Proseminar
„Ethische Aspekte der Informationsverarbeitung“

Computerviren

WS 07/08 BTU Cottbus

Martin Noack

Inhaltsverzeichnis:

1. Was ist ein Virus

- 4 Typen: Viren, Trojanische Pferde, Würmer, Hintertüren (backdoors)

- *Viren:* Stück Code in einem host Programm, dupliziert sich, infiziert neue ausführbare Dateien eines Systems, braucht Wirt (Applikation) um agieren zu können, findet man meist nur noch in „Nischen“, können logische Bomben enthalten (Programmteil der absichtlich schädigend ist), Verbreitung hängt von Anwender ab (Tauschbörsen, Disketten, FTP-Server, USB-Stick, …), fast vollständig von Würmern verdrängt

- *Würmer:* brauchen kein host Programm zur Verbreitung, bedienen sich der Mittel die von Netzwerken bereitgestellt werden (Netzwerkdienste, Anwendungsprogr. die Netzwerkdienste nutzen, …), aktive Verbreitung, nutzen Sicherheitslücken und schwache Passwörter aus, versuchen meist sich im System zu verstecken und es so anzupassen das sie beim nächsten Start mit ausgeführt werden

- *Trojanische Pferde:* auch Trojaner genannt, Programme die sich als nützliche Anwendung tarnen, im Hintergrund ohne Wissen des Nutzers andere Funktionalitäten haben, dabei müssen diese nicht zwangsweise schädigend sein (z.B. verschicken von unsensiblen statistischen Daten an den Programmierer), Verbreitung durch Tauschbörsen, Free- / Shareware, …, über Wurm im E-Mail Anhang

- *Hintertüren (backdoors):* Teil eines Programms der es einem ermöglicht Zugang zu einer Anwendung oder einem Computer zu bekommen ohne die normalen Authentifizierungsmechanismen zu nutzen, oft durch Passwort geschützt, das nur dem Autor bekannt ist

2. Geschichte der Computerviren

- 1949, Theorie/These von sich selbst reproduzierenden Automaten von John von Neumann

- 70er Jahre, „core war“ von Bell AT&T Laboratories, Ziel war es innerhalb eines begrenzten Memorybereiches kleine Programme gegeneinander antreten zu lassen damit sie sich gegenseitig zerstören, Spielinteresse war wissenschaftlicher Natur

- 1980, Jürgen Kraus von der Universität Dortmund verfasste Diplomarbeit mit dem Titel *„Selbstreproduktion bei Programmen“*, Vergleich zwischen Programmen und biologischen Viren, sie verhalten sich ähnlich

- 1984, Fred Cohen veröffentlichte seine umstrittene Doktorarbeit, in der nicht nur Informationen über den ersten Virus von 1983 inklusive Quellcodes enthalten waren sondern auch über verschiedene andere experimentelle Viren berichtet wurde, er wies auf die Gefahren dieser Codes hin, neue Gelder für eine Erforschung von Gegenmitteln wurden ihm damals nicht genehmigt

- 1985, über Mailbox wurde Programm zur Aufarbeitung von Grafiken verteilt, dieser getarnte Trojaner löschte beim Start alle Dateien auf der Festplatte und zeigte Meldung "Arf, Arf, hab dich" auf dem Bildschirm an

- 1986, erster MS-DOS Virus kam in Umlauf, von 2 pakistanischen Geschäftsmännern programmiert die gebrannte Software verkauften,
  im Dezember stellte Ralf Burger vom deutschen Chaos Computer Club den ersten Virus vor, der sich über den Bootsektor von Disketten verbreitete

- 1987, Christmas Tree Virus legt innerhalb von 4 Tagen Großnetzwerk einer deutschen Universität lahm

- 1988, Jerusalem Virus löscht immer am Freitag den 13. alle *.com und *.exe Dateien, wurde vermutlich von Palästinensern programmiert und ist noch heute in 500 Varianten zu finden,
  im November legte "Morris" einige tausend Computersysteme in den USA lahm, darunter Rechner der NASA, Schaden wurde auf 100 Millionen Dollar geschätzt

- 1989, erster polymorphe Virus, erste Stealth-Viren, ersten Antivirenprogramme erscheinen

- 1990, Verband deutscher Virenliebhaber verbreitet das erste Virus Construktion Kit für DOS-Systeme

- im Laufe der 90er kommen Macroviren, erster polymorpher Windows Virus, Viren für fast alle Microsoft Office Anwendungen, erster Linux-Virus dazu

- 2000, LoveLetter lässt viele Mailserver in die Knie gehen, er verbreitet sich rasant, der ILoveyou-Virus setzt auf die Neugier der Menschen und verursacht ein enormes Medien Interesse

- ab 2002 werden Viren von Würmer nach und nach verdrängt, da sie höhere Verbreitungsgeschwindigkeit haben,
  erster Virus der Win32-Anwendungen und ELF-Dateien infizieren konnte!

- 2004, erster Virus für PocketPCs (Windows CE)

- 2005, erster Virus fürs Handy (Symbian OS)

- 2007, Viren für Taschenrechner entdeckt

3. Viren unter Linux

- bei Systemdateizerstörung & Lesen von vertraulichen Daten lassen sich zwei Fälle unterscheiden
  - wenn logische Bombe (Schadcode) unter *root* ausgeführt wird, hat der Schadcode gesamte Macht über das System, z.B. Löschen von Partitionen, eventuelle Gefahren für die Hardware (Löschen von CMOS, Änderungen in flash memory, zerstörerische Bewegungen auf Drucker-, Plotter-, Scannerköpfen, beschleunigte Bewegung beim Lesen von Festplattenköpfen, …)
  - wenn Schadcode unter normalem Benutzermodus ausgeführt wird kann er nicht mehr anrichten als der Benutzer selbst, also die Dateien vom Benutzer zerstören/ändern

- unter normalem Benutzermodus ist es aber möglich das System lahm zu legen durch Benutzen vieler Ressourcen, z.B. C Programm was jeden Eintrag aus Prozesstabelle benutzt (wenn keine Beschränkung der Anzahl der Prozesse für einen Benutzer existiert) und jede Verbindung verhindert, die versucht, es zu töten, oder Programm das den ganzen verfügbaren Speicher benutzt und in einer Schleife läuft, frisst die CPU Zyklen, ist sehr störend für andere Prozesse (bekommen nicht den Speicher den sie brauchen und beenden sich)

- es reicht ein paar wenige fork(), malloc() und connect() zu kombinieren um System und Netzwerkdienste stark zu belasten

- Viren existieren entgegen weitläufiger Meinung unter Linux, finden nur keinen Weg/Nährboden sich zu verbreiten außer auf Maschine selbst, aber auch nur die Dateien können infiziert werden, wofür der Benutzer Schreibrechte besitzt,
  gelangen auf Rechner durch korrumpierte Dateien

- Vielfalt an Assemblersprachen und Bibliotheken beschränkt Reichweite für vorkompilierten Code, heute stimmt das nicht mehr ganz

- Bsp.e für Viren unter Linux
  - *Winux*, enthält zwei verschiedene Codes, kann Windows wie auch ELF Dateien infizieren, jedoch nur auf der Partition wo er gespeichert wurde, kein Schadcode
  - *ZipWorm*, fügt „Troll“ Text in *.zip Dateien ein die er findet

- Schutz den Linux durch Benutzertrennung erreicht, wird durch Viren die von Windows aus auf Linuxpartitionen zugreifen umgangen (Problem dual- oder multiboot Systeme), allgemeiner Schutz des Ganzen hängt von schwächster Komponente ab

- Quellcode einer Applikation (hier Trojaner) zu haben ist keine Sicherheit, Schadcode kann z.B. im *configure* Script (das, was während *./configure; make* aufgerufen wird) versteckt sein, oder Quellcode ist sauber aber Schadcode ist im *makefile* versteckt, welcher sich selbst beim letzten *make install* aktivieren kann (was normalerweise unter *root* gemacht wird!!)

- durch den frei zugänglichen Quellcode ist es „sehr einfach“ Verwundbarkeiten aufzudecken (buffer overflow, …)

- Bsp.e für Würmer unter Linux
  - *Lion*, installiert backdoor & root-kit, schickt Systeminformationen an E-Mail Adresse in China
  - *Adore (Red Worm)*, installiert backdoor, schickt Informationen an E-Mail Adresse in die USA und China, installiert modifizierte *ps* Version um seine Prozesse zu verstecken

4. Ausbreitung von biologischen Viren / Computerviren / Marketingviren

- ***biologischer Virus:*** am besten erforscht, benötigt Kontakt/Nähe um übertragen zu werden, oder indirekt über biologische Waffen, vorbelastetes Tierfutter, mutiert oft, Ursprung zu bestimmen ist schwer, bei hoher Verbreitung schwächt er die betroffene Population durch Krankheit und dem Wunsch der Gesunden kontaminierte Gebiete zu verlassen, Bsp.e für BV
  - *Geschlechtskrankheiten*, HIV, Syphilis, …
  - *Grippeviren*, Vogelgrippe, …

- ***Marketingvirus:*** nutzt existierende soziale Netzwerke aus um Nachrichten epidemisch zu verbreiten, es wird auf die Mund zu Mund Propaganda gesetzt, Jesus sagte schon damals sinngemäß: „Geht bei Gott und verkündet der Welt das Evangelium“, MV wird von vielen nicht als schlecht angesehen (neuste Informationen, Gefühl trendy zu sein, …) im Gegensatz zu CV & BV,
  Effekt (positiv/negativ) schwer zu kontrollieren, durch persönlichere Übertragung effizienter als Werbung über Massenmedien, Internet hat seine eigenen Formen des viralen Marketings hervorgebracht, Petitionen, Gerüchte & lustige Geschichten, …, Bsp.e für MV
  - *Hotmail*, an jede Free-Mail wurde „Get your FREE download of MSN Explorer at http://explorer.msn.com“ angehangen, zwei Monate nach Launch 100.000 registrierte User
  - *Bionade*, alkoholfreies Erfrischungsgetränk, gab es erst in Hamburg dann Schritt für Schritt in ganz Deutschland

- *Moorhuhn-Jagd,* eigentlich von Johnnie Walker initiiert
- *Napster, Skype, StudiVz, Blair Witch Project, ...*

- ***Verbreitung:*** betrachten zunächst zwei gegensätzliche Netzstrukturen/Archetypen, *densely knit* und *ramified*

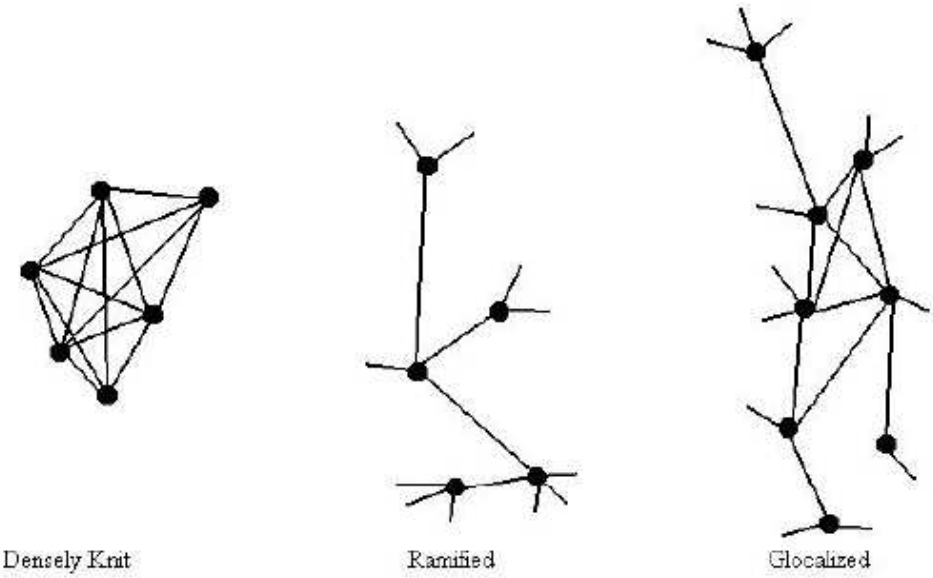

Figure 1: Three Models of Network Structure.

- *densely knit groups,* die meisten Mitglieder kennen sich, haben oft Kontakt miteinander aber mit Außenstehenden nicht, Virus kann sich schnell ausbreiten durch Synergieeffekte, solche Gruppen entstehen durch z.B. Homophilie (gleiches gesellt sich gern zu gleichem), also gleiche Geschmäcker, sexuelle Neigungen, ähnliche Denkweisen, sozialer Status, …, das erhöht die Wahrscheinlichkeit vom selben Virus befallen zu werden, Bsp.e sind
  - HIV, in den späten 70er frühen 80er Jahren, Schwulenszene war eine solche Gruppe, häufiger ungeschützter sexueller Kontakt mit wechselnden Partner aus der selben Gruppe, durch Überlappungen breitete sich der Virus schnell aus

    - Moni, Ulf & Lutz sitzen an unterschiedlichen Teilen einer Forschungsarbeit, wenn Moni's Rechner infiziert ist und sie Ulf eine infizierte Datei schickt, dann ist die Wahrscheinlichkeit doppelt so hoch das Lutz auch den Virus bekommt
    - „SirCam" Wurm verschickte sich selber an alle Adressen aus dem Adressbuch des Wirts, dadurch wurden dicht gestrickte Gruppen sehr schnell infiziert
    - PayPal, Käufer und Verkäufer brauchen Account um Transaktion durchführen zu können, wenn auch nur wenige einer Gruppe dieses System nutzen wird es sich in dieser ausbreiten, der Einfachheit halber
    - durch Telefon und Internet ist es sehr einfach geworden neue Nachrichten schnell zu verbreiten

- *ramified networks,* nicht das gesamte Netzwerk ist bei Befall betroffen so wie bei densely knit groups, verbreiten sich über eine heterogenere größere Population, Mitglieder solcher Netzwerke sind meist in mehreren densely knit groups vertreten mit meist losen Beziehungen zu ihren Mitgliedern, nehmen Schlüsselstellung bei Verbreitung von Viren ein, transportieren Virus in neue Gruppen/Milieus, Bsp.e sind
    - HIV, Vermittler waren da die Männer sie außerhalb ihrer Gruppe Sex hatten, infizierten so Frauen oder andere Schwulengruppen, was zu einer größeren Verbreitung führte
    - aktuelleres Bsp. ist Epidemie von Syphilis in Baltimore Mitte der 90er, begann in den weniger gut situierten Vierteln der Stadt, bis durch sexuellen Kontakt einiger weniger mit den anderen Bewohnern aus besseren sozialen Schichten die „gesamte Stadt" den Virus hatte

  - angenommen ein Vermittler ist in zwei dicht gestrickten Gruppen präsent, die eine hat 6 die andere 10 Mitglieder, wenn er den Virus nun einmal aus der 6er Gruppe bekommt so bekommt er ihn selbst 45 mal aus der 10er Gruppe zurückgesandt, damit sind Mitglieder von ramified networks einer Vielzahl an verschiedenen Viren ausgesetzt, mehr als Mitglieder die sich nur in einer Gruppe bewegen
  - virale Werbebotschaften werden gezielt über Meinungsmacher verbreitet welche meist in mehreren Gruppen aktiv sind

- *glocalization,* kommt der Realität am nächsten, Wortkreation aus global & local

5. Fazit der Autoren

- freie Software nicht sicher vor Viren, Würmern und Co
- wichtig sich anzugewöhnen seine Software auf dem neusten Stand zu halten um entdeckte Lücken zu schließen
- Programme nur von vertrauenswürdigen Quellen beziehen
- Hauptgefahren für Linuxsysteme der Zukunft sind Office Anwendungen – *blind macros* und multi-Plattform Viren
- Forderung nach leistungsstarken Virenscannern für die Linuxwelt

---

- obwohl die 3 Formen von Viren unterschiedlich sind so ist ihre Verbreitung über Netzwerke doch sehr ähnlich
- in der Realität hat man einen Mix aus beiden Archetypen, genannt *glocalization* (global & local)
- Viren nutzen verzweigte Netzwerke um Fuß zu fassen, um sich dann über enge/dichte Strukturen ausbreiten zu können

6. Quellen

- A plague of viruses: Biological, computer and marketing.
  Jeffrey Boase and Barry Wellman
  http://www.chass.utoronto.ca/~wellman/publications/viruspaper/...
  …version.PDF
  03.04.06

- Viren: Sie gehen uns alle an.
  Christophe Blaess
  http://www.tldp.org/linuxfocus/Deutsch/Archives/lf-2002_...
  …09-0255.pdf
  17.10.07

- http://www1.ku-eichstaett.de/urz/inkuerze/2_05/it-sicherheit.html
  04.01.08

- http://www.trojaner-info.de/viren/virenwas.shtml
  04.01.08

- http://de.wikipedia.org/wiki/Computervirus
  04.01.08

- http://home.intekom.com/neumann/viren.html
  04.01.08

- http://www.panda-software.de/pandawebsite/infos/geschichte.htm
  04.01.08