Certificate sharing system for secure certificate distribution in mobile environment

Zhang Zhong

April 3, 2017

Outline

Motivation

- Security of mobile services (e.g., Internet banking, social commerce)
- Secure authentication systems with two-factor authentication (TFA or 2FA)
- A factor from two-factor authentication: public key infrastructure (PKI), certificates, X.509, X316-Chameleon, and short message service (SMS)

Motivation

PKI: A distributed database of public-key certicates and further information (e.g. revocation lists, recommendations, etc.)

Problem

- Share the same certificate between smartphones and personal computers

Existing solution

System for sharing certificates between a smartphone and a PC from: Kookmin Bank (KB), Shinhan Bank, Wooribank, Hyundai Securities, and Samsung Securities.

Disadvantages

- Smartphone and PC have to be turned on.
- Smartphone and PC have to be in the operable state.
- Sharing of the certificate occurs in a single cycle.

Existing solution

Security of a X.509 certificate:

Related works

- A certificate converter toolkit (cannot guarantee a similar security level as X.509)
- Saving certificates in a mobile by minimizing the data size (cannot equip a system with the end-to-end security of an X.509 certificate and X.509 certificates are different in PC and in smartphone)
- A method of developing the mobile-PKI (provides a comparable security level as that of X.509-based wired PKI, cannot prevent an copying the X.509 certificate)
- another method applied to mobile payments (cannot avoid hard copying of an X.509 certificate)

Existing solution

Certificate scheme related to mobile phones: Authentication via a Kerberos, Lightweight PKI based on elliptic curve cryptography (ECC), Enhanced-ADOPT...

- Efficient functionalities
- Cannot provide a method to share the certificates between a PC and a mobile phone

Approach & Solution

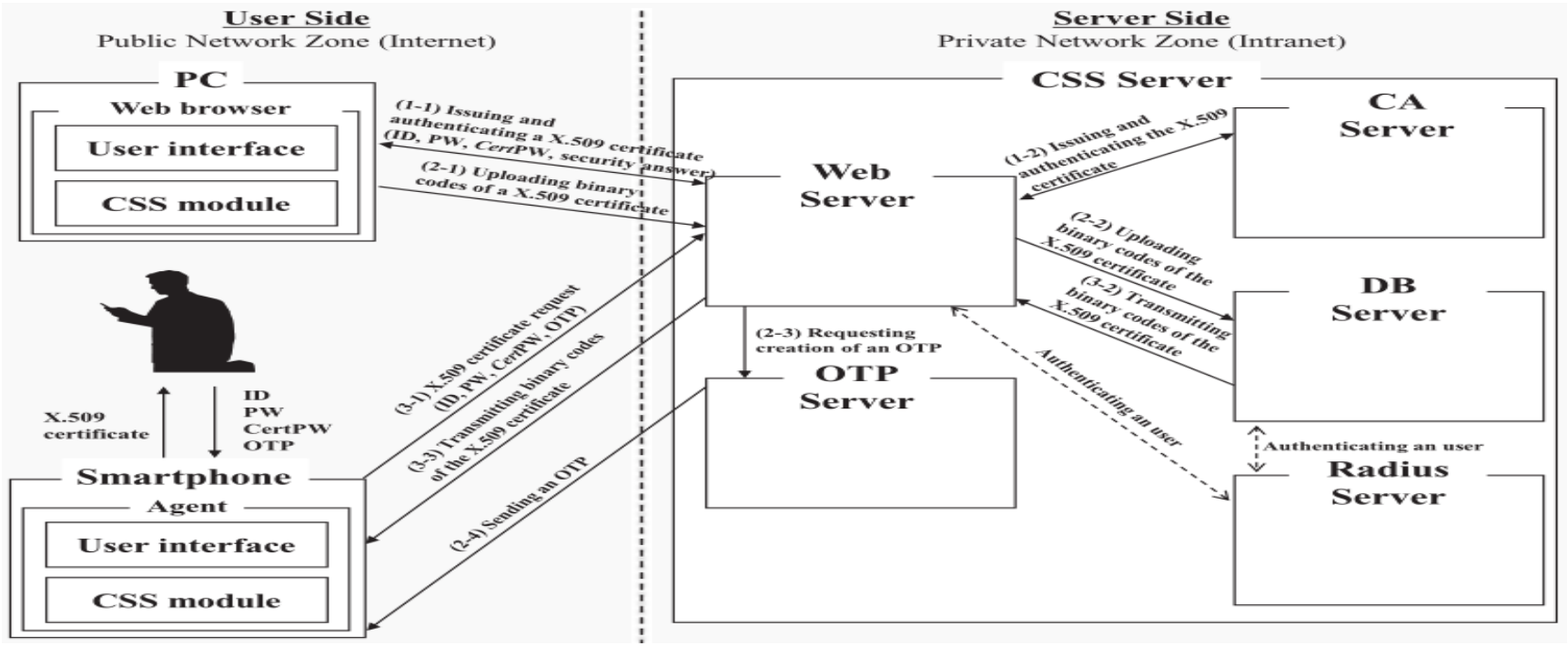

Figure: Overview of the CSS procedure

Source: Kim, Sundeuk, Hyun-Taek Oh, and Young-Gab Kim. : "Certificate sharing system for secure certificate distribution in mobile environment." Expert Systems with Applications 44.

Evaluation

	Method for sharing an X.509 certificate	Same certificate between devices	End-to-end data security	Physical security	Wireless PKI (WPKI)	Security strength of an X.509 certificate	Standards compliant
Ou et al. (2007)	Not supported	No	Guaranteed	Not guaranteed	Unknown	Unknown	Unknown
Ray et al. (2011)	Not supported	No	Guaranteed	Not guaranteed	Supported (mobile PKI)	Unknown	Unknown
Lee et al. (2005)	Not supported	No	Unknown	Guaranteed (security card)	Unknown	Unknown	No
Lee et al. (2008)	Not supported	No	Guaranteed	Not guaranteed	Supported	Unknown	No
Yan et al. (2006)	Not supported	No	Unknown	Not guaranteed	Supported	Unknown	No
Proposed approach	Supported	Yes	Guaranteed	Guaranteed	Supported	Over three years	Yes

Figure: Comparison of existing schemes and our proposed scheme

Source: Kim, Sundeuk, Hyun-Taek Oh, and Young-Gab Kim. : "Certificate sharing system for secure certificate distribution in mobile environment." Expert Systems with Applications 44.

Contribution

- Share identical certificate between a smartphone and a PC at any time
- Strong end-to-end data security for the certificate
- Strong data security on physical devices
- No dependency in terms of web browsers
- CSS module is small and flexible

Limitation

- There is a way in which the X.509 certificate can be captured when it is in the form of binary codes (but more than three years to find out the right combination of binary codes)

Others

- Handy change

Suggestions or future work

Biological or behavioral characteristic (e.g., fingerprint, face recognition, and voice pattern recognition) can be used for identification

References

Maurer, Ueli. "Modelling a public-key infrastructure." European Symposium on Research in Computer Security. Springer Berlin Heidelberg, 1996.

Kim, Sundeuk, Hyun-Taek Oh, and Young-Gab Kim. "Certificate sharing system for secure certificate distribution in mobile environment." Expert Systems with Applications 44.

Questions ?

Limitation 0.1

- Repetition
- Lack of Connection sentence
- Error in References
- Description of related work
- Description of abbreviation (AES-128-CBC)