Das OpenAntivirus Projekt

http://www.openantivirus.org/

Kurt Huwig <kurt@iku-netz.de>

iKu Netzwerklösungen

http://www.iku-netz.de/

Aufbau

- Motivation
- Bestandteile
- Status / Technik / Demonstration
- Zukunft

iKu
Netzwerklösungen
http://www.iku-netz.de/

Warum?

- Linux Viren werden zunehmen
  - XML Virus befällt Mozilla 0.9.8
- hoher wirtschaftlicher Schaden durch Viren
  - > 3 Milliarden € Schaden alleine durch CodeRed und Nimda (Quelle: Computer Economics)

➔ Viren sollten so gut es geht bekämpft werden

iKu Netzwerklösungen
http://www.iku-netz.de/

Das Problem

- hohe Lizenzkosten kommerzieller Virenscanner
  - 10-20 € pro Nutzer und Jahr
- viele können sich das nicht leisten
  - Universitäten, Schulen
  - kleine Unternehmen

Die Folge

- Es werden Systeme infiziert mit
  - guter Internetanbindung
  - oftmals schlechter Wartung
  - wenig Sicherheitsbewusstsein

➔ rasante Ausbreitung von Viren

Können wir es schaffen?

- z.Zt. existieren > 60.000 Viren
- sehr wenige Viren sind wirklich im Umlauf
- 2001: < 10 unterschiedliche Viren auf einem Mailserver gefunden
- Erkennen dieser Viren ist machbar

Freie Lizenz

- GNU Public License (GPL)
- Copyright von Dritten muss auf das Projekt übertragen werden

iKu Netzwerklösungen
http://www.iku-netz.de/

Kommerzielle Lizenz

- Lizenzen für Closed Source Projekte können gekauft werden
- Einnahmen dienen der Weiterentwicklung

➔ Virenschutz in vielen Produkten

➔ wer nicht offen sein will, muss das Projekt finanziell unterstützen

iKu Netzwerklösungen
http://www.iku-netz.de/

Die Bestandteile

- PatternFinder (Java)
  - Virensignaturen bestimmen
- ScannerDaemon (Java)
  - Virenscan-Dienst
- VirusHammer (Java)
  - eigenständiger Virenscanner mit GUI
- Samba-vscan (C)
  - Zugriffsscan für Samba
- Squid-vscan (C)
  - Zugriffsscan für Squid

Projektstatus

- etwa 1.300 Viren werden erkannt
- seit 4 Monaten auf einem Mailserver aktiv
  - Integration in AMaViS
  - parallel mit einem kommerziellen Scanner
  - alle aktuellen Viren werden erkannt
  - ➔ Virenschutz für Mailserver ist praktikabel
- VirusHammer ist benutzbar
- Squid-vscan ist z.Zt. Proof-of-concept
  - noch nicht für Produktiveinsatz geeignet
- Samba-vscan ist benutzbar
  - läuft auf einigen Servern

Warum Java?

- plattformunabhängig
  - einziger Scanner für AS/400 PPC
- keine Buffer Overflows
- schnell

iKu
Netzwerklösungen
http://www.iku-netz.de/

PatternFinder: das Problem

- Virenscanner suchen nach charakteristischen Bestandteilen von Viren (Signaturen)
  - sind nicht frei verfügbar
  - Erstellung erfordert Analyse des Virus

iKu Netzwerklösungen
http://www.iku-netz.de/

PatternFinder: die Lösung

- Voraussetzung
  - Virus
  - (kommerzieller) Virenscanner, der ihn erkennt
- Virus wird systematisch überschrieben
  - Virenscanner wird gefragt, ob der Virus noch vorhanden ist
    - wenn ja: weiter überschreiben
    - wenn nein: diese Stelle nicht überschreiben

iKu Netzwerklösungen
http://www.iku-netz.de/

PatternFinder: das Ergebnis

- Gerüst des Virus, das der Virenscanner erkennt
- vereinfachte Analyse dieses Gerüstes
- evtl. direkte Verwendung im Scanner
- ~ 1.300 Signaturen sind bekannt

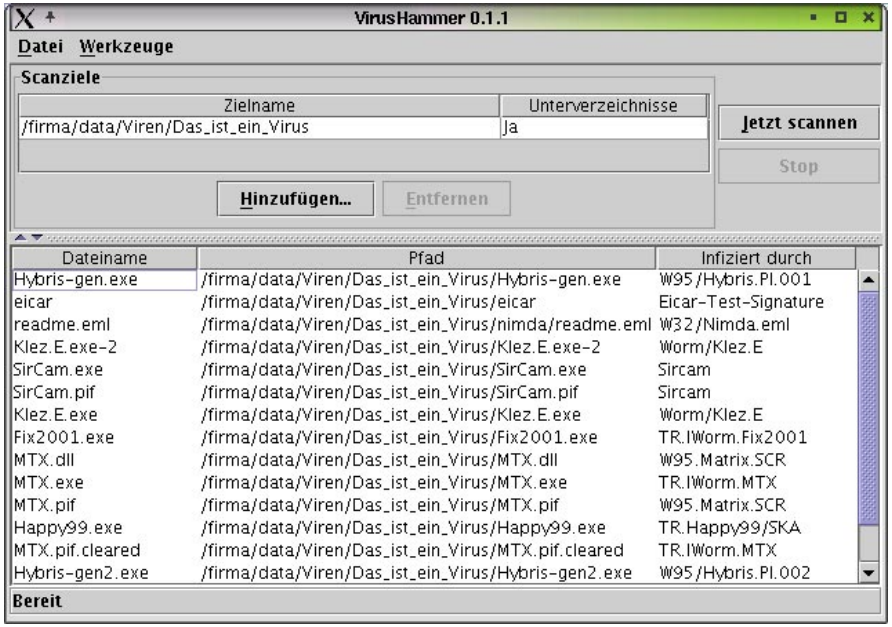
PatternFinder: Beschleunigung

- Starten eines Virenscanners braucht Zeit
- mehrere Kopien des Virus werden unabhängig voneinander gelöscht
- alle werden bei einem Start geprüft

iKu
Netzwerklösungen
http://www.iku-netz.de/

VirusHammer

- einfache Verwendung



iKu Netzwerklösungen
http://www.iku-netz.de/

VirusHammer

- internationalisiert
- bereits lokalisiert auf
  - Englisch, Deutsch, Französisch, Italienisch
- geplant
  - Integration von PatternFinder
  - besserer Fortschrittsanzeiger
  - Angabe von DOS-Laufwerksbuchstaben
  - JavaWebStart: Scannen ohne Installation

iKu Netzwerklösungen
http://www.iku-netz.de/

Squid-vscan

- verwendet Squid-Filter von Olaf Titz
  - http://sites.inka.de/sites/bigred/devel/squid-filter.html
- benötigt laufenden ScannerDaemon
- Problem: Meldung eines Virus
  - HTTP-Header sind bereits versendet
  - Übertragung lässt sich nur abbrechen
  - Umleitung auf eine Fehlerseite ist nicht möglich
- momentan keine Unterstützung für ZIP etc.
- andere Scanner lassen sich einbauen

Samba-vscan

- Projekt von Rainer Link
- Realisierung über Samba Virtual Filesystem
  - Patch für Samba 2.2.0 - 2.2.3a
  - Samba 3.0 benötigt keinen Patch
- Scannen aller Dateien vor dem Lesen
  - Zugriff wird bei Infektion verweigert
- Unterstützt mehrere Scanner über C-API
  - OAV ScannerDaemon
  - Sophos
  - Trend Micro
  - Kaspersky
  - Symantec

iKu Netzwerklösungen
http://www.iku-netz.de/

ScannerDaemon

- Starten des Scanners braucht Zeit
  - Duron 800MHz: 4s
- als Dienst entfällt das Starten
- `echo "SCAN /home/kurt" | netcat localhost 8127`
- Antwort:
  - OK
  - FOUND: <Virusname>
- Integration in
  - AMaViS
  - MIMEDefang
  - OdeiaVir
  - Samba/Squid-vscan

iKu Netzwerklösungen
http://www.iku-netz.de/

ScannerDaemon: Aufbau

- Aufteilung in
  - Filter
  - Scanner
  - Finder
- Filter
  - Vorverarbeitung von Dateien
  - Extrahierung von Programmdaten
- Scanner
  - Weiterleitung der Daten an die Finder
- Finder
  - Suche nach Viren

iKu Netzwerklösungen
http://www.iku-netz.de/

ScannerDaemon: Finder

- erhält Puffer mit
  - Präfix
  - Datenblock
  - Postfix
- Finder kann auf mindestens +/- 4kB zugreifen

Scan-Technik: Stringsuche

- viele (binäre) Strings müssen erkannt werden
  - auch für polymorphe oder verschlüsselte Viren
- Aho/Corasick arbeitet unabhängig von der Zahl der zu suchenden Strings
  - http://www-sr.informatik.uni-tuebingen.de/~buehler/AC/AC.html

Aho/Corasick Stringsuche

- erstellt einen Baum zur Erkennung
- besonderes Merkmal: Failure Function
  - bei Nichterkennung wird in einen anderen Teil des Baumes gesprungen
  - jedes Zeichen muss nur einmal in O(1) verarbeitet werden
- Beispiel
  - Suchstrings: baumhaus, auffahrt
  - Text: bauffahrt
  - Erkennung: b - a - u - f (passt nicht)
  - Sprung nach: a - u - f

Modifizierter Aho/Corasick

- Knoten im Baum verbrauchen viel Speicher
- unwahrscheinlich, dass viele Pattern lange identische Präfixe haben
- maximale Tiefe wurde auf 3 begrenzt
- danach lineare Suche

Aho/Corasick mit Tiefe 3

- Stand 06.03.2002:
  - 2.072 Knoten (inkl. Wurzel)
  - 200 Knoten mit Tiefe 1
    - Trefferwahrscheinlichkeit: 200/256 = 78%
  - 855 Knoten mit Tiefe 2
    - Trefferwahrscheinlichkeit: 855/65.536 = 1,3%
  - 1.016 Knoten mit Tiefe 3
    - Trefferwahrscheinlichkeit: 1.016/16.777.216 = 0,006%
    - 1kB: 6%, 32kB: 86%
  - Praxis (Windows-EXE): Ein Treffer alle 74 Byte
- Duron 800MHz: 10MB/Sekunde

Aho/Corasick mit Tiefe 4

- 3178 Nodes (+53%)
- 1 Treffer alle 153 Byte
- Duron 800MHz: 12MB/Sekunde (+20%)

iKu
Netzwerklösungen
http://www.iku-netz.de/

Aho/Corasick: Fazit

- ausreichend schnell für Internetverbindungen
  - E-Mail
  - Proxy
- Programmcode ist noch nicht optimiert
- optimierte Simulation ergab > 100MB/Sekunde

iKu Netzwerklösungen
http://www.iku-netz.de/

Zukunft

- Viren von den Erschaffern
  - eigenes Virenanalyseteam
  - Sourcer
  - Virenreportpolitik
- Scanner
  - Erkennung des Dateityps
  - Heuristiken
  - MS-Office Dateien
  - signiertes Dateiformat
  - Scannen von Archiven (tar.gz, ZIP, ...)

iKu
Netzwerklösungen
http://www.iku-netz.de/

Zukunft

- Squid-vscan
  - Squid v2.[456]
  - Integration weiterer Virenscanner
- VirusHammer
  - mehr Sprachen
  - bessere Fortschrittsanzeige
  - Laufwerksbuchstaben auswählbar
- Samba-vscan
  - Scan beim Schreiben
  - Quarantäne
  - Auto-clean

iKu Netzwerklösungen
http://www.iku-netz.de/

Zukunft

- Beta Tester
- geplant
  - Linux Kernelmodul
- Wohin mit Viren?
  - Mail an <kurt@iku-netz.de>

iKu Netzwerklösungen
http://www.iku-netz.de/

Fragen?

- http://www.openantivirus.org/
- http://www.iku-netz.de/
- Kurt Huwig <kurt@iku-netz.de>

iKu Netzwerklösungen
http://www.iku-netz.de/