Trusted Computing - eine unendliche Geschichte

Ruediger Weis, cryptolabs Amsterdam
Andreas Bogk, Chaos Computer Club Berlin

Abstract

Nach heftigen Protesten ist die Trusted Computing Group 2004 auf einige Kritikpunkte teilweise eingegangen. So kündigte Microsoft eine grundlegende Überarbeitung von NGSB an. Die TCG schrieb einen verbesserten Schutz der Privatsphäre in den neuen Standard 1.2. Auch zeichnet sich eine grössere Dialogbereitschaft in Teilbereichen ab. Ärgerlich hingegen ist, dass einige Firmen versuchen im zweistelligen Millionenbereich Geräte mit der veralteten weniger benutzerfreundliche Version TCG1.1b in den Markt zu drücken. Auch durch die trotz gegenteiliger Anfrage der Bundesregierung vorgenommene Integration der kryptographischen Funktionalitäten in "Super-I/O-Chips" treten neue Sicherheitsprobleme auf. Auch sind zentrale Fragestellungen wie, die Problem der Nutzerbevormundung und der Wettbewerbsbehinderungen, weiterhin ungelöst. Dies wird inzwischen auch von Forschern aus der Industrie offen eingeräumt. Eine wissenschaftliche Analyse zeigt weiterhin, dass der neu eingeführte verbesserte Nutzerschutz (DAA) einfach wieder aufgehoben werden kann. Zudem erschweren zahlreiche Fehler und Unklarheiten im Standard die Implementierung. Die Hindernisse für die Entwicklung und Verwendung von Open Source Software sind aktuelle Entwicklungen insbesondere im Bereiche der Software-Patente sogar noch weiter angewachsen.

1 Trusted Computing

Die Trusted Computing Platform Alliance (TCPA) [TCPA03] wurde 1999 von Intel, Microsoft, HP, Compaq und IBM gegründet. Im Februar 2002 wurde die TCPA Main Specification v1.1b veröffentlicht. Im April 2003 gründeten AMD, HP, IBM, Intel und Microsoft die Trusted Computing Group (TCG) [TCG03]. Im Gegensatz zur TCPA verfügt die TCG über eine straffe Organisation mit stark unterschiedlichen Mitwirkungsrechten der beteiligten Firmen (siehe auch [Koe03]). Neben der von der TCG erarbeiteten Architektur plant Microsoft mit hohem Aufwand ein von Software-Patenten geschütztes eigenes Konzept für Trustworthy Computing unter dem Namen Palladium. Dieses wurde 2003 in next-generation secure computing base (NGSCB) umbenannt. Im Mai 2004 kündigt Microsoft eine umfassende Überarbeitung von NGSCB an.

Zentraler Hardwarebaustein der TCG Architektur ist das sogenannte Trusted Platform Module (TPM) (vgl. Fritz Chip) [BR04]. In den ersten Implemen-

tationen kann man sich dies als eine an den LPC Bus festgelötete Smart-Card vorstellen. Es bestehen jedoch auch Planungen, die kryptographischen Funktionalitäten direkt in Prozessoren (vgl. Intel LaGrande) oder Input/Output-Bausteinen zu integrieren.

Wesentliche Designpunkte der Architektur sind

- Hardware-Speicher für kryptographische Schlüssel
- Unterstützung von sicherem Booten
- Remote Platform Attestation und
- kryptographisches Sealing.

2 Chancen ...

Sicherer Hardwarespeicher und ein kontrollierbarer Bootprozess werden allgemein als eine wünschenswerte Verbesserung der Systemsicherheit angesehen.

2.1 Sicherer Hardware-Speicher

Die Tatsache, dass auf den meisten Computersystemen kein geschützter Bereich zur Speicherung von kryptographischen Schlüsseln und anderer besonders schützenswerter Informationen zur Verfügung steht, ist eines der Kernprobleme der Computersicherheit. In der Regel können beispielsweise Angreifer, welche für kurze Zeit die Kontrolle über ein System erhalten, geheime Schlüssel kopieren. Eine Verschlüsselung der Schlüsselinformationen mit Hilfe eines Benutzerpasswortes ist zwar eine durchaus empfehlenswerte Manahme, jedoch sind in diesem Szenario Wörterbuchattacken erschreckend erfolgreich.

2.2 Sicheres Booten

Die Unterstützung eines sicheren Bootprozesses ist insbesondere nach dem Entdecken einer Systemkompromittierung eine höchst hilfreiche Erweiterung der Sicherheitsarchitektur. Überraschenderweise ist aber auch dieser Bereich durch eine hohe Unsicherheit bezüglich existierender Software-Patenten gezeichnet (s.a. [ASF97, AFS98]).

2.3 Smart-Card Systeme

Recht ähnliche Sicherheitsfeatures können bereits heute mit Smart-Card-basierten Systemen erreicht werden. Smart-Cards bieten darüber hinaus eine weit höhere Flexibilität. In groer Vielzahl erhältliche Kombinationen aus Smart-Card und Smart-Card-Leser für den USB Anschluss ersparen die Beschaffung von separaten Lesegeräten. Entwürfe für eine kryptographische Absicherung des USB-Ports befinden sich im Moment in der Standardisierungsdiskussion.

3 ... und Risiken

Eine grundlegende Änderung der gesamten IT Struktur ist natürlich auch mit Problemen verbunden. Insbesondere die Bereiche der Remote Platform Attestation und des Sealings sind hoch umstritten.

3.1 Remote Platform Attestation

Remote Platform Attestation ermöglicht einer externen Partei, über das Netzwerk den genauen Zustand des Nutzer-Computers auszulesen. Hierdurch kann der Computer vor dem Besitzer zum Vorteil von Diensteanbietern geschützt werden.

3.2 Sealing

Sealing wird dazu eingesetzt Daten an einen bestimmten Computer zu binden. Damit sollen beispielsweise Geschäftsmodelle unterstützt werden, bei denen für jedes Endgerät eine eigene Lizenz erworben werden muss.

3.3 Virtuelle Set-Top-Box

MIT-Professor Ron Rivest formulierte diesen Sachverhalt folgendermaen:

> The right way to look at this is you are putting a virtual set-top box inside your PC. You are essentially renting out part of your PC to people you may not trust.

Dass existierende Befürchtungen betreffend erheblicher Eingriffe in die persönlichen Computersysteme nicht völlig aus der Luft gegriffen sind, zeigt unter anderem eine Lektüre von Microsoft Lizenzen:

> Microsoft may provide security related updates to the OS Components that will be automatically downloaded onto your computer. These security related updates may disable your ability to copy and/or play Secure Content and use other software on your computer. (Microsoft, Windows Media Player 7.1, EULA)

Viele Endnutzer-Lizenzen vom Microsoft sind innerhalb der EU juristisch nicht haltbar. Ein sich nicht unter der vollständigen Kontrolle des Computerbesitzers befindlicher Hardwarebaustein könnte dazu verwendet werden, rechtswidrige, verbraucherunfreundliche Lizenzen technisch zu erzwingen.

3.4 Kryptographische Kritikpunkte

Dreh- und Angelpunkt der diskutierten Architekturen ist ein eindeutiger privater Schlüssel (Endorsement Key), über welchen der Anwender keine volle Kontrolle hat. Auf der RSA Conference im April 2003 in San Francisco äuerten sich viele der führenden Kryptographen sehr kritisch zu dieser Designentscheidung.

Whitfield Diffie, einer der Entdecker der Public-Key Kryptographie, zeigte sich besorgt über die dominierende Stellung vom Microsoft und forderte, dass die Benutzer die vollständige Kontrolle über die Schlüssel des eigenen Computers behalten sollten:

- (The Microsoft approach) lends itself to market domination, lock out, and not really owning your own computer. That's going to create a fight that dwarfs the debates of the 1990's.
- To risk sloganeering, I say you need to hold the keys to your own computer.
-

Auch Professor Ron Rivest (MIT), 2002 Gewinner des Turing Award, welcher allgemein als eine Art Nobelpreis der Informatik angesehen wird, mahnte eindringlich, die möglichen Konsequenzen gründlich abzuwägen:

- We should be watching this to make sure there are the proper levels of support we really do want.
- We need to understand the full implications of this architecture. This stuff may slip quietly on to people's desktops, but I suspect it will be more a case of a lot of debate.
- Privacy tends to go down in inverse to the number of transistors in the world. Interessanterweise ist Ron Rivest unter anderem auch Mitentwickler des RSA-Algorithmus und der MD4-Hash-Funktionen-Familie also den zentralen kryptographischen Algorithmen, welche im TPM Anwendung finden.

Von der kryptographischen Forschergemeinde wird einhellig begrüt, dass die TCG bei der Algorithmenwahl auf standardisierte Verfahren (RSA, SHA-1, AES) setzt. Allerdings erscheint die Verwendung der 160-bit Hashfunktion SHA-1 nicht mehr zeitgemä. Für den Bereich der symmetrischen Verschlüsselung sei zur Erhöhung der Sicherheit nochmals die grundsätzliche Verwendung von AES256 angeregt [LW02].

3.5 Gefahren von Black-Box-Kryptographie

Seit vielen Jahren warnen Kryptographen, dass verdeckte Kanäle bei der Verwendung von kryptographischer Hardware leicht zu implementieren sind. Im August 2003 warnte sogar die NSA in einer Stellungnahme explizit vor derartigen Möglichkeiten [HN03]. Es ist unter anderem möglich, mit veröffentlichten Verfahren geheime Informationen aus einem beweisbar sicherem Blackbox System sogar beweisbar sicher heraus zu schmuggeln. Bei einigen Systemen (siehe z.B. [WL02]) kann selbst eine Hardware-Analyse nicht aufdecken, welche Informationen verdeckt übertragen wurden, und für einen erfolgreichen Angriff müssen lediglich eine kleine Anzahl von zeitlich nicht notwendigerweise zusammen hängenden Chiffre-Texten passiv abgehört werden.

Aus diesem Grunde ist es von grossem Belang, dass sämtliche Designunterlagen und auch der eigentliche Herstellungsprozess von vertrauenswürdigen, internationalen Institutionen vollständig kontrolliert werden.

3.6 Neue Probleme durch Integration

Eine zunehmende Intgration von elektronischen Bausteinen macht diesen Evaluationsprozess in der Praxis immer schwieriger. IBM verbaute Millionenfach die Super-I/O Baustein PC8374T bzw. PC8392T von National Semiconductors.

Diese kombinieren Schnittstellen für Tastaur, Maus, Drucker, Floppy-Laufwerk und RS-232 mit eine TCG-1.1b-Trusted Platform Module. Neben der Tatsache, dass hierbei die veraltete Version des TCG Standards , ohne die in TCG 1.2 eingeführten Sicherheitsverbesserungen Verwendung findet, warnten Wissenschaftler schon seit Jahren vor einer derartigen Vermischung.

So findet man auch in der Stellungnahme der Bundesregierung zu den Sicherheitsinitiativen TCG und NGSCB im Bereich Trusted Computing auf Seite 2 f., Absatz 2.2. folgendes klares Statement:

"Um die Funktionen des Sicherheitsmodules eindeutig zuordnen zu können und eine eindeutige Prüffähigkeit zu gewährleisten, müssen sie Sicherheitsfunktionen an eine zentralen Stellle in einem seperaten Baustein (TPM) gebündelt werden. Eine Vermischung des Sicherheitsmoduduls mit anderen Funktionseinheiten (z.B. CPU, Chipsatz, etc.) führt zu Intransparenz und dazu, dass eine sicherheitstechnische überprüfung nicht mehr einfach durchführbar ist."

3.7 (US) Regierungszugriffe

Da Microsoft sowie die anderen führenden Unternehmen der TCG als privatrechtliche Firmen der US Gesetzgebung unterstehen, sollten auch mögliche Eingriffe durch US-Behörden Berücksichtigung finden. Auf die mehrfach vorgebrachte Sorge, dass die Verwendung von starker Kryptographie Begehrlichkeiten der US Behörden wecken könnte, antwortete Microsoft folgendermaen [MS03]:

- Q: Won't the FBI, CIA, NSA, etc. want a back door?
- A: Microsoft will never voluntarily place a back door in any of its products and would fiercely resist any government attempt to require back doors in products. From a security perspective, such back doors are an unacceptable security risk because they would permit unscrupulous individuals to compromise the confidentiality, integrity, and availability of our customers' data and systems. ... Zwar wird Microsoft bezüglich der Ablehnung von Hintertüren weithin Glauben geschenkt, jedoch weisen insbesondere die Worte never voluntarily auf ein offensichtliches Dilemma hin. Es dürfte Microsoft schwer fallen, Weisungen der US-Regierung beispielsweise im Kampf gegen den Terrorismus nicht Folge zu leisten.

3.8 Open Source

Software Da Microsoft einen überwältigenden Anteil des Betriebssystem-Marktes beherrscht, können Trusted Computing und NGSCB nur schwerlich isoliert betrachtet werden. Zusätzlich sind allerdings auch die Auswirkungen der neuen Architekturen auf Open Source Software zu untersuchen.

Einige Firmen forschen an einer TCG-enhanced-Version von GNU/Linux. Nach Ansicht der meisten Experten ist es erforderlich, Programme, welche in einem trusted Bereich laufen, auf Sicherheit zu untersuchen. Dies hat umfangreiche Auswirkung auf die Entwicklung von freier Software [San04]. Nach einer wahrscheinlich kostspieligen Evaluation könnte eine Version des Programmes digital unterzeichnet werden. Diese Entwicklung muss unter GPL bleiben. Jedoch macht jede Änderung, die ja laut GPL weiterhin möglich sein muss, die Signatur ungültig.

Peter N. Biddle, Microsoft Product Unit Manager Palladium, äuerte sich zu dieser Problemstellung auf der Comdex 2002:

> Grundsätzlich könnte die gesamte Palladium-Architektur auch nach Linux portiert werden, wenn die Lizenzvorbehalte im Stil der GPL nicht wären. Jeder Code für ein TPM wird von der TCPA signiert und verschlüsselt. Wird irgendetwas weiter geben, verändert und neu kompiliert, so ist eine neue TCPA-Lizenz erforderlich. So gesehen wird das Trustworthy Computing niemals mit einer Open-Source-Lizenz kompatibel sein. [HN02]

3.9 Patente

Anlässe zu Sorge, dass insbesondere Microsoft auch über Patente der freien Wettbewerb behindern könnte, werden auch durch Microsofts offizielle Stellungnahme [MS03] nicht gerade aus der Welt geräumt.

- Q: Could Linux, FreeBSD, or another open source OS create a similar trust architecture?
- A: From a technology perspective, it will be possible to develop a nexus that interoperates with other operating systems on the hardware of a nexus-aware PC. Much of the next-generation secure computing base architecture design is covered by patents, and there will be intellectual property issues to be resolved. It is too early to speculate on how those issues might be addressed. Beim Hearing des Bundeswirtschaftsministeriums im Juli 2003 bedauerten selbst hochrangige Microsoftvertreter die in diesem Bereich bestehenden Unklarheiten.

4 VerbesserungsVorschläge

Um die möglichen Vorteile von Trusted Computing insbesondere im Unternehmensbereich mit einer Reduktion der durch diese neue Architektur induzier-

ten Risiken für den Schutz der Privatsphäre und den fairen Wettbewerbes zu kombinieren, wurden verschiedene Vorschläge in die Diskussion eingeführt.

4.1 Ersetzbarer Endorsement-Schlüssel

Die mögliche Kontrolle über die sogenannten Endorsement Keys stellt ein hohes Missbrauchsrisiko dar. Aus diesem Grunde ist es insbesondere in Firmenumgebungen wünschenswert, Vertrauensstrukturen unter eigener Kontrolle zu betreiben. Aus diesem Grunde sollte die Möglichkeit bestehen, einen eigenen Endorsement Key als Ausgangspunkt für eine selbstkontrollierte Sicherheits-Architektur in das kryptographische Modul einzubringen.

4.2 Owner Override

Für eine feinere Granularität von Sicherheitspolitiken stellt auch der sogenannte "Owner Override" eine interessante Möglichkeit dar. Owner Overide ist eine Technik, welche von der amerikanischen Bürgerrechtsorgeniation Eletronic Frountier Foundation [EFF03] vorgeschlagen wurde. Vereinfacht gesprochen soll der Besitzer eines Computers die Möglichkeit erhalten, nach seinem eigenen Willen auf externe Anfragen reagieren zu können. Hierdurch könnte sich der Computerbesitzer selbst gegen Wettbewerbsbehinderungen zu Wehr setzen. In einer Firmenumgebung könnte Owner Override beispielsweise dazu so eingesetzt werden, dass nur die Geschäftsleitung in der Präsentation nach auen Änderungen durchsetzen kann. Im Falle von Privatrechnern soll der Computerbesitzer auch weiterhin die Kontrolle über die persönliche Hardware behalten.

5 Diskussion

Neben vielen kritisch zu bewertenden Teilaspekten sind insbesondere zwei Punkte von groer wirtschaftlicher und gesellschaftlicher Bedeutung: die Frage der Kontrolle über die kryptographischen Schlüssel und die Gefahr, dass mit technischen Mitteln der freie Austausch von Informationen behindert und unliebsame Konkurrenz (z.B. GNU/Linux) ausgesperrt werden kann. Es drohen zwei Welten zu entstehen, welche Schwierigkeiten haben werden, Informationen auszutauschen. Jedoch hat gerade die Offenheit des Netzes eine Wissensexplosion ausgelöst. In diesem Sinne bedrohen TCG und NSGB die Fundamente der Wissensgesellschaft. DRM und Plattformbindung machen beispielsweise auch Archivierung von Wissen schwierig bis unmöglich. Die Fremdkontrolle von kryptographischen Schlüsseln, welche eine gewichtige Rolle in der zukünftigen IT-Infrastruktur spielen, durch eine privatwirtschaftliche Firma, welche unter der Rechtsaufsicht einer ausländischen Regierung steht, bringen auch interessante politische und kartellrechtliche Fragestellungen mit sich.

6 Ausblick

Unter anderem auf Hearings des Bundeswirtschaftsministeriums wurden verschiedene Kritikpunkte von Datenschützern und Kartellrechtlern vorgetragen, von denen einige vom TCG Konsortium in der aktuellen Überarbeitung TCG 1.2 zumindest teilweise angegangen wurden. Nach längerem Drängen hat die TCG seit kurzem ebenfalls erweiterte Mitwirkungsrechte insbesondere für den Wissenschaftsbereich zugebilligt. Bleibt zu hoffen, dass diesen Schritten in die richtige Richtung weitere folgen werden. Zentrale Punkte werden dabei unter anderem die Fragen einer besseren Nutzer-Kontrolle beispielsweise durch Owner Override, ersetzbare Endorsement Keys und die leidigen Patent-Fragen sein.

Die vor allem in Europa seit geraumer Zeit betriebenen Entwicklungen von Smart-Card basierten Systemen bietet darüber hinaus interessante Möglichkeiten, erhöhte Sicherheit, Flexibilitat und persönliche Kontrolle von kryptographischen Schlüsseln zu kombinieren.

Acknowledgements

Ausdrücklich bedanken möchten wir uns bei Lucky Green, Ross Anderson, Volker Grassmuck, Carla und Rop Gonggrijp für zahlreiche wertvolle Anregungen. Die Zusammenarbeit mit der Vrije Universiteit Amsterdam bot und bietet ausgezeichnete Forschungsmöglichkeiten. Stellvertretend hierfür sei insbesondere Andy Tanenbaum, Maarten van Steen, Guido v. Noordende, Kees Bot, Philip Homburg und Jan-Mark Wams nochmals herzlich gedankt.

References

[And03] Anderson, R., Homepage, http://www.ck.cam.ac.uk/~rja14

[AFS97] Arbaugh,B., Farber, D., Smith, J., “A Secure and Reliable Bootstrap Architecture”, IEEE Symposium on Security and Privacy, 1997.

[BMWA03] Bundesministerium fr Wirtschaft und Arbeit, Symposium: ”Trusted Computing Group (TCG)” Juli 2003 (Berlin), Streams http://www.webpk.de/bmwa/willkommen.php

[BWL00] Bakker, B., Weis, R.,Lucks, S., ’How to Ring a Swan - Adding Tamper Resistant Authentication to Linux IPSec’, SANE2000 - 2nd International System Administration and Networking Conference, Maastricht, 2000.

[Cit03] Citi Smart Card Reserch, http://www.citi.umich.edu/projects/smartcard/

[CNN99] CNN.com, ”NSA key to Windows: an open question”, http://www.cnn.com/TECH/computing/9909/03/windows.nsa.02/

[Cry03] Cryptolabs, "TCPA and Palladium", http://www.cryptolabs.org/tcpa/

[EFF03] EFF, Trusted Computing: Promise and Risk, http://www.eff.org/Infra/trusted_computing/20031001_tc.php

[HN1a] Heise News, "Microsoft Server-Zertifikate abgelaufen', http://www.heise.de/newsticker/data/wst-06.05.01-003/

[HN1b] Heise News, "Microsoft warnt vor Cracker-Zertifikat", http://www.heise.de/newsticker/data/jo-24.03.01-001/

[HN02] Heise News, "Comdex: Zeitmaschine von Microsoft", 2002. http://www.heise.de/newsticker/data/wst-21.11.02-000/

[HN03] Heise News, "NSA will gegen Hintertren vorgehen ", 2003. http://www.heise.de/newsticker/data/ghi-09.08.03-000/

[Koe03] Koenig, C., "Trusted Computing im Fadenkreuz des EG-Wettbewerbsrechts", TRUSTED COMPUTING - Neue Herausforderungen für das deutsche und europäische Wirtschaftsrecht, Bonn, Mai 2003.

[LW02] Lucks, S., Weis, R., "Neue Erkenntnisse zur Sicherheit des Verschluesselungsstandard AES", Datenschutz und Datensicherheit, DuD 11/02, Vieweg, 2002.

[LM03] Linux Magazine, "Microsoft's Power Play",Januar 2003. http://www.linux-mag.com/2003-01/palladium_02.html

[MS03] Microsoft Next-Generation Secure Computing Base - Technical FAQ, February 2003. http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/news/NGSCB.asp

[TCG03] Trusted Computing Group (TCG), http://www.trustedcomputinggroup.org

[tcpa03] TCPA - Trusted Computing Platform Alliance, http://www.trustedcomputing.org/

[WC01] Weis, R., Crowley, P, "Tamper-resistant key storage for GnuPG" http://www.cryptolabs.org/gnupG/

[WL02] Weis, R., Lucks, S., "All Your Keybit are belong to us - The Truth about Blackbox Cryptograpy", SANE 2002, Maastricht 2002. http://www.nluug.nl/events/sane2002/papers/WeisLucksAllYourKeybit.ps