

Die Alumni der Informatik Dortmund e.V.
Ein Netzwerk der Chancen

- Sie sind Ehemalige(r) des Fachbereichs Informatik?
- Sie sind dem Fachbereich freundschaftlich verbunden?
- Sie möchten Kontakte halten oder wieder aufnehmen?
- Sie möchten sich am Informatik-Netzwerk beteiligen?
- Sie möchten den Fachbereich unterstützen?

Die Alumni der Informatik Dortmund

- helfen den Ehemaligen, in Kontakt zu treten und zu bleiben,
- erleichtern Kooperationen mit dem Fachbereich,
- bieten ein Netzwerk gegenseitiger Unterstützung
- fördern den Fachbereich.

Nutzen Sie die Chancen!
Werden Sie Mitglied bei den Alumni!

Begrüßung
Roland Bracht
1. Vorsitzender 26. Oktober 2007, ab 15 Uhr

Grußwort an den DAT 2007
von **Prof. Dr. Volker Claus**, *Universität Stuttgart*
Betreuer Diplomarbeit Jürgen Kraus

**Selbstreproduktion bei Programmen 1980 -
von einer Idee zum Virus**
Jürgen Kraus, *Autor der weltweit ersten wissenschaftlichen
Arbeit über Computerviren, Absolvent Fachbereich Informatik 1980*

Back to the Future:
From Dortmund to present and future malware challenges
Prof. Dr. Daniel J. Bilar
Wellesley College, Massachusetts, USA

**Von Michelangelo bis MPack -
eine kurze Geschichte verbreiteter Computer-Schädlinge**
Frank W. Felzmann
BSI - Bundesamt für Sicherheit in der Informationstechnik, Bonn

Vorträge

Wir bedanken uns herzlich für die freundliche Unterstützung bei



Alumni der Informatik Dortmund e.V.
<http://www.alumni-informatik-dortmund.de>

Dortmunder Alumni-Tag 2007

26. Oktober 2007

DAT 2007

**Von der Selbstreproduktion zur
polymorphen Bedrohung**

**Warum die Geschichte der Computerviren
neu geschrieben wird und
welche Rolle Dortmund dabei spielt**

Prof. Dr. Volker Claus
Universität Stuttgart
Betreuer Diplomarbeit Jürgen Kraus



Grußwort an den DAT 2007 aus der Ferne:

Schon in den 1960er Jahre wurden Maschinenprogramme geschrieben, die ihren eigenen Text ausgeben konnten. Dies wurde kurz darauf auf Programmiersprachen wie BASIC, FORTRAN, PASCAL usw. übertragen und es gab viele Schüler, die damals relativ kurze Programme schrieben, die ihren eigenen Programmtext ausdrückten. Die Existenz solcher Programme nennt man 'Selbstreproduktion'.

Diese Programme waren für mich immer recht faszinierend. Ich formulierte es wie folgt: "Fasst man eine Datenverarbeitungsanlage in futuristischer Abstraktion als eine künstliche Welt auf, so kann man nach lebensähnlichen Vorgängen hierin fragen. Programme könnten die Rolle von einfachen Lebewesen spielen, sofern sie gewisse, in Analogie zur Biologie zu definierende Eigenschaften (z.B. Stoffwechsel, Reproduktion, Mutation) besitzen."



1978/79 hielt ich die Vorlesung "Rekursive Funktionen" an der Universität Dortmund. Hier wurde neben der Universalität von Funktionen auch die Frage angesprochen, ob gewisse Funktionenklassen gegen Selbstreproduktion abgeschlossen sind. Als Anwendung hatte ich hervorgehoben, dass man Computer in Zukunft im Falle von Konflikten nicht zerstören werde (dies bemerken die Besitzer ja sofort), sondern dass man sie mit anderweitigen Tätigkeiten beschäftigen müsse, vor allem mit Hilfe von Programmen, die sich selbst reproduzieren und ständig in die Warteschlange des Betriebssystems neu einschleusen. Herr Kraus sollte nun in seiner Diplomarbeit untersuchen, für welche Funktionenklassen diese

Eigenschaft zutrifft und wie man diese Eigenschaft mit beliebiger Funktionalität der Klasse erweitern kann. Das heißt: Konstruiere zu einem gegebenen Programm ein neues Programm, das dessen Funktion ausführt und anschließend sich selbst reproduziert.

Auf Grund des Rekursionstheorems war klar, dass es erweiterte selbstreproduzierende Programme geben musste; man kann einige sogar mit Hilfe dieses Theorems konstruieren. Aber diese Konstruktion ist nicht praktikabel. Herr Kraus hat daher zu Beginn seiner Diplomarbeit entsprechende kurze Programme in Assembler, Pascal und Simula ausformuliert. Seine besondere Leistung bestand aber darin, dass er die Generierung solcher Programme in Simula programmiert und hiermit das wohl erste Virenerzeugungsprogramm entdeckt hat. Herr Kraus konnte auch beweisen, dass diese erweiterte Selbstreproduktion bereits für sehr einfache Sprachen (sog. Loop-1-Programme über Wörtern) zutrifft, dass somit praktisch alle existierenden Programmiersprachen selbstreproduzierend sind und dass (und wie) man entsprechende Programme (mit beliebig vielen eigenen Kopien) erzeugen kann.

Diese sehr gute Konstruktionsleistung von Herrn Kraus steht somit sicher zu Recht am Anfang des DAT 2007. Leider bin ich verhindert, hieranteizunehmen, und wünsche daher allen (und insbesondere Herrn Kraus) aus der Ferne eine erfolgreiche Veranstaltung.

Volker Claus

Jürgen Kraus Absolvent Fachbereich Informatik 1980 Selbstreproduktion bei Programmen 1980 - von einer Idee zum Virus

Ende der 70er Jahre des vergangenen Jahrhunderts gewannen Computersysteme insbesondere durch Vernetzung eine immer größere Leistungsfähigkeit. In ihrer Komplexität erinnerten sie durchaus an ein Universum aus Schaltkreisen, Bits und Bytes, Nullen und Einsen - ähnlich unüberschaubar wie die molekularen Verhältnisse auf unserer Erde in frühen Phasen der Evolution.



Ausgehend von der eher philosophischen Erkenntnis, dass die spontane Entstehung von Leben auf der Erde letztlich auch eine Folge von Komplexität war, entstand schließlich die Fragestellung, ob sich auch innerhalb von Computersystemen Strukturen identifizieren lassen, die zumindest einfachen Lebensformen vergleichbar erscheinen. Sciencefiction-Filme, in denen Computersysteme in einer vernetzten Welt die Herrschaft über fremde Computer erlangen und schließlich ausser Kontrolle geraten lassen, regten zusätzlich die Fantasie an.



Eine Grundeigenschaft von Leben ist die Selbstreproduktion, also die Fähigkeit, eine identische Kopie von sich selbst - ohne Steuerung von aussen - erzeugen zu können. Aus der Theorie der Berechenbarkeit folgt die Existenz einer rekursiven Funktion, die - manifestiert als textuelle Formulierung in einer höheren Programmiersprache - in der Lage ist, ihren eigenen Quellcode zu kopieren. Der theoretische Existenzbeweis liefert allerdings keinen Konstruktionshinweis für selbstreproduzierende Programme.

In Form einer Diplomarbeit gelang es, selbstreproduzierende Programme in höheren Programmiersprachen zu entwickeln. Dabei zeigte es sich, dass die Reproduktionseigenschaft algorithmisch sehr einfach (loop1) und textuell recht kurz (lines of code) formuliert werden kann.

Wichtig war insbesondere die Erkenntnis, dass selbstreproduzierenden Programmen beliebige Zusatzfunktionen - also auch schädliche - so hinzugefügt werden können, dass die Reproduktionseigenschaft erhalten bleibt. Mit anderen Worten, auch jeder Schadsoftware kann die Fähigkeit, sich zusätzlich auch noch zu kopieren, mitgegeben werden.

Beim Vergleich mit lebenden Organismen zeigte sich jedoch, dass man auf Grund des fehlenden Stoffwechsels ein selbstreproduzierendes Programm maximal als Virus bezeichnen kann. Zusammen mit der Fähigkeit, Schadsoftware zu transportieren, war somit bereits 1980 der Computervirus vorweggenommen.

Prof. Dr. Daniel J. Bilar
Wellesley College, Massachusetts, USA
Back to the Future: From Dortmund to present and
future malware challenges



The forgotten past is not forgotten, and it is not even past. I will discuss the recently resurfaced 1980 thesis on self-reproducing programs by a Dortmund alum, Juergen Kraus. His work is not only pioneering in that it changes the commonly known history of computer virology, but perspicacious in the theoretical description of threats that have only relatively recently begun to become a cause for concern.

I will give an overview of such metamorphic and novel k-ary threats and the push towards interactive detection techniques.

Frank W. Felzmann
Bundesamt für Sicherheit in der Informationstechnik, Bonn
Von Michelangelo bis MPack - Eine kurze
Geschichte verbreiteter Computer-Schädlinge

Computer-Viren, wie sie Jürgen Kraus in seiner Diplomarbeit von 1980 erstmals beschrieb, sind nicht nur Theorie geblieben, sondern leider zur täglichen Bedrohung geworden.

Der Vortrag gibt einen Überblick über massenhaft aufgetretene Computer-Viren, die hauptsächlich Ursachen für deren Verbreitung, sowie den gegenwärtigen Stand der Gefährdung der IT-Sicherheit - neuerdings durch Trojanische Pferde.

