

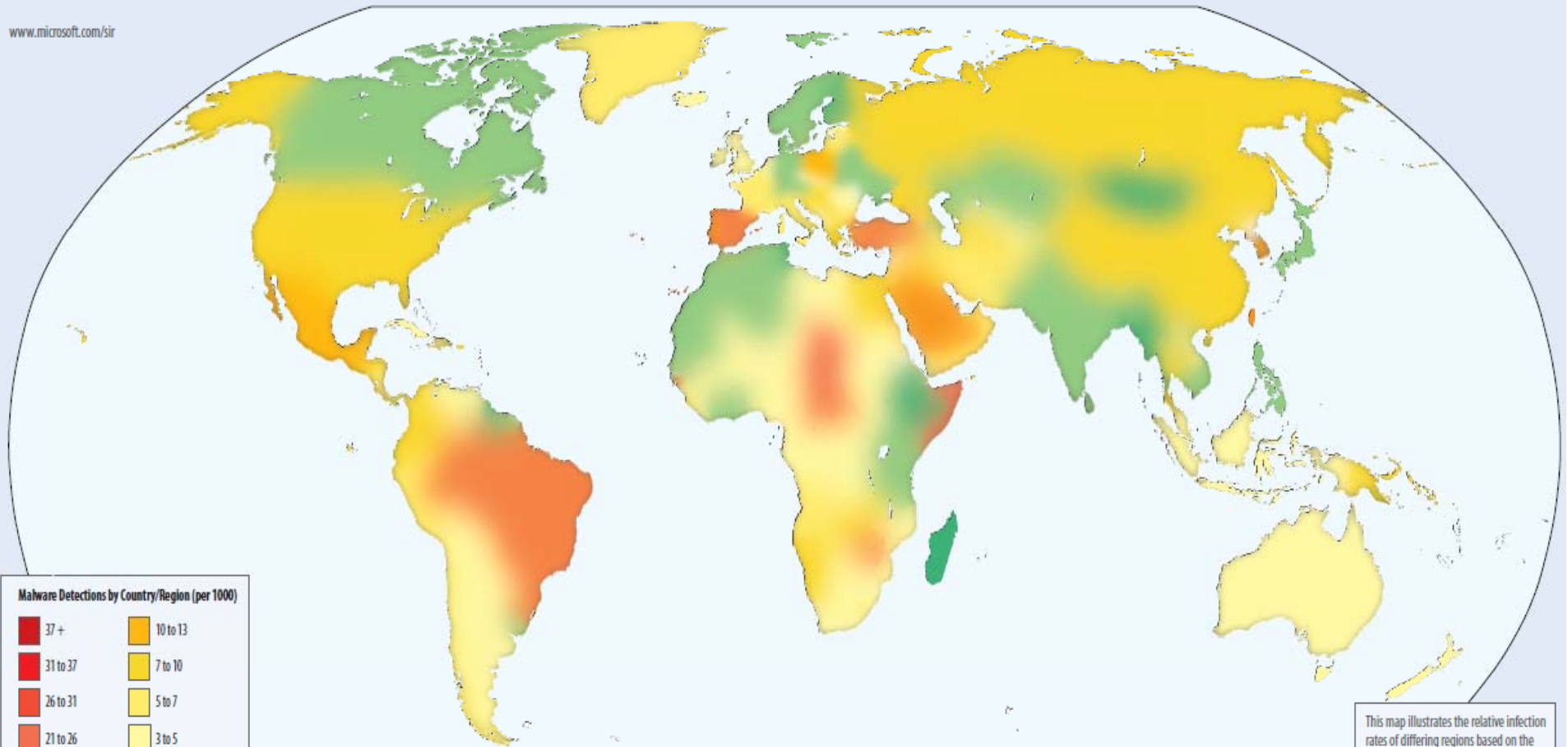
How to deal with risks associated to network services

Kazukuni Kobara

National Institute of Advanced Industrial
Science and Technology, Japan as well as
Japan Science and Technology agency,
Center for Research and Development
Strategy

of infected computers/(1000 MSRT executions)

www.microsoft.com/sir



Malware Detections by Country/Region (per 1000)

37+	10 to 13
31 to 37	7 to 10
26 to 31	5 to 7
21 to 26	3 to 5
17 to 21	1.5 to 3
13 to 17	0 to 1.5
	Insufficient data

MSRT detects only major malwares and if minor ones are taken into account, the situation would be even worse.

This map illustrates the relative infection rates of differing regions based on the number of infected computers discovered per 1,000 executions of the MSRT. For example, a region colored yellow would have an infection rate of between 7 and 10 computers per 1,000 executions of the MSRT.

Countermeasures Against Infected Terminals

- Construction of clean environment
 - ◆ Secure/trusted boot
 - ◆ Code signing
- Detection and removal of malwares
- So enhancement of these ability is primarily important.

- But, taking the following facts into account
 - Users **have to use infected terminals unwittingly** with certain probability since it is almost impossible to remove all the malwares
- we need to **study another approach** as well

Public Terminal: ATM



Public Terminal: ATM



<http://www.snopes.com/fraud/atm/atmcamera.asp>



Fabricated Terminal



Skimming devices!!



Fabricated Terminal



Small camera!!



<http://www.snopes.com/fraud/atm/atmcamera.asp>

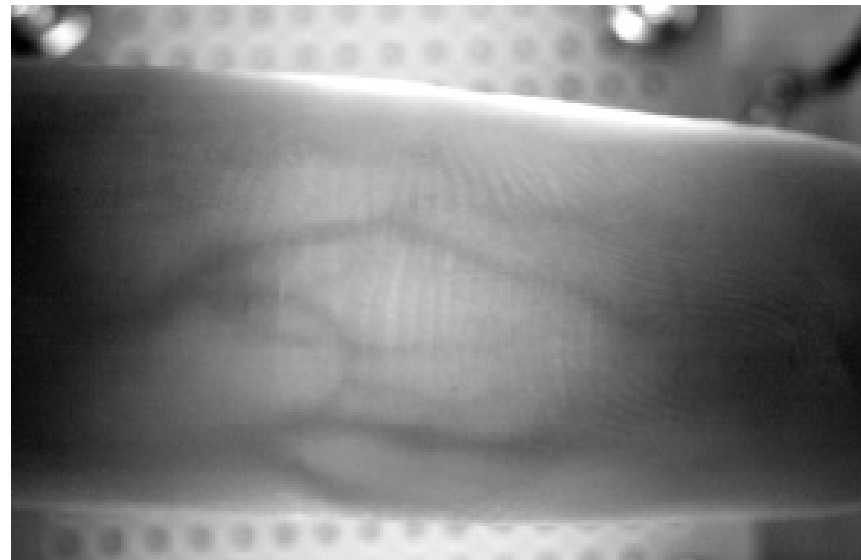
Countermeasures Against Fabricated Terminals

- Supervising terminals
 - Does not work against unsupervised terminals
 - ◆ Easy to place fake terminals somewhere
 - Not easy to remove all the fabrications immediately
- Employing more advanced authentication against both skimming and peeping
 - ◆ One-time password
 - ◆ Smart card
 - ◆ Biometrics (not necessarily advanced)
 - Advanced authentication does not work against more advance hijacked terminals

Biometrics information can be copied



Copied fingerprint
using gummy candy



Vein pattern taken by a
infrared camera

T. Matsumoto “On Biometrics for Financial Transactions (in Japanese)”,
http://www.fsa.go.jp/singi/singi_fccsg/gaiyou/f-20050415-singi_fccsg/02.pdf

- It is also possible to attach a sheet of cellophane on fingers, on which other’s fingerprint pattern is printed.

Advanced Hijacked Terminals

- Are not necessarily interested in stealing identity of users anymore but in making money directly by modifying critical e-transactions
 - By altering users' inputs and displayed information to the users after a user logs in the system

Example of attacking on remittance

Adversary

1. Waits until a user logs in the system and remit money.



2. remit \$10000
to 1234567



3. remit \$10000
to **4819231**

Banking
Server



5. OK to remit
\$10000 to **1234567** ?

Hijacked
Terminal

4. OK to remit
\$10000 to **4819231** ?

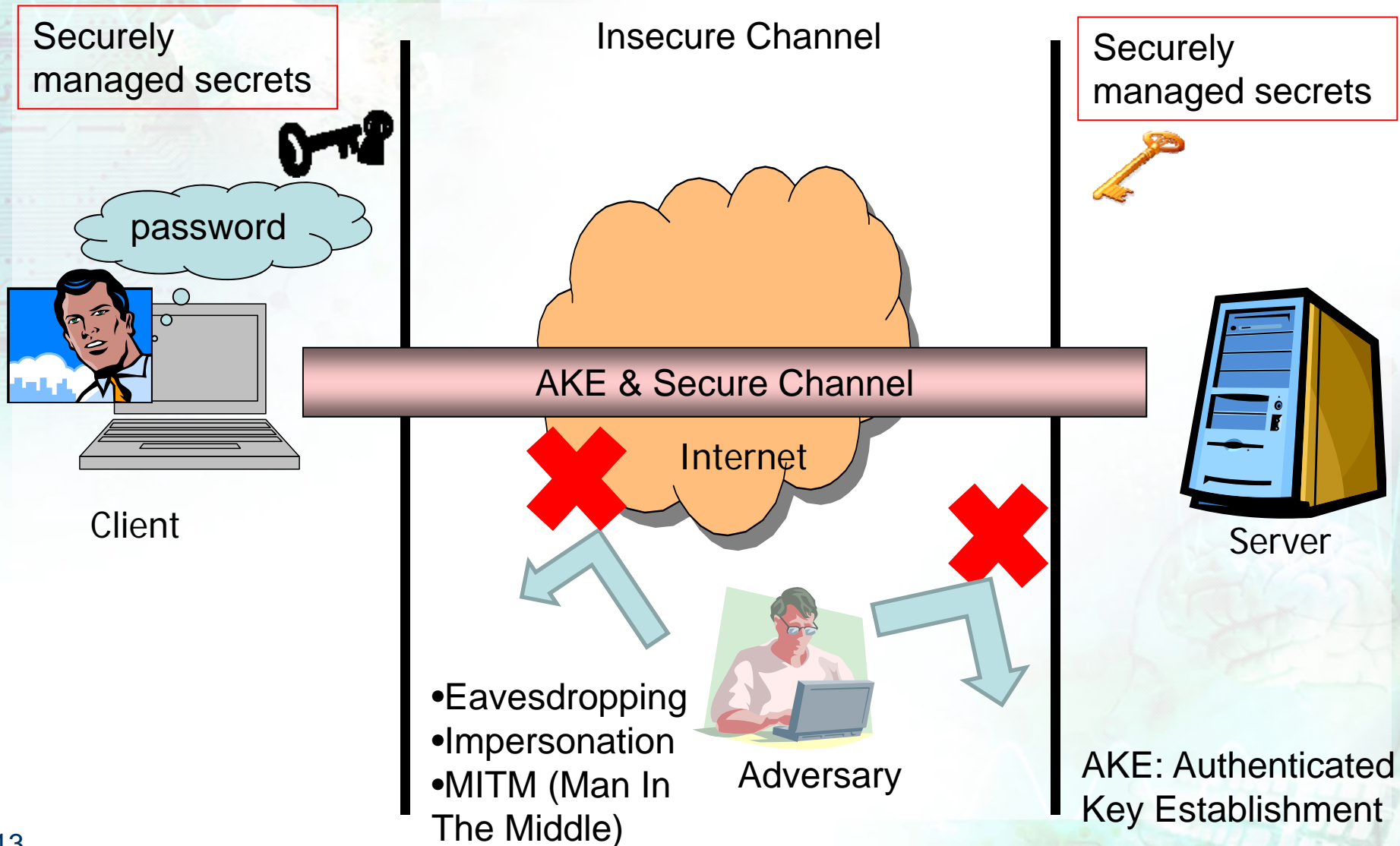
6. OK

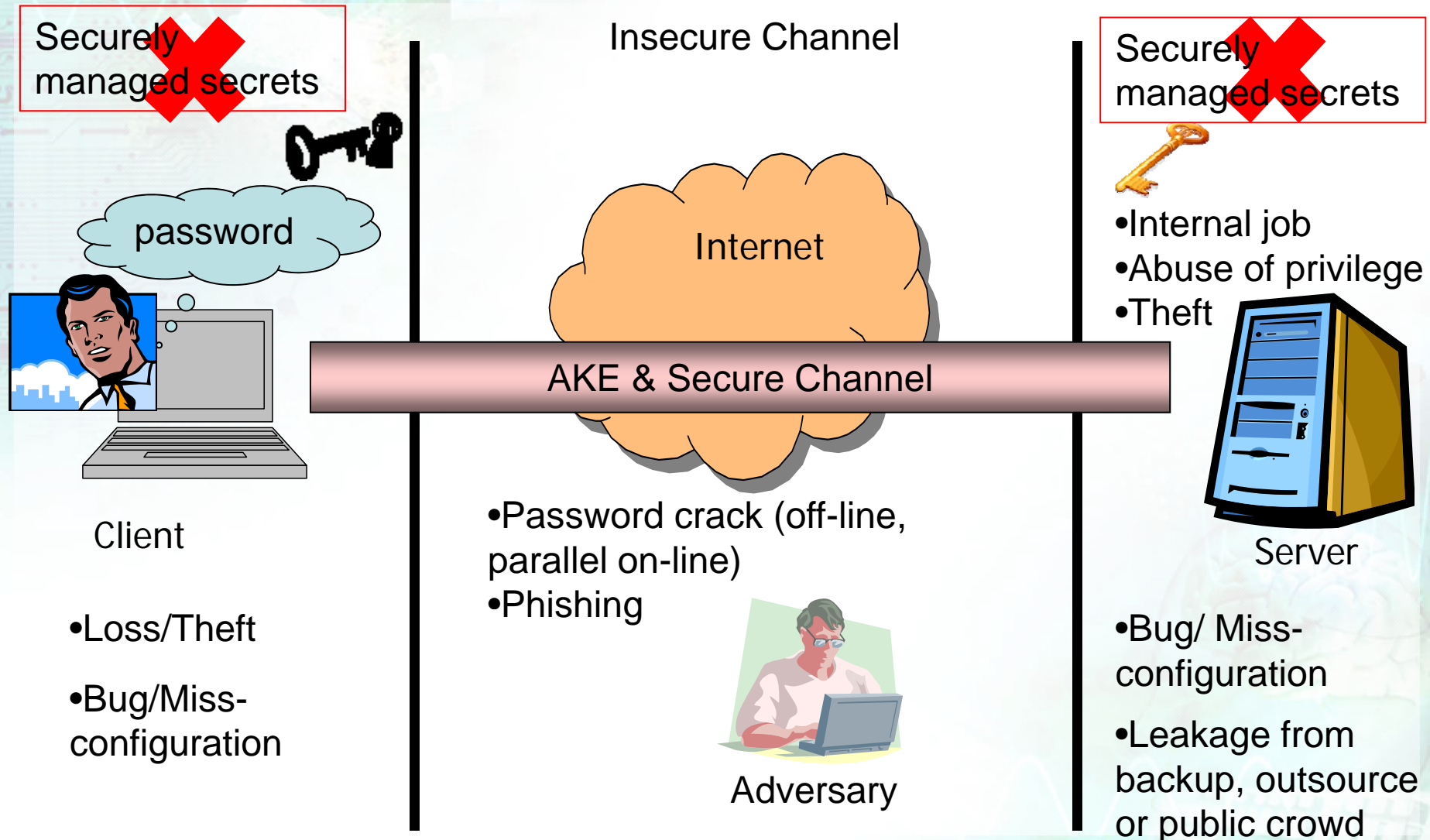
Secure Channel



Money is illegally transferred !

Against insecure channels, AKE plays an important role

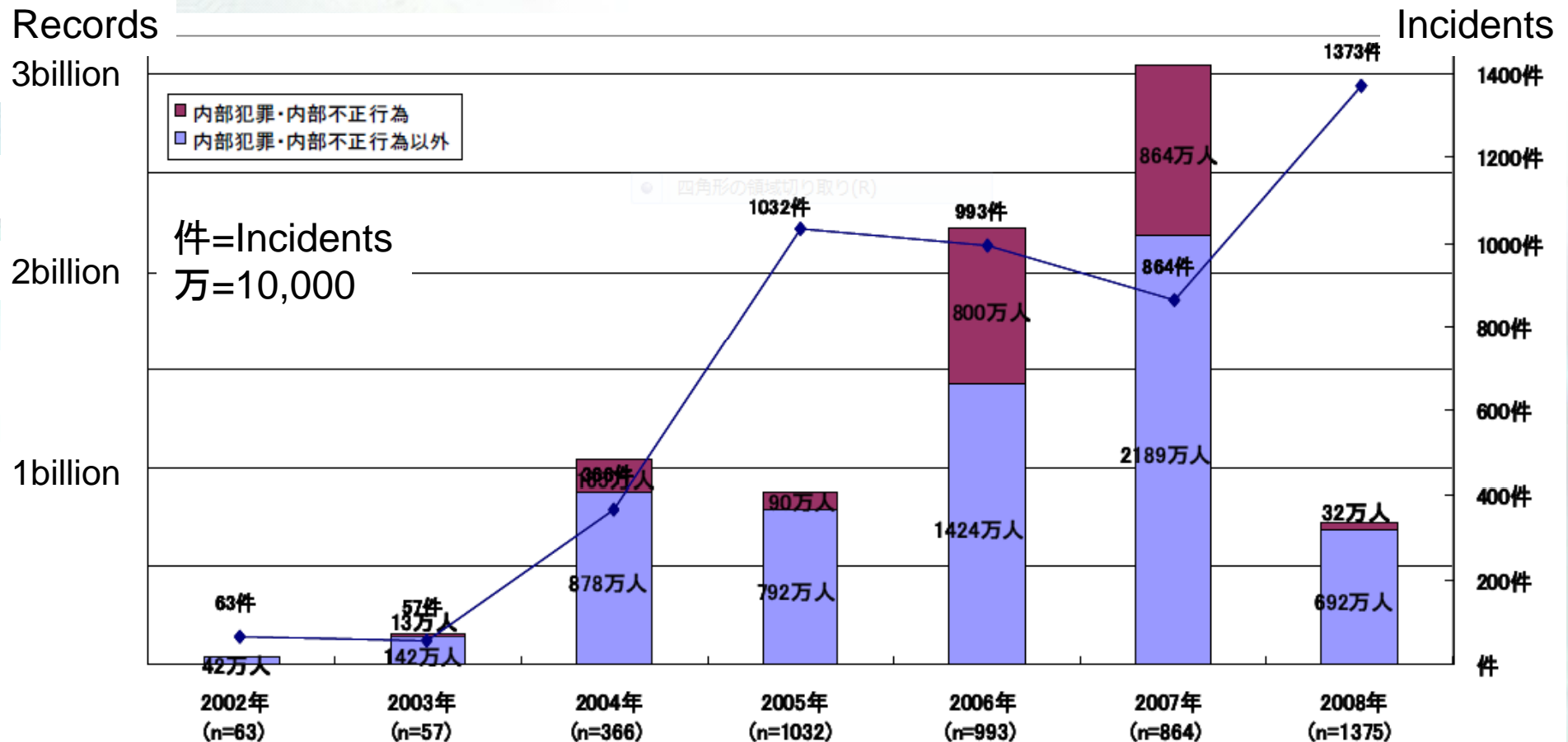




of information leakage incidents in Japan

“(Ref) JNSA2008 Report on Information Security Incidents”, ver. 1.3

of leaked records/incident: 5,668
Expected compensation/record: \$460
Expected compensation/incident: \$2 million



Countermeasures Against Leakage

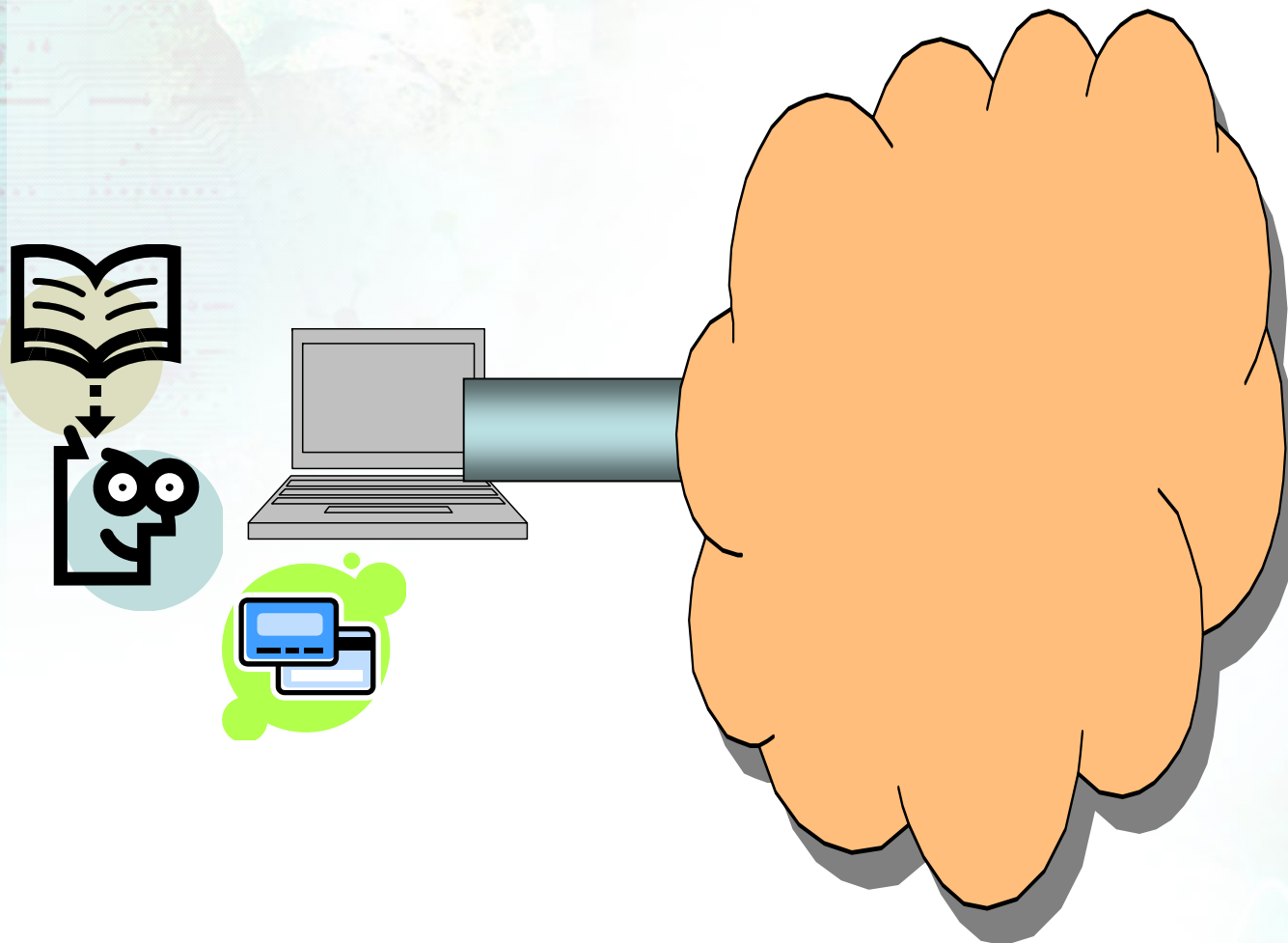
- Enhancement of Tamper Resistance against side channel attacks
 - while taking the cost into account
- Making cryptosystems resist against key leakage
 - so far a lot of schemes have been proposed for
 - ◆ Cryptographies
 - ◆ Digital signatures
 - ◆ AKEs (Authenticated Key Establishments)
 - Putting them into practical use seems important.

LR-AKE (Leakage-Resilient AKE)

- We have been studying on Leakage-Resilient AKEs since around 2000 [SKI03,SKI07]
 - Our schemes resist against **full leakage of stored secrets**
 - Whereas recent LR-AKEs resist against only **partial key leakage**

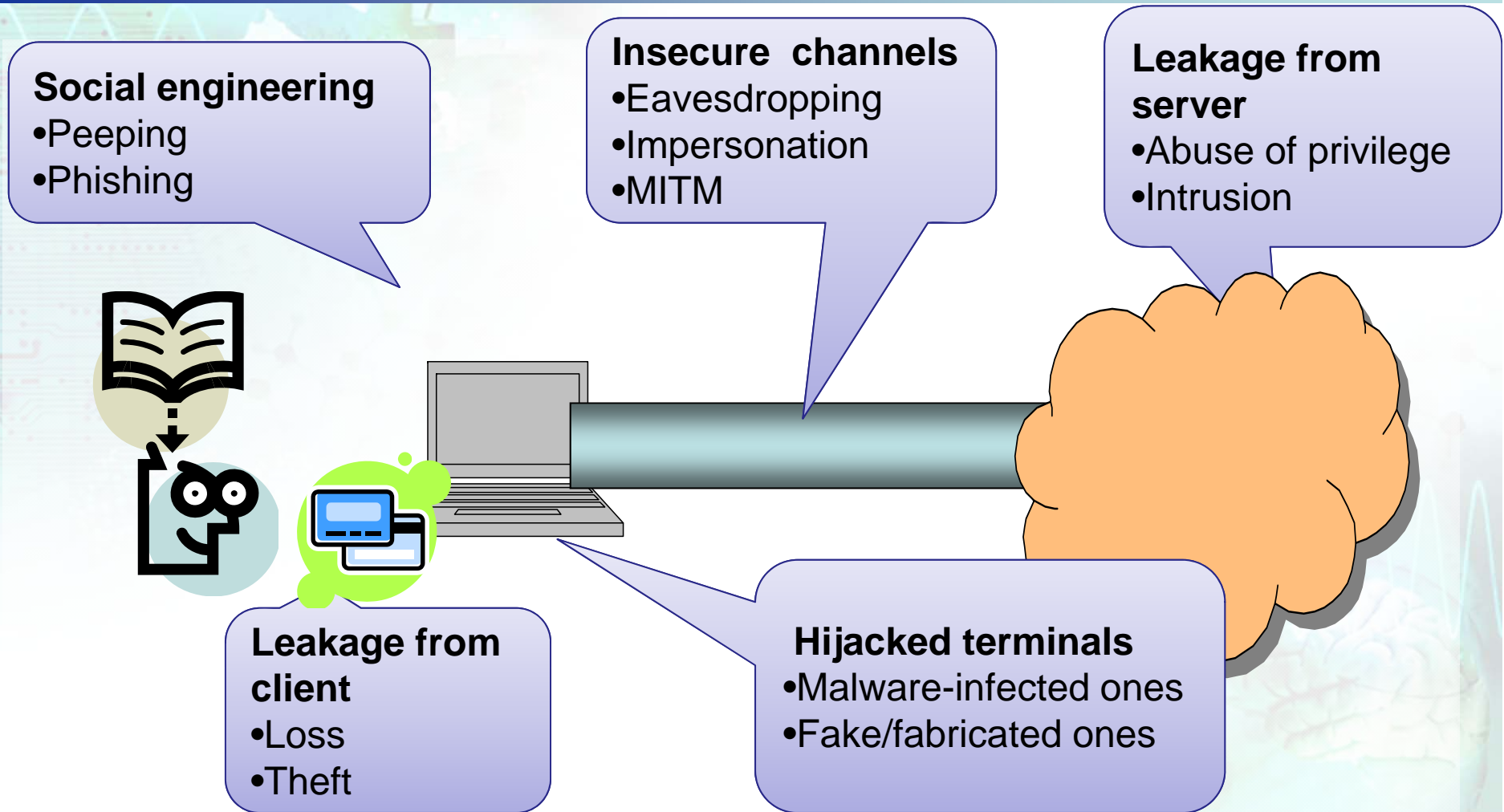
[SKI03] S. H. Shin, K. Kobara, and H. Imai, "Leakage-resilient authenticated key establishment protocols," Proc. of ASIACRYPT 2003, LNCS 2894, pp.166-172, 2003
[SKI07] S. H. Shin, K. Kobara, and H. Imai, "An Efficient and Leakage-Resilient RSA-Based Authenticated Key Exchange Protocol with Tight Security Reduction", IEICE Trans. Vol. E90-A, No. 2, pp. 474-490, 2007

Most of services are provided via network



- Web banking
- Online trading
- Intra access
- Net shopping
- Net auction
- ...

Risks Around Network Services



Security of a total system depends on the weakest part. So we need to promote the studies to improve the weakest part.