Information Security and Our Society

1.5nd: Course Description
September 31, 2015

Jun Murai, Keio University
Masaaki Sato, Keio University
Suguru Yamaguchi, Nara Institute of Science and Technology

- This class is 11:05~12:35.

Purpose of attackers

- Money
- Principle
- Intelligence
- Etc.

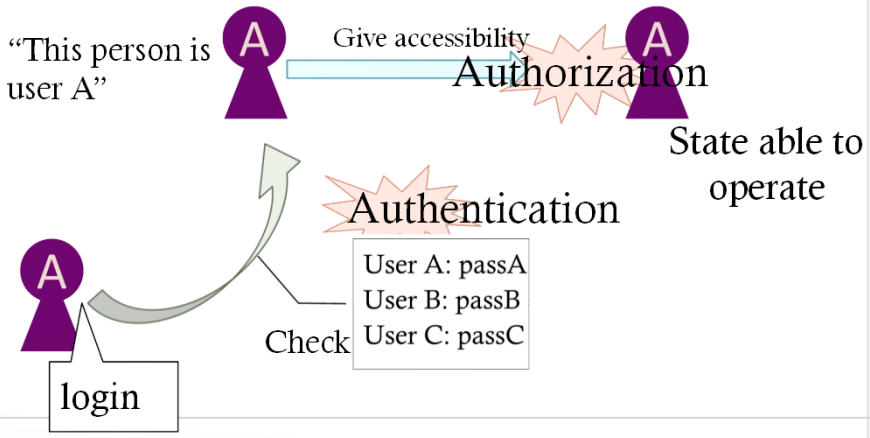
https://ja.wikipedia.org/wiki/%E3%82%A2%E3%83%8E%E3%83%8B%E3%83%9E%E3%82%B9_(%E9%9B%86%E5%9B%A3)
https://upload.wikimedia.org/wikipedia/en/2/24/GoldenEye_-_UK_cinema_poster.jpg

Security basics

- **Privilege management**
  - Authentication, authorization
- **Password management**
  - Hash
- **Encrypt communication**
  - Public key cryptosystem
  - Electronic signature

Authorization and Authentication

"Login" looks a step for users, actually consists from two steps, authentication and authorization



Hash

- **What's Hash ?**
  - Pseudo random number of a fixed length which gives the characteristic of a given data

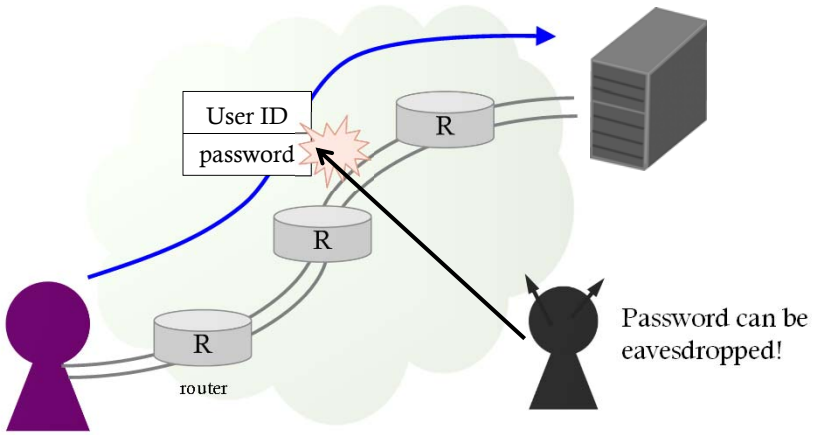
Hash (passA) = hashed_passA

UserA hashed_passA	UserA passA
UserB hashed_passB	UserB passB
UserC hashed_passC	UserC passC

To authenticate, compare hashed input password with stored hashed password

Storing plaintext produce vulnerability →store hashed data

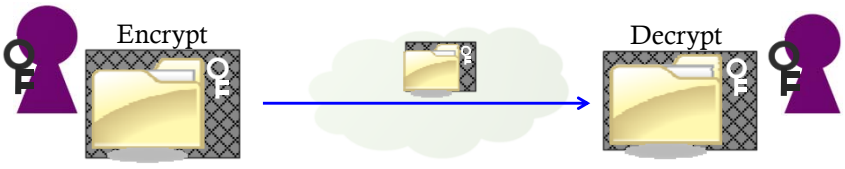
Problem of password

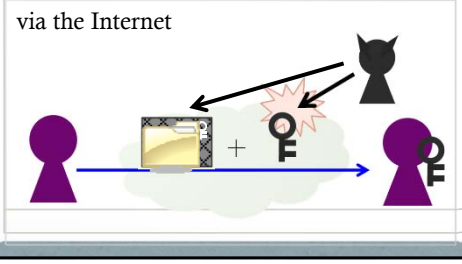


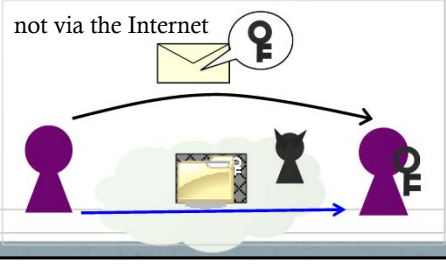
Key distribution problem

- **How can we share the key for encryption?**

  If we share secret keys via the Internet, they may be eavesdropped.



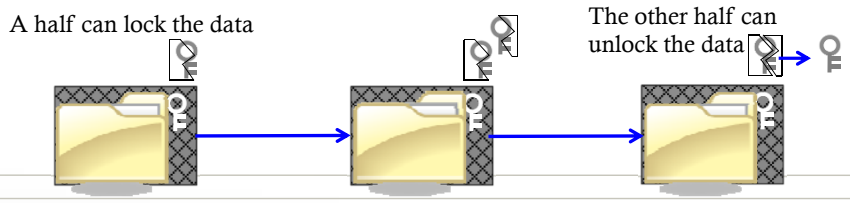




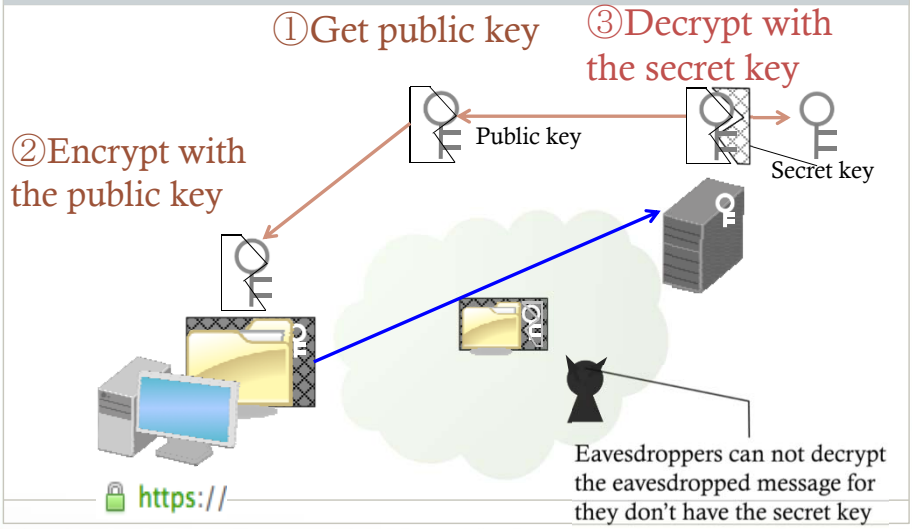
Public key cryptosystem

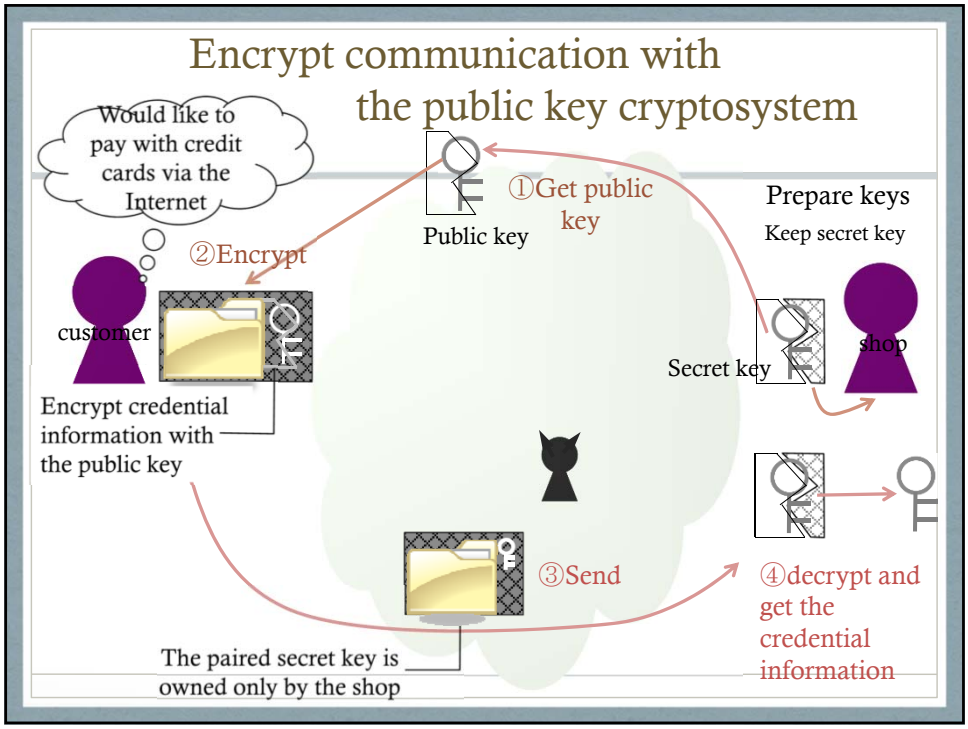
- **What's public key cryptosystem ?**
- By using different keys to encrypt and decrypt, the encrypt key can be disclosed.
- "Public key" to encrypt, "Secret key" to decrypt
- Encrypted messages which are encrypted with a public key can be decrypted only by the secret key paired with the public key

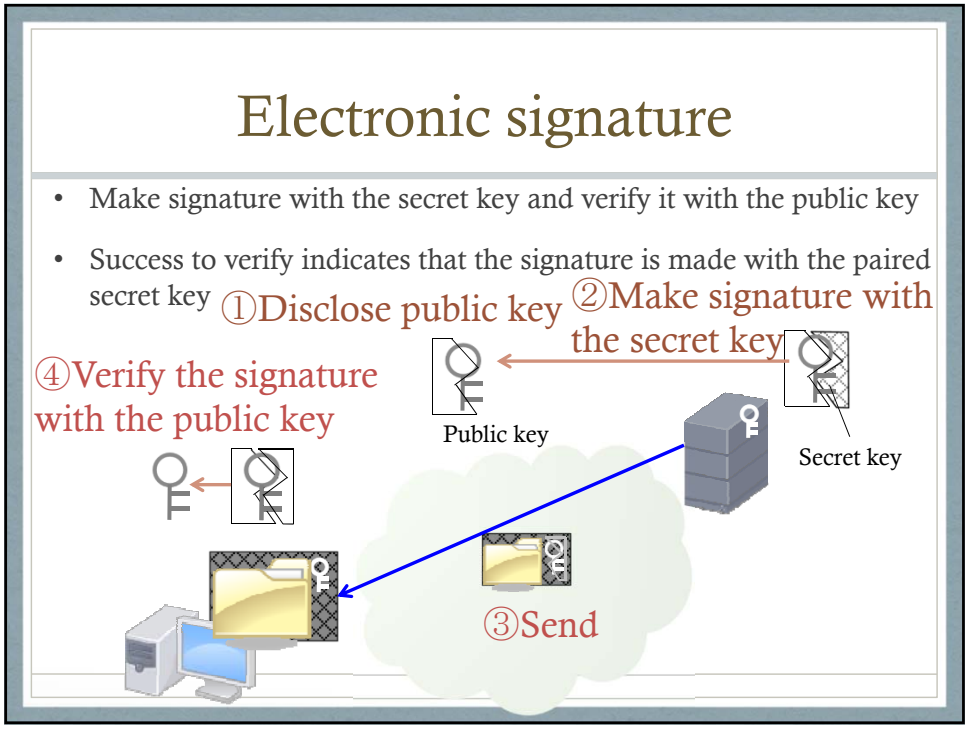
Public key cryptosystem is like 「割り符」 traditionally used in Japan



Encrypt communication with the public key cryptosystem




Encrypt communication with the public key cryptosystem
Would like to pay with credit cards via the Internet
①Get public key
Public key
Prepare keys
Keep secret key
②Encrypt
customer
Secret key
shop
Encrypt credential information with the public key
③Send
④decrypt and get the credential information
The paired secret key is owned only by the shop


Electronic signature
• Make signature with the secret key and verify it with the public key
• Success to verify indicates that the signature is made with the paired secret key
①Disclose public key
②Make signature with the secret key
④Verify the signature with the public key
Public key
Secret key
③Send

Categories of attacks

- **Brute Force** – Trial and error method to obtain personal information
- **Denial of Service** – Attack on network by flooding the system with useless traffic
- **Bug of programs** – Bugs in code are vulnerability
- **Malware** – Malicious software such as virus and worm
- **Cheating user** – Attacks/Scams towards users such as phishing and targeted attack
- **Insecure configuration** – Unsuitable settings are causes of security holes/issues
- Etc.

Brute Force Attack

- To try possible passwords as many as possible
- From small number, from large number, along dictionaries, along some algorithms, etc.

Brute Force Attack

ID	Password
123456789	000000
123456789	000001
123456789	000002
123456789	000003
123456789	000004

Reverse Brute Force Attack

ID	Password
123456781	000000
123456782	000000
123456783	000000
123456784	000000
123456785	000000

Dictionary Attack

ID	Password
123456789	199457
123456789	940507
123456789	751994
123456789	070594
123456789	050794

Issue instance: Unauthorized access to Japan Air Line

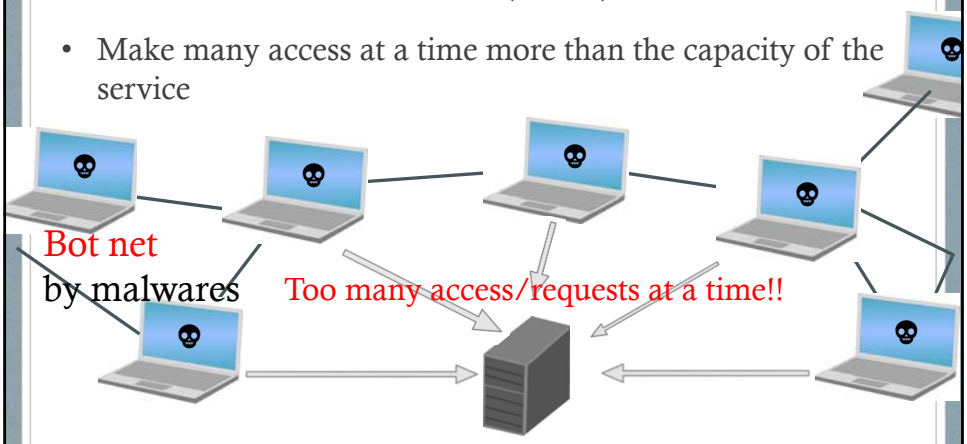
- A hacker used Brute Force Attack to JMB
- The password was fixed to 6 numbers
- 40 users' virtual coin was exchanged to vouchers by the hacker

http://blog.tokumaru.org/2014/02/jal.html
http://www.aviationwire.jp/archives/31928

How can we protect against Brute Force attack?

Denial of Service attack

- Distributed Denial of Service (DDoS) attack
- Make many access at a time more than the capacity of the service



Issue instance: Network services of Sony and Microsoft for game are down

- PlayStation Network and XBox Live are down by DDoS.
- A hacker group claimed responsibility for taking down PlayStation Network on Twitter.

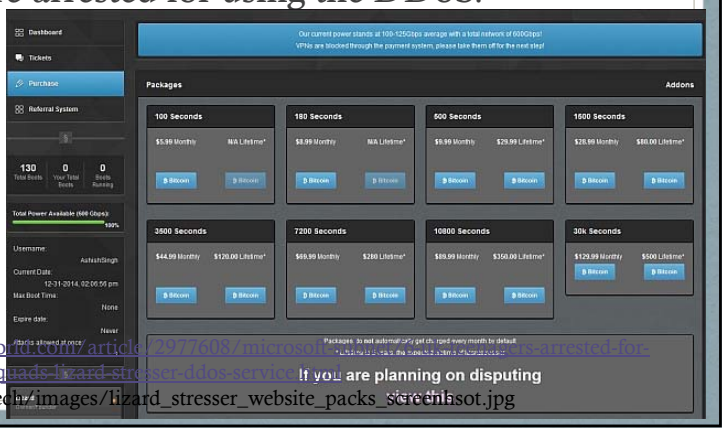
PlayStation Network

XBOX

http://www.businessinsider.com/playstation-network-and-xbox-live-are-down-and-the-notorious-hacker-gang-lizard-squad-is-taking-credit-2014-12

Issue Instance: Network services of Sony and Microsoft for game are down

- The hacker group started to sell DDoS.
- 6 teens are arrested for using the DDoS.
- A kind of black market



http://www.networkworld.com/article/2977608/microsoft-subnet/6-teens-arrested-for-allegedly-using-lizard-squads-lizard-stresser-ddos-service.html

http://cdn.ndtv.com/tech/images/lizard_stresser_website_packs_screenshot.jpg

How can we protect against DDoS?

Bug of programs

- Programs may contain bugs which is the vulnerability that attackers can abuse
- Buffer over flow, Directory traversal, OS command injection, SQL injection, Insecure privilege, etc.

http://krebsonsecurity.com/wp-content/uploads/2010/11/bugs.jpg

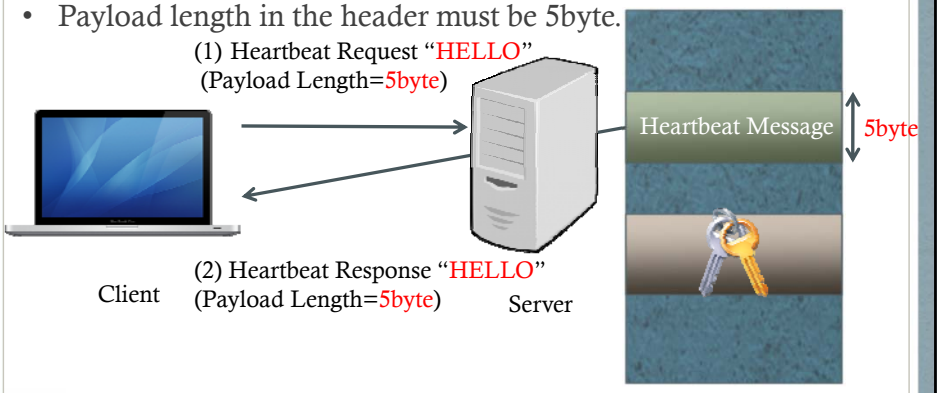
Issue Instance: Heartbleed

- A serious security bug in the widely used OpenSSL., found in Apr, 2014.
- Attacker can get secret-key, password, cookie contained in the targeted system's memory by sending modified Heartbeat message.

http://unseennow.com/blog/protect-heartbleed-bug/

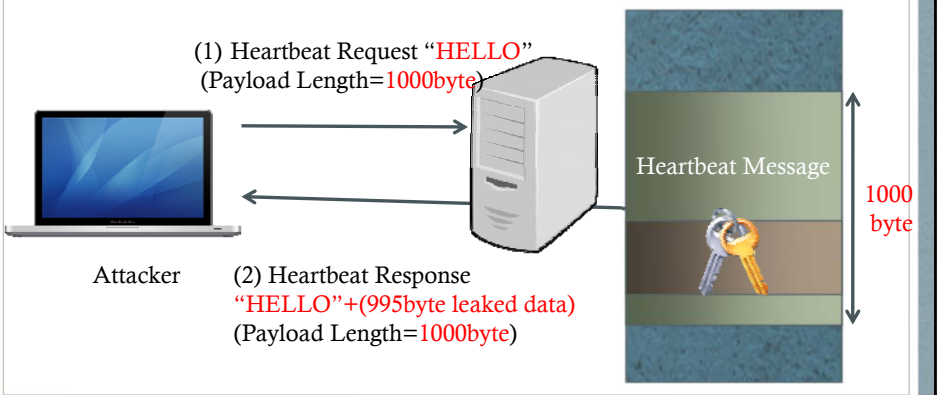
Attack Sequence: Heartbleed

- Normal Heartbeat packet consists of header and 5byte payload "HELLO".
- Payload length in the header must be 5byte.



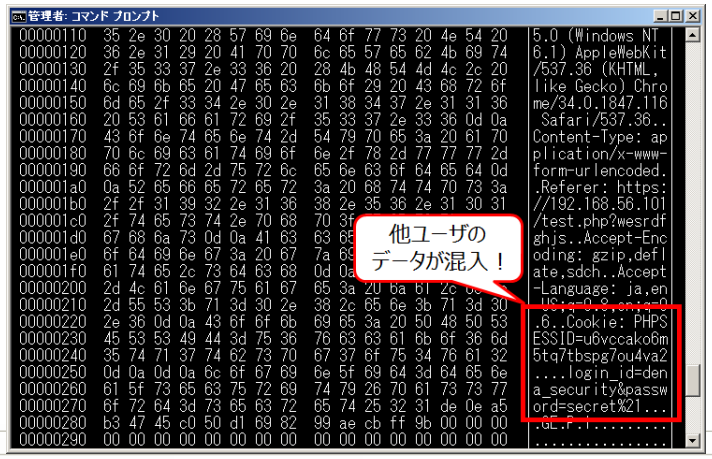
Attack Sequence: Heartbleed

Attacker can get memory containing secret data by controlling payload length field.



Issue Instance: Heartbleed

- Trying to get other's secret data(Session ID).



http://developers.mobage.jp/blog/2014/4/15/heartbleed

Issue Instance: Heartbleed

- Mitsubishi UFJ Nicos announced 894 personal information leaked out.
- Canada Revenue Agency announced about 900 Social Security Number(SSN) leaked out.

http://www.security-next.com/048185

http://internet.watch.impress.co.jp/docs/news/20140415_644351.html

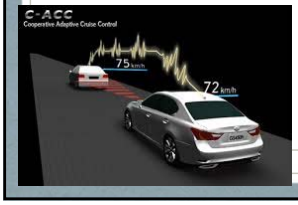
Issue Instance: Shellshock

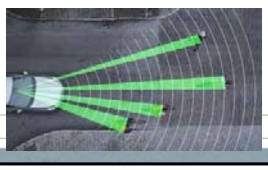
- Shellshock is a security vulnerability in the widely used GNU Bash (CVE-2014-6271).
- Any commands may be executed as a root (Administrator) remotely and quickly.
- So many server and embedded system are vulnerable.

http://d.hatena.ne.jp/Kango/20140928/1411939683

Autonomous/Automated Driving

- ACC(Adaptive Cruse Control), CACC(Cooperative ACC)
  - Vehicle following / radar cruise control
  - Platooning vehicle
- Auto-Parking
  - Smartphone control
- Great benefit, but there is a risk

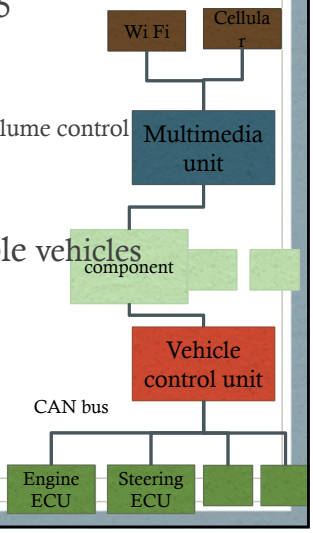




Remote control

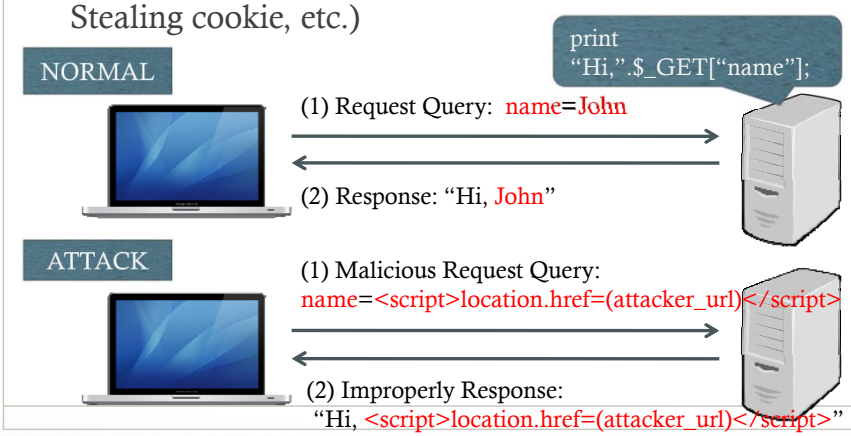
- GM Jeep Cherokee @ Black Hat USA 2015
  - Remote access/control via WiFi
  - Remote access/control via Sprint network
    - Vehicle Position Tracking, Radio station tuning / Volume control
  - Rewrite the control unit setting
    - Control everything via CAN bus
- Chrysler is recalling 1.4 million hack-able vehicles

Source: https://twitter.com/CNNMoney/status/624745649267806210/photo/1?ref_src=twsrc%5Etfw



XSS(Cross Site Scripting) Attack

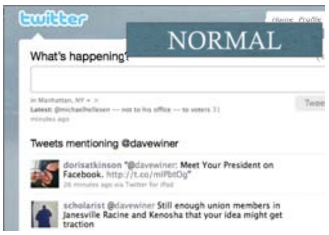
- Client-side code injection attack. Attacker can execute malicious scripts (e.g. Redirecting to malicious website, Stealing cookie, etc.)



http://tezawaly.jp/archives/2010/09/twitter_hack_patched/

XSS attacking to Twitter

- Japanese security researcher has found large-scale XSS vulnerability on Sep, 2010.
- Many twitter-users were trying to attack by writing JavaScript.



This is one of XSS attacking to Twitter. If you hover a tweet containing exploit code, It seems that Twitter is broken.

How can we deal with bugs?

Malware

Malware (generic name)

- Spyware
- Ransomware
- Adware
- Scareware

- Virus
  - Infect files and software.
  - When the infected is operated, unintended evil work is operated.

- Worm
  - Evil program
  - Stand alone, without parasitizing other programs.

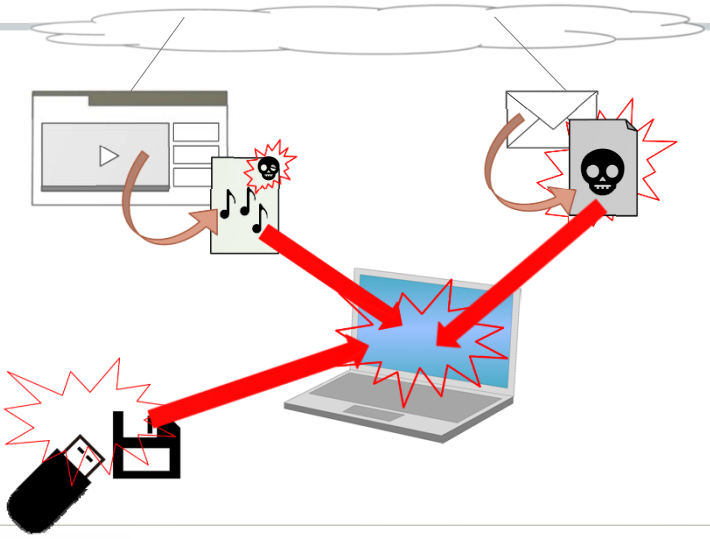
…etc

Issue instance: Stuxnet

- A malicious computer virus targeting nuclear power plants, found in June 2010
- 100 thousands computers were infected
- Broke 1,000 of 9,000 centrifuges, with faking displaying system working status
- Has multiple complex entry route
- Knowledge
  - Control system may be attacked
  - Closed system can be attacked
  - Special system can be attacked by crackers outside
  - Infected computer may seem to work properly

http://www.nisc.go.jp/inquiry/pdf/so_honbun.pdf
http://www.nids.go.jp/publication/commentary/pdf/commentary020.pdf

Routes of malware entry



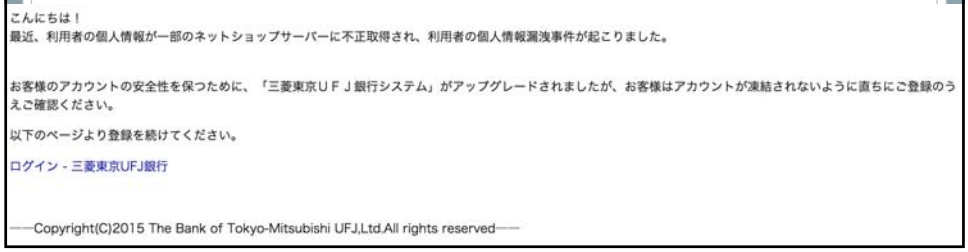
How can we protect against Malwares?

Cheating users

- Cheating on users so that malicious programs get run or information get leaked.
- Phishing, Targeted attack, etc.

Issue instance: Phishing by replicating the Bank of Tokyo-Mitsubishi UFJ

- Scam to obtain confidential information from users, typically by sending an e-mail containing a link to a replicated fake website.
- A Phishing e-mail usually pretends as a legitimate organization.


こんにちは！
最近、利用者の個人情報が一部のネットショップサーバーに不正取得され、利用者の個人情報漏洩事件が起こりました。

お客様のアカウントの安全性を保つために、「三菱東京ＵＦＪ銀行システム」がアップグレードされましたが、お客様はアカウントが凍結されないように直ちにご登録のうえご確認ください。

以下のページより登録を続けてください。

ログイン - 三菱東京UFJ銀行

----Copyright(C)2015 The Bank of Tokyo-Mitsubishi UFJ,Ltd.All rights reserved----

Phishing website

Phishing website

Actual website
(The bank of Tokyo-Mitsubishi UFJ)

Targeted attack

- Emails specialized (targeted) to someone, which look normal emails.
- Ex)

```
Dear students,

This is the TA of the security class by Jun Murai.
The attached file is the slides of the last class.
Check the group and the date of the midterm presentation.

--Shota
```

- Of course, the attached file, URL etc. are malicious.

Issue instance: Japan Pension Service infected by a Virus (Emdivi)

- Employees in JPS opened an attached file in an e-mail containing a virus of targeted attack.
- JPS realized the attack after 15 days and at least 27 computers got hacked
- As a result, about 1.25 million cases of personal data has been leaked

http://itpro.nikkeibp.co.jp/atcl/news/15/061602005/?ST=security&P=2
http://internet.watch.impress.co.jp/docs/news/20150608_705826.html
http://www.japantimes.co.jp/news/2015/06/01/national/crime-legal/japan-pension-system-hacked-1-25-million-cases-personal-data-leaked/

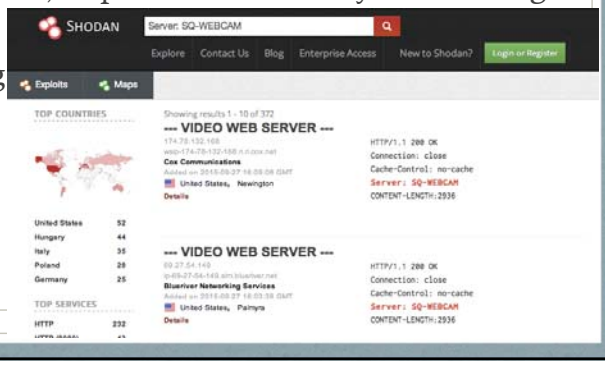
How can we protect against such cheating?

Insecure configuration

- Unsuitable configuration causes security issues.
- Ex) configuration not using any password
- Ex) putting files involving privacy in “public_html” in the servers of SFC-CNS by mistake causes leaking your privacy

Shodan(shodan.io)

- Shodan is a search engine for Internet connected devices.
- Cameras, sensors and so on connected to the Internet are accessed and disclosed involuntarily
- As IoT device increases, Importance of security is increasing day by day.
- Leak, eavesdropping



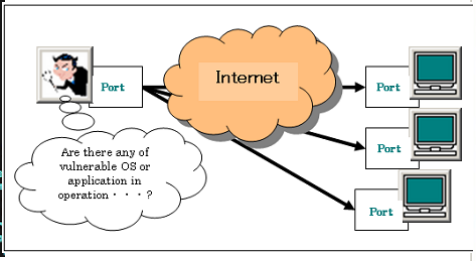
Searching Webcam →

How can we avoid insecure configuration?

Penetration route

- Brute-force attack
- Dictionary Attack
- Port scanning
- Exploit code (Privilege escalation by malicious payload)

```
void build_tif(Node &sp, Node &pc) {
  char tif[] = {
    0x49,0x49,        // header
    0x2a,0x00,        // version
    0x1e,0x00,0x00,0x00,    // IFD location
    0x00,0x00,0x00,0x00,    // padding to IFD
    0x00,0x00,0x00,0x00,
    0x00,0x00,0x00,0x00,
    0x00,0x00,0x00,0x00,
    0x00,0x00,0x00,0x00,0x00,0x00,
    0x08,0x00,        // 8 tags in the image
    0x00,0x01,0x03,0x00,0x01,0x00,0x00,0x00,0x08,0x00,0x00,0x00,    // image
    0x01,0x01,0x03,0x00,0x01,0x00,0x00,0x00,0x08,0x00,0x00,0x00,    // image
    0x03,0x01,0x03,0x00,0x01,0x00,0x00,0x00,0xaa,0x00,0x00,0x00,    // sample
    0x06,0x01,0x03,0x00,0x01,0x00,0x00,0x00,0xbb,0x00,0x00,0x00,    // photom
    0x11,0x01,0x04,0x00,0x01,0x00,0x00,0x00,0x08,0x00,0x00,0x00,    // strip
    0x17,0x01,0x04,0x00,0x01,0x00,0x00,0x00,0x15,0x00,0x00,0x00,    // strip
    0x1c,0x01,0x03,0x00,0x01,0x00,0x00,0x00,0x01,0x00,0x00,0x00,    // planar
    0x50,0x01,0x03,0x00,0xff,0x00,0x00,0x00,0x84,0x00,0x00,0x00,    // dot ra
    0x00,0x00,0x00,0x00,                    // padding to dot range data
```



iPhone Jailbreaking (TIFF image exploit)

Port scanning

http://www.toc2rta.com/?q=node/30

https://www.ipa.go.jp/security/english/virus/press/200501/images/Portscan.png