

Wurm-Ausbreitung in Internet

Svetozar Koychev
(koychev@in.tum.de)

Hauptseminar „Internet-Measurement“ ,
Technische Universität München

SS 2005 (Version vom 26. Juli 2005)

Zusammenfassung

In diesem Paper betrachten wir die Ausbreitung von Computerwürmern im Internet. Das sind kleine, sich selbst reproduzierende Computerprogramme, die sich nach dem Zufallsprinzip verbreiten. Trotzdem kann man aber eine gewisse Ordnung in ihrer Fortpflanzung beobachten. Wir versuchen formale Methoden zu repräsentieren, die uns sehr hilfreich beim Verstehen des Verhaltens von Computerwürmern sein können und ein starkes Instrumentarium für ihre Bekämpfung zur Verfügung stellen. Die Modelle, die hier vorgestellt werden, basieren auf schon vorhandenen Techniken zur Erklärung der Übertragung von biologischen Viren, da die Computerviren und -würmer viele Gemeinsamkeiten mit den organischen Viren haben. In Betracht kommen die klassischen epidemischen Modelle, auf deren Basis das Zwei-Faktor-Internet-Wurm-Modell vorgestellt wird. Wir analysieren die Ausbreitung des Wurms Code-Red, der im Juli und August 2001 tausende PCs infizierte und viele Schäden verursachte.

1 Einleitung

Die schnelle Ausbreitung des Internets in den letzten Jahren ermöglicht es Millionen von PC-Benutzern weltweit miteinander zu kommunizieren und so private oder geschäftliche Daten auszutauschen, die über andere Medien (Telefon, Fax) nicht übertragbar sind. Diese Datenübertragung ist aber nicht immer sicher und ungefährlich, da sich manchmal mit den eigentlichen Daten auch kleine, sich selbst reproduzierende Computerprogramme verbreiten - die Würmer. Das Thema der Wurm-Ausbreitung im Internet ist nicht neu, aber in den letzten Jahren immer aktueller geworden. Die Ereignisse im Jahr 2001, bei denen sich Code-Red und Nimda ausgebreitet haben, haben uns gezeigt, wie verwundbar das weltweite PC-Netz ist und wie wenig wir die Gefahr kennen. Deshalb sind Untersuchungen in diesem Bereich sehr hilfreich, um uns in Zukunft gegen Würmer verteidigen zu können. Ziel dieser Untersuchungen sind die Wurm-Eigenschaften und die Faktoren, die sich auf die Wurm-Ausbreitung im Internet auswirken:

- Übertragungsmuster während ihrer Lebenszeit
- Einfluss des Netzverkehrs, der Netzwerkarchitektur
- Bewusstheit der Menschen und die Gegenmassnahmen, die sie unternehmen

Ein präzises Wurm-Modell gewährt Einblicke in das Wurm-Verhalten. Es ist hilfreich zum Identifizieren der Schwächen der Wurmausbreitungskette und stellt Methoden für Abschätzung der Schäden bei einer neuen Wurm-Bedrohung zur Verfügung.

Im folgenden Kapitel werden wir den Begriff „Wurm“ definieren. Im Kapitel 3 betrachten wir näher die Funktionsweise der Würmer anhand von Beispielen. Kapitel 4 beschreibt drei verschiedene Modelle der Wurm-Ausbreitung, die in einer Simulation verwendet werden.

2 Was ist ein Wurm?

In [4] ist ein **Wurm** wie folgt definiert:

Definition 1 (Computerwurm) *Eine selbständige Programm-Routine, die sich selbst reproduziert, indem sie über ein Computernetzwerk an Computerprogrammen oder Betriebssystemen anderer Computer Manipulationen vornimmt.*

Das Ziel des Wurms dabei ist, in einem Netzwerk so viele Computer wie möglich zu befallen. Er benötigt zum Ausbreiten kein menschliches Zutun. Beispielsweise versendet er sich mit Hilfe der E-Mail-Funktionen. Manche Würmer haben zusätzlich noch eine Ladung (Payload), welches dann ein Schadprogramm, wie z.B. ein herkömmlicher Virus, ist. Dieses wirkt sich dann innerhalb des PC's aus. [9]

3 Wie funktionieren Würmer?

Wir betrachten näher die Würmer Code-RedI, Code-RedII und Nimda.

3.1 Code-RedI

Im Juni 2001 wird eine Bufferoverflow-Sicherheitslücke in der ISAPI.DLL des Microsoft Internet Information Servers (IIS) entdeckt und Microsoft veröffentlicht einen Patch (Programm zur Korrektur), um sie zu schließen. Am 12. Juli 2001 beginnt der Wurm Code-RedI diese Schwäche des IISs auszunutzen, indem er sich auf Rechner mit IIS verbreitet. Der Wurm überprüft, ob das Systemdatum auf der infizierten Maschine zwischen dem 1. und dem 19. eines Monats liegt. Wenn ja, generiert er 100 zufällige IP-Adressen und versucht die zugehörigen Rechner zu infizieren. Zwei Stunden nach der Infizierung ersetzt der Wurm die Webseiten auf den angesteckten Servern mit der folgenden HTML-Seite:



Abbildung 1: Die ersetzte Webseite auf einem infizierten IIS-Server

Nach Ablauf von 10 Stunden ist wieder die ursprüngliche Webseite zu sehen. Der Wurm bleibt solange in dem Hauptspeicher und kann durch einen Neustart des Rechners deaktiviert werden. So wird der Rechner aber vor einer neuen Infektion nicht geschützt.

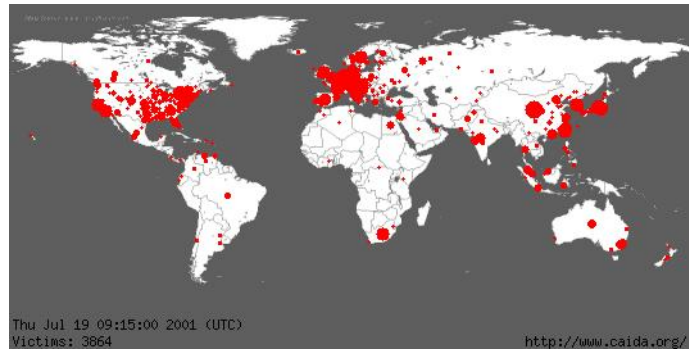


Abbildung 2: Um 10.00 Uhr UTC am 19. Juli 2001 waren „nur“ 4.000 PCs mit Code-RedI v2 infiziert

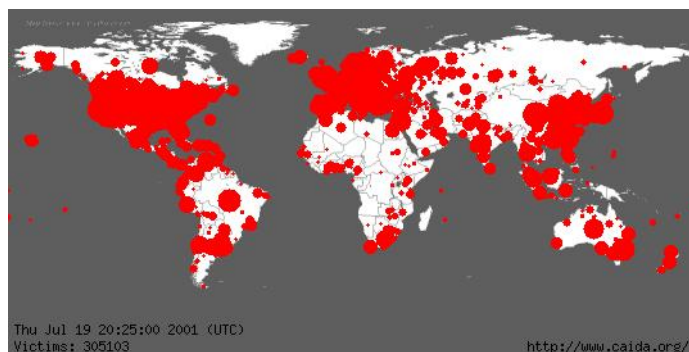


Abbildung 3: ... in 14 Stunden waren es mehr als 359.000

Vom 20. bis zum 27. jedes Monats war der Wurm programmiert, mit der Infizierung entfernter Computer aufzuhören und mit der nächsten Phase fortzufahren. Er startet eine Denial-of-Service- Attacke auf `www1.whitehouse.gov`, indem er große Datenmengen an den Server schickt, mit dem Ziel, dass dieser nicht mehr erreichbar ist. Bis Ende des Monats ist er inaktiv. Am 19. Juli 2001 gegen 10.00 Uhr UTC wurde eine Veränderung in dem Verhalten des Wurms beobachtet [1]. So ist Code-RedI v2 entstanden. Code-RedI v1 verbreitete sich langsam, weil er nicht sehr unterschiedliche Listen mit zu infizierenden IP-Adressen auf jedem PC erzeugte. Bei Code-RedI v2 war das ganz anders: innerhalb von 14 Stunden wurden mehr als 340.000 Rechner weltweit infiziert. Wie aus Abbildung 2 und Abbildung 3 (Quelle: [7]) ersichtlich ist, hat sich Code-RedI v2 rasant verbreitet.

3.2 Code-RedII

Am 4. August 2001 begann ein ganz neuer Wurm die Schwäche des IISs auszunutzen und sich zu verbreiten. Obwohl er keine der Eigenschaften von Code-RedI hatte, bekam er den Namen Code-RedII, weil in seinem Source-Code der String „CodeRedII“ vorkam. Er verursachte komplett andere Schäden als Code-RedI, indem er auf dem befallenen Rechner eine Hintertür installierte, durch die ein entfernter Zugriff auf den Computer, z.B. Ausführung von Code, möglich war und die für zukünftige Attacken benutzt werden konnte. Der Trojaner befand sich in der Datei `explorer.exe`. Weitere Dateien versuchten gleichzeitig, andere Rechner zu infizieren. Dabei wurden alle IP-Adressen in demselben Subnetz gescannt. Obwohl ein Patch zur Beseitigung der Schwäche schon vorhanden war, verbreitete sich auch Code-RedII rasant.

3.3 Nimda

Es dauerte nicht lange und Mitte September 2001 kam die von Code-RedII installierte Hintertür zum Einsatz. [6] Der Wurm W32/Nimda-A legte in Windows NT/2000-Rechnern einen Gast-Account mit Administrator-Rechten an, kopierte sich in das Windows-Verzeichnis mit den Dateinamen *load.exe* und *riched20.dll* und veränderte die Datei *system.ini*, so dass sie folgende Zeile enthielt:

```
shell=explorer.exe load.exe -dontrunold
```

Somit wurde sie beim Start von Windows ausgeführt. Nimda ist der erste Wurm, der sich auf unterschiedliche Art und Weise verbreitete, u.a. via E-Mail, Netzwerkfreigaben und Websites. Die infizierten Mails trugen wechselnde Betreffzeilen und enthielten häufig einen Anhang mit dem Mime-Typ Audio/WAV, hinter dem sich EXE- oder DOC-Dateien versteckten. Der Wurm befahl Webserver, die unter Microsofts IISs laufen und baute in deren Webseiten Java-Skript-Code ein, der eine Datei namens *readme.eml* nachlud. In dem Wurm-Code war der folgende Text enthalten: „Copyright 2001 R.P.China“.

4 Modelle der Wurm-Ausbreitung

Dieses Kapitel beschäftigt sich mit den Modellen zur Beschreibung der Wurm-Ausbreitung im Internet. Zuerst werden die benutzten Begriffe vorgestellt.

4.1 Terminologie

Computerviren und -würmer sind biologischen Viren in deren Reproduzierung und Verhalten sehr ähnlich. So können die mathematischen Techniken, die für die Studie der Ausbreitung von biologischen Viren entwickelt wurden, an die Studie von Computerviren angepasst werden. Die Methoden können in zwei Gruppen unterteilt werden:

- stochastische Modelle - passend für eine einfache Virus-Dynamik in einem kleinen System (kleine Menge von Daten)
- deterministische Modelle - geeignet für große Systeme und beruhend auf dem Gesetz der großen Zahlen

Beim Modellieren der Internet-Wurm-Ausbreitung werden Millionen von Computern betrachtet. Für die Untersuchung einer so großen Menge von Daten sind die bereits erwähnten deterministischen Modelle hilfreich. Im nächsten Kapitel werden zwei klassische deterministische epidemische Modelle vorgestellt, die als Basis des Zwei-Faktor-Internet-Wurm-Modells dienen, das wir später in diesem Papier betrachten.

Die Anzahl aller Rechner N , deren Verhalten in diesen Modellen analysiert wird, kann in Gruppen anhand ihres Zustandes zum Zeitpunkt t aufgeteilt werden [2]:

- gefährdete Rechner $S(t)$ (*susceptible*) - können von anderen Rechnern infiziert werden
- infizierende Rechner $I(t)$ (*infectious*) - wurden angesteckt und versuchen andere Rechner zu infizieren
- eliminierte Rechner $R(t)$ (*removed*) - Rechner, die infiziert wurden, zum Zeitpunkt t aber immun sind, deshalb nicht infiziert werden können und nie andere Rechner zu infizieren versuchen
- eliminierte Rechner $Q(t)$ - Rechner, die noch nicht infiziert wurden, zum Zeitpunkt t immun sind, deshalb nicht infiziert werden können und nie andere Rechner zu infizieren versuchen
- infizierte Rechner $J(t) = R(t) + I(t)$ (*infected*) - wurden vor dem Zeitpunkt t infiziert, können eliminiert $R(t)$ oder infizierend $I(t)$ sein

Tabelle 1: Alle Bezeichnungen in diesem Papier auf einem Blick

Bezeichnung	Erläuterung
$S(t)$	Anzahl der gefährdeten Rechner zum Zeitpunkt t
$I(t)$	Anzahl der infizierenden Rechner zum Zeitpunkt t
$R(t)$	Anzahl der eliminierten Rechner in t , die bereits infiziert wurden
$Q(t)$	Anzahl der eliminierten Rechner in t , die noch nicht infiziert wurden
N	Anzahl der betrachteten Rechner $N = S(t) + Q(t) + R(t) + I(t)$
$J(t)$	Anzahl der infizierten Rechner $J(t) = R(t) + I(t)$ zum Zeitpunkt t
$\beta(t)$	Infektionsrate zum Zeitpunkt t

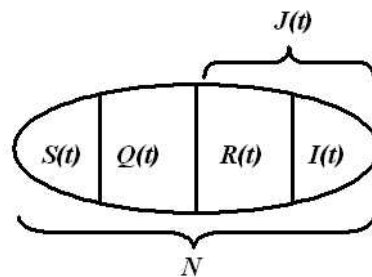


Abbildung 4: Anzahl aller betrachteten Rechner $N = S(t) + Q(t) + J(t)$

- alle eliminierten Rechner $C(t) = R(t) + Q(t)$ - alle Rechner, die zum Zeitpunkt t immun sind und nicht infiziert werden können

In der Tabelle 1 und in Abbildung 4 sind noch mal kurz alle Bezeichnungen, die wir in den nächsten Kapiteln benutzen werden, dargestellt.

4.2 Das klassische einfache epidemische Modell

Bei diesem Modell werden die betrachteten Rechner in zwei Gruppen unterteilt: gefährdete und infizierende [2]. Es wird angenommen, dass ein infizierter Computer in diesem Zustand für immer bleibt. Ein Übergang in einen anderen Zustand ist nur in Richtung *gefährdet* \rightarrow *infizierend* möglich. Die folgende Formel beschreibt das Modell für eine feste Anzahl an Computern N :

$$\frac{dJ(t)}{dt} = \beta J(t)[N - J(t)] \quad (1)$$

wobei

- $J(t) = I(t)$ - Anzahl der infizierenden Rechner zum Zeitpunkt t , da $R(t) = 0$
- β - die konstante Infektionsrate
- $N - J(t) = S(t)$ - Anzahl der gefährdeten Rechner zum Zeitpunkt t , da $Q(t) = 0$

sind. Am Anfang, für $t = 0$, sind $J(0)$ Rechner infizierend und der Rest $S(0) = N - J(0)$ ist gefährdet. Die Veränderung der Anzahl der infizierenden Rechner hängt, wie aus Formel (1) ersichtlich, positiv von $J(t)$ und $S(t)$ ab. D.h. wenn viele Rechner infizierend und viele Rechner gefährdet sind, verbreitet sich der Internet-Wurm sehr schnell. Das Modell definiert noch

$$a(t) = \frac{J(t)}{N} \quad (2)$$

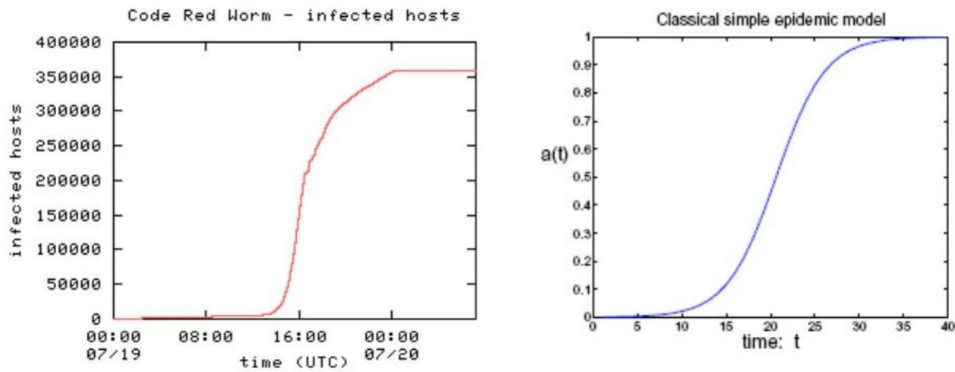


Abbildung 5: a) Von Code-Red-I infizierte Rechner b) Das klassische einfache epidemische Modell

als relativer Anteil der infizierenden Rechner zum Zeitpunkt t von der gesamten Menge der betrachteten Rechner N .

Am Anfang, wenn der relative Anteil der gefährdeten Rechner $1 - a(t) \approx 1$ ist (fast alle Rechner sind gefährdet) und $a(t) \approx 0$ (nur wenig Rechner sind infizierend), beginnt die Wurm-Ausbreitung exponentiell zu wachsen und die Rate der Ausbreitung fällt erst dann, wenn fast 80% aller gefährdeten Rechner infiziert sind.

Wie in Abbildung 5a) und 5b) (Quelle: [8]) sehr gut zu erkennen ist, entspricht das klassische einfache epidemische Modell der Code-Red-Ausbreitung in der ersten Phase genau, kann sie aber in den letzten fünf Stunden von 19.00 bis 00.00 UTC am 19. Juli 2001 nicht erklären. Der Abbildung zufolge sollten gegen 19.00 Uhr alle online IIS Server infiziert sein, andere Methoden zeigen aber, dass dies nur bei 60% der Fall war.

4.3 Das klassische generelle epidemische Modell: Kermack-Mckendrick-Modell

Im Bereich der Epidemiologie betrachtet das Kermack-Mckendrick-Modell den Prozess der Beseitigung von infizierenden Rechnern [2]. Die Zustände, in denen sich ein Computer bei diesem Modell befinden kann, sind gefährdet, infizierend und eliminiert. Es wird angenommen, dass ein infizierter Rechner entweder infizierend $I(t)$ oder eliminiert $R(t)$ wird und somit kann er nicht wieder angesteckt werden. Die möglichen Zustandsänderungen bei diesem Modell sind *gefährdet* \rightarrow *infizierend* \rightarrow *eliminiert*, *gefährdet* \rightarrow *infizierend* oder ein Rechner bleibt für immer im Zustand gefährdet. In diesem Kapitel benutzen wir die Bezeichnungen, die in Tabelle 1 definiert wurden. Basierend auf dem im Kapitel 4.2 vorgestellten klassischen einfachen epidemischen Modell, lautet das Kermack-Mckendrick-Modell:

$$\begin{cases} \frac{dJ(t)}{dt} = \beta J(t)[N - J(t)] \\ \frac{dR(t)}{dt} = \gamma I(t) \\ J(t) = I(t) + R(t) = N - S(t) \end{cases} \quad (3)$$

wobei γ die Rate der Beseitigung von infizierenden Rechnern ist. Der erste Teil der Formel (3) ist nicht neu und vom Kapitel 4.2 bekannt. Der zweite beschreibt, wie sich die Anzahl der eliminierten Rechner $R(t)$ in Abhängigkeit von den infizierenden $I(t)$ und von der Beseitigungsrate γ verändert. Der dritte Teil ist die Definition von $J(t)$ vom Kapitel 4.1, wobei $Q(t) = 0$.

Wir definieren $\rho \equiv \gamma/\beta$ als die relative Beseitigungsrate der infizierenden Rechner. Das

Modell führt zu dem interessanten Ergebnis, dass die Veränderung der Anzahl der infizierenden Rechner in Abhängigkeit von der Zeit t

$$\frac{dI(t)}{dt} > 0 \quad (4)$$

ist, genau dann wenn $S(t) > \rho$ [2]. Unter der Annahme, dass keine neuen gefährdeten Rechner hinzukommen (N konstant), ist ihre Anzahl $S(t)$ eine monoton fallende Funktion in Abhängigkeit von der Zeit t . Wenn $S(t_0) < \rho$ ist, dann ist $S(t) < \rho$ und $\frac{dI(t)}{dt} < 0$ für alle $t > t_0$. Mit anderen Worten, wenn am Anfang die Anzahl der gefährdeten Rechner kleiner als ein kritischer Wert ist, also $S(0) < \rho$, existiert keine Gefahr von einem Epidemieausbruch.

Das Kermack-Mckendrick-Modell erweitert das klassische einfache epidemische Modell und berücksichtigt noch, dass einige der infizierenden Rechner nach gewisser Zeit von Infizierung befreit werden oder nicht mehr im Einsatz sind. Dennoch ist dieses Modell aber nicht ganz zur Beschreibung der Internet-Wurm-Ausbreitung geeignet. *Erstens* werden im Internet viele Gegenmaßnahmen zum Schutz vor einer Infizierung unternommen, die noch nicht infizierten Hosts aus dem Gefahr ausschalten. Dieses Modell besagt aber, dass nur infizierte Rechner auch beseitigt werden können. *Zweitens* nimmt das Modell an, dass die Infektionsrate β konstant ist. Das entspricht nicht der Realität, wie bei der Ausbreitung des Code-Red betrachtet werden konnte. In dem nächsten Kapitel wird das Zwei-Faktor-Internet-Wurm-Modell vorgestellt, das die Realität genauer als die bis jetzt betrachteten Modelle wiedergibt.

4.4 Das Zwei-Faktor-Internet-Wurm-Modell

Nach der Auswertung von Berichten und Meldungen über das Code-Red-Ereignis vom 19. Juli 2001, hat man zwei Faktoren als ausschlaggebend für die Beschreibung der Internet-Wurm- Ausbreitung bezeichnet, die in den traditionellen Epidemie-Modellen fehlen:

- Maßnahmen, die die Menschen unternehmen, um sich zu schützen. Dadurch wird die Anzahl der Rechner, die zu einem Zeitpunkt gefährdet sind, nicht vorhersehbar. Solche Gegenmaßnahmen können unter anderem Anti-Virus- und Patch-Programme, Filter, Firewalls und Router sein, die die Viren stoppen, oder einfach eine Unterbrechung der Verbindung zum Internet.
- die Infektionsrate $\beta(t)$ fällt mit der Zeit und ist nicht konstant, wie bisher angenommen. Sie kann als fallende Funktion der Zeit t dargestellt werden.

Die Veränderung der Infektionsrate $\beta(t)$ besteht aus zwei Teilen: Eliminierung von infizierenden Rechnern ($R(t)$) und Eliminierung von gefährdeten Rechnern ($Q(t)$). Nach dem Kermack- Mckendrick-Modell entspricht die Änderung der Anzahl der gefährdeten Computer $S(t)$ von der Zeit t zur Zeit $t + \Delta t$ der folgenden Gleichung:

$$S(t + \Delta t) - S(t) = -\beta(t)S(t)I(t)\Delta t - \frac{dQ(t)}{dt}\Delta t \quad (5)$$

oder

$$\frac{dS(t)}{dt} = -\beta(t)S(t)I(t) - \frac{dQ(t)}{dt} \quad (6)$$

Es gilt dabei immer $N = S(t) + I(t) + R(t) + Q(t)$. Nach Einsetzen von $S(t) = N - (I(t) + R(t) + Q(t))$ in (6) bekommen wir die folgende Gleichung:

$$\frac{dI(t)}{dt} = \beta(t)[N - I(t) - R(t) - Q(t)]I(t) - \frac{dR(t)}{dt} \quad (7)$$

die dem Zwei-Faktor-Internet-Wurm-Modell entspricht. Gleichung (7) besagt, dass die Anzahl der infizierenden Rechner $I(t)$ sich im Laufe der Zeit verändert und die Veränderung von den folgenden Faktoren abhängt:

- die variable Infektionsrate $\beta(t)$
- die Anzahl der gefährdeten Rechner $S(t) = N - I(t) - R(t) - Q(t)$
- die Anzahl der infizierenden Rechner $I(t)$ zum Zeitpunkt t
- die Veränderung der Anzahl der eliminierten Rechner $R(t)$

In diesem Papier betrachten wir nur dauerhaft aktive Internet-Würmer [2]. Wir nehmen an, dass ein infizierter Rechner ständig andere zu infizieren versucht, so wie dies der Fall am 19. Juli 2001 mit Code-RedI war. In der Realität verbreiten sich aber die Computervürmer nicht andauernd, sondern halten irgendwann an, wie z.B. Code-RedI um 00.00 Uhr am 20. Juli 2001. Solche Unterbrechungen können nicht vorhergesagt, sondern nur durch Analyse des Wurm-Codes in Erfahrung gebracht werden. Der Wurm Code-Red ist von der Internet-Struktur unabhängig; die Ausbreitung anderer Würmer, wie Melissa und Love-Bug, die sich per E-mail übertragen, hängen von der logischen Struktur der E-Mail-Adressbücher der betroffenen Benutzer ab.

4.5 Simulation der Code-Red-Ausbreitung

In diesem Kapitel werden wir anhand des im Kapitel 4.4 vorgestellten Zwei-Faktor-Internet-Wurm-Modells eine Simulation von Code-Red beschreiben [2]. Das betrachtete System besteht aus N Rechnern, wobei jeder Computer mit allen anderen direkt verbunden ist. So kann die Netzwerkstruktur die Ergebnisse der Simulation nicht beeinflussen. Jeder Host befindet sich zu einem Zeitpunkt t in einem der folgenden Zustände: gefährdet, infizierend oder eliminiert. Ein Rechner kann im Zustand eliminiert sein, wenn er immun ist, unabhängig davon ob er schon oder noch nicht infiziert wurde. Die möglichen Zustandsübergänge sind *gefährdet* \rightarrow *infizierend* \rightarrow *eliminiert* oder *gefährdet* \rightarrow *eliminiert*. Am Anfang der Simulation sind ein Teil der Rechner infizierend, die anderen - gefährdet.

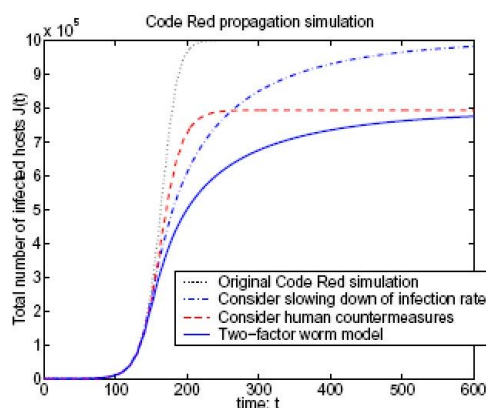


Abbildung 6: Code-Red Simulation basiert auf verschiedenen Modellen

Wir betrachten die Simulation von vier Szenarien:

1. Szenario - entspricht dem klassischen einfachen epidemischen Modell vom Kapitel 4.2 mit konstanter Infektionsrate β

2. Szenario - mit fallender Infektionsrate β
3. Szenario - die Effekte der menschlichen Gegenmaßnahmen werden betrachtet, β konstant
4. Szenario - basierend auf dem Zwei-Faktor-Internet-Wurm-Modell mit fallender Infektionsrate β

Für jedes Szenario läuft die Simulation 100 Mal und die Anzahl der infizierten Rechner $E[J(t)]$ zu jedem Zeitpunkt t ist das arithmetische Mittel aller Ergebnisse. Die anderen Parameter sind: $N = 1.000.000$, wobei 10 davon am Anfang bei $t = 0$ infiziert sind.

Die Ergebnisse sind in Abbildung 6 (Quelle: [2]) zu sehen. Wenn wir sie mit der Graphik in Abbildung 5a, die die Ausbreitung von Code-RedI am 19. Juli 2001 darstellt, vergleichen, sehen wir, dass das Zwei-Faktor-Internet-Wurm-Modell der Code-Red-Ausbreitung genau entspricht. Es ist also ein sehr starkes Instrument zur Beschreibung der Eigenschaften von Internet-Würmern. Einzelne zufällige Ereignisse haben kaum einen Einfluss auf die Ergebnisse, da die Menge der betrachteten Computer sehr groß ist und jede Wurm-Kopie sich unabhängig von den anderen verbreitet.

5 Zusammenfassung

Wir haben gesehen, dass die Internet-Wurm-Ausbreitung ein sehr komplexer Prozess ist, der aber dank verschiedenen Techniken beschrieben und zusammengefasst werden kann. Als sehr geeignet hat sich das Zwei-Faktor-Internet-Wurm-Modell erwiesen. Es besagt, dass zwei wichtige Faktoren die Ausbreitung von Würmern in Internet beeinflussen:

- das Effekt der menschlichen Gegenmaßnahmen - z.B. Installation von Anti-Virus- und Patch-Programmen, Firewalls usw.
- die Infektionsrate β ist nicht konstant und fällt mit der Zeit.

Eine exponentielle Ausbreitung der Würmer wird nur in der ersten Phase beobachtet. Wenn 50 % aller Rechner schon infiziert wurden, beginnt langsam die Abschwächung der Infektionsrate.

Laut [2] ist das Zwei-Faktor-Internet-Wurm-Modell ein generelles Internet-Wurm-Ausbreitungsmodell und gilt nicht nur für Code-Red. Es ist aber leider nicht immer aussagekräftig, da es nur für eine ununterbrochene Wurm-Ausbreitung entwickelt wurde, d.h. die Vorhersage von einem Stillstand ist mit diesem Modell nicht möglich. Außerdem wurden bei den Modellen einige Parameter wie β und γ benutzt, die nicht von Anfang an bekannt sind, sondern an den Code-Red-Daten angepasst wurden. Bevor aber die vorgestellten Modelle auch angewendet werden können, sollten diese Parameter bestimmt werden. Deshalb sind noch Forschungen in diesem Gebiet notwendig, um zukünftige Würmer, Viren und ihre Schäden vorhersagen zu können.

Die Modelle können aber die Gefahr von einer rasanten Internet-Wurm-Ausbreitung gut abschätzen und sind deshalb sehr hilfreich. Durch neue Erkenntnisse und Erfahrungen werden sie ständig weiter verbessert und entwickelt.

Literatur

- [1] David Moore, Colleen Shannon, k claffy: *Code-Red: a case study on the spread and victims of an Internet worm*; Proceedings of the Second Internet Measurement Workshop IMW, 2002
- [2] Cliff Changchun Zou, Weibo Gong, Don Towsley: *Code Red Worm Propagation Modeling and Analysis*; Proceedings of the 9th ACM Conference on Computer and Communication Security (CCS-02)
- [3] Peter Klau: *Hacker, Cracker, Datenräuber*; Vieweg 2002.
- [4] Wikipedia - die freie Enzyklopädie: <http://de.wikipedia.org/wiki/Computerwurm> vom 24. Mai 2005
- [5] eEye Digital Security, Published Advisories vom 17. Juli 2001:
<http://www.eeye.com/html/Research/Advisories/AL20010717.html>
- [6] Sophos Virenlexikon: <http://www.sophos.de/virusinfo/analyses/w32nimdaa.html> vom 4. Juni 2005
- [7] Cooperative Association for Internet Data Analysis (CAIDA):
http://www.jump.org.uk/caida_code_red_animations/newframes-small-log.mov vom 4. Juni 2005
- [8] Cooperative Association for Internet Data Analysis (CAIDA):
<http://www.caida.org/analysis/security/code-red/coderedv2.analysis.xml#animations> vom 4. Juni 2005
- [9] SpaceNet: <http://www.space.net/support/informationen/security/virenwuermerund/trojanischepferde/wurm/> vom 22. Juli 2005