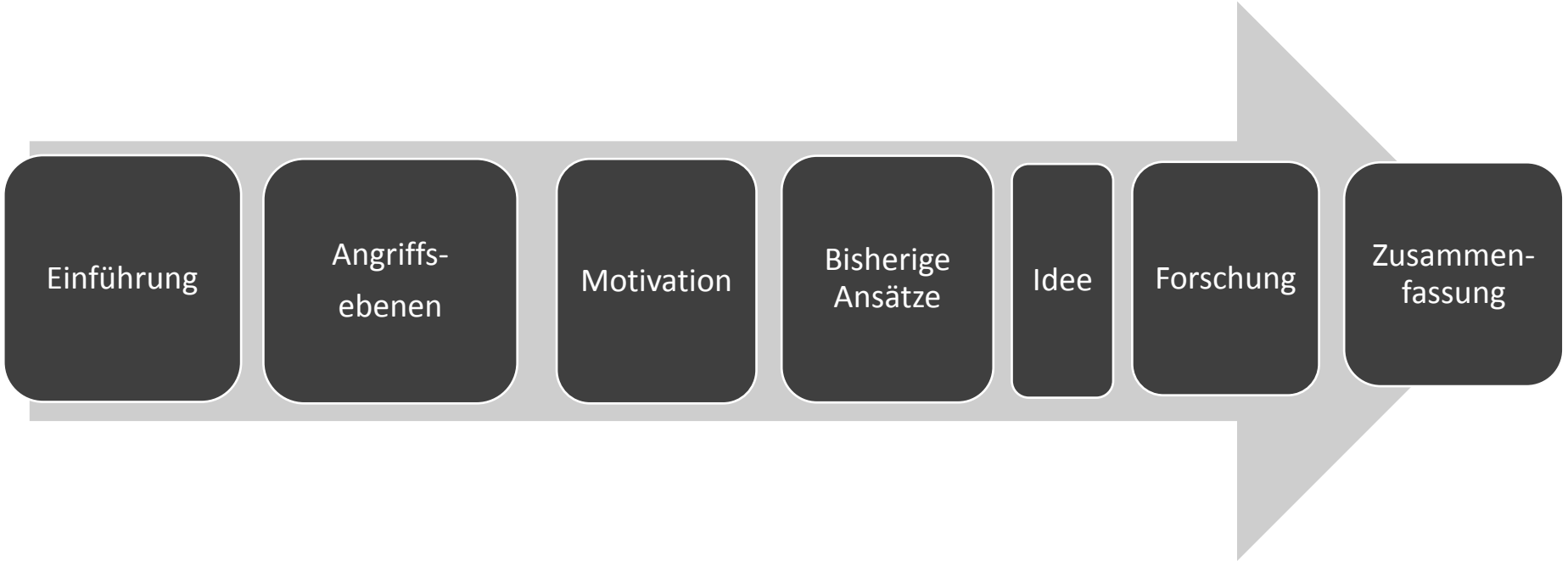
Simulation von Cyberangriffen

André Harms

Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

Simulation von Cyberangriffen

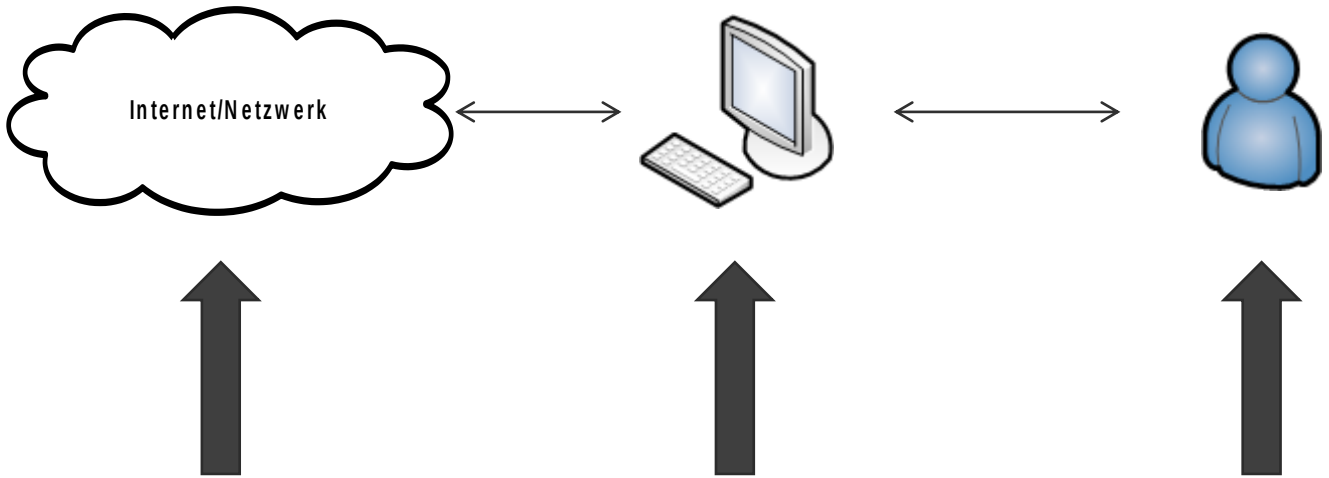


Einführung

- Was ist ein Cyberangriff?
  - Verschiedene Vorstellungen und Ausprägungen:
    - Industriespionage
    - Informationskrieg/Falschinformationen
    - Schädigung von Infrastruktur
    - Aber: alles mit Mitteln der IT
  - Cyberwar → Asymmetrischer Krieg [1] [11]
    - Kein Kräftegleichgewicht
    - Angreifer schwer identifizierbar
  - Beispiele:
    - Angriff auf Estland (2007) durch russische Hacker [1] [2]:
      - Politisch motiviert
      - DDoS Attacken legten Notrufnummern und Banken lahm
    - Stuxnet [3]

Angriffsebenen

Einfache Darstellung:



Infrastruktur- u. Protokollangriffe, Daten abfangen

Angriffe auf Anwendungen und Programmlogik

Soziale Manipulation (Social Engineering)

Motivation

- Immer mehr Vernetzung von schützenswerten Systemen
- Häufung von Angriffen in jüngerer Vergangenheit [1][2][3][10]
- Bevölkerungsschutz:
  - Unterstützung bei Absicherung von kritischer Infrastruktur (z.B. Smart Grid)
  - Möglichkeiten zur Eindämmung erforschen
  - *“One of the problems related to the simulation of attacks against critical infrastructures is the lack of adequate tools for the simulation of malicious software (malware).”*
    Rafał Leszczyna et al. [5]
- Forensik
  - Wie konnte ein Angriff wahrscheinlich realisiert werden

Bisherige Ansätze

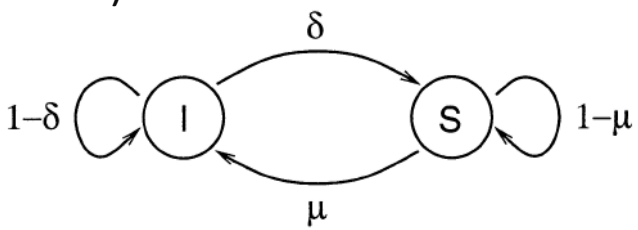
Ausbreitung von Schadsoftware

- Mathematische Modelle aus der Epidemiologie [4] [9]
  - Von biologischen Modellen abgeleitet
  - Ausbreitungsgeschwindigkeit vorhersagen anhand von:
    - Differentialgleichungen
    - Markow-Modelle

Bisherige Ansätze

Ausbreitung von Schadsoftware

- Beispiel (SIS-Modell):



Aus [4]

S → Susceptible

I → Infected

μ → Wahrscheinlichkeit, dass Knoten infiziert wird

δ → Wahrscheinlichkeit, dass Knoten wieder geheilt wird

Wobei:

μ => Konnektivität zu infiziertem Knoten und Wahrscheinlichkeit eine Infektion zu übertragen

Bisherige Ansätze

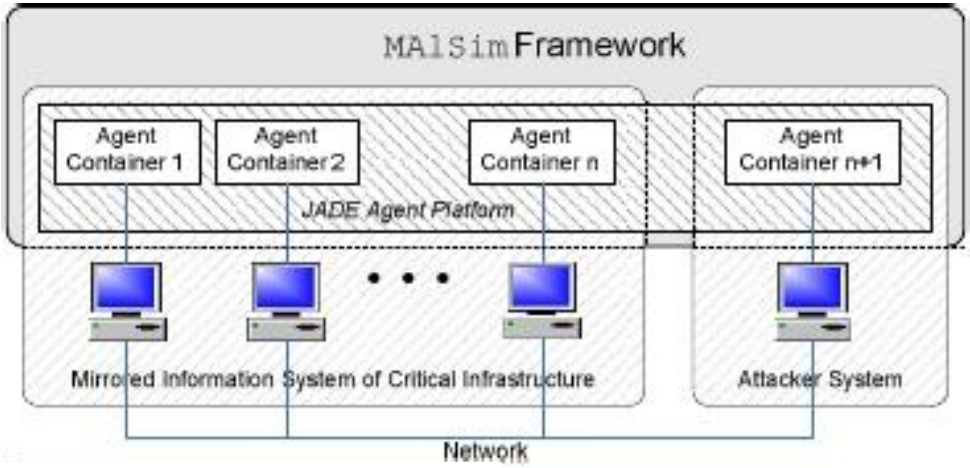
Ausbreitung von Schadsoftware

- Nachteile :
  - Berücksichtigt keine Patches (keine Immunisierung)
  - Keine geolokalen Informationen
  - Benutzerverhalten nur bedingt abgebildet

Bisherige Ansätze

Ausbreitung von Schadsoftware

- Beispiel: MAlSim (Mobile Agent Malware Simulator)[5]
  - Verschiedenartige Schadsoftware als mobile Agenten implementiert
  - Verwendung von JADE
  - Vorhandene Infrastruktur wird genutzt oder gespiegelt
  - Agent-Container als Ausführungsumgebung



Aus [5]

Bisherige Ansätze

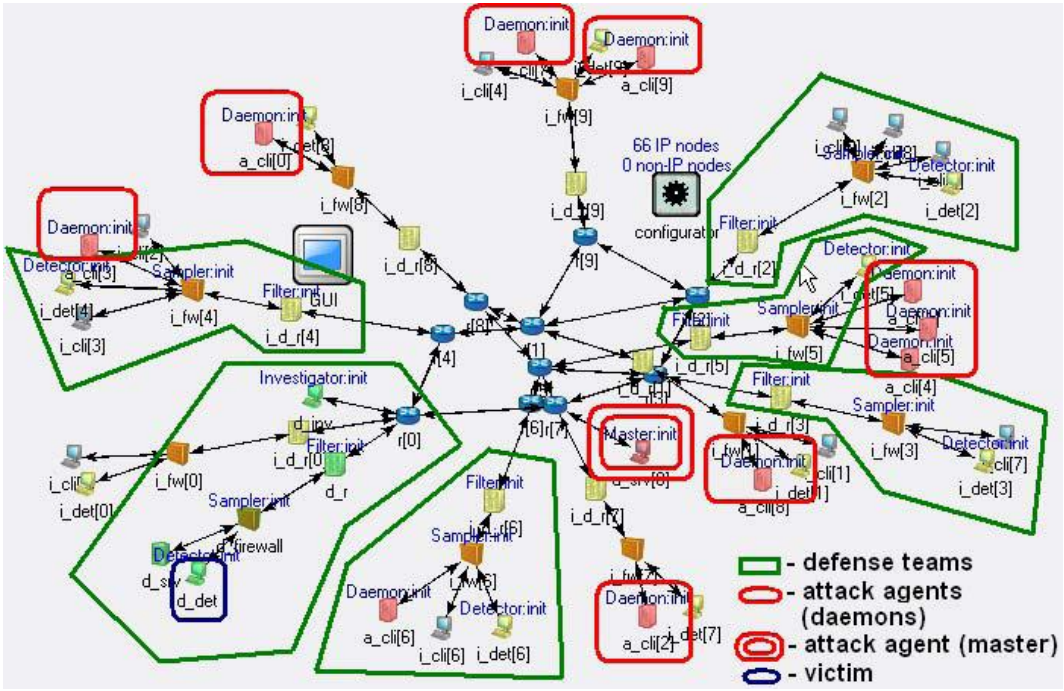
Ausbreitung von Schadsoftware

- Nachteile
  - Kopie eines Netzes muss erstellt werden
  - Benutzerverhalten findet keine Berücksichtigung
  - Beschränkung auf Geräte, die Ausführung von Agent-Container unterstützen

Bisherige Ansätze

Simulation von Netzwerkangriffen

- Beispiel: Ein Multi-Agenten Ansatz [8]
  - Simulation des Packet-Flows
    (Kompromiss zw. Skalierbarkeit und Genauigkeit)
  - Angreifer und Abwehrende als Agenten modelliert



Aus [8]

Bisherige Ansätze

Simulation von Netzwerkangriffen

- Nachteile
  - Benutzerverhalten nicht berücksichtigt
  - Nur aktive Angriffe werden betrachtet

Idee

- Simulation durch Multiagentensystem
  - Benutzerverhalten kann modelliert werden
  - Schadsoftware als Agenten
  - Geolokale Informationen können berücksichtigt werden
  - Implementierungsmöglichkeiten (beispielhaft):
    - SPADE2(Python)
    - JADE (Java)
    - eXAT (Erlang)
- Risiken
  - Betrachtungslevel muss definiert werden
  - Modellierung von Schwachstellen und Ausnutzung dieser
  - Aufbau von kritischer Infrastruktur muss bekannt sein

Forschung

Konferenzen & Magazine

- Konferenzen
  - **W**inter **S**imulation **C**onference (WSC) [I1]
  - Black Hat Conference [I2]
  - DEF CON in Las Vegas [I3]

- Magazine
  - Journal in computer virology

Forschung

Akteure

- Sicherheit/kritische Infrastruktur
  - BSI – Bundesamt für Sicherheit in der Informationstechnik [I4]
  - BKA – Bundeskriminalamt [I5]
  - BMI – Bundesministerium des Inneren [I6]
  - Fraunhofer-Einrichtung für Angewandte und Integrierte Sicherheit (AISEC) [I7]

- Cyberwar:

  John Arquilla, Ph.D.

- Schadsoftware

  Frederick B. Cohen, Ph.D.

Zusammenfassung

- Interessantes Themengebiet
- Interdisziplinär
- Aktualität und Interesse durch
  - Zunehmende Vernetzung
  - Konkrete Vorfälle
  - Bevölkerungsschutz

Literaturverzeichnis

[1] John J. Kelly, Lauri Almann:
eWMDs, In: Policy Review No. 152, 2008

[2] John Arquilla:
From Blitzkrieg to Bitskrieg: The Military Encounter with Computers, In: Communications of the ACM Volume 54 Issue 10, 2011

[3] Bundesamt für Sicherheit in der Informationstechnik:
Die Lage der IT-Sicherheit in Deutschland 2011, 2011, S.14-16, 28-29, 40-41

[4] Lora Billings a , William M. Spears b , Ira B. Schwartz:
A unified prediction of computer virus spread in connected networks, 2002

[5] Rafał Leszczyna, Igor Nai Fovino, Marcelo Masera:
MAlSim – Mobile Agent Malware Simulator, 2008

[6] S. G. Henderson, B. Biller, M.-H. Hsieh, J. Shortle, J. D. Tew, and R. R. Barton, eds.:
Cyber Attack Modeling and Simulation for the network analysis, In: Proceedings of the 2007 Winter Simulation Conference, 2007

[7] Claudia Eckert, Christoph Krauß, Peter Schoo:
Sicherheit im Smart Grid - Eckpunkte für ein Energieinformationsnetz, 2011

[8] Igor Kotenko:
Multi-agent Modelling and Simulation of Cyber-Attacks and Cyber-Defense for Homeland Security, In: Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, 2007

[9] Romualdo Pastor-Satorras Alessandro Vespignani:
Epidemic spreading in scale-free networks, 2008

[10] Bundesamt für Sicherheit in der Informationstechnik:
Lagebericht 1. Quartal, 2011, S. 10-11

[11] Bundesamt für Bevölkerungsschutz und Katastrophenhilfe :
Vierter Gefahrenbericht, 2011, ISBN-13: 978-3-939347-35-4, S. 44-60

Internetquellen

[I1] Winter Simulation Conference, URL: http://wintersim.org Datum: 06. November 2011

[I2] Black Hat Conference , URL: http://blackhat.com Datum: 07. November 2011

[I3] DEF CON, URL: http://defcon.org Datum 08. November 2011

[I4] BSI, URL: http://www.bsi.de Datum 10. November 2011

[I5] BKA, URL: http://bka.de Datum 10. November 2011

[I6] BMI, URL: http://www.bmi.bund.de Datum 10. November 2011

[I7] Fraunhofer AISEC, URL: http://www.aisec.fraunhofer.de Datum 10. November 2011

Vielen Dank für die Aufmerksamkeit

Fragen