mobiman
www.mobiman.me

Avoiding Man-in-the-Middle Attacks When Verifying Public Terminals

Gergely Alpár, Jaap-Henk Hoepman

IFIP Summer school 2011, 8 September

Participants in the Mobiman project:

TU/e Technische Universiteit Eindhoven University of Technology Where innovation starts
Radboud University Nijmegen
TNO
novay
ERICSSON

mobiman

Outline

- Motivation
- Man in the middle
- TPM
- Local verification

mobiman

Outline

- Motivation
- Man in the middle
- TPM
- Local verification

mobiman

Public terminals



ATM



POS



Public PC

mobiman

1999-2011



?



mobiman

Verification

Main transaction

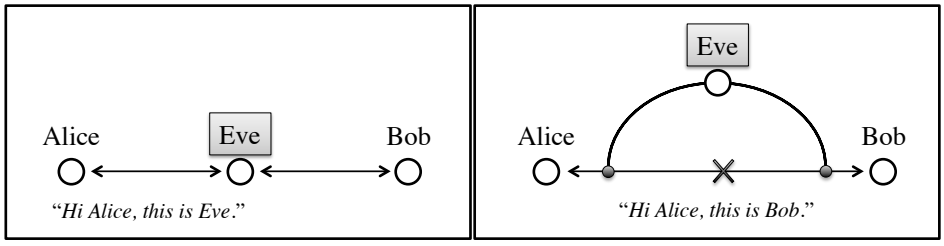
mobiman

Outline

- Motivation
- Man in the middle
- TPM
- Local verification

mobiman

Man-in-the-middle attacks



mobiman

Outline

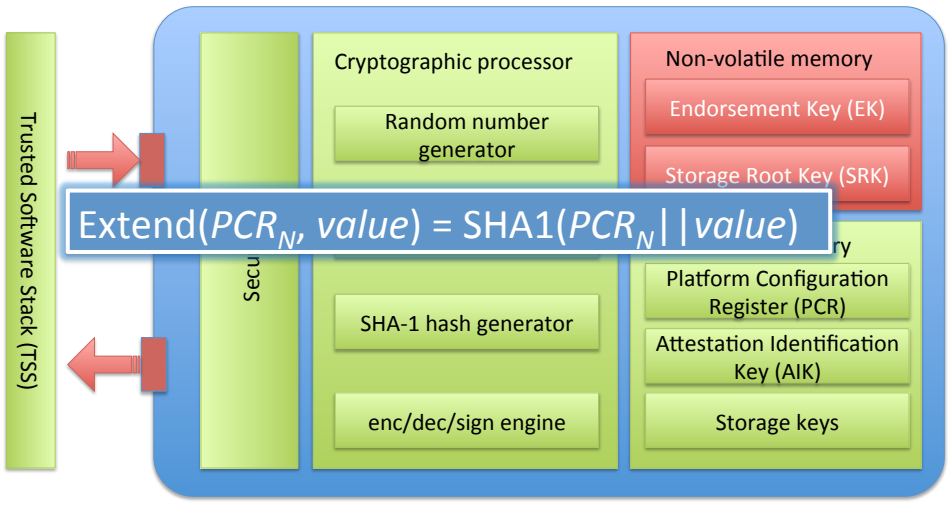
- Motivation
- Man in the middle
- TPM
- Local verification

mobiman

TPM

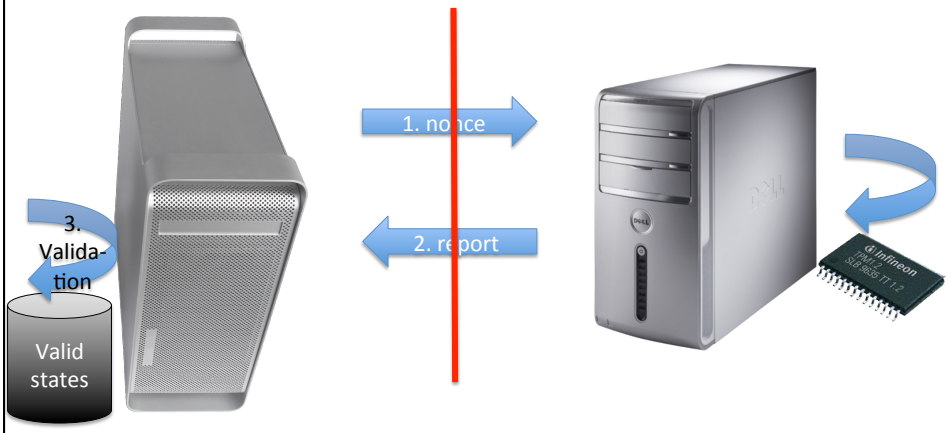


TPM Architecture



September 8, 2011. IFIP Summer school G. Alpár: Verifying Public Terminals 11

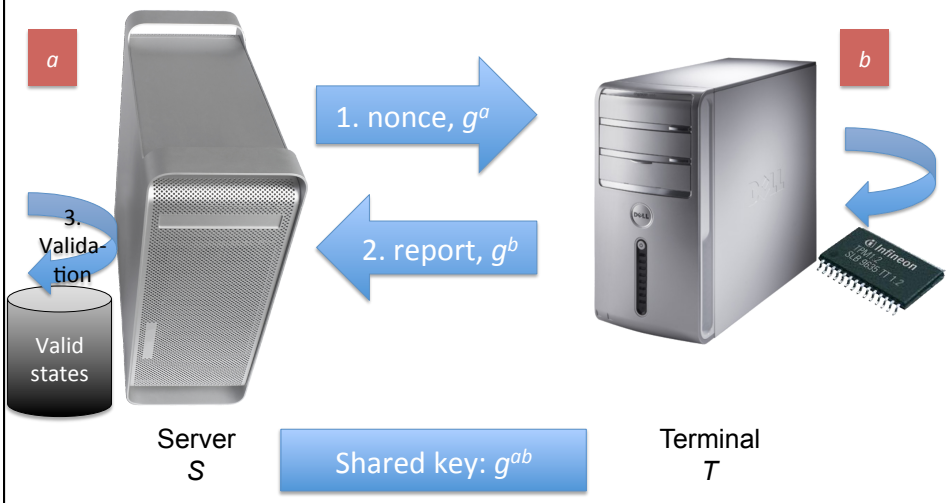
Remote Attestation



September 8, 2011. IFIP Summer school G. Alpár: Verifying Public Terminals 12

mobiman

Robust Integrity Reporting [Stumpf 2006]



mobiman

Outline

- Motivation
- Man in the middle
- TPM
- Local verification

mobiman

Scenario

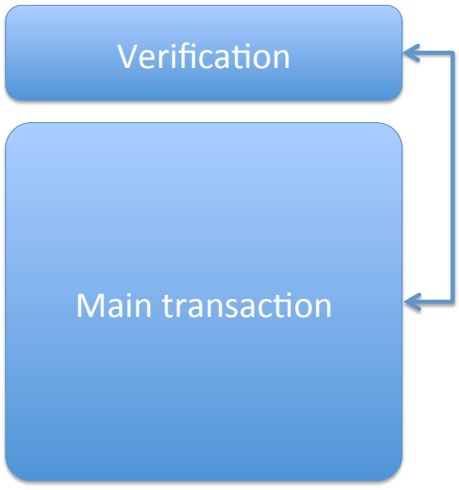
User + Mobile Device
U + M

Terminal/kiosk
T

Server
S

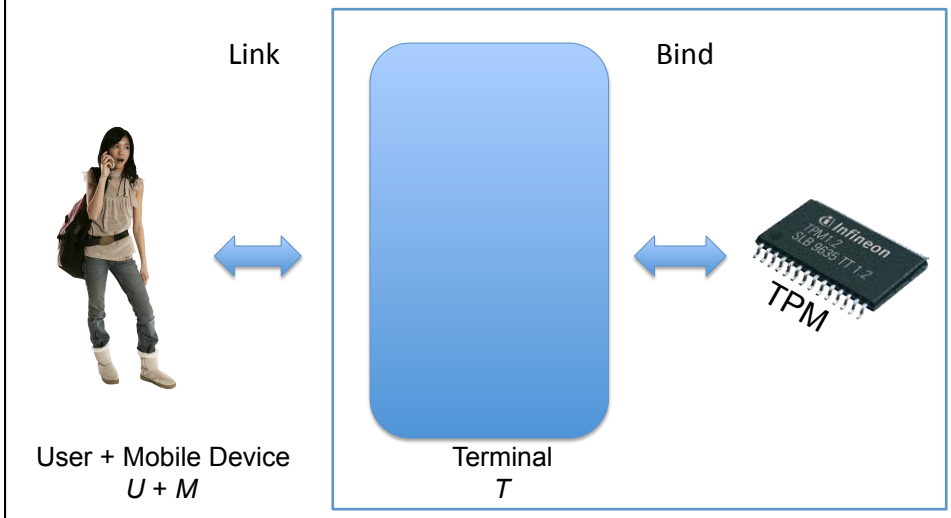


mobiman



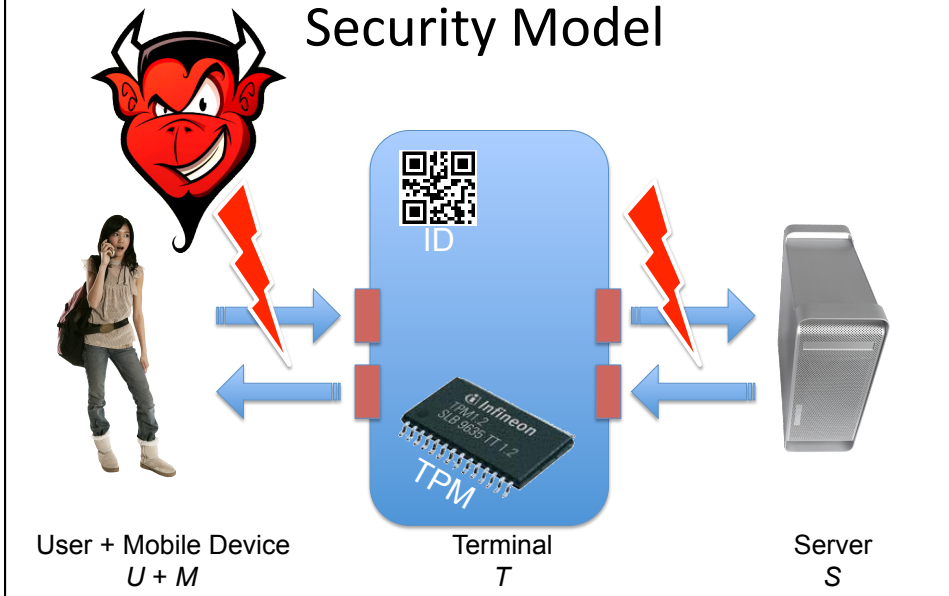
mobiman

Goal



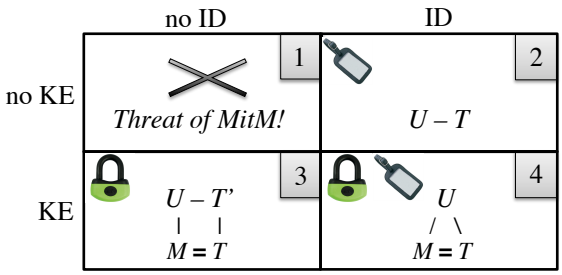
mobiman

Security Model



mobiman

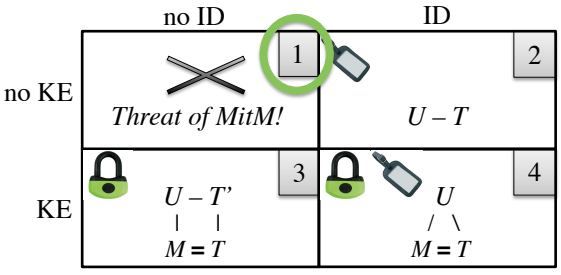
Identification and/or key exchange

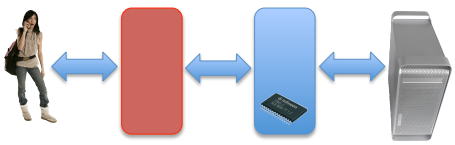




mobiman

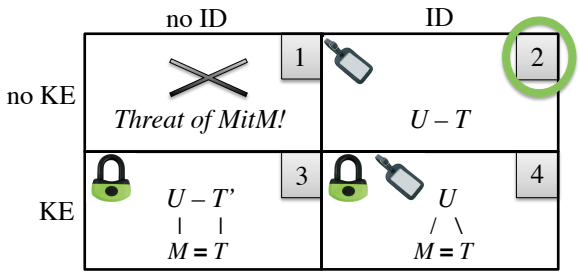
Identification and/or key exchange

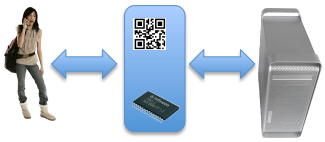




mobiman

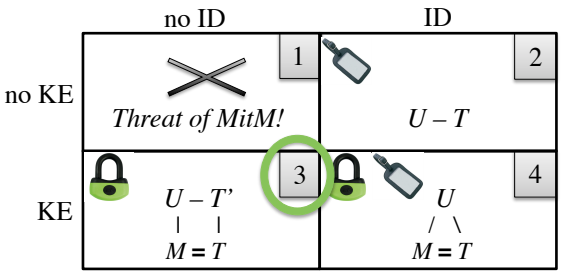
Identification [SiB, McCune et al. 2009]

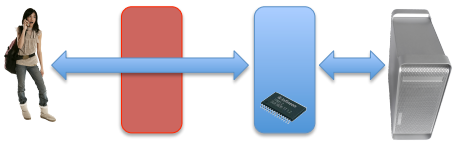




mobiman

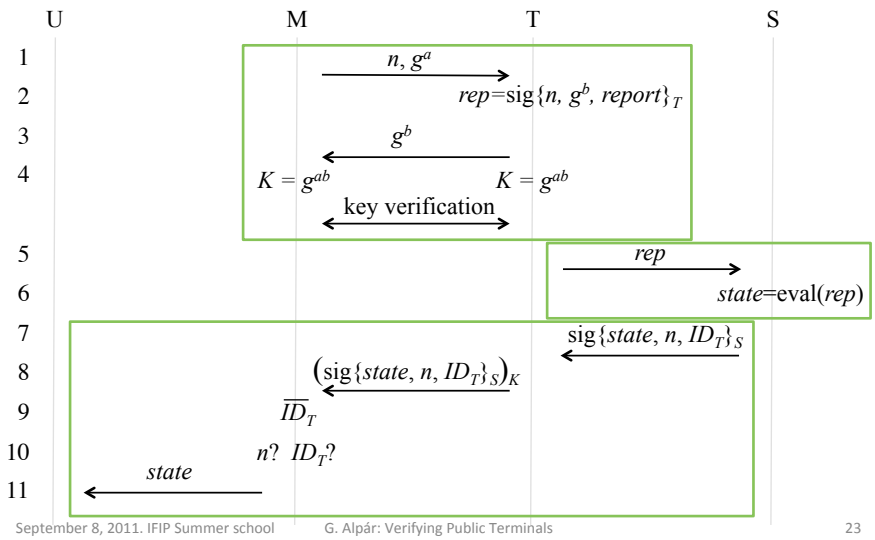
Key exchange





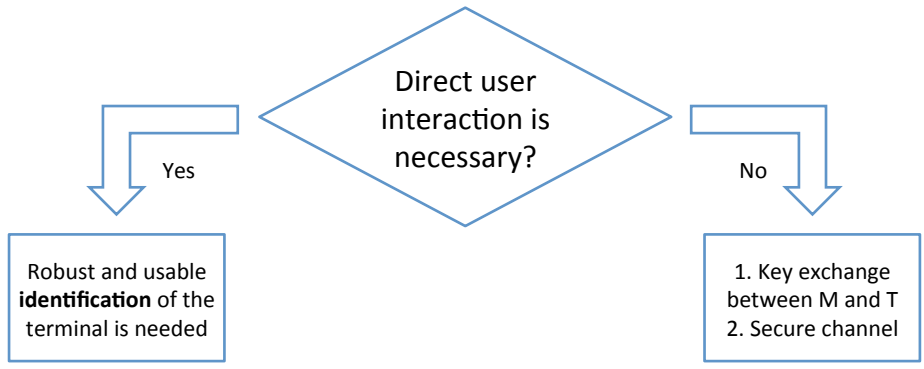
mobiman

Local verification



mobiman

Take away



mobiman

Open questions

- Verification of other devices
- Verification of environment
- Connection: M—S
- Semi-trusted or not trusted mobile device

Thanks for your attention!

Gergely Alpár
gergely@cs.ru.nl

mobiman

References

- **[ADSW99]** N. Asokan, H. Debar, M. Steiner and M. Waidner. *Authenticating public terminals*. Computer Networks, Volume 31, Issue 8, 23 April 1999, Pages 861-870.
- **[ATM2009]** ATM Fraud and Security Digest, March 2009. Source: http://www.atmsecurity.com/monthly-digest/atm-security-monthly-digest/atm-fraud-and-security-digest-march-2009.html
- **[BDS08]** E. Bangerter, M. Djackov, A.-R. Sadeghi. *A demonstrative ad hoc attestation system*. In ISC '08: Proceedings of the 11th international conference on Infor- mation Security, Berlin, Heidelberg, 2008. Springer-Verlag.
- **[McCune2009]** Jonathan M. McCune, Adrian Perrig, and Michael K. Reiter. Seeing-is-believing: using camera phones for human-verifiable authentication. International Journal of Security and Networks, 4(1- 2):43–56, 2009.
- **[Parno08]** Bryan Parno. *Bootstrapping trust in a "trusted" platform*. Proceedings of the 3rd conference on Hot topics in security, p.1-6, July 29, 2008, San Jose, CA
- **[Stumpf2006]** F. Stumpf, O. Tafreschi, P. Roeder, and C. Eckert. A Robust Integrity Reporting Protocol for Remote Attestation. In Proceedings of the Second Workshop on Advances in Trusted Computing (WATC '06 Fall), Tokyo, Dec. 2006.
- **[TH10]** R. Toegl and M. Hutter. *An approach to introducing locality in remote attestation using near field communications*. The Journal of Supercomputing, Springer, Volume 55, Number 2, 207-227, 2011.