



Trusted Computing

Direct Anonymous Attestation

Heiko Stamer <stamer@theory.informatik.uni-kassel.de>

76F7 3011 329D 27DB 8D7C 3F97 4F58 4EB8 FB2B E14F



⋮⋮⋮ Vertrauenswürdiges Rechnen?!

1. „Trusted Computing“ (TCG/TCPA)

- TCG Konsortium: AMD, HP, IBM, Intel, Sun, M\$
- „preiswerte“ Hardwareerweiterung (TPM)

2. „Trustworthy Computing“ (Microsoft)

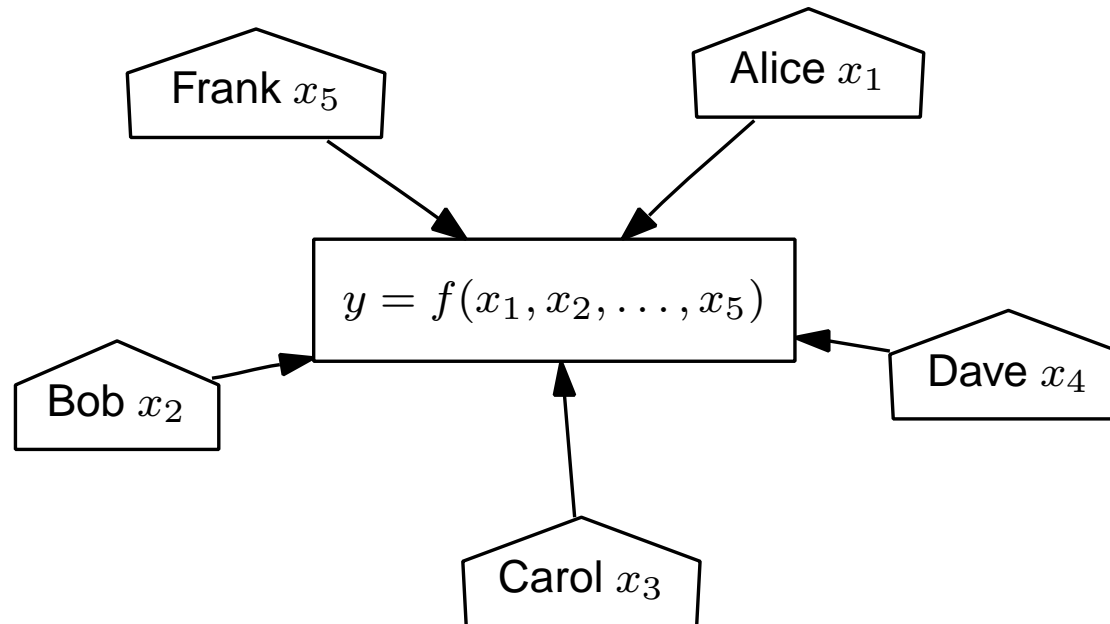
„We will have to overcome the distrust that people now feel for computers.“

- Security, Privacy, Reliability, Business Integrity
- NGSCB (Palladium) irgendwann im Longhorn

3. „Treachurous Computing“ (FSF)

- R. STALLMAN: „. . . the plan is designed to make sure your computer will systematically disobey you.“

Secure Multiparty Computation



- Berechnung einer Funktion f mit geheimen Argumenten x_i
- Anforderungen: Geheimnisbewahrung, Korrektheit, Robustheit
- Beispiele: Yao's Millionärs-Problem, Mentale Spiele, Wahlen

⋮⋮⋮ Richtlinien (TCG)

■ Privacy Effect of TCG Specifications

„ . . . to ensuring that TCG specifications provide for an increased data capability to secure personally identifiable information.“

■ Open Platform Development Model

„ . . . to preserving the open development model that enables any party to develop hardware, software or systems.“

„ . . . to preserving the freedom of choice that consumers enjoy with respect to hardware, software and platforms.“

■ Platform Owner and User

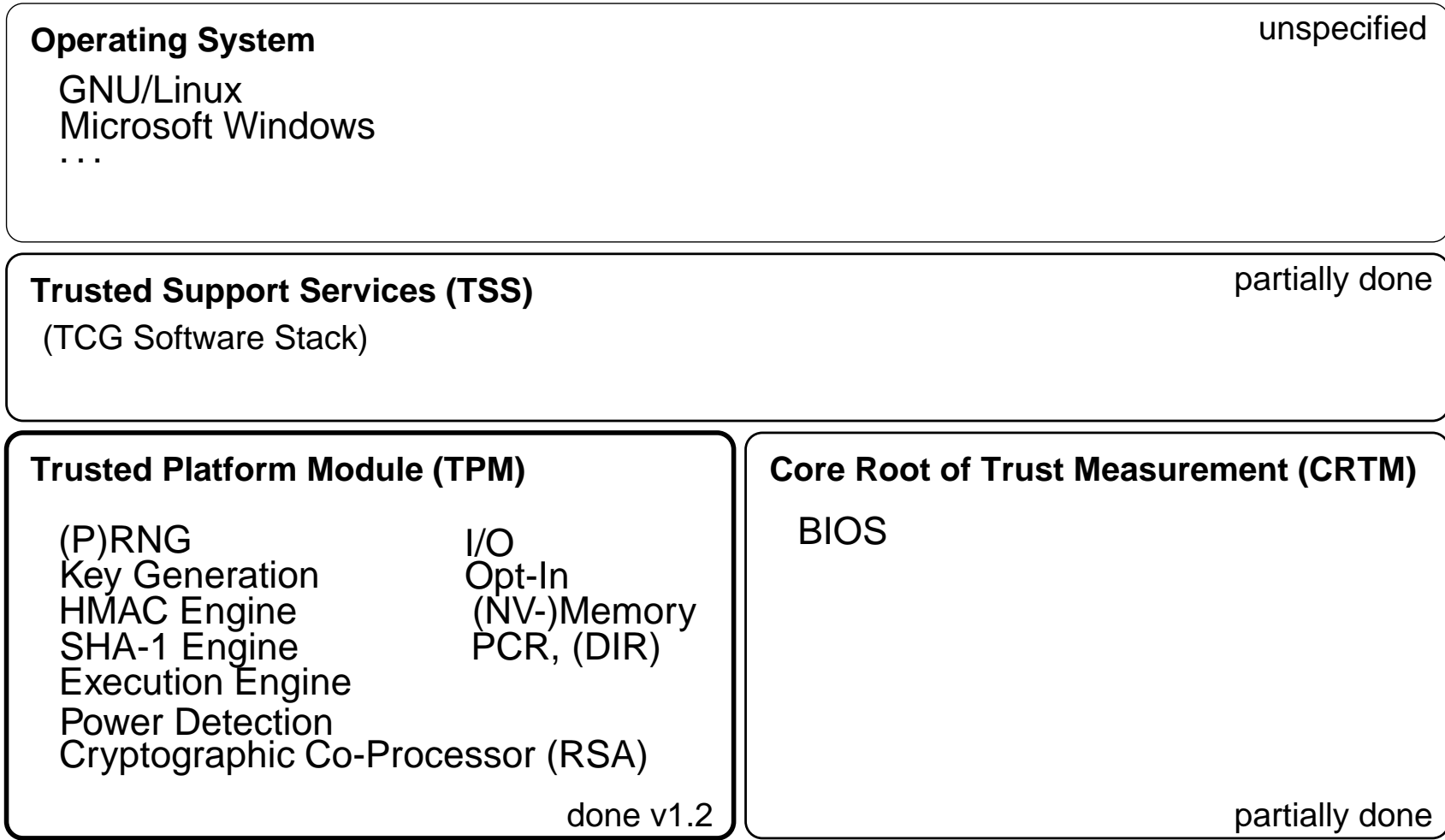
„ . . . to ensuring owners and users of computing platforms remain in full control of their computing platform.“

⋮⋮⋮ Funktionalität (TCG)

- Benutzermanagement (Unterscheidung Owner/ User)
 - Initialisierung, Aktivierung, Authentifizierung, ...
- Schlüsselmanagement (Eigentümer, Attribute ^a)
 - kryptographische Schlüssel sicher speichern
 - Endorsement Key (EK), Storage Root Key (SRK)
- Identitätsmanagement, Attestation
 - Erstellung und Verwaltung von Identitäten (Credentials)
- „Sicheres Booten“ (TPM als passiver Beobachter)
 - Akkumulierung eines Hashwertes im internen Register (PCR)
 - Vergleich mit vorher gespeicherten Daten (Manipulation?)

^a(nicht-)migrierbar, Passwort geschützt, an Bootsequenz gebunden, ...

⋮⋮⋮ Komponenten (TCG)



⋮⋮⋮ Neuerungen in Version 1.2 (TCG)

■ Erasable Endorsement Key

- neu: interner Schlüssel löscher, falls mit Attribut „löscher“ vom Hersteller erzeugt
- aber: neue (EK-)Zertifikate notwendig (Computer-TÜV?)

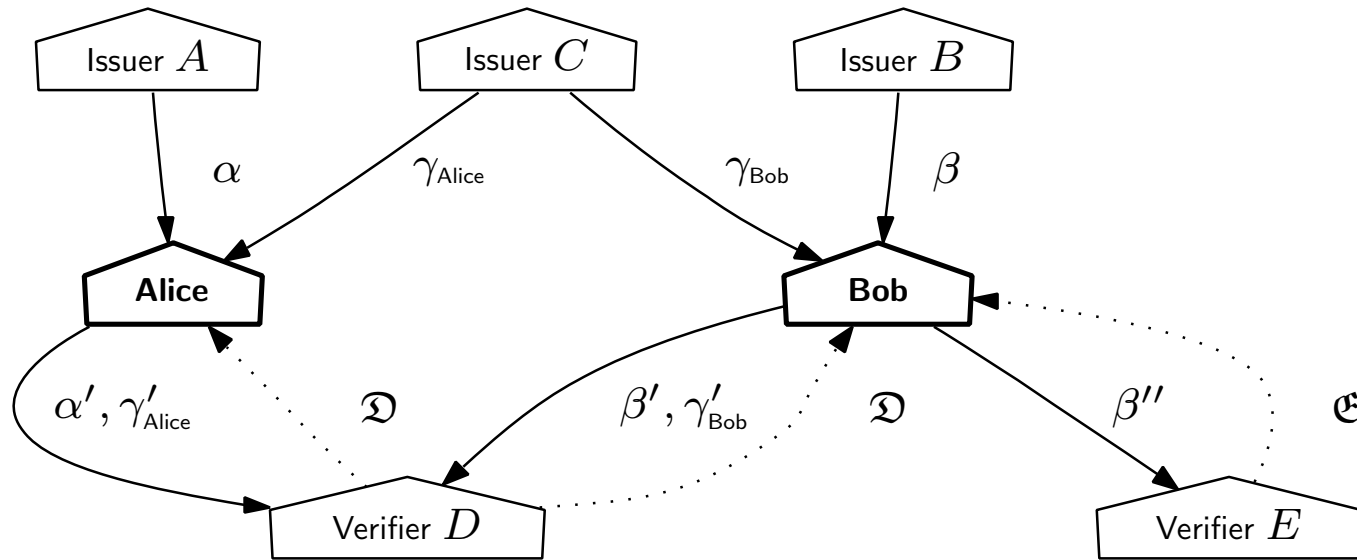
■ Transport Protection

- neu: Schutz der Transportkanäle TPM ↔ (remote) Anwendung
- aber: optionales Logging der TPM-Operationen innerhalb einer Transportsitzung als Ausführungsgarantie (assurance)

■ Direct Anonymous Attestation (DAA)

- bisher: Attestation durch beglaubigte AIKs (CA Infrastruktur)
- neu: Anonymous Credential System (Gruppensignaturschema)
- aber: Einschränkung durch Named-Base/ Rogue Tagging

Anonymous Credential System



- Unforgeability of Credentials (attack of colluding users)
- Consistency of Credentials (pooling doesn't help)
- Protection of User's Privacy (anonymity, unlinkability)

Anonymous Credential System (2)

- Anonymity Revocation (local, global)
- Sharing of Credentials (all-or-nothing)
- One-Show vs. Multi-Show Credentials
- Revocation of Credentials
- Encoding of Attributes (EPAL, ...)

JAN CAMENISCH, ANNA LYSYANSKAYA: *Efficient Non-transferable Anonymous Multi-show Credential System with Optional Anonymity Revocation*, EUROCRYPT 2001, Lecture Notes in Computer Science, Vol. 2045

- IBM idemix: <http://www.zurich.ibm.com/security/idemix/>

Direct Anonymous Attestation

ERNIE BRICKELL, JAN CAMENISCH, LIQUN CHEN: *Direct Anonymous Attestation*
Technical Report HPL-2004-93, HP Labs, 2004

- „... group signature scheme without the capability to open signatures (or anonymity revocation) but with a mechanism to detect rough members (TPMs).“

Assumption 1 (Strong RSA, Flexible RSA Problem)

On input of a random RSA modulus n and $u \in \mathbb{Z}_n^$ it is computational infeasible, to compute values $e > 1$ and v such that $v^e \equiv u \pmod{n}$.*

$$S - \text{RSA} \leq_{\mathcal{P}} \text{RSA} \leq_{\mathcal{P}} \text{FACTORING}$$

Theorem 1 (CAMENISCH et al.)

Unforgeability of DAA-Credentials holds under S – RSA assumption.

Direct Anonymous Attestation (2)

Assumption 2 (Decisional Diffie-Hellman in prime order subgroup)

Let Γ be an ℓ_Γ -bit prime and ρ is an ℓ_ρ -bit prime such that $\rho | (\Gamma - 1)$.

Let $\gamma \in \mathbb{Z}_\Gamma^*$ be an element of order ρ .

Then, for sufficiently large values of ℓ_Γ and ℓ_ρ , the distribution $\{(\delta, \delta^a, \delta^b, \delta^{ab})\}$ is computationally indistinguishable from distribution $\{(\delta, \delta^a, \delta^b, \delta^c)\}$, where δ is a random element from the subgroup generated by γ , and a, b, c are random elements from $[0, \rho - 1]$.

$$\text{DDH} \leq_{\mathcal{P}} \text{CDH} \leq_{\mathcal{P}} \text{DLOG}$$

Theorem 2 (CAMENISCH et al.)

Privacy/Anonymity in DAA is guaranteed under the DDH assumption.

Further, for turning the proofs of knowledge into signatures (Fiat-Shamir heuristic), the cryptographic hash function (SHA-1) is assumed to behave like a random oracle.

Direct Anonymous Attestation (3)

- TPM computes secret message f from DAAseed and cnt
- Host verifies issuer's public key (check parameters and NIZK-proofs)

DAA_JOIN: only pseudonymity, fixed base $\zeta_I := (H_\Gamma(1||\text{bsn}_I))^{(\Gamma-1)/\rho} \bmod \Gamma$

1. TPM computes: pseudonym $N_I = \zeta_I^f \bmod \Gamma$, commitment U
2. Issuer checks rough list: $\forall f' : N_I \stackrel{?}{\neq} \zeta^{f'} \pmod{\Gamma}$
3. TPM proves knowledge of f w.r.t. U to the issuer
4. Issuer computes: CAMENISCH-LYSYANSKAYA (CL) signature v
5. Issuer proves correctness of CL-signature v to the host

DAA_SIGN: unlinkability, only if random base $\zeta_V \in_R \langle \gamma \rangle$ used

1. TPM computes: (random) pseudonym $N_V = \zeta_V^f \bmod \Gamma$
2. Host and TPM compute together „signature of knowledge“ σ w.r.t. v
3. Verifier checks σ and rough list: $\forall f' : N_V \stackrel{?}{\neq} \zeta^{f'} \pmod{\Gamma}$

⋮⋮⋮ Verbesserungen, Forderungen

KLAUS KURSAWE, CHRISTIAN STÜBLE: *Improving End-user Security and Trustworthiness of TCG-Platforms*, 33. GI-Fachtagung, 2003

CHAOS COMPUTER CLUB: *TCPA - Whom do we have to trust today?*
<http://www.ccc.de/digital-rights/forderungen>

SETH SCHOEN: *Trusted Computing — Promise and Risk*
http://www.eff.org/Infrastructure/trusted_computing/20031001_tc.php

- „Owner Override“ prevents some DRM scenarios
 - PCR-Werte können vom Plattformeigentümer mit virtuellen Werten substituiert werden („fake PCR“ analog „fake user agent“)
- Key Migration for SRK (little changes in 1.2)
 - migrierbare Schlüssel (EK, SRK non-migratable) sind unter „kontrollierten Umständen“ (TPM₁ → TPM₂) übertragbar
- DAA-„random base“ for privacy (EU-Datenschutzgruppe 01/2004)

⋮ Kritik und Diskussion

- Monopolförderung durch Plattformbindung
 - Szenarien: proprietäre Dateiformate, DRM, „Browserkrieg“
- Wieso sollten wir den TPM-Herstellern vertrauen?
 - Aus Kostengründen: Erzeugung des EK, SRK, DAAseed außerhalb des TPM? Wer hat Zugriff auf diese Schlüssel?
 - Hardwareanalyse ist oft schwieriger als Softwareanalyse!
- „trügerische Sicherheit“ durch Trusted Computing
 - ↳ Softwarehersteller werden schnell nachlässig
- Werden die Interessen der Benutzer gegenüber den Interessen der Wirtschaft gleichrangig berücksichtigt?
 - kein Vertreter der Benutzerschaft (EFF, CCC, ...) in der TCG
 - „reasonable and non-discriminatory“ Patentlizenzierung (RAND)

Quellen und Literatur

- [Wei04] RÜDIGER WEIS: *T* Computing – Big Brothers are watching You*,
<http://www.cryptolabs.org/tcpa/DStcWeis23.html>
- [Pfi03] ROY PFITZNER: *TCPA, Palladium und DRM – Technische Analyse und Aspekte des Datenschutzes*, Landesbeauftragter für den Datenschutz (Brandenburg), 2003
- [TCG03] TRUSTED COMPUTING GROUP: *TPM Specification Version 1.2 (Design Principles, Structures, Commands)*, 2003,
<https://www.trustedcomputinggroup.org/>
- [Kur03] KLAUS KURSAWE: *TCG und NGSCB Überblick*,
Vortragsfolien RTWH Aachen, 2003
- [MüBib] MICHAEL MÜHLE: *TCPA-Info (Literatursammlung)*
<http://www.mouling.de/projects/tcpainfo/lokal/bib/>

Direct Anonymous Attestation

[BCC04] ERNIE BRICKELL, JAN CAMENISCH, LIQUN CHEN: *Direct Anonymous Attestation*, Technical Report HPL-2004-93, HP Labs, 2004

<http://www.hpl.hp.com/techreports/2004/HPL-2004-93.html>

- „... group signature scheme without the capability to open signatures (or anonymity revocation) but with a mechanism to detect rogue members (TPMs).“

Why should users trust the vendors?

- „... Another extension would to guaranteed anonymity/pseudonymity to the host (in fact to its user) even if the TPM deviates from the protocol [ChP93].“
- ~> new threat cases (imH) and (ImH) for security proofs
scenario: corrupted TPM with uncorrupted host (CPU/ TSS)

⋮ One possible Covert Channel in DAA

Example 1 (DAA-Signing Protocol [BCC04])

3. (b) ii. The TPM chooses a random $n_t \in \{0, 1\}^{\ell_\emptyset}$ and computes

$$c := H(H(c_h || n_t) || b || m) \in [0, 2^{\ell_\kappa} - 1]$$

and sends c, n_t to the host.

...

4. The host outputs the signature

$$\sigma := (\zeta, (T_1, T_2), N_V, c, n_t, (s_v, s_{f_0}, s_{f_1}, s_e, s_{ee}, s_w, s_{ew}, s_r, s_{er})) .$$

Dora can use n_t to establish a subliminal channel. (outflow of secrets)

RÜDIGER WEIS, STEFAN LUCKS: „All Your Keybit Are Belong To Us“ — The Truth about Blackbox Cryptography, 3rd International SANE Conference 2002, Maastricht

Privacy-enhanced DAA protocols

[ChP93] DAVID CHAUM, TORBEN P. PEDERSEN: *Wallet Databases with Observers*
Advances in Cryptology — CRYPTO '92, LNCS Vol. 740, pp. 89–105, 1993

- C : computer (hard- and software) controlled by the user (host)
- T : tamper-proof module issued by organizations (TPM)
- ~> A tamper-proof only solution provides only *pure trust* instead of *computational or unconditional privacy*.
- DAA protocols should be protected against unexpected and subliminal *information outflow/ inflow* from/ to T .
- ~> Solution: *coin-flipping protocols* and *blind signatures*

Is the TCG really interested in such privacy enhancements?