## Technische Erklärung

Dieser Text enthält die technische Erklärung der "Entdecker des Hacks" und richtet sich eher an die Informatiker oder "Technikversteher" unter euch.

Er wurde von mir größtenteils übersetzt und an vielen Stellen ergänzt.
Es ist auf jeden Fall hilfreich, ihn zu lesen, da er zu besserem Verständnis der Materie beiträgt und es sich somit leichter hackt :-P

Für eine erfolgreiche Anwendung des Reset Glitch Hacks ist die Kenntnis dieser Fakten jedoch nicht zwingend notwending.

## Was ist der Reset Glitch Hack ?

Um es kurz zu fassen: das Ergebnis des Reset-Glitch-Hacks ist identisch mit dem des JTAG Hacks, nur der Weg dahin ist etwas anders (CPU Glitching mittels Xilinx Coolrunner II / CMOD). Microsoft kann jedoch keine Updates gegen kompatibele Konsolen herausbringen.

Die einzige Einschränkung ist, dass der Bootvorgang bis zu 2 Minuten dauern kann.
In der Regel passiert dies jedoch, je nach Timing optimierung und Glück, innerhalb weniger Sekunden. Besonders die Falcon Boxen booten bei mir sofort und das sogar schneller als eine JTAG Konsole.

## Einleitung / wichtige Fakten

Die Software bzw. das Betriebssystem der XBOX360 wurde (ganz im Gegensatz zur PS3 oder Wii) sehr effizient gegen äußere Eingriffe abgesichert (wirksame Public Key Kryptografie, sämtliche Checks und Hashing Verfahren, ein Hypervisor usw). Selbst wenn softwareseitige Sicherheitslücken, die das Ausführen von unsigniertem Code ermöglichen (z.B. King Kong Exploit oder Teile des JTAG SMC Hacks), entdeckt werden, können diese seitens Microsoft mit einem Update schnell geschlossen- und durch das setzen einer "E-Fuse" ein Downgrade auf ein älteres, für den Hack anfälliges, Update unterbunden werden. Somit werden durch Updates von XBOX Live oder neuen Spielen diese Konsolen extrem schnell extrem selten.

Die CPU der XBOX 360 beginnt beim Start der Konsole den Code des 1BL (1. Bootloader) aus einem prozessorinternen ROM-Speicher auszulesen uns auszuführen. Da dieser Speicher im Prozessor nur lesbar ist (ein ROM halt) kann dieser nicht von Microsoft gepatcht werden. Nur durch neue CPU-Chips oder andere Hardwareänderungen sind solche Patches möglich und genau das ist bei den ganz neuen Slim Modellen (ab ca. 15.08.2011) der Fall. Diese haben keinen HANA Chip mehr auf dem Mainboard und somit fällt eine wichtige Signalleitung aus. Auch bei den alten FAT Konsolen könnte es durchaus möglich sein, dass die Geräte, welche vom Support repariert oder refurbished wurden, später einmal mit einer neue CPU bestückt werden. Dieser 1. Bootloader ist mit dem 1BL Key verschlüsselt, welcher bei allen Konsolen identisch und bekannt ist. Der 1BL läd dann den CB (2. Bootloader), welcher sich im NANDspeicher befindet sowie RSA signiert und RC4 verschlüsselt ist, und startet ihn. Der CB ist unser Knackpunkt, denn er initialisiert das Sicherheitssystem der CPU (Echtzeitverschlüsselung und Hash-Checks des RAMs) und genau dort hat der alte JTAG Hack

angesetzt, welcher jedoch durch ein Update des CB verhindert wurde.

Als Sicherheitsmethoden wird eine 128 Bit AES Verschlüsselung sowie vermutlich das Toeplitz Hashverfahren angewendet. Die Verschlüsselung variiert bei jedem Start der Konsole, da sie bzw der Schlüssel sich aus folgenden Teilen zusammensetzt:
-Eine Hashsumme des kompletten fusesets (die z.B. auch den CPU Key enthalten, JTAG Usern bekannt sein sollten)
-Ein zeitbasierter Zähler
-Eine (im Gegensatz zur PS3) wirklich zufällige Zufallszahl, welche dem Zufallszahlengenerator der CPU entspringt. Es gibt zwar bei den FAT Konsolen einen Weg, diesen Generator elektrisch zu deaktivieren, jedoch prüft der CB, ob die Zahl auch wirklich zufällig und eben nicht statisch ist.
Danach führt der 2. Bootloader eine bytecodebasierte, schlichte Softwareengine aus, die z.B. den RAM initialisiert und letztendlich den CD (3. Bootloader) aus nem NAND läd, entschlüsselt und ausführt.

Der CD beinhaltet und startet den Kernel und somit auch den Hypervisor, welcher im Originalzustand der Software eine Virtuelle Hardwareumgebung zur Verfügung stellt (ähnlich wie bei einer Virtuellen Maschine am PC) und somit sämtliche Datenströme kontrollieren und gegen Hacks absichern kann. Nur dieser Hypervisor hat genug Rechte um unsignierten Code auszuführen. Ausschließlich in den Kernelversionen 4532 und 4548 (ursprünglich bekannt durch den KingKong Exploit) existiert eine kritische Schwachstelle. Alle bekannten XBOX360 Dashboard Hacks basieren auf einem dieser Kernel und nutzen diese Schwachstelle aus, um unsignierten Code auszuführen.
Leider beinhaltet der CD bei allen Konsolen mit neuerem Kernel Hashsummen dieser anfälligen Versionen und blockiert somit den Startvorgang wenn man versucht, einen dieser Kernel zu laden.

TMBINC (ein Hacker) hat jedoch festgestellt, dass die XBOX360 nicht gegen Hardwareattacken wie z.B. die "Timing Attacks" aus dem KingKong Exploit oder eben das "Glitching" abgesichert wurden.

Unter Glitching versteht man grundsätzlich das Auslösen von Prozessorschwachstellen durch elektronische Mittel und genau auf diese Art und Weise sind wir endlich wieder in der Lage, unsignierten Code auf unseren XBOXen auszuführen.

## Der Reset Glitch Hack in ein paar Worten

Die Hacker haben herausgefunden, dass durch das Senden eines winzigen Reset Impulses an die CPU, während deren Taktrate extrem reduziert ist, diese nicht resettet wird, sondern sich die Art der Befehlsausführung ändert. Dieser Vorgang ist eine sehr effiziente Methode die Funktion "memcmp" (memory compare => Vergleich von 2 Speicherbereichen) zu veranlassen, keine Unterschiede in den verglichenen Speicherbereichen zu erkennen, selbst wenn diese Existieren. Memcmp wird oft verwendet um einen SHA Hashwert des nächsten zu ladenden Bootloaders mit einem gespeicherten Wert zu vergleichen und diesen auszuführen, falls die verglichenen Werte identisch sind. Somit ist es möglich, einen Bootloader, welcher den Hash Check nicht besteht, trotzdem zu laden und zwar in dem der vorherige Bootloader "geglitcht" wird und somit den darauffolgenden ausführt, selbst wenn dieser den Hash Check nicht besteht (z.B. läd dann der geglitchte CB anstandslos den CD).

## Details über den Hack bei FAT Konsolen a.k.a. Zephyr/Opus/Falcon/Jasper

Bei den FAT XBOXen wird der CB geglitcht und läd somit einen beliebigen CD.

Der Hacker "cjak" hat herausgefunden, dass sich durch die Belegung des "CPU_PLL_BYPASS" Signals die Taktrate des Prozessors erheblich verringert.
Somit arbeitet die CPU mit einer Taktrate von 200MHz wenn das Dashboard läuft, mit 66,6MHz wenn die Konsole bootet und mit 520kHz wenn das Signal eingespeist wird.

Dieser Vorgang läuft folgendermaßen ab:
-Das CPU_PLL_BYPASS Signal wird zeitlich gesehen in der Nähe des POST-Codes (power-on self-test - sollte euch vom PC bekannt sein) 0x36 aktiviert
-Es wird auf den POST-Code 0x39 gewartet (zu diesem Zeitpunkt wird die memcmp Funktion ausgeführt und somit der Check der Hashwerte durchgeführt) und senden dann einen 100ns Impuls auf die CPU_RESET Leitung des Prozessors
-Nach etwas Wartezeit wird die CPU_PLL_BYPASS Leitung wieder freigegeben und somit die originale Taktrate der CPU wieder aktiviert
-Mit etwas Glück wird der Bootvorgang nun fortgesetzt und der CB führt den gehackten CD aus, anstatt den Vorgang mit dem POST-Code 0xAD abzubrechen

Der NANDSpeicher muss einen "zero-paired" CB (nicht wie das original von Microsoft paired, sodass das Image nicht an die originale Konsole gebunden ist [Pairing Data wird durch Nullen ersetzt]), den Payload (sollte von der PS3 bekannt sein) im CD und ein modifiziertes SMC Image (eine Art BIOS der XBOX) enthalten.
Der Glitch ist von Natur aus unzuverlässig. Es wird daher ein modifiziertes SMC Image eingesetzt, welcher so lange rebootet, bis der Glitch erfolgreich war (bei originalen Konsolen erscheint nach 5x Rebooten ein ROD).
In den meisten Fällen funktioniert der Glitch innerhalb von 30 Sekunden nach Start der Konsole. Ich kann jedoch aus persönlichen Erfahrungen sagen, dass es meist nicht länger als 10 Sekunden dauert. Insebsondere Falcon Revisionen starten sogar schneller als eine JTAG Box - und das jedes mal!

## Details über den Hack bei SLIM Konsolen a.k.a. Trinity/Valhalla

Hier wird der Bootloader CB_A geglitcht, um einen beliebigen CB_B auszuführen.
Die Hacker konnten auf dem Mainboard der XBOX360 Slim keine Leiterbahn für das CPU_PLL_BYPASS Signal finden.
Auf der Suche nach Alternativen fanden sie heraus, dass der HANA Chip (Zuständig für die Skalierung von Videosignalen) ein konfigurierbares PLL Register besitzt, das die CPU und GPU mit einer 100MHz Taktrate versorgt. Glücklicherweise werden diese Register über einen I2C Bus vom SMC beschrieben. Dieser Bus ist frei zugänglich und besitzt sogar einen Lötpunkt auf dem Mainboard (J2C3). Somit ist der HANA Chip die neue Geheimwaffe um die Taktrate der CPU bei slim Konsolen zu verringern.
Leider ist in neuen Slim Revisionen mit Produktionsdatum ab Anfang bis Mitte August 2011 kein HANA Chip mehr verfügbar, was den Glitch Hack für diese Konsolen vorerst unmöglich macht.

Der Glitching Vorgang läuft folgendermaßen ab:
-Es wird beim POST-Code 0xD8 ein I2C Befehl an den HANA Chip gesendet, der die Taktrate der CPU verringert
-Es wird auf den Start des POST-Codes 0xDA gewartet (an dieser Stelle wird die memcmp Funktion ausgeführt) und danach ein Zähler gestartet
-Wenn der Zähler einen bestimmten Wert erreicht wird ein 20ns Impuls an die CPU_RESET Leitung des Prozessors gesendet
-Nach etwas Wartezeit wird erneut ein I2C Befehl an den HANA Chip gesendet und die CPU somit wieder auf ihre Ausgangstaktrate gesetzt

-Mit etwas Glück wird der Bootvorgang nun fortgesetzt und der CB_A führt den gehackten CB_B (2. Teil des 2. Bootloaders) aus, anstatt den Vorgang mit dem POST-Code 0xF2 abzubrechen

Wenn der CB_B startet ist der RAM noch nicht initialisiert und somit können ein paar Patches angewendet werden, um einen beliebigen CD auszuführen

-Es wird immer der zero-paired Modus aktiviert umd ein gehacktes SMC ausführen zu können
-Der CD wird nicht verschlüsselt. Es wird ein entschlüsselter CD im NAND erwartet
-Der Bootvorgang wird fortgesetzt, auch wenn die Hashprüfung des CD fehlschlägt

CB_B ist mit dem RC4 Algorithmus verschlüsselt. Dieser Schlüssel wiederum wird mithilfe des CPU-Keys entschlüsselt. Auf die Methode der Entschlüsselung seitens der Hacker möchte ich hier nicht eingehen. Jeder der Interesse an Kryptografie hat kann sich damit auseinandersetzen, für den Rest ist dieser Schritt relativ unwichtig.

Der NAND enthält nun den originalen CB_A, einen gepatchten CB_B, den Payload in einem unverschlüsselten CD sowie ein modifiziertes SMC Image.
Das SMC Image wurde modifiziert um einen unendlichen Neustart der Konsole zu realisieren (bis der Hack erfolgreich war) und um die Konsole daran zu hindern, periodisch I2C Befehle an den HANA Chip zu senden, sodass die Einspeisung zur Realisierung der niedrigen CPU Taktrate problemlos funktioniert.

## Der Clou

Der CB_A **(bei Slim Konsolen)** enthält keinen Check der E-Fuses. Somit ist dieser Hack NICHT DURCH MICROSOFT PATCHBAR (da die Chain of Trust direkt an ihrem ersten Glied gebrochen wird) und wird uns, ganz im Gegensatz zu den JTAG Konsolen, bei den bisher produzierten Slim Konsolen hoffentlich ewig erhalten bleiben!!! Für die FAT Version heißt es abwarten ob eventuell der 2-Stage CB der Slim für die FAT portiert wird, wodurch dann auch die 6752 Jasper Konsolen laufen sollten (gleicher Aufbau).

## Vorbehalte

-Der Glitch ist relativ zuverlässig (durchschnittlich 25% Erfolg pro Reset), kann jedoch auch im worst case mehrere Minuten dauern (was eigentlich nie der Fall ist und durch ausgefeiltere Firmwares der Glitch Chips [Xilinx] vermutlich noch weiter reduziert wird)
-Die Erfolgsrate scheint abhängig von der Hashsumme des zu ladenden, modifizierten Bootloaders zu sein (CD für die FAT Konsolen und CB_B für die Slims)
-Es ist präzise und schnelle Hardware erforderlich um den extrem kurzen Reset Impuls zu senden