



- Case Study -
Efforts to Secure
Electronic Financial Transactions
in Korea

2008. 6. 27
20th FIRST Annual Conference



금융보안연구원
Financial Security Agency

jwchoi@fsa.or.kr

Contents

I Introducing FSA & KFCERT

II Electronic transactions in Korea

III Incident cases

IV New threats

V Countermeasures & Conclusion

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

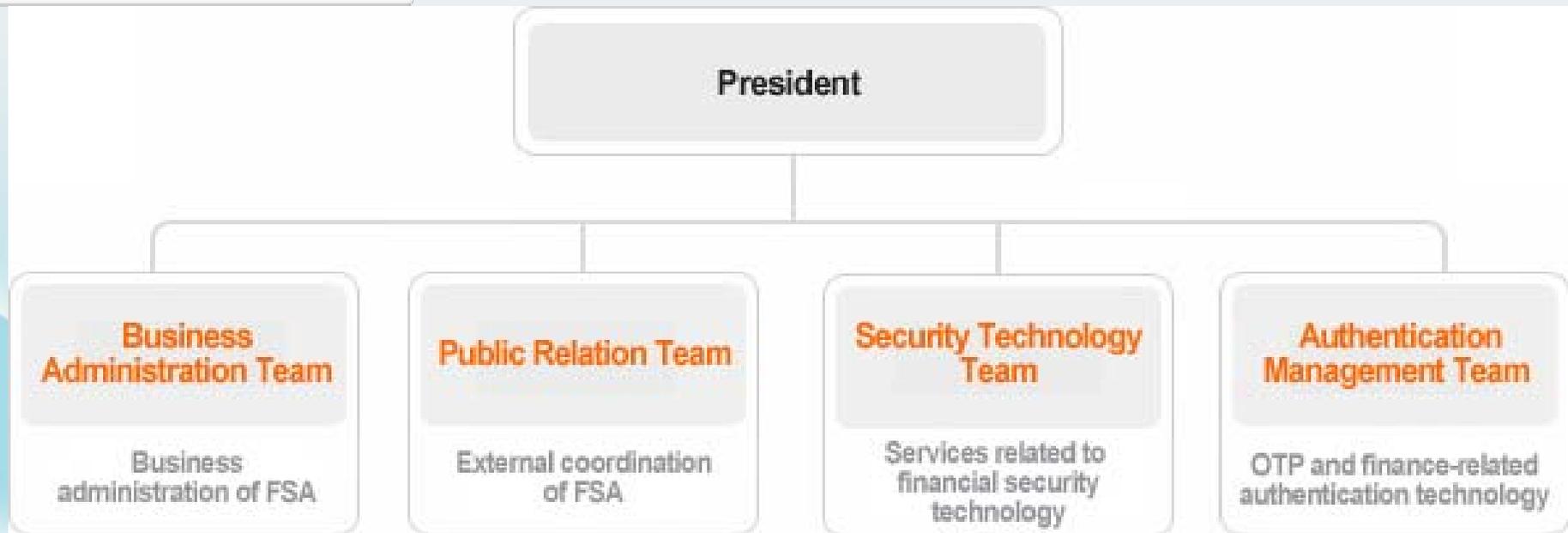
- ⇒ FSA is a non-profit organization initiated by government (Financial Services Commission)
- ⇒ Established in December, 2006
- ⇒ Has 129 member financial companies including Banks, Security Companies, Credit Card Companies, Insurance Companies and others.

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



I. Introducing FSA & KFCERT

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

I. Introducing FSA & KFCERT

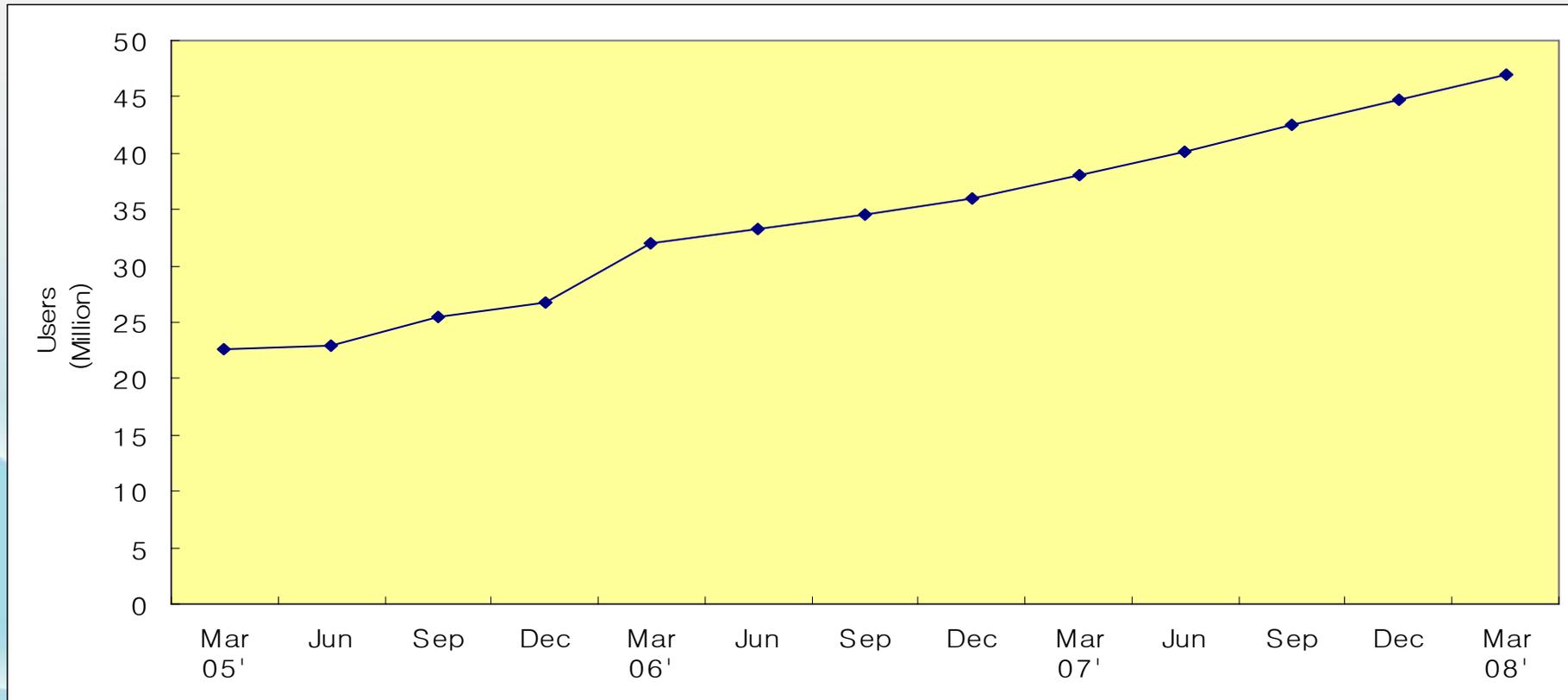
6. Role and Responsibility of FSA

- ⇒ 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

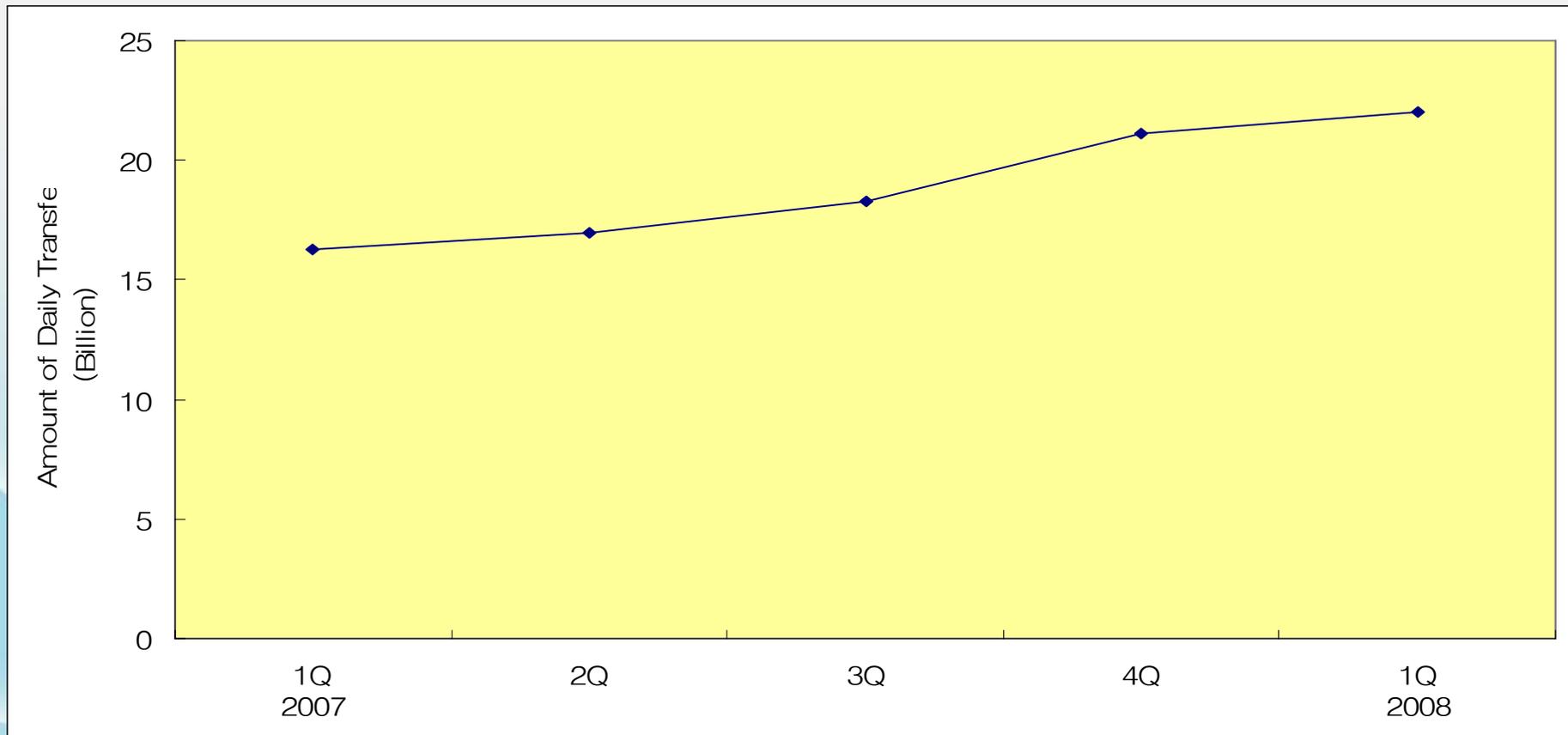


* Source : Bank of Korea

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.)

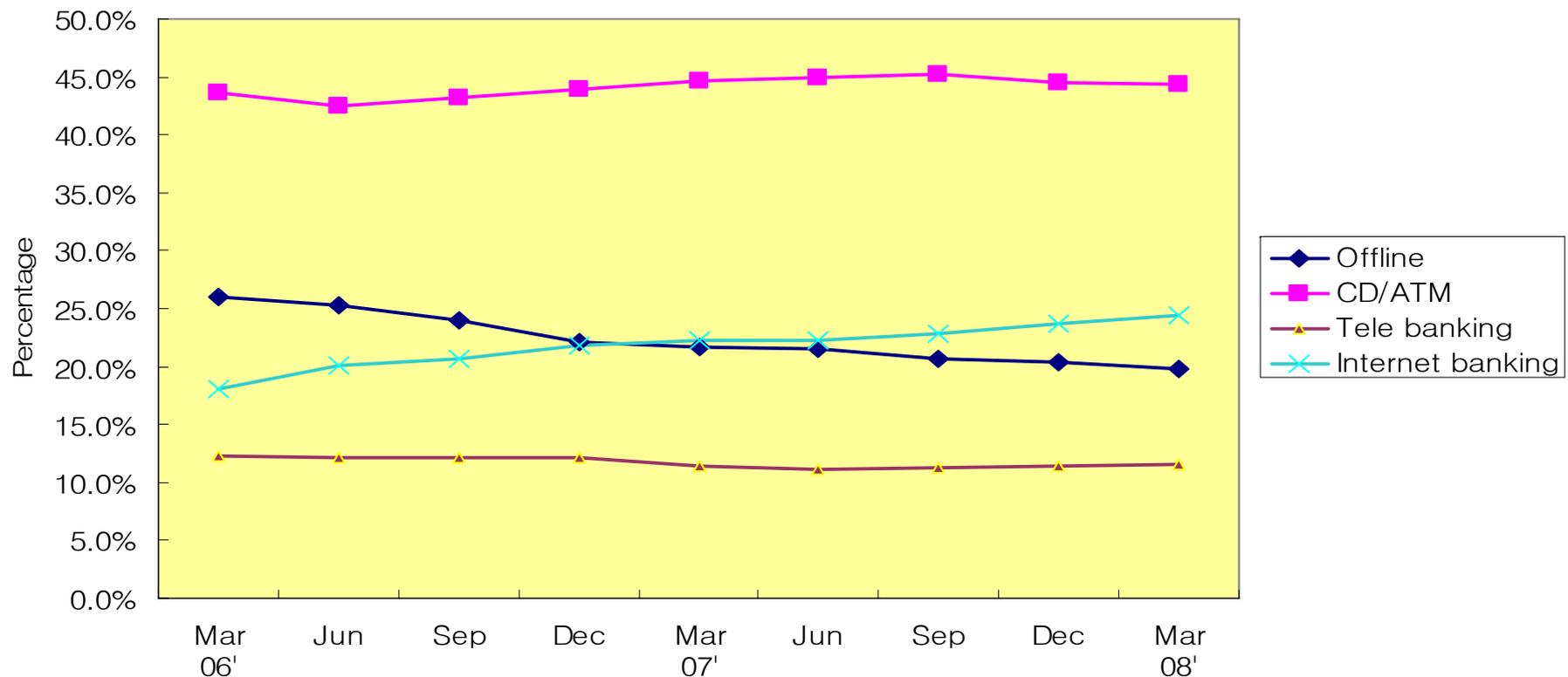


* Source : Bank of Korea

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

The screenshot shows a web browser window displaying the homepage of a Korean internet banking service. The browser's address bar shows the URL `http://ibn.kbs.or.kr/quics?page=s_ibn`. The website header includes navigation links for '인터넷뱅킹', '금융섹션', '부동산', '외환', '복권', and 'KB'. The main content area features a navigation menu with options like '조회', '이체', '신규/해지', '대출금입금/상환', '공과금납부', '사고신고', and '뱅킹사용자 관리'. A central banner displays the slogan '고객의 마음으로 더 가까이 다가하겠습니다.' and lists services such as '빠른조회 잔액/거래내역', '전예금 계좌조회', '당행 타행이체', '펀드 이체/이체예약', and '대학 등록금납부'. Below this, there are sections for '추천상품' and '추천서비스'. A red box highlights a '로그아웃' button in the left sidebar. Another red box highlights a '베스트상품관' (Best Product View) window in the bottom right, which displays a table with columns for '은행', 'IP Address', 'Port', and 'Process'. The table contains one entry: '신용협회은행' with 'IP Address', 'Port', and 'Process' fields, and a 'Process' value of 'nProtect Netizen V3 Build 4.11.1.68'. Below the table are buttons for 'Stop', 'Option', and 'Online Scan', along with the text '해킹 및 바이러스 차단을 하나로!'. A third red box highlights a '키보드 보안 동작중' (Keyboard Security Active) notification in the bottom right corner. The Windows taskbar at the bottom shows the system tray with the time '오후 8:45' and the '연구원' (Researcher) logo.

II. Electronic Transactions in Korea

3. Security programs in internet banking(2)

➔ Digital certificate

The screenshot shows a web browser window displaying a login page for a Korean internet bank. The page is titled "로그인" (Login) and features a "로그인할 인증서 선택" (Select Certificate for Login) dialog box. The dialog box has a header image of hands holding a document and lists four certificate types: "하드 디스크" (Hard Disk), "이동식 디스크" (Removable Disk), "스마트 카드" (Smart Card), and "표준보안매체" (Standard Security Medium). Below this is a table of installed certificates:

구분	사용자	만료일	발급자
은행/신...	Choi...	2008-08-04	금융결제원
은행/보...		2008-08-02	한국정보...

Below the table, there is a text input field for the certificate password, currently containing "*****". Buttons for "확인" (OK), "취소" (Cancel), and "인증서 보기/검증" (View/Verify Certificate) are at the bottom of the dialog. The background page shows a sidebar with navigation links like "로그인", "상품찾기", and "자세히", and a main content area with sections for "인증서 로그인" and "개인고객 ID로그인".

II. Electronic Transactions in Korea

3. Security programs in internet banking(4)

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

○ | 당행/타행이체

도움말

GUIDE >

- 내역을 확인하시고 소지하고 계신 보안카드의 첫번째 지시번호 앞쪽 두자리와 두번째 지시번호 뒤쪽 두자리를 차례대로 입력 후 [확인]버튼을 선택하십시오.
- [확인]버튼 선택 후 5분 이내에 결과를 받지 못한 경우, 이체실행여부를 반드시 확인하시기 바랍니다.

입금은행	국민은행
입금계좌	800000-01-000000
받는분	김민준
이체금액	10,000
수수료	0
의뢰인	김민준
출금계좌번호	800000-01-000000



! 고객님의 입력한 입금은행 계좌번호, 이체금액 및 받는분을 다시 한번 확인하세요.

입력방법 선택	<input checked="" type="radio"/> 마우스로 입력 <input type="radio"/> 키보드로 입력
비밀번호	<input type="password"/>
	? 보안카드 비밀번호 입력방법
	<input type="button" value="» 확인"/> <input type="button" value="» 취소"/>

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
- Lack 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)

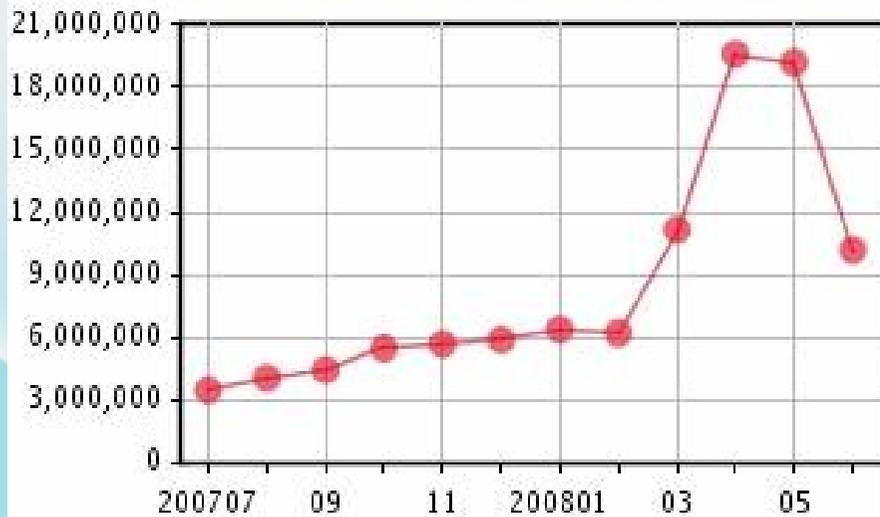
Security Level	Security Measure	Transfer Limit (USD, approximately)	
		Each	A Day
Level 1	OTP + Certificate	100,000	500,000
	HSM(Certificate) + Security Card		
	Security Card + Certificate + 2 Channel Authentication		
Level 2	Security Card + Certificate + SMS Notice	50,000	250,000
Level 3	Security Card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

II. Electronic Transactions in Korea

5. Integrated OTP Authentication center

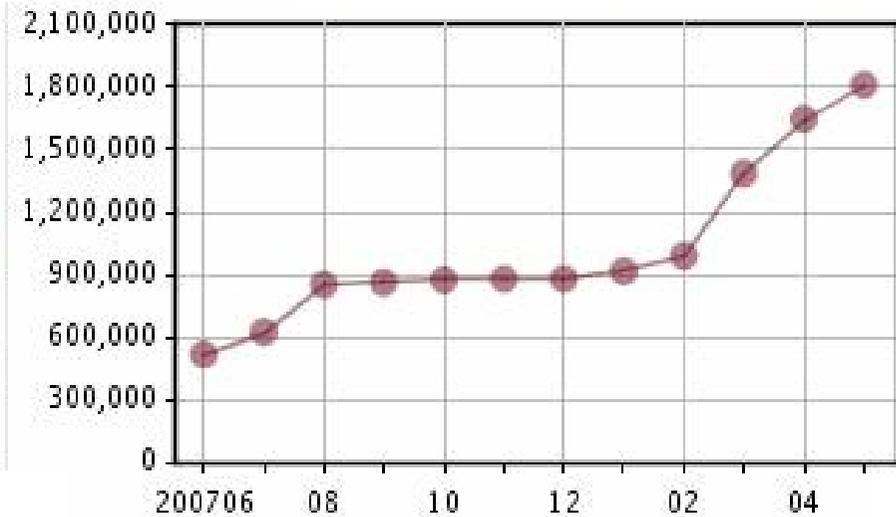
- ⇒ FSA operates Integrated OTP Authentication center 24x7
- ⇒ 55 Financial institutions joined integrated center
(19 Banks, 30 Security Companies, etc)
- ⇒ Users can use all financial institutions with only one OTP token

Accumulated Transactions : 102,158,357



■ Transactions(Monthly)

OTP Users : 1,864,357

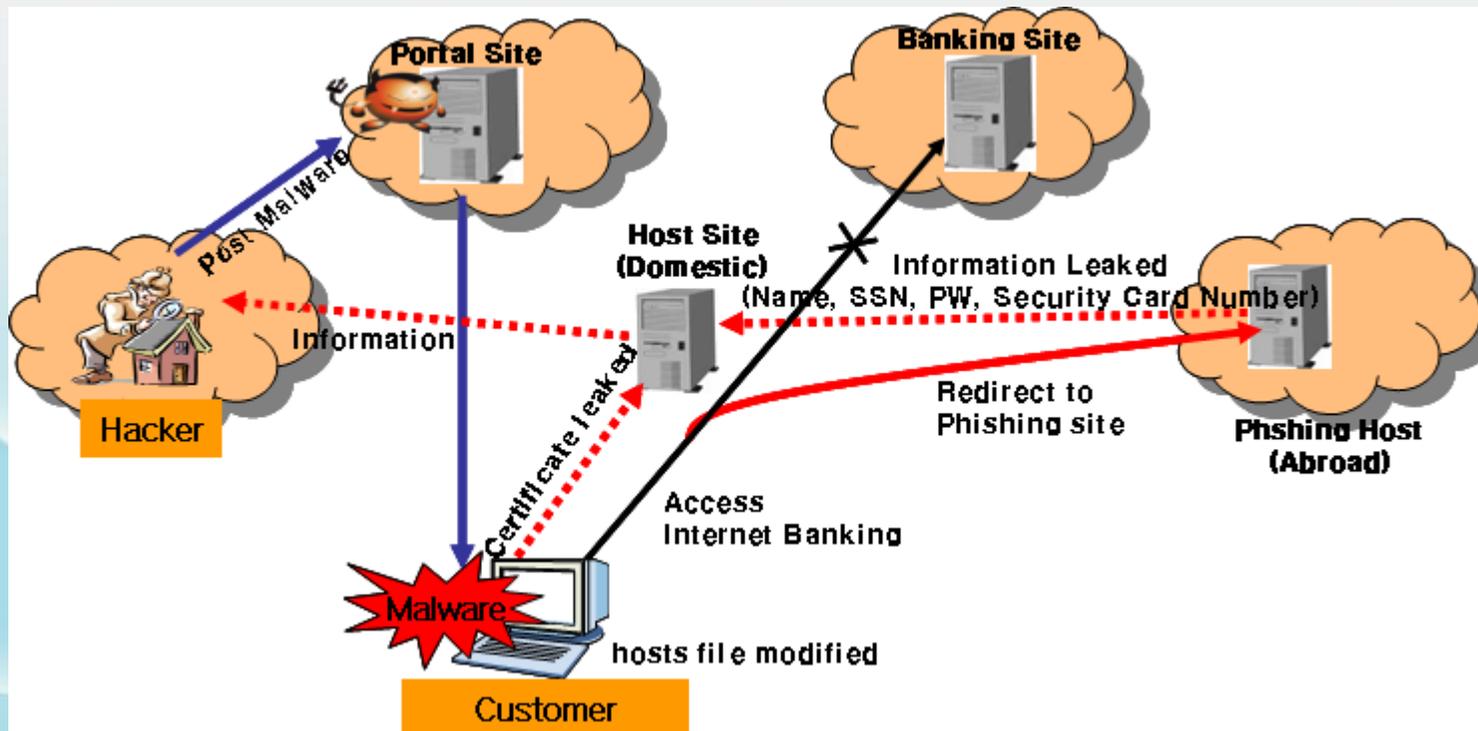


■ Accumulated Users(Monthly)

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)

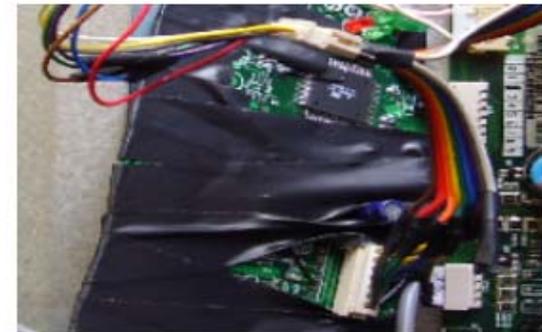
- ➔ ATM owner installed a duplication reader in the ATM
- ➔ Passwords were recorded with hidden camera
- ➔ Stored card information was used to duplicate for fraudulent withdrawal



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

출금계좌번호	110-207-301338	> 출금가능잔액조회
출금계좌비밀번호	●●●● (4자리 입력)	<input checked="" type="checkbox"/> 추가이체등록시 출금계좌를 동일하게 지정
입금은행		> 장애은행조회
입금은행계좌번호	34113014972 (- 없이 입력)	> 자주쓰는입금계좌
이체금액	10 원	> 금액입력기 > 계산기
받는분 통장표시내용	(7자리내)	* CMS 코드
보내는분 통장표시내용	(7자리내)	* 우수그룹코드 숫자 4자리(일반고객 입력 불필요)
		확인 추가이체

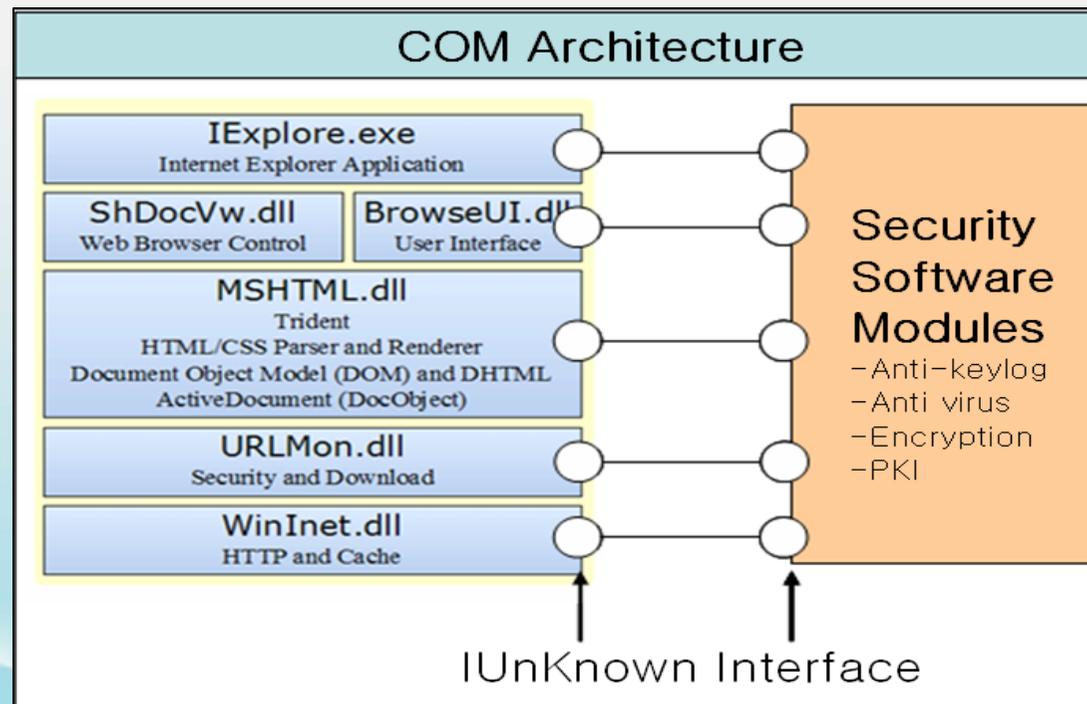
[Memory]
0x00123456 : 061-21-1085-102
0x0012345a :
...
...
0x0012347b : 6050496677
...

- ⇒ Account Number '34113014972' will be changed to the hacker's account number '6050496677' on clicking 'OK'.

IV. New threats

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

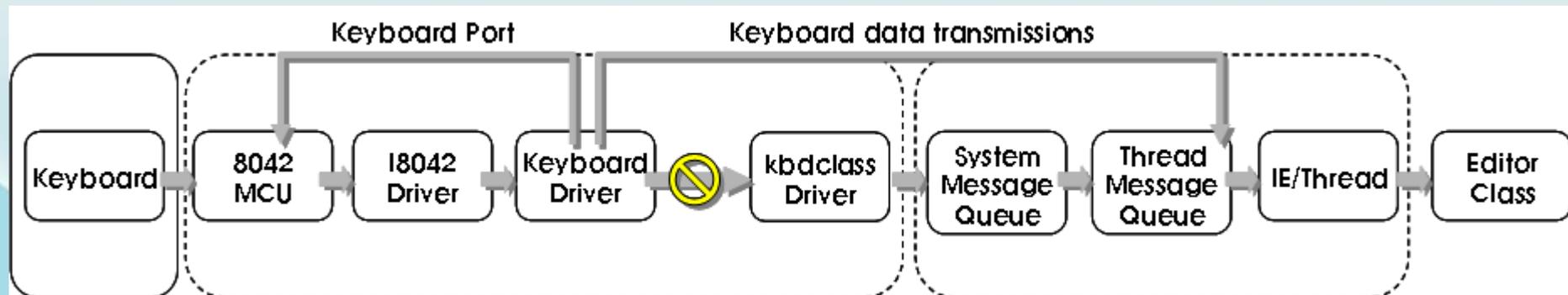


- ⇒ IUnknown interface can be monitored so that the hacker can forge account information

IV. New threats

3. Keyboard Logging

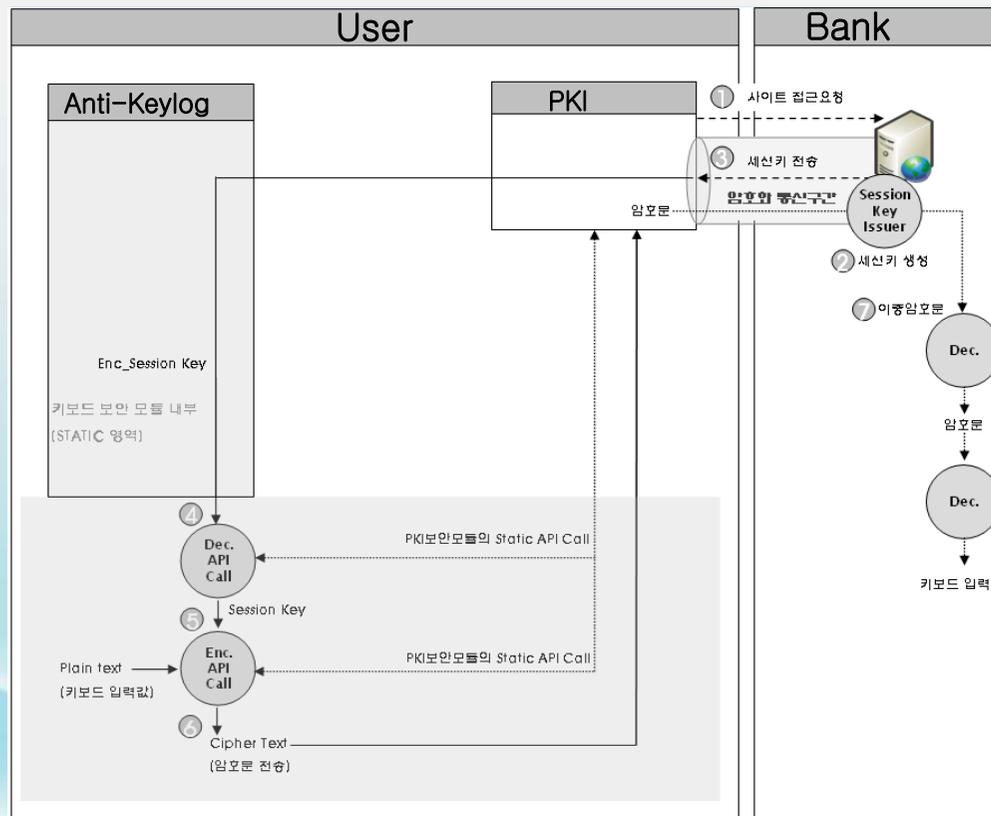
- Even though anti-keylog software protects many key loggers from logging the passwords,
- new hacking technology bypasses security technology
- It is necessary to monitor the technology and trends to develop complementary security measures



V. Countermeasures and Conclusion

1. Countermeasures(1)

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

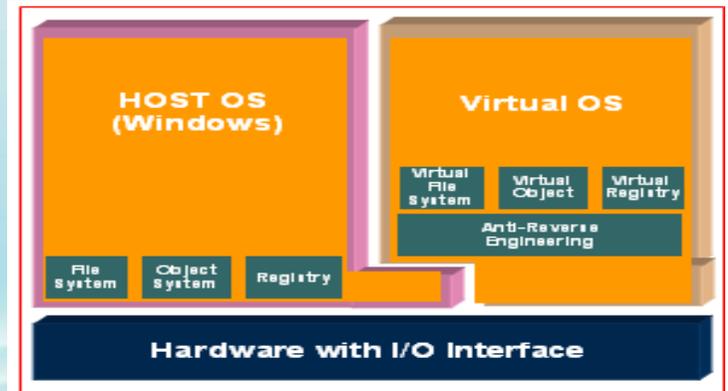
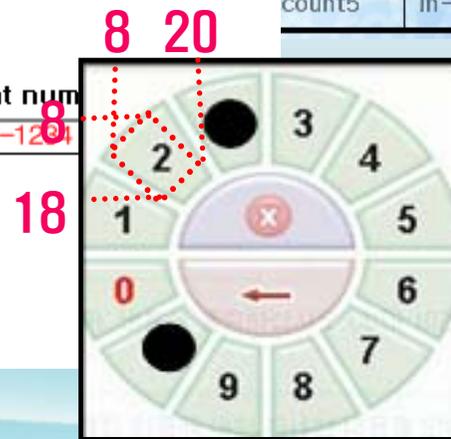
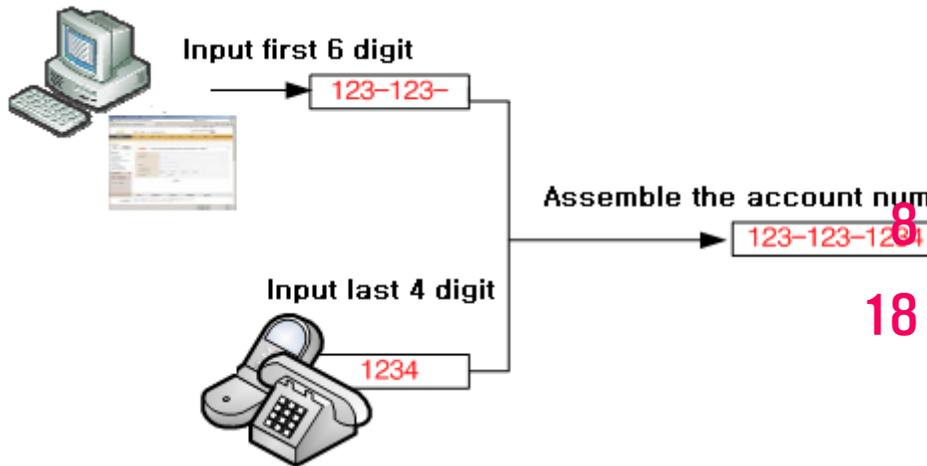


V. Countermeasures and Conclusion

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



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



금융보안연구원
Financial Security Agency