Computer Security

Public Key Infrastructure

Hyoungshick Kim

Department of Software

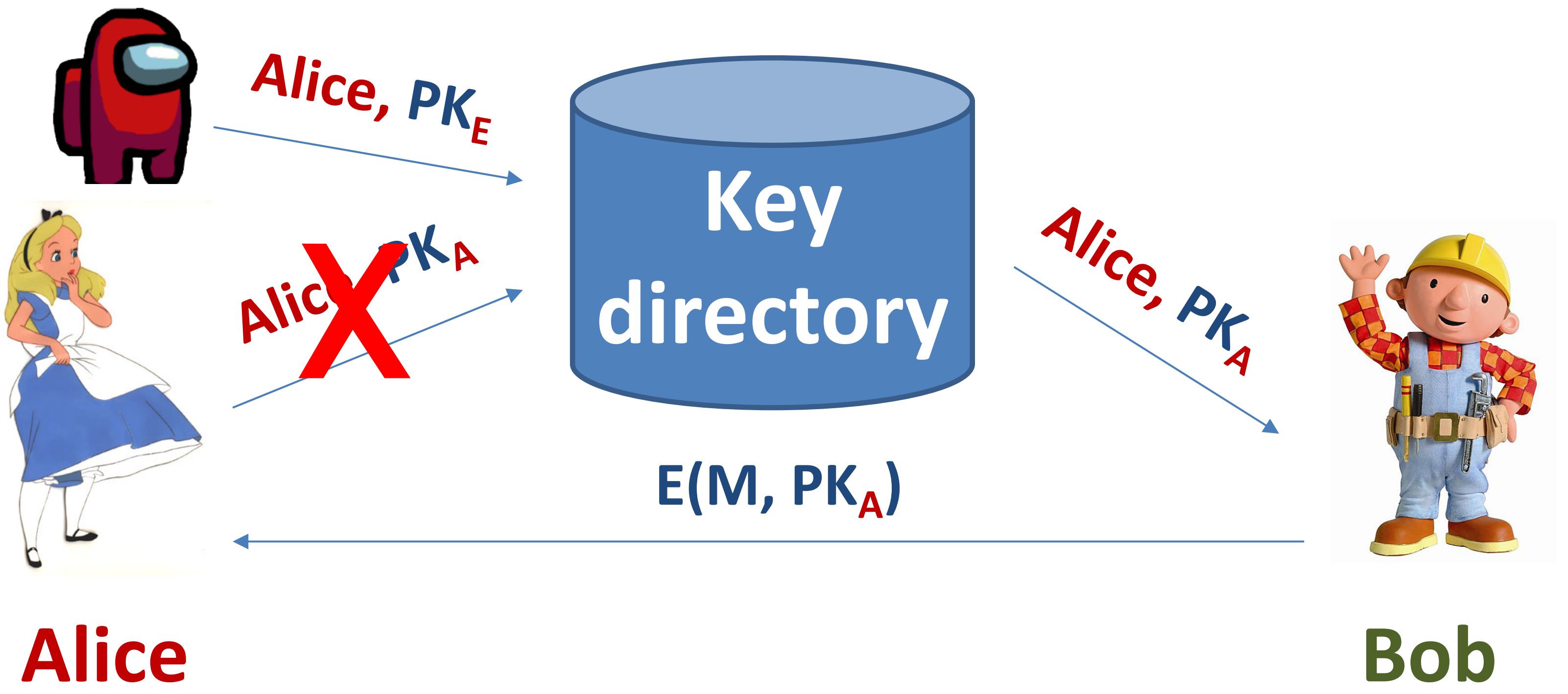
College of Software

Sungkyunkwan University

General problems with PKC

- Keys need to be long – we can factor / do discrete log to about 700 bits. For DSA/RSA, 1024 is marginal, 3072 bits should be considered safe for now
- Elliptic curve variants can use shorter keys – but it is tricky to implement securely, the standard curves
- Computations are too slow
- Power analysis is a big deal: difference between squaring and doubling is visible. Timing attacks too
- For many applications, PKC just isn't worth it

Key management problems with PKC

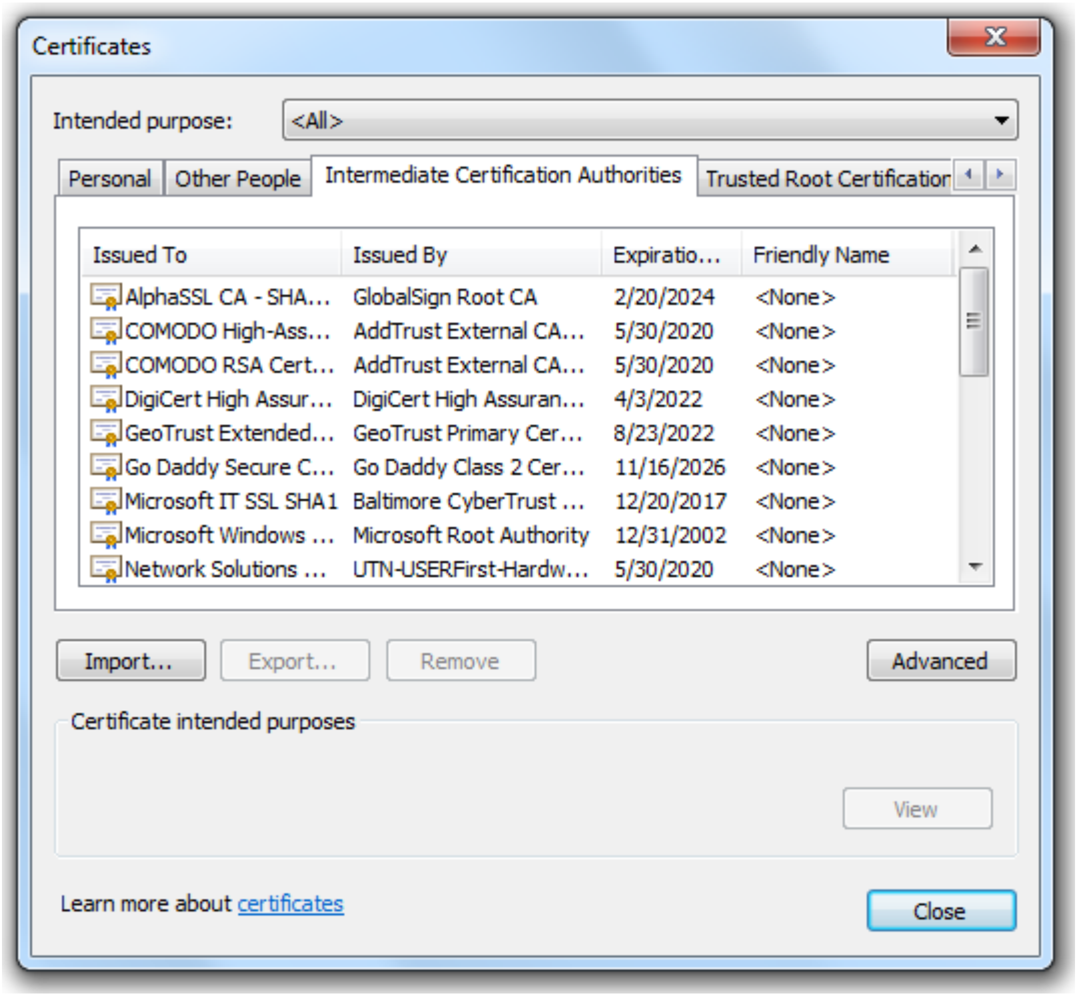


- Anyone can send Alice a secret message
- However, how do we know a key belongs to Alice?
  - If imposter substitutes another key, she can read Alice's mail

Public-Key Infrastructure (PKI)

- One solution is to use PKI
  - Trusted root authority (VeriSign, IBM, Korean government)
    - Everyone must know the verification key of root authority
    - Check your browser; there are hundreds!
  - Root authority can sign certificates
  - Certificates identify others, by linking their ID (e.g., domain name or legal name) to a verification key they own
  - Certificates can also delegate trust to other certificate authorities
    - Leads to certificate chains
  - Most common standard "X.509"

Certificates in a browser


Certificates

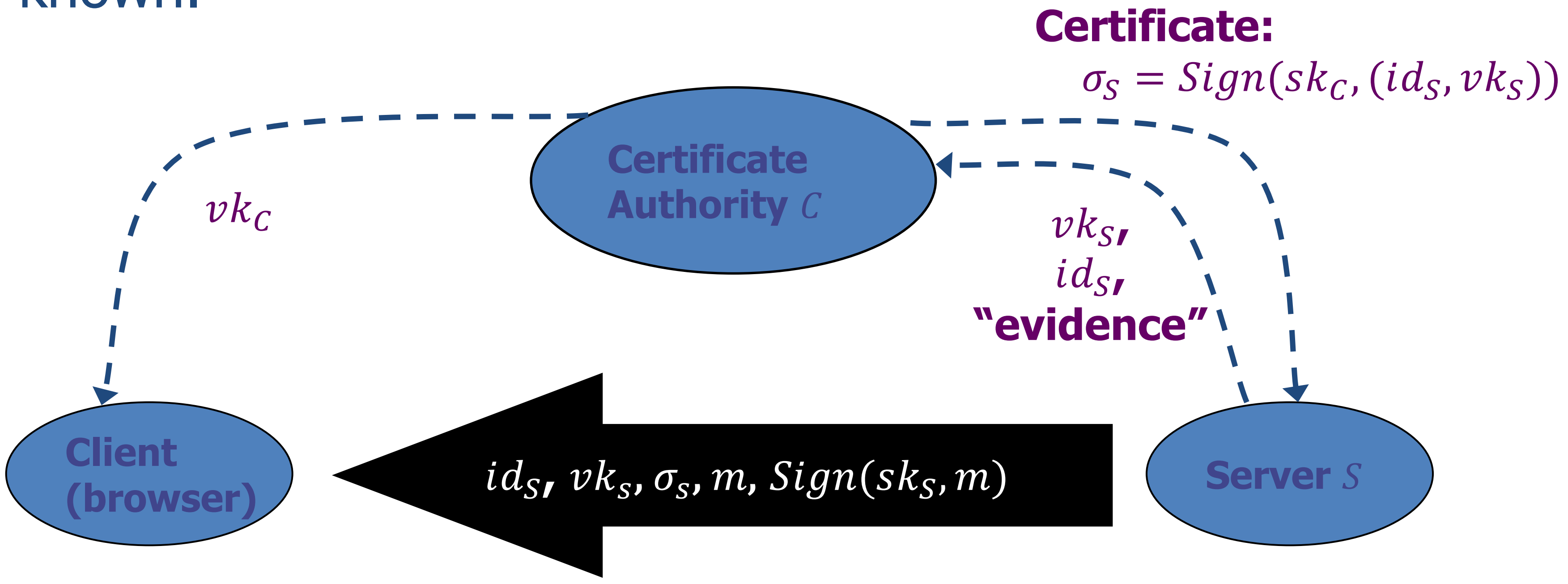
Intended purpose: <All>

Personal
Other People
Intermediate Certification Authorities
Trusted Root Certification

Issued To	Issued By	Expiratio...	Friendly Name
AlphaSSL CA - SHA...	GlobalSign Root CA	2/20/2024	<None>
COMODO High-Ass...	AddTrust External CA...	5/30/2020	<None>
COMODO RSA Cert...	AddTrust External CA...	5/30/2020	<None>
DigiCert High Assur...	DigiCert High Assuran...	4/3/2022	<None>
GeoTrust Extended...	GeoTrust Primary Cer...	8/23/2022	<None>
Go Daddy Secure C...	Go Daddy Class 2 Cer...	11/16/2026	<None>
Microsoft IT SSL SHA1	Baltimore CyberTrust ...	12/20/2017	<None>
Microsoft Windows ...	Microsoft Root Authority	12/31/2002	<None>
Network Solutions ...	UTN-USERFirst-Hardw...	5/30/2020	<None>

Concept of PKI

We assume that verification key vk_C of certificate authority is known.



Certificate:
$\sigma_S = Sign(sk_C, (id_S, vk_S))$
Certificate Authority C
vk_C
vk_S,
id_S,
"evidence"
Client (browser)
id_S, vk_s, σ_s, m, $Sign(sk_S, m)$
Server S

Server certificate can be verified by any client that has CA key vk_C.

In theory, PKI (or digital certificate) may provide a neat solution for user authentication.

In practice, however, PKI has proved to be difficult to deploy due to the difficulty of protecting the private keys and the high maintenance costs. (Read “Ten Risks of PKI: What You’re not Being Told about Public Key Infrastructure”)

The Korean PKI is well established?

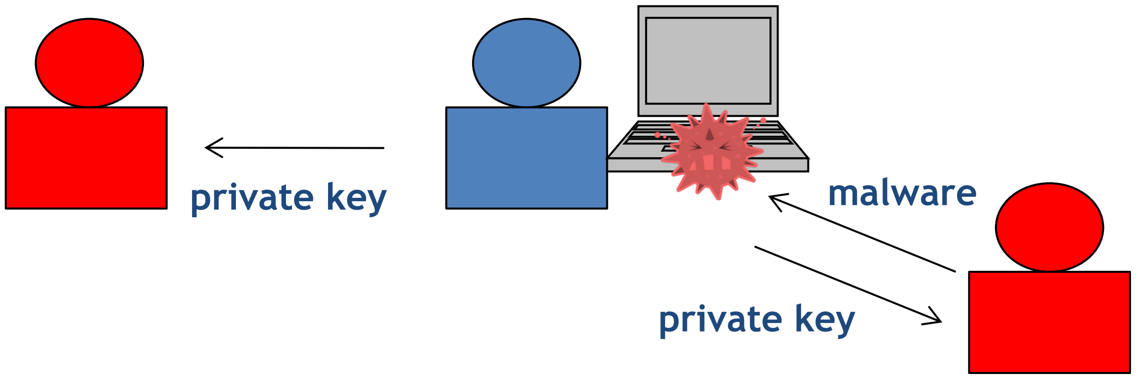
◇왼쪽부터 루카스 마담스키, 허준호, 김형식연구원, 브루스 슈나이어

Good news: the number of issued certificates is over 25 million (2012)

Bad news: The private keys are mostly (about 98.2%, 2008) stored on unprotected memory (e.g., hard disk or USB) in practice

Is software-based private key enough for online banking?

The private key can be copied to the following attackers:
- local attackers who can physically access the user’s PC
- remote attackers who can control malware in the user’s PC



The security is **only as good as the password.**

Is non-repudiation guaranteed?

Digital signature provides technical non-repudiation.

Can banks claim non-repudiation when the private key is insecurely managed like this?

Is a digital signature alone enough? - alternatively, transaction log or money flow analysis (i.e., FDS) were mainly used in practice

Are HSMs used securely?

Only 2~4 services support HSM (Hardware Security Modules)

In Korea, HSMs are commonly used as follows:

USB key token

Smart Card

The protection of private key alone may not be enough.

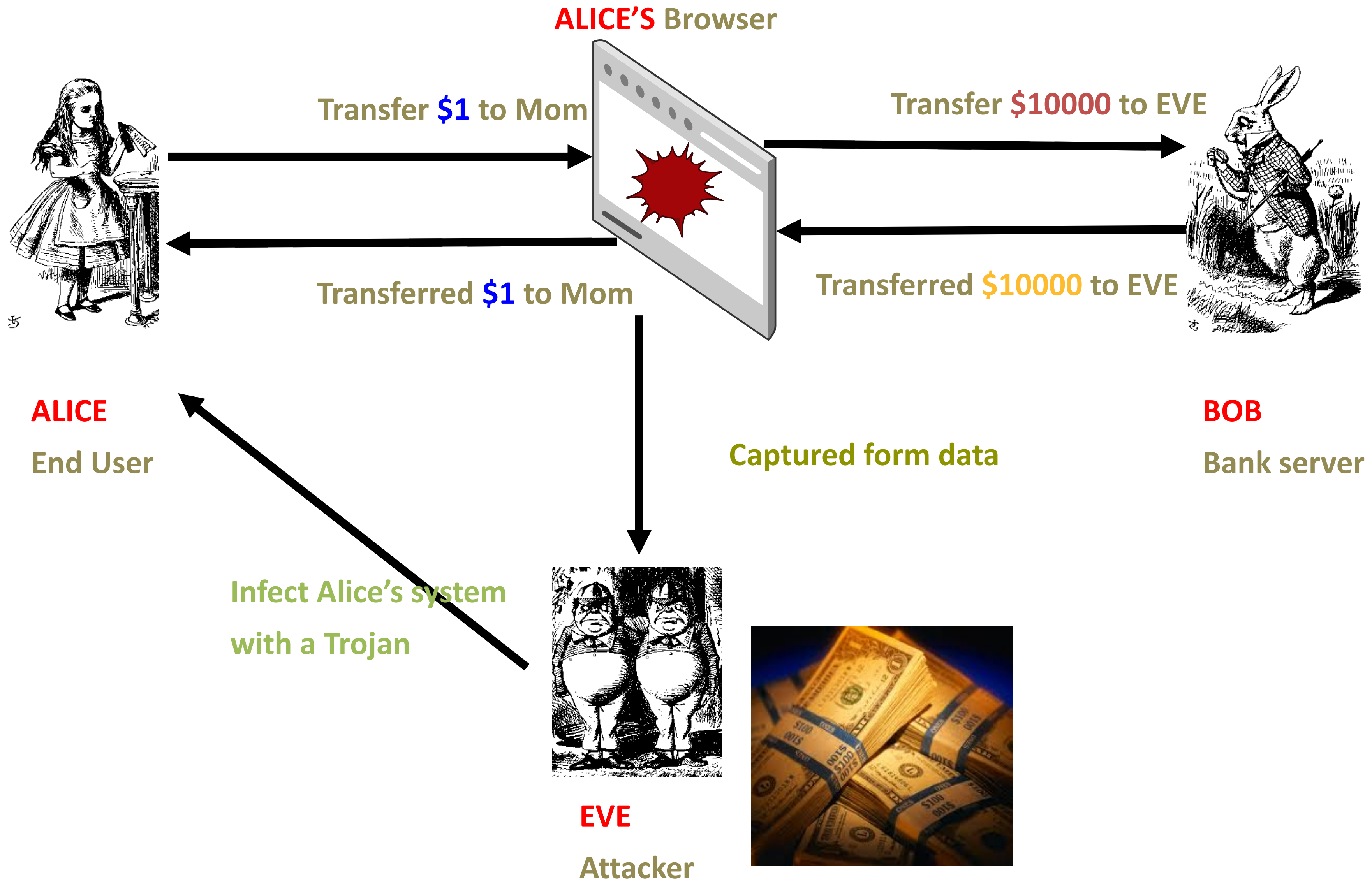
Not easy to use private key securely

How can we enter PIN for HSM securely **without keypad**?

How can we detect a **mismatch** between the data a user originally requested and the data authorized by the card without a **trustworthy display**?

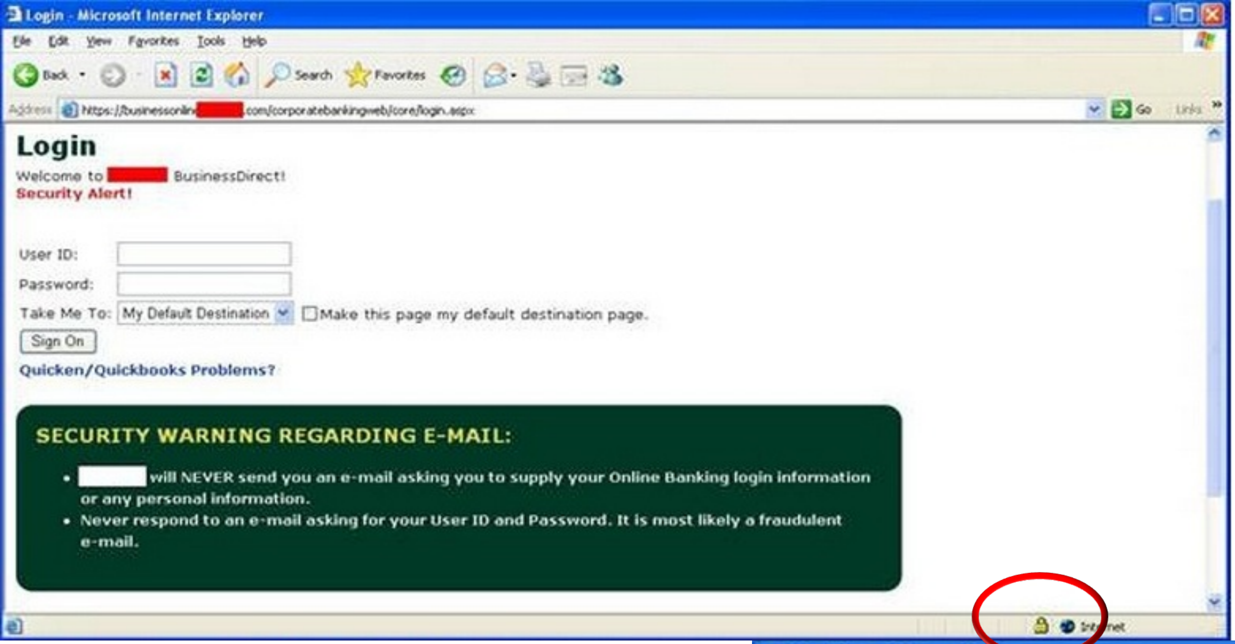
Are the protocols secure enough for HSMs?

Man-in-the-browser (MITB)



CLEAN BROWSER

- No extra fields
- Just the required information


Login - Microsoft Internet Explorer

Address https://businessonlin[redacted].com/corporatebankingweb/core/login.aspx

Login

Welcome to [redacted] BusinessDirect!
Security Alert!

User ID:
Password:
Take Me To: My Default Destination ☐ Make this page my default destination page.

Sign On

Quicken/Quickbooks Problems?

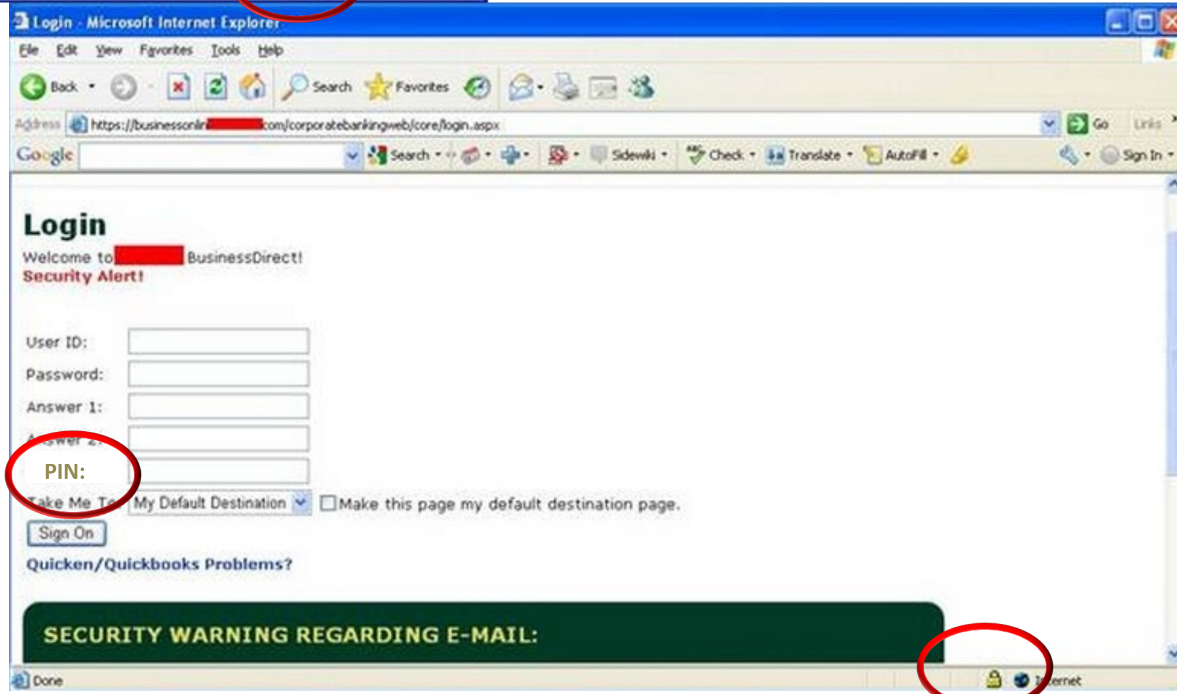
SECURITY WARNING REGARDING E-MAIL:

- [redacted] will NEVER send you an e-mail asking you to supply your Online Banking login information or any personal information.
- Never respond to an e-mail asking for your User ID and Password. It is most likely a fraudulent e-mail.

Internet

INFECTED BROWSER

- Extra fields e.g.: PIN
- Asks for critical information usually not required


Login - Microsoft Internet Explorer

Address https://businessonlin[redacted].com/corporatebankingweb/core/login.aspx

Login

Welcome to [redacted] BusinessDirect!
Security Alert!

User ID:
Password:
Answer 1:
Answer 2:
PIN:
Take Me To: My Default Destination ☐ Make this page my default destination page.

Sign On

Quicken/Quickbooks Problems?

SECURITY WARNING REGARDING E-MAIL:

Done Internet

Trustworthy user interface is necessary

A USB smartcard reader with a trustworthy display and keypad is required.

If you are interested in my personal opinion, please read "On the security of Internet Banking in South Korea", 2010.

Questions?

Sungkyunkwan
Campus
established
Sciences
University
university
Suwon
School
Seoul
Natural
Graduate
campus
Korean
Social
Global
English
Professors
constructed
edit