

Proseminar Software Disaster
Thema: Computervirenbekämpfung

Valentin Pletzer

13. November 2002

Inhaltsverzeichnis

1. Einleitung	Seite 3
2. Hauptteil	
a. Präventive Maßnahmen	Seite 4
b. Software-Zertifikate	Seite 4
c. Virensuche	
i. signaturgestützt	Seite 5
ii. heuristisch	Seite 6
d. TCPA/Palladium	Seite 6
e. Proof carrying code	Seite 7
3. Fazit	Seite 8
4. Quellenverzeichnis	Seite 9

1) Einleitung

Der Vortrag gibt einen Überblick über den aktuellen Stand der Technik im Bereich der Virenbekämpfung. Im Zuge der immer stärkeren Nutzung von Computersystemen spielt auch die Bekämpfung von bösartigen Programmen und Viren eine immer wichtigere Rolle.

Nach einem kurzen Überblick über die aktuelle Situation der Viren im Jahr 2002, speziell im Oktober 2002, geht es dann um die Möglichkeiten für die Bekämpfung von Viren.

Zuerst werden einige präventive Maßnahmen erläutert. Danach werden Software-Zertifikate erklärt und Vor- und Nachteile genauer betrachtet. Beim Thema Virensuchen werden dann zwei der gängigsten und bekanntesten Verfahren von so genannter Antiviren-Software oder auch Virentkillern erklärt. Es handelt sich dabei um die signatur-gestützte und die heuristische Suche nach Viren.

Danach gibt es einen Ausblick auf die Zukunft. Zuerst wird TCPA und Palladium vorgestellt und diskutiert, das nach den Wünschen von Microsoft zum neuen Sicherheitsstandard werden soll.

Als letztes wird das aktuell in der Forschung befindliche Konzept des „Proof Carrying Code“ vorgestellt und dessen Vor- und Nachteile aufgezeigt.

Zur Zeit sind nach Angaben verschiedener Hersteller von Antivirensoftware, wie zum Beispiel McAfee und Symantec, mehr 50.000 Viren bekannt. Allein 21 Stück sind im Oktober 2002 hinzugekommen. Zusätzlich werden Tag für Tag Viren aktiv, die mit einer so genannten Zeitbombe ausgestattet sind. Etwa 100 verschiedene Viren sind so geschrieben, dass sie im Oktober bis dahin inaktive Programmroutinen ausführen. Je nach Tag sind es zwischen 3 und 15 verschiedene Viren.

Allerdings wird von den Herstellern angegeben, dass nur etwa 1 bis 2 Prozent der bekannten Viren sich auch tatsächlich im Umlauf befindet. Alle anderen Viren sind Laborzüchtungen die entweder nie zum Einsatz gekommen sind oder erst gar nicht dafür gedacht sind. Vielmehr handelt sich dabei um Forschungsexemplare von Viren- und Antivirenautoren.

2.a) präventive Maßnahmen

Als eine der ersten Möglichkeiten der Virenbekämpfung sollte man eine Reihe von präventiven Maßnahmen in Betracht ziehen. Allein durch den richtigen Umgang mit der Software lässt sich bereits eine ganze Menge von Viren von vorne herein ausschließen.

Falls vorhanden, sollte man verfügbare Updates möglichst bald einspielen. Oft greifen Viren auf Lücken in Systemen zu, die durch ein älteres Update bereits behoben sind. Ein gutes Beispiel liefert hier auch wieder der I LOVE YOU-Virus, der die Möglichkeit der automatischen Skriptausführung ausgenutzt hat. Neuere Versionen der Microsoft Outlook-Reihe sind nicht mehr anfällig, da eine zusätzliche Abfrage das automatische Starten der Viren verhindert. Das gleiche kann auch mit Updates bei älteren Versionen erreicht werden.

Software die auf einem Rechner ausgeführt werden soll, sollte immer aus einer vertrauenswürdigen Quelle stammen. Möglichkeiten dies zu überprüfen werden nachher besprochen. Als vertrauenswürdige kann man auch Open Source Software betrachten. Diese hat den Vorteil das meist in Teams daran gearbeitet wird und so ein Missbrauch eher unwahrscheinlich ist. Außerdem kann man den ausgeführten Code vorher im Quelltext selbst überprüfen.

Grundsätzlich gilt, dass ein vorsichtiges Verhalten bereits eine Menge Schaden verhindert werden kann. Der I LOVE U-Virus konnte sich vor allem durch seine geschickt gewählte Betreffzeile besonders gut vermehren.

Diese präventiven Maßnahmen verlangen eine Menge Disziplin. Oft werden diese simplen aber wirkungsvollen Möglichkeiten auf Grund von Bequemlichkeiten vernachlässigt.

2. b) Software Zertifikate

Software Zertifikate sind eine einfache Methode um Manipulationen an Dateien zu erkennen. Man kann die Methode grob in drei Möglichkeiten zerlegen.

Erstens der Vergleich von Dateieigenschaften, wie etwa Größe, Erstelldatum, Dateiname oder Attribute. Vorteil ist in diesem Fall natürlich die einfache Anwendung. Jedoch lassen sich solche Eigenschaften ebenfalls sehr leicht manipulieren, so dass dies nur sehr ungenügend ist.

Etwas besser sind da schon so genannte Checksummen. Bekannte Verfahren sind etwa MD5 oder SHA1. Checksummen bieten eine sehr gute Möglichkeit Veränderungen an Daten zu erkennen. Eine Checksumme ist das Ergebnis einer Funktion die verschiedenste Faktoren von Daten berücksichtigt. Etwa die

Reihenfolge der enthaltenen Informationen genauso wie auch die Dateigröße. Nachteil dabei ist vor allem, dass die Verfahren bekannt sind und sich auch leicht Checksummen für veränderte Dateien erstellen lassen. Der Anwender müsste also sichergehen, dass die übermittelte Checksumme authentisch ist.

Zu diesem Zweck setzt man Digitale Signaturen ein. Der Absender benutzt ein kryptographisches Verfahren wie zum Beispiel RSA und verschlüsselt die Checksumme mit einem privaten Schlüssel und hängt die daraus resultierende Bitsequenz an. Die Sicherheit beruht darauf dass es bisher keine effizienten Verfahren zur Faktorisierung großer Zahlen gibt. Mit dem öffentlichen Schlüssel des Absenders kann der Empfänger nur prüfen aber keine eigene Signatur erstellen.

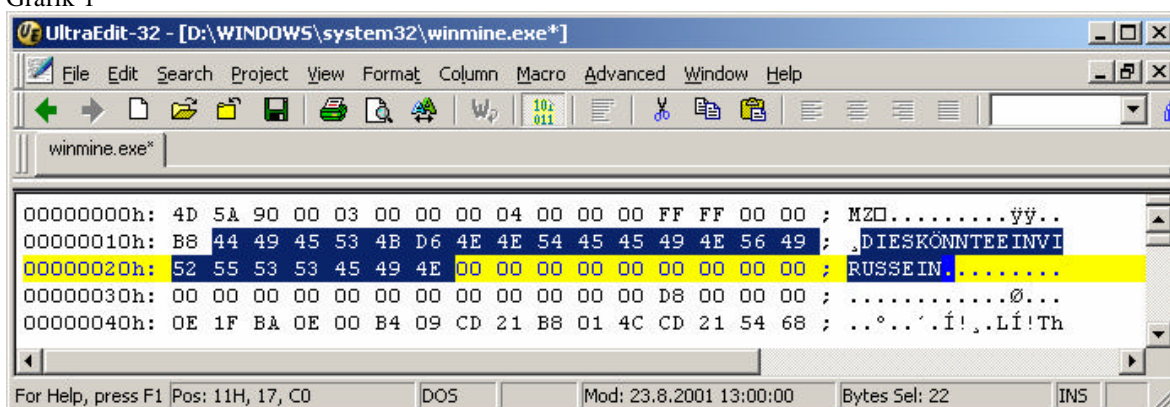
2. c) Virensuche

i. Signatur gestützte Virensuche

Moderne Virenspürprogramme verwenden noch immer eine alte, einfache aber oft noch sehr effektive Methode zum Erkennen von Viren. Da ein Virus immer auch einen Teil des Speichers (Festplatte, Diskette, Arbeitsspeicher...) belegen muss, kann man Viren aufspüren, indem man gezielt nach den Bitmustern ihres Maschinencodes sucht.

Der Programmspeicher wird dann nach solchen Mustern durchforstet und im Fall eines Treffers ein Alarm angezeigt oder eine entsprechende Gegenmaßnahme eingeleitet. Gegenmaßnahmen reichen vom einfachen löschen der Virendaten, bis hin zum löschen der ganzen befallenen Datei.

Grafik 1



Das große Problem dieser Suchmethode ist die Polymorphie. Schon seit längeren verwischen Viren ihre Muster durch das Verändern ihres Codes. Das reicht vom simplen umsordieren der Funktionen bis hin zur Verschlüsselung der

Daten. Ein Virenkiller hat dann mit der signatur-gestützten Suche nur noch dann eine Chance wenn er alle möglichen Formen kennt.

ii. heuristische Virensuche

Eine neuere Form der Virenerkennung ist die heuristische Suche. Dabei werden keine Datenmuster mehr gespeichert sondern das Verhalten.

Ein einfacher Virus versucht zum Beispiel möglichst viele Dateien auf einem Rechner zu infizieren indem er möglichst alle ausführbaren Dateien auf dem Rechner infiziert. Dazu muss der Virus eine Liste der ausführbaren Dateien anfertigen, die Dateien öffnen und den Virus-Code schreiben. Ein solches Verhalten kann dann bei auftreten als typisches Verhalten entlarvt werden. Großes Problem ist der Unsicherheitsfaktor. Zum einen würde in unserem Beispiel auch ein anderer Virenkiller als Virus erkannt werden, da dieser unter Umständen ebenfalls alle ausführbaren Dateien öffnet und bearbeitet.

Erschwerend kommt hinzu, dass auch die Programmierer von Viren diese Taktiken kennen und durch entsprechende Veränderungen am Viren-Code das Verhalten so ändern können, dass kein Alarm mehr ausgelöst wird.

2. d) TCPA / Palladium

TCPA

TCPA heisst „Trusted Computing Platform Alliance“ und soll den PC durch zusätzliche Hardware sicher machen.

TCPA schreibt vor, dass Motherboards künftig mit einem sogenannten Fritz-Chip ausgestattet werden sollen. Dieser Chip bietet die Möglichkeit fälschungssichere Checksummen nach dem SHA1-Verfahren schnell zu berechnen und dient dazu Software- und Hardwarekomponenten vor unlizensierten Veränderungen zu schützen. Erkennt der Chip eine Manipulation wird der Rechner abgeschaltet.

Der Chip arbeitet sobald der PC eingeschaltet wird. Als erstes wird das BIOS dann die CPU überprüft. Danach folgen weiter Komponenten wie zum Beispiel die Grafikkarte. Jeder Schritt wird mit einer SHA1-Prüfsumme festgehalten und gespeichert. Liegt eine Veränderung vor wird Alarm ausgelöst.

Jede neu eingebaute Hardware muss zertifiziert werden. Mittels einer Online verfügbaren Listen werden gesperrte Seriennummern und geprüfte Hardware mit dem Rechner abgeglichen. Nach dem Hardwarecheck wird dann der Inhalt der Festplatte auf dieselbe Weise überprüft. Wird das Betriebssystem als TCPA-konform angenommen so startet der PC.

Palladium

Microsoft möchte in kommende Betriebssysteme das Konzept Palladium integrieren, das die Ausführung böse Code verhindern soll. Palladium ist der Codename für das TCPA konforme Betriebssystem von Microsoft. Derzeit ist nicht besonders viel bekannt weshalb das Konzept hier nur grob umrissen wird.

Palladium setzt auf der TCPA-Hardware-Architektur auf, die von namhaften Chipherstellern wie Intel oder AMD für künftige PC Generationen vorgesehen ist. Ein vor Veränderungen sicherer Chip, der es dem Betriebssystem ermöglicht nicht authentifizierte Hard- und Software zu erkennen und bei Bedarf den Betrieb zu verweigern. Optional würde sich das System einfach selbst beenden um so einem Angriff zu entgehen.

Mögliches Anwendungsgebiet ist zum Beispiel die eindeutige Identifizierung des Anwenders. Der Anwender muss das System auf sich personalisieren lassen und kann von nun an eindeutig identifiziert werden. Im eigenen Interesse wird der Schlüssel nicht preisgegeben da sonst ein Missbrauch möglich wäre.

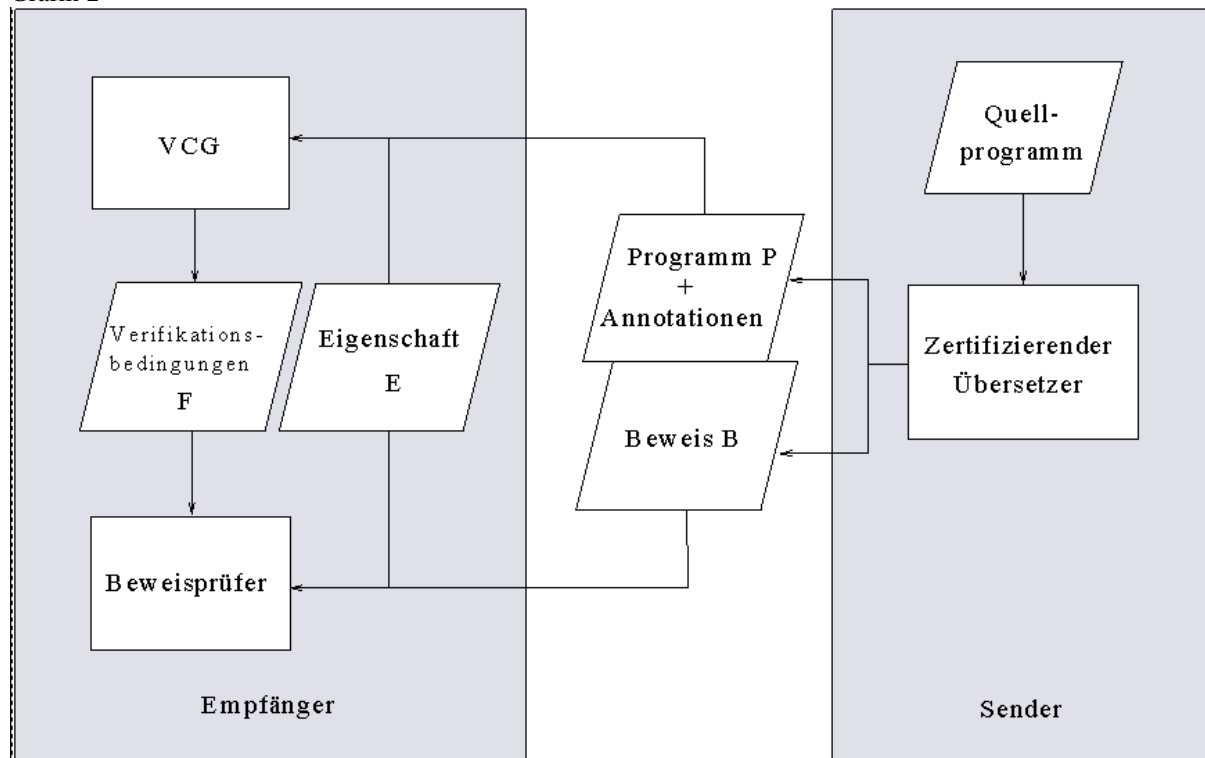
Großer Vorteil des Verfahrens ist die scheinbar absolute Sicherheit für den Anwender. Er muss keinerlei Kenntnisse vom System haben und sollte er auf die Zertifizierungsstelle vertrauen, kann er jede Software gefahrlos starten. Nachteil ist, dass bei fehlendem Vertrauen in die Zertifizierungsstelle der Rechner unbrauchbar wird und sollte die die Sicherheit des Zertifikat-Ausstellers kompromittiert werden so ist auch gleichzeitig jeder Rechner mit dem System gefährdet. Zudem zeigen System wie etwa die Xbox, die dieses System schon in ähnlicher Form benutzen, dass mit genügend Wissen auch der Chip auf jeden Rechner mit entsprechender Hardware-Kenntnis abgestellt werden kann.

2. e) Proof Carrying Code

Das vermutlich aktuellste Konzept, das Abhilfe gegen alle möglichen Variationen von böse Programmcode also Viren verspricht ist „Proof Carrying Code“. Die Idee dahinter ist, dass Programme Beweise von bestimmten Programmeigenschaften enthalten, die dann von einem Programm auf der Zielplattform überprüft werden können.

Ein logisch fundiertes System ist die Grundlage für das ganze Konzept. Nach der Entwicklung des Programmcodes muss der Programmierer Schritt für Schritt die einzelnen Programmabschnitte mit den Beweisen versehen die Eigenschaften wie etwa die Abwesenheit von Buffer Overflows garantieren. Ein solcher Beweis könnte sehr klein sein und außerdem sehr schnell zu prüfen.

Grafik 2



Größter Vorteil des Konzepts dürfte die große Unabhängigkeit von der Software-Quelle sein. Egal wer das Programm geschrieben hat und von wo man das Programm herunter lädt, der Beweis muss stimmen und kann auch nicht gefälscht werden.

Nachteil ist allerdings ein Mehraufwand bei der Entwicklung eines Programms. Neben dem Programmcode sind auch Beweise zu erstellen. Dies wird aber durch den Vorteil ausgeglichen, dass ein Anwender dem Hersteller nicht vertrauen muss. Dem Anwender reicht es wenn das Betriebssystem, den Beweis nachvollziehen kann und damit die Gefährlosigkeit garantiert bekommt. Damit ist der Anwender unabhängig von den Quellen und Zertifizierungsstellen.

3. Fazit

Abschließend kann man sagen, dass die Virenbekämpfung sich zwar schwierig gestaltet und auch viel Arbeit kostet aber sicherlich nicht unmöglich ist. Anwender müssen sich zurzeit noch auf die gegebenen Möglichkeiten einlassen und die Disziplin haben auch regelmäßig Updates der Anwendungen und der Antivirensoftware zu installieren. Bis neue Möglichkeiten wie etwa „Proof Carrying Code“ zum Einsatz kommen dauert es sicherlich noch einige Zeit und ob Knebel wie Palladium geplant sind, ist fraglich.

4. Quellenverzeichnis

- <http://www.mcafee.com/default.asp>
- <http://www.symantec.de>
- c't 2002 / Heft 22 Der versiegelte PC
- Working Material for the lectures of Georg Necula on Proof-Carrying Code