

A good security architecture can kill online fraud



## Objective

...to show you how to avoid single-point-of-failures (SPOFs) and prevent fraud

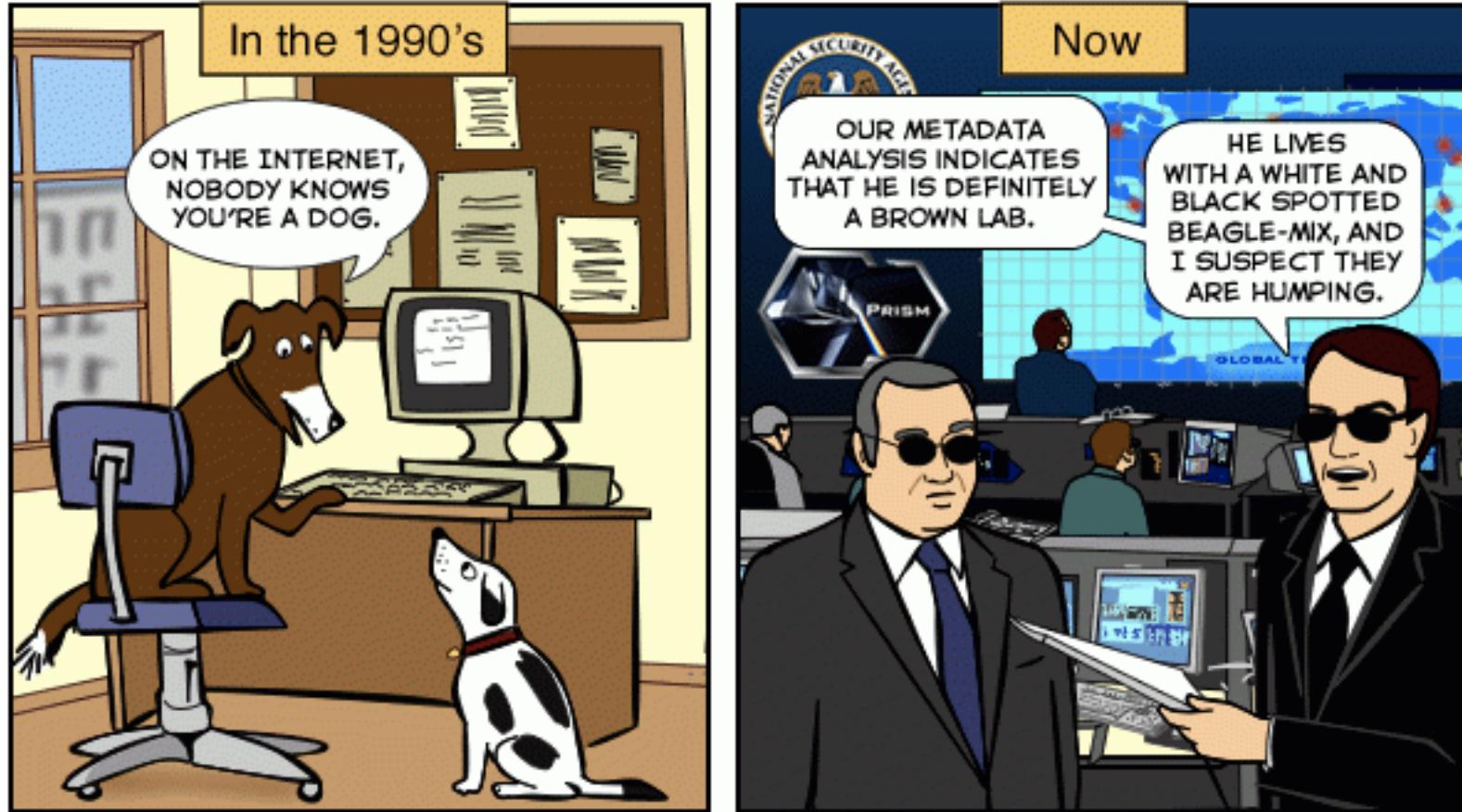
What is a single-point-of-failure?

*One place, which compromises the whole security if hacked.*

*What's behind most fraud online?  
..... a fundamentally broken nature of identity online...*



## US government approach to this problem: sneaky surveillance



Chinese government  
approach to this problem:  
Real ID online



## What's needs to be done to kill fraud?

- 1. *Identity: Our learnings from fixing the online identity***
  
- 2. *Communication: Applying the principles to security of TLS***

# Why should you even listen to me?

ADUCID (The world's most advanced authentication system)

## ***Our background:***

- > 20 years of experience in IT security
- We helped shape the standard for digital identities in the European Union

## ***Our products:***

- 10 years of unique research in authentication & secure communication
- 7+ million USD in direct investments
- 7+ international patents
- several rounds of penetration tests without a single relevant weakness

# PASSWORDS HAVE SOOO MANY PROBLEMS...



Reliant on users



Physical ID online



Copying identities



Lack of mutual trust



Centralization



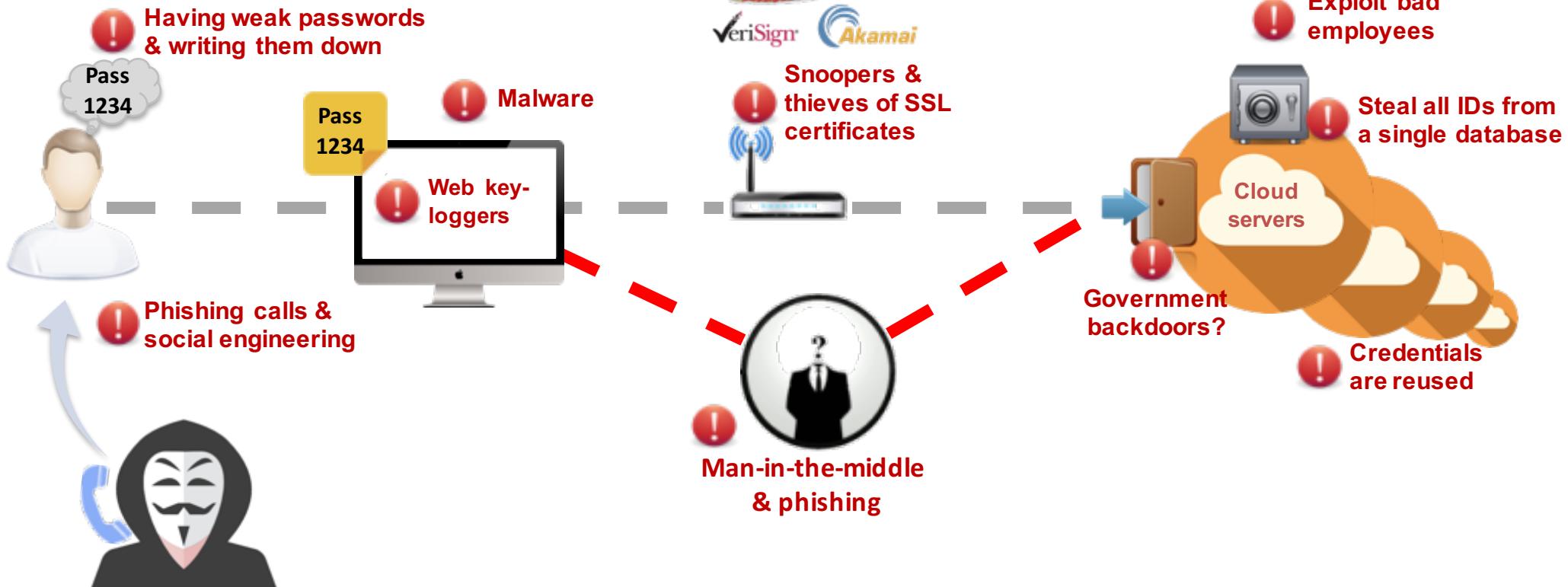
Credentials reuse



Static protection



Reliant on HTTPS



EACH OF THEM REPRESENTS A SINGLE-POINT-OF-FAILURES

## HOW TO SOLVE THESE PROBLEMS?



Reliant on users



Physical ID online



Copying identities



Lack of mutual trust



Centralization



Credentials reuse



Static protection



Reliant on HTTPS

### 2 key design principles & 6 main tools:

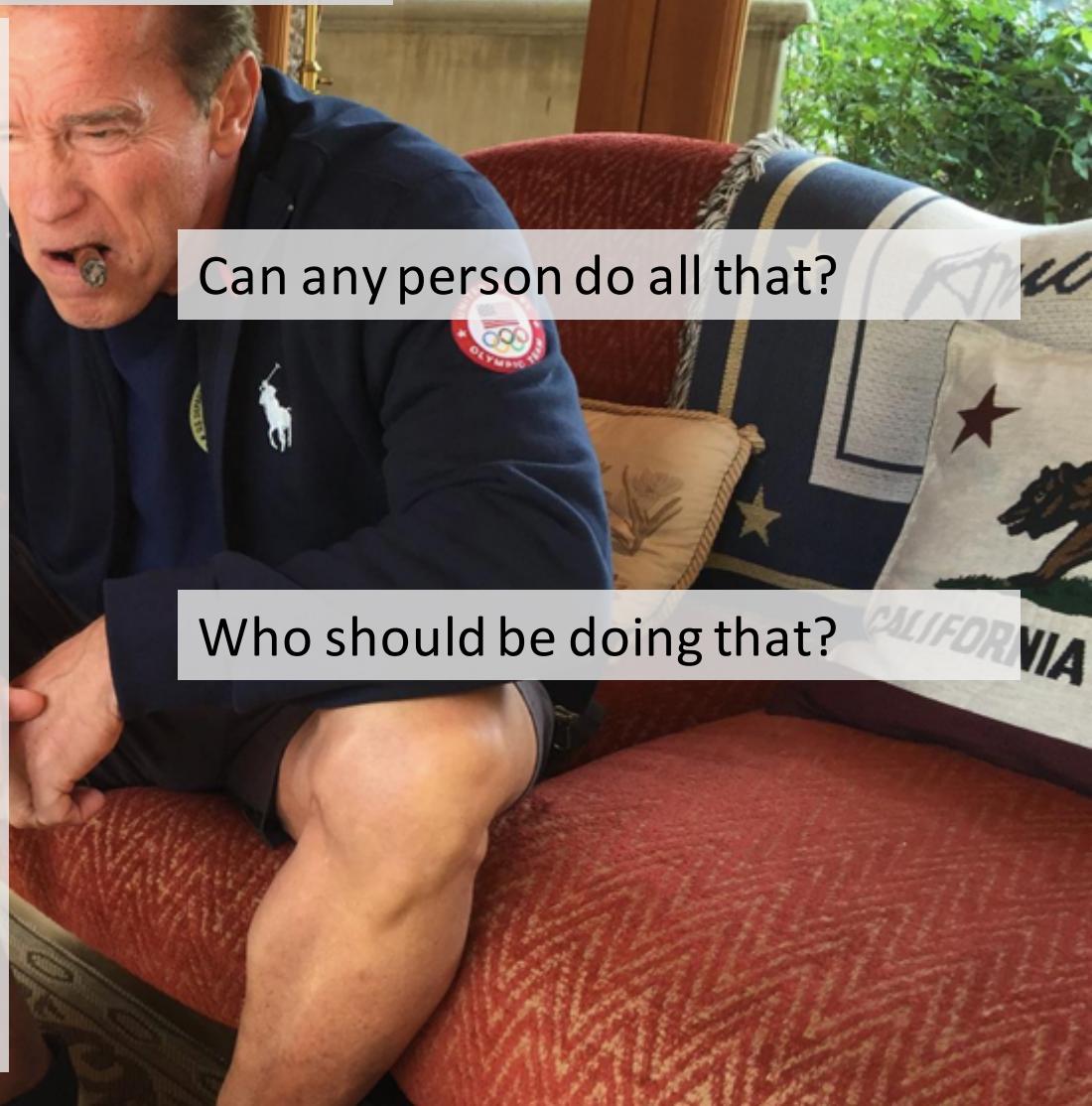
1. Remove the people from security
2. Fix the architecture instead of “plugging holes”
  - Separate cyber IDs
  - Asymmetric cryptography
  - Mutual trust
  - Distributed design
  - Dynamic protections
  - Dual authentication



# REMOVE USER

How much of security do users handle?

1. Create strong passwords
2. Never reuse passwords
3. Change password frequently
4. Make sure communication is secure
5. Recognize fake websites & phishing
6. Recognize fake calls or fraudsters
7. Make sure all apps, systems and devices are up-to-date
8. Fight against viruses
9. NEVER EVER make a mistake



Can any person do all that?

Who should be doing that?

Physical world

## REMOVE USER

Online world



I don't handle security  
... I just have my device



My app handles security

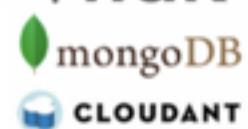


The app handles reliably all the security actions for the users

# REMOVE DEVELOPER & ADMIN

Developers and admins must never make a mistake in...

## Databases



## Cloud Servers



## Services



Front E



... and they have to face a huge number of attack vectors

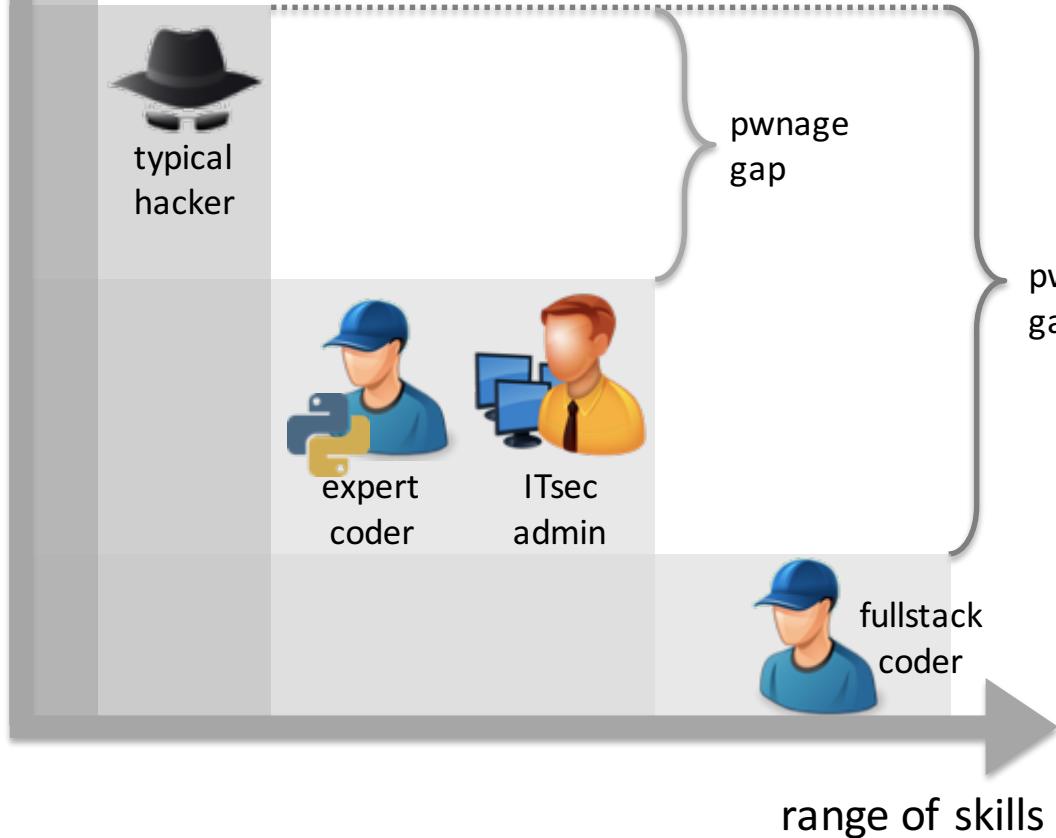


Expertise

# REMOVE DEVELOPER & ADMIN



Narrowly specialized experts stand  
the best chance against hackers



## World's Biggest Data Breaches

Selected losses greater than 30,000 records  
(updated 18th Feb 2015)

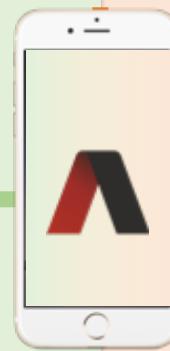
YEAR    BUBBLE COLOUR    METHOD OF LEAK    BUBBLE SIZE    NO. OF RECORDS STOLEN    DATA SENSITIVITY    SHOW FILTER

Physical world



I don't handle security  
... I just have my device

## REMOVE DEVELOPER & ADMIN



My app handles security



Security should be developed by experts & work as a service

Online world

## SEPARATE CYBER IDs

### Why is it a problem to use physical identity online?

3 factors in physical world (I know, I have, I am) ... but only 1 online (I know)

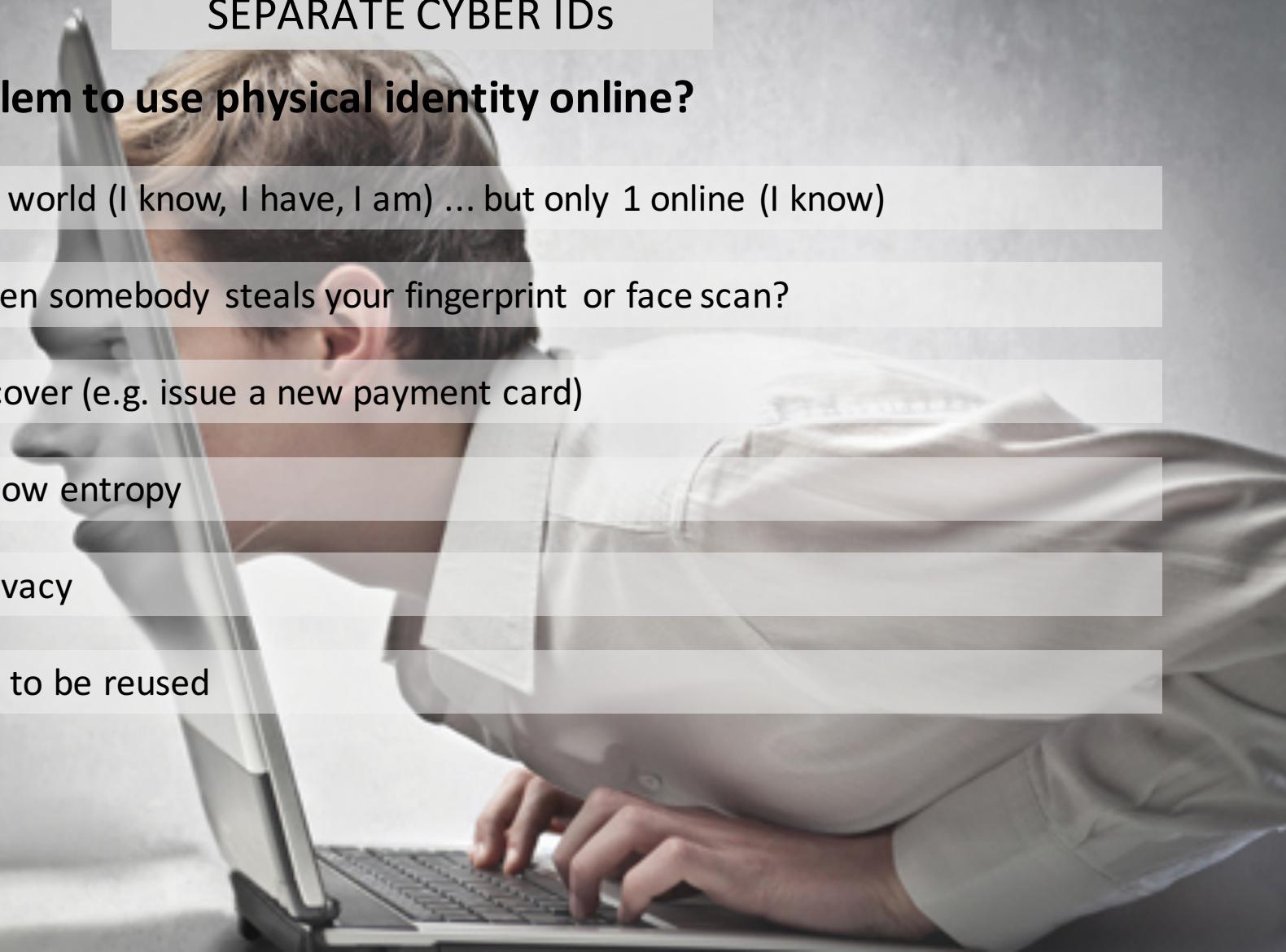
What do you do when somebody steals your fingerprint or face scan?

It's expensive to recover (e.g. issue a new payment card)

Physical IDs have a low entropy

Physical IDs limit privacy

Physical ID is bound to be reused



Physical world

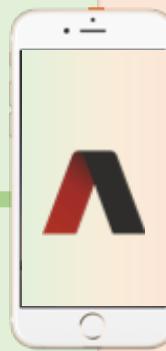
## PHYSICAL & CYBER IDs

Online world



I have my device

Physical ID: Ivo Toman



My app handles  
security



Cyber ID:  
6F\_j7+hl\$ps&6aF3^9f;k?fs  
dK97jkJ975u...R.;'u&5dh8  
K3I;9asd-k)\*2@'',96&(8o3

Your physical ID cannot be misused online.  
Your cyber ID cannot be misused in physical world.



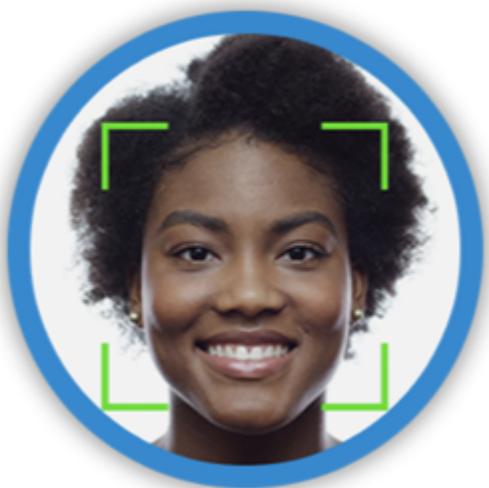
Would you give the credit  
card and walk away?



Would you give the driving  
license and drive away?



... but that's exactly what you do online today when you enter your password, face-scan or payment card info....



After how many days from a security breach do Asian companies discover that they have been hacked?



**A typical Western company discovers a breach after ~200 days**



**A typical Asia company discovers a breach after ~500 days**

Physical world

## ASYMMETRIC IDs

Online world



I have my device

Physical ID: Ivo Toman



My app handles  
security



Cyber ID:  
6F\_j7+hl\$ps&6aF3^9f;k  
?fsdK97jkJ975u....R.;'u  
&5dh8K3l;9asd-k&(8o3

Cyber IDs are asymmetric and never leave user's hands.

No hack on server or communication can compromise user's cyber ID



Is this service who it claims to be?

Phishing

Man-in-the-middle

FRAUD

Theft of user's identity

Is this user who she claims to be?

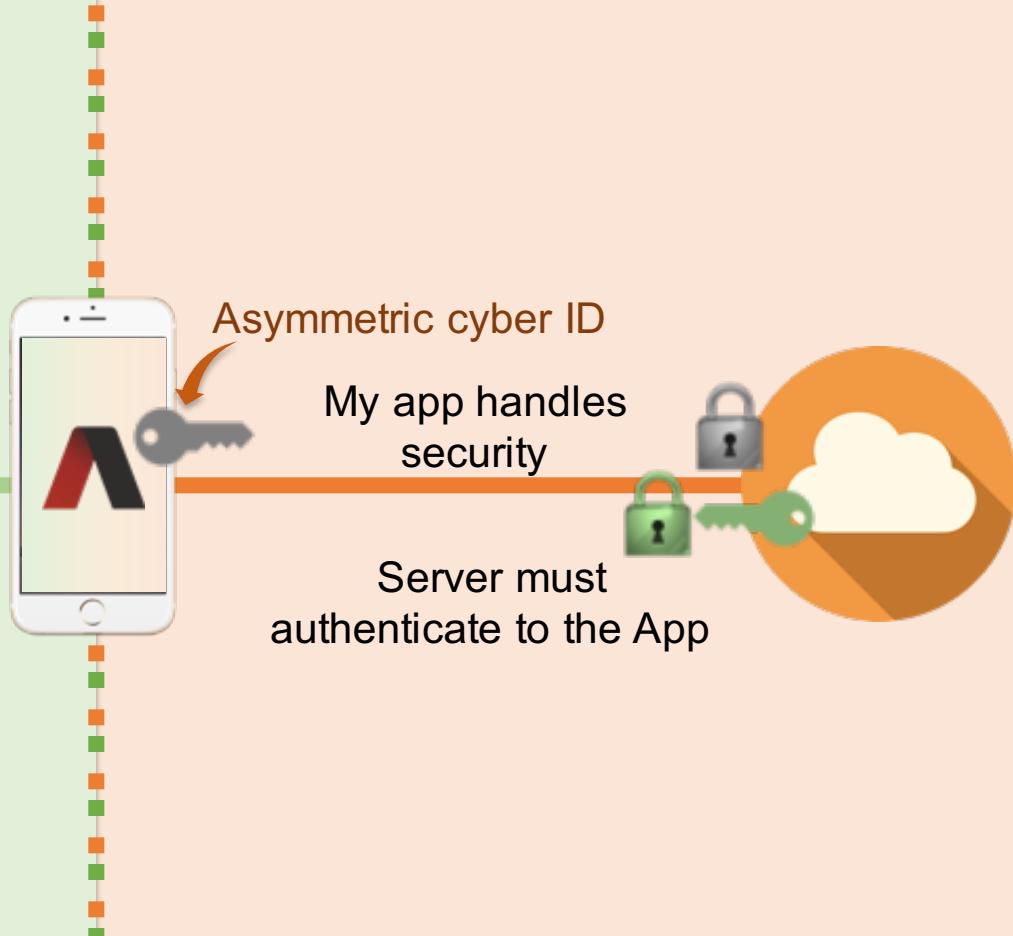
Physical world

## MUTUAL TRUST

Online world



I have my device



No user or App proves its identity until the server proves its identity the user/App.  
AND! This is HTTPS independent and largely quantum resistant.

# *Internet Map*



Physical world

# DISTRIBUTED MODEL

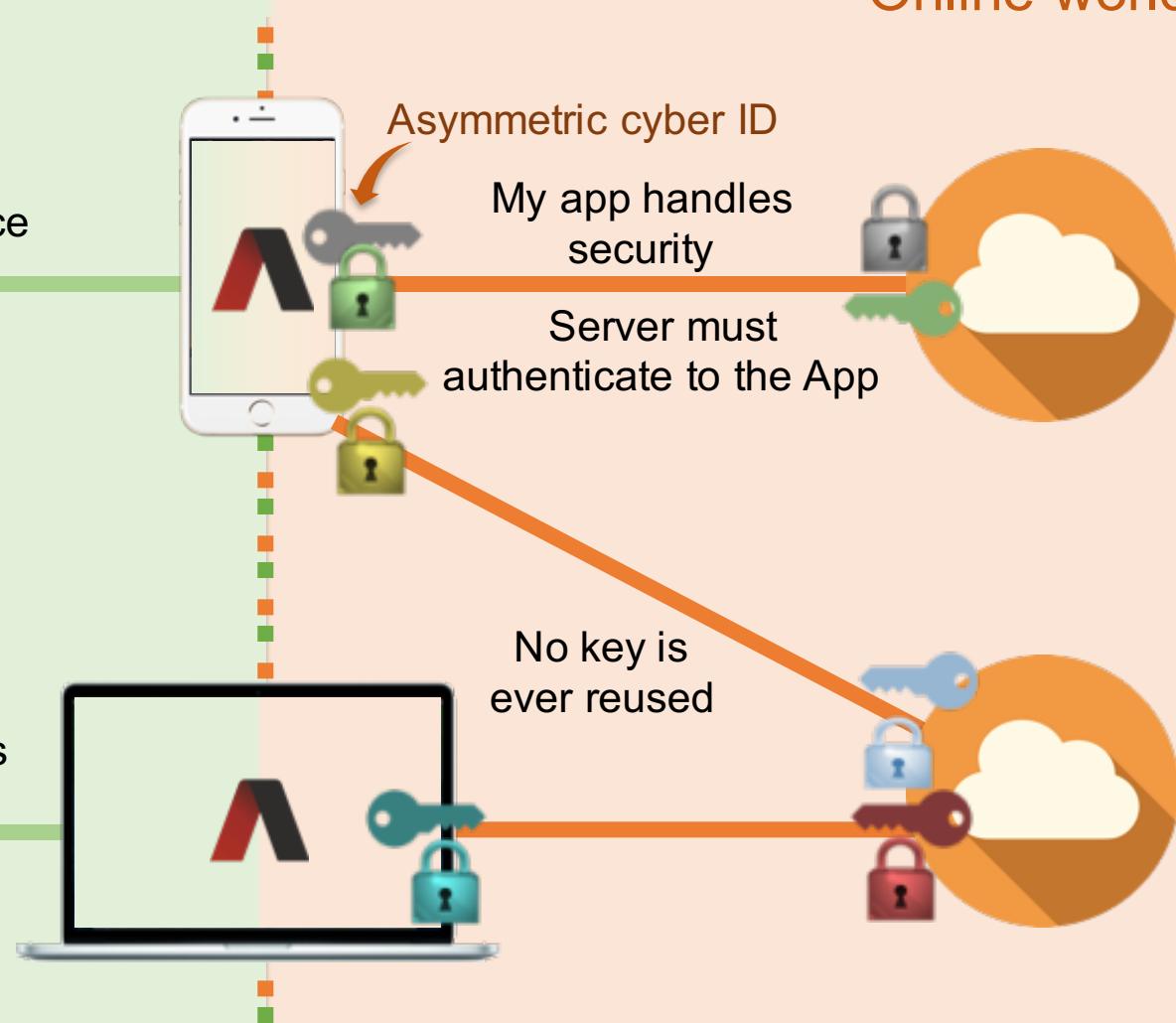
Online world



I have my device



Different user has  
her device



No master key, no reuse of keys, no single point of failure, all automatic

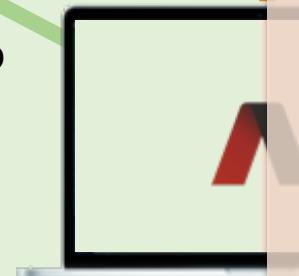
Physical world

# USER CENTRIC UX

Online world



I have my phone

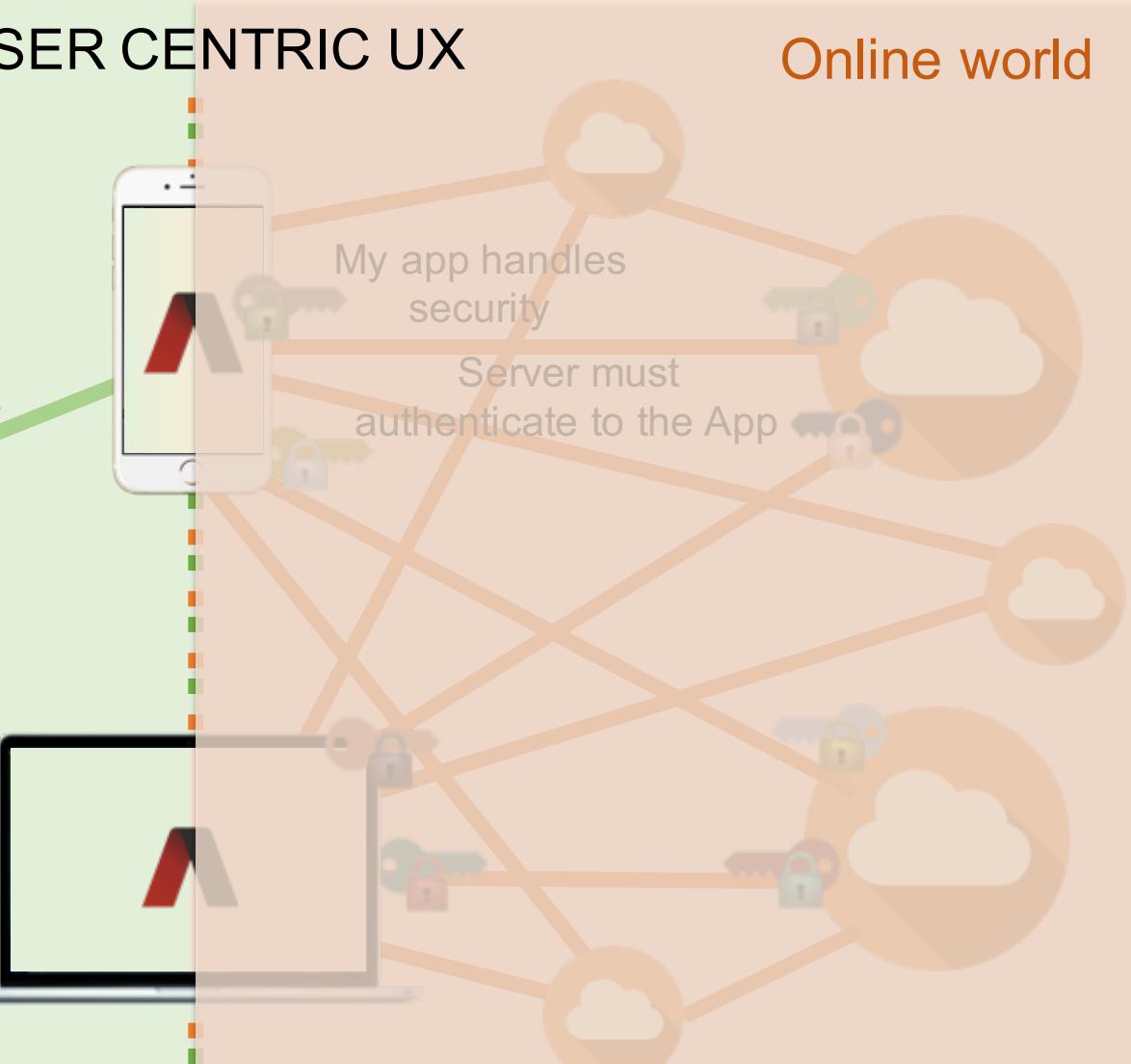


and my laptop



My app handles security

Server must authenticate to the App



Absolute user simplicity. Ultimate network security. Foundation of accountability.



Are the Apps/devices a single-point-of-failure for individual users?

**what should we do about it?**

## Local locks or data encryption?

- ✗ still a single-point-of-failure
- ✗ bad for user experience
- ✗ bad for recovery process
- ✗ static protection reliant on the user



# What about specialized HW chips, smartcards or USB keys?



Maginot line  
马奇诺防线





# How to Crack Android Full Disk Encryption on Qualcomm Devices

Friday, July 01, 2016    Mohit Kumar

[G+1](#) 148    [Like 6.5K](#)    [Share](#) 3784    [Tweet](#) 430    [Share](#) 56    [share](#) 4371

## How to Crack Android Full Disk Encryption

```
$ python fde_bruteforce.py \
    metadata.bin \
    08DF57BED3F2396BACB6719444A308F2 \
```

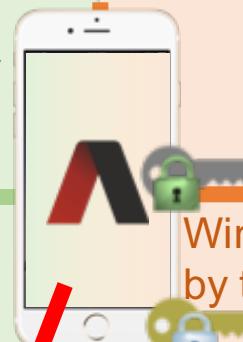
Physical world

# DYNAMIC PROTECTIONS

Online world



Sandboxing &  
protections by OS



Window of opportunity limited  
by the user's next login



Sharing of  
security events  
between services



Multi-level  
HW footprint

Dynamic protections make misuse very hard

## **We need a security solution, which:**

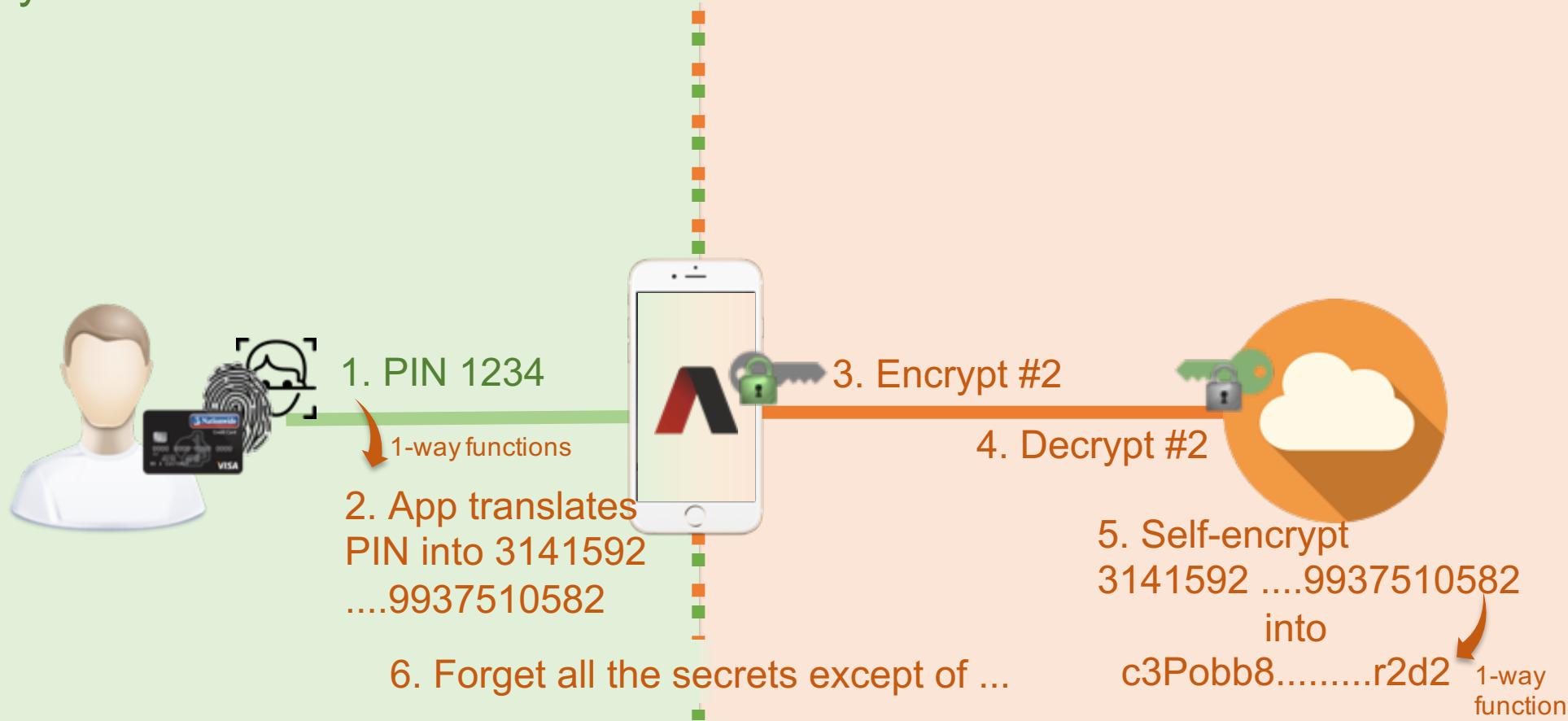
- is dynamically enforced
- dynamic in time
- not limited by user's abilities
- never stores secret on the device
- cannot be stolen from the server

**Sounds impossible?**

Physical world

# DUAL AUTHENTICATION

Online world



Factors are never stored and never sent.

Their “cyber ID” (#2) can change over time.

Only the server can evaluate the correctness of a factor.

# THE MOMENT OF TRUTH

	Remove user	Separate cyber IDs	Asymmetry	Mutual trust	Distributed design	Dynamic protections	SCORE
Weak passwords & writing them down							3x
Prone to online & call phishing							4x
Credentials reuse							2x
Every login creates a copy of ID							2x
Malware							2x
Anyone who knows any ID can enter							2x
All IDs in a database							2x
Easy to crack stolen passwords							2x
Snoopers & thieves of SSL certificates							3x
Man-in-the-middle							2x



# Do you ever visit these pages?

www.bankcomm.com/Ba

www.12306.cn/mormhweb/

www.abchina.com/en/

**交通銀行**  
BANK OF COMMUNICATIONS  
始于1908 您的财富管理银行

中国农业银行  
AGRICULTURAL BANK OF CHINA

Personal Corporate Agro-related Investor Relations About Us

Log on to...

2016年6月13日 星期一

一步式好礼 活动时间 2016

高铁动卧、夕发朝至

旅客服务质量调查问卷

新版售票 点击进入>

网上购票用户注册

购票

我的保险

退票

余票查询

2016关于端午假

NEW

王记网银安全四  
社网络诈骗

Latest from ABC

## ABC and Huaneng Group Accomplish First DFI for Central Enterprises

On March 10, China Huaneng Group (Huaneng) issued RMB4 billion of short-term commercial papers in DFI (unified registration of a variety ...)

Read more +

News Update >

Corporate Social Responsibility Report >

Branches Structure >

# What's the problem?

The screenshot shows a web browser with three tabs open:

- www.bankcomm.com/Ba
- www.12306.cn/mormhweb/
- www.abchina.com/en/ (Active tab)

The main content area displays the official website of the Agricultural Bank of China (ABC). The header includes the bank's logo, name in Chinese and English, and navigation links for Personal, Corporate, Agro-related, Investor Relations, and About Us. A yellow "Log on to..." button is also present.

A large orange arrow points upwards from the bottom left towards the ABC logo. Three other orange arrows point downwards from the top left towards the three tabs.

The ABC website content includes:

- Latest from ABC**
- ABC and Huaneng Group Accomplish First DFI for Central Enterprises**
- On March 10, China Huaneng Group (Huaneng) issued RMB4 billion of short-term commercial papers in DFI (unified registration of a variety ...)
- Read more +**
- 旅客服务质量调查问卷**
- 新版售票 点击进入>**
- 网上购票用户注册**
- 购票** (highlighted with an orange arrow)
- 我的保险**
- 退票**
- 余票查询**
- News Update >**
- Corporate Social Responsibility Report >**
- Branches Structure**

# Any more problems?

https://pbank.95599.

https://kyfw.12306.cn/otn/leftTicket/init

https://www.95599.cn/PersonalBank\_EN/startUpHtmlSessionAction.ebf

交通银行  
BANK OF COMMUNICATIONS  
您的财富管理银行

扫一扫，立享  
第二代手

扫

Your connection is not private

Attackers might be trying to steal your information (for example, passwords, messages, or credit cards). NET::ERR\_CERT\_AUTHORITY\_INVALID

Automatically report details of possible security incidents to Google. [Privacy policy](#)

Your connection is not private

Attackers might be trying to steal your information from [www.95599.cn](http://www.95599.cn) (for example, passwords, messages, or credit cards). NET::ERR\_CERT\_AUTHORITY\_INVALID

Automatically report details of possible security incidents to Google. [Privacy policy](#)

**Tip**

1. Dear customers: by us  
"BOCOM Personal E-  
nsaction Rules", plea

ADVANCED

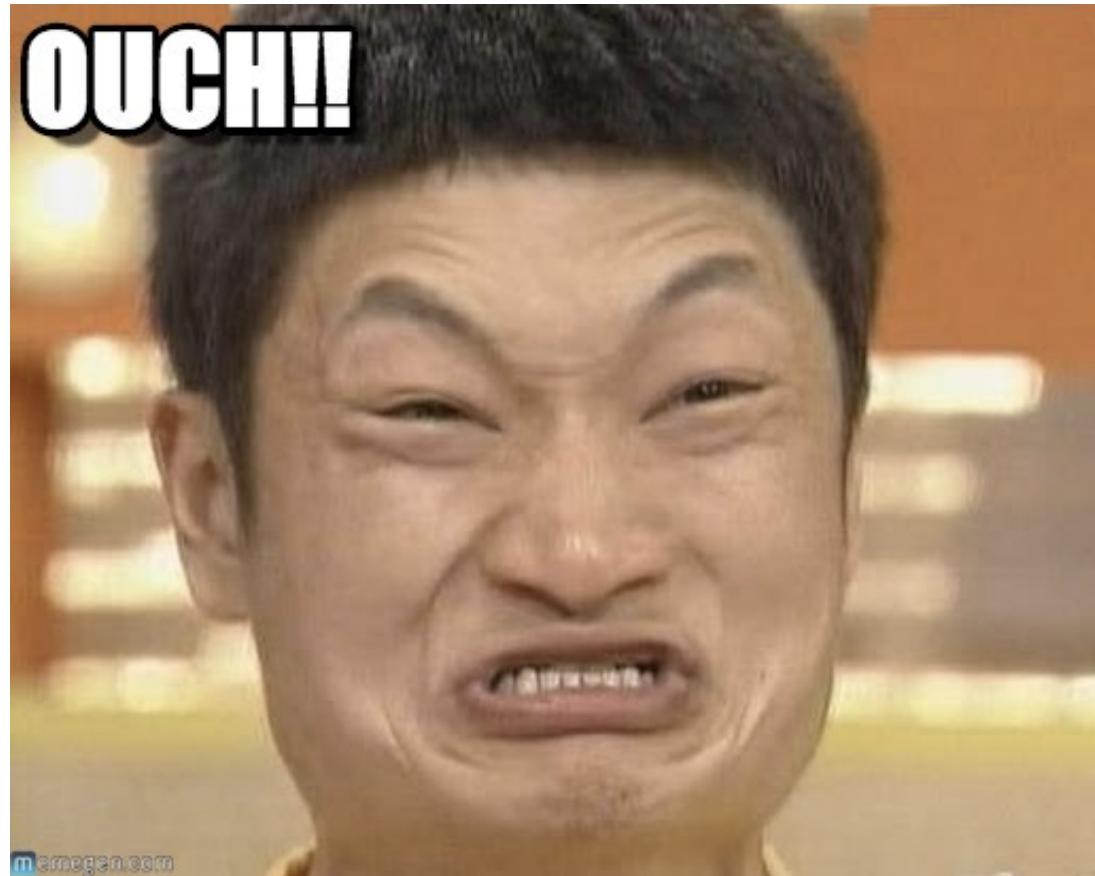
ADVANCED

Awesome. Our victims are taught to get phished :)

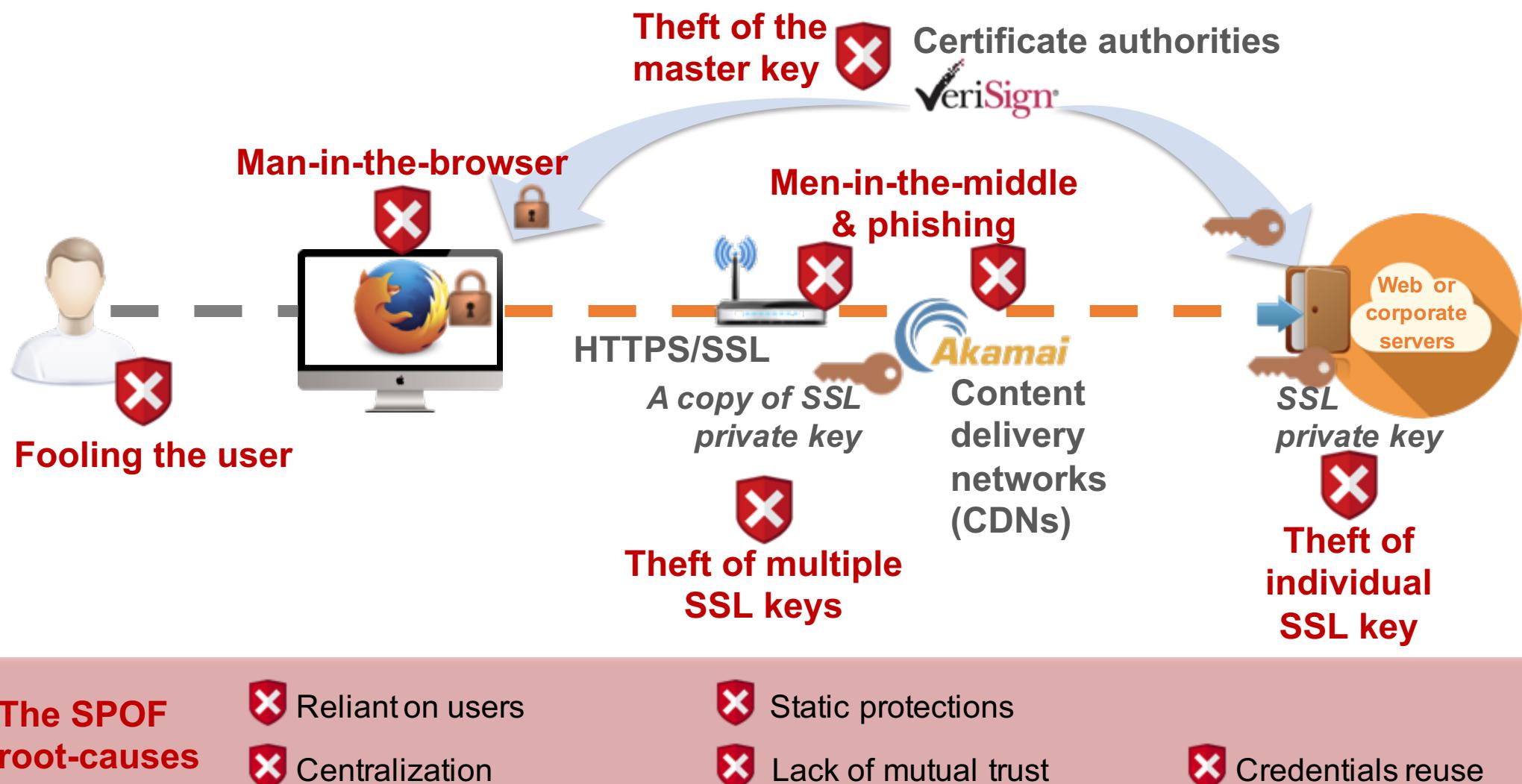
Back to safety

# These must be anomalies and the worst possible examples, right?

	Configuration score (overall)	HSTS	HPKP
 中国银行 BANK OF CHINA	B	✗	✗
 中国建设银行 China Construction Bank	C+	✗	✗
 支付宝 ALIPAY	C+	✗	✗
 中信银行 CHINA CITIC BANK	C	✓	✗
 中国农业银行 AGRICULTURAL BANK OF CHINA	C	✗	✗
 ICBC	F	✗	✗
 兴业银行 INDUSTRIAL BANK CO.,LTD.	F	✗	✗
 招商银行 CHINA MERCHANT'S BANK	F	✗	✗
 浦发银行 SPD BANK	F	✗	✗
 中国邮政储蓄银行 POSTAL SAVINGS BANK OF CHINA	F	✗	✗
 中国民生银行 CHINA MINSHENG BANKING CORP.,LTD.	F	✗	✗
 交通银行 BANK OF COMMUNICATIONS	F	✗	✗
 中国平安 Ping An Bank	F	✗	✗



# Case in point: Can you spot any way how you would break it?



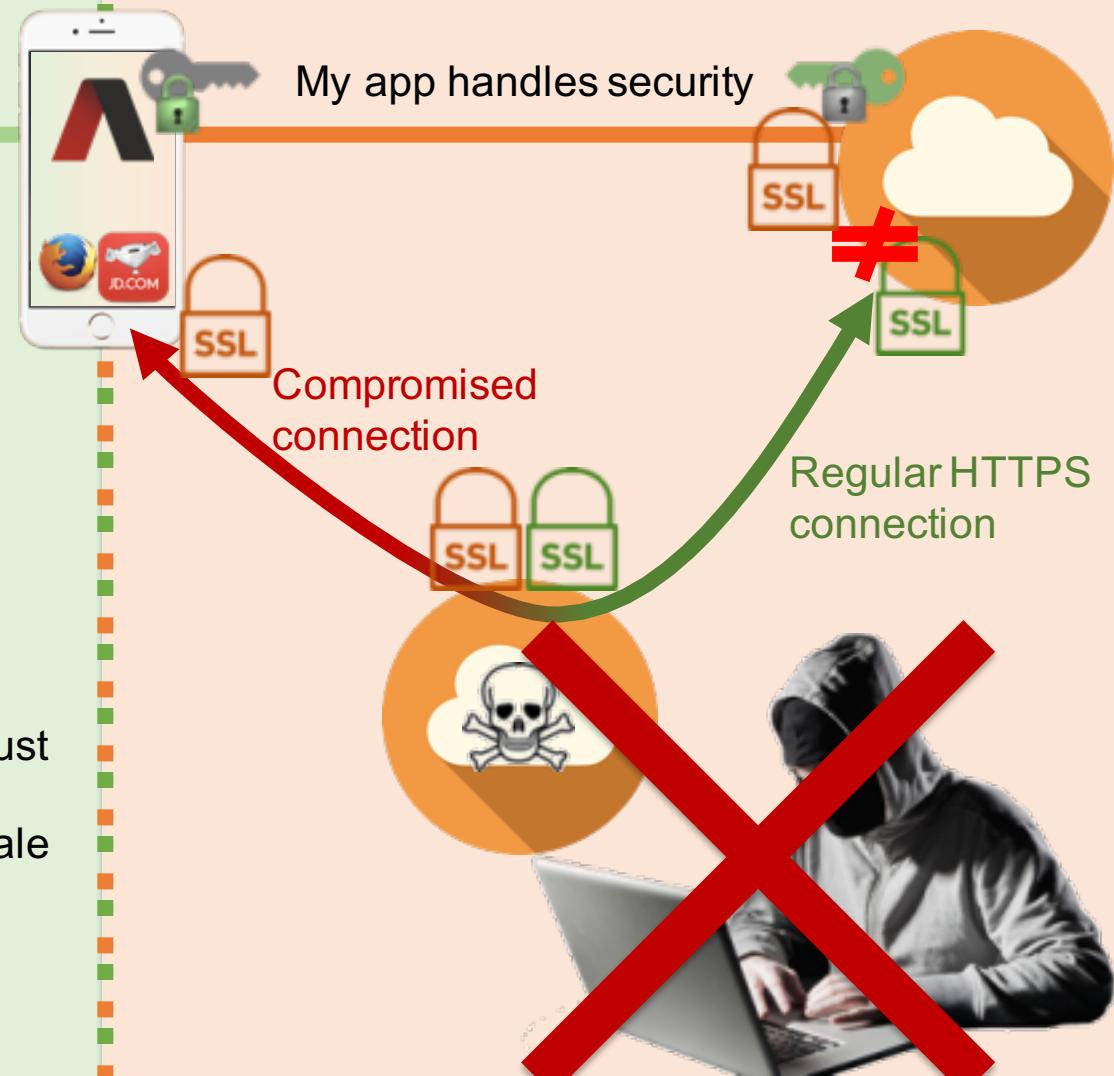
## Physical world



I have my device

## CASE IN POINT: HTTPS/SSL

## Online world



# THE MOMENT OF TRUTH v2

	Remove user	Separate cyber IDs	Asymmetry	Mutual trust	Distributed design	Dynamic protections	Score
Weak passwords & writing them down							3x
Prone to online & call phishing							4x
Credentials reuse							2x
Every login creates a copy of ID							2x
Malware							2x
Anyone who knows any ID can enter							2x
All IDs in a database							2x
Easy to crack stolen passwords							2x
Snoopers & thieves of SSL certificates							2x
Man-in-the-middle							2x



### Electronic payments



Centralization



Reliant on users



Credentials reuse



Lack of mutual trust



Copying identities



Physical ID online



Static protection



### Electronic signatures



Centralization



Reliant on users



Credentials reuse



Copying identities



Static protection



**Multi-party operations** (e.g.  
online elections, real ID  
verification etc.)



Accumulation of weak-points  
of the individual transactions



BLOCKCHAIN

### Blockchain distributed database & smart contracts



Separate cyber IDs



Reliant on users



Asymmetry



Credentials reuse



Distributed design



Lack of mutual trust

## Conclusions:

- Systematically identify single-point-of-failure
- Use following tools:
  - Remove people from security (especially users and developers)
  - Separate cyber IDs
  - Asymmetry
  - Mutual trust
  - Distributed design
  - Dynamic protections
  - Dual authentication
- These measures can be transferred to solutions of different problems