

Simulation of malware propagation

André Harms



Simulation of malware propagation

Rückblick +
Einführung

Historische
Arbeiten

Botnet
Simulation

Drive-by-
Download
Simulator

MALSim

Zusammen-
fassung

Eigener
Ansatz

Rückblick

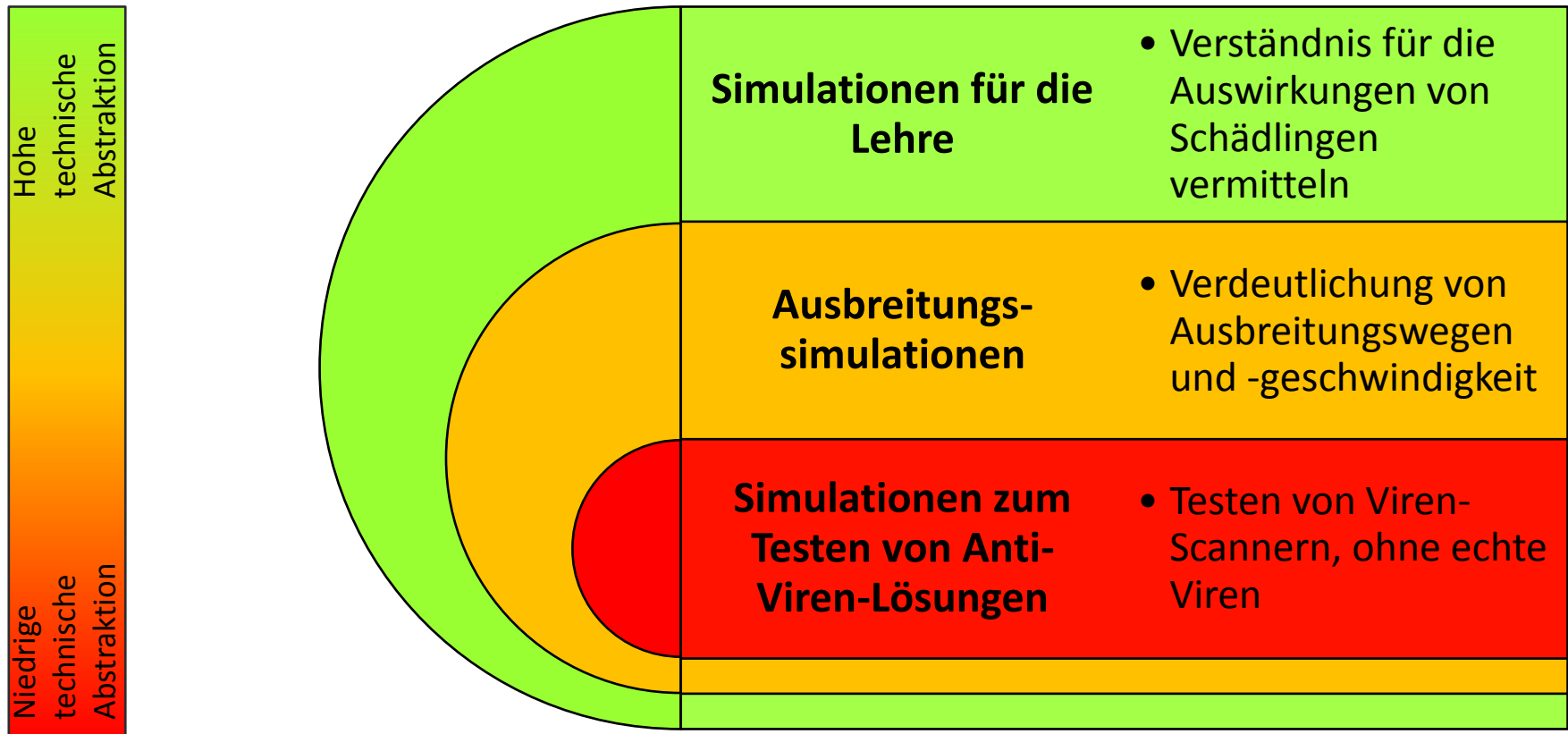
- Simulation von Cyberangriffen
 - Netzwerkangriffe
 - Ausbreitung von Schadsoftware
 - Mathematische Ansätze
 - Multiagenten-Simulation

- Warum?
Prävention, Handlungsempfehlungen, Forensik

- Ziel
Ausbreitung von Schadsoftware simulieren

Einführung

- Kategorien von Simulationen^{[1][2]}:



4/29

Rückblick +
Einführung

Historische
Arbeiten

Botnet
Simulation

Drive-by-
Download
Simulator

MALSim

Zusammen-
fassung

Eigener
Ansatz

Historische Arbeiten

Verschiedene Simulationen kurz erläutert

Historische Arbeiten

Virus Simulation Suite

- Joe Hirst 1990
- Zur Lehre gedacht
- Simuliert das Verhalten / die Auswirkung einer überschaubaren Anzahl von Viren (13), z.B. Cascade-Virus

```

DOSBox 0.74, Cpu speed: 3000 cycles, Frameskip 0, Program: DOSBOX
YANK-SIM COM          2,275 12-02-1990 15:27
NK-SIMX COM          2,329 12-02-199 15:17
15 File(s)          43,337 Bytes  0
Dr(s)              26 ,111, 44 Bytes fre .
Y  Z i )
: > AS -SIM COM
.          2      7      .      e

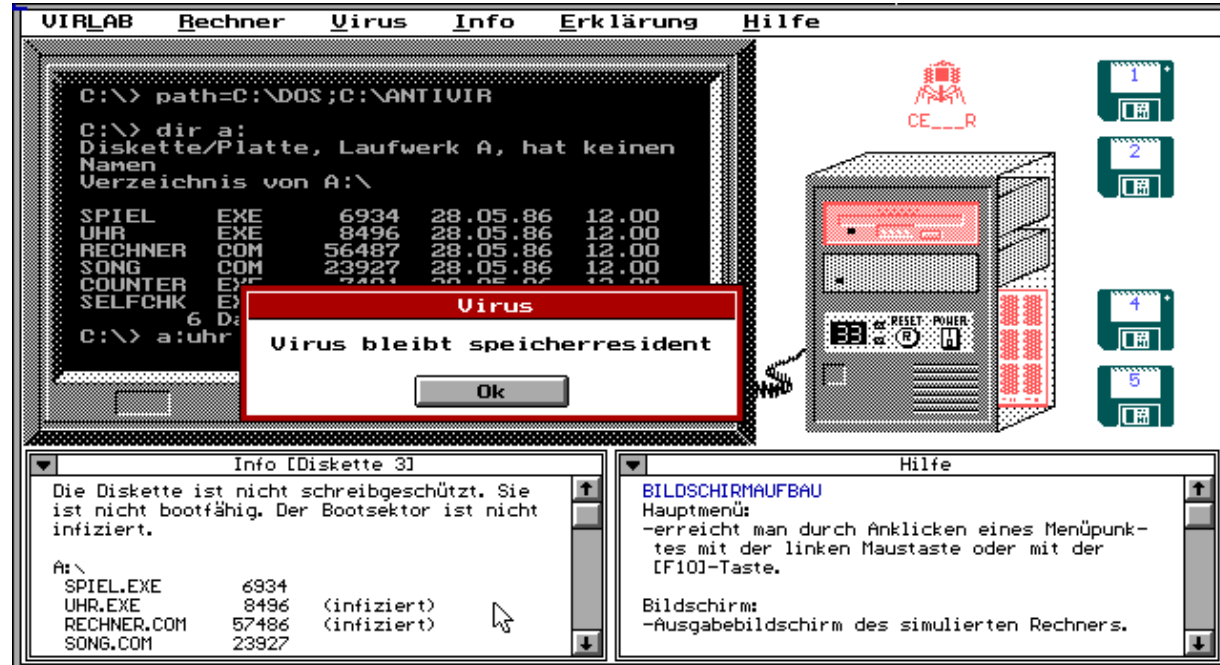
British Comput r Virus Research Centre      (Tel: 0273-26105)
2 Guildfo d Sereet, Bri hton, East us ex, N1 3LS England
1 r B
irus imu atitn Sui e                          Writ en by 'oe Hirst
l o S s t J
Progr m t CA C- IM.C M U1.1
C sc ae v ir s - Standard a i S ion
a u g c t 0
pyrig t ( ) Joe Hi s S1 a , 1 0.
U S a C h c r 9 9
is p ogr m d NOT vi us, nor s t v fec o s
a io a tit9 n
Resetsprogr m r - <ALT>8<+> 9
Th r Remove fromamemory - i<Alt>i<-> ti u 0

C \
C:\>C C
  
```

Historische Arbeiten

Virlab

- Karlhorst Klotz, et al. 1993
- Simulation zum Veranschaulichen von Effekten bei Vireninfection



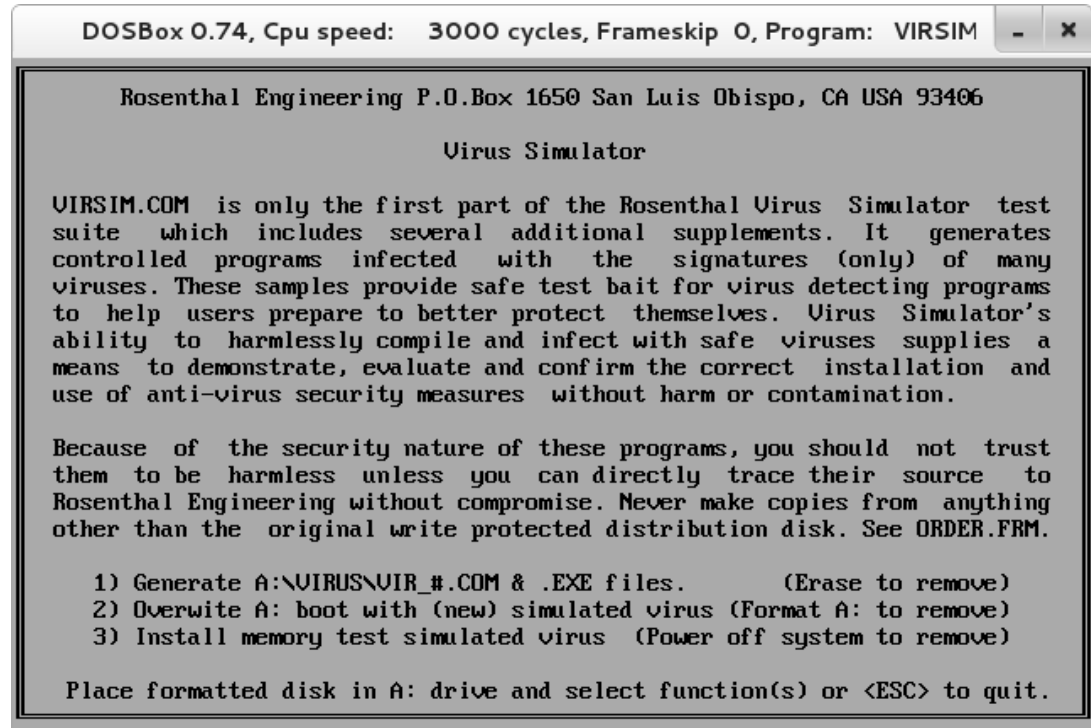
[1]

7/29

Historische Arbeiten

Rosenthal's Virus Simulator

- Von Rosenthal Engineering
- Sicheres Überprüfen von Anti-Viren Programmen
- Letzte Version: 1996



```
DOSBox 0.74, Cpu speed: 3000 cycles, Frameskip 0, Program: VIRSIM

Rosenthal Engineering P.O.Box 1650 San Luis Obispo, CA USA 93406

Virus Simulator

VIRSIM.COM is only the first part of the Rosenthal Virus Simulator test
suite which includes several additional supplements. It generates
controlled programs infected with the signatures (only) of many
viruses. These samples provide safe test bait for virus detecting programs
to help users prepare to better protect themselves. Virus Simulator's
ability to harmlessly compile and infect with safe viruses supplies a
means to demonstrate, evaluate and confirm the correct installation and
use of anti-virus security measures without harm or contamination.

Because of the security nature of these programs, you should not trust
them to be harmless unless you can directly trace their source to
Rosenthal Engineering without compromise. Never make copies from anything
other than the original write protected distribution disk. See ORDER.FRM.

1) Generate A:\VIRUS\VIR_#.COM & .EXE files. (Erase to remove)
2) Overwrite A: boot with (new) simulated virus (Format A: to remove)
3) Install memory test simulated virus (Power off system to remove)

Place formatted disk in A: drive and select function(s) or <ESC> to quit.
```


Toward Botnet Mesocosm^[3]

Botnet Simulation

Paul Barford, Mike Blodgett (2007)

University of Wisconsin-Madison

9/29

Rückblick +
Einführung

Historische
Arbeiten

Botnet
Simulation

Drive-by-
Download
Simulator

MALSim

Zusammen-
fassung

Eigener
Ansatz

Botnet Simulation

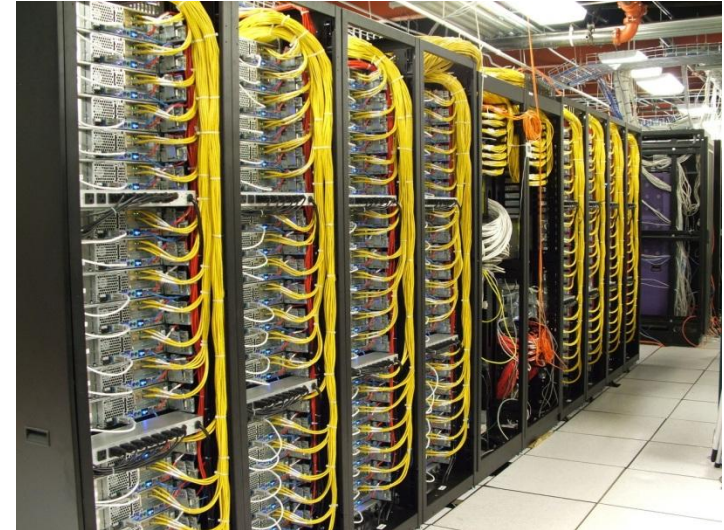
Ziele

- Verhalten von Botnets in Laborumgebung nachstellen
- Botnet Evaluation Environment (BEE)
- Umgebung soll sicher sein
- Realistische Botnet Konfigurationen und Topologien
- Simulation von Blackbox Clients als auch Whitebox Clients
(reine Binaries + kompiliert aus den Quellen)

Botnet Simulation

Umsetzung

- Toolkit für Emulab
- OS- und Botnet-Images
 - Binaries → VM Detection
(wenn vorhanden: keine Virtualisierung)
 - Aus Quellen → VM Detection kann auskommentiert werden
- Notwendige Dienste (DNS, IRC, DHCP)



[12]

11/29

Rückblick +
Einführung

Historische
Arbeiten

Botnet
Simulation

Drive-by-
Download
Simulator

MALSim

Zusammen-
fassung

Eigener
Ansatz

Botnet Simulation

Bewertung



- Vollständig virtualisiert

- Nahe an der Realität (Verwendung echter Schadsoftware)

- Verhaltensweise kann exakt beobachtet werden

- Funktioniert nur in Verbindung mit Emulab

- Spezialisiert auf eine Schädlingskategorie

- Nicht auf Ausbreitung spezialisiert

12/29

Rückblick +
Einführung

Historische
Arbeiten

Botnet
Simulation

Drive-by-
Download
Simulator

MALSim

Zusammen-
fassung

Eigener
Ansatz

A Lightweight Drive-by Download Simulator ^[4]

Drive-By-Download Infektions-Simulation

Matthew McDonald, James Ong. John Aycocock,
Heather Crawford, Nathan Friess (2009)

University of Calgary

13/29

Rückblick +
Einführung

Historische
Arbeiten

Botnet
Simulation

Drive-by-
Download
Simulator

MALSim

Zusammen-
fassung

Eigener
Ansatz

Drive-by-Download Simulator

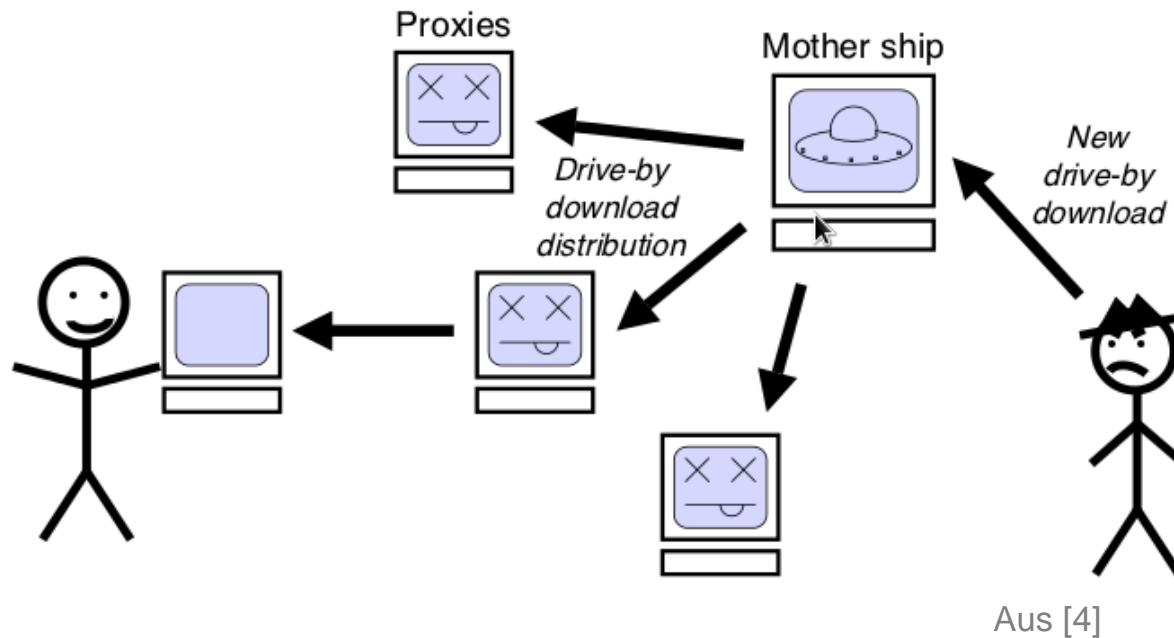
Ziele

- Vermitteln von Wissen über Malware
- Herstellen einer isolierten Umgebung
- Ausführen und Testen echten beliebigen Codes ermöglichen
- Skalierungsprobleme (hohe Komplexität) → daher Simulation von Drive-by-Downloads

Drive-by-Download Simulator

Umsetzung

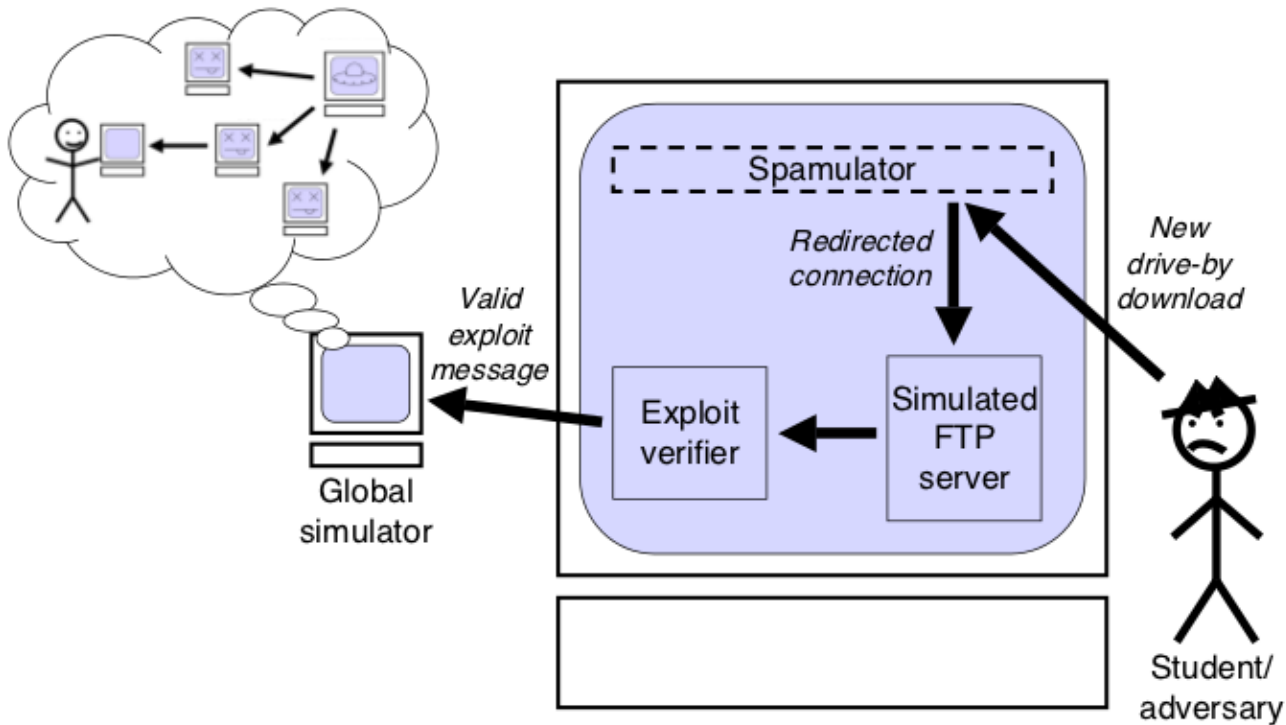
- Erweiterung von Spamulator



15/29

Drive-by-Download Simulator

Umsetzung



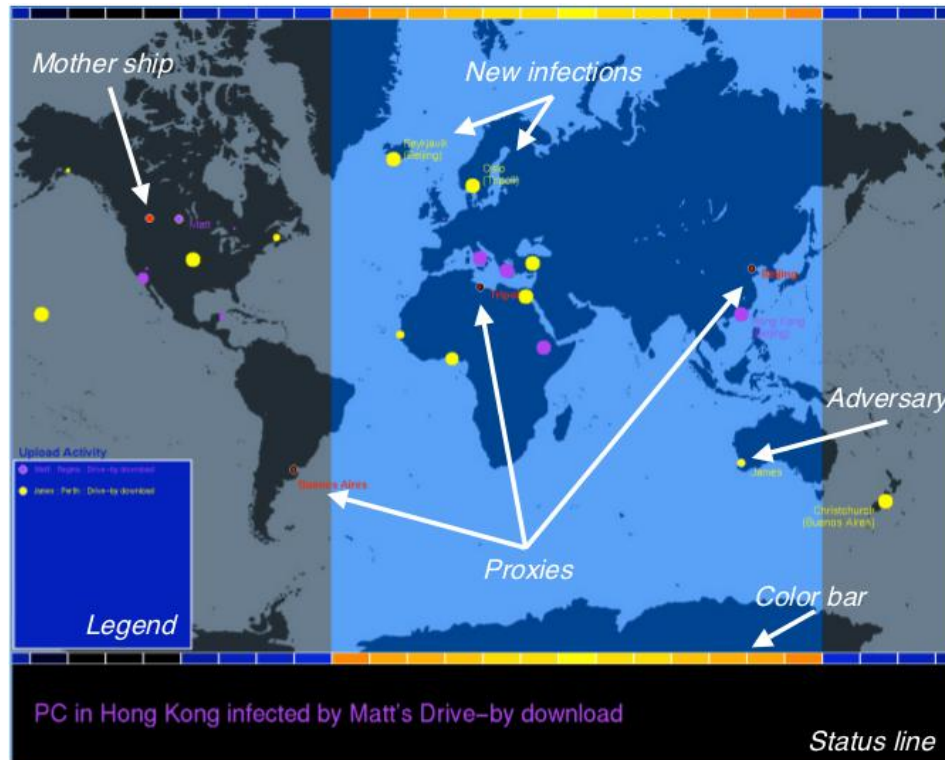
Aus [4]

- Exploitverifier: Einzelner Prozess → Firefox wird überwacht
- Läuft auf n Rechnern

16/29

Drive-by-Download Simulator

Umsetzung



Aus [4]

- „Global simulator“ aggregiert Simulationsergebnisse mehrerer Rechner

17/29

Rückblick +
Einführung

Historische
Arbeiten

Botnet
Simulation

Drive-by-
Download
Simulator

MALSim

Zusammen-
fassung

Eigener
Ansatz

Drive-by-Download Simulator

Bewertung



- Nahe an der Realität (Verwendung echter Schadsoftware)
- Genaue Beobachtung möglich

- Nur ein Verbreitungsweg simuliert
- Nutzerverhalten nur bedingt simuliert
- Nur für einen Browser geeignet. Erweiterung aufwändig.

18/29

Rückblick +
EinführungHistorische
ArbeitenBotnet
SimulationDrive-by-
Download
Simulator

MALSim

Zusammen-
fassungEigener
Ansatz

MALSim ^{[2][5][6]}

Mobile Agent Malware Simulator

Rafał Leszczyna, Igor Nai Fovino, Marcelo Masera (2007)

*European Commission
Joint Research Centre*

19/29

Rückblick +
Einführung

Historische
Arbeiten

Botnet
Simulation

Drive-by-
Download
Simulator

MALSim

Zusammen-
fassung

Eigener
Ansatz

MALSim

Ziele

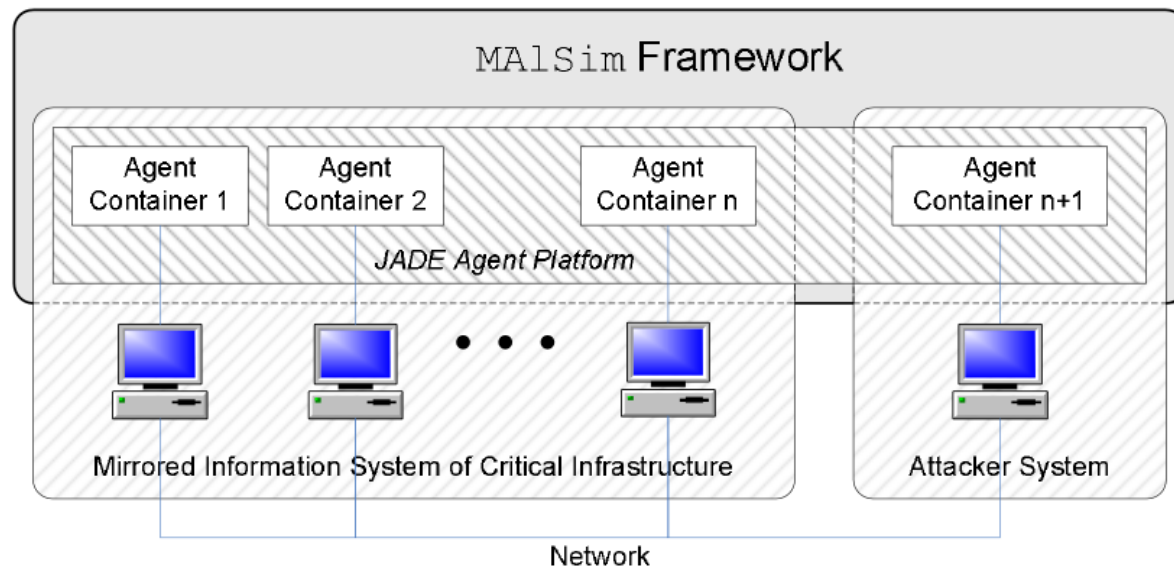
- Simulation von Malware
 - Ausbreitung
 - Verhalten

- Simulation im Kontext „Security of critical networked infrastructure“

MALSim

Umsetzung

- Simulation mit mobilen Agenten
- Mehrere Typen von Schadsoftware realisierbar (Würmer, Viren, ...)
- Spiegeln der realen Umgebung



Aus [2]

21/29

MALSim

Bewertung



- Berücksichtigt mehrere Arten von Malware
- Nahe an der Realität (durch 1:1 System-Abbildung)

- Skaliert nicht
- Nicht alle relevanten Ausbreitungswege werden berücksichtigt
- Interessante sekundäre Angriffsvektoren können nicht realisiert werden

22/29

Rückblick +
EinführungHistorische
ArbeitenBotnet
SimulationDrive-by Download
Simulator

MALSim

Zusammen-
fassungEigener
Ansatz

Zusammenfassung

	Skalierbar	Ausbreitungswege	Malwaretypen	Nutzerverhalten
Botnet Simulation	Ja	0	1	nein
DBD-Simulator	Ja	1	>1	ja, aber nicht simuliert
MALSim	Schlecht	>1 (keine mobilen Einheiten)	>1	nein
Eigener Ansatz	Ja	>1 (mit mobilen Einheiten)	>1	ja (simuliert)

Eigener Ansatz

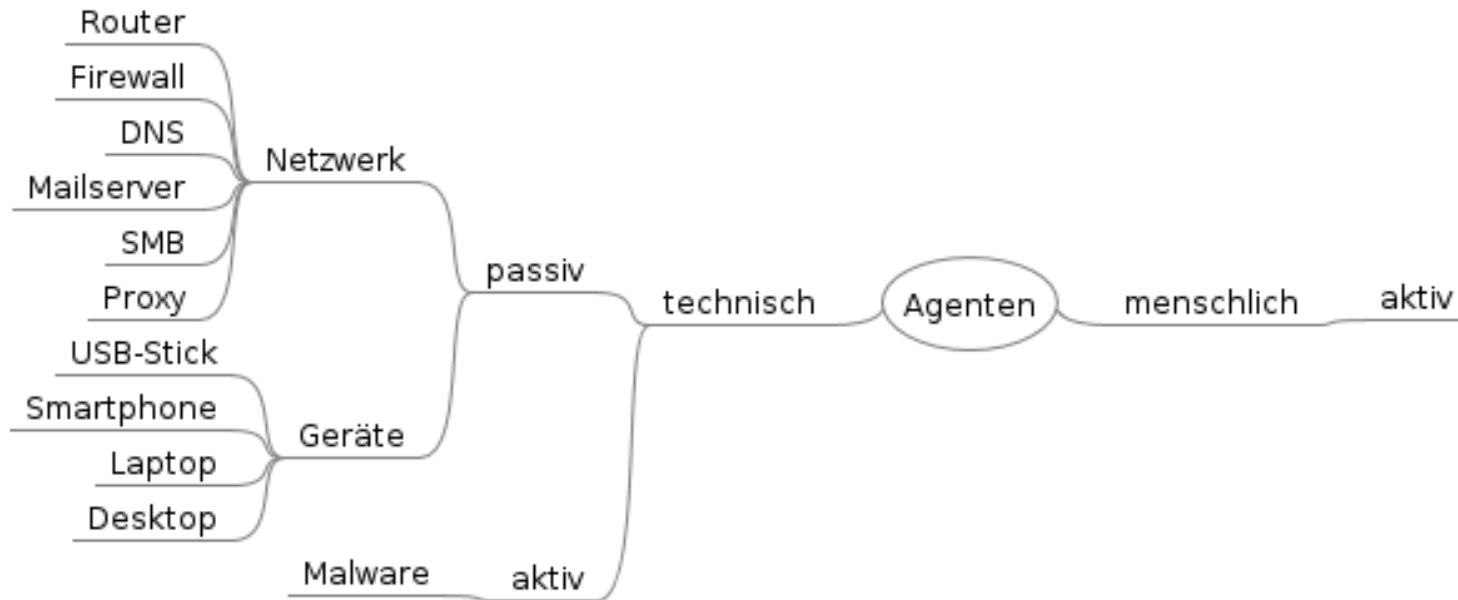
Multi Agenten Ausbreitungssimulation

Eigener Ansatz

- Ausbreitungssimulation mit Multi Agenten System
- Virtualisierung/Abbildung der zu testenden Umgebung
 - Netzwerkskans
 - Footprinting
- Simulation verschiedener Ausbreitungsmöglichkeiten
 - Exploits
 - Nutzer(fehl)verhalten
 - Mobile Geräte
- Ergebnisse verwenden für:
 - Vorsorge
 - Handlungsempfehlungen
 - Forensik

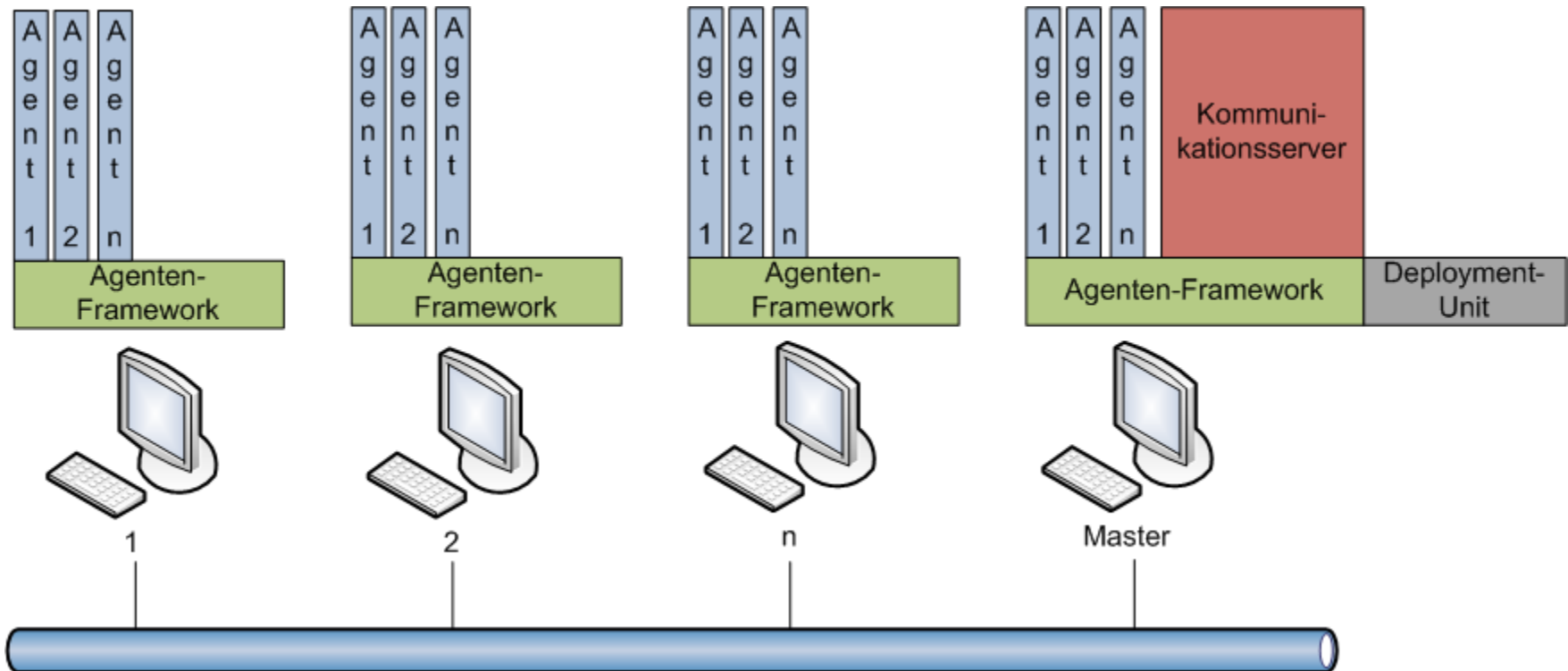
Eigener Ansatz

Architektur



Eigener Ansatz

Architektur



27/29

Rückblick +
EinführungHistorische
ArbeitenBotnet
SimulationDrive-by-
Download
Simulator

MALSim

Zusammen-
fassungEigener
Ansatz

Literaturverzeichnis

- [1] Paul Barford, Mike Blodgett:
Are Good Virus Simulators Still a Bad Idea, in *Network Security 1996(9):7–13*, 1996

- [2] Rafał Leszczyna, Igor Nai Fovino, Marcelo Masera:
MAISim – Mobile Agent Malware Simulator, 2007

- [3] Paul Barford, Mike Blodgett:
Toward Botnet Mesocosms, 2007

- [4] Matthew McDonald, James Ong, John Aycock, Heather Crawford, Nathan Friess:
A Lightweight Drive-by Download Simulator, 2009

- [5] Rafał Leszczyna, Igor Nai Fovino, Marcelo Masera:
MAISim Deployment, 2008

- [6] Rafał Leszczyna, Igor Nai Fovino, Marcelo Masera:
Malware Templates for MAISim, 2008

Internetquellen

[I1] VIRLAB, URL: <http://www.kklotz.de/html/virlab-screenshot.html> Datum: 06. Mai 2012

[I2] Emulab, URL: <http://www.emulab.net/> Datum: 06. Mai 2012

Vielen Dank für die Aufmerksamkeit

Fragen