Neue Werkzeuge gegen PC-Viren

Bernd Lehle / Oliver Reutter

Oft wurden Witze ü ber unbedarfte Benutzer gemacht, denen man glaubhaft versichern konnte, daß sie mit Computerviren infizierte Disketten oder Festplatten nicht mehr berü hren sollen, da

sonst Ansteckungsgefahr bestehe und Gedächtnisverlust drohe. Kürzlich veröffentlichte Arbeiten [1], [2] vom San Diego National Cancer Research Institute SDNCRC (San Diego / USA) zeigen aber, daß zumindest bei der Bekämpfung von biologischen und Computerviren die Disziplinen Informatik und Medizin durchaus voneinander lernen können.

Biologische und Computerviren sind durch die Unterschiede der zugrundeliegenden physikalischen und biochemischen Phänomene natürlich nicht vergleichbar. Trotzdem gibt es Ähnlichkeiten im Verhalten und damit auch in der Bekämpfung, wodurch die Computerviren auch zu ihrem Namen kamen. Wenn auch die Technik der Bekämpfung dieser beiden Virenspezies immer unterschiedlich bleiben wird, so kann man doch versuchen, die zugrundeliegenden Strategien zu übertragen.

Nachdem ihr Desktop-Rechner zum wiederholten Male auf einfache Weise von Computerviren befreit wurde, wünschte sich die Medizinerin Dr. Amanda Sniffles aus dem Virology Department des SDNCRC, daß es für biologische Viren auch eine so einfache und sichere Methode gäbe. Von der anderen Seite betrachtete das Problem der Informatiker Dr. Jacob Solomon vom System Support Department, der nach einer erfolgreichen Impfung gegen Masern und Windpocken sich eine solche aktive Immunisierung gegen Computerviren wünschte.

Der Zufall brachte die beiden Forscher vor vier Jahren zusammen und nun konnten sie das Ergebnis der gemeinsamen Arbeit präsentieren. Es handelt sich dabei um eine Schnittstelle zwischen einem biologischen und einem Computersystem. Auf beiden Seiten sind die Kontrahenten (Viren und Immunsystem) in ihrer jeweiligen physikalischen Welt vorhanden und folgen ihren Gesetzen. Das Neue an dieser Schnittstelle ist nun die Tatsache, daß Methoden und Strategien der Virenbekämpfung, die als Meta-Information nicht an physikalische Gegebenheiten gebunden sind, ausgetauscht werden können.

So bestanden die ersten Versuche darin, die wirksamsten Werkzeuge des jeweiligen Systems für das Gegenüber verfügbar zu machen, sie quasi zu portieren. Der erste Erfolg war die Implementierung der unspezifizierten Immunantwort, die aus dem Organismus auf den Computer übertragen wurde. Wichtig ist dabei die Fähigkeit des Körpers, schnell und flexibel auf Erreger reagieren zu können, die er vorher nicht kannte.

Dazu wurde ein Hausschwein mit einem seltenen Stamm des Epstein-Barr-Virus infiziert und für die Dauer des Versuches mit einem Teil seines Blutkreislaufes an die Schnittstelle angeschlossen. Die im Blut des Schweines ablaufende Immunreaktion gegen den ihm unbekannten Erreger wurde durch entsprechende Sensoren in der Schnittstelle einige Tage lang beobachtet, bis das Expertensystem im Computer die zugrundeliegende Strategie hinreichend analysiert hatte und eine erste Version zur Abwehr von Computerviren implementiert werden konnte. Bestehenden Virenprogrammen hat diese Software voraus, daß sie auf eine ständig zu erneuernde Datenbasis der bekannten Viren verzichten kann und daher die Probleme mit ständig veralteten Daten nicht auftreten.

So wie ein biologischer Organismus jeden beliebigen Fremdkörper als solchen erkennen und bekämpfen kann, ohne ihn vorher kennen zu müssen, kann das entstandene Programm jede virusartige Fremdsoftware im Rechner sofort erkennen und beseitigen. Wiederholt sich der Befall oder wird er akut, kann das Programm flexibel durch Bildung von Datenbeständen, in etwa entsprechend den T-Helferzellen im Immunsystem, und massiv parallelem Einsatz kleiner Code-Pakete, analog den monoklonalen Antikörpern, schnell und zuverlässig reagieren. Die Portierung von Makrophagen zum Einsatz gegen Makroviren steht kurz vor dem Abschluß.

In der umgekehrten Richtung bestand hauptsächlich der Wunsch nach Portierung der Mö glichkeit, Viren komplett und schnell zu entfernen, um lange Rekonvaleszenzen oder Komplikationen durch starken Virenbefall zu vermeiden. Ein Durchbruch im Kampf gegen viele Viruskrankheiten wären die unmittelbare Folge. Und in der Tat konnte die Schnittstelle beweisen, daß der Transfer von Methoden und Strategien auch in der Ge-genrichtung funktionierte. Die Datenbank eines führenden Herstellers für Antiviren-Software, konnte in großen Teilen in Form von Enzymen synthetisiert werden, die durch den

Antiviren-Code gesteuert wurde. Nach Katalogisierung der Enzymstruktur konnte für die meisten der bekannten biologischen Viren ein Serum isoliert werden, das ähnlich schnell und zuverlässig funktioniert wie Antiviren-Software.

Probleme machen momentan hauptsächlich die Retroviren, zu denen auch das AIDS-Virus gehört. Der Einsatz rekursiver Antiviren-Software scheint aber einen vielversprechenden Ansatz darzustellen, der in einigen Tests schon gute Ergebnisse geliefert hat. Auf die genaue Funktion der Schnittstelle befragt, gaben sich die Forscher recht offen und bekräftigten die verwendeten Verfahren so schnell wie möglich offenzulegen, um eine möglichst breite Anwendung zu ermöglichen. Die verwendeten Sensoren seien heutzutage Stand der Technik, ebenso die Enzymsynthese-Baugruppe. Die Anschlüsse für den Blutkreislauf müssen bis zur endgültigen Freigabe noch ausgiebiger am menschlichen Körper getestet werden, um Infektionen durch Fehlbedienung vermeiden zu können. Verhandlungen mit einem großen Hersteller von Medizintechnik und den wichtigsten Herstellern von Antiviren-Software stehen kurz vor dem Abschluß. Die Auslieferung tragbarer Geräte für Kliniken, die im Preis mit anderer medizinischer Standard-Hardware vergleichbar sein sollen, wurde für Herbst 1997 in Aussicht gestellt.

Die Reaktionen in der Computerindustrie waren unterschiedlich. Sun Microsystems arbeitet fieberhaft an der Portierung auf Java und kündigte die flächendeckende Versorgung von Apotheken mit Netzwerk-Computern an. So könne über einen Server, der über die Bio-Schnittstelle an eine Schafherde angeschlossen ist, tausenden von Endbenutzern Virenschutz geliefert werden. Der Microsoft-Konzern zog die Ankündigung eines großzügigen Sponsorings zurück, nachdem das Programm mehrfach das Betriebssystem Windows 95 als Virenbefall erkannte und in einer Art allergischem Schock beseitigte.

Literatur

[1] Solomon, J., Sniffles, A.: Advances in interdisciplinary virology, Journal of Medical Technology, Vol. 5, pp. 145-163, 1997

[2] Solomon, J., Sniffles, A.: A bio-computer interface to transfer anti-viral strategies, IEEE Journal, Letters to the Editor 73, 167-180, 1997

[3] Pschyrembel, W.: Klinisches Wörterbuch, Walter de Gruyter, 1982

Bernd Lehle, NA-5531
E-Mail: lehle@rus.uni-stuttgart.de

Oliver Reutter, NA-4513
E-Mail: Oliver.Reutter@rus.uni-stuttgart.de

P.S.: Eigentlich sollte dieser Artikel in der April-Ausgabe erscheinen. Die Plazierung in dieser Ausgabe ist rein technischer Natur.