1

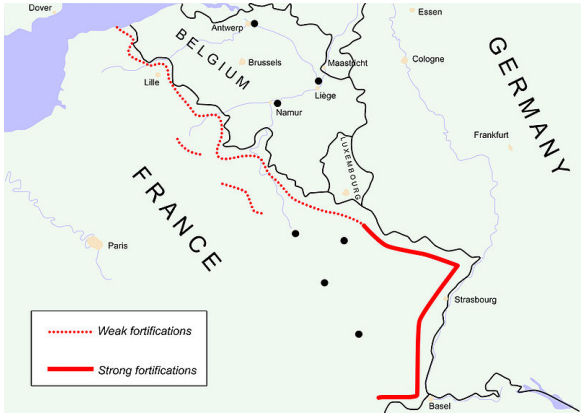
Security is hard, and it is much harder than ever before

请同学们讨论两个问题：

1. 为什么安全是一件困难的事？
2. 为什么目前的安全形势比以往任何时间都要严峻？

2

Why security is hard?

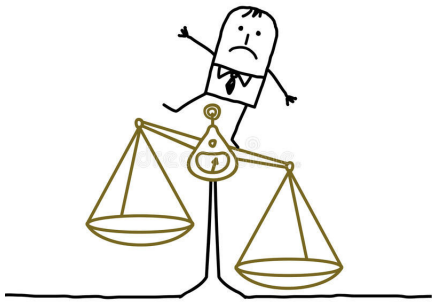


3

Why security is hard?

Attacker

Defender



4

Why security is hard?

Software

Hardware

Data

Target rich

Cloud

IoT

People

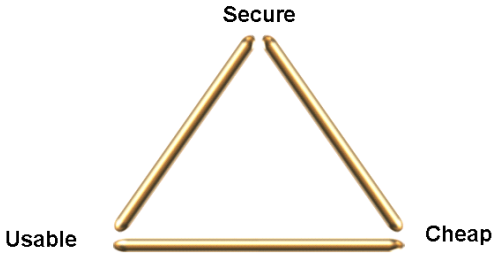
5

Why security is hard?

- **Security is often an afterthought.**

6

Security is a tradeoff



7

- He who defends everything defends nothing.
- 处处设防等于不设防。

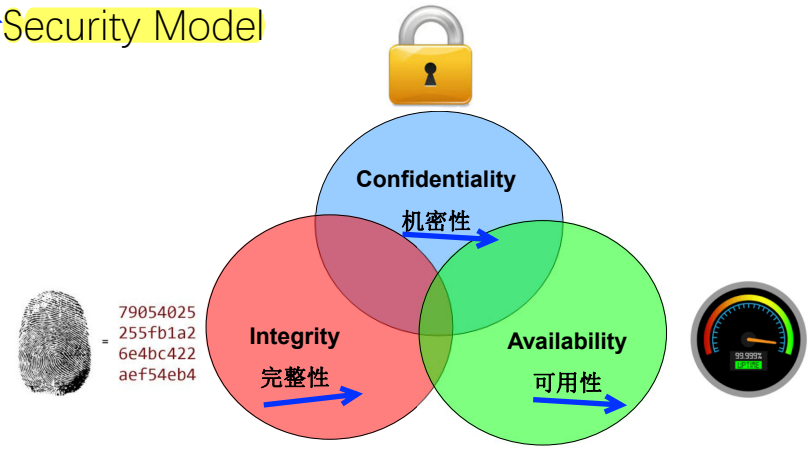
8

CIA model

- A simple but widely-applicable security model is the CIA triad.
- These are the three key principles which should be guaranteed in any kind of secure system.

9

Security Model



10

Confidentiality

- How secure is the information?
- How secure does the data need to be?
- Best methods
  - Physical protections
  - Electronic protections
- Failure of confidentiality occurs if someone can obtain and view the data

11


```
-----BEGIN PGP MESSAGE-----
Version: PGPsdk version 1.1.1 (C) 1997 Pretty Good Privacy, Inc.

qANQR1DBwU4DODM1G9a+wPwQCACtqlc5XlgE/hHOftEeF985UJ1kAtUDvRRyojH8
C+0HcmywLcZoAQ6slotbEM42rMZ3gldn8PeahXVjV500xOJSw1la+eJr1GA+SBUE
+fDDpRMAvQ5z5Rn16K9pvyU3gpgSxCc7yDfZroVhqvHGS9fVDuFNZ338GCk/D41+
RCLr3W+gCBPCV6RIiPiKL5vxQGWb2tWJudcd7L/1THEd3rTPJ9d07Yz72fB90Kng
v5x+yEP+bHa+SJ9Wyc6tdMQydCwAl6Ju3vHudkKULC0jC5vGw42WJ6SNEUlnZ8jG
Bqn0H8StnpEgQgVFBlmZ95H8atpiw9SiduzbMmmpiD6xP3u2CACHnm51dPTSW0Vx
Vm6dArfjvWjSmrajuTcFW8JUy3RuXzXQxPVnyKZVXUfT19PhB09HBJ2S19Eht/kb
K3P34xgJgX5Pt2MqTpOl6n2yg76uzgVJv+5uQF6txy2S73/20bkmfZ7EOjNAE4FLF
VPRbl/MrN9xYpruXzwV8xkBvwFB9CRef3i+080geVYTRLv03GLy8dHaV8K0mqTMP
d8xsfynW3fd1Xe/oLjSTwjXbEhoQlzRajxitkCFb81RnGTtdE9eM5ire8FH7mxm
97/0biqES/LJbT0RmgXpDiQ1ystMXmTe2Hg+LPReb9S0mmGj5JFmQM0+DnpkUmSVR
0qMFRDKtwcF0R5GCUuUeOT8OERf/SqYVWl+O9yT/4olH8JoRrsZbKxR7SnZxcGhV
/pAmuvQ8RJKrz3P0dLcwmCayAWlyu3uQJl31xfZA8AeQGeQsgwDqln8Kcqrkrlqv
UGHH7p5hVdkbPffU6sVnsLzQTllTpJBsXis+M+PHkR2lq4liKwhgZKuo5Vb68xEV
vGCs2FNVFCPKkgP0Rwmv1fSH254mVBf/vfcQl3jAsZTJs9SvATLqldxdR3T/Kpu5
RDSkQHW8A+pKpWNQZxbE9KFGrubigVZ4DldpaIyQOxa17fkBaXLxOH7gSC15K/Qm
ofov3dsVWl2ejBX3wF9vcOBvf6rcQrieZbWfSm03vT2xL3Qm1ggArHCq7U62Fb8M
jdj0UEIzk2UQ6gB7Uxb6t8alQ+7nJORQrr++zPSafLPfD3/1l/2eatdGOfPlbdw8
Qu2vHlpPVGVfVQvDbdtsFEqkhVtLLl4ClF6pzNRpe5q6/AFdKVjbJcPCXmHksWZV
imTBkacR/TMmtM5xODO6rzZ6baZdtlPoE19GdLv6nPoQ9baLayL0JVjwulkt3HfM
lwbhcnqPUDehe3Hy3Zl0k+fNt82HgA9Nz0r7AjqVLsrVpjdE0T5EHlcdh9nR8X7l
EsWVLXHgpys1ic0QsERGuBB1UaQTkyp9cl+Po6u61Uweyp4hkRMKYAZVW7jNDxNP
Y1TvGJXCtcnAjs7MM1ykh4vgLSvH8AKUPh6FiG7lP+QtUQaZe2w7idD4gP6btvMP
ZhpslW8in8D/tQplIyotfP7JEXsZ9rM4aavCipqxz+gmMh4istmf2y9GecpcMhdA
J4wyrO4BvkA+sZPNgs06iGXQJ1nHZ4E+LDgkbnaC9eJTFAQ4JLA8S0JPgOcT8ngc
UxG03kUqBVqJVJcsfVTFOVLuswx+NrqG8bHBLQxECU+xMBFxk350m4Ibv3R+u+HH
jTbC0e/AuJmklJvzrF4tJFmz8Gncx0J0fveaMLCiA2aKBuynAqiqWlcH5RZL8RlM
/CL1xNs/H0q1NnCifPHdvf1AhhVnjWeHX6Nz8t3xzocOJmRV7irsX1byq7zR4UJP
JTiAzakltim7dFzgv9LL4Wg1RUm/1sMUtpgt7erCXzhQ6f7Fti+K4zhL2W79GMk8
meWagv3RVms=
=UQgs
-----END PGP MESSAGE-----
```


12

Integrity

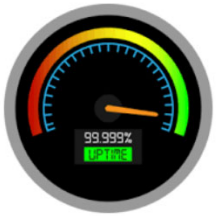
- How correct is the information?
- Has the data been modified during retrieval, in transit, or in storage?
- Best methods
  - Hashing of files and information
  - Checksums
- Failure of integrity occurs if someone modifies the data being stored or in transit.

13

Image Name	Download	Size	Version	sha256sum
Kali Linux 64 Bit	HTTP | Torrent	2.9G	2018.1	ed88466834ceeba65f426235ec191fb3580f71d50364ac5131daec1bf976b317
Kali Linux 32 Bit	HTTP | Torrent	2.9G	2018.1	b541a78a063b6385365ac00248631c4a18c92b8c4e3618db0b1bf751b495149f
Kali Linux Light 64 Bit	HTTP | Torrent	846M	2018.1	e47646078a5f31a952e9b5243a292d61bf6fc7af0d325f996c1fb45e0f721286
Kali Linux Light 32 Bit	HTTP | Torrent	846M	2018.1	5bf5ac2b1bfa969527c5125c404049400f9df0c44dbeb5ed716135f040ef95dc

14

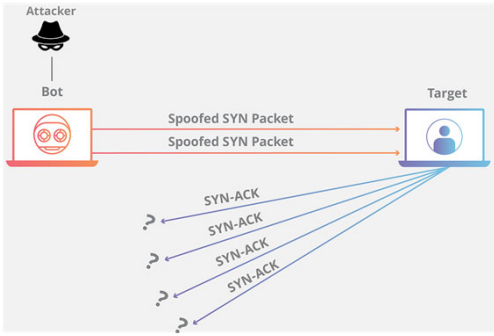
Availability



- How much uptime is the system providing?
- Is the data accessible by users at all times?
- Best methods
  - Redundancy in system design
  - Backup strategies and disaster recovery plan
- Failure of availability occurs if the data cannot be accessed by the end user

15

SYN flood attack



16

单选题 1分 设置

John copies Mary's homework.

A Confidentiality
B Integrity
C Availability

提交

17

单选题 1分 设置

Paul crashes Linda's system.

A Confidentiality
B Integrity
C Availability

提交

18

单选题 1分 设置

Carol changes the amount of Angelo's check from $100 to $1,000.

A Confidentiality
B Integrity
C Availability

提交

19

单选题 1分 设置

Gina forges Roger's signature on a deed.

A Confidentiality
B Integrity
C Availability

提交

20

信息安全事件中的CIA

- 2017年3月7日，维基解密（WikiLeaks）网站公布了大量据称是美国中央情报局（CIA）的内部文件，其中包括了CIA内部的组织资料，对电脑、手机等设备进行攻击的方法技术，以及进行网络攻击时使用的代码和真实样本。利用这些技术，不仅可以在电脑、手机平台上的Windows、iOS、Android等各类操作系统下发起入侵攻击，还可以操作智能电视等终端设备，甚至可以遥控智能汽车发起暗杀行动。
- 维基解密将这些数据命名为“7号军火库”（Vault 7），其中共包含8761份文件，包括7818份网页以及943个附件。

21

最大代码分发平台Github在周三遭受了一系列大规模分布式拒绝服务（DDoS）攻击。

在攻击的第一阶段，Github的网站遭受了惊人的每秒1.35太比特（Tbps）的高峰，而在第二阶段，Github的网络监控系统检测到了400Gbps的峰值。攻击持续了8分钟以上，并且由于攻击使用了大量流量，这是迄今为止见过的最大的DDoS攻击。

22

快讯 | 入侵监狱网站篡改记录帮朋友提前释放？结果自己也进去了

上周一名密西根人因入侵Washtenaw县监狱被捕，原因竟然是他想修改监狱记录，好让朋友提前释放。这名男子名叫Konrads Voits，27岁，来自密西根Ann Arbor，今年早些时候也曾遭逮捕。社工监狱员工根据法庭文件，自2017年1月24日开始到3月10日，Voits使用邮件钓鱼和电话社工欺骗监狱员工下载运行病毒。Voits以Daniel Greene的名义发送邮件，然后他又注册了域名ewashtenavv.org，这个域名跟ewashtenaw.org很像，后者是Washtenaw县官方门户。不过，钓鱼邮件攻击并没有很顺

发布时间：2017 年 12 月 6 日

ROPEMAKER：利用简单CSS属性就可以篡改已发送的邮件内容

邮件与云安全公司 Mimecast 的安全研究人员 Francisco Ribeiro 最近发现一种名为 ROPEMAKER 的攻击手法。ROPEMAKER 全称叫 Remotely Originated Post-delivery Email Manipulation Attacks Keeping Email Risky。攻击者利用这个攻击方法，可以让一封合法邮件瞬间变身恶意邮件，一般的安全工具还检测不出来。攻击者给受害人发送一封 HTML 格式的邮件，在这封原本合法的邮件发出之后，攻击者还能篡改邮件内容，比如将其中的合法 URL 地址置换成恶意地址。整个过程可躲避垃

发布时间：2017 年 8 月 28 日

“隐魂”木马篡改主页分析：史上反侦察力最强木马的犯罪素描

前不久，360安全中心率先发布了MBR木马——“隐魂”的预警，对木马入侵过程分析《史上反侦察力最强木马“隐魂”：撑起色情播放器百万推广陷阱》后发现，“隐魂”的反侦察能力极高，堪称迄今最复杂的MBR木马。360安全中心随即对该木马展开了持续追踪，本篇是对其篡改主页的行为详细介绍。1 摘要首先，我们来进一步了解“隐魂”木马的反侦察能力和复杂性。（1） 隐蔽性极高：“隐魂”木马会通过挂钩磁盘底层驱动实现自我保护，普通的ARK工具或查杀类工具无法深入磁盘底层，

发布时间：2017 年 8 月 26 日

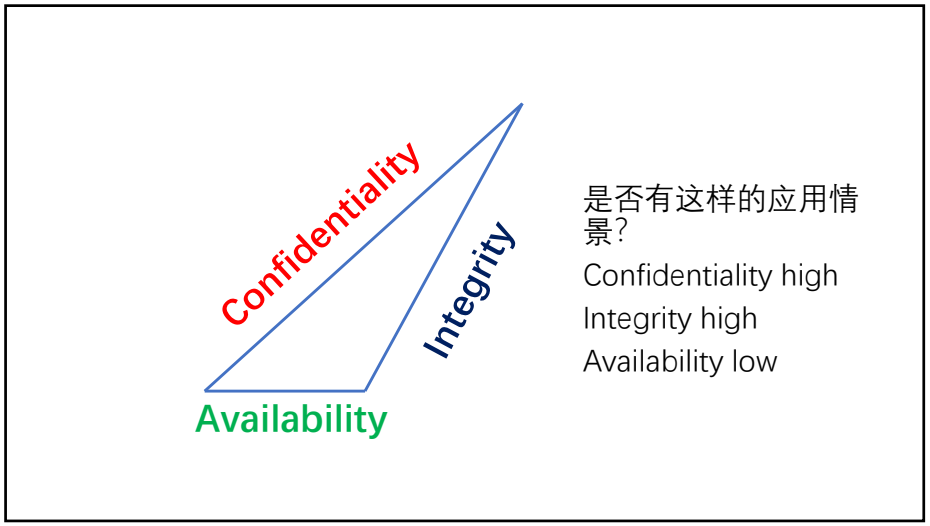
重放攻击无线键盘实验，篡改你的输入信息

23

Which is most important?

- Q: Of confidentiality, integrity, and availability, which is the most important?
- A: It all **depends** on the context(上下文).
  - For a national defense system protecting the national war plan, confidentiality may be paramount.
  - For a bank protecting financial data, integrity may count most.
  - For an online retailer, availability may be a matter of survival.

24



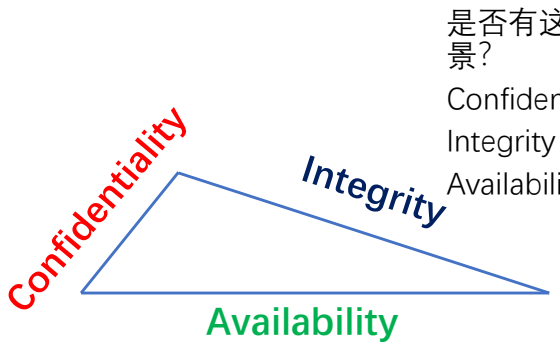
是否有这样的应用情景?

Confidentiality high

Integrity high

Availability low

25



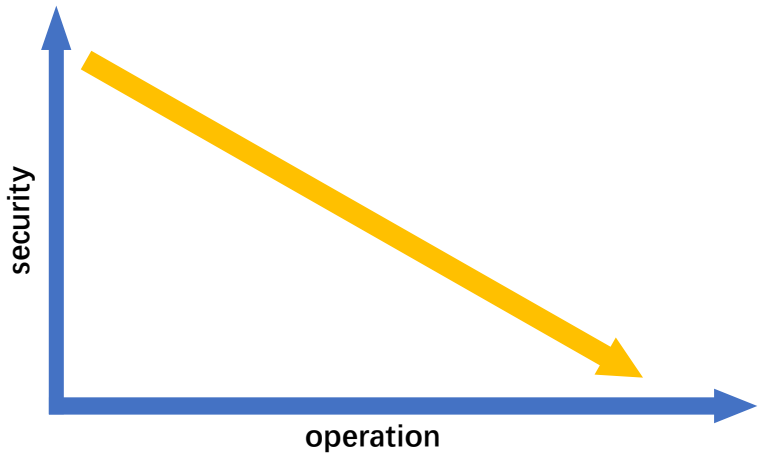
是否有这样的应用情景?

Confidentiality low

Integrity high

Availability high

26



27

White hat principles

- Black list, white list 黑名单、白名单
- Least privilege principle 最小权限原则
- Defense in depth 纵深防御原则
- Data and code separation 数据与代码相分离原则
- Unpredictability 不可预测性原则

Web security a white hat perspective

28

Black list, white list 黑名单、白名单

- Network access control policy
- Exercise:
- Do not allow SSH (secure shell) port open to the Internet.

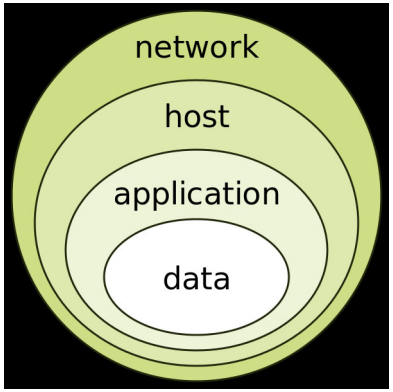
29

Least privilege principle 最小权限原则

- -rwxrw-r-- (this user, the user's group, other users)
- Chmod +x chmod 755
- drwxr-xr-x 2 root root 4096 Sep 7 09:16 Templates
- -rwxr-xr-x 1 root root 8119757 Feb 13 03:35 VBoxLinuxAdditions.run

30

Defense in depth 纵深防御原则



31

Data and code separation 数据与代码相分离原则

```
<html>
<head>test</head>
<body>
$var
</body>
</html>
```

```
<html>
<head>test</head>
<body>
<script>
alert("$var1");
</script>
</body>
</html>
```

32

Unpredictability 不可预测性原则

- ASLR（Address space layout randomization）
- ISN (Initial sequence number)