All rights are reserved by Li Jingtao, and content may not be reproduced, downloaded, disseminated, published, or transferred in any form or by any means, except with the prior written permission of Li Jingtao.

Information Security 08

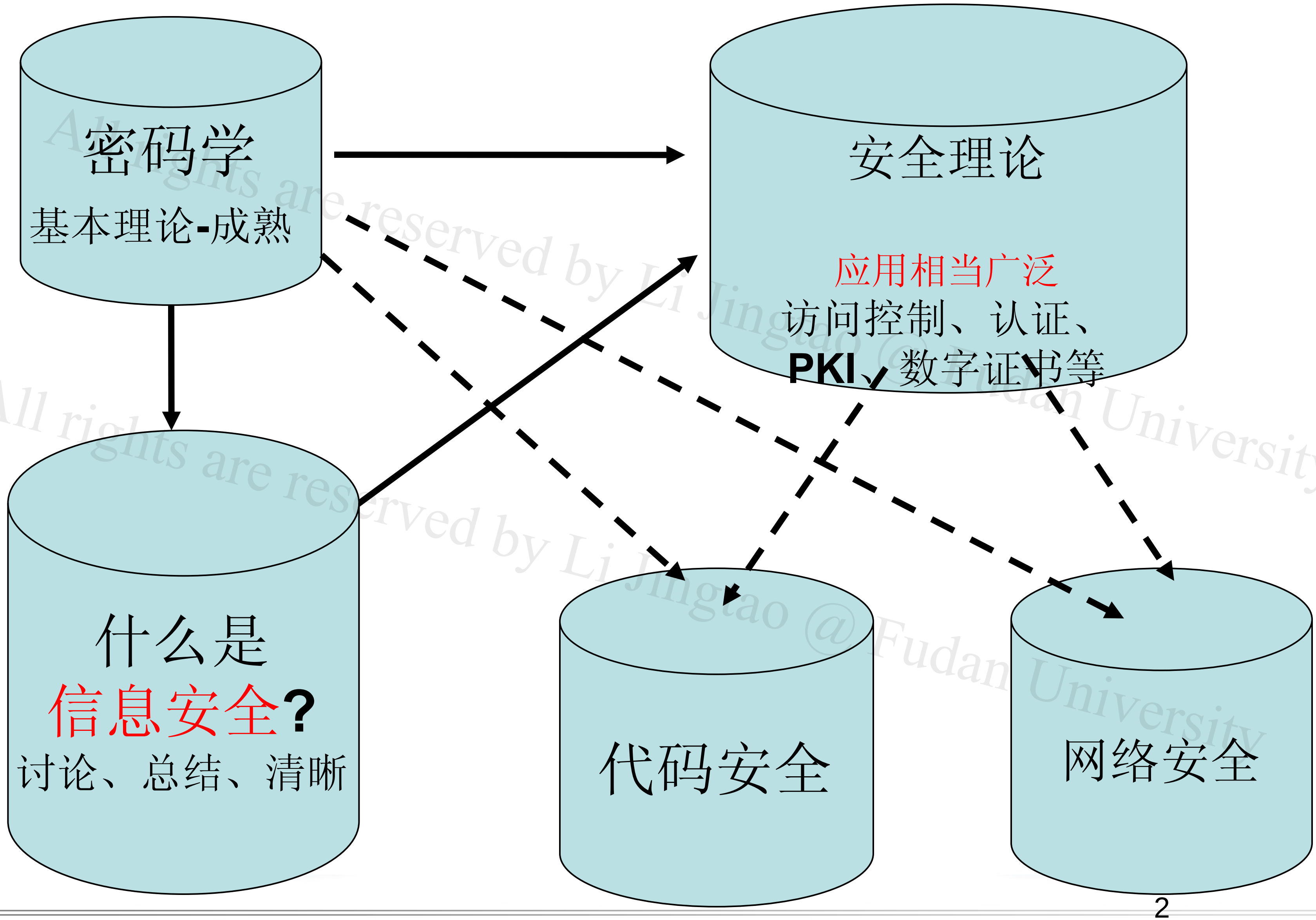
Authentication

All rights are reserved by Li Jingtao @ Fudan University

All rights are reserved by Li Jingtao @ Fudan University

All rights are reserved by Li Jingtao, and content may not be reproduced, downloaded, disseminated, published, or transferred in any form or by any means, except with the prior written permission of Li Jingtao.

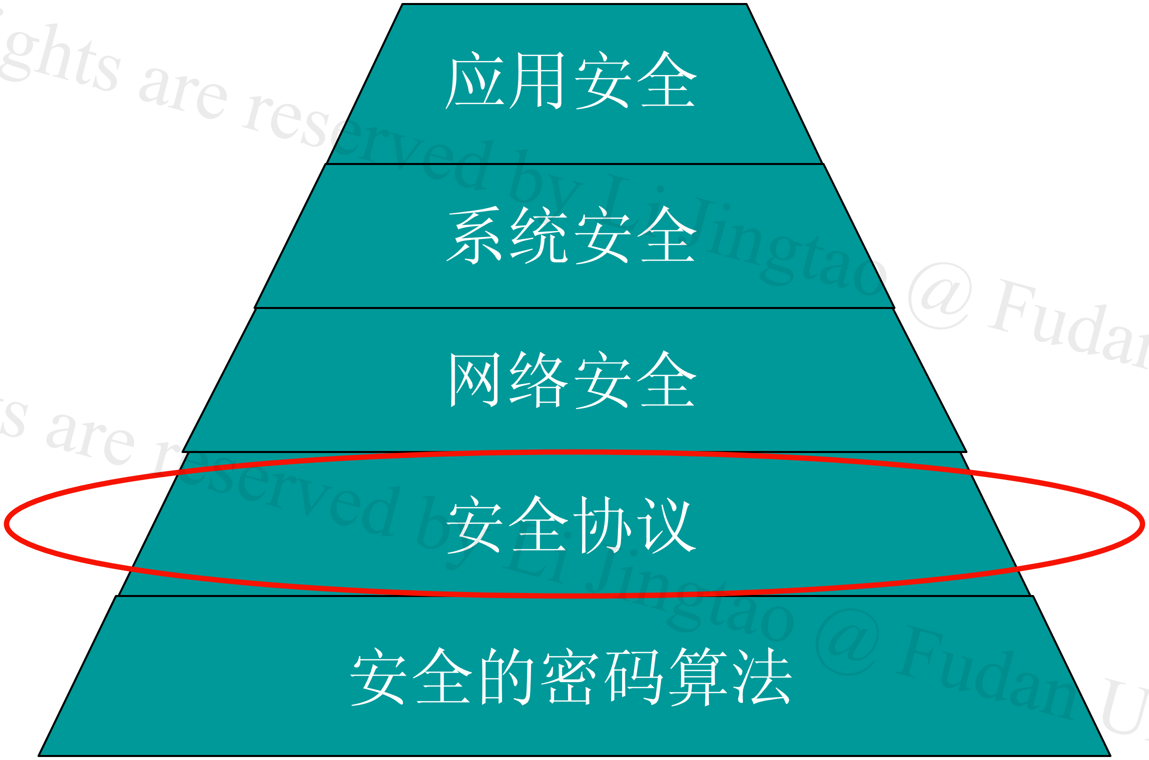
内容间的联系



All rights are reserved by Li Jingtao @ Fudan University

All rights are reserved by Li Jingtao, and content may not be reproduced, downloaded, disseminated, published, or transferred in any form or by any means, except with the prior written permission of Li Jingtao.

Review: 安全层次



All rights are reserved by Li Jingtao @ Fudan University

All rights are reserved by Li Jingtao @ Fudan University

All rights are reserved by Li Jingtao, and content may not be reproduced, downloaded, disseminated, published, or transferred in any form or by any means, except with the prior written permission of Li Jingtao.

Outline of Talk

- Definitions
- Passwords
  - Unix Passwords
  - One time passwords
- Challenge-response techniques

All rights are reserved by Li Jingtao @ Fudan University
All rights are reserved by Li Jingtao @ Fudan University

All rights are reserved by Li Jingtao, and content may not be reproduced, downloaded, disseminated, published, or transferred in any form or by any means, except with the prior written permission of Li Jingtao.

Definitions

Authentication:

- A *claimant* tries to show a *verifier* that the claimant is as declared
  - identification

- Different from *message authentication*
  - which enables the recipient to verify that messages have not been tampered with in transit (data integrity) and that they originate from the expected sender (authenticity).

All rights are reserved by Li Jingtao @ Fudan University

All rights are reserved by Li Jingtao, and content may not be reproduced, downloaded, disseminated, published, or transferred in any form or by any means, except with the prior written permission of Li Jingtao.

Definitions

Authentication

- 消息认证/报文的鉴别
- 身份认证
  - Message authentication has no *timeliness*
  - Entity authentication happens in *real time*
- 双向和单向认证

All rights are reserved by Li Jingtao @ Fudan University
All rights are reserved by Li Jingtao @ Fudan University

All rights are reserved by Li Jingtao, and content may not be reproduced, downloaded, disseminated, published, or transferred in any form or by any means, except with the prior written permission of Li Jingtao.

A good authentication scheme is…

- ***Sound:*** an honest party can successfully authenticate him/herself
- ***Non-transferable***
- ***No impersonation***
- All this is true even when
  - A large number of authentications are observed
  - Eve is able to spoof/eavesdrop
  - Multiple instances are run simultaneously

All rights are reserved by Li Jingtao @ Fudan University

All rights are reserved by Li Jingtao @ Fudan University

All rights are reserved by Li Jingtao, and content may not be reproduced, downloaded, disseminated, published, or transferred in any form or by any means, except with the prior written permission of Li Jingtao.

Basis of Authentication

- Something *known* - passwords, PINs, keys…
- Something *possessed* - cards, handhelds…
- Something *inherent* - biometrics

All rights are reserved by Li Jingtao @ Fudan University

All rights are reserved by Li Jingtao @ Fudan University

All rights are reserved by Li Jingtao, and content may not be reproduced, downloaded, disseminated, published, or transferred in any form or by any means, except with the prior written permission of Li Jingtao.

PINs and keys

- Long key on physical device (card), short PIN to remember
- PIN unlocks long key
- Need possession of both card and PIN
- Provides ***two-level*** security

All rights are reserved by Li Jingtao @ Fudan University
All rights are reserved by Li Jingtao @ Fudan University

All rights are reserved by Li Jingtao, and content may not be reproduced, downloaded, disseminated, published, or transferred in any form or by any means, except with the prior written permission of Li Jingtao.

Outline of Talk

- Definitions
- Passwords
  - Unix Passwords
  - One time passwords
- Challenge-response techniques

All rights are reserved by Li Jingtao @ Fudan University

All rights are reserved by Li Jingtao @ Fudan University

All rights are reserved by Li Jingtao, and content may not be reproduced, downloaded, disseminated, published, or transferred in any form or by any means, except with the prior written permission of Li Jingtao.

Basic password authentication

- Setup
  - – User chooses password
  - – Hash of password stored in password file
- Authentication
  - – User logs into system, supplies password
  - – System computes hash, compares to file

All rights are reserved by Li Jingtao @ Fudan University
All rights are reserved by Li Jingtao @ Fudan University

All rights are reserved by Li Jingtao, and content may not be reproduced, downloaded, disseminated, published, or transferred in any form or by any means, except with the prior written permission of Li Jingtao.

Passwords -weak authentication

- Usually fixed
- Stored either in the clear, or “encrypted” with a OWF
- *Rules* reduce the chance of easy passwords
- *Salt* increases search space for a dictionary attack

- There are many examples using password-based authentication
  - – how to manage passwords

All rights are reserved by Li Jingtao @ Fudan University

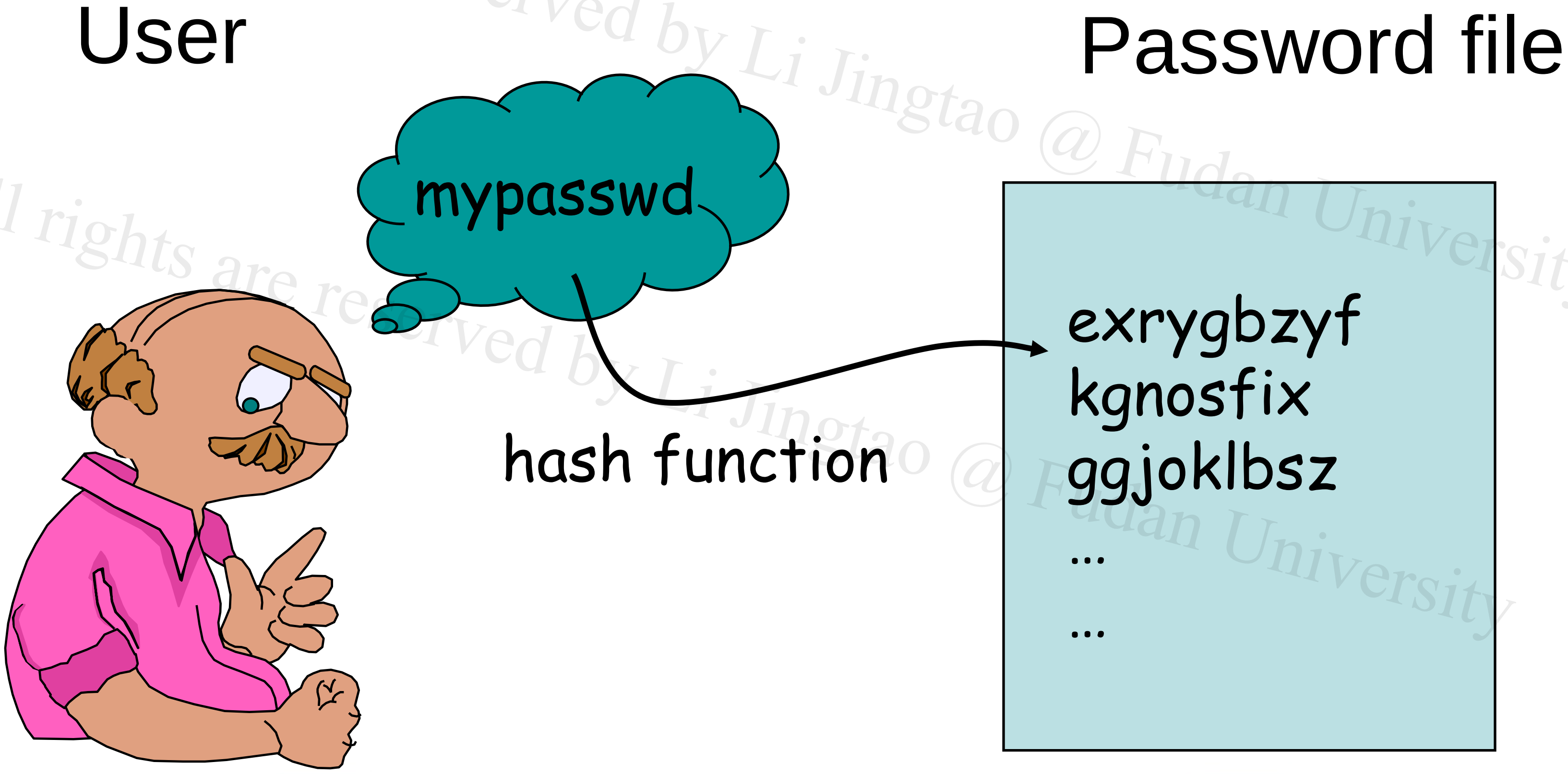
All rights are reserved by Li Jingtao @ Fudan University

All rights are reserved by Li Jingtao, and content may not be reproduced, downloaded, disseminated, published, or transferred in any form or by any means, except with the prior written permission of Li Jingtao.

Example: UNIX passwords

/etc/passwd
/etc/shadow

Username: password: UID : GID: USERINFO: HOME: SHELL



All rights are reserved by Li Jingtao @ Fudan University
All rights are reserved by Li Jingtao @ Fudan University

All rights are reserved by Li Jingtao, and content may not be reproduced, downloaded, disseminated, published, or transferred in any form or by any means, except with the prior written permission of Li Jingtao.

Attacks on password schemes

- ***Replay*** of fixed passwords
- Exhaustive ***search***
  - – 8 character password has 40-50 bits
- More directed ***dictionary*** *attacks*
  - – Crack - widely available tool for doing this
  - – Online dictionary attack
    - Guess passwords and try to log in
  - – Offline dictionary attack
    - Steal password file, try to find p with hash(p) in file

All rights are reserved by Li Jingtao @ Fudan University

All rights are reserved by Li Jingtao, and content may not be reproduced, downloaded, disseminated, published, or transferred in any form or by any means, except with the prior written permission of Li Jingtao.

Dictionary Attack – some numbers

- Typical password dictionary
  - 1,000,000 entries of common passwords
    - people's names, common pet names, and ordinary words.
  - Suppose you generate and analyze 10 guesses per second
    - This may be reasonable for a web site; offline is *much* faster
  - Dictionary attack in at most 100,000 seconds = 28 hours, or 14 hours on average
- If passwords were random
  - Assume six-character password
    - Upper- and lowercase letters, digits, 32 punctuation characters
    - 689,869,781,056 password combinations.
    - Exhaustive search requires 1,093 years on average

All rights are reserved by Li Jingtao @ Fudan University

All rights are reserved by Li Jingtao, and content may not be reproduced, downloaded, disseminated, published, or transferred in any form or by any means, except with the prior written permission of Li Jingtao.

UNIX passwords

- User password serves as key to encrypt known plaintext (64 bit zeroes)
- Encryption - modification of DES, iterated 25 times
- 12 bit salt added - total 64 + 12 = 76 bits
  - Salt taken from system clock, [a-zA-Z0-9./]
  - Alters expansion function of DES
  - char *crypt(const char *key, const char *salt);

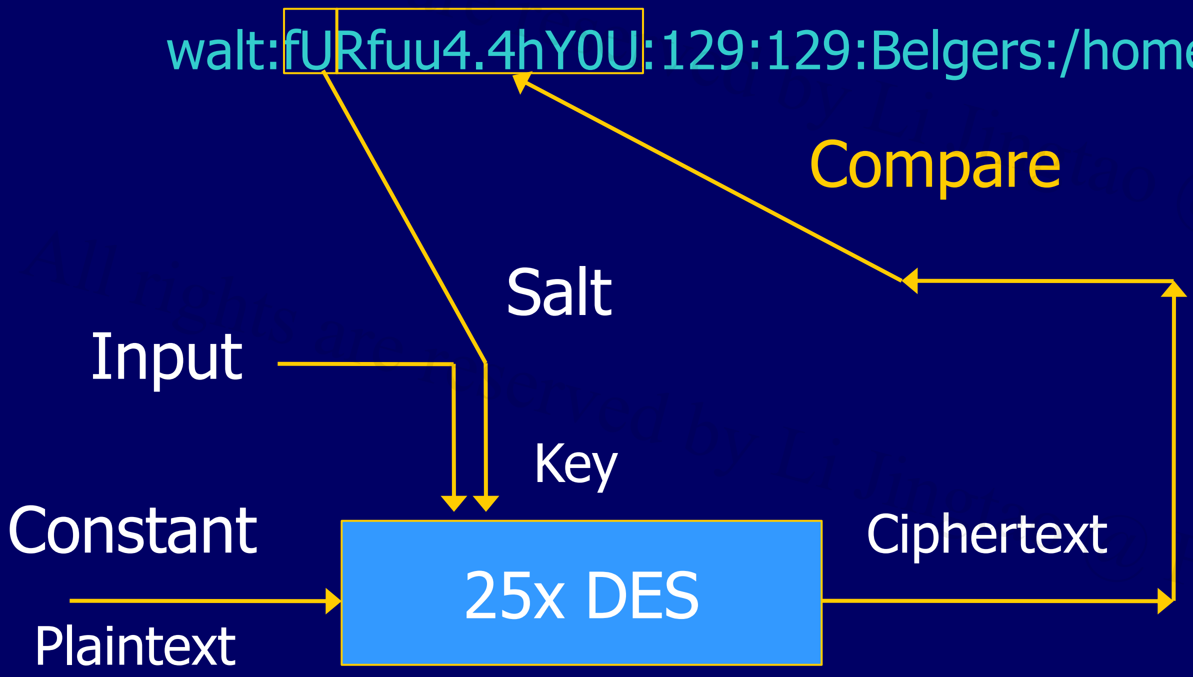
All rights are reserved by Li Jingtao @ Fudan University

All rights are reserved by Li Jingtao @ Fudan University

All rights are reserved by Li Jingjiao, and content may not be reproduced, downloaded, disseminated, published, or transferred in any form or by any means, except with the prior written permission of Li Jingjiao.

Salt(使用加密技术生成的随机数)

- Unix password line


walt:fURfuu4.4hY0U:129:129:Belgers:/home/walt:/bin/csh

When password is set, salt is chosen randomly

All rights are reserved by Li Jingtao, and content may not be reproduced, downloaded, disseminated, published, or transferred in any form or by any means, except with the prior written permission of Li Jingtao.

Advantages of salt

- Without salt
  - – Same hash functions on all machines
    - Compute hash of all common strings once
    - Compare hash file with all known password files
- With salt
  - – One password hashed 2^{12} different ways
    - Precompute hash file?
      - – Need much larger file to cover all common strings
    - Dictionary attack on known password file
      - – For each salt found in file, try all common strings
- Now, SHA1 is recommended

All rights are reserved by Li Jingtao @ Fudan University

All rights are reserved by Li Jingtao @ Fudan University

All rights are reserved by Li Jingtao, and content may not be reproduced, downloaded, disseminated, published, or transferred in any form or by any means, except with the prior written permission of Li Jingtao.

Summary: Passwords

  - Easy to implement
  - Easy to use
- But, The Weakest form of Authentication
  - ???
  - 窃取A的password，将在很长一段时间拥有A的权限，直到A发现
  - 特别的，网络环境下远程认证
    - 远程登录Unix主机，password传递形式？

All rights are reserved by Li Jingtao @ Fudan University

All rights are reserved by Li Jingtao @ Fudan University

All rights are reserved by Li Jingtao, and content may not be reproduced, downloaded, disseminated, published, or transferred in any form or by any means, except with the prior written permission of Li Jingtao.

基于口令的认证+明文传输！！！

- Telnet远程登录
  - 逐个字母发送，明文方式
- POP3邮件登录
- Ftp服务
- ……

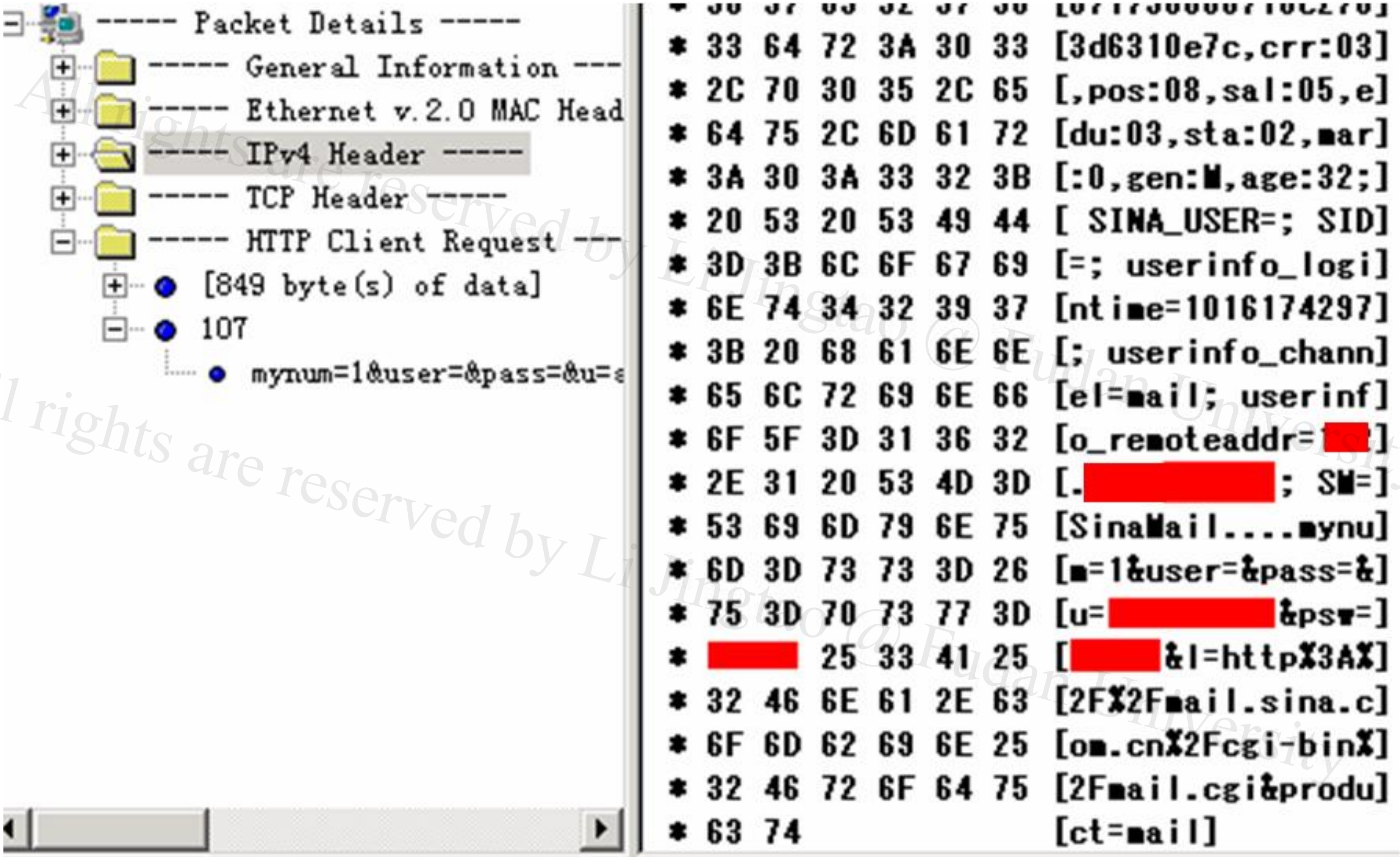
- 嗅探（Sniffer）相当容易

All rights are reserved by Li Jingtao @ Fudan University

All rights are reserved by Li Jingtao @ Fudan University

All rights are reserved by Li Jingtao, and content may not be reproduced, downloaded, disseminated, published, or transferred in any form or by any means, except with the prior written permission of Li Jingtao.

认证例子：sina的邮件登录



```
----- Packet Details -----
  ----- General Information ---
  ----- Ethernet v.2.0 MAC Head
  ----- IPv4 Header -----
  ----- TCP Header -----
  ----- HTTP Client Request ---
      [849 byte(s) of data]
      107
        mynum=1&user=&pass=&u=s
```

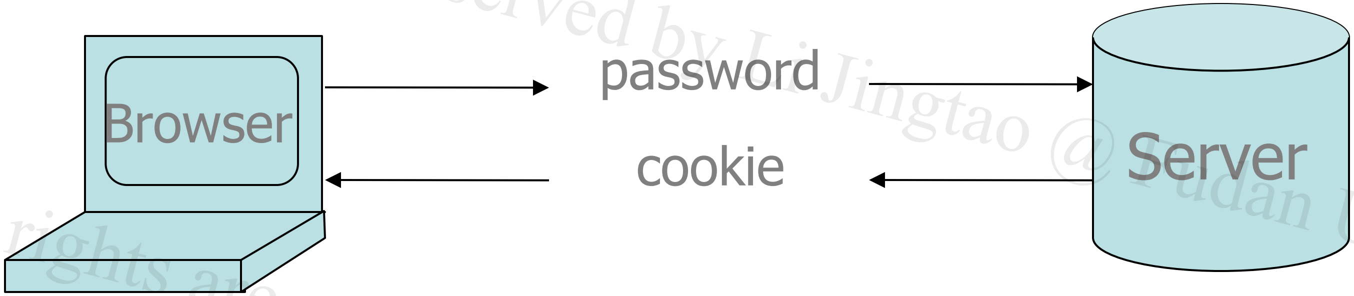
```
* 33 64 72 3A 30 33 [3d6310e7c,crr:03]
* 2C 70 30 35 2C 65 [,pos:08,sal:05,e]
* 64 75 2C 6D 61 72 [du:03,sta:02,mar]
* 3A 30 3A 33 32 3B [:0,gen:M,age:32;]
* 20 53 20 53 49 44 [ SINA_USER=; SID]
* 3D 3B 6C 6F 67 69 [=; userinfo_logi]
* 6E 74 34 32 39 37 [ntime=1016174297]
* 3B 20 68 61 6E 6E [; userinfo_chann]
* 65 6C 72 69 6E 66 [el=mail; userinf]
* 6F 5F 3D 31 36 32 [o_remoteaddr=[redacted]]
* 2E 31 20 53 4D 3D [.[redacted]; SM=]
* 53 69 6D 79 6E 75 [SinaMail....mynu]
* 6D 3D 73 73 3D 26 [m=1&user=&pass=&]
* 75 3D 70 73 77 3D [u=[redacted]&psw=]
* [redacted] 25 33 41 25 [[redacted]&l=http%3A%]
* 32 46 6E 61 2E 63 [2F%2Fmail.sina.c]
* 6F 6D 62 69 6E 25 [om.cn%2Fcgi-bin%]
* 32 46 72 6F 64 75 [2Fmail.cgi&produ]
* 63 74             [ct=mail]
```

All rights are reserved by Li Jingtao @ Fudan University

All rights are reserved by Li Jingtao, and content may not be reproduced, downloaded, disseminated, published, or transferred in any form or by any means, except with the prior written permission of Li Jingtao.

网络环境下的认证

- 基本假设：
  - C/S 模型

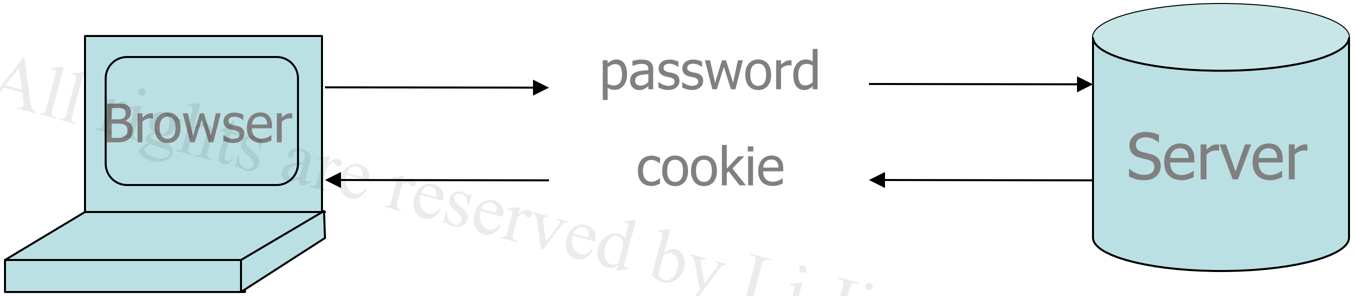


- 多server，
  - 同样的口令，还是不同的？
- 单向->双向，
  - Server需要对每个user出示独特的口令吗？

All rights are reserved by Li Jingtao @ Fudan University

All rights are reserved by Li Jingtao, and content may not be reproduced, downloaded, disseminated, published, or transferred in any form or by any means, except with the prior written permission of Li Jingtao

Authentication Problems



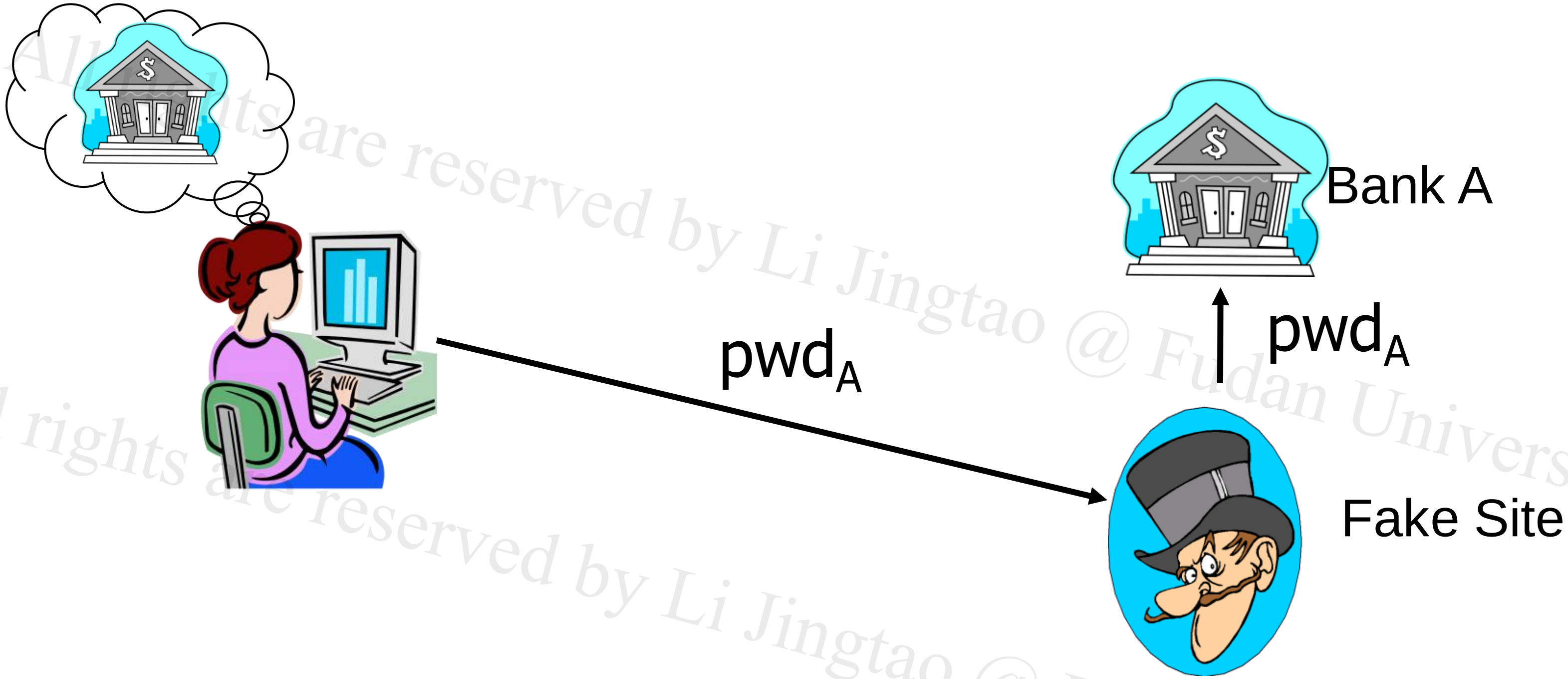
- Problems
  - Network sniffing → Encryption, but key distribution problems
  - Malicious or weak-security website → OWF, hashing
    - Phishing
    - Common password problem
    - Pharming – DNS compromise

    } next few slides
  - Malware on client machine
    - Spyware
    - Trojan Horse

All rights are reserved by Li Jingtao @ Fudan University

All rights are reserved by Li Jingtao, and content may not be reproduced, downloaded, disseminated, published, or transferred in any form or by any means, except with the prior written permission of Li Jingtao.

Password Phishing Problem

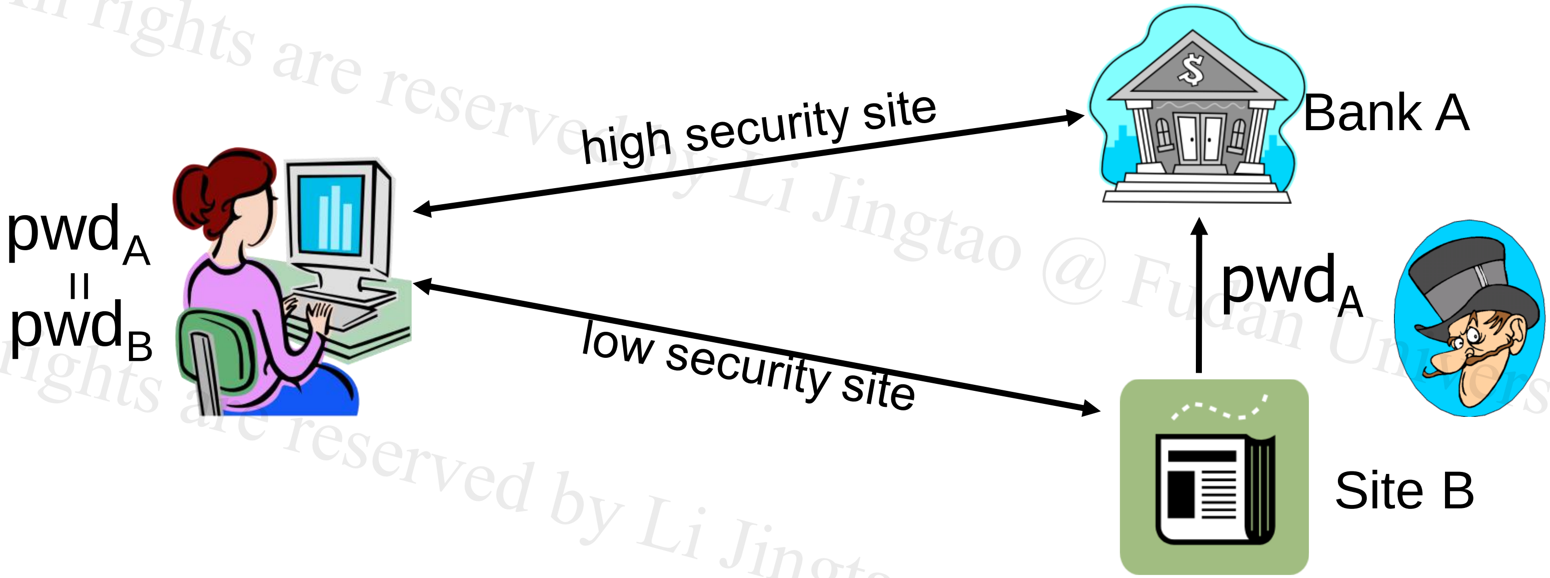


All rights are reserved by Li Jingtao @ Fudan University
All rights are reserved by Li Jingtao @ Fudan University

- User cannot reliably identify fake sites
- Captured password can be used at target site

All rights are reserved by Li Jingtao, and content may not be reproduced, downloaded, disseminated, published, or transferred in any form or by any means, except with the prior written permission of Li Jingtao.

Common Password Problem

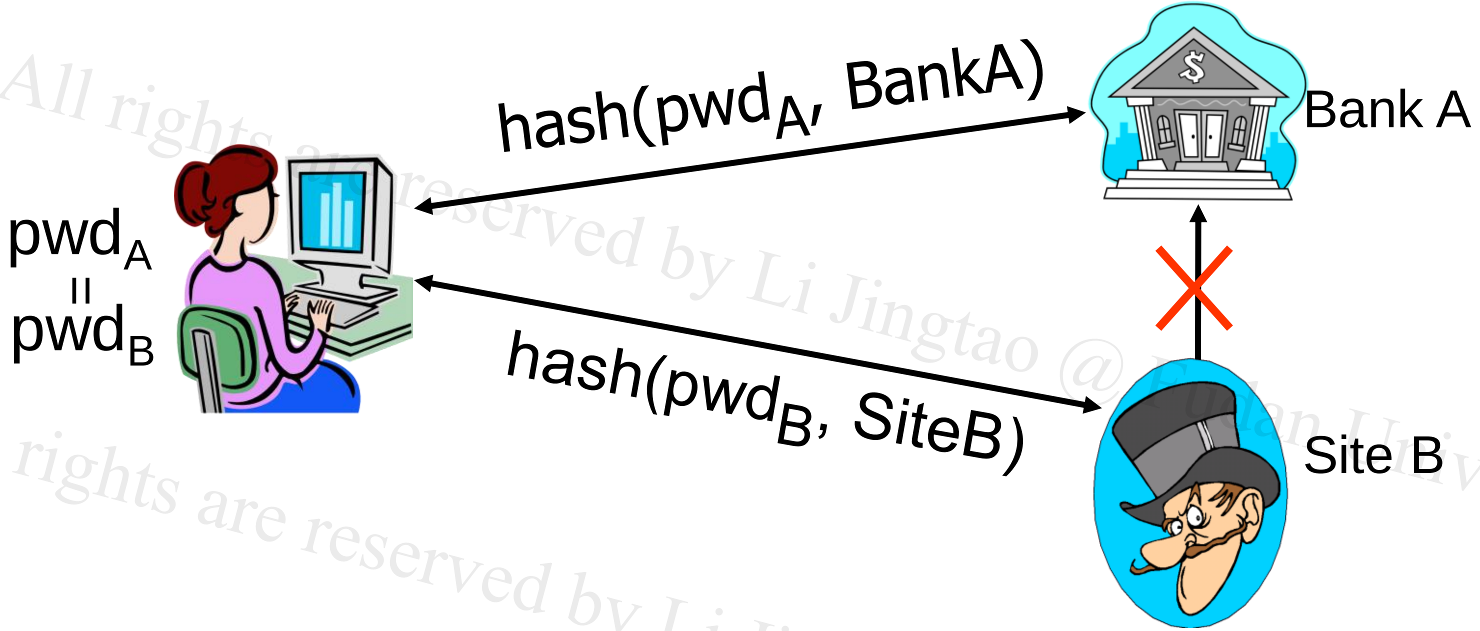


All rights are reserved by Li Jingtao @ Fudan University

- Phishing attack or break-in at site B reveals pwd at A
  - Server-side solutions will not keep pwd safe
  - Solution: Strengthen with client-side support

All rights are reserved by Li Jingtao, and content may not be reproduced, downloaded, disseminated, published, or transferred in any form or by any means, except with the prior written permission of Li Jingtao.

Defense: Password Hashing



All rights are reserved by Li Jingtao @ Fudan University

- Generate a unique password per site
  - HMAC$_{fido:123}$(banka.com) ® Q7a+0ekEXb
  - HMAC$_{fido:123}$(siteb.com) ® OzX2+ICiqc
- Hashed password is not usable at any other site
  - Protects against password phishing
  - Protects against common password problem

All rights are reserved by Li Jingtao, and content may not be reproduced, downloaded, disseminated, published, or transferred in any form or by any means, except with the prior written permission of Li Jingtao.

Outline of Talk

- Definitions
- Passwords
  - Unix Passwords
  - One time passwords
- Challenge-response techniques

All rights are reserved by Li Jingtao @ Fudan University
All rights are reserved by Li Jingtao @ Fudan University

All rights are reserved by Li Jingtao, and content may not be reproduced, downloaded, disseminated, published, or transferred in any form or by any means, except with the prior written permission of Li Jingtao.

One time passwords

- Avoids *replay attacks*
- ***Shared lists*** - pre-distribute list
- ***Sequentially updated*** - create next password while entering current password
- ***Based on one way functions*** - Lamport's scheme…

All rights are reserved by Li Jingtao @ Fudan University

All rights are reserved by Li Jingtao @ Fudan University

All rights are reserved by Li Jingtao, and content may not be reproduced, downloaded, disseminated, published, or transferred in any form or by any means, except with the prior written permission of Li Jingtao.

Lamport’s One Time Passwords

- 1981, by Lamport
- Initialization
  - User has a secret *w*
  - Using a OWF *h*, create the password sequence:

$$w, h(w), h(h(w)), \ldots, h^t(w)$$

  - Bob knows only $h^t(w)$
- Authentication：
  - Password for i^{th} identification is:

$$w_i = h^{t-i}(w)$$

All rights are reserved by Li Jingtao @ Fudan University

All rights are reserved by Li Jingtao @ Fudan University

All rights are reserved by Li Jingtao, and content may not be reproduced, downloaded, disseminated, published, or transferred in any form or by any means, except with the prior written permission of Li Jingtao.

S/KEY One-Time Password System

- Based on Lamport's OTP
- Initialization
  - User has a secret: *w*, *seed* (non-secret)
  - Using a OWF *h*, create the password sequence:

    $w, h(w,seed), h(h(w), seed), \ldots, h^t = h(h^{t-1}, seed)$
  - Bob server knows: *seed*, Sequence#, h^t
- Authentication：
  - Password for i^{th} identification is:

    $$w_i = h^{t-i} = h(w_{i-1}, seed)$$

All rights are reserved by Li Jingtao @ Fudan University

All rights are reserved by Li Jingtao, and content may not be reproduced, downloaded, disseminated, published, or transferred in any form or by any means, except with the prior written permission of Li Jingtao.

使用seed, Sequence#

- 多个server，Password 可重用(使用不同seed即可)

- Server 可发起Challenge:
  - [seed, sequence#]

All rights are reserved by Li Jingtao @ Fudan University

All rights are reserved by Li Jingtao @ Fudan University

All rights are reserved by Li Jingtao, and content may not be reproduced, downloaded, disseminated, published, or transferred in any form or by any means, except with the prior written permission of Li Jingtao.

Attacks on OTPs..

- ***Pre-play attack*** - Eve intercepts an unused password and uses it later
- Make sure you're giving password to the right party
- Bob server must be *authenticated*

All rights are reserved by Li Jingtao @ Fudan University

All rights are reserved by Li Jingtao @ Fudan University

All rights are reserved by Li Jingtao, and content may not be reproduced, downloaded, disseminated, published, or transferred in any form or by any means, except with the prior written permission of Li Jingtao.

Shortcomings of OTPs..

- 使用500-1000次需要Reinitialization
  - 开销不小
- 不支持双向认证
- 保密性没考虑

All rights are reserved by Li Jingtao @ Fudan University
All rights are reserved by Li Jingtao @ Fudan University