Meditationen über Trusted Computing

Fred von Lohmann

1641 stellte der Mathematiker und Philosoph René Descartes in seinen „Meditationen über die Grundlagen der Philosophie“ die Frage, wie wir unseren Sinnen vertrauen können. Was, wenn alles, was wir erleben, in Wahrheit Teil einer Illusion ist, die von einem allmächtigen Dämon geschaffen wurde, um uns zu täuschen?

Tatsächlich beschäftigen sich Microsoft, Intel und eine Reihe anderer Computerfirmen seit einiger Zeit mit einem ähnlichen Problem. Woher wissen wir, dass unser Computer das ist, was er zu sein scheint? Es könnte ja sein, dass sich Hacker Zugang zu unserem Gerät verschafft und unsere Software gegen andere Programme ausgetauscht haben, die der Originalsoftware bis ins Detail ähneln. Wir würden keine Veränderung bemerken. Unser Computer wäre jedoch völlig in der Hand des Hackers, der jeden Tastenanschlag verfolgt, unsere intimsten Informationen kopiert und sie über unsere eigene Internetverbindung versendet.

Diese Überlegung lässt weitere erkenntnistheoretische Zweifel aufkommen – wie kann eine Software, die wir verwenden, den anderen Programmen auf unserem Computer vertrauen? Wie können wir zum Beispiel, wenn wir einen Anti-Virus-Check durchführen, sicher sein, dass das Betriebssystem nicht irgendwie unterlaufen wurde? Es könnte ja sein, dass die von den Hackern installierte Software sämtliche Virus-Warnungen abfängt, bevor sie auf dem Bildschirm erscheinen, und sie durch die Meldung „Keine Probleme festgestellt“ ersetzt.

Wie können wir also sicher sein, dass nicht alles, was wir auf unserem Computer erleben, Teil einer Illusion ist, die von Hackern geschaffen wurde, um uns zu täuschen?

Das sind keine müßigen Fragen. Heutzutage sind Anwender in zunehmendem Maß heimtückischer, schwer zu entdeckender Software ausgesetzt, die dazu programmiert ist, Computer zu unterlaufen – Viren, Trojaner, Würmer und Spyware, um nur einige zu nennen. Dieses Schreckgespenst betrifft nicht nur Einzelanwender, sondern auch zahlreiche Unternehmen, zum Beispiel im Bereich der Gesundheitsfürsorge, Filmstudios, Nachrichtendienste und andere, die ihren Computern regelmäßig wertvolle oder geheime Informationen anvertrauen.

Genau hier tritt die *Trusted Computing Group* (TCG) auf den Plan, zu der Microsoft, Intel, AMD und einige andere große Computertechnologiefirmen gehören. Die Unternehmen der TCG arbeiten an Technologien, mit deren Hilfe wir uns sicher sein können, dass unser Computer genau das ist, was er zu sein scheint.

Was genau ist Trusted Computing?

Zuerst müssen wir uns einen neuen Computer kaufen (Sie haben doch nicht wirklich auch nur eine Sekunde gedacht, dass ein von den weltgrößten Software-, Chip- und Computerherstellern entwickelter Plan anders anfangen könnte?), der einen Spezialchip mit kryptografischer Hardware und Schlüsseln enthält. Wir können den neuen Chip nun bewusst ignorieren, und unser Computer wird genau wie der alte funktionieren. Wir können jedes Betriebssystem und jede beliebige Software installieren. Der Chip ruht, bis wir beschließen ihn zu nutzen.
Sobald wir die vom Chip gestützten Trusted-Computing-Features aktivieren und wenn unser Betriebssystem für den Einsatz des Chips aktualisiert wurde, wird unser Computer „virtuell" in zwei Teile gespalten, und zwar in einen „ungesicherten" und einen „gesicherten". Beide Seiten teilen sich CPU, Festplatte, Tastatur und Schirm, die gesicherte Seite hat jedoch eine ganz spezielle Zusatzeigenschaft – sie kann von keiner anderen Software auf unserem Computer unterlaufen werden. Mit anderen Worten können wir also auf der gesicherten Seite Software verwenden, die mit hoher Wahrscheinlichkeit genau das ist, was sie zu sein scheint.
Wie funktioniert das? Nun, das Ganze hat mit jeder Menge ausgeklügelter Kryptografie zu tun. Speichert die gesicherte Seite unseres Computers über eine bestimmte gesicherte Softwareapplikation Daten auf der Festplatte oder in den Speicher, so geschieht das in einem sicheren, verschlüsselten Format. Diese verschlüsselten Daten können nur von der Softwareapplikation auf der gesicherten Seite des Computer gelesen werden.
Eventuell auf dem Computer vorhandene bösartige Software (sei es auf der gesicherten oder der ungesicherten Seite) kann die verschlüsselten Daten einer gesicherten Applikation nicht lesen. Zusätzlich verfügt die gesicherte Seite über einen sicheren, verschlüsselten Zugang zu Tastatur und Schirm, sodass bösartige Software Daten nicht abfangen oder sich zwischen uns und die gesicherte Applikation stellen kann.
So können wir also der Integrität der Software auf der gesicherten Seite vertrauen und sicher sein, dass die über diese Software gesicherten Daten für möglicherweise manipulierte Software auf der ungesicherten Seite unzugänglich sind. (Der Computer ist jedoch weiterhin anfällig für Angriffe von Hardware-Seite, sofern der Hacker darauf Zugriff hat.)
So weit, so gut.

Trusted Computing: Beunruhigende Auswirkungen

Trusted Computing führt allerdings nicht nur dazu, dass wir unserem eigenen Computer vertrauen können. Die Technologie soll dies auch *anderen* ermöglichen. Der Schlüssel dazu liegt in einem Feature namens „indirekte Authentifizierung". Es ermöglicht einer anderen Person, die Software auf der gesicherten Seite unseres Computers um Identifizierung zu bitten. Die Antwort kommt von der gegen Manipulation geschützten Hardware auf der Hauptplatine unseres Computers, und die „Authentifizierung" ist daher relativ verlässlich. Dieses Feature hat gewiss nützliche Anwendungen (etwa für Mitarbeiter, die sich von außerhalb in Firmennetzwerke einloggen).
Es gibt jedoch auch eine Kehrseite der Medaille. Sobald Außenstehende feststellen können, dass auf der gesicherten Seite unseres Computers eine bestimmte Software zur Anwendung kommt, könnten sich einige überhaupt weigern, mit uns zu kommunizieren, wenn wir ihre Software *nicht* verwenden. Anders gesagt, könnten Firmen von uns verlangen, auf der gesicherten Seite unseres Computers die Software *ihrer Wahl* zu installieren, womit sie im Endeffekt die Kontrolle über einen Teil des Computers hätten. Natürlich könnten wir dies ablehnen, doch würden wir mit dem jeweiligen Unternehmen dann keine Geschäfte mehr machen.
Dieses Problem stellt sich möglicherweise auf einem wettbewerbsfähigen Markt nicht, da die Anbieter alles tun würden, um potenzielle Kunden nicht zu verlieren. Ist der Wettbewerb jedoch beeinträchtigt, so kann Trusted Computing es einem Monopolisten oder Kartell gefährlich leicht

machen, nach dem Motto „Alles oder nichts!“ zu arbeiten, da sie mittels Trusted Computing auf der relativen Zugriffssicherheit unseres Computers bestehen können.

Stellen wir uns zum Beispiel vor, dass die Hollywood-Studios beschließen, ihre Filme in einem Format zu veröffentlichen, das nur über bestimmte gesicherte Media-Player-Softwareprogramme abspielbar ist. Über die „indirekte Authentifizierung“ ließe sich feststellen, ob die Media-Player-Software tatsächlich auf der gesicherten Seite unseres Computers installiert ist und dass sich niemand daran zu schaffen gemacht hat. So hätten die Filmstudios eine beispiellose Kontrolle darüber, wie unser Computer mit ihren Filmen umgeht. Es wäre Hollywood überlassen, ob wir weiterhin Kopien machen und Ausschnitte herausnehmen, den Schnellvorlauf betätigen oder den Ton abschalten könnten. Folglich würde ein Teil unseres Computers nicht länger unseren Befehlen folgen, sondern denen Hollywoods.

Die Auswirkungen gehen jedoch weit über das „Digital Rights Management“-System hinaus, das die Unterhaltungsindustrie durchzusetzen versucht. Anderen Industriezweigen wäre es vielleicht ebenfalls nur allzu lieb, als Voraussetzung für mögliche Geschäftsbeziehungen einen geeigneten Brückenkopf in unseren Computer zu verlangen. So könnte zum Beispiel der marktführende Anbieter einer bestimmten Softwareapplikation (wie Microsoft Word für die Textverarbeitung) in Zukunft eine geschützte Version so modifizieren, dass wir unsere Dokumente nicht länger über die Applikation eines Konkurrenten bearbeiten können.

So wie viele Technologien hat auch das Trusted Computing positive und negative Implikationen und sollte daher kritisch betrachtet werden. Andernfalls endet der Anwender möglicherweise mit den Worten Descartes „[w]ie ein Gefangener, der zufällig im Traume einer eingebildeten Freiheit genoss, bei dem späteren Argwohn, dass er nur träume, sich fürchtet aufzuwachen und deshalb den schmeichlerischen Täuschungen sich lange hingibt.“

Aus dem Amerikanischen von Elisabeth Wiellander