– Case Study –

Efforts to Secure Electronic Financial Transactions

in Korea

2008. 6. 27

20th FIRST Annual Conference

jwchoi@fsa.or.kr

Contents

I. Introducing FSA & KFCERT

1. Background

- Government decided to set up a organization dedicated to secure electronic financial transactions after the first internet banking incident in may, 2005
- It is also decided to operate an integrated OTP center for the financial companies

2. FSA

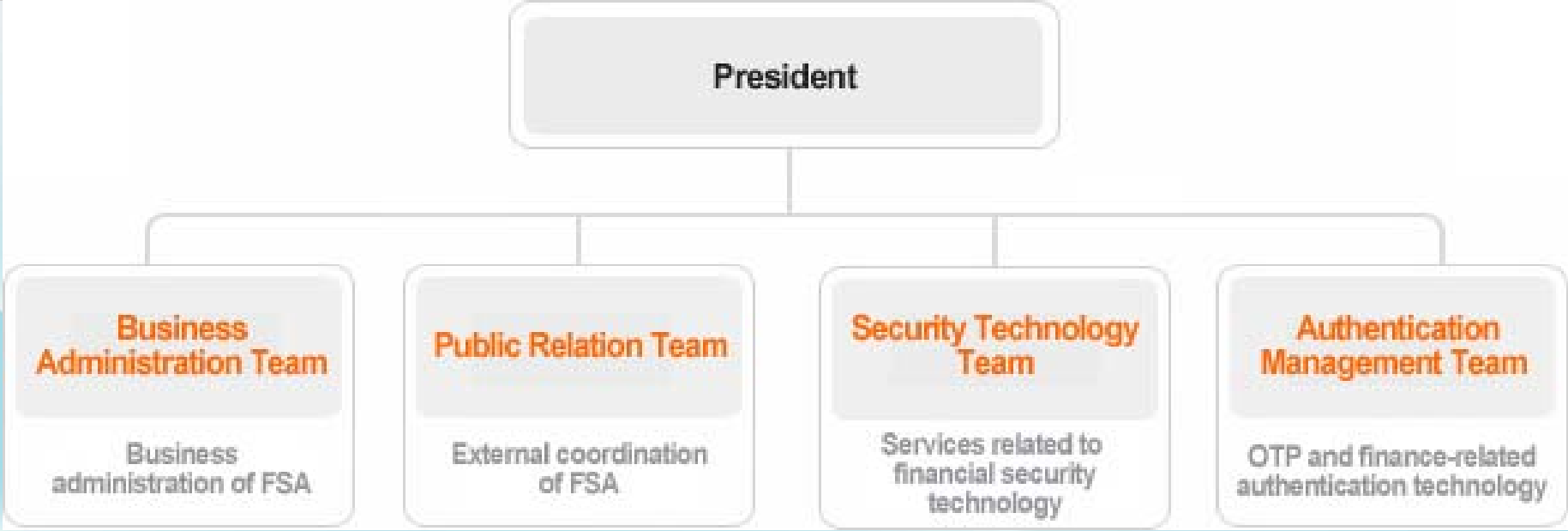
- FSA is a non-profit organization initiated by government (Financial Services Commission)
- Established in December, 2006
- Has 129 member financial companies including Banks, Security Companies, Credit Card Companies, Insurance Companies and others.

I. Introducing FSA & KFCERT

3. KFCERT

- Korea Financial CERT is a part of FSA
- Response financial incidents and monitors threat information
- Is a FIRST full member since December, 2007

4. Organization



5. History

- 2005. 5 : Internet banking incident occurred using keylogger and backdoor for the first time in Korea
- 2006.12.21 : Financial Security Agency started its work
- 2007.1.17 : Joined Anti-Phishing Working Group
- 2007.1.19 : New pharming incident occurred using malware
- 2007.1.29 : KFCERT has created
- 2007.1.31 : Joined CONCERT (CONsortium of CERT)
- 2007. 2. 9 : Joined Korea National CERT Council
- 2007.3.27 : Joined MS SCP (Security Cooperation Program)
- 2007.12.20 : Joined FIRST

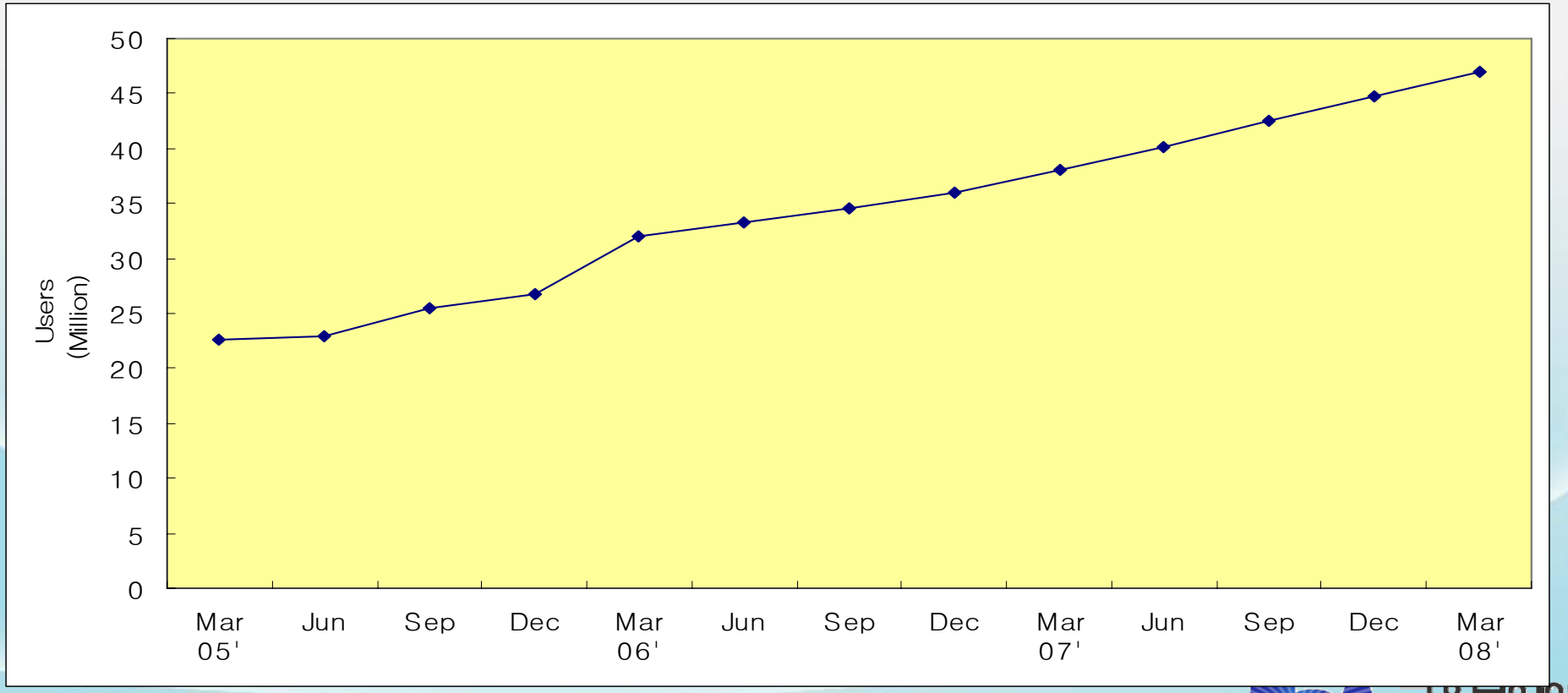
6. Role and Responsibility of FSA

- Support developing security policy and counter plans
- Incident Response
- Vulnerability Analysis
- Penetration Test
- Product Conformity Test
- Operate Integrated OTP Center
- Coordinate other financial companies
- Cooperate with other security organization and law enforcement

II. Electronic Transactions in Korea

1. Internet banking in Korea (Number of Users)

- Internet banking users are 47 Million
- Mobile banking users are 5.7 Million
- 12 Million digital certificates issued

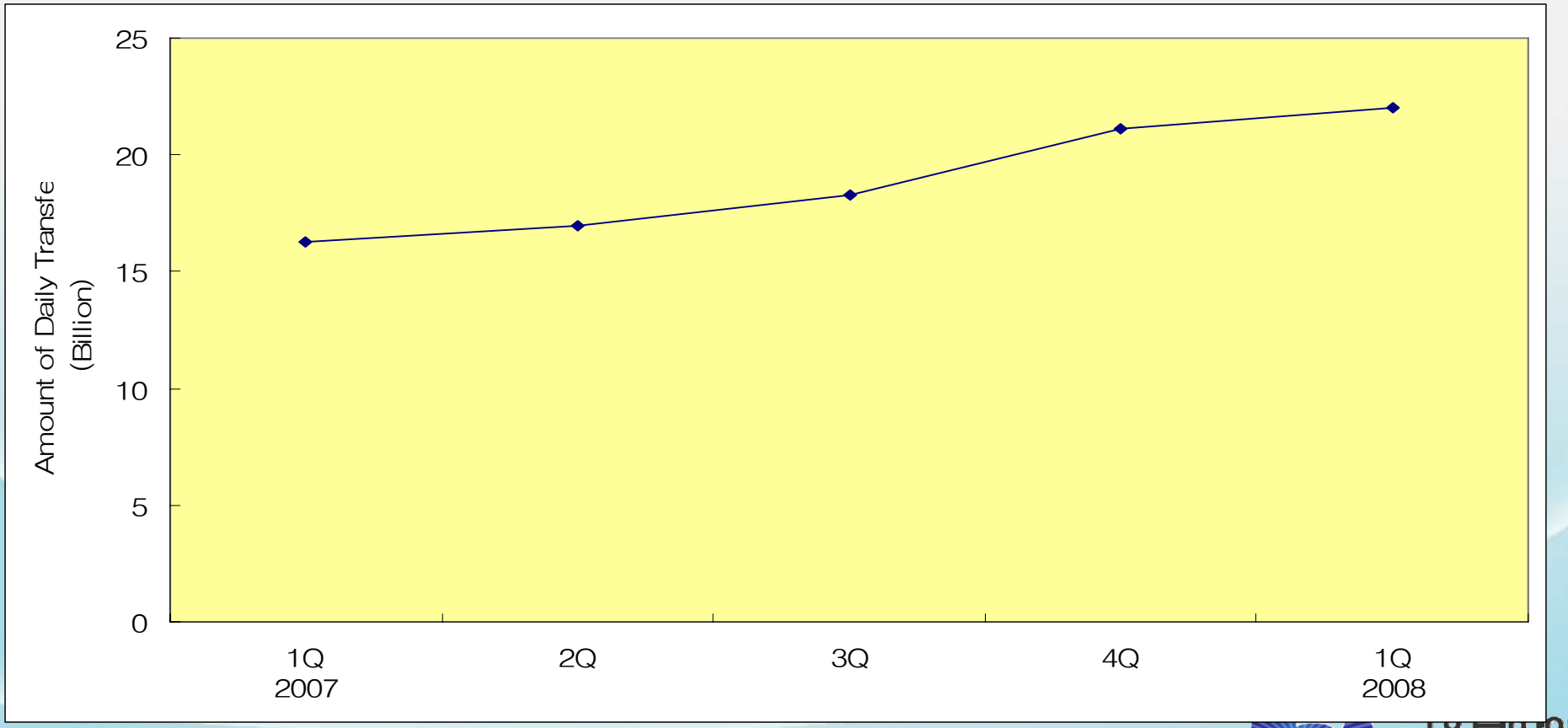


* Source : Bank of Korea

II. Electronic Transactions in Korea

1. Internet banking in Korea (Amount of Transfers)

- Daily transfers hit 21 Million (Number of Transfers)
- Daily transfers reach 22 Billion USD (Approx.)

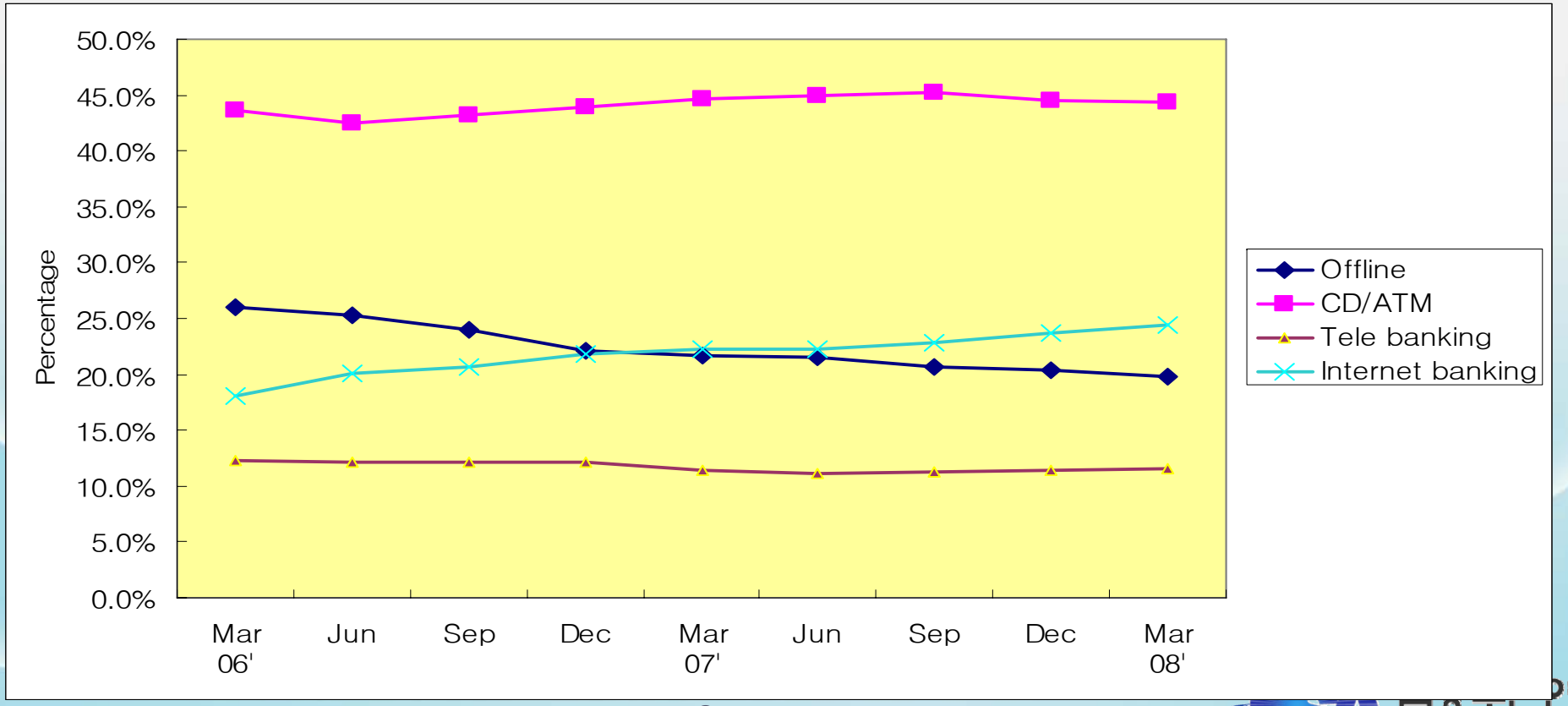


* Source : Bank of Korea

II. Electronic Transactions in Korea

2. Transaction portion for each channel

- CD/ATM's are the most popular channel
- Internet banking transactions (transfers) are increasing(24.4%)
  - * Inquiry only in internet banking reaches 56.8%



* Source : Bank of Korea

II. Electronic Transactions in Korea

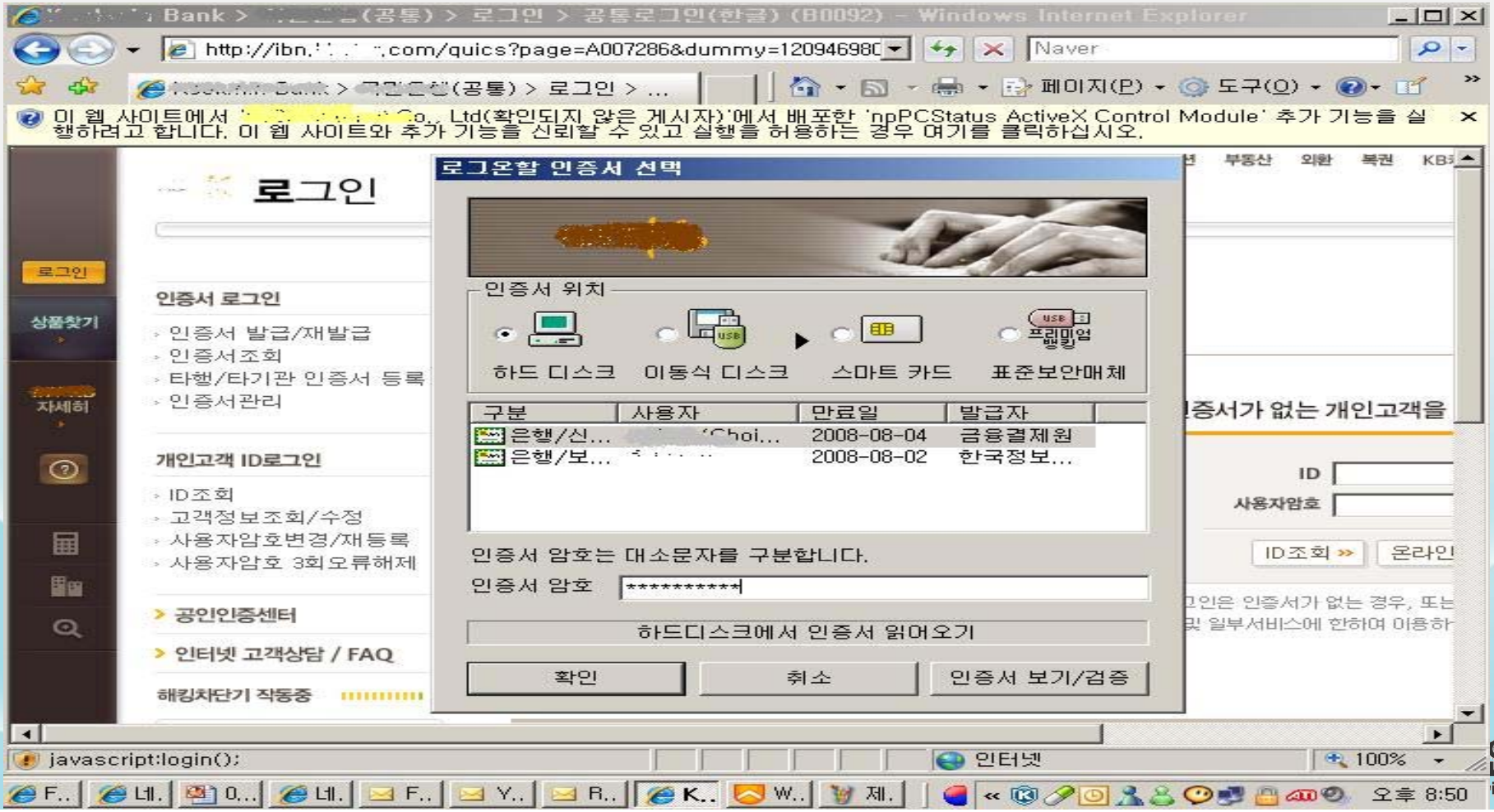
3. Security programs in internet banking(1)

➲ Anti-Keylog / AntiVirus / Encryption should be provided

II. Electronic Transactions in Korea

3. Security programs in internet banking(2)

➲ Digital certificate



II. Electronic Transactions in Korea

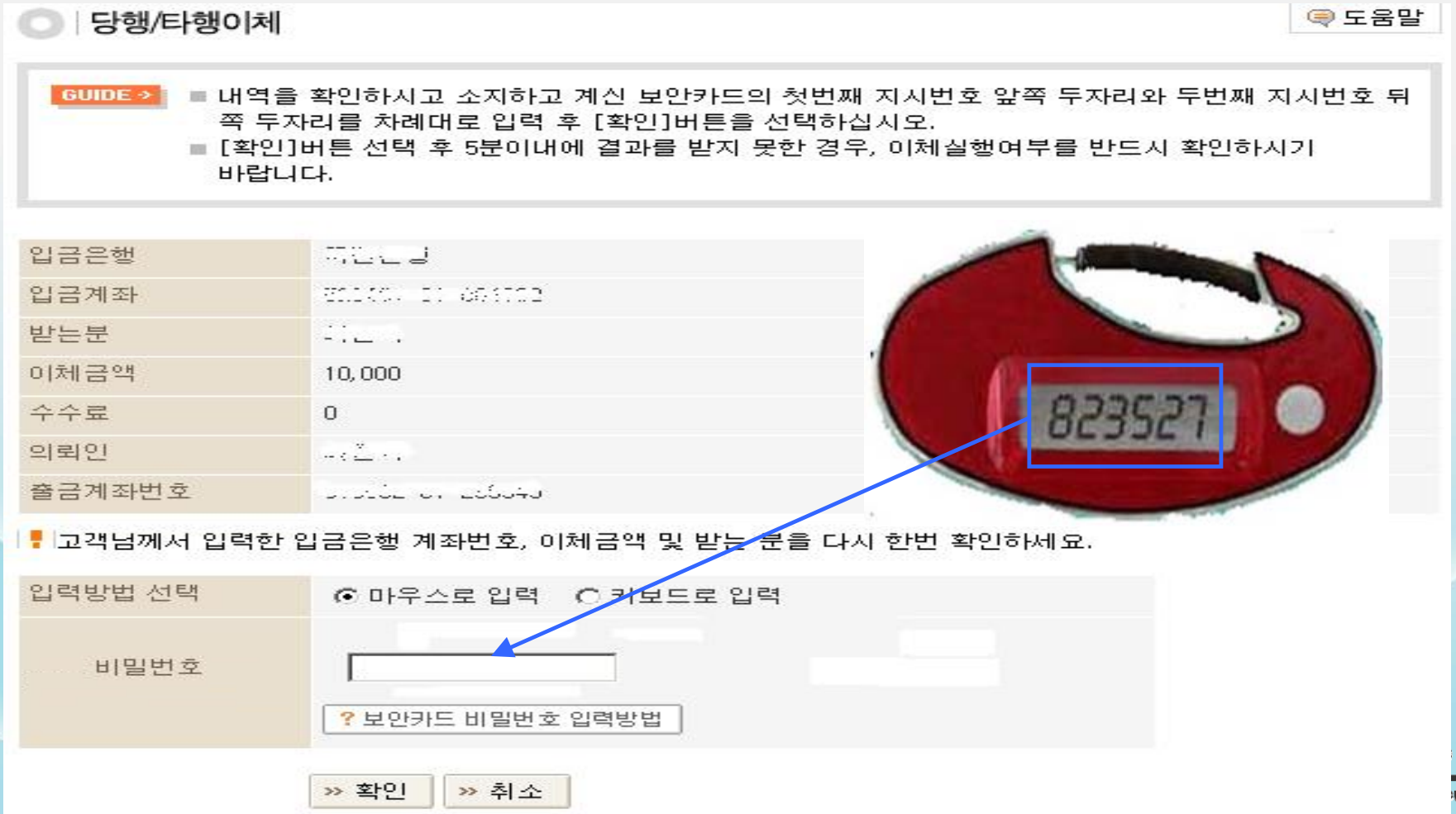
3. Security programs in internet banking(3)

➲ Security Card (Random Number)

II. Electronic Transactions in Korea

3. Security programs in internet banking(4)

➲ OTP (One Time Password) : Valid only for 1 minute



II. Electronic Transactions in Korea

4. Related Law & Policy(1)

➲ Back grounds of Electronic Financial Transaction Act

- Absence of regulation on the electronic transactions
- Need customer safeguards due to the increasing incident
  . Hard to prove the responsibility for the incident
  . Heavy responsibility to the customers
- Rack of supervise to the companies dealing with electronic transactions which is not a financial company

➲ Supervise more electronic financial services

➲ More responsibility to the incidents

➲ Protect the Customers

II. Electronic Transactions in Korea

4. Related Law & Policy(2)

➲ Electronic Financial Transaction Act (Article 9)

- Financial Institutions are basically responsible for transaction incidents except the user's intention and negligence
- Financial Institutions must prove user's negligence

➲ Electronic Financial Transaction Act (Article 22)

- Financial institutions should store related logs to trace and search the transaction within 5 years

II. Electronic Transactions in Korea

4. Related Law & Policy(3)

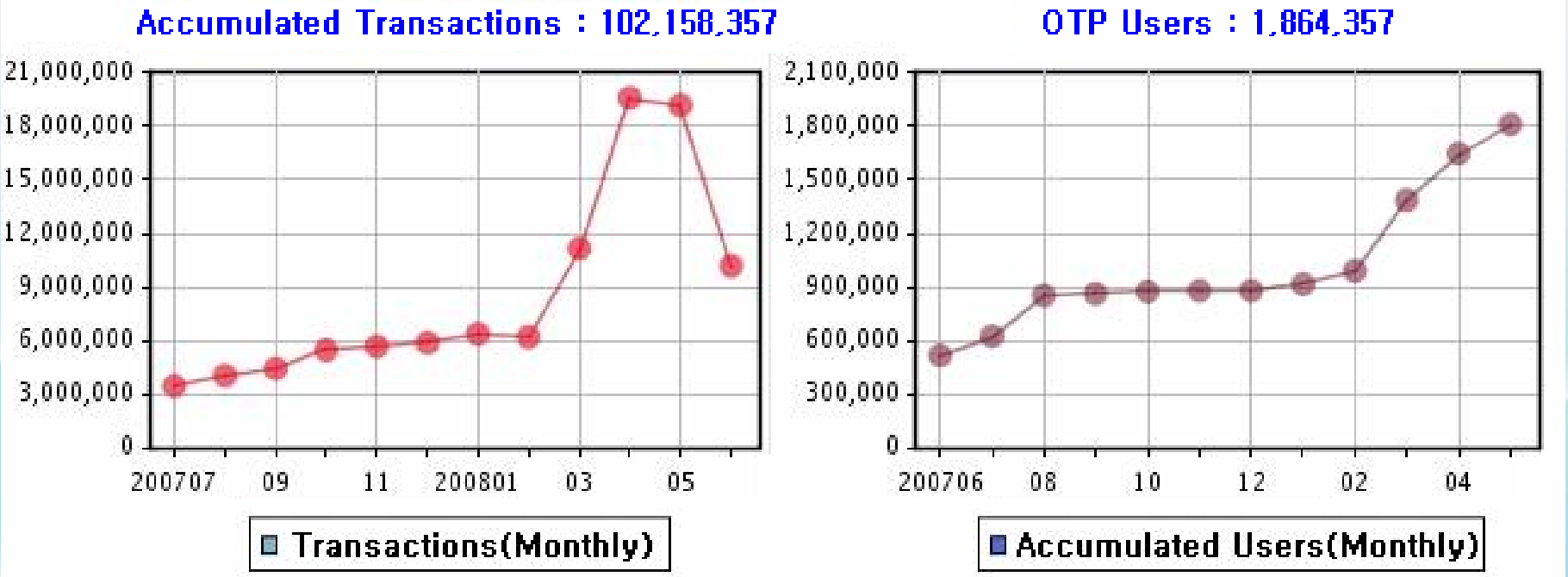
➲ Transaction limit for each security level (08′ April)

Security Level	Security Measure	Transfer Limit (USD, approximately)	
		Each	A Day
Level 1	OTP + Certificate	100,000	500,000
	HSM(Certificate) + Security Card		
	Security Card + Certificate + 2 Channel Authentication		
Level 2	Security Card + Certificate + SMS Notice	50,000	250,000
Level 3	Security Card + Certificate	10,000	50,000

II. Electronic Transactions in Korea

5. Integrated OTP Authentication center

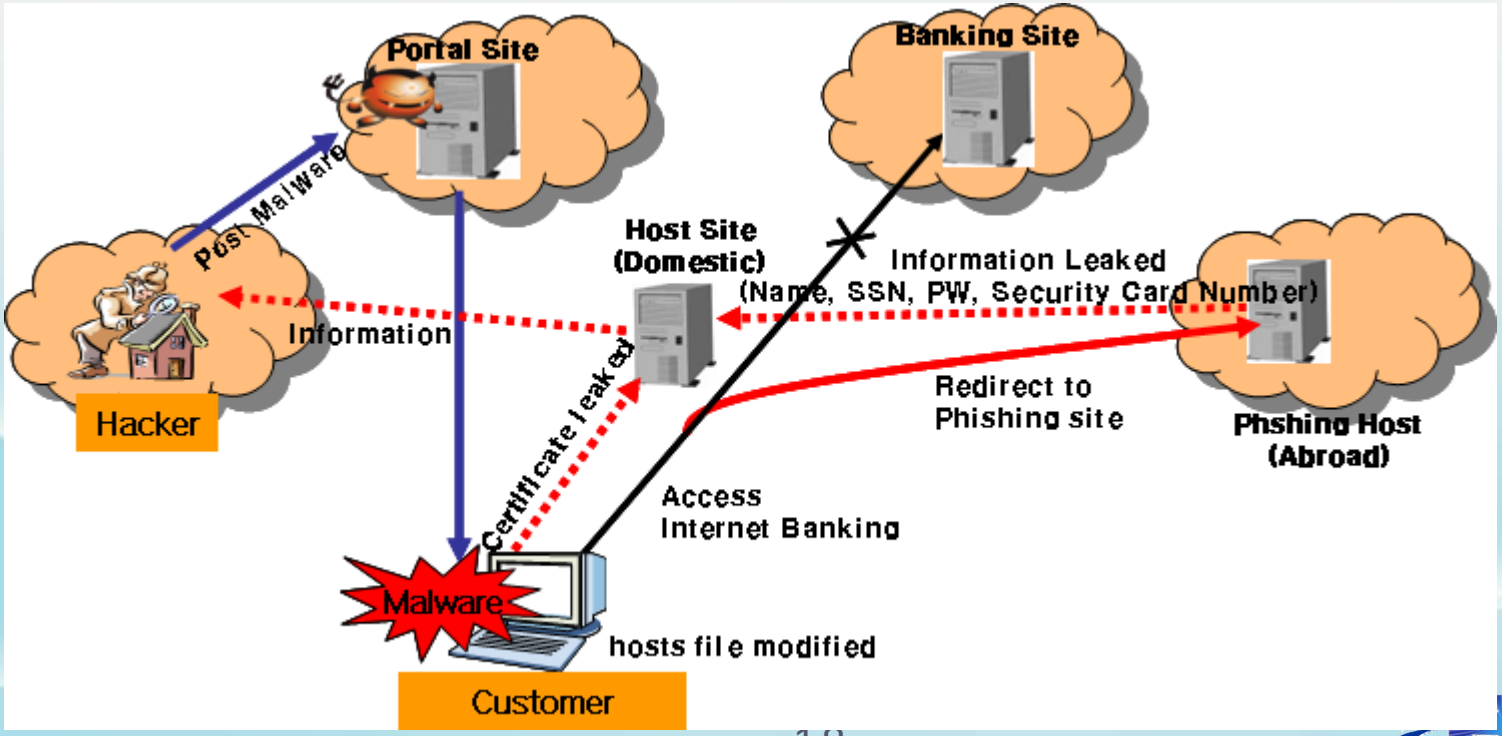
- FSA operates Integrated OTP Authentication center 24x7
- 55 Financial institutions joined integrated center
  (19 Banks, 30 Security Companies, etc)
- Users can use all financial institutions with only one OTP token



III. Incident Cases

1. Pharming with Malware (07'Jan)

- Malware distributed through portal site
- Unpatched PCs are infected, 'hosts' file was modified for pharming
- Host site was storing 4,000 certificates
- No economical loss due to quick response



III. Incident Cases

2. Internet payment incident (07'Apr)

- Internet payment system(V3D-Secure) should check CVC code
- 111 Credit card number were used for 6 month
- Had about 100,000 USD loss in a institution that didn't check the CVC
- Password for the payment were guessed easily

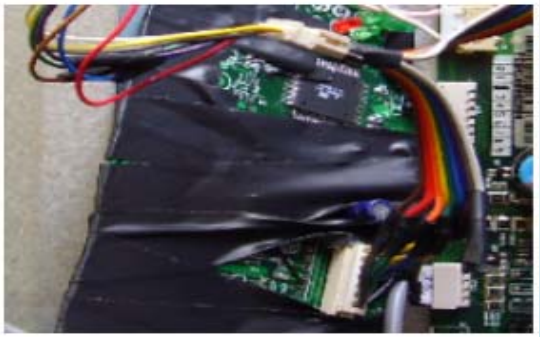
III. Incident Cases

3. Card Duplication (07'Apr)

- ATM owner installed a duplication reader in the ATM
- Passwords were recorded with hidden camera
- Stored card information was used to duplicate for fraudulent withdrawal

Card Tapping

Skimming



Tapping

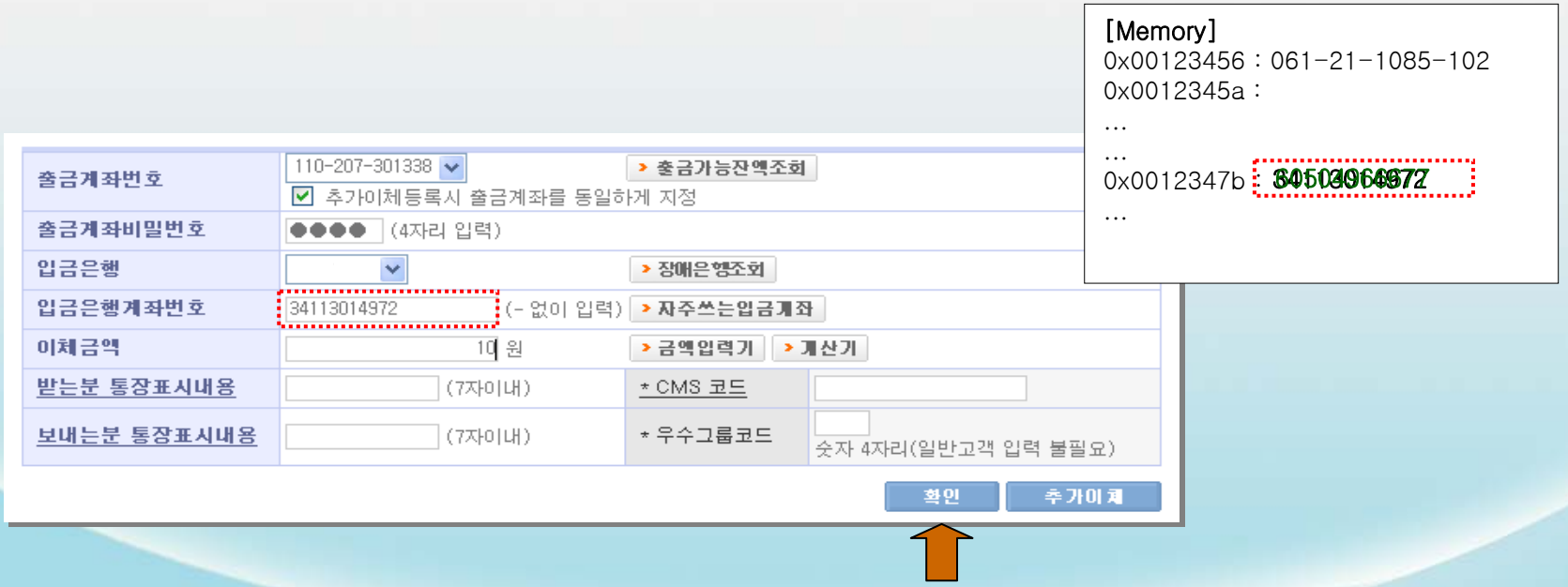
Hidden Camera

Fake PinPad

IV. New threats

1. Memory Forgery

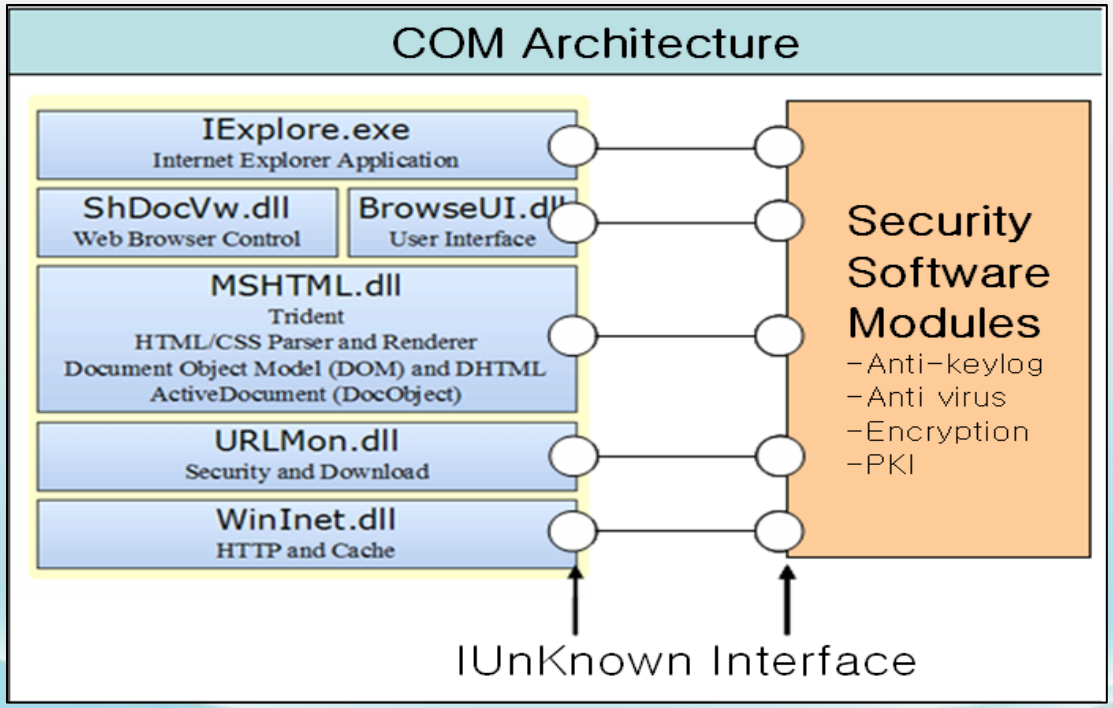
- Malware is also able to alter memory of IE allocation
- So that the hacker modifies account number which will be transferred
- But the HTML screen prompts that the transfer was successful



- Account Number '34113014972' will be changed to the hacker's account number '60504966677' on clicking 'OK'.

2. COM Hooking

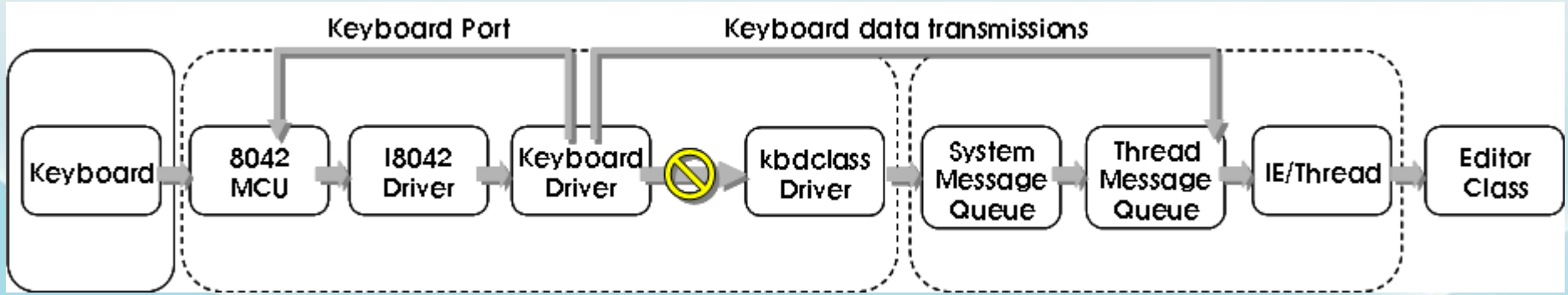
- Almost every online software use ActiveX based on MS Windows COM(component object model)
- ActiveX is one of the technology that uses COM IUnKnown interface



- IUnKnown interface can be monitored so that the hacker can forge account information

3. Keyboard Logging

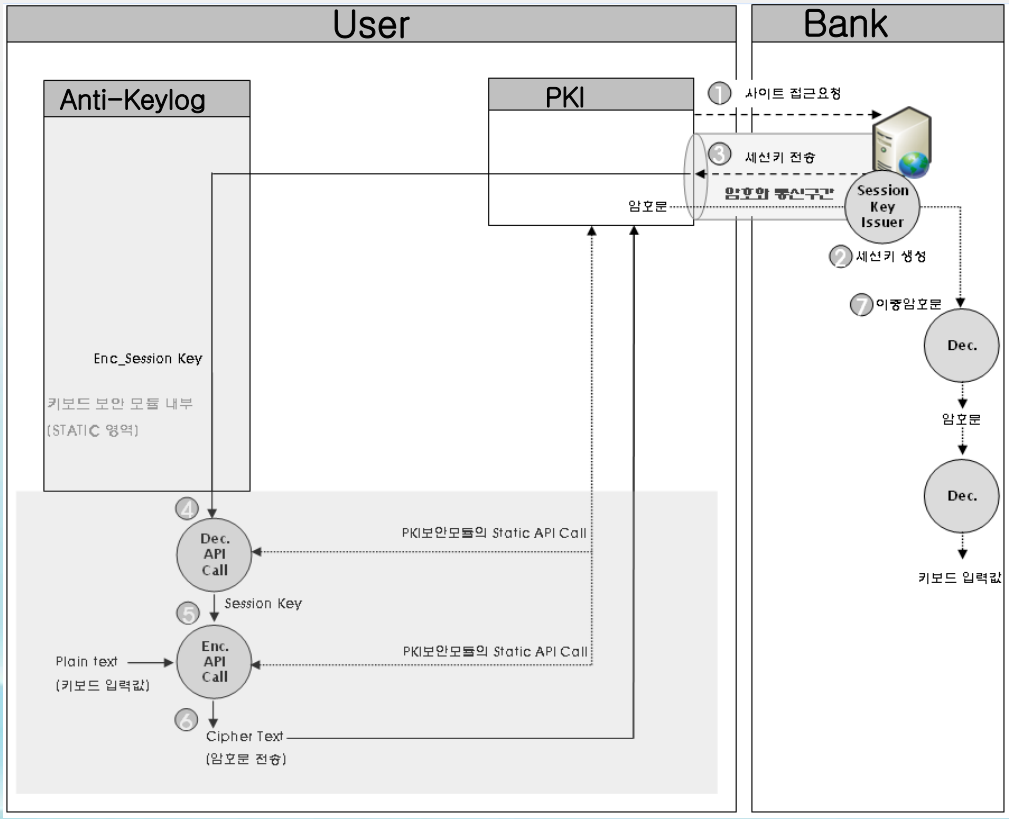
- Even though anti-keylog software protects many key loggers from logging the passwords,
- new hacking technology bypasses security technology
- It is necessary to monitor the technology and trends to develop complementary security measures



V. Countermeasures and Conclusion

1. Countermeasures(1)

➲ Recommend kernel level end-to-end encryption to prevent COM hooking and Memory forgery

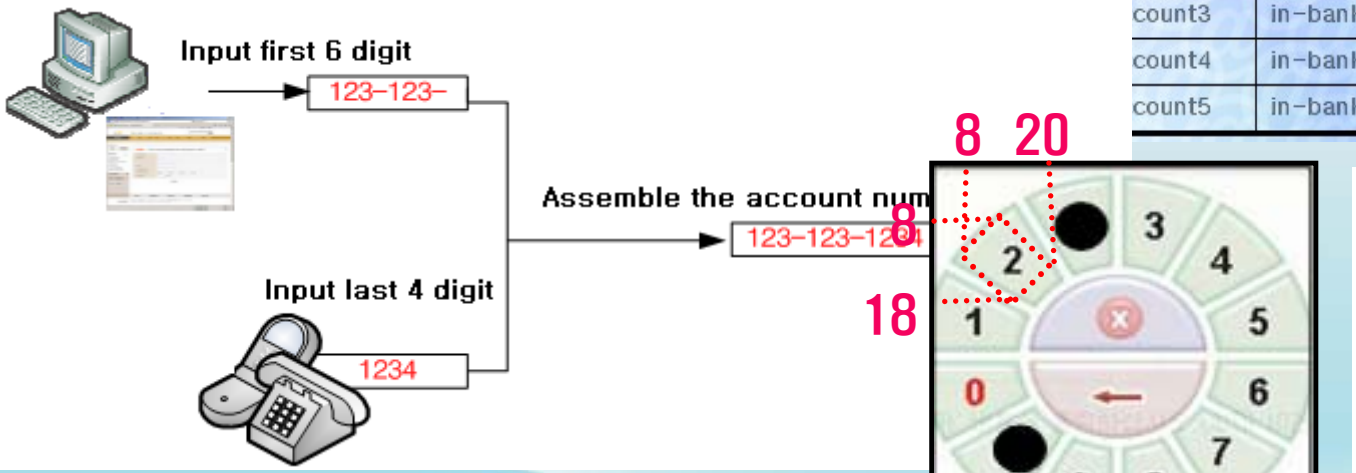


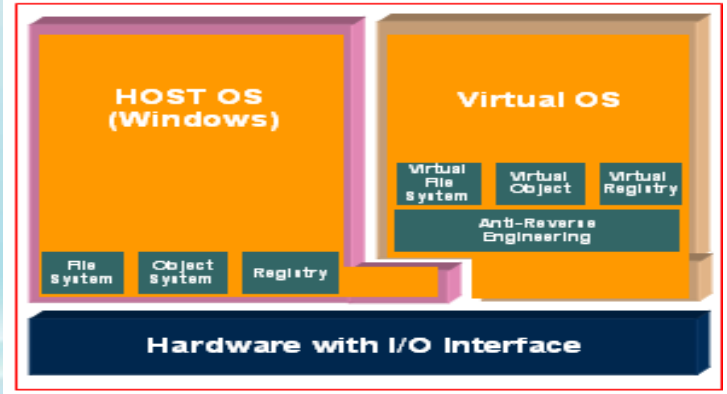
V. Countermeasures and Conclusion

1. Countermeasures(2)

- Research and recommend security solutions such as
  - Two channel authentication
  - Secure keypad
  - Secure image (Captcha)
  - Virtualization

출금계좌번호	입금은행	입금계좌번호	예금주	이체금액	수수료
out-account0	in-bank0	in-account0	in-owner0	out-money0	out-fee0
out-account1	in-bank1	in-account1	in-owner1	out-money1	out-fee1
out-account2	in-bank2	in-account2	in-owner2	out-money2	out-fee2
count3	in-bank3	in-account3	in-owner3	out-money3	out-fee3
count4	in-bank4	in-account4	in-owner4	out-money4	out-fee4
count5	in-bank5	in-account5	in-owner5	out-money5	out-fee5





금융보안연구원
Financial Security Agency

V. Countermeasures and Conclusion

2. Conclusion

- There's no perfect security
- Consistent efforts to cover the weakness are necessary
- Emphasis user the importance of security
- Financial institutions should do their best to care its customer safe
- Lead PC users to install security patches automatically (50~60% are patched)
  - Produce Flash animations, Patch site for financial customers

Thank You