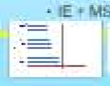
On the Security of Internet Banking in South Korea

Jan Dolecek, FI MU
juzna.cz@gmail.com

PV177

Introduction

- curious security
- sued by OpenWeb
- many advantages
- proprietary
- enthusiastic users
- IE + MS only



Aim of paper

- describe security mechanisms in Korea
- evaluate it
- discuss it
- solution

Security mechanisms

User Authentication

- properties
- Korean properties

summary

Not Effective?

[illegible]

User issues

Difficulty

"False" better security

70% prefer other banks

Compatibility problems

Speed

Recommendations

Provide more options

Compatible and/or open mechanisms

User-friendly documentation

Trustworthy approach

Conclusion

Korean banking

Solution

TLS

Trusted platform

CAP devices

Q&A

Thank you

On the Security of Internet Banking in South Korea

Jan Dolecek, FI MU
juzna.cz@gmail.com

PV177

Introduction

- curious security

anti-keylogger

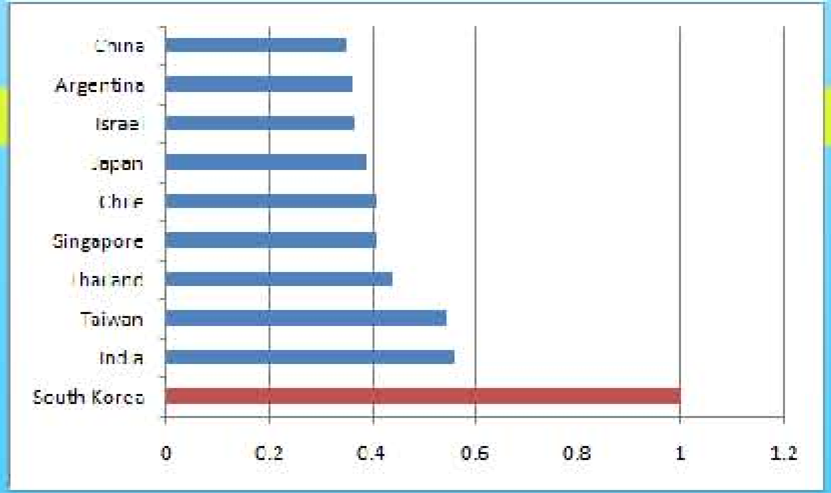
firewall

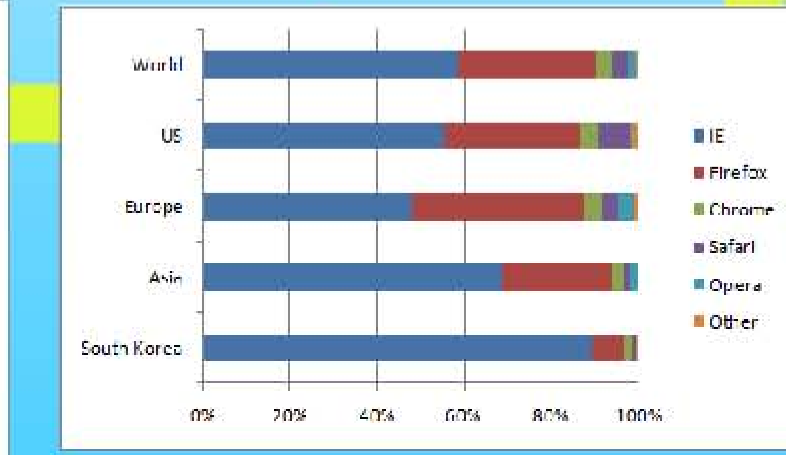
ActiveX

anti-virus

secure tunnel

- sued by OpenWeb
- many advantages
- proprietary
- enthusiastic users
- IE + MS only





anti-keylogger

firewall

- curious security

ActiveX

anti-virus

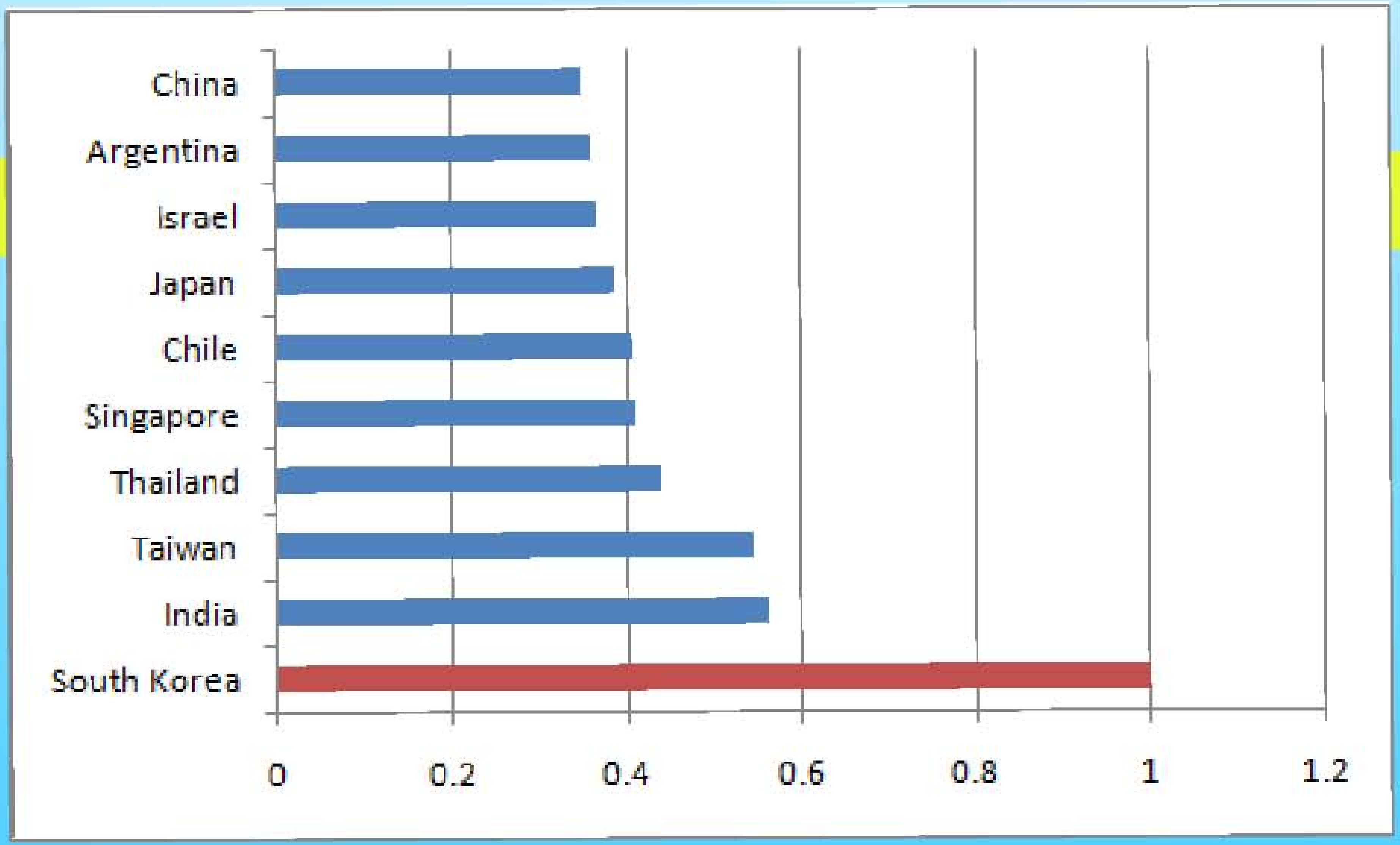
secure tunnel

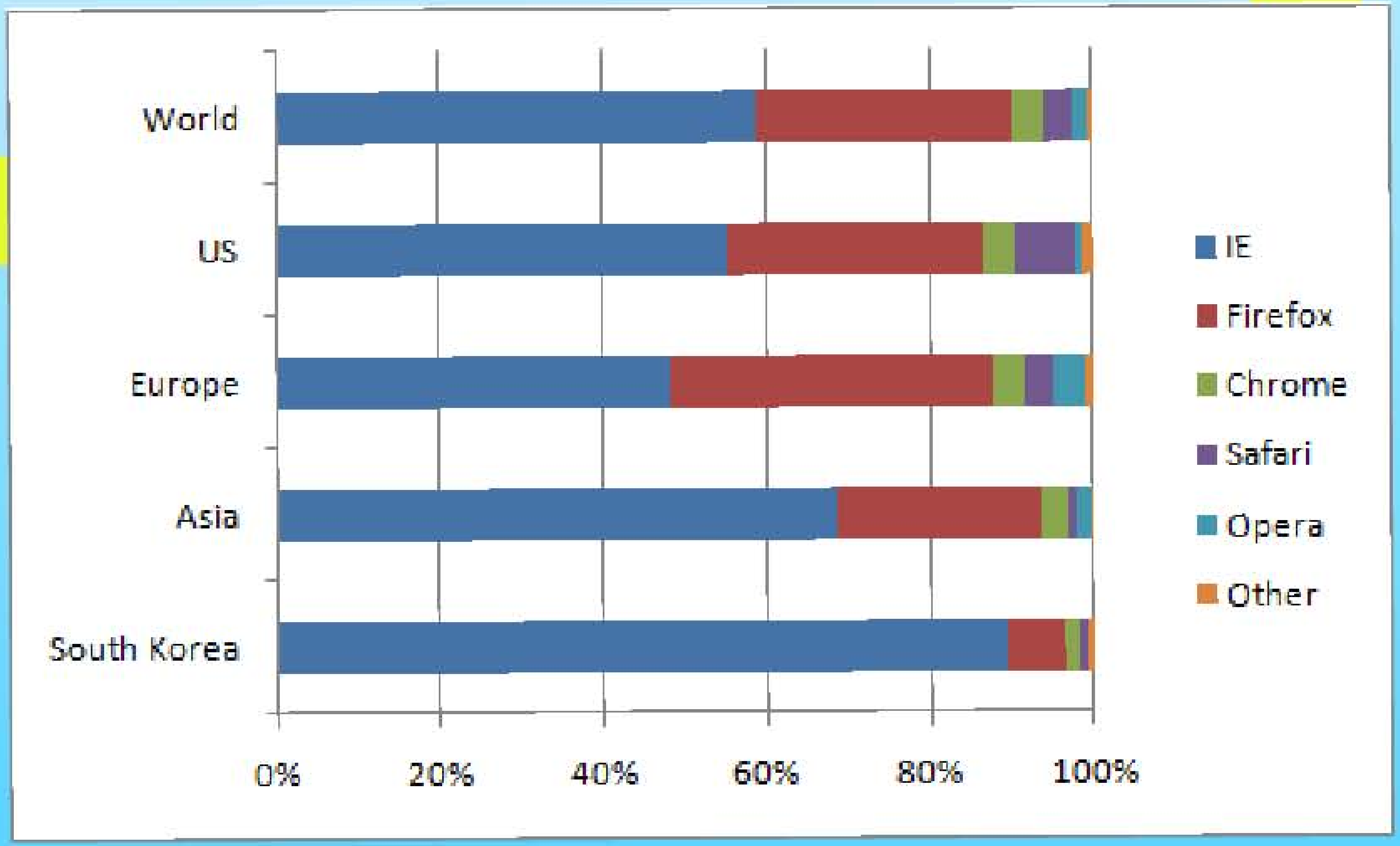
on

- sued by Open

rietary

- IE + MS only





Aim of paper

- describe security mechamisms in Korea
- evaluate it
- discuss it
- solution

C is untrusted

- physical token
- PIN
- certificate (PKI)

User Authentication

- biometrics
- password
- one-time password

combines 2-3 -> secure

Security mechanisms

• properties

non-repudiation

data integrity

confidentiality

user/server authentication

• Korean properties

anti-keylogger

one-time password

detect and remove malware

network access control

proprietary protocols

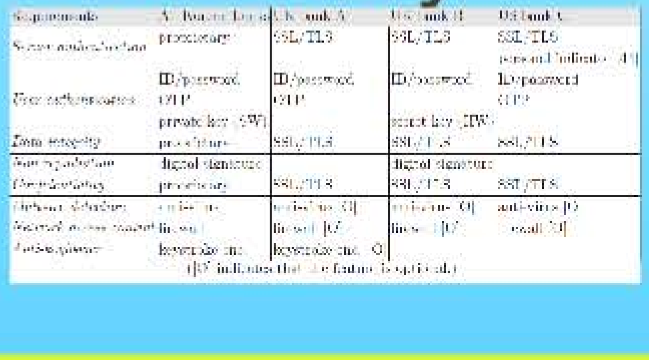
because of Crypto wars

RSA+HMAC

SEED

Secure and Authenticated Communication Channel

summary



Requirements	A: Korean bank	UK bank A	US bank B	US bank C
Server authentication	proprietary	SSL/TLS	SSL/TLS	SSL/TLS personal indicator [O]
User authentication	ID/password OTP private key (SW)	ID/password OTP	ID/password secret key (HW)	ID/password OTP
Data integrity	proprietary	SSL/TLS	SSL/TLS	SSL/TLS
Non-repudiation	digital signature		digital signature	
Confidentiality	proprietary	SSL/TLS	SSL/TLS	SSL/TLS
Malware detection	anti-virus	anti-virus [O]	anti-virus [O]	anti-virus [O]
Network access control	firewall	firewall [O]	firewall [O]	firewall [O]
Anti-keylogger	keystroke enc.	keystroke enc. [O]		

([O] indicates that the feature is optional.)

ty r

non-repudiation data integrity

- properties

confidentiality

user/server authentication

hanne

anti-keylogger

one-time password

- Korean properties

because of Crypto wars

detect and remove malware

network access control

proprietary protocols

SEED

Secure and Authentica
Communication Chan

RSA+HMAC

rties

control

because of Crypto wars

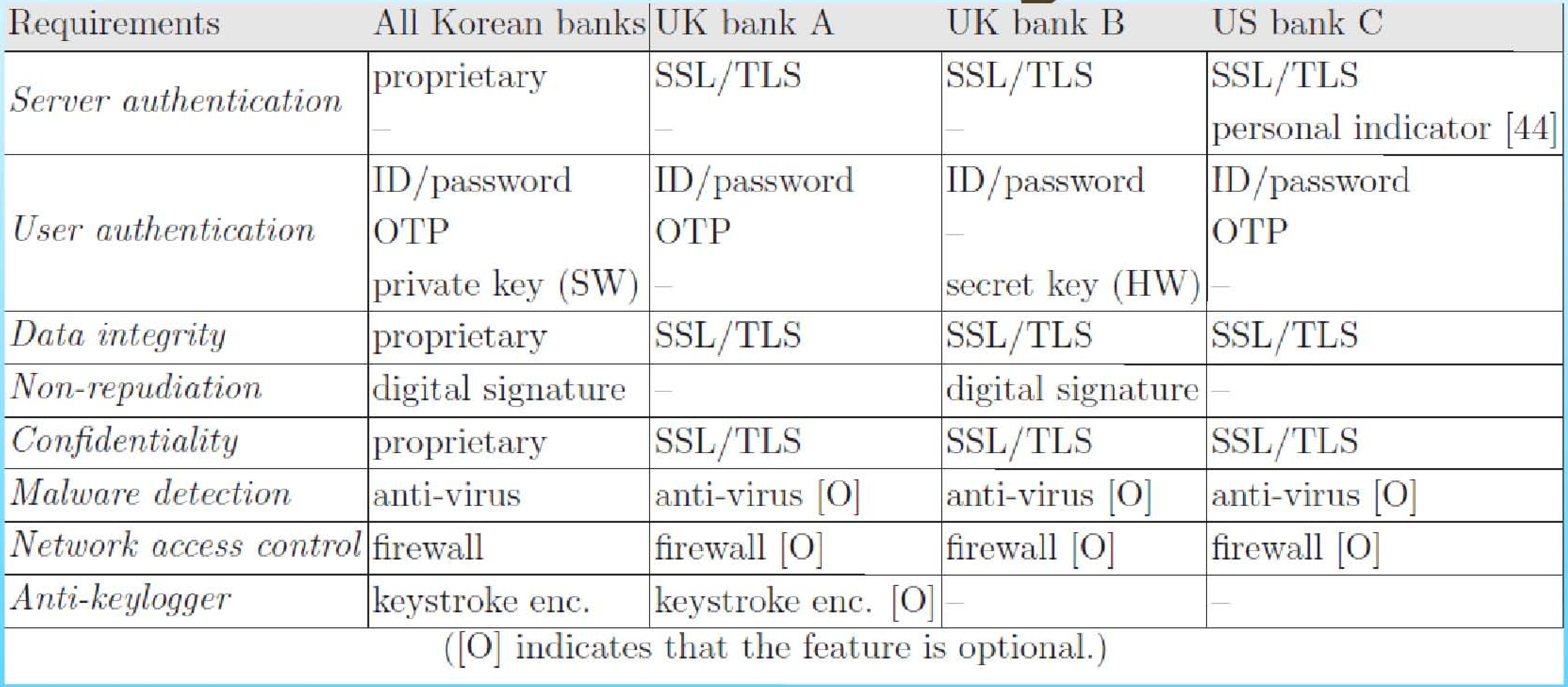
proprietary protocols

RSA+HMAC

SEED

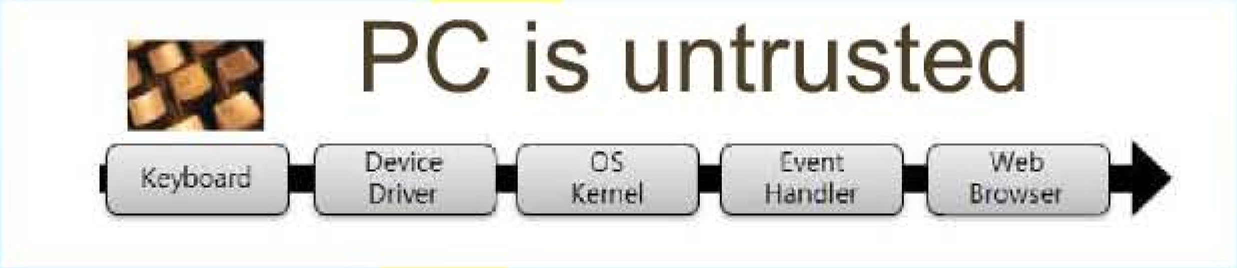
Secure and Authenticated
Communication Channel

summary



Requirements	All Korean banks	UK bank A	UK bank B	US bank C
Server authentication	proprietary –	SSL/TLS –	SSL/TLS –	SSL/TLS personal indicator [44]
User authentication	ID/password OTP private key (SW)	ID/password OTP –	ID/password – secret key (HW)	ID/password OTP –
Data integrity	proprietary	SSL/TLS	SSL/TLS	SSL/TLS
Non-repudiation	digital signature	–	digital signature	–
Confidentiality	proprietary	SSL/TLS	SSL/TLS	SSL/TLS
Malware detection	anti-virus	anti-virus [O]	anti-virus [O]	anti-virus [O]
Network access control	firewall	firewall [O]	firewall [O]	firewall [O]
Anti-keylogger	keystroke enc.	keystroke enc. [O]	–	–

([O] indicates that the feature is optional.)


PC is untrusted

User Authentication

- physical token
- PIN
- certificate (PKI)
- biometrics
- password
- one-time password

combines 2-3 -> secure

Not Effective?

Firewall

feature count is higher?

security through obscurity

Anti-virus

Keystroke encryption

Passphrase redundancy?

Phishing attacks?

Private key storage?

Security proof?

User issues

Difficulty

"False" better security

70% prefer other banks

Compatibility problems

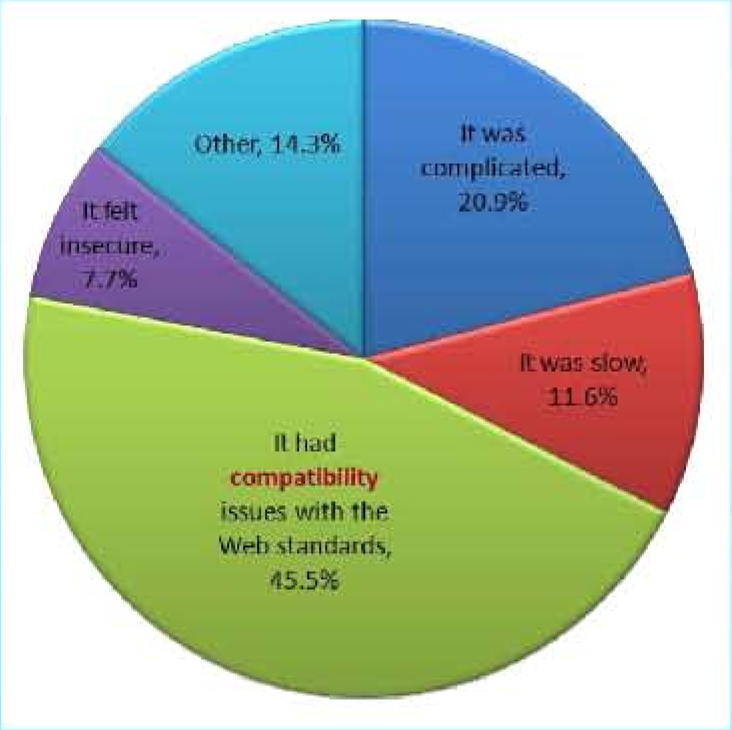
Speed

Recommendations

Provide more options

Compatible and/or open mechanisms

User-friendly documentation



Trustworthy approach

- Bootable USB token
- CAP device
- Virtualization

ns

and/or open
mechanisms

entation

Trustworthy approach

- Bootable USB token
- Virtualization
- CAP device

Conclusion

Korean banking

non-secure

non-compatible

non-standard

Solution

TLS

Trusted platform

CAP devices

Q&A

Thank you