

Spezielle Gebiete der Kryptologie
**Sicherheitskonzept der
Microsoft Xbox**



Christian Hedemann
und
Andreas Kluth

Spezielle Gebiete der Kryptologie

Sicherheitskonzept der Microsoft Xbox

Gliederung

1. Einleitung	3
2. Die Xbox als Palladium-Feldversuch	3
2.1 Am Anfang stand die Idee	3
2.2 Was ist eigentlich Palladium?	4
3. Die Palladium-Systemarchitektur	5
3.1 Palladium und Hardware	5
3.2 Vier neue Aspekte	6
3.3 Ein neuer Kernel muss her	7
4. Ein Konzept wird Realität	8
4.1 Welche Sicherheitskonzepte wurden wie realisiert?	8
4.2 Analyse der Stärken und Schwächen	9
5. Das Konzept auf dem Prüfstand	9
5.1 Welche Motivationen hat der Hacker?	9
5.2 Chronologie der erfolgreichen Angriffe	10
5.3 Konzeptionsfehler	11
6. Fazit	12
6.1 Bewertung der Xbox als erstes Palladium-System und als Spielekonsole	12
6.2 Grenzen der Architektur im Sinne der Umsetzbarkeit zum jetzigen Zeitpunkt	12
6.3 Gefahren der Technik, mögliche Szenarien	12
7. Demonstration	12
Anhang	
A. Quellenangaben	13
B. Weiterführende Literatur	13
C. Wahrheit und Spekulation über Palladium und TCPA	14
D. Verzeichnis der Akronyme	17

1. Einleitung

Die Xbox ist Microsofts erstes Videospielsystem.

Mit dem Wissen aus dem PC- und Online-Markt und einem riesigen Budget versuchte man sich Ende 2001 / Anfang 2002 als Neuling unter den Videospielekonsolenherstellern direkt hinter Sony mit der PlayStation 2 zu positionieren, um mit der kommenden Generation der Konsolen endlich Marktführer zu werden.

Beim Bau des Systems verließ man sich im Gegensatz zur Konkurrenz ganz auf althergebrachte Technologie und verwendete hauptsächlich leicht modifizierte PC-Technologie. Durch diesen Schritt sollten einerseits Forschungs-, Entwicklungs- und Produktionskosten gesenkt und andererseits die Entwickler dazu bewegt werden, auf einer gewohnten Umgebung Spiele entwerfen zu können. Da aber PC-Hardware sich grundsätzlich nur bedingt eignet, um ein proprietäres System mit Lizenzmodell zu entwerfen, fand das von Microsoft entwickelte Softwaresicherheitsmodell Palladium Verwendung. Diese Technik erlaubt es unter anderem, sogenannte signierte Software auf einem System abzuspielen und wenn man auf Kritiker hört, erlaubt sie noch viel mehr... aber nicht dem Endanwender, sondern Microsoft.

2. Die Xbox als Palladium Feldversuch

2.1 Am Anfang stand die Idee

Sicherheit in Computersystemen ist ein sensibles Thema was Microsoft auch im Vorfeld der Entwicklungen bereits gemerkt hat. Andere Firmen wie z.B. Intel oder Real Networks - um einige von vielen zu nennen - haben sich in der Vergangenheit bereits an das Thema gewagt, um Sicherheit dadurch zu definieren, dass Rechner eindeutig durch bspw. fest verdrahtete Kennnummern oder aus verschiedenen fixen Daten (Hardware- und Betriebssystemelementen) errechneten IDs identifiziert werden können und haben dadurch einen Sturm der Entrüstung auf sich gezogen mit entsprechenden temporären Imageschäden.

Um dem vorzubeugen hielt sich Microsoft lange Zeit mit Pressemitteilungen bedeckt, um in Ruhe etwas zu entwickeln und mit etwas ausgegorenem an die Öffentlichkeit zu treten.

Doch sie haben nicht damit gerechnet, dass die Öffentlichkeit ein reges Interesse an der Thematik zeigt: Mitte 2002 meldeten sich viele Sicherheitsexperten, die Weltuntergangsszenarien skizzierten, die Presse versuchte in ihren Artikeln auf mehr oder weniger verlässlichen Quellen zu bauen und die Öffentlichkeit wurde mit einer Mischung aus Fakten, Falschmeldungen, aber hauptsächlich Stimmungen konfrontiert.

Erst knapp ein Jahr später versuchte man sich in Redmond daran, seine Pläne vorzustellen und mit den vielen Vorurteilen zumindest im Ansatz aufzuräumen. Anhang A gibt einem ein gutes Bild davon, was alles an die Öffentlichkeit gelangte und was davon im nachhinein der Wahrheit entsprach.

Inzwischen hat fast jede involvierte Gruppierung entweder ihren Namen oder den Namen ihres Produktes geändert. Eine kleine Chronologie der Verwirrung:

Aus	Wurde	Weil
Palladium	NGSCB (Next-Generation Secure Computing Base)	Es gab Probleme mit dem Markennamen Palladium.
TCPA	TCG	Die TCPA war derart basisdemokratisch aufgebaut, dass nur einstimmige Beschlüsse in die Spezifikation übernommen werden konnten. Bei der TCG, die als Ablösung der TCPA angesehen wird, reicht eine 2/3 Mehrheit.

An dieser Stelle noch einmal zum Mitschreiben, um nicht aus dem Konzept zu kommen:

1. Palladium:
Softwarelösung, die sichere Hardware braucht um zu funktionieren
2. TCPA Spezifikation, bzw. TCG Spezifikation
Hardwarelösung, auf der spezielle Software sicher laufen kann
3. Punkt 1 und Punkt 2 wurden unabhängig voneinander konzipiert
4. Palladium soll ab TCG Spezifikation 1.2 auf deren Hardwarelösung aufbauen
5. Der Name eines sicheren Hardwaresystems wird mit TCB (Trusted Computing Base) betitelt
6. Der Name des Krypto-Chips bei Palladium lautet SSC (Secure Support Component)
7. Der Name des Krypto-Chips bei der TCPA / TCG lautet TPM (Trusted Platform Module)

2.2 Was ist eigentlich Palladium?

Palladium ist in diesem Falle kein Edelmetall, sondern ein von Microsoft entwickeltes Sicherheitskonzept für Betriebssysteme, das in neuen Windows-Versionen (Arbeitstitel „Longhorn“) Anwendung finden soll. PCs und Betriebssysteme heutzutage sind bis auf ganz wenige Ausnahmen grundsätzlich als unsicher anzusehen. Angreifer können Software installieren ohne Wissen des Benutzers, können nach belieben Speicherwerte auslesen und ändern und sogar mit der richtigen Ausrüstung noch in zig Metern Entfernung Computer abhören.

Palladium greift an dieser Stelle ein und erweitert Windows um Komponenten, die einerseits sicherstellen, dass Daten nicht verändert werden können sollen, dass der Pfad zwischen Computern untereinander sicher ist und gibt Schnittstellen zur Hardware und HIDs vor, damit der Weg zwischen dem Computer und dessen Benutzer auch als sicher anzusehen ist.

Doch schauen wir uns die Systemarchitektur einmal im Detail an.

3. Die Palladium Systemarchitektur

3.1 Palladium und Hardware

Startet man an der Stelle ohne die Palladium nicht laufen würde, fängt man automatisch an der Hardware an. Palladium setzt als sichere Windows-Erweiterung einen sicheren PC voraus, der auch die neuen Features direkt in der Hardware unterstützt. Ein heutiger PC wäre dazu nicht imstande: Man müsste nur eine Grafikkarte per Treiber im Busmastermodus ansprechen und schon kann man jede x-beliebige Adresse im RAM ansprechen.

Nur ist diese Stelle der Spezifikation bei Palladium am schwächsten ausgebaut. Es wird lediglich ein Krypto-Chip (SSC) vorausgesetzt, der minimal RSA-Operationen (Verschlüsselung, Entschlüsselung, Generierung von digitalen Signaturen und Verifizierung), AES-Verschlüsselung und –Entschlüsselung und eine Hash-Berechnung nach SHA-1 durchführen kann. Weiterhin muss der Chip mindestens einen privaten RSA-Schlüssel und einen symmetrischen AES-Schlüssel beinhalten, die niemals exportiert werden.

An dieser Stelle sei noch gesagt, dass die TCPA-Spezifikation die Voraussetzungen noch um einen sicheren Zufallsgenerator und einen sicheren Timer erweitern.

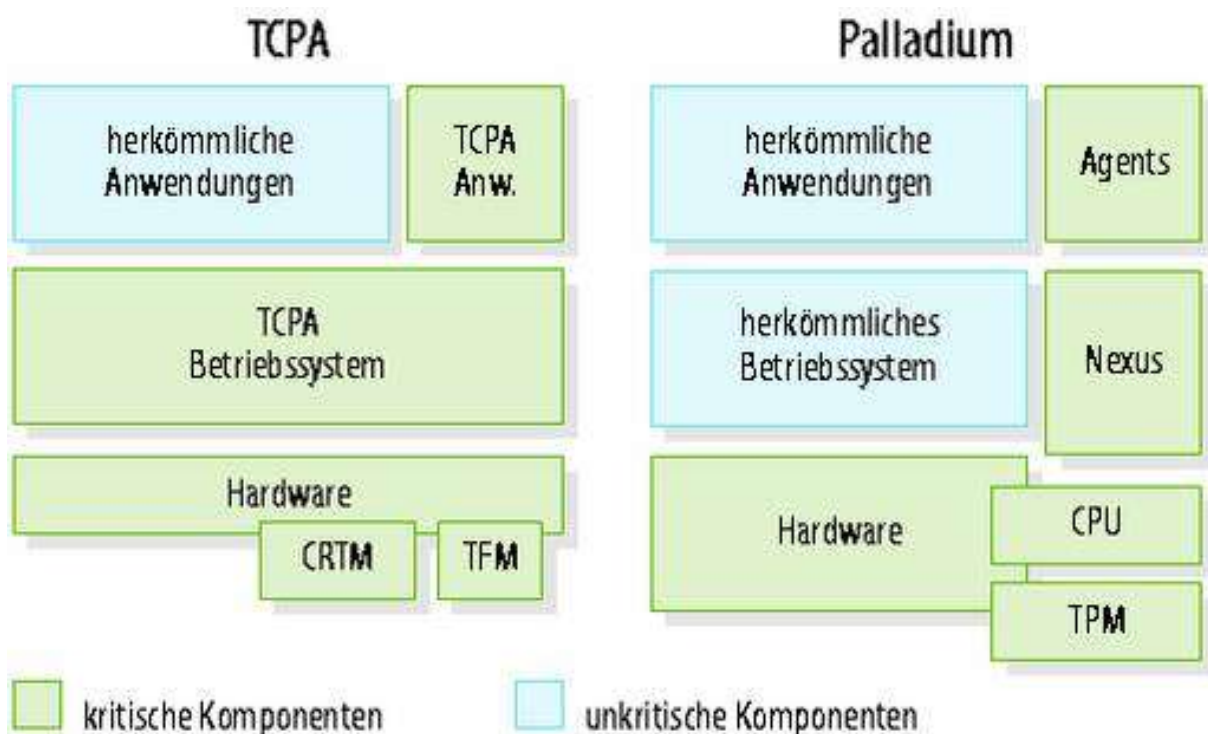


Abbildung 1

Quelle: [2]

Wie man an Abbildung 1 gut erkennen kann, kümmert sich die TCPA Spezifikation überhaupt nicht um die Interna des Betriebssystems, sondern Beschränkt sich auf die Hardware mit den Komponenten CRTM (Core Root of Trusted Module – eine manipulationssichere BIOS-Erweiterung für den Boot-Prozess), dem TPM und der restlichen Hardware.

Palladium hingegen setzt die Hardware mit TPM und einer CPU, die sichere Operationen für das Betriebssystem gewährt, voraus und konzentriert sich auf die Umsetzung in Software.

3.2 Vier neue Aspekte

Und eben jene Software wird um vier Aspekte erweitert:

- x Strong Process Isolation
- x Sealed Storage
- x Attestation
- x Trusted Path

Strong Process Isolation

Strong Process Isolation heißt die Technik, um einen Teil des RAM exklusiv für sichere Anwendungen zu reservieren.

In heutigen Computern ist das RAM durch die CPU in zwei Bereiche unterteilt. In Ring 0 laufen die Systemnahen Programme wie z.B. Treiber, oder die Speicherverwaltung und in Ring 3 laufen die Anwendungen des Users. Palladium fügt einen neuen Ring –1 ein, damit die Speicherzuteilung für sichere Anwendungen in Hardware erfolgen kann und nicht virtuell per Software geschrieben werden muss. Software könnte man abändern.

Ebenfalls werden durch die CPU DMA-Zugriffe auf den geschützten Speicherbereich blockiert.

Sealed Storage

Daten werden verschlüsselt auf dem Datenträger abgelegt.

Für Daten, die länger zur Verfügung stehen sollen, als das Programm im System läuft, wird die SSC zur Verschlüsselung verwendet, bevor sie auf dem Datenträger gesichert werden. Sie können später nur noch von der Anwendung gelesen werden, die sie gesichert hat, oder von Anwendungen die von der Ursprungsanwendung als „sicher“ anerkannt werden.

Cryptographic Attestation

Sichere Anwendungen signieren Daten für andere sichere Anwendungen.

Mit Hilfe der SSC werden anderen Anwendungen attestiert, dass bestimmte Daten im allgemeinen (dies können auch andere Programme sein) als sicher einzustufen sind und auch nicht verändert wurden. Wie bei bisher bekannten Signierverfahren werden hierbei 2048-Bit RSA Schlüssel verwendet, die sich fest verdrahtet im SSC befinden, jedoch aufgrund der als sicher anzunehmenden Hardware ohne dritte Zertifizierungsstelle auskommen.

Interessant wird dieses Feature unter anderem auch zur Einführung von Lizenzmodellen:

Programme könnten zentral von einer Firma signiert werden ohne deren Zertifizierung diese Software nicht beim Benutzer funktioniert (wie es bei der Xbox der Fall ist).

Trusted Path

Der Weg zwischen zwei Punkten wird mit Hilfe von spezieller Hardware sicher.

Erreicht wird dieses Ziel durch rigoroses Austauschen sämtlicher bisher vorhandener (und unsicherer) Hardware. Angefangen von der Maus über USB-Hubs bis hin zum VGA-Anschluss muss alles so angepasst werden, dass ein Verändern und Mithören von Daten nicht mehr möglich ist. Hardware-Keylogger oder mit Antennen abgehörte Computerverbindungen sollen dadurch der Vergangenheit angehören.

Palladium definiert hierzu lediglich Richtlinien und überlässt die endgültige Ausgestaltung der Hardwareindustrie in Form der jetzigen TCG.

3.3 Ein neuer Kernel muss her

Nun haben wir etwas über die Hardware und die zugrundeliegenden Ideen erfahren, doch wie sieht die Umsetzung im Betriebssystem selber aus, das einen Spagat zwischen alter Software und neuer Software machen muss?

Die Lösung liegt in diesem Diagramm:

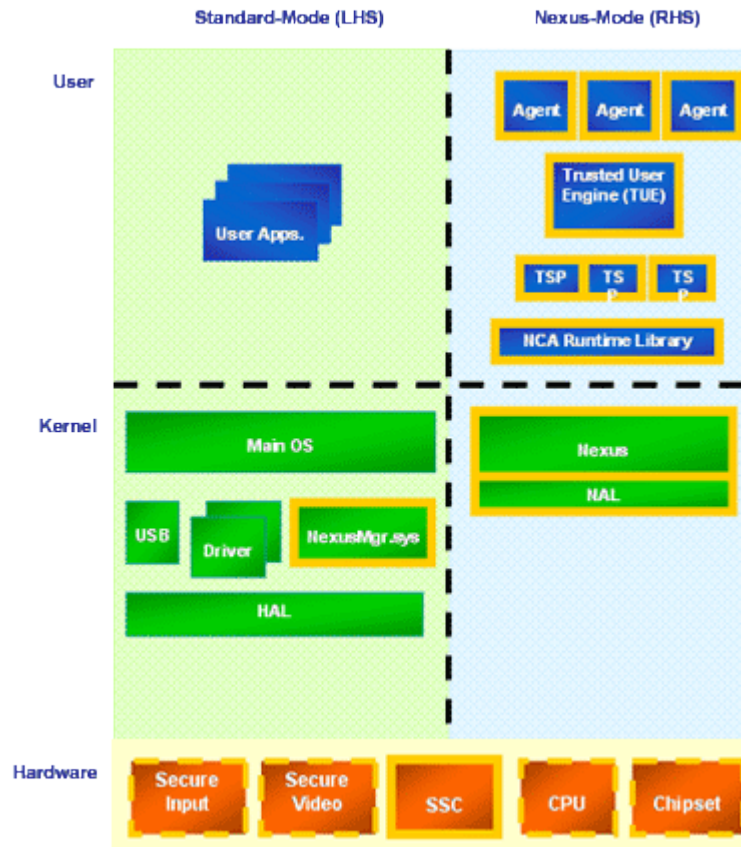


Abbildung 2

Quelle [5]

Das auf die Hardware aufbauende Betriebssystem wird in vier Quadranten unterteilt nach folgendem Schema:

1. ein Standardmodus (auch LHS oder Left Hand Side genannt) und ein neuer, sicherer Modus „Nexus-Mode“ (RHS oder Right Hand Side)
2. eine Benutzerebene in der die Programme laufen und eine Kernebene in der sich der Betriebssystemkern befindet

Ein üblicher Startvorgang sähe dann so aus:

- zuerst startet die Hardware und bietet dem Betriebssystem eine sichere Basis
- danach wird das Standardbetriebssystem geladen (Kernel LHS), welches aufgrund der Abwärtskompatibilität und bisher mangelnder Usersoftware noch im Standardmodus läuft

Lädt der User nun ein Programm, welches keine sichere Umgebung benötigt, wird dieses in der Benutzerebene auf der linken Seite platziert – ein Unterschied zwischen Palladium und existierenden Windowsversionen besteht nicht.

Benötigt das Programm jedoch eine sichere Umgebung, greift es auf einen Nexus zurück. Der Nexus ist ein modularer Teil des Betriebssystems, der nur die sicherheitsrelevanten Teile beherbergt. Ebenfalls interessant am Nexus ist, dass Microsoft plant diesen Kernelteil nicht zu monopolisieren: Im Endeffekt soll jeder seinen eigenen Nexus schreiben können – die Frage nach einem Lizenzmodell, oder die Frage ob es überhaupt eins geben wird ist, ist zur Zeit noch offen. Einzige Beschränkung zum Nexus ist, dass immer nur einer auf einmal laufen darf.

Nun darf die sicherheitskritische Anwendung nicht im linken Teil der Benutzerebene laden, sondern muss in den rechten Teil geladen werden mit allen Rechten und Pflichten. Die Rechte sind die zusätzliche Sicherheit und die Pflichten fangen damit an, dass von dem Programm auf der RHS ab sofort nur noch vom NCA gesprochen wird (Nexus Computing Agent), welches über diverse Stufen (siehe Schema und Glossar) auf dem Nexus aufsetzt. Sichere Programme können im Gegensatz zum Nexus mehrere gleichzeitig laufen.

Als letzte Frage ist nun noch offen, wie der NCA mit dem Rest der Hardware kommuniziert, da der Nexus bekannterweise nur Code zur Sicherheit beinhaltet... an dieser Stelle kommt der NexusMgr.sys ins Spiel, der die Schnittstelle zwischen dem sicheren Teil und sämtlicher Hardware wie z.B. Laufwerken, Netzwerkkomponenten, etc. darstellt. Der ausgehende Datenverkehr ist verschlüsselt und bedarf keiner Sonderbehandlung. Der eingehende Datenverkehr ist jedoch trotz allem nicht unbedingt sicher, weshalb im Nexus noch zusätzlich die Signatur geprüft wird und ob es möglicherweise Daten sind, die einen Angriff auf das System darstellen. NexusMgr.sys ist also quasi als Schleuse zur Außenwelt zu verstehen.

4. Ein Konzept wird Realität

4.1. Welche Sicherheitskonzepte wurden realisiert?

Die Microsoft Xbox implementiert alle Funktionen eines Palladium konformen Systems, wobei die Sealed Storage und Process Isolation in einer frühen Form Verwendung findet.

Hardwareseitig kommt als Sicherheitschip ein Nvidia MCPX-Controller (SSC) zum Einsatz, dieser überwacht den Bootvorgang und übergibt einem angepasstem Windows 2000 Kernel die Kontrolle über das System_[13].

Durch ein abgestecktes System mit genau spezifizierter Hardware ist ein sicherer Systemzustand zu jeder Zeit gegeben, einen Standard Mode sieht die Xbox als Betriebsmodus nicht vor.

Zusätzlich zur TC-Technologie werden noch weitere Konzepte verfolgt. Ein neues proprietäres Dateisystem basierend auf Fat32 (FatX) findet Verwendung. Weiterhin sind die Festplatten über das ATA Security Feature mit unique Keys gelockt, so soll sichergestellt werden, dass die Datenträger nicht in anderen Systemen gelesen und manipuliert werden können.

Medien für die Xbox haben einen üngültigen via RSA verschlüsselten TOC, sind mit CSS geschützt und auf zweischichtigen DVD9s gepresst, lassen sich also nicht mit handelsüblichen DVD-Laufwerken einlesen geschweige denn kopieren. Die verwendeten DVD Laufwerke sind auf diese Medien mit einer angepassten Firmware optimiert; haben dadurch Schwierigkeiten andere Medien zu lesen. Von Haus aus akzeptiert die Konsole nur drei Arten von USB-Geräten, Human Input Devices, Speicherdevices und das Xbox-DVD-Dongle, ein proprietärer USB-Anschlussstecker stellt eine weitere Hürde dar.

4.2. Analyse der Stärken und Schwächen

Pro

- TC Technologie mit starker Verschlüsselung
- nur signierte Software kann ausgeführt werden (XBE signing)
- Zentrale Zertifizierung und Qualitätsprüfung der Software
- abgestecktes System mit fester Spezifikation
- neues Dateisystem
- IDE Devices mit unique ATA Keys geschützt
- Verzicht auf legacy Support
- geschützte Medien

Kontra

- übliche x86 Hardware findet Verwendung
- IDE Devices schlecht geschützt (Hotplugging), keine Verschlüsselung der Daten
- HyperTransport Bus in v1.0 und v1.1 ungeschützt
- Implementierungsfehler der Software/Dashboard
- USB-Port nur mechanisch inkompatibel
- Debug- bzw. Diagnoseport

5. Das Konzept auf dem Prüfstand

5.1. Welche Motivationen hat der Hacker

Prinzipiell sollte sich zuerst einmal verdeutlicht werden, warum es ein Interesse gibt ein geschlossenes System wie die Xbox auf Schwachstellen zu untersuchen.

Die Intentionen die zu den Hacks führen sind im Falle der Xbox sehr vielschichtig. Generell sind jedoch fünf Motivationsarten zu erkennen und zwar Geld, Ruhm, Wissen, Langeweile und Microsoft.

Konkret wurde die Intensitäten der Bemühungen durch ein 200.000\$ Preisgeld und diverse Prämien der Modchipindustrie erhöht. Insbesondere der sehr günstige Preis für ein vollwertiges PC-System und die kompakte, hochintegrierte Hardware macht das System als Multimediaplayer und platzsparender Server für die breite Masse attraktiv.

5. 2. Chronologie der erfolgreichen Angriffe

Bunnie Hack

Der Bunnie Hack bietet die eigentliche Grundlage für den klassischen Xbox Modchip. Der MIT Student Andrew S. Huang schaffte im Januar 2002, nur 2 Monate nach dem Xbox-Launch, mittels eines in den unverschlüsselten, mit 200Mhz getaktetem, HyperTransport Bus eingehängten Sniffer den Datenverkehr zwischen CPU und MCPX abzuhören. Dadurch hatte Huang neben dem Bios im Klartext, auch den eigentlichen Bootprozess offen gelegt. Kurze Zeit später, im Mai 2002, waren die ersten Modchips der Generation.1 auf dem Markt. Diese mussten über 29 Kontaktpunkte verlötet werden, die Xbox war offen, unsigned Software konnte ausgeführt werden. Es folgten weitere Generationen, die sich durch reduzierte Lötstellen und einen erweiterten Funktionsumfang unterscheiden. Aktuell sind solderless und flashbare Modchips der Generation.4.a.



Abbildung 3

LDT bus tapping Quelle[8]

007 und Mech Assault Savegame

Im März 2003 postete der User habibi_xbox im xboxhacker.net Forum, er habe das mit 100.000\$ dotierte ProjectB (Linux auf der Xbox ohne Hardwaremodifikation) gelöst. Er entdeckte einen BufferOverflow im Savegamehandling von James Bond 007: Agent im Kreuzfeuer, der es ermöglichte selbst signierte Software auszuführen. Das beigefügte Proof of Concept schaffte es einen Loader bereitzustellen der ein LiveLinux in Knoppix Manier zum Laufen brachte. Einem Microsoft Titel, dem Spiel Mech Assault, ereilte das gleiche Schicksal im Juni 2002, bot jedoch zwei klare Vorteile es startete wesentlich schneller und die Qualität des Spiels war deutlich höher. Zuvor waren Gerüchte laut geworden, die Electronic Arts eine schlampige Programmierung bei 007 vorwarfen.

Die beiden Hacks weisen, unabhängig von ihrem Potential, einen kleinen Schönheitsfehler auf. Ein knapp 50-60 Euro teures Spiel musste bei jedem Konsolenstart geladen werden, für eine permanente Modifikation musste zu diesem Zeitpunkt die Konsole noch geöffnet und modifiziert werden.

Dashboardhack (UnsignedCode Hack)

Fonthack

Stefan Esser rief am 4 Juli 2003 in einem Security Advisory auf der Mailingliste Full-Disclosure den Unabhängigkeitstag der Xbox aus. Eine Sicherheitslücke im Xbox-Dashboard erlaubt es, sämtliche Sicherheitsmechanismen der Spielkonsole zu umgehen. Bevor das Dashboard eine Datei verwendet, vergleicht es einen SHA1-Hash der Dateien mit einem intern gespeicherten Hash. Allerdings führt das Dashboard diese Prüfung nicht bei Audio-Dateien mit der Endung „.wav“ und Font-Dateien mit der Endung „.xtf“ durch. Ein Fehler im Font-Loader, mit speziell präparierten Font-Dateien gefüttert, ermöglicht die Ausführung beliebigen Codes auf der Konsole. Eine Benutzerinteraktion ist nicht nötig.

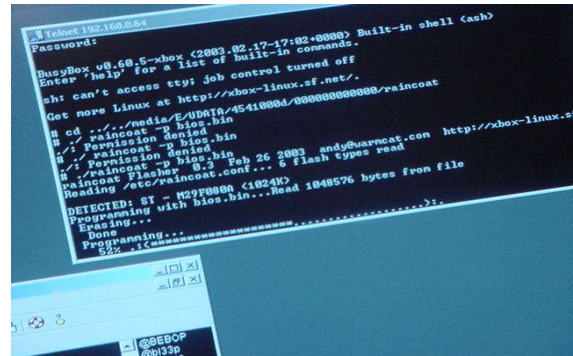


Abbildung 4

Xbox-telnet

Audiohack

Zusätzlich zum Fonthack setzt der Audiohack auf ein ähnliches Konzept. Ein Flaw in der Titeldatenbank „ST.DB“ des integrierten Mediaplayer ermöglicht es einen BufferOverflow zu produzieren. Die Benutzerinteraktion reduziert sich hier auf ein Minimum, eine beliebige Audio-CD muss eingelegt und die Titeldatenbank abgefragt werden.

5. 3. Konzeptionsfehler

Die Xbox ist natürlich kein perfektes System, die Konzeption und Umsetzung ist jedoch sicher als gelungen und sicher zu betrachten. Den im Silizium des MCPX verborgenen initial Bootloader und den passenden RC4-Key sind nicht und werden in naher Zukunft nicht bekannt werden. Einen mit 200Mhz getakteten HyperTransport Bus abzuhören, war bis zum Bunny Hack kein realistisches Angriffsszenario und ist in den neueren Versionen der Xbox durch TEA-Verschlüsselung auf dem ht-Bus nicht mehr so leicht realisierbar. Aus den gemachten Fehlern lernt Microsoft äußerst schnell und die Erfahrungen werden direkt in das aktuelle Produkt eingebracht. Der Versuchsballon Xbox ist rein vom eingebrachten Wissen für Microsoft jetzt schon ein voller Erfolg, Palladium wird in diesem groß angelegten Beta Test weiter gehärtet.

6. Fazit

6. 1. Bewertung der Xbox als erstes Palladium-System und als Spielekonsole

Die Xbox ist auf beiden Seiten ein klarer Gewinner.

Der aktuelle Marktanteil der Xbox scheint im Vergleich zur Sony Playstation2 vor allem im asiatischen Markt gering, dennoch hat es Microsoft geschafft durch konsequentes Marketing, eine hohe Produktqualität und eine ruinöse Preispolitik ihr System besonders im westlichem Markt gut zu platzieren.

Ferner wird Palladium in einem riesigen Feldversuch getestet, ohne das ein Großteil der User überhaupt registriert ein via NGSCB geschütztes System zu nutzen; dies hat den Vorteil das der Imageschaden, wie er Intel erfahren hat, ausbleibt. Die aus der Xbox gewonnenen Erfahrungen haben das Wissen der NGSCB-Entwickler erweitert, Technologien wie Sealed Storage, Strong Process Isolation wurden stark verbessert. Die Anforderungen an die verwendete Hardware wurden im TCG-Konsortium angepasst und erweitert.

6. 2. Grenzen des Systems zum jetzigen Zeitpunkt

Solange nicht die komplette, aktuell eingesetzte PC-Hardware ausgetauscht wird, ist NGSCB nicht umsetzbar. Dies kann aber auch als Glück im Unglück gesehen werden. Denn so beschränkt sich die Implementierung von Palladium zuerst auf weniger offensichtliche Sektoren, wie Videospiele-systeme oder ggf. Handys, die als proprietäre Systeme ein in sich geschlossenes System bilden. Auch werden dadurch erste Designfehler frühzeitig erkannt, die bei Einsatz im PC-Sektor zu einer Welle der Abneigung gegen die neue Technik geführt hätte.

6. 3. Gefahren der Technik

Das Potenzial zum Missbrauch von NGSCB ist äußerst groß, kritische Stimmen sprechen von einer Umschichtung der Macht auf längere Sicht. Auf einem TCG Symposium in Berlin kommentierte Ross Anderson die Bemühungen der TC-Bewegung „Im Jahre 2010 wird Präsidentin Hillary Clinton zwei rote Knöpfe auf ihrem Schreibtisch haben. Einer der die Raketen Richtung China abfeuert und einer der sämtliche chinesischen PCs abschaltet. Und nun raten Sie mal, welchen Knopf die Chinesen am meisten fürchten“. Dies fällt sicher schon in den Bereich Endzeitszenario, zeigt aber doch die Gefahren auf, die durch Zertifizierungs- und Kontrollinstanzen entstehen. Das Ziel ein sicheres System zu erschaffen ist ohne Frage das Richtige, nur endet der Weg den NGSCB einschlägt, in meinen Augen, für den End-User in eine Sackgasse.

7. Demonstration

Am Beispiel des MechAssault Savegamehacks in Kombination mit einem Audiohack wird verdeutlicht, wie einfach sich die Sicherheitsmechanismen einer unmodifizierten Xbox aushebeln lassen. Ein modifiziertes Savegame lädt den PhoenixBiosLoader, welcher on the fly das laufende Bios im Ram überschreibt und die „ST.DB“ permanent überschreibt. Danach kann beliebige unsigned Software ausgeführt werden, z.B. eine angepasste LinuxDistribution.

Anhang

A. Quellenangabe

- [1]Windows Platform Design Notes – Security Model for the Next-Generation Secure Computing Base http://www.microsoft.com/resources/ngscb/documents/NGSCB_Security_Model.doc
- [2]Christian Stüble, Ahmad-Reza Sadeghi:
Vertrauen ist gut, Sinn und Unsinn von TCPA und Palladium, c't 13/03, S. 232
- [3]Gerald Himmelein:
Blick ins Schloss, Details zu Palladium / NGSCB, c't 12/03, S. 192
- [4]http://www.microsoft.com/resources/ngscb/four_features.msp
- [5]Gerald Himmelein:
Ganz im Vertrauen, TCPA ist tot, es lebe die TCG, c't 09/03, S. 52
- [6]<http://www.xbox-scene.com>
- [7]<http://www.xboxhacker.net>
- [8]<http://www.xenatera.com/bunnie/proj/anatak/xboxmod.html>
- [9]<http://warmcat.com/milksop/>
- [10]<http://lists.netsys.com/pipermail/full-disclosure/2003-July/010895.html>
- [11]<http://moon.hipjoint.de/tcpa-palladium-faq-de.html>
- [12]<http://www.microsoft.com/presspass/features/2002/jul02/0724palladiumwp.asp>
- [13]<http://xbox-linux.sourceforge.net/docs/msbios.html>

B. Weiterführende Literatur

Homepages

Trusted Computing Platform Alliance
<http://www.trustedcomputing.org>

Trusted Computing Group
<http://www.trustedcomputinggroup.org>

Next-Generation Secure Computing Base
<http://www.microsoft.com/resources/ngscb/default.msp>

The Xbox Linux Project
<http://xbox-linux.sourceforge.net>

Linux on Unmodified Xbox Wiki
<http://unmodded.mine.nu/docs/>

Literatur

Hacking the Xbox
Andrew Huang ISBN: 1593270291

Opening the Xbox: Inside Microsoft's Plan to Unleash an Entertainment Revolution
Dean Takahashi ISBN: 0761537082

C. Wahrheit und Spekulation zu Palladium und TCPA

Bereich	Behauptung	Wahrheitsgehalt
TCPA: Sicherheitsinitiative von 201 Unternehmen		
Allgemein	TCPA-Chips sollen in den USA Pflicht werden (c't 24/02, S. 186)	unwahrscheinlich (auch wenn es Bemühungen gibt)
	teure Zertifizierung aller Anwendungen nötig (c't 22/02, S. 204)	falsch
	bei Hardware-Änderungen muss der Rechner neu zertifiziert werden (c't 22/02, S. 204)	falsch (bei Palladium möglich)
	greift auf zentrale Listen mit geprüfter Hardware und Software, gesperrten Dokumenten und Seriennummern zurück (c't 22/02, S.204)	falsch (bei Palladium möglich)
	nicht ohne Weiteres zu Linux kompatibel (c't 22/02, S. 204)	falsch (Linux-Treiber bereits verfügbar)
	ermöglicht die Bindung von Software an Hardware („Verdongelung“) (c't 22/02, S. 204)	richtig (geht aber auch ohne TCPA)
	kein Schlüssel-Export vorgesehen (c't 26/02, S. 58)	mit Einschränkung (es gibt „Migrateable Keys“)
TCPA-Chip	wg. Senator Fritz Hollings auch Fritz-Chip genannt (c't 15/02, S. 18)	eher unüblich, generell TPM (Trusted Platform Module)
	Integration in PDAs, Mobiltelefonie und Unterhaltungselektronik geplant (c't 22/02, S. 204)	richtig
	ist ein Co-Prozessor (c't 22/02, S. 204)	falsch, Chip ist nicht direkt an Haupt-CPU gekoppelt
	kann sich und PC abschalten (c't 22/02, S. 204)	falsch (passiver Prozessor)
	entspricht einer fest integrierten SmartCard (c't 24/02, S. 186)	richtig
	ersetzt SmartCards (c't 15/02, S. 18)	falsch, SmartCards als Ergänzung sinnvoll

	wird ins Mainboard integriert (c't 22/02, S. 204)	richtig (IBM arbeitet mit Aufsteckplatine)
	Integration in Hauptprozessor geplant (c't 22/02, S. 204)	möglich (Intel bestreitet derartige Vorhaben)
	abschaltbar (c't 15/02, S. 18)	richtig (Default-Einstellung)
	steuert den Boot-Vorgang (c't 15/02, S. 18)	falsch, Chip bleibt durchgehend passiv
	Physical Presence Switch soll Rechner-Fernsteuerung verhindern (c't 24/02, S. 186)	richtig (dient aber nicht der Überwachung des Nutzers)
	überprüft beim Start alle Systemkomponenten (c't 15/02, S. 18)	möglich
	erkennt Manipulationen an Systemkomponenten (c't 22/02, S. 204)	indirekt (veränderter Hash-Wert)
	enthält eindeutige Identifikation des Rechners (c't 15/02, S. 18)	richtig
	dient zur Identifizierung und Authentifizierung des Rechners (c't 22/02, S. 204)	richtig
	dient zur Identifizierung und Authentifizierung des Anwenders (c't 22/02, S. 204)	möglich (indirekt)
	überprüft Zertifikate von Hard- und Software (c't 15/02, S. 18)	falsch (bei Palladium möglich)
	speichert Schlüssel und Passwörter (c't 26/02, S. 56)	richtig
	dient zur Ver- und Entschlüsselung (c't 22/02, S. 204)	richtig
	verweigert Hardware-Komponenten den Zugriff auf geschützte Inhalte (c't 15/02, S. 18)	falsch (bei Palladium möglich)
	sendet bei Start eines nicht TCPA-konformen Programms ein Warnsignal an alle TCPA-Anwendungen, die sich dann beenden (c't 22/02, S. 204)	falsch
TCPA-Anwendung	TCPA-Anwendungen funktionieren nur bei aktivem TCPA-Chip (c't 15/02, S. 18)	richtig

Palladium: Sicherheitskomponente für zukünftige Windows-Versionen		
Allgemein	Palladium baut nicht auf TCPA auf (c't 15/02, S. 18)	falsch (soll auf TPM 1.2 aufbauen)
	läuft nicht auf aktuellen PCs (c't 5/03, S. 86)	richtig (benötigt zahlreiche Hardware-Anpassungen)
	Palladium ist Umsetzung von Microsofts Patent für ein DRM-Betriebssystem (c't 15/02, S. 18)	unbestätigt (DRM war ursprüngliches Ziel)
	zentrale Trust-Server kontrollieren das System (c't 15/02, S. 18)	unbestätigt
	nicht vertrauenswürdige Anwendungen werden blockiert (c't 15/02, S. 18)	richtig (Sicherung von Inhalten und Speicherbereichen)
	kein Schlüssel-Export vorgesehen (c't 26/02, S. 58)	mit Einschränkung (es gibt „Migrateable Keys“)
	beendet illegale Software automatisch (c't 22/02, S. 204)	angeblich nicht geplant
	vor dem Start einer nicht vertrauenswürdigen Anwendung werden alle DRM-Inhalte aus dem Speicher entfernt (c't 15/02, S. 18)	falsch (unsichere und sichere Anwendungen arbeiten in getrennten Speicherbereichen)
	Palladium akzeptiert nur zertifizierte Treiber (c't 15/02, S. 18)	unbestätigt, gilt evtl. für Kern (Nexus)
Einsatzfeld	Passwörter aufbewahren (c't 15/02, S. 18)	falsch (wird an TCPA-Chip delegiert)
	Verifikation von E-Mails (c't 15/02, S. 18)	möglich (durch Palladium-Anwendung)
	schützenswerte Inhalte aufbewahren (c't 15/02, S. 18)	richtig (Secure Storage)
Anwendungen	ermöglicht die Bindung von Software an Hardware (c't 22/02, S. 204)	richtig (geht aber auch ohne Palladium)
	alle Palladium-Anwendungen müssen zertifiziert sein (c't 15/02, S. 18)	falsch (Zertifizierung optional)

Quelle: In Anlehnung an c't 09/2003, Seite 52

D. Verzeichnis der Akronyme

AES	Advanced Encryption Standard
CRTM	Core Root of Trusted Module
CSS	Content Scrambling System
GUID	Generic User ID
HAL	Hardware Abstraction Layer
HID	Human Interface Device
MCPX	Media Communications Processor
NCA	Nexus Computing Agent
NGSCB	Next-Generation Secure Computing Base
RSA	Akronym aus den Namen der Erfinder
SHA-1	Secure Hash Algorithm
SSC	Secure Support Component
TCB	Trusted Computing Base
TCG	Trusted Computing Group
TCPA	Trusted Computing Platform Alliance
TEA	Tiny Encryption Algorithm
TPM	Trusted Platform Module
TSP	Trusted Service Provider