Solving Terminal Revocation in EAC by Augmenting Terminal Authentication

ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

Rafik Chaabouni

TARTU ÜLIKOOL · UNIVERSITAS TARTUENSIS · 1632

What is the problem?

Revocation of integrated terminals in the EAC.

«Due to the inexactitude of date in MRTD, a terminal can fake its authentication even after its expiration date in his certificate.» [CV09]

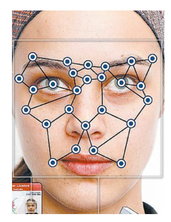
«[...] a stolen reader can be used to perform Terminal Authentication [...]» [BfSidI09]

Why is it important?

Privacy threat: illegitimate access to all MRTDs data

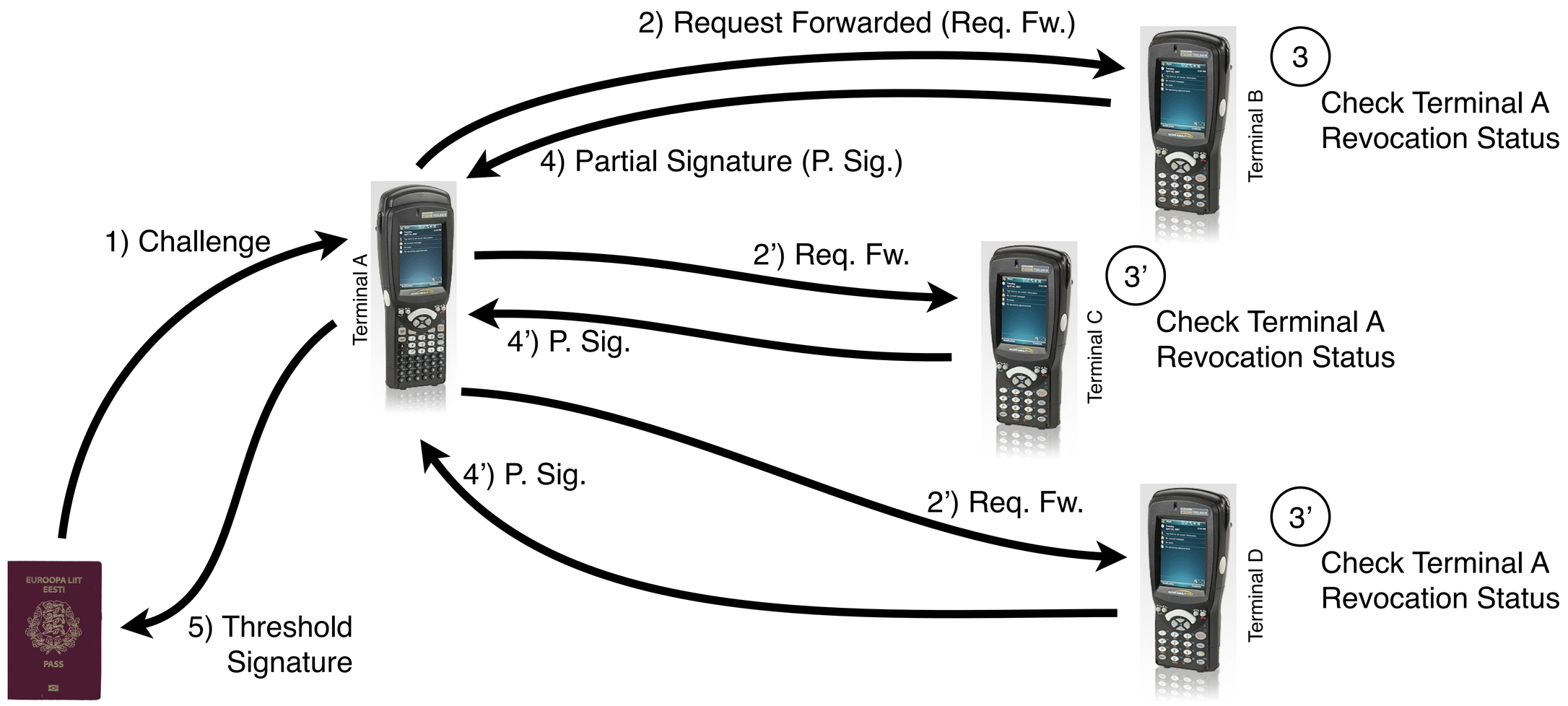
Targeting threat: remote attack against individuals or groups

Mass collection of biometrics into a database in order for the attacker to train themselves and select closest match for cloned ID.



How do we solve it?

We augment Terminal Authentication by **enforcing terminal collaboration** for a complete authentication, with a threshold (RSA) signature.



References

[BfSidI09] Bundesamt für Sicherheit in der Informationstechnik. PKIs for Machine Readable Travel Documents – Protocols for the Management of Certificates and CRLs. Technical report, Federal Office for Information Security, 53133 Bonn, Germany, 2009. Technical Guideline TR-03129, Version 1.10.

[CV09] Rafik Chaabouni and Serge Vaudenay. The Extended Access Control for Machine Readable Travel Documents. In Arslan Brömme, Christoph Busch, and Detlef Hühnlein, editors, BIOSIG, volume 155 of LNI, pages 93-103. GI, 2009.

[Cha13a] Rafik Chaabouni. Solving Terminal Revocation in EAC by Augmenting Terminal Authentication (short paper version). In Arslan Brömme and Christoph Busch, editors, BIOSIG, volume 212 of LNI. GI, 2013.

[Cha13b] Rafik Chaabouni. Solving Terminal Revocation in EAC by Augmenting Terminal Authentication (full paper version). Cryptology ePrint Archive, Report 2013/460, 2013. http: //eprint.iacr.org/2013/460.

This work has been supported:
from research theme IUT2-1 and European Regional Development Fund through the Estonian Center of Excellence in Computer Science, EXCS ;
and by the Tiger University Program of the Information Technology Foundation for Education

tiigriülikool