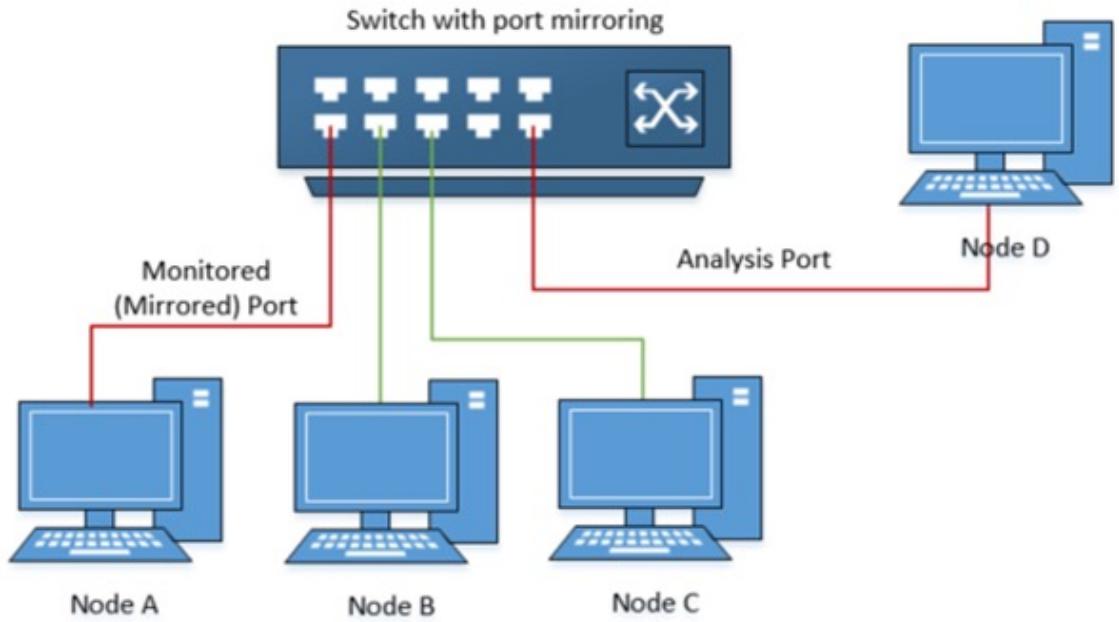
Holy moly. Prolexic reports my site was just hit with the largest DDOS the internet has ever seen. 665 Gbps. Site's still up. #FAIL
3:02 AM - 21 Sep 2016

Largest DDoS attack the Internet has ever seen!
665 Gbps!

Or by accidents



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>

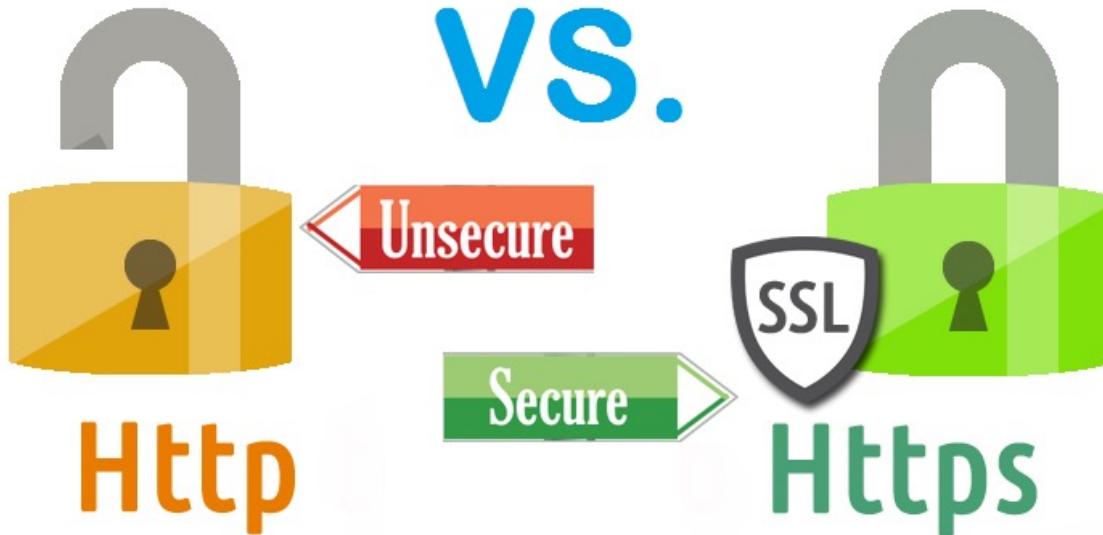
<https://v.qq.com/x/page/g0188shm2gf.html>

<https://www.zhihu.com/question/41432680>

Even happens to me



Case study: Https and Password



Http is NOT a protocol with encryption

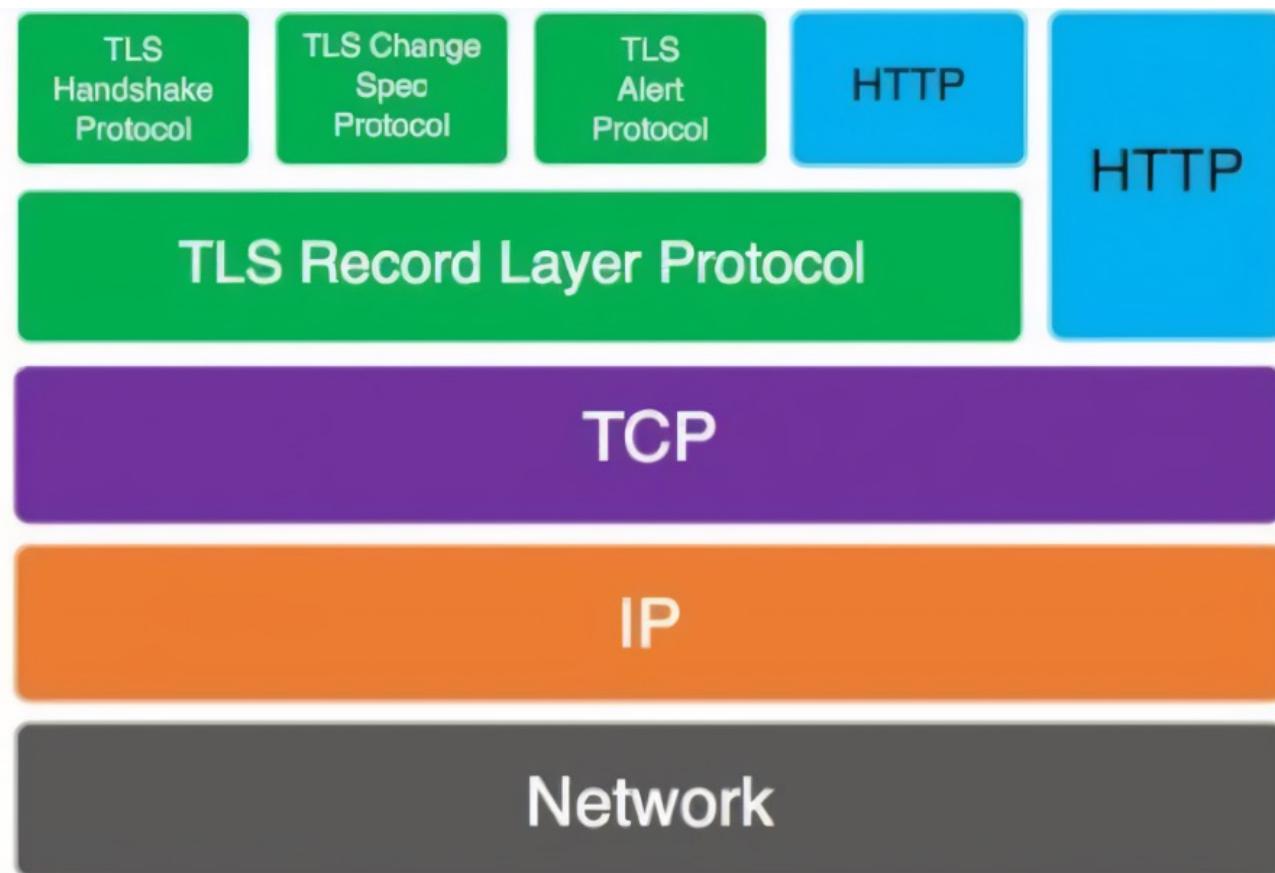
```
1 行      HTTP/1.1 200 OK
2 头      Content-Type: text/html; charset=utf-8
3          Content-length: 2048
4          Content-encoding: gzip
5 空行
6 体      <html>
7          <head>
8          </head>
9          <body>
10         <h1>尚硅谷</h1>
11         </body>
12     </html>
```



https://blog.csdn.net/weixin_43210113

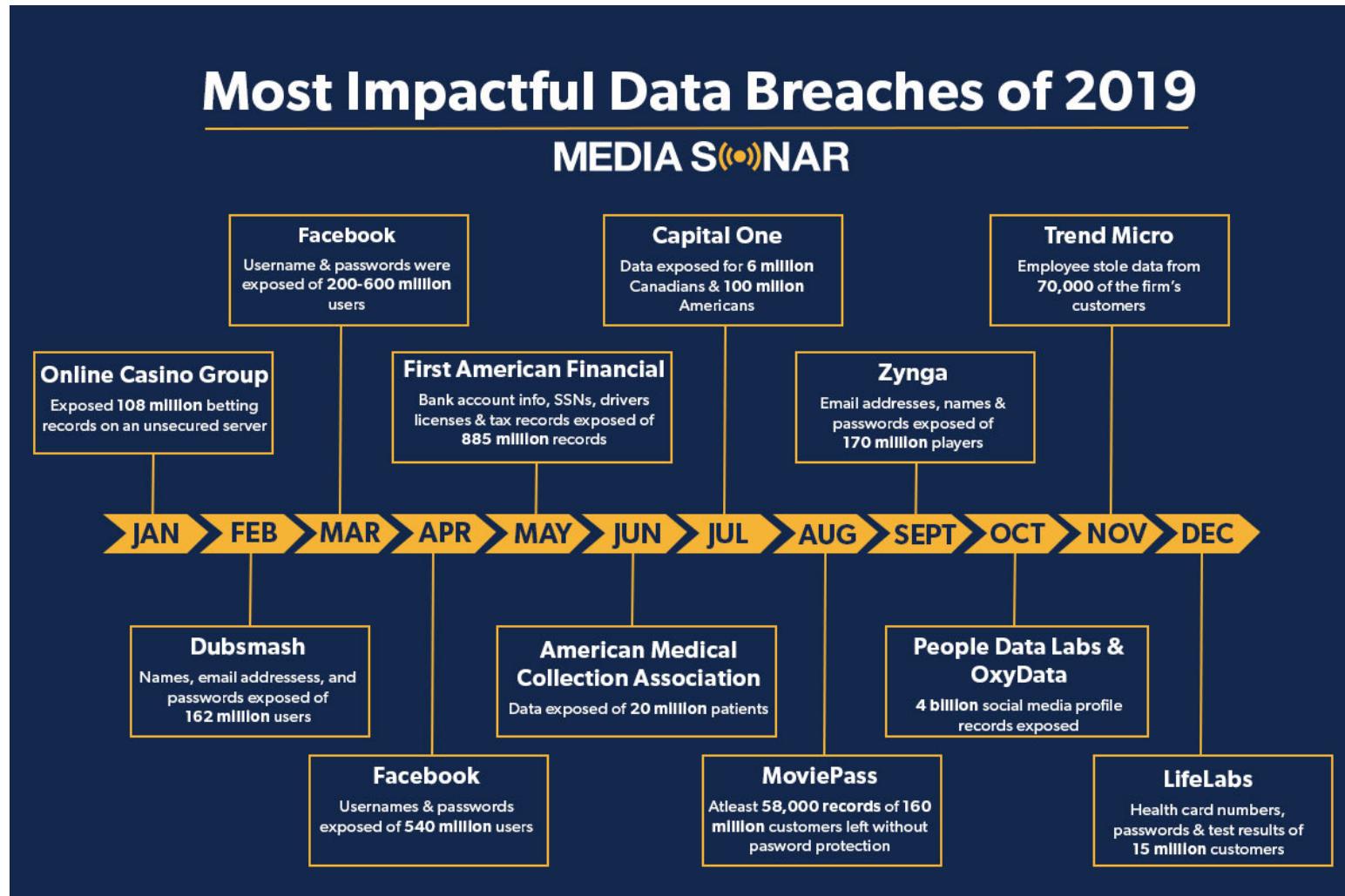
- All message in plain text.
- The biggest Vulnerability is Http protocol itself!

Https - add a lock for the Http protocol



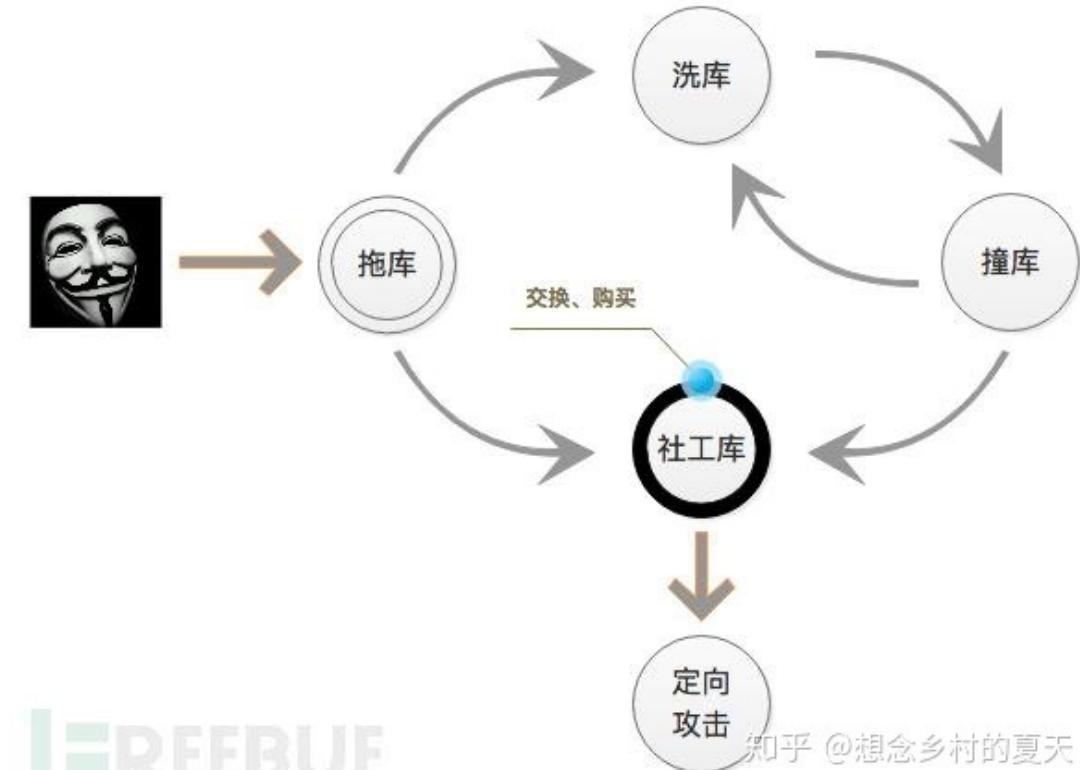
<https://v.qq.com/x/page/b0188l0shhr.html>
<https://v.qq.com/x/page/g0188shm2gf.html>
<https://www.zhihu.com/question/41432680>

Some many databases for username/passwd



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

Collision attacks



FREEBUF

知乎 @想念乡村的夏天

<https://zhuanlan.zhihu.com/p/126243422>

<https://www.scoopwhoop.com/most-dangerous-passwords-that-can-be-hacked/>

CIA triad



<https://www.cybernewsbox.com/cia-triad/>

<https://digitalforensicforest.com/2017/12/14/confidentiality-integrity-availability-cia/>

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
------------	------------	-------------

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>

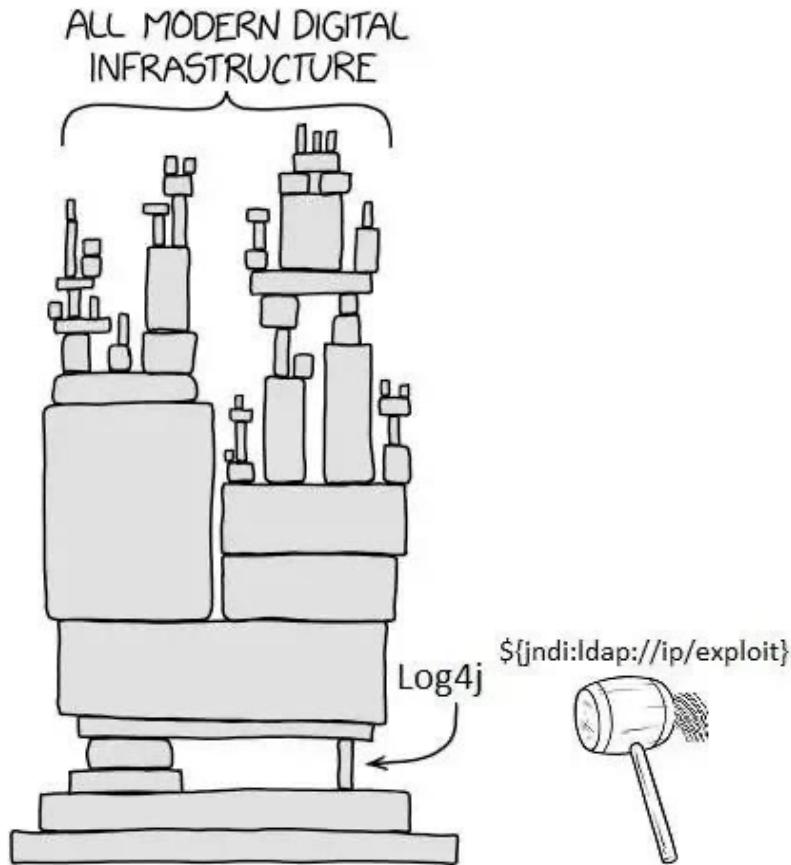
<https://www.securingpeople.com/security-risk-assessment/threat-vulnerability-risk/>

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

Vulnerability



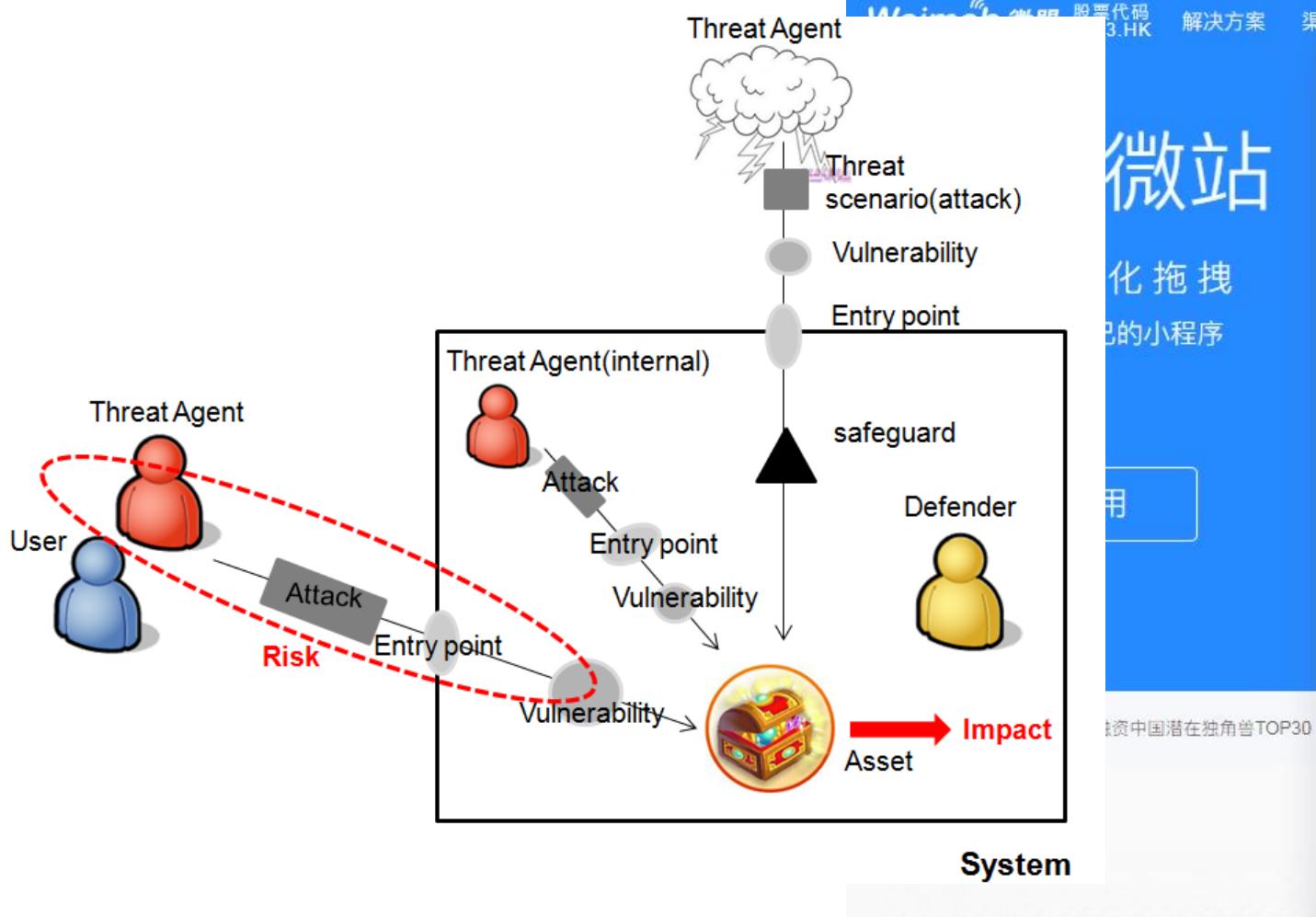
- A **vulnerability** is a weakness in hardware, software, personnel or procedures, which may be exploited by threat actors in order to achieve their goals.
- Many famous vulnerabilities, such as Log4j in 2020.
- Vulnerabilities can be marked by Common Vulnerability Scoring System or CVSS.
- It is **not**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

关于微盟系统故障的通告



关于微盟系统故障的通告

尊敬的微盟商户：

和您一样，我们一起度过了煎熬的36小时，我们预计此次故障还会持续一段时间，现就此次系统故障作如下通告：

2月23日19点，我们收到系统监控报警，服务出现故障，随后我们立刻召集相关技术人员进行定位，发现大面积服务集群无法响应，生产环境及数据遭受严重破坏。我们立刻启动紧急响应机制，并与腾讯云技术团队一起研究制定生产环境和数据修复方案。

截止到2月25日7点，我们的生产环境和数据修复都在有序的进行，我们预计2月25日晚上24点前我们的生产环境将修复完成，微盟所有新用户将可恢复服务，老用户由于数据修复时间问题，我们将提供临时过渡方案，我们预计老用户数据修复将可在2月28日晚上24点前完成。

我们事后对恶意破坏生产环境的犯罪嫌疑人进行追踪分析，成功定位到犯罪嫌疑人登录账号及IP地址，并于2月24日向宝山区公安局报案，目前犯罪嫌疑人已经被宝山区公安局进行刑事拘留，犯罪嫌疑人承认了犯罪的事实。犯罪嫌疑人乃微盟研发中心运维部核心运维人员贺某，贺某于2月23日晚18点56分通过个人VPN登入公司内网跳板机，因个人精神、生活等原因对微盟线上生产环境进行了恶意的破坏。

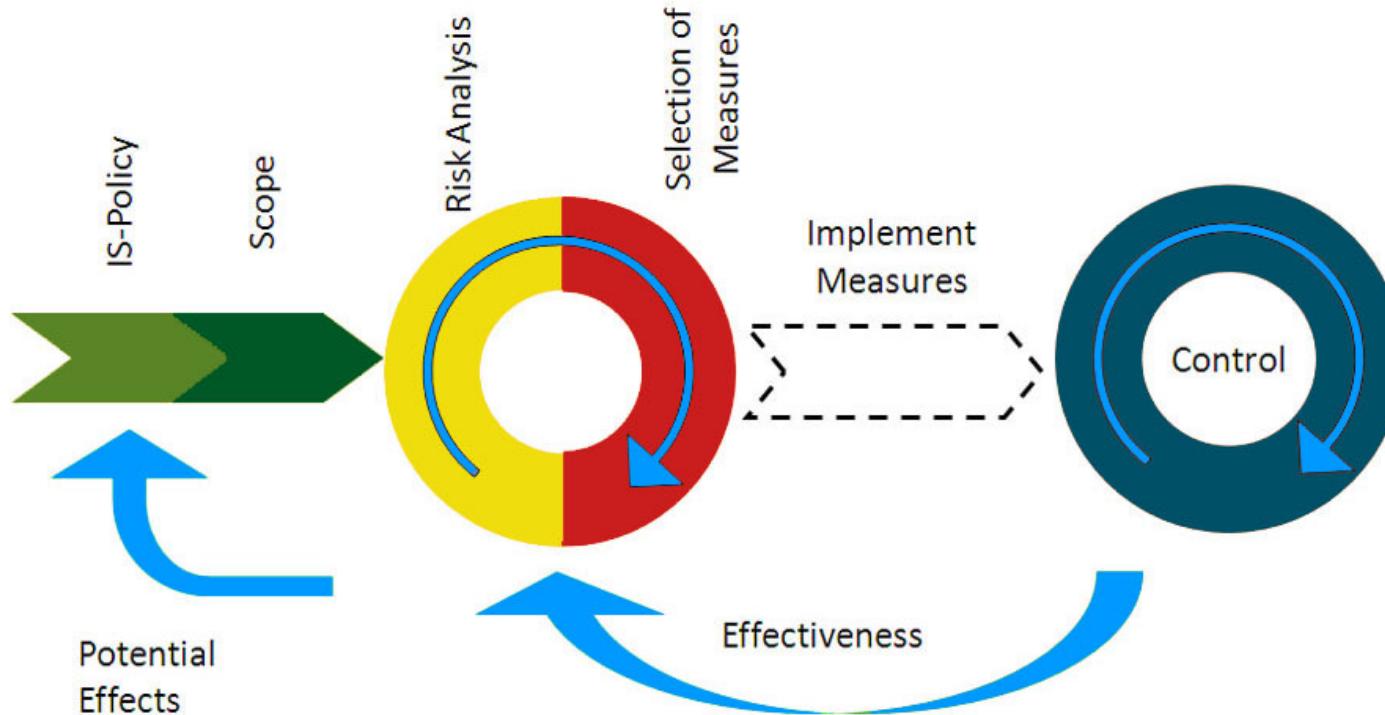
针对此次事故微盟深表歉意，我们正在拟定相关赔付方案来补偿因此次事故而遭受损失的商家，我们对此次因人为造成事故灾难无比愧疚，我们今后将一定吸取这个惨痛的教训，加强对线上运维的治理，同时我们也对因远程办公而疏忽对员工的精神状态的关注而深表痛惜！

微盟集团

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

Manage the risks

ISO / IEC 27000 Information Security Management System (ISMS)



- 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

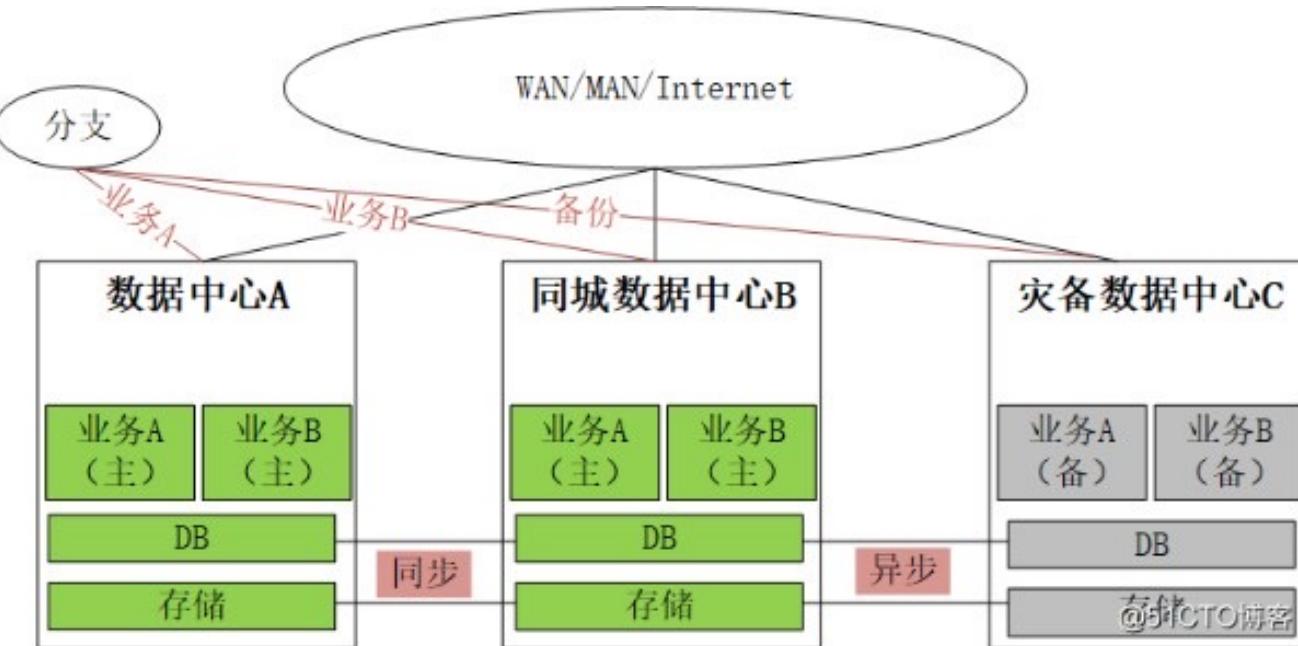
Which one of **CIA** is **NOT** covered?



<https://www.trueability.com/security/>

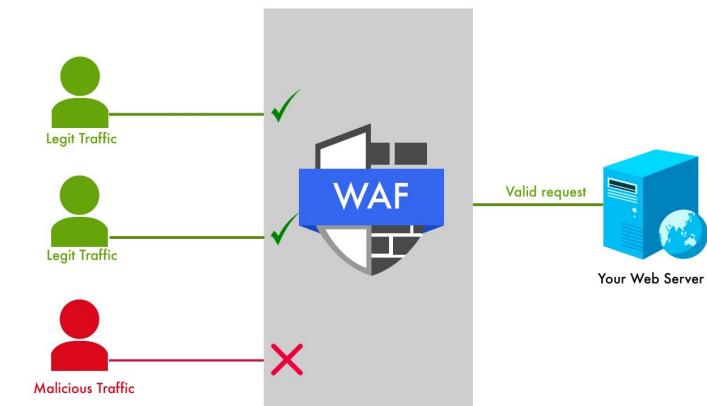
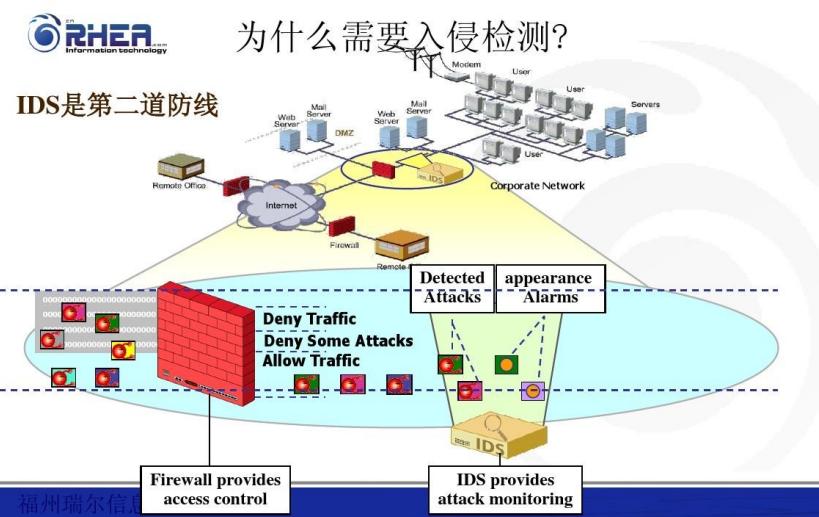
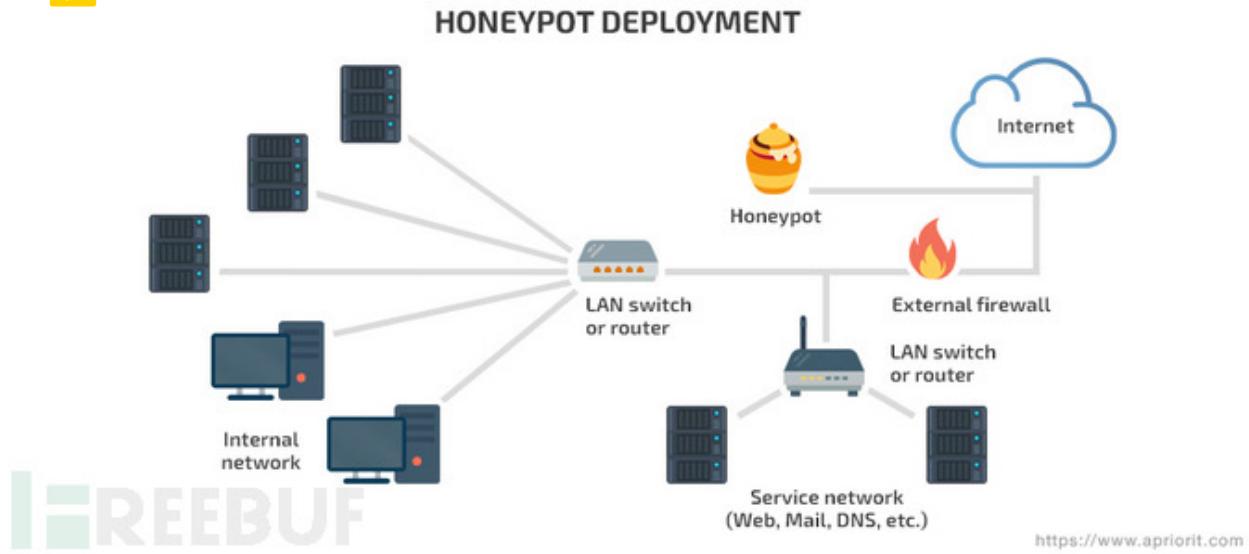
<https://www.mitre.org/capabilities/cybersecurity/overview/cybersecurity-blog/more-ancient-wisdom-for-the>

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!!!"

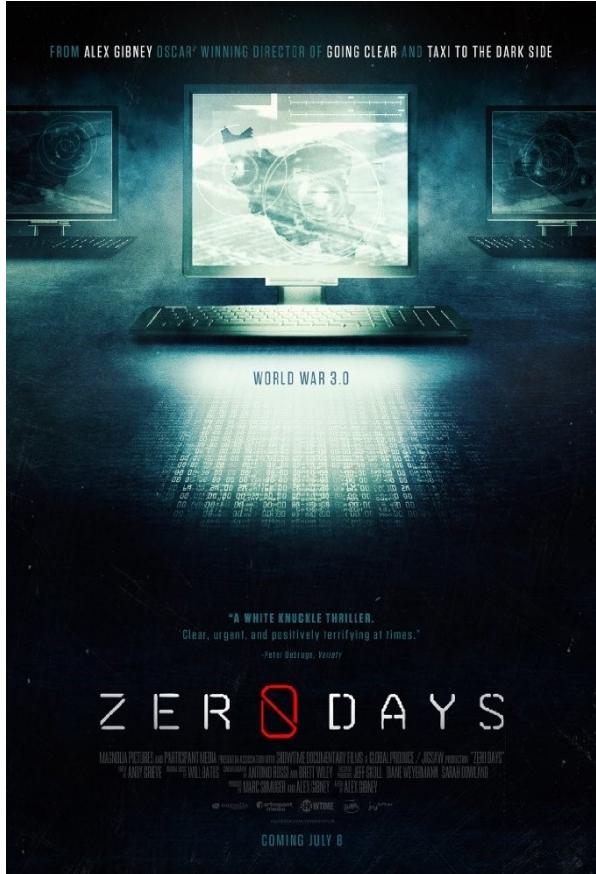
<https://zhuanlan.zhihu.com/p/143757293>

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

Or by nations



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

You may know these cases



The Washington Post
@washingtonpost

For decades, countries all over the world trusted a single company to keep the communications of their spies, soldiers and diplomats secret.

The Swiss company, Crypto AG, was secretly owned by the CIA.

由翻译自 英语 Google

几十年来，全世界的各个国家都信任一家公司来保护其间谍，士兵和外交官的通讯保密。

瑞士公司Crypto AG由CIA秘密拥有。

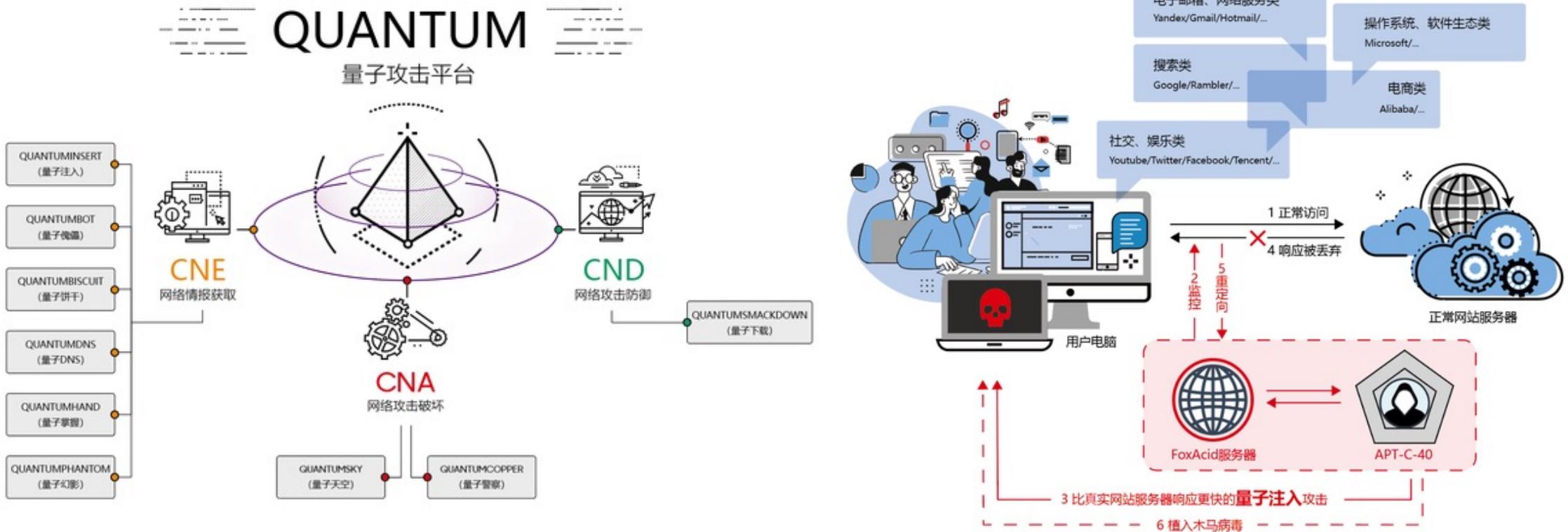


The CIA secretly bought a company that sold encryption devices across the U.S. and German intelligence agencies partnered on a scheme to dupe dozens of nations into buying rigged encryption systems — taking their ...
[washingtonpost.com](#)

上午3:14 · 2020年2月12日 · SocialFlow

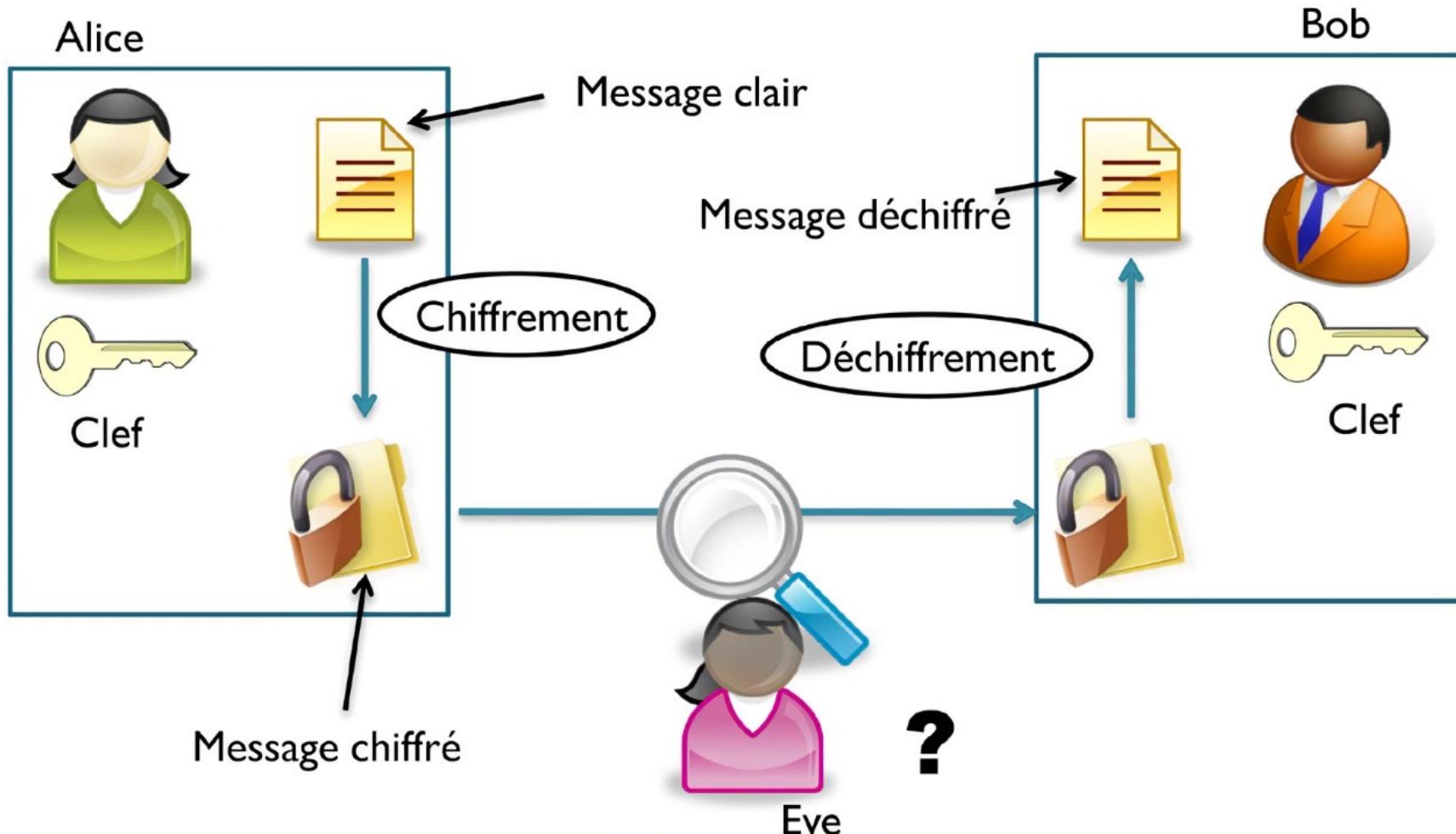
<https://www.zhihu.com/question/371511579/answer/1013863094>

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?



Hash: message digest



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

<https://www.merriam-webster.com/dictionary/hash>

<https://www.zhihu.com/question/26762707/answer/40119521>

Hash Viewer

CRC32	D96472E5	<input checked="" type="checkbox"/>
SHA1	7B0041E50D621B7EFB45FFF8D05	<input checked="" type="checkbox"/>
SHA256	FC3DA10B42BB81B3796AC6FFA6	<input checked="" type="checkbox"/>
SHA384	08A3CCF189E9E55F2D811C5405S	<input checked="" type="checkbox"/>
SHA512	CDD23B8623A93346DA1A601BBF	<input checked="" type="checkbox"/>
MD5	9FCA53A5FF8903277AAD8994750	<input checked="" type="checkbox"/>

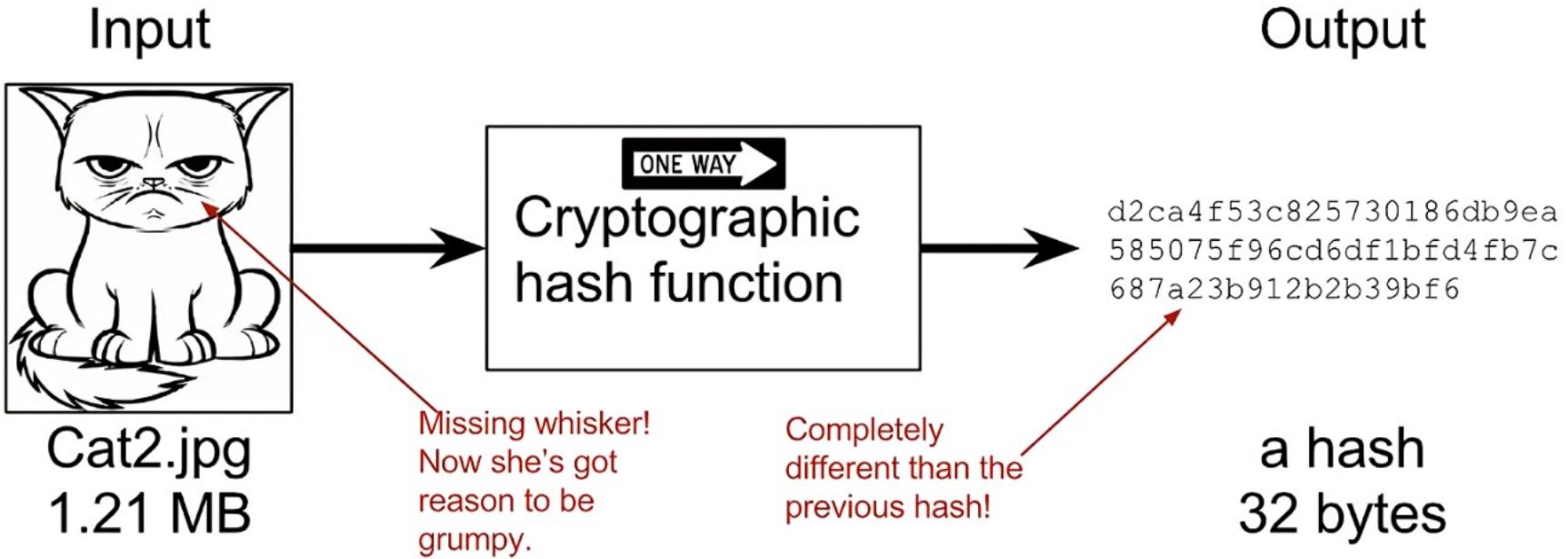
File Name: 0.txt
File Size: 9.05 KB

Verify

Uppercase Context menu TopMost Select file or drag and drop

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

Hash: message digest

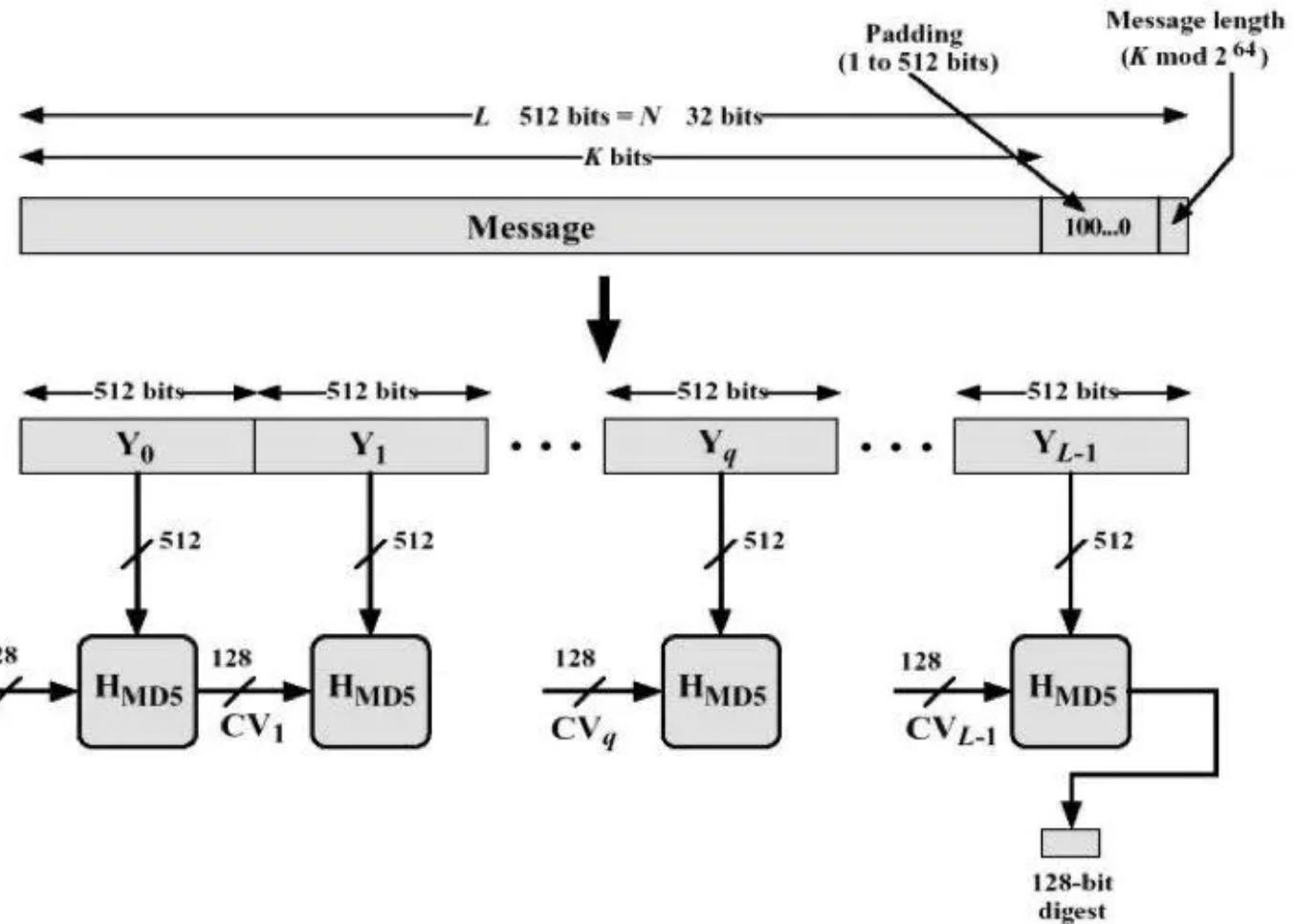


Only one way, “NO” way to decode it back

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

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



A widely used hash algorithm

SHA series

$$H_0^{(0)} = 67452301$$

$$H_1^{(0)} = \text{efcdab89}$$

$$H_2^{(0)} = 98badcfe$$

$$H_3^{(0)} = 10325476$$

$$H_4^{(0)} = \text{c3d2e1f0.}$$

3. For $t = 0$ to 79 :

$$\begin{aligned} T &= \text{ROTL}^5(a) + f_t(b, c, d) + e + K_t + W_t \\ e &= d \end{aligned}$$

$$d = c$$

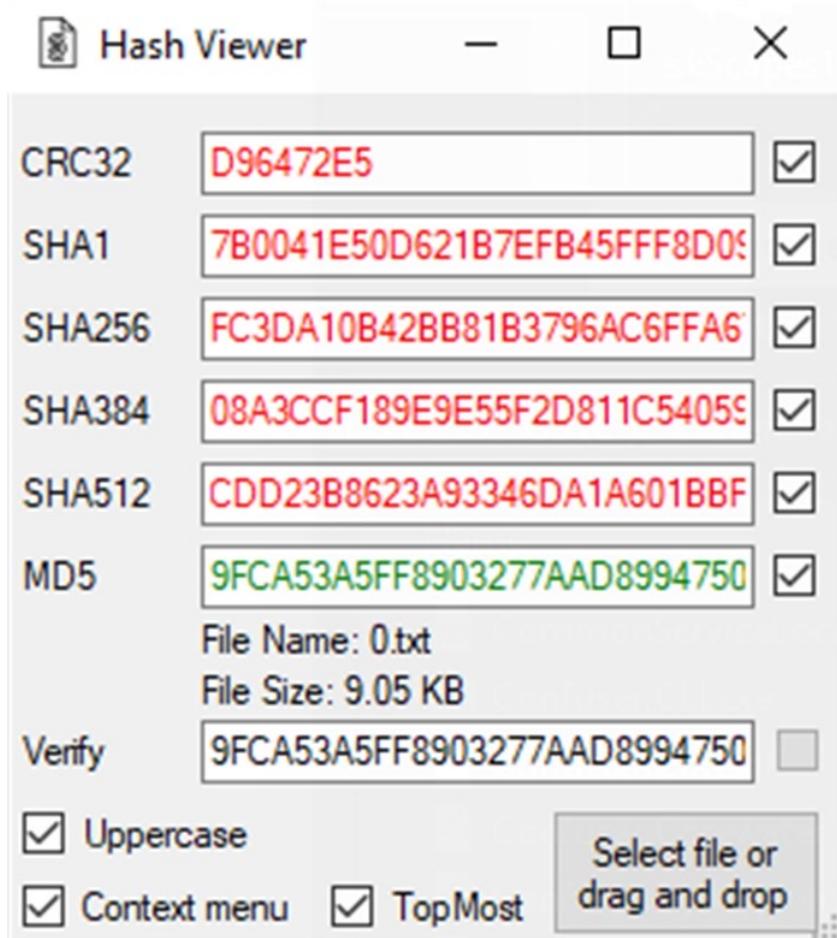
$$c = \text{ROTL}^{30}(b)$$

$$b = a$$

$$a = T$$

}

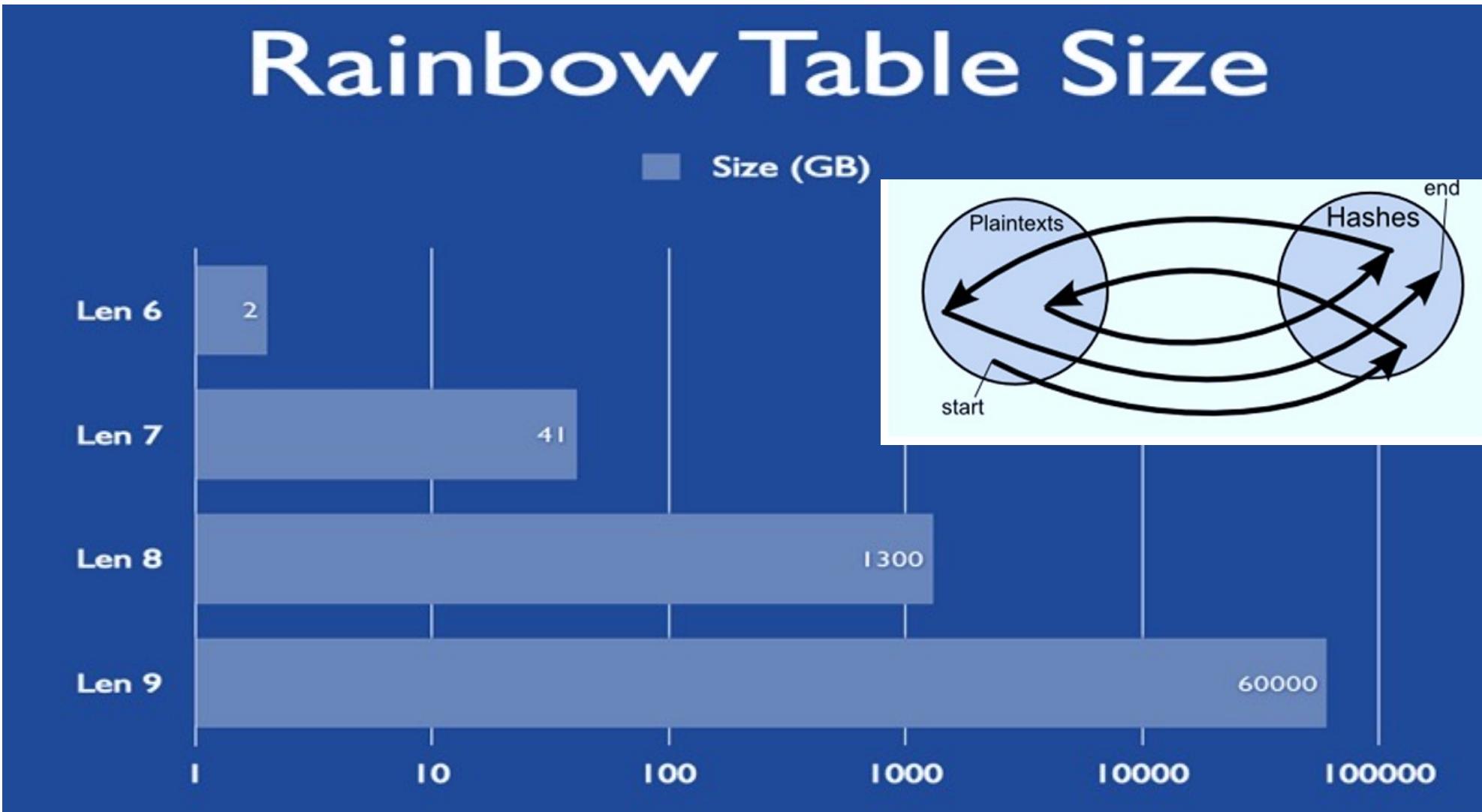
$$K_t = \begin{cases} 5a827999 & 0 \leq t \leq 19 \\ 6ed9ebal & 20 \leq t \leq 39 \\ 8f1bbcdcc & 40 \leq t \leq 59 \\ ca62c1d6 & 60 \leq t \leq 79. \end{cases} \quad (4.14)$$



Rainbow table



Rainbow Table Size



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

Hash collision attack

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

55 MD5 Hash: 79054025255fb1a26e4bc422aef54eb4

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

 
d131dd02c5e6eec4693d9a0698aff95c 2fcab**58**712467eab4004583eb8fb7f89
55ad340609f4b30283e4888325**f1**415a 085125e8f7cdc99fd91dbdf280373c5b
d8823e3156348f5bae6dacd436c919c6 dd53e2**b4**87da03fd02396306d248cda0
e99f33420f577ee8ce54b67080**a8**0d1e c69821bcb6a8839396f9652b6ff72a70

and

d131dd02c5e6eec4693d9a0698aff95c 2fcab**50**712467eab4004583eb8fb7f89
55ad340609f4b30283e4888325**f1**415a 085125e8f7cdc99fd91dbd**72**80373c5b
d8823e3156348f5bae6dacd436c919c6 dd53e2**34**87da03fd02396306d248cda0
e99f33420f577ee8ce54b67080280d1e c69821bcb6a8839396f965**ab**6ff72a70



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

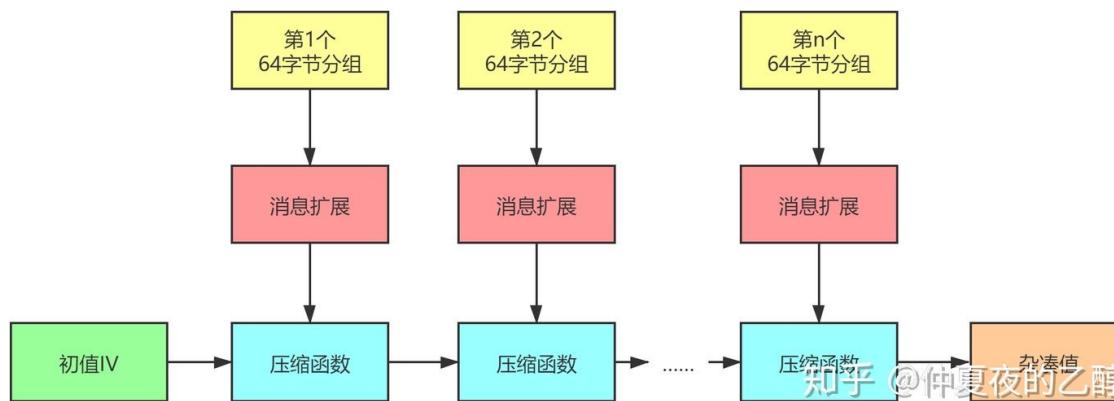
<https://baike.baidu.com/item/%E7%8E%8B%E5%B0%8F%E4%BA%91/29050>
<https://zhuanlan.zhihu.com/p/377468857>

Chinese algorithms of HASH



国家密码管理局

WWW.SCA.GOV.CN



- SM3 for HASH function

