Direct Anonymous Attestation in the Wild

10th January 2019, RWC 2019, San Jose

Matthew Casey, Liqun Chen, Thanassis Giannetsos, Chris Newton, Ralf Sasse, Steve Schneider, Helen Treharne, **Jorden Whitefield**

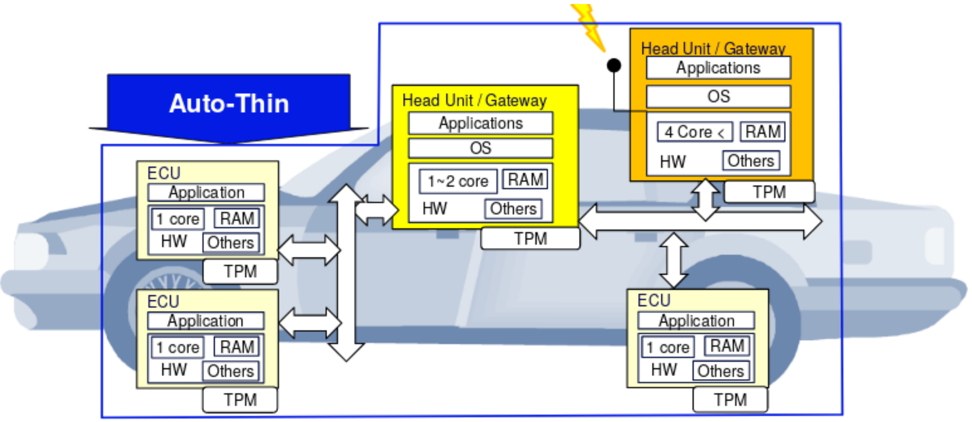
Outline

DAA in Theory

- History
- Formal Analysis

DAA in the Real World

- Vehicular use case
- Implementation challenges



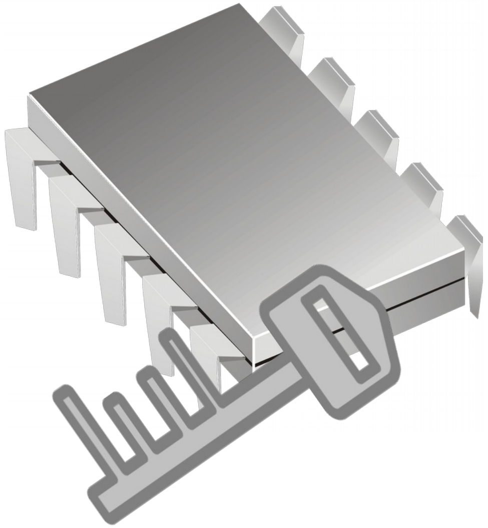
Direct Anonymous Attestation (DAA)

- Anonymous Digital Group Signature scheme
  - Strong but privacy-preserving authentication
  - ISO/IEC 20008 2013

- Hardware-backed attestation using Trusted Platform Modules (TPM)

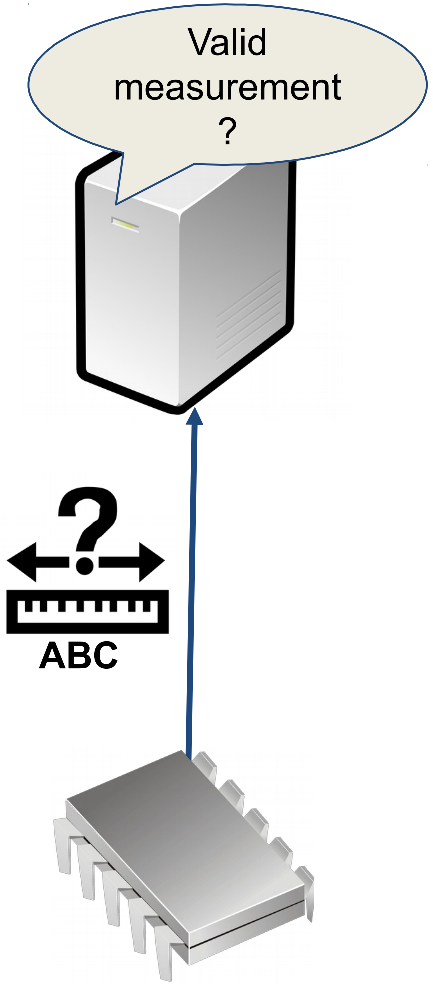
- Properties of DAA:
  - **User-controlled Anonymity**

  - **User-controlled Traceability**
    - Host controls whether signatures can be linked



DAA Schemes

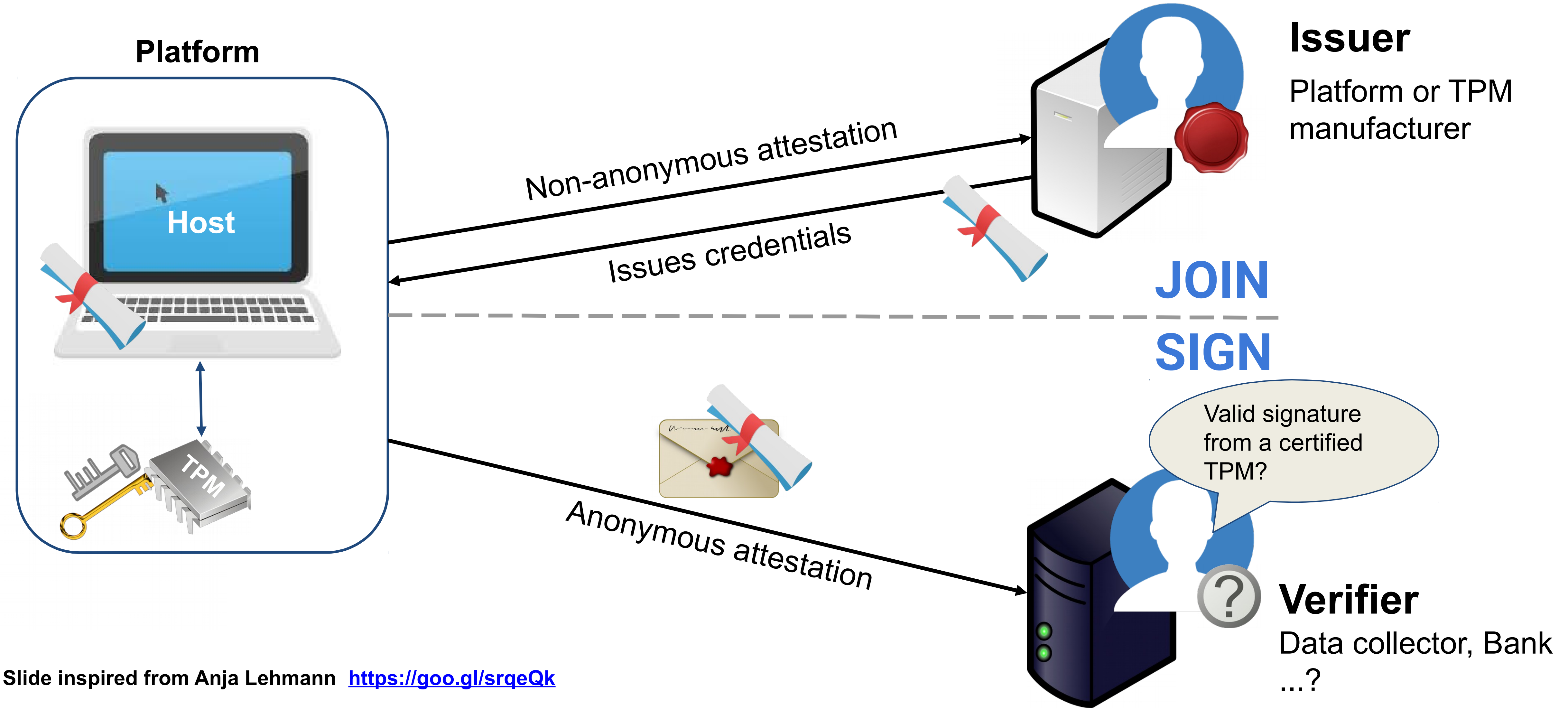
- **TPM 1.2** (RSA-based) [BCC04]
  - ISO/IEC 20008-2 mechanism 2
- **TPM 2.0** (pairing-based) [BCL08, BCL09]
  - ISO/IEC 20008-2 mechanism 4 & ISO/IEC 11889
  - Smaller keys & signatures!
  - Proposed for FIDO 2
- **Enhanced Privacy ID** (EPID) [BL07, BL11, BL12]
  - Used by Intel SGX
  - Improved revocation



TPM 2.0 DAA Vulnerabilities

- **TPM 2.0 API was insecure** [ANZ13]
  - Static Diffie-Hellman oracle present
  - Fix: updated protocol
- **Use of BN P256 curve**
  - 128-bit security reduced to 85-bit
  - Fix: Move to a larger curve
    - BN P638 already in standards

Overview of DAA

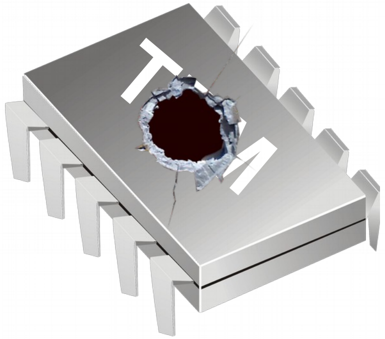


Platform
Host
TPM
Non-anonymous attestation
Issues credentials
Issuer
Platform or TPM manufacturer
JOIN
SIGN
Valid signature from a certified TPM?
Anonymous attestation
Verifier
Data collector, Bank ...?

* Slide inspired from Anja Lehmann https://goo.gl/srqeQk

Formal Analysis of ECC-DAA

Found an attack when the endorsement key of one TPM is compromised, the security of all TPMs cannot be guaranteed in a JOIN

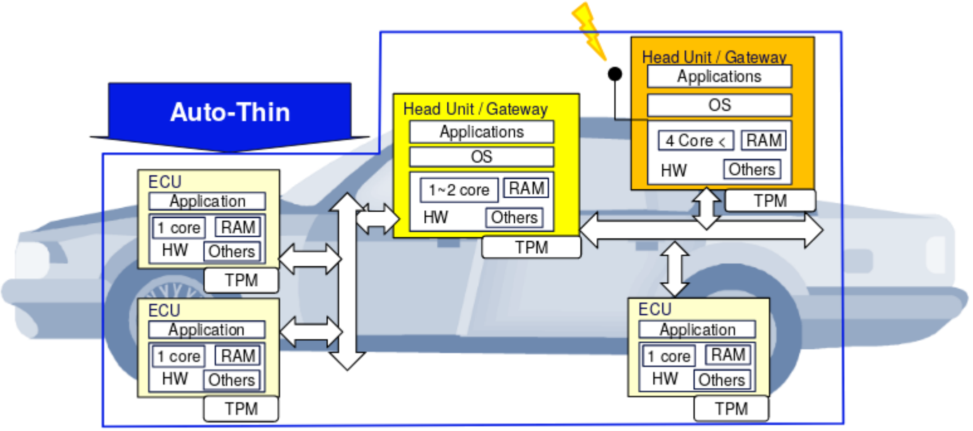


We have identified a fix by including a TPM endorsement public key during a JOIN

Proofs and Disproofs obtained using the Tamarin Prover
https://tamarin-prover.github.io/

DAA implementation in vehicular architecture

- Use-case targeting V2X communication using DAA
  - V2X requires authentication and privacy
  - State-of-the-art: Public Key Infrastructure



- TCG Automotive-thin profile for TPMs in vehicles [TCG15]

- Vehicle credentials (pseudonyms) can be **created**, **signed** and **verified** using DAA

"Privacy-Enhanced Capabilities for VANETS Using Direct Anonymous Attestation."
In *2017 IEEE Vehicular Networking Conference,*
VNC 2017

Implementation of vehicular architecture

Hardware

- Raspberry Pi 3B
- Infineon TPM 2.0 developer module
- NexCom VTC in-vehicle computer

Software

- C++ / Java
- OpenSSL
- AMCL Crypto Library
- IBM Trusted Software Stack

Implementation Timings

Operation	Approx. Time* (ms)
JOIN	820 + Issuer
CREATE and **CERTIFY** a pseudonym key	420
SIGN a message to send (ECDSA)	80
VERIFY a received message	
VERIFY the pseudonym key	200
VERIFY the message signature (ECDSA)	10
REVOKE	330

*Timings based upon measurements of the TPM commands and of the operations on the NexCom box. Values are given to the nearest 10ms.

TPM Implementation Challenges

- **Multiple TPMs had different versions**:
  - ECDAA signature for TPM 2.0 version 1.16 up to Errata 1.4, different to TPM 2.0 version 1.16 Errata up to 1.5 and TPM 2.0 version 1.38
  - Accommodating these differences made the system more complicated

- **Complexity:** >1600 pages of documentation!

- **Insecure curves**
  - BN P256 insecure
  - BN P638 secure but unimplemented in TPM
    - TCG should update standards to require more secure curves

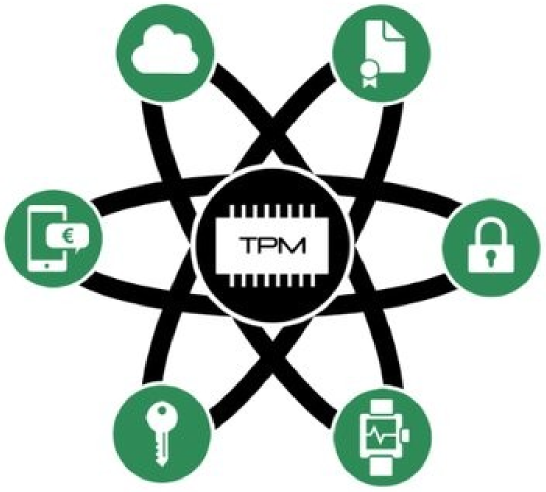
- **Compatible crypto libraries**
  - “*Exotic*” cryptography not widely implemented

Future TPM: A Quantum-Resistant TPM

Goal: To develop a **Quantum-Resistant** TPM

www.futuretpm.eu

@FutureTPM_H2020



HORIZON 2020

UNIVERSITY OF SURREY

infineon

UNIVERSITY OF BIRMINGHAM

ROYAL HOLLOWAY UNIVERSITY OF LONDON

TECHNIKON

IBM

Viva payments.com

UBITECH ubiquitous solutions

Suite5 We Deliver Intelligence

UNIVERSITY OF PIRAEUS RESEARCH CENTER

HUAWEI

inesc id lisboa

SnT securityandtrust.lu

DTU

Conclusion

TPM development is hard

Consider other use cases for DAA

Analysis of FIDO 2 ECDAA scheme

https://jwhitefield.co.uk

@sudo_jorden

Surrey Centre for Cyber Security

SCCS

ETH

Pervasive Intelligence

Emerging technologies. Real impact.

References

[BCC04] Brickell, Camenisch, Chen. Direct anonymous attestation. ACM CCS 04

[BCL08] Brickell, Chen, Li. A new direct anonymous attestation scheme from bilinear maps. Trust 2008

[BCL09] Brickell, Chen, Li. Simplified security notions of DAA and a concrete scheme from pairings. Int. J. Inf. Sec., 2009.

[BL07] Brickell, Li. Enhanced privacy ID: a direct anonymous attestation scheme with enhanced revocation capabilities. WPES 2007

[BL11] Brickell, Li. Enhanced privacy ID from bilinear pairing for hardware authentication and attestation. IJIPSI, 1(1):3 33, 2011.

[BL12] Brickell, Li. Enhanced Privacy ID: A Direct Anonymous Attestation Scheme with Enhanced Revocation Capabilities. TDSC 2012

[ANZ13] Acar, Nguyen, and Zaverucha, "A TPM Diffie-Hellman Oracle," Cryptology ePrint Archive, Report 2013/667, 2013, [link]

[BG04] Brown and Gallant, "The Static Diffie-Hellman Problem," Cryptology ePrint Archive, Report 2004/306, 2004 [link]

[TCG15] TCG TPM 2.0 Automotive Thin Profile For TPM Family 2.0; Level 0 [pdf]

[CCD+17] Camenisch, Chen, Drijvers, Lehmann, Novick, Urian. One TPM to Bind Them All: Fixing TPM2.0 for Provably Secure Anonymous Attestation. IEEE S&P 2017