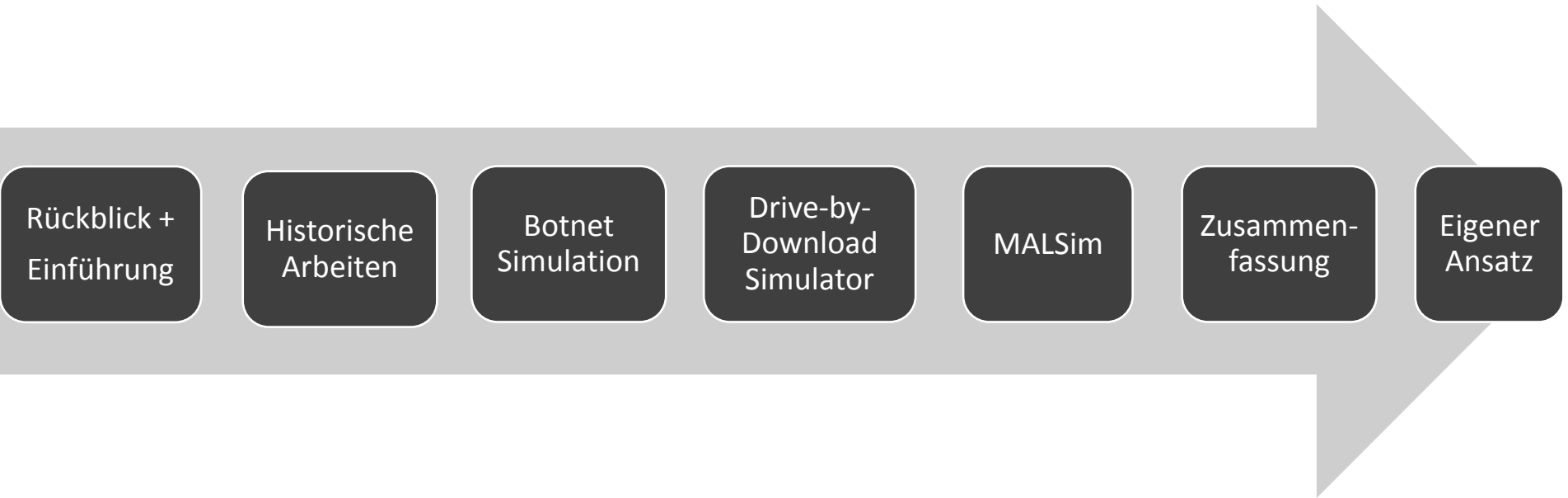
Simulation of malware propagation

André Harms

Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

Simulation of malware propagation



Rückblick

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

- Warum?

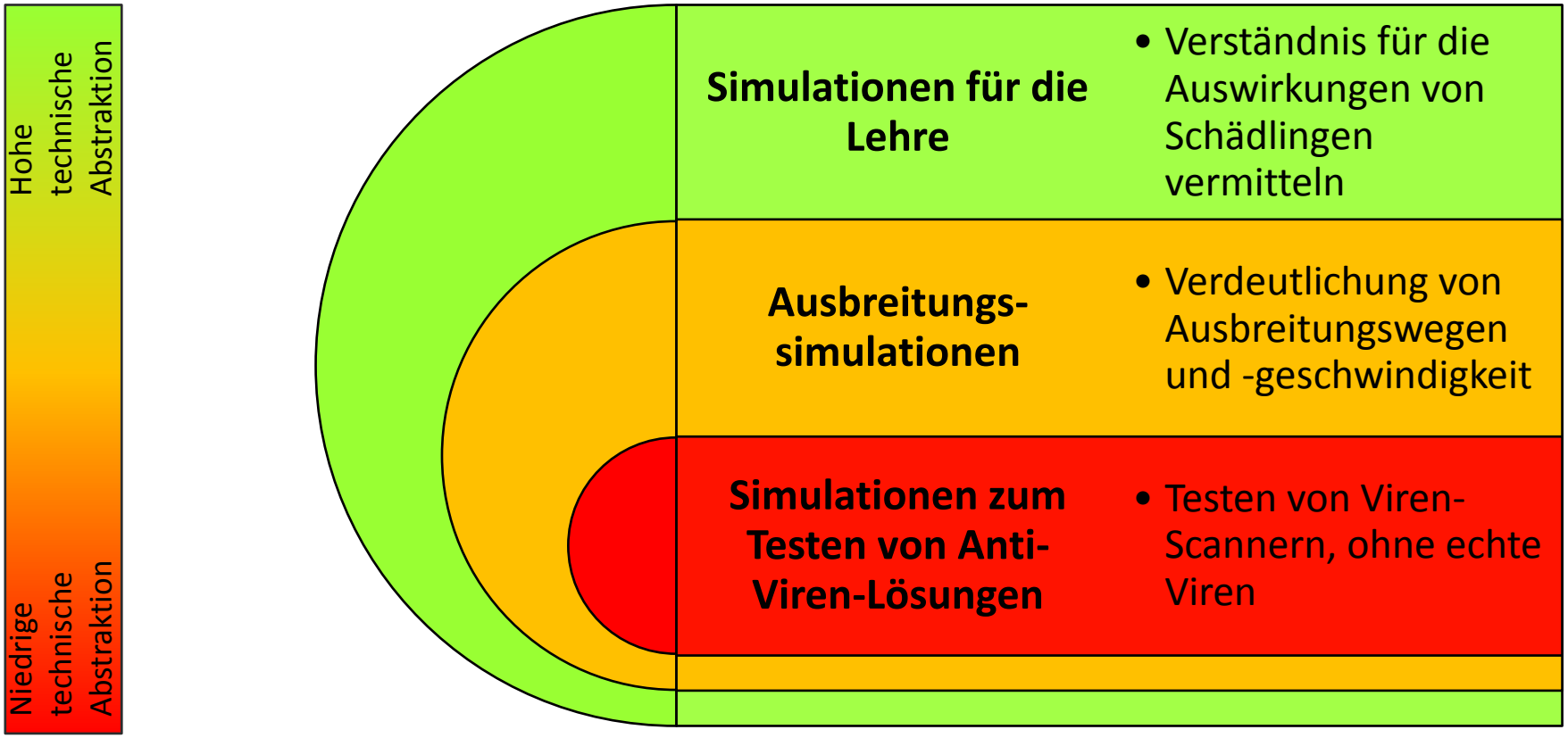
  Prävention, Handlungsempfehlungen, Forensik

- Ziel

  Ausbreitung von Schadsoftware simulieren

Einführung

- Kategorien von Simulationen[1][2]:



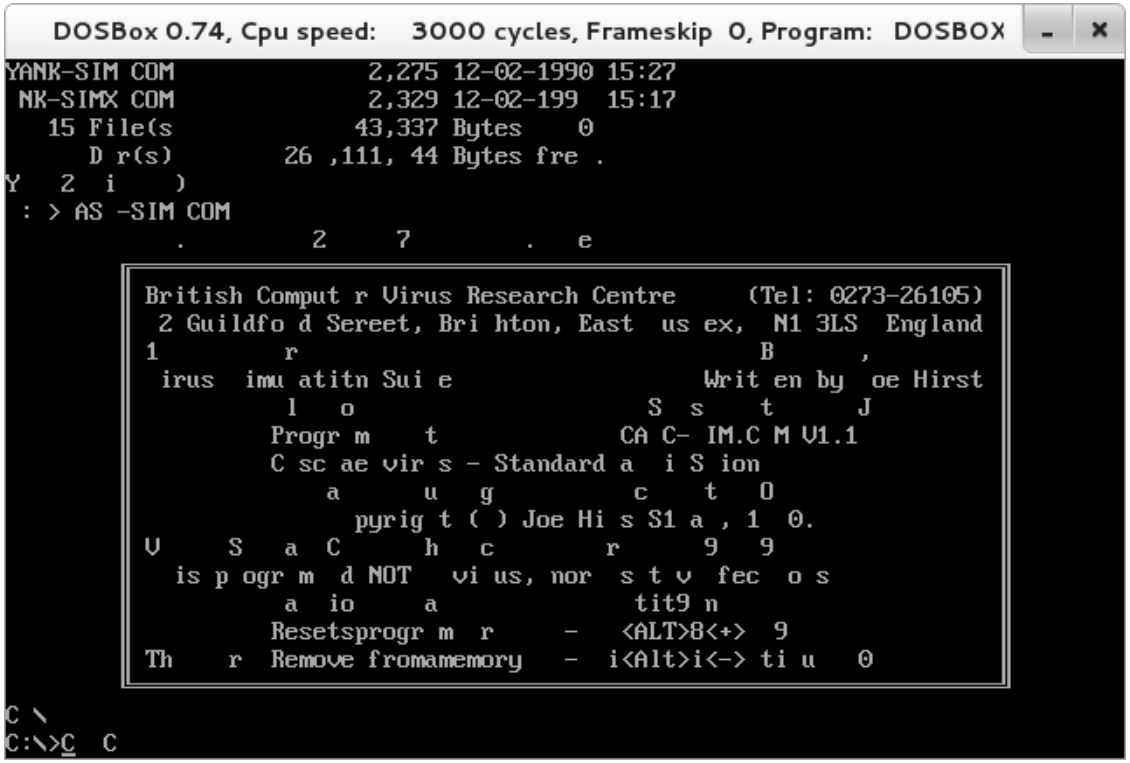
Historische Arbeiten

Verschiedene Simulationen kurz erläutert

Historische Arbeiten

Virus Simulation Suite

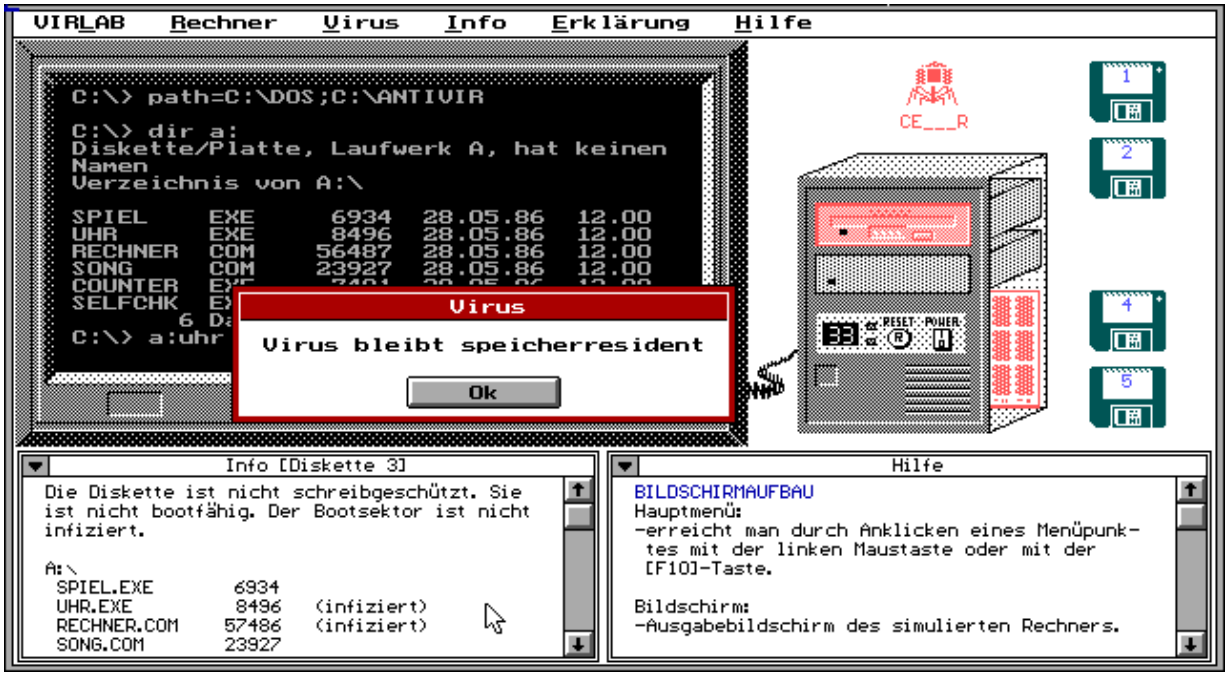
- Joe Hirst 1990
- Zur Lehre gedacht
- Simuliert das Verhalten / die Auswirkung einer überschaubaren Anzahl von Viren (13), z.B. Cascade-Virus



Historische Arbeiten

Virlab

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

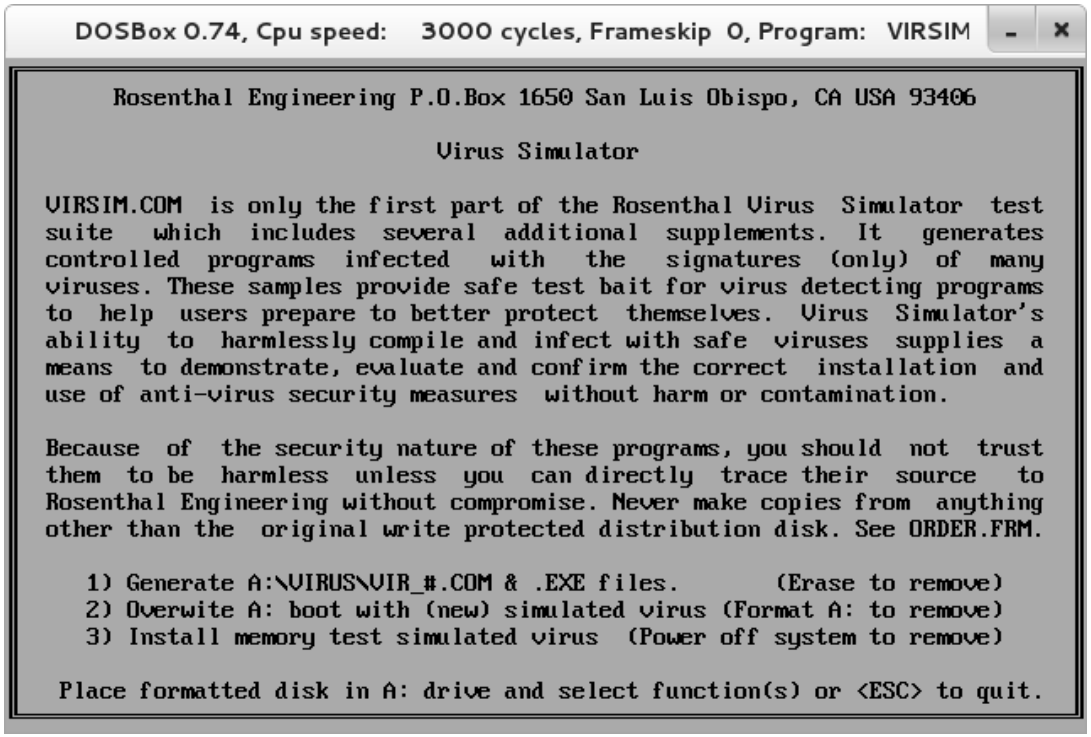


[I1]

Historische Arbeiten

Rosenthal's Virus Simulator

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



Toward Botnet Mesocosm[3]

Botnet Simulation

Paul Barford, Mike Blodgett (2007)

University of Wisconsin-Madison

Botnet Simulation

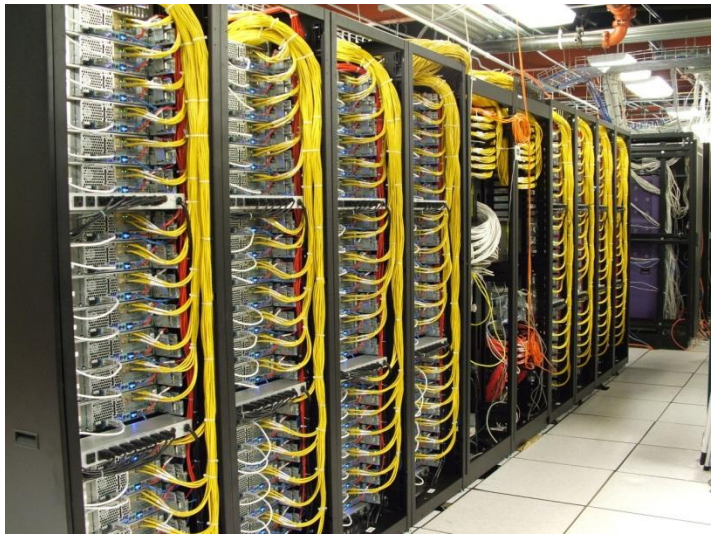
Ziele

- Verhalten von Botnets in Laborumgebung nachstellen
- Botnet Evaluation Environment (BEE)
- Umgebung soll sicher sein
- Realisitische 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)



[I2]

Botnet Simulation

Bewertung

- Vollständig virtualisiert

- Nahe an der Realität (Verwendung echter Schadsoftware)

- Verhaltensweise kann exakt beobachtet werden

- Funktioniert nur in Verbinung mit Emulab

- Spezialisiert auf eine Schädlingskategorie

- Nicht auf Ausbreitung spezialisiert

A Lightweight Drive-by Download Simulator [4]

Drive-By-Download Infektions-Simulation

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

University of Calgary

Drive-by-Download Simulator

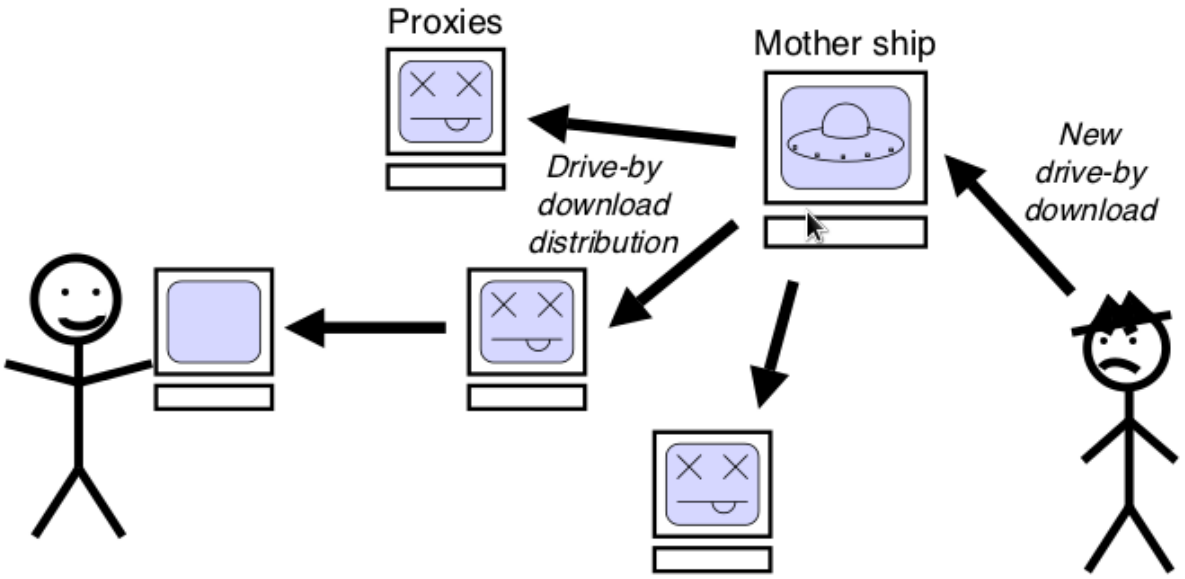
Ziele

- 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

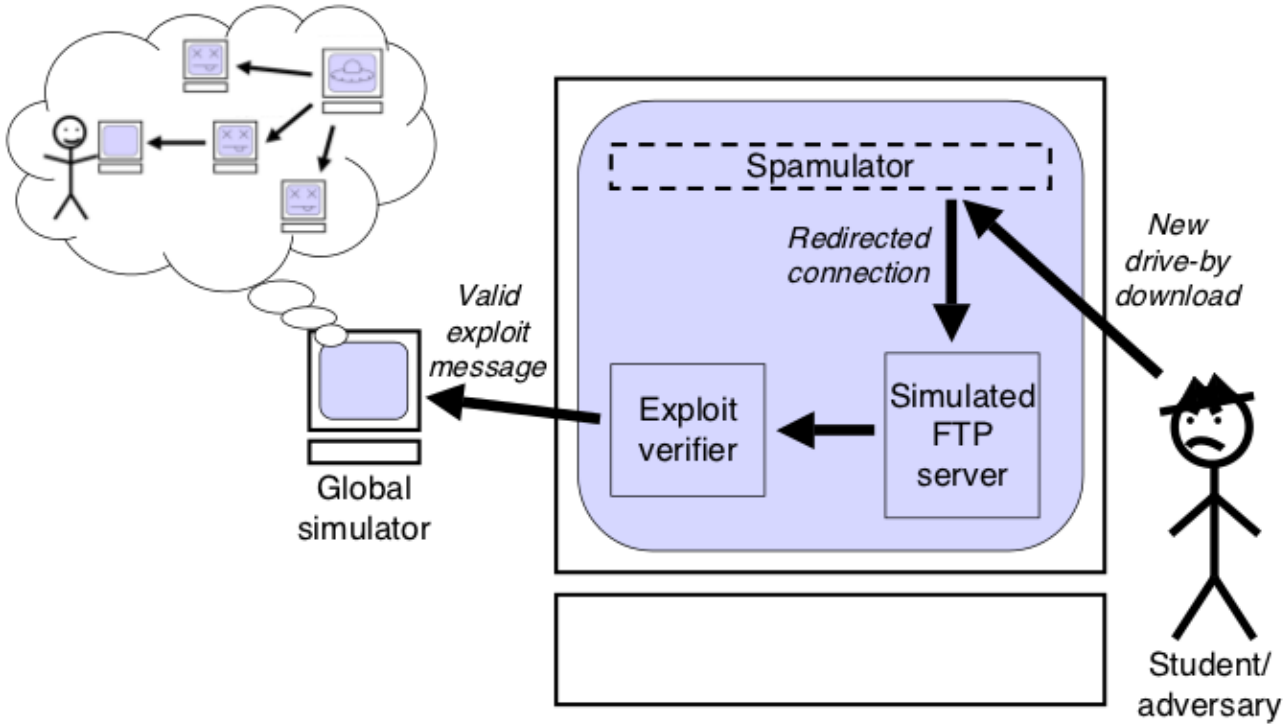
- Erweiterung von Spamulator



Aus [4]

Drive-by-Download Simulator

Umsetzung

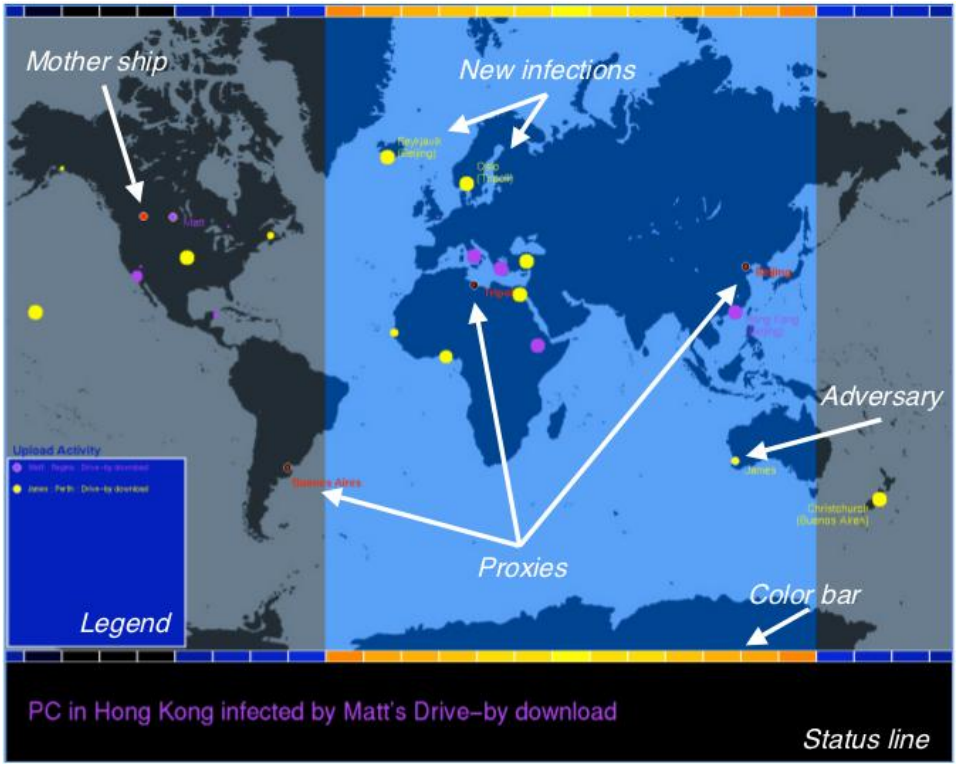


Aus [4]

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

Drive-by-Download Simulator

Umsetzung



Aus [4]

- „Global simulator“ aggregiert Simulationsergebnisse mehrerer Rechner

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.

MALSim [2][5][6]

Mobile Agent Malware Simulator

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

European Commission
Joint Research Centre

MALSim

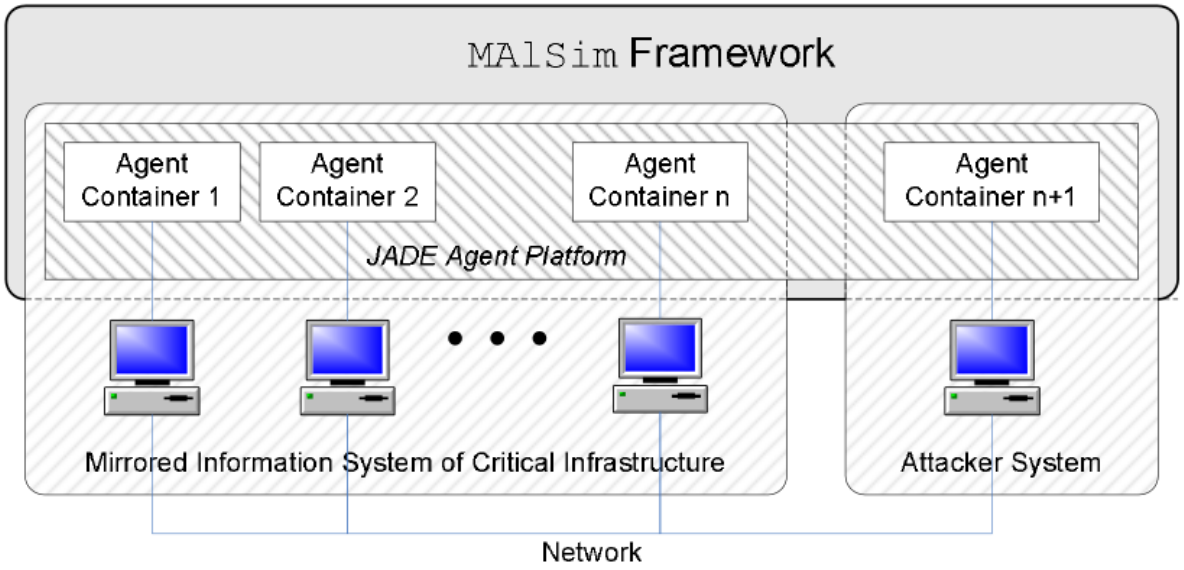
Ziele

- Simulation von Malware
  - Ausbreitung
  - Verhalten
- Simulation im Kontext „Security of critical networkted infrastructure“

MALSim

Umsetzung

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



Aus [2]

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

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

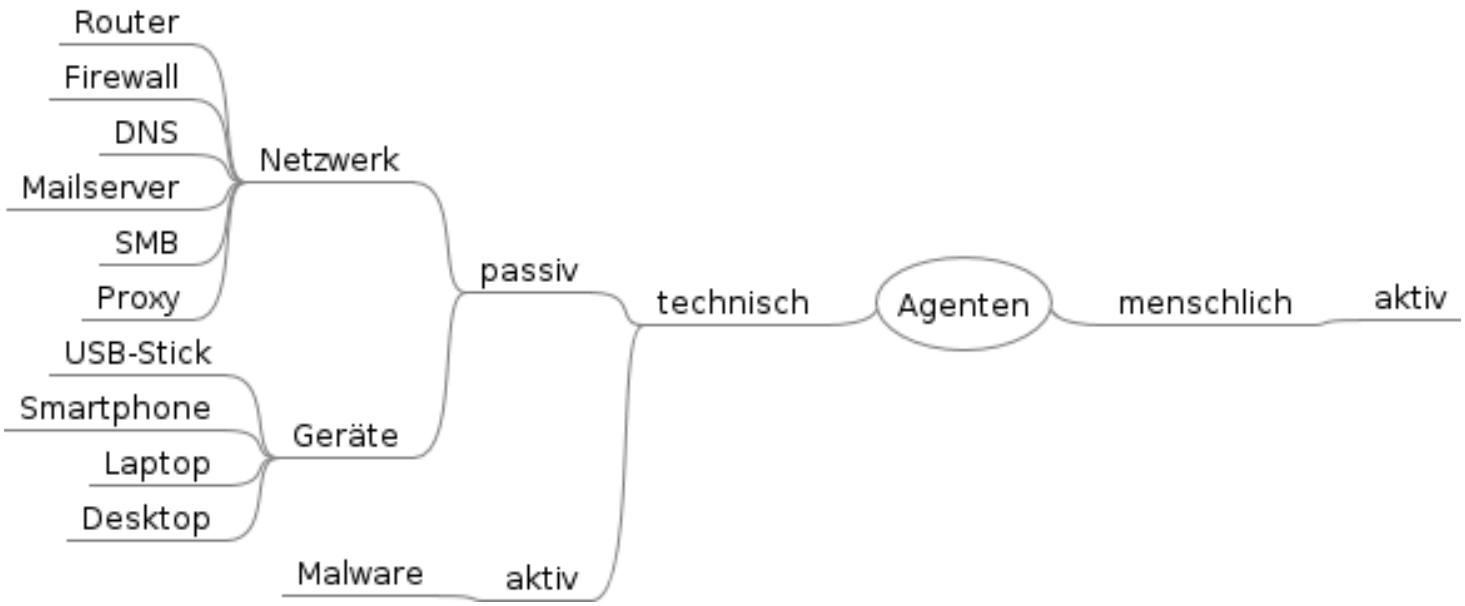
Multi Agenten Ausbreitungssimulation

Eigener Ansatz

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

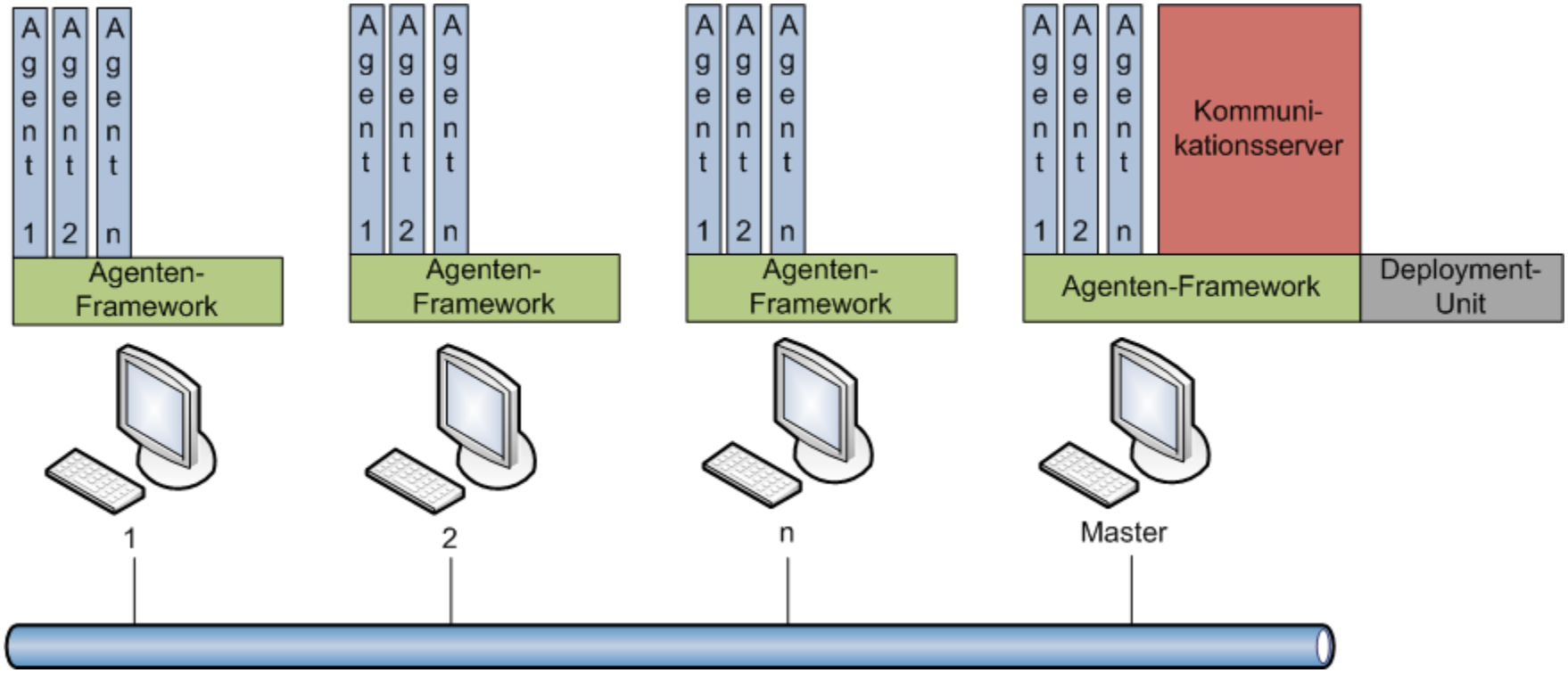
Eigener Ansatz

Architektur



Eigener Ansatz

Architektur



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:
MAlSim – 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:
MAlSim Deployment, 2008

[6] Rafał Leszczyna, Igor Nai Fovino, Marcelo Masera:
Malware Templates for MAlSim, 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