Mobile Security Framework; Advances in Mobile Governance in Korea

TaeKyung Kim
tkkim@stu.ac.kr
I. e-banking in Korea

1. e-banking ?

- **BIS (Bank for International Settlements)**
  - e-finance(electronic banking) refers to the provision of retail and small value banking products and services through electronic channels

- **FFIEC (Federal Finance Institutions Examination Council, US)**
  - e-banking is defined as the automated delivery of new and traditional banking products and services directly to customers through electronic, interactive communication channels.
  - Customers access e-banking services using an intelligent electronic device, such as a personal computer (PC), personal digital assistant (PDA), automated teller machine (ATM), kiosk, or Touch Tone telephone.
I. e-banking in Korea

2. Features of e-banking

- Electronic
  - Increasing convenience

- Paperless
  - Increasing profit

- Increasing IT’s role
  - Raising the risk on IT

- Open networks
  - Security and customer protection
I. e-banking in Korea

3. Banking Environments

- **Broadband User**
  - 77.2% of total households (36 million subscribers)

- **Mobile User**
  - 97% of total population (48 million users)

- **Digital Certificates**
  - 30% of total population (15 million certificates)

**Online banking Users**

Real time money transfer to any other banks is widely possible in Korea

**FINS (Financial Information Network System)**

- **Bank-1**
- **Bank-2**
- ... 
- **Bank-n**

**Securities & Others**
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
1. e-banking 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.)
I. e-banking 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%
I. e-banking in Korea

3. Security programs in internet banking(1)

- Anti-Keylog / AntiVirus / Encryption should be provided
I. e-banking in Korea

3. Security programs in internet banking (2)

Digital certificate
I. e-banking in Korea

3. Security programs in internet banking

Security Card (Random Number)

<table>
<thead>
<tr>
<th>동행/타행이체</th>
</tr>
</thead>
<tbody>
<tr>
<td>GUIDE:</td>
</tr>
<tr>
<td>- 내역을 확인하시고 소지하고 계신 보안카드의 첫번째 지시번호 앞쪽 두자리와 두번째 지시번호 뒤쪽 두자리를 차례대로 입력 후 [확인] 버튼을 선택하십시오.</td>
</tr>
<tr>
<td>- [확인] 버튼 선택 후 5분이내에 결과를 받지 못한 경우, 이체실패여부를 반드시 확인하시기 바랍니다.</td>
</tr>
</tbody>
</table>

| 입금은행 | 1. 3.1. 1. 1. 1. |
| 입금계좌 | 2222 |
| 발행은행 | SK카드 |
| 이체금액 | 10,000 |
| 수수료 | 0 |
| 의무인 | SK카드 |
| 출금계좌번호 | 3333 |

고객님께서 입력한 입금은행 계좌번호, 이체금액 및 발행은행 등이 위와 일치하며 확인하시면.

<table>
<thead>
<tr>
<th>입력방법 선택</th>
<th>마우스로 입력</th>
<th>키보드로 입력</th>
</tr>
</thead>
<tbody>
<tr>
<td>보안카드 비밀번호</td>
<td>[20]</td>
<td>[20]번 내자리 중 앞의 두자리</td>
</tr>
<tr>
<td></td>
<td>[17]</td>
<td>[17]번 내자리 중 뒤의 두자리</td>
</tr>
<tr>
<td></td>
<td>?</td>
<td>보안카드 비밀번호 입력방법</td>
</tr>
</tbody>
</table>

>> 확인  >> 취소
3. Security programs in internet banking (4)

**OTP (One Time Password):** Valid only for 1 minute
I. e-banking in Korea

4. Related Law & Policy(1)

- **Backgrounds 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**
1. e-banking 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
### 4. Related Law & Policy (3)

**Transaction limit for each security level (08’ April)**

<table>
<thead>
<tr>
<th>Security Level</th>
<th>Security Measure</th>
<th>Transfer Limit (USD, approximately)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Each</td>
</tr>
<tr>
<td><strong>Level 1</strong></td>
<td>OTP + Certificate</td>
<td>100,000</td>
</tr>
<tr>
<td></td>
<td>HSM(Certificate) + Security Card</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Security Card + Certificate + 2 Channel Authentication</td>
<td></td>
</tr>
<tr>
<td><strong>Level 2</strong></td>
<td>Security Card + Certificate + SMS Notice</td>
<td>50,000</td>
</tr>
<tr>
<td><strong>Level 3</strong></td>
<td>Security Card + Certificate</td>
<td>10,000</td>
</tr>
</tbody>
</table>
I. e-banking in Korea

5. Strength of Collaboration Model

❖ Cost-effectiveness
- Collaboration center prevents the duplicate investment
- Massive use may lead to reduce the retail cost of OTP devices

❖ The benefit of the user’s convenience
- Only one OTP device can be used in many financial companies

❖ Security enhancement
- Managed and operated by security professionals in OTP center
- 2FA can provide stable and secure electronic financial service
II. Incident Cases

1. Pharming with Malware

- Malware distributed through portal site
- Unlatched PCs are infected, ‘hosts’ file was modified for pharming
- Host site was storing 4,000 certificates
- No economical loss due to quick response
II. Incident Cases

2. Internet payment incident

- 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
II. Incident Cases

3. Card Duplication

- 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
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 ‘34******972’ will be changed to the hacker’s account number ‘60******677’ on clicking ‘OK’.
Almost every online software uses 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
IV. Countermeasures

1. Countermeasures

Recommend kernel level end-to-end encryption to prevent COM hooking and Memory forgery.
IV. Countermeasures

2. Countermeasures

- Research and recommend security solutions such as
  - Two channel authentication
  - Secure keypad
  - Secure image (Captcha)
  - Virtualization
V. Smartphone Security Status and Major Issues

1. Kind of smartphone

- Apple - IPhone OS(OS X)
- Google – Android
- Microsoft - Windows Mobile

<table>
<thead>
<tr>
<th>IPhone OS(OS X)</th>
<th>Android</th>
<th>Windows Mobile</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1" alt="iPhone OS(OS X)" /></td>
<td><img src="image2" alt="Android" /></td>
<td><img src="image3" alt="Windows Mobile" /></td>
</tr>
</tbody>
</table>
2. The proliferation of smartphones

In the entire mobile phone market, smart phones are expected to increase by 40 percent in 2012.
V. Smartphone Security Status and Major Issues

3. Smartphone security threats

**Platform attack**
Attacks on smartphone OS and platform-specific vulnerabilities
- Viruses and malicious code
- Keyboard hacking
- SMS Hooking
- Processes and memory(dump) hacking

**Application attack**
Unlike viruses, attacks on application
- Fishing Program
- Changes in data and executable files
- Reverse Engineering
- DoS and DDoS

**Storage attack**
Confidential information extraction attacks on internal/external memory and file system
- Access and extraction of Smartphone's internal storage
- Extracting the active and deleted confidential information
V. Smartphone Security Status and Major Issues

4. Smartphone Security Technology

- **Platform threat response**
  - Anti-virus program
  - Code signing for licensed software
  - Apply encryption to protect data
  - Detection and control of processes and memory access API

- **Application threat response**
  - Apply Anti-Reversing technology
  - Using verified encryption algorithm

- **Storage threat response**
  - Apply encryption to prevent information leakage
  - Remove confidential information (Wiping)
5. Mobile Malware, by Platform

Source: McAfee® Labs, "McAfee Threats Report: First Quarter 2011"
6. Example of mobile malware 1

- **Android/DrdDream Family**
  - To comprise a variety of legitimate games and apps that have been injected with malicious code

- **Two root exploits**
  - Exploit/Lvedu
  - Exploit/DiutesEx

- **They were initially used by users trying to gain legitimate root access to their own devices (rooting)**

- **For mobile devices**
  - Malware has required user interaction at present
  - Mobile exploits will allow automatic malware installation in the future
7. Example of mobile malware 2

- Android/Drad Family
  - To be made up of maliciously modified applications
- This family sends device information to an attacker-controlled site
  - Android/Drad listens for commands from the attacker
  - The malware can also download additional software, though it stops short of being a full-fledged mobile botnet
V. Smartphone Security Status and Major Issues

8. Total Mobile Malware Samples

Source: McAfee® Labs, "McAfee Threats Report: First Quarter 2011"
V. Smartphone Security Status and Major Issues

9. Mobile Malware Growth by Quarter

- Increased by 46% (Q3 2009 ~ Q3 2010)

Source: McAfee® Labs, "McAfee Threats Report: Fourth Quarter 2010"
VI. 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
"Environmental change and security of electronic financial services, technology trends", FSA, 2010,
