Sony: DRM per Rootkit

Thomas Meilleroux

Januar 2007

Inhaltsverzeichnis

1 Einleitung

Ende Oktober 2005 bekam Sony BMG, ein Musikvertrieb, eine Menge negativer Publicity. Warum?

Mark Russinovitch, ein Informatiker von Sysinternals, testete ein Rootkitaufdeckungsprogramm, das er entwickelt hatte. Dabei merkte er, dass ein Rootkit[1] auf seinen System war. Während seiner Nachforschungen merkte er, dass dieses Rootkit installiert wurde, als er eine Sony-BMG CD gespielt hatte. Als diese CD eingelegt wurde, installierte sie das Rootkit, dessen Name XCP lautet.

Er hat sofort seine Entdeckung auf seiner Webseite bekanntgegeben. Damit brachte er die Nachricht in Umlauf. Tatsächlich handelte es sich um zwei Rootkits: XCP und MediaMax. Später bestätige Sony diesen Vorwurf, und vertrieb ein Programm, das diese Rootkits entfernt.

Aber diese Entfernungsprogramme öffneten Sicherheitslöcher auf dem Computer. Zum Schluss gab diese Episode Anlass für einen Prozess.

2 Wer wollte was?

In diesem Abschnitt wird die Rede von zwei Akteuren sein. Einerseits der Musikvertrieb und auf der anderen Seite die Gesellschaft, die das Kopieschutzprogramm entwickelt hat.

2.1 Der Musikvertrieb

Man kann sich denken, dass der Musikvertrieb nur will, dass seine CD's nicht kopierbar sind. Damit kann er eine CD pro Hörer verkaufen. Aber jeder Musikvertrieb weiss wohl, dass die Musik immer kopierbar bleibt, sei es nur Analog. Das Ziel ist nicht die Peer-to-peer-Teilung zu verhindern, sondern sie auszuschieben (Der Benutzer wird tatsächlich die Musik kopieren können, egal wie. Bevor das passiert, will der Musikvertrieb ein Maximum CD's verkaufen.).

Mit XCP und MediaMax ist auch noch etwas weiteres möglich: Werbung durch das Spielprogramm anzuzeigen. Es ist sehr einfach, da der Benutzer dieses Programm braucht. Durch die Internetverbindung wird gezielte Werbung angezogen.

2.2 Der Entwickler

Wie der Musikvertrieb will der Entwickler des DRM-Programm Geld verdienen. Ein Weg dazu ist andere Musikvertriebe zu bestricken, damit sie neue Kunden werden. Darum muss die Entwicklungsfirma eine funktionale Technologie einsetzen. Dann muss diese Firma ihr Programm auf mehrere Computer einstellen. Im Unterschied zum Musikvertrieb ist diese Firma nicht sehr bekannt. Deshalb hat sie kein Image zu behaupten. Manchmal handelt sie gegen das Interesse des Musikvertriebs. Sie kann auch den Schutz ihres Programmes hinpfuschen, um Entwicklungszeit (und Entwicklungsgeld) zu sparen. Der Musikvertrieb wird Mühe haben, um diese Einsparung zu merken, da er oft kein Technikwissen hat.

Abschließend kann man behaupten, dass die Digitale Rechteverwaltung (DRM[2]) einen starken Einfluss auf dem Musikmarkt ausüben. Die DRM-Verkäufer (oder die DRM-Software-Entwicklern) kämpfen um ihre Programme zu verbreiten. Die Musikvertriebe kämpfen gegen das Monopol eines DRM-Verkäufer, damit die Preise nicht sehr hoch steigen.

[1] Rootkit: Ein Programm, dass ein betrügerischen Zugriff zu einem System erlaubt.

[2] DRM (engl. Digital Rights Management) ist ein Verfahren, mit dem die Verbreitung digitaler Medien kontrolliert werden kann

3 Wie funktioniert dieser Schutz?[2]

Diese Schutzmaßnahmen haben zwei Hauptziele. Sie zielen auf die Verhinderung

1. Der Kopie auf eine andere CD und
2. Die Enkodierung dieser CD (z.B. als mp3).

Aber man muss die Musik, die man gekauft hat, immer genießen können. Deshalb sollen diese Schutzsysteme die Lesbarkeit über Lesegeräte nicht verhindern. Aus Erfahrung merkt man, dass es leider nicht ganz möglich ist. Besonders wenn man mit alten Geräten rechnen will.

Wir setzen in diesem Abschnitt voraus, dass die Kopie der CD mit einem Computer gemacht wird[3].

3.1 Der temporäre Schutz

Die beiden Schutzmaßnahmen SCP und MediaMax benutzen das Autorunsystem von Windows™ um das aktive Schutzsystem zu installieren. Dieses System funktioniert aber nur mit Windows™ . Mit Linux und MacOS zum Beispiel wird die CD normal, oder gar nicht lesbar sein. Es wird später noch die Rede von dieser CD-Anerkennung sein.

Es ist aber aus ethischen Gründen nicht möglich, das aktive Erkennungsystem zu installieren, ohne den Benutzer zu warnen[4]. Während dieser Zeit könnte der Benutzer ein Fremdprogramm starten, um die CD zu kopieren oder zu kodieren. MediaMax und XCP behandeln diese Lücke verschiedent.

3.1.1 XCPs temporäre Schutz

Wenn man eine XCP geschützte CD einlegt, wird der Lizenzvertrag angezeigt. Während dieser Zeit wird ein anderes Programm gestartet. Diese Anwendung läuft im Hintergrund und sucht nach laufende Brenn- oder Kodierprogramme. Wenn sie eins gefunden hat gibt sie dem Benutzer 30 Sekunden um es zu schließen, dann wirft sie die CD aus.

Der Hauptnachteil dieses Systems besteht darin, dass es auf eine Liste von Brenn- und Kodierprogrammen angewiesen ist. Es ist doch einfach für einen Benutzer, eine Anwendung so umzubenennen, damit diese den Schutz sprengt.

Dieses System hat auch andere Lücken. Man kann zum Beispiel den Untersuchungsprozess killen, oder eine Brennsoftware, die das CD-ROM-Laufwerk sperrt.

3.1.2 Der temporäre Schutz von MediaMax

Der Hauptunterschied zwischen MediaMax und XCP Systeme besteht darin, dass MediaMax den Aktivschutz startet, bevor der Benutzer den Lizenzvertrag angenommen hat.

Das stellt zwar ein akutes Rechtsproblem, aber der Schutz ist daher natürlich viel wirksamer !

[3] Es gibt auch autonome CD-Brenner, von denen nicht die Rede sein wird.

[4] Der Benutzer muss erst den Endbenutzer-Lizenzvertrag (engl. EULA) annehmen.

3.2 Das CD-Anerkennungssystem

Der aktive Schutz besteht in einem Anerkennungssystem. Die CD ist auf einem Computer nur durch das DRM-Programm lesbar. Um diese Bedingung zu erfüllen leitet die Software die Datenblöcke zwischen dem Betriebssystem und dem CD-ROM-Laufwerk um. Wenn der Benutzer seine CD mit seiner eigenen Software abspielen will, dann wird er nur einen undefinierbaren Lärm hören. Dasselbe wird auch mit einem Kopier- oder Kodierungsversuch geschehen.

3.2.1 Anforderungen an das Erkennungssystem

Idealerweise sollen die Erkennungssysteme die folgende Bedingungen erfüllen:

1. *Einzigkeit*: Die CD muss unbedingt erkannt werden, damit andere CD's nicht korrumpiert würden.

2. *Festellbarkeit*: Das System soll zuverlässig und schnell sein, um die Leistungen nicht zu verringern.

3. *Unzerstörbarkeit*: Das Schutzsystem soll keine Deaktivierung erlauben, es sei denn dass eine Verminderung der Qualität geschehe.

4. *Unfälschbarkeit*: Es soll schwierig sein, diesen Schutzsystem auf eine andere CD einzuführen, ohne mit der DRM-Programmentwicklungsfirma zu kooperieren.

3.2.2 Wie funktioniert es?

Die beiden Schutzsysteme benutzen ein Markierungsverfahren. Eine unhörbare Marke[5] wird in eine Tonspur geschrieben. Diese Marke wird nur von dem MediaMax System analysiert werden[6].

Die Marke ersetzt einen von den 3 Bits mit dem niedrigsten Stellenwert von 288 Audiostücke, die 16-Bits lang sind. Das System folgt dieser Regel:

2, 3, 1, 1, 2, 2, 3, 3, 2, 3, 3, 3, 1, 3, 2, 3, 2, 1, 3, 2, 2, 3, 2, 2, 2, 1, 3, 3, 2, 1, 2, 3, 3, 1, 2,
2, 3, 1, 2, 3, 3, 1, 1, 2, 2, 1, 1, 3, 3, 1, 2, 3, 1, 2, 3, 3, 1, 3, 3, 2, 1, 1, 2, 3, 2, 2, 3, 3, 3, 1,
1, 3, 1, 2, 1, 2, 3, 3, 2, 2, 3, 2, 1, 2, 2, 1, 3, 1, 3, 2, 1, 1, 2, 1, 1, 1, 2, 3, 2, 1, 1, 2, 3, 2, 1,
3, 2, 2, 2, 3, 1, 2, 1, 3, 3, 3, 3, 1, 1, 1, 2, 1, 1, 2, 2, 2, 2, 3, 1, 2, 3, 2, 1, 3, 1, 2, 2, 3, 1, 1,
3, 1, 1, 1, 1, 2, 2, 3, 2, 3, 2, 3, 2, 1, 2, 3, 1, 3, 1, 3, 3, 3, 1, 1, 2, 1, 1, 2, 1, 3, 3, 2, 3, 3, 2,
2, 1, 1, 1, 2, 2, 1, 3, 3, 3, 3, 3, 1, 3, 1, 1, 3, 2, 2, 3, 1, 2, 1, 2, 3, 3, 2, 1, 1, 3, 2, 1, 1, 2, 2,
1, 3, 3, 2, 2, 3, 1, 3, 2, 2, 2, 3, 1, 1, 1, 1, 3, 2, 1, 3, 1, 1, 2, 2, 3, 2, 3, 1, 1, 2, 1, 3, 2, 3, 3,
1, 1, 3, 2, 1, 3, 1, 2, 2, 3, 1, 1, 3, 2, 1, 2, 2, 2, 1, 3, 3, 1, 2, 3, 3, 3, 1, 2, 2, 3, 1, 2, 3, 1, 1,
3, 2, 2, 1, 3, 2, 1, 3

Ein 1 bedeutet, dass das 1. Bit mit dem niedrigsten Stellenwert geändert wird, 2 bedeutet, dass das Bit mit dem zweiten niedrigsten Stellenwert geändert wird usw.

Es sind die Bits mit dem niedrigsten Stellenwert, die geändert werden, denn sie beeinflussen die Daten weniger.

Es gibt auch eine Regel um zu wissen, womit diese Bits ersetzt werden können:

[5] Auf Englisch wird diese Methode "Watermark" genannt.
[6] XCP Schutz benutzt ein ähnliches Markesystem, aber es ist leichter.

$0, a, b, c, d, e, 0, 0, f, 0, g, 0, h, i, d, j, \bar{j}, k, 0, l, m, 0, n, o, p, \bar{e}, q, \bar{e}, r, 0, \bar{p}, s, d, \bar{m}, t, u, v, w, t, \bar{l}, a, x,$
$c, u, 0, \bar{r}, l, f, \bar{d}, v, 0, m, 0, \bar{q}, 0, y, c, z, 0, j, \bar{i}, \bar{g}, \alpha, \bar{s}, \bar{w}, \bar{h}, v, y, n, 0, 0, \bar{h}, \bar{j}, \bar{u}, \alpha, \beta, 0, \bar{v}, g, j, 0, 0, \bar{\beta}, \bar{i},$
$e, \bar{z}, 0, r, \gamma, \bar{a}, \delta, \bar{d}, \bar{z}, 0, \bar{v}, \epsilon, 0, x, s, \bar{g}, \bar{r}, 0, \bar{b}, o, b, r, 0, y, \bar{\beta}, \bar{m}, h, 0, \bar{a}, n, \bar{f}, \bar{t}, 0, \bar{o}, 0, \bar{\gamma}, \bar{\epsilon}, \bar{e}, 0, 0, \bar{k}, \bar{c},$
$\bar{x}, 0, \bar{f}, p, z, \bar{x}, i, 0, 0, \alpha, \bar{g}, 0, 1, w, \bar{t}, \bar{n}, \bar{w}, i, 0, 0, \bar{j}, m, x, \beta, \bar{y}, \bar{p}, \bar{q}, 0, 0, 0, e, \bar{\beta}, 0, 0, 1, g, 0, p, l, 0, \bar{\alpha},$
$t, h, \bar{d}, \bar{\epsilon}, \bar{w}, \gamma, \bar{\delta}, 0, \bar{p}; q; \bar{f}, 0, 1, \zeta, 0, \bar{c}, \zeta, \bar{\alpha}, \bar{s}, \bar{b}, \bar{\gamma}, \bar{\beta}, 0, o, 0, q, \bar{i}, 0, 0, \bar{\alpha}, s, \epsilon, \bar{\epsilon}, \bar{h}, 0, \bar{k}, \bar{n}, \bar{\zeta}, \alpha, \bar{s}, \bar{z}, \bar{n},$
$\bar{c}, \bar{o}, \bar{b}, 0, \bar{t}, 0, \bar{y}, \bar{v}, 0, \zeta, \bar{o}, 0, \bar{\zeta}, 0, u, \gamma, 0, \bar{y}, k, \bar{u}, z, \bar{\delta}, \bar{q}, k, \bar{r}, \bar{u}, \bar{\zeta}, \bar{\gamma}, \bar{l}, \bar{l}, w, \bar{k}, \bar{a}, 0, \bar{\zeta}, 0, \epsilon, \bar{m}, b, f, 0, 0,$
$\bar{x}, \delta, \delta, 0, *$

Also es gibt:

- 64 Bits, die einen festen Wert haben (0 oder 1)
- 192 Bits, die in 32 Gruppen geteilt werden ($a - z$ und $\alpha - \zeta$). Damit wird eine 32-Bit-Variable kodiert: A. ($\bar{a}$ ist gleich 0 wenn a gleich 1 ist, und umgekehrt)
- 32 Bits (die Sternchen), die eine 32-Bit-Variable: B repräsentieren.

Die Variable A erlaubt zwischen Alben zu unterscheiden. Sie wird eindeutig für jedes Album kodiert.

Die Variable B wird in MediaMax 5 benutzt, um zu unterscheiden, ob die CD original ist, oder ob sie eine erlaubte Kopie ist[7].

3.2.3 Analyse des " Watermarking" System

Das System ist sehr einfach, deshalb erfüllt es nicht die 3. und die 4. Bedingungen. SunnComm[8] sollte nie eine CD in die beide Formen verkaufen. Das erlaubte das Reverse Engineering, einfach vergleichend eine japanische CD und eine US CD. Im Gegenteil sollte der Schutzschlüssel geheim behalten werden.

Was auch nicht abgezeichnet wird, ist das Verhalten dieses System im Streichenfall. Man könnte (vorsätzlich oder nicht) die CD streichen, damit könnten einige Bits geändert werden, und die Schutzmaßnahme entfernen werden.

Das "Watermarking" hat zwei Nachteile[3]:

- Im Vergleich zu verschlüsselten Systemen, denen man die Robustheit verbessern kann, verlängernd die Schlüssellange, werden die Verbesserungstechniken der "Watermark" Systeme beschränkt. Die veränderbare Informationsmenge in einem Inhalt ist gering, und könnte immer geringer werden. Der technische Progress im Komprimierungsfach will die nutzlose Informationsmenge reduzieren (zu denen gehört das " Watermark").
- Das "Watermarking" braucht einen Detektor. Die Software kann deshalb einfach ein Reverse Engineering erleiden. Darüber hinaus gibt es manchmal CDs, die nicht geschützt werden (z.B. Die Probe-CD).

[7] MediaMax 5 Programm kann auch die Kopie (privat) erlauben, aber nur ein Mal (Die Kopie soll nicht kopierbar sein)

[8] Die Firma, die MediaMax entwickelt.

4 Computer bedroht?

Eine wichtige Frage wird gestellt: Wird mein Computer bedroht?

4.1 XCP

Der Betrieb von XCP ist gefährlich in dem Sinn, dass XCP alle die Dateien versteckt, deren Name mit einer gewissen Sequenz anfängt. Das kann von einem Computervirus ausgenutzt werden, um sich zu verstecken, damit es nicht von Anti-Virus-Software feststellbar ist.

4.2 MediaMax

Das MediaMax System ist gefährlicher als XCP, da es ungefähr 12MB an Daten auf die Festplatte des Benutzers kopiert, wenn der Lizenzvertrag noch nicht angenommen ist. Darüber stellt es die Zugriffsrechte so ein, dass irgendwelche Programme diese Daten ändern könnten. Ein Computervirus kann diese Lücke ausnutzen, um einen Bösen Code an der Stelle des Quellcode dieser Datei zu installieren. Diese Methode wird durch die Zugriffskontrolle erleichtert, da das MediaMax Spielprogramm die Zugriffsrechte des Administrators braucht, um zu funktionieren. Dies ist auch der Grund warum der Benutzer nicht einfach die Zugriffsrechte korrigieren kann. Tatsächlich "'repariert" MediaMax diese Zugriffsrechte, um sie anzupassen, jedesmal wenn der Benutzer seinen Computer startet.

In den beiden Fälle wird der Computer bedroht. Die beide Firmen hatten ein Löschprogramm verbreitet, um diese Lücke zu korrigieren. Es hat leider nicht die richtige Wirkung gehabt. Zum Glück haben einige Informatiker Wege gefunden, um diese Sicherheitslöcher zu überschütten.

5 Wie deaktivieren?

In diesem Abschnitt werden die Deaktivierungswege erklärt. Der Benutzer wird damit die normale Benutzung seiner CD wiederhaben. Wir werden uns hier nur mit Windows^{TM} beschäftigen.

5.1 MediaMax

Der MediaMax Schutz ist relativ einfach zu deaktivieren. Der Benutzer soll ein Command-Line-Programm dessen Name "SC" lautet. Dieses Programm erlaubt, alle Dienste von Windows zu verwalten. Man soll diesen Befehl eintippen:

```
sc stop sbcphid
```

Um den Prozess zu halten, und

```
sc delete sbcphid
```

Um den Prozess zu löschen, damit wird er dauerhaft entfernt wird.

5.2 XCP

Der aktiver Schutz von XCP ist viel schwieriger zu entfernen als der von MediaMax. Der Grund dafür ist, dass XCP mehrere Prozesse enthält die tief im System stehen. Die Manipulation besteht in drei Stufen:

1. Entfernung des Rootkits:

   ```
   sc delete \$sys\$aries
   ```

   Entfernung der:

   ```
   %windir%\system32\$sys$filesystem\aries.sys
   ```

   Computer neustarten

2. Entfernen aus der Registrierung:

   - Alles was `$sys$cor` enthält.
   - Alles was `$sys$crater` enthält.

   `$sys$caj.dll` in der Registrierung suchen und darin `CoInstallCdrom` und `CoInstallPC` entfernen

3. XCP Services entfernen (in Befehlsfenster): `sc delete $sys$crater`
   ```
   sc delete $sys$lim
   sc delete $sys$oct
   sc delete cd_proxy
   sc delete $sys$drmserver
   sc delete $sys$cor
   sc delete $sys$
   del %windir%\system32\$sys$filesystem\crater.sys
   del %windir%\system32\$sys$filesystem\lim.sys
   del %windir%\system32\$sys$filesystem\oct.sys
   del %windir%\system32\drivers\$sys$cor.sys
   del %windir%\system32\$sys$caj.dll
   del %windir%\system32\$sys$upgtool.exe
   ```
   Neustarten und:
   ```
   del %windir%\CDProxyServ.exe
   del %windir%\system32\$sys$filesystem\$sys$DRMServer.exe
   ```

Und endlich sind Sie befreit !

6 Die menschlichen Aspekte der DRM

6.1 Was können die DRM (am schlimmsten) machen?

Hier wird die Rede von den Nachteilen der DRM sein[1]:

- Das Lesen mit dem Autoradio oder Computer vermeiden: Es ist ja wahrscheinlich, wenn das Autoradio älter als ein Paar Jahre ist, dass es nicht das Sicherheitssystem erträgt. Ebenso für die CD-Laufwerk.
- Die Kopie von der CD zum MP3-Spieler vermeiden
- Die Kopie von dem MP3-Spieler zur CD vermeiden: Diese beiden letzten Aspekte behindern die Kunden. Sie können nicht verfügen wie sie wollen, von der Musik die sie gekauft haben.
- Der Zugriff zur Musik verbieten: Manchmal kommunizieren die DRM-Schutzmaßnahmen mit einem Zentralserver. Dieser Server gibt die Erlaubnis zum Benutzer, damit kann er die Musik spielen oder kopieren. Wenn der Benutzer seine Musikdaten von einer Plattform geladen hat, ist er total abhängig von dieser Plattform. Wenn sie Bankrott erleidet, dann kann der Zentralserver ausgeschaltet werden. Das bedeutet, dass dieser Benutzer kein Zugriff mehr hat, um seine Musik zu hören !
- Die musikale Vorzüge spionieren: Durch diesen Server kann auch der Musikvertrieb wissen, was die Vorzüge der Benutzer sind, um zum Beispiel gezielte Werbung zu senden.

6.2 Wie kann man die DRM-CD erkennen?

Es gibt ein Logo, das die DRM-CD identifiziert:

Dieses Logo ist aber oft sehr klein. Manchmal gibt es auch eine Erklärungssatz über die DRM, aber nicht immer. Zum Glück gibt es einen anderen Weg, um eine DRM-CD zu identifizieren. Wahrscheinlich kennen Sie dieses Logo:

Es identifiziert alle CDs, die mit einer Stereoanlage lesbar sind. Phillips, eigentümer dieses Logo, lehnt ab, es auf DRM-CDs bringen.

6.3 Die Vorteile der DRM-CDs

Die DRM versuchen, die wilde Kopie zu vermeiden, aber der Kunde soll auf seinem Recht der Privatkopie verzichten.

Ein Vorteil besteht darin, dass die DRM die Musikvermietung erlauben. In der Tat kauft der Kunde die Musik nicht, sondern er mietet sie !

6.4 Die Musiker und die DRM

Die Musiker werden nicht befragt, wenn der Musikvertrieb sich entscheidet, um ein DRM auf ihrer CD einzusetzen. Aber meistens sind sie dagegen. Das Ziel der DRM war mehr CDs zu verkaufen, aber in der Tat werden die geschützten CDs weniger verkauft. Dieses Phänomen wird so erklärt, dass die Kunden kein Beschränkung auf ihre Musik wollen. Sie ziehen es vor, eine unbeschränkte Version illegalerweise zu erlangen.

7 Fazit

Diese Analysen zeigen, dass XCP und MediaMax als Kopierschutz technisch nicht ohne Einverständnis der Nutzer wirksam sind, auf deren Geräten sie installiert werden. Diese Schutzmaßnahmen öffnen auch wichtige Sicherheitslücke auf den Computern auf denen sie installiert werden. Man kann natürlich diese Programme als Rootkit behandeln, da sie eine Fernadministration erlauben, von dem Softwareentwickler sowie von Piraten.

Aber der wichtigste Aspekt ist kein technologisches Problem, sondern ein ethisches Problem. Der Kunde ist vom König zum Feind mutiert und wird auch als Feind behandelt. Es ist doch normal, und niemand darf sich darüber wundern, dass die Kunden damit nicht zufrieden sind.

Die von den Sicherheitslücken betroffenen Nutzer wollten übrigens einfach nur Musik hören !

Literatur

[1] Corsario. Les drm pour les nuls. 2006. http://stopdrm.info/index.php?2006/04/02/28-les-drm-pour-les-nuls.

[2] J. Alex Halderman and Edward W. Felten. Lessons from the sony cd drm episode. 2006.

[3] Marc Herubel and Franck Tarrier. Mesures techniques de protection des oeuvres & drms. 2003. fr.