Trusted Platform Module:
Vertrauen und Sicherheit in der Informationsverarbeitung?

Diplomarbeit

zur Erlangung des Grades eines Diplom-Ökonomen der
Wirtschaftswissenschaftlichen Fakultät der Universität Hannover

vorgelegt von

Name: **Seliger** Vorname: **Thomas**

[redacted]

Erstprüfer: **Professor Dr. H. Breitner**

Hannover, den 30.01.2004

INHALTSVERZEICHNIS

1. Einführung

Der Stärkere ist als solcher noch lange nicht der Bessere.
(Carl Jackob Burckhardt)

Als die Bibel 1380 vom Lateinischen ins Englische übersetzt wurde konnte diese Bewegung vom Klerus noch leicht unterdrückt werden, da nur wenige Exemplare handschriftlich hergestellt wurden. Bei der Übersetzung des Neuen Testaments 1524 wurden bereits 50.000 Exemplare gedruckt, bevor die damalige Widerstandsbewegung gegen die Kirche gefasst werden konnte. Dies reichte aber aus, um in Europa ein neues Zeitalter beginnen zu lassen.[1]

Gesellschaften, die seither versuchten Informationen zu kontrollieren, verloren meistens ihre Wettbewerbsfähigkeit. Der Zusammenbruch der Sowjetunion ist hierfür ein Beispiel. Wurde dort noch versucht sämtliche Schreibmaschinen und Faxgeräte des Landes zu registrieren, steht nun mit der Trusted Computing Group (TCG) eine Organisation an der Spitze der Trusted Computing (TC) Bewegung, die ähnliches bei Computern zu leisten versucht. Hard- und Software sollen lizenziert werden und dadurch sicherer und vertrauenswürdiger werden. Unerwünschte Eindringlinge wie Viren, Würmer, Spam oder Trojaner sollen der Vergangenheit angehören und das Eindringen in Informationstechnologie (IT) Systeme unmöglich werden. Dies soll mittels eines speziellen Sicherheitsbausteins und sicherer Hardware geschehen. Die TCG entwickelt hierfür Spezifikationen, deren zentraler Baustein ein Trusted Platform Modul (TPM) ist, mittels dem ein oder mehrere Institutionen über die Sicherheit aller TPM-basierten IT-Systeme wachen. Eng verbunden mit TC ist die digitale Rechteverwertung (DRM)[2], deren Einführung insbesondere von den großen Medienkonzernen erwartet wird, um digitales Kopieren überwachen und einschränken zu können.

Gegenstand dieser Arbeit ist die Untersuchung der Frage, ob TPM der Informationsverarbeitung zu mehr Sicherheit und Vertrauen helfen können. Weiterhin sollen die Fragen erörtert werden, ob und unter welchen Voraussetzungen dies zu einer marktbeherrschenden Stellung der TCG führt und ob nicht der Anwender selber an der Spitze der Sicherheitskette stehen sollte. Um diese Fragen zu beantworten, sollen zunächst die für dieses Thema grundlegenden Sicherheitsaspekte im Bereich der IT vorgestellt werden. Daran anschließend erfolgt eine kurze Vorstellung des TC mit einigen Beispielen von

[1] Hermanns [o. D.]
[2] Digital Rights Management

Anwendungen in diesem Bereich, die bereits heute zum Einsatz kommen. TC kann nicht nur im Computersektor eingesetzt werden, sondern auch dort, wo eingebettete Kleinstcomputer[3] heute schon Einzug erhalten haben, beispielsweise im Kraftfahrzeugbereich, im Bereich der Mobilkommunikation oder in naher Zukunft auch in intelligenten Haushaltsgeräten, wobei sich diese Arbeit hauptsächlich auf einige ausgewählte Bereiche des Computersektors bezieht. Hier soll auch die Verbindung zum Internet, zu DRM und zu freier Software aufgezeigt werden. Im Anschluss daran soll die TCG vorgestellt werden. Dies beginnt mit einer Beschreibung der Organisationsstruktur. Danach erfolgt eine kurze Einführung in die Funktionsweise des TPM und die Vorstellung einiger Konzepte von Mitgliedern auf Basis des TPM. Abschließend sollen die Ziele der TCG dargestellt werden.

Im anschließenden Kapitel werden die rechtlichen Grundlagen erörtert, auf deren Basis TC, TPM und DRM beruhen, und einige mögliche rechtliche Entwicklungen aufgezeigt. Diesen Ausführungen folgt eine Bewertung des TC und des TPM, wobei zunächst Chancen und Risiken auf Anbieter- und Anwenderseite und anschließend ausgewählte wirtschaftliche Erfolgsfaktoren analysiert werden. Abschließend sollen dann einige ausgesuchte Szenarien aufgezeigt werden, welche die Risiken bei der Etablierung und der Folgen beschreiben sollen. Den Schluss bildet eine zusammenfassende Einschätzung der Folgen des möglichen Einsatzes von TC auf Basis von TPM.

2. Sicherheit in der Informationstechnologie

Seit Ende der sechziger Jahre besteht ein zunehmendes Interesse an Datenschutz und Datenschutzkonzepten. Die Beschäftigung mit Themen der IT-Sicherheit ist von einem Spezialgebiet zu einem grundlegenden globalen Problem moderner Industriegesellschaften geworden.

Ein Jahrzehnt später wurden erste Gesetze erlassen, die den Umgang mit Daten, besonders mit deren Manipulation und Vervielfältigung, reglementierten. Was man unter den Begriffen Informationen, Daten und Sicherheit versteht, welche Arten von Sicherheit im heutigen IT-Sprachgebrauch verwendet werden und welche Schwierigkeiten durch die zunehmende Vernetzung im IT-Sektor entstanden sind, soll in diesem Kapitel erläutert werden.

[3] sogenannte „embedded Coputers“

einer Aufteilung in moderne aber TC-abhängige Nutzer und zu unabhängigen Anwendern führen. Würde die Produktion dieser Produkte dann eingestellt, könnte es zu einem rasant ansteigenden Handel von gebrauchter Hardware kommen, die aufgrund der hohen Nachfrage im Preis steigen würde. Dies könnten sich wiederum manche Hersteller von Hardware, die nicht der TCG angeschlossen sind, zu nutze machen um für diesen Nischenmarkt TPM-freie Hardware zu produzieren. Insbesondere amerika-feindliche Staaten, könnten sich gegen die flächendeckende Einführung von TC auflehnen und ebenfalls versuchen mittels TPM-freier Hardware der ungewollten Kontrolle durch US-amerikanische Einrichtungen der Firmen zu entgehen.

7. Ausblick und Fazit

„Copyright and freedom of speech cannot coexist. One of them has to go."
(Ian Clarke, Gründer von Freenet)

Schaffen die hier vorgestellten TC-Systeme auf Basis von TPM wirklich eine sichere und vertrauenswürdigere IT-Verarbeitung?
Im Rahmen dieser Untersuchung können Zweifel daran erhoben werden. Die Ansätze, die bis jetzt im Bereich TC vorgestellt wurden, müssen sich alle der Kritik aussetzen, nicht dem Verbraucher mehr Sicherheit zu bieten, sondern die Firmen, insbesondere die Rechteverwerter, vor dem Kunden zu beschützen. Der Nutzen, der den Mitgliedern der TCG und den Vertretern von Rechten, insbesondere in den USA, entsteht, überwiegt bei weitem den Nutzen, der sich für den Anwender bietet. Die Nutzer werden mit den allgemeinen Aussagen geködert, dass ihre Computerapplikationen durch TC sicherer und vertrauenswürdiger ausgeführt werden. Es ist zweifelhaft, dass Malware durch die Einführung von TPM vollständig vernichtet werden kann. Durch die Aufteilung der Computersysteme in einen sicheren und einen unsicheren Bereich wird der Anwender gezwungen werden, Programme im sicheren Systemteil auszuführen, um die Gefahr durch Viren, Würmer und Trojaner einzudämmen. Computer werden nicht allein durch das Hinzufügen eines TPM und dem Austausch sonstiger Hardware sicherer. Ein Restrisiko bleibt bestehen und wird sich auch nicht beheben lassen. Dies vermag auch TC und TPM nicht zu ändern. Diese Systeme bauen auf Erkenntnissen auf, die bereits vor 20 Jahren zum Grundverständnis eines sicheren Computersystems gehörten. Die TCG hat von daher keine grundlegenden Neuerungen entwickelt, sondern lediglich altbekanntes versucht in die Tat umzusetzen.

Ob die TCG eine marktbeherrschende Stellung als Verband erreichen kann bleibt abzuwarten. Festgehalten werden kann jedoch, dass die Spezifikationen der TCG einen kompletten Austausch der Hardware beim Anwender erfordern würde und dies natürlich im Interesse der Verbandsmitglieder ist. Auch die darauf aufsetzende neue Software befindet sich bereits in der Entwicklung. Selbst wenn es von der TCG und ihren Mitgliedern bestritten wird, scheint TPM eher die Grundausrüstung für die Implementierung von DRM- und IRM-Systemen zu sein und weniger das Allheilmittel gegen Malware.

Es stellt sich hierbei die grundsätzliche Frage, ob es der Anwender selber ist, der dem Rechner Sicherheit attestieren sollte, oder ob es dritte Institutionen sein sollten, die mittels eines Hard- und Softwareansatzes bescheinigen, dass dieser Rechner nach deren Ansicht sicher ist. Daran schließt sich die Frage an, ob dieses Konzept nicht so umgestellt werden müsste, dass der Anwender an der Spitze der Sicherheitskette steht und nicht eine Gruppierung. Der Beantwortung dieser Frage bedarf es weiterer Erfahrungen mit TC. Es ist sicherlich nicht die TC-Technik, die einen Nachteil für die IT darstellt, sondern die Möglichkeit ihrer Anwendung bzw. ihres Missbrauchspotentiales durch Institutionen, die dieses System zur Erhaltung ihrer Macht oder ihrer monopolartigen Stellung ausnutzen könnten.

Sollte TPM und damit verbunden DRM- und IRM-Systeme flächendeckend etabliert werden, wirkt sich dies nicht nur auf die wirtschaftlichen Interessen dieser Firmen aus. Auch diejenigen Institutionen, die Einfluss auf dieses System ausüben können, haben dann eine erhebliche Macht über die gesamte Informationverteilung des 21. Jahrhunderts. Dies birgt die Gefahr einer Zensur durch Rechteinhaber, Firmen und Regierungseinrichtungen, deren Folgen nicht abzuschätzen wären. Es wäre damit zu rechnen, dass das Recht auf informationelle Selbstbestimmung und die Persönlichkeitsrechte der eigenen freien Meinungsbildung auf Basis von frei zugänglichen Informationen massiv beschnitten würde. Letztendlich würde es auch zu einem völligen Zusammenbruch der in den letzten Jahren entwickelten Netzkultur kommen. Daten würden mittels DRM- und IRM-Systemen überwacht und wären nicht mehr direkt erhältlich. Jeder Nutzungsvorgang würde von diesen Systemen aufgezeichnet und wäre abrufbar. Das Recht auf freie Meinungsäußerung könnte dadurch eingeschränkt werden, da nicht mehr über jedes Thema frei berichtet werden könnte, wenn dadurch Urheber- oder Copyrightrechte verletzt würden. Dies hätte auch erhebliche Auswirkungen auf die Wissenschaft und Forschung. Informationen würden sich dadurch verknappen und würden teurer werden.

Die Macht der Unterhaltungskonzerne würde stark ansteigen und zu einer Nivellierung der kulturellen Landschaft führen. Medienkonzerne könnten darüber entscheiden, welche Werke angeboten würden. Es ist fraglich, ob dann nicht nur noch aktuelle stark gefragte Massenware angeboten würde und Werke, für die sich nur einige Hundert Personen interessieren würden, vollständig vom Markt verschwinden, da deren Bereitstellung nicht rentabel wäre. Letztendlich würde dies eine Verdrängung von freier Software bedeuten, da die Gefahr besteht, dass diese Software nicht lizenziert würde. Dies würde auch das Ende des Linux-Betriebssystems bedeuten. Die Beseitigung dieses Betriebssystems wäre insbesondere für Microsoft ein großer Erfolg, da Linux die monopolartige Stellung Microsofts gefährdet. Open-Source-Betriebssysteme wie Linux gelten als besonders zuverlässig und sicher, ein Status, den Windows-Betriebssysteme bis jetzt noch nicht erreicht haben. Das gerade zum jetzigen Zeitpunkt, wo freie Software wie beispielsweise Linux in einigen süd- und mittelamerikanischen Schwellenländern, in fernöstlichen Staaten und auch in Deutschland als Alternative zu proprietärer Software diskutiert wird, eine derartiges System etabliert werden soll, kann nicht als Zufall gewertet werden und scheint der Verteidigung proprietärer Software zu dienen.[154]

Bei der Einführung der TPM-Systeme gibt es für die Hersteller zwei Möglichkeiten. Zum einen eine sofortige Umstellung auf dieses System. Die Bereitschaft zu diesem Wechsel soll durch neue Eigenschaften der Systeme geweckt werden. Zum anderen könnten die Firmen den Weg der Unterwanderung und Desinformation gehen und die TPM-Systeme die ersten Jahre deaktiviert ausliefern. Diese Maßnahme würde greifen, falls die erste Möglichkeit für den Verbraucher zu offensichtlich wäre. Selbst Personen, die die nötigen Informationen über TC besäßen, wären nach einigen Jahren gezwungen auf diese Systeme umzusteigen, da ihre alte Hard- und Software nach und nach von den aktuellen Produkten ersetzt werden müsste. Sollte dies noch durch die Legislative unterstützt werden, so wären auch kleinere Drittanbieter, die TPM-freie Hardware produzieren, nicht mehr vorstellbar. Es würde auch auf dieser Ebene zu einer Zwei-Klassen-Gesellschaft bei dem Einsatz der Hardware führen. Einerseits gäbe es die Anwender, die TC positiv gegenüber stehen oder ahnungslos diese neue Technik einsetzen, da sie über die aktuellste Hardware verfügen. Andererseits gäbe es die Personen, die TC ablehnen und daher mit veralteter Hardware arbeiten müssen, da diese TPM-frei sind. Zu dem Zeitpunkt, wo TPM-basierte Hardware den Bestand an alter Hardware übersteigt, könn-

[154] Ermert [2004, S. 44]

te sich auch die Option der freiwilligen Nutzung als ein leeres Versprechen erweisen, da dann der Einsatz von TPM aufgrund der Vormachtsstellung der TCG erzwungen werden könnte.

Würden alle hier aufgezeigten Möglichkeiten in dieser Form eintreten, würde dies in der Schaffung eines totalitären Systems enden. Damit dies nicht geschieht, ist es wichtig, den Anwender auf die Vorteile, aber auch die Gefahren hinzuweisen, die TC mit sich bringen kann. Insbesondere sollte an die Legislative appelliert werden, die es schlussendlich in der Hand hat, diese Entwicklung zu überwachen und wenn nötig die negativen Auswirkungen zu verhindern. Es muss daher überprüft werden, ob die Techniken im TC-Bereich, die zum jetzigen Zeitpunkt zur Verfügung stehen, wie beispielsweise in Europa die Smartcard-Technologie, nicht zur Absicherung der IT bereits ausreichen. Sollte dies verneint werden, ist zu klären, ob nicht ein TC-System auf der Basis von freier Software größere Akzeptanz erhalten würde. Weiterhin wird sich zeigen, ob es nicht notwendig ist, dass Daten in Zukunft nur noch mittels offener Dateiformate gespeichert werden, um zu verhindern, dass Werke durch proprietäre Dateiformate an deren Rechteinhaber gebunden werden.

Weiterhin bleibt anzumerken, dass die Diskussion um TC und TPM zum Teil sehr emotional abläuft und Behauptungen häufig ohne Begründung aufgestellt werden. Das beweist auch, wie sehr dieses Thema die Gemüter aller Seiten bewegt, da die Einschnitte, die dieses System mit sich bringen würde, erheblich wären. Dass die laute Kritik an diesem Vorhaben nicht zu ignorieren ist, zeigen die Änderungen und Auflockerungen der TCG TPM-Spezifikation. Diese Veränderungen führen, durch die Möglichkeit der Einführung eigener EK, zu dem Verlust des bisherigen Vertrauensystems, dass die TCG eigentlich schaffen wollte. Der von der TCG versprochene Sicherheitsstandard ist damit schon in dieser Version nicht mehr zu garantieren.