Simulation of malware propagation

a multi-agent approach

André Harms

Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

Inhalt

Rückblick
- Projekt 1

Aktuell
- Projekt 2

Masterarbeit
- Ziele
- Vorgehen
- Risiken

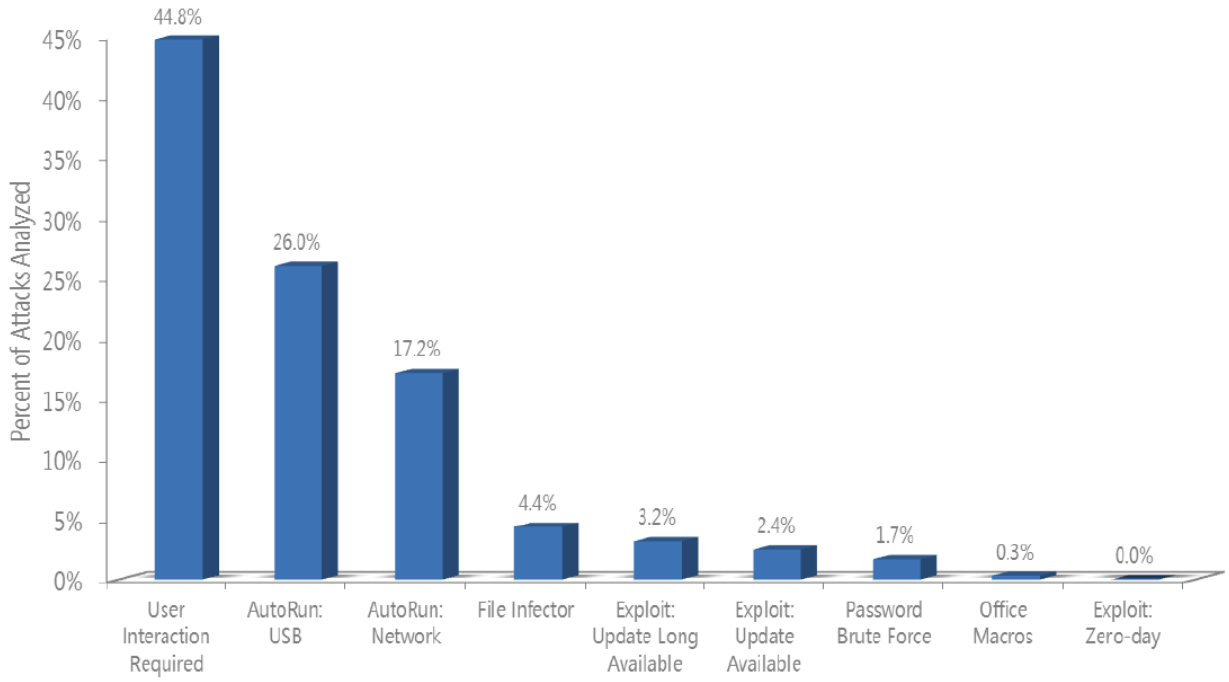
Rückblick

Projekt 1

Rückblick

Projekt 1 - Ausbreitungssimulation von Schadsoftware

Malware-Propagation Varianten (2011)

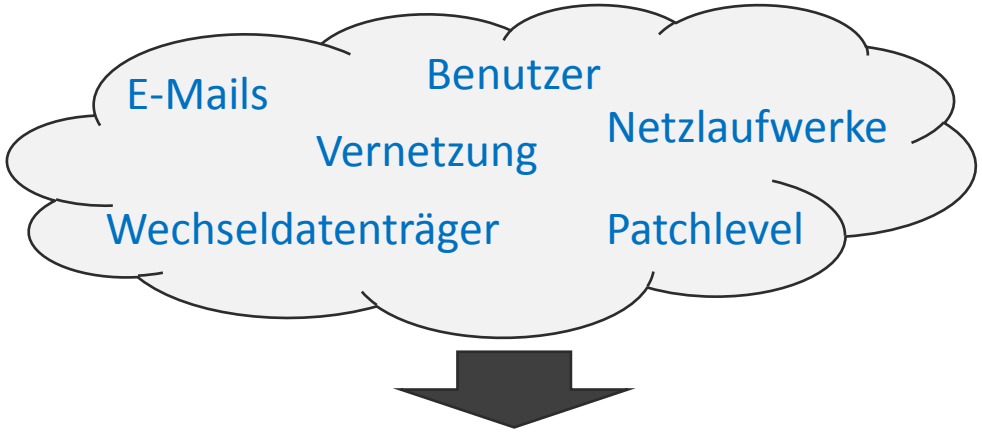


Aus [1]

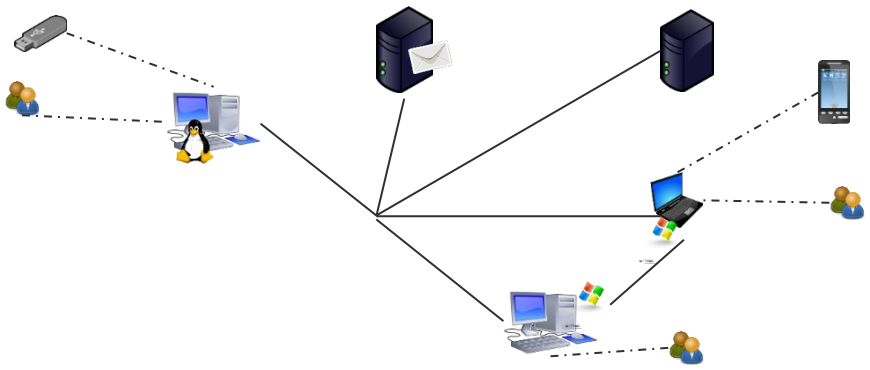
Rückblick

Projekt 1 - Ausbreitungssimulation von Schadsoftware

- Ermitteln relevanter Faktoren zur Ausbreitung



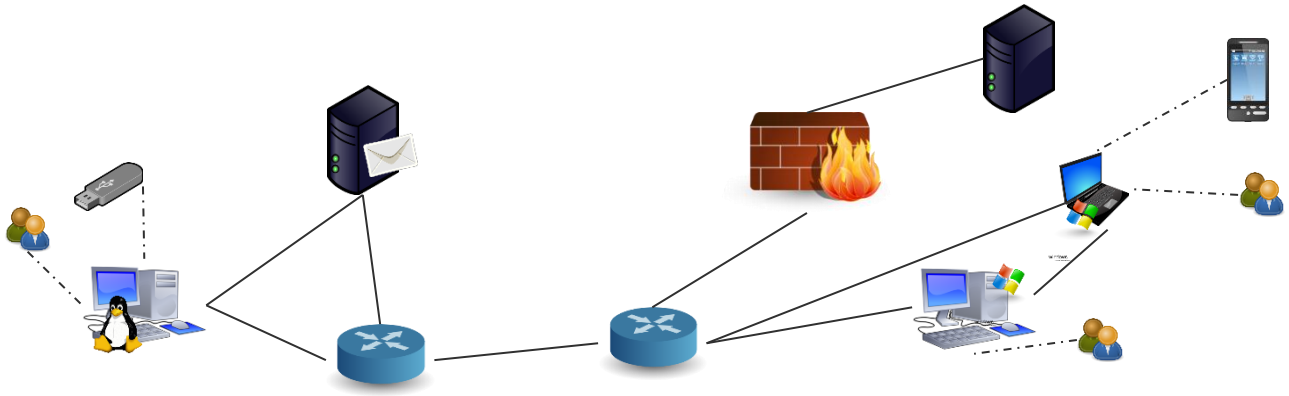
- Agentenbasierter Ansatz



Rückblick

Projekt 1 - Ausbreitungssimulation von Schadsoftware

- Berücksichtigung relevanter Kommunikationsknoten

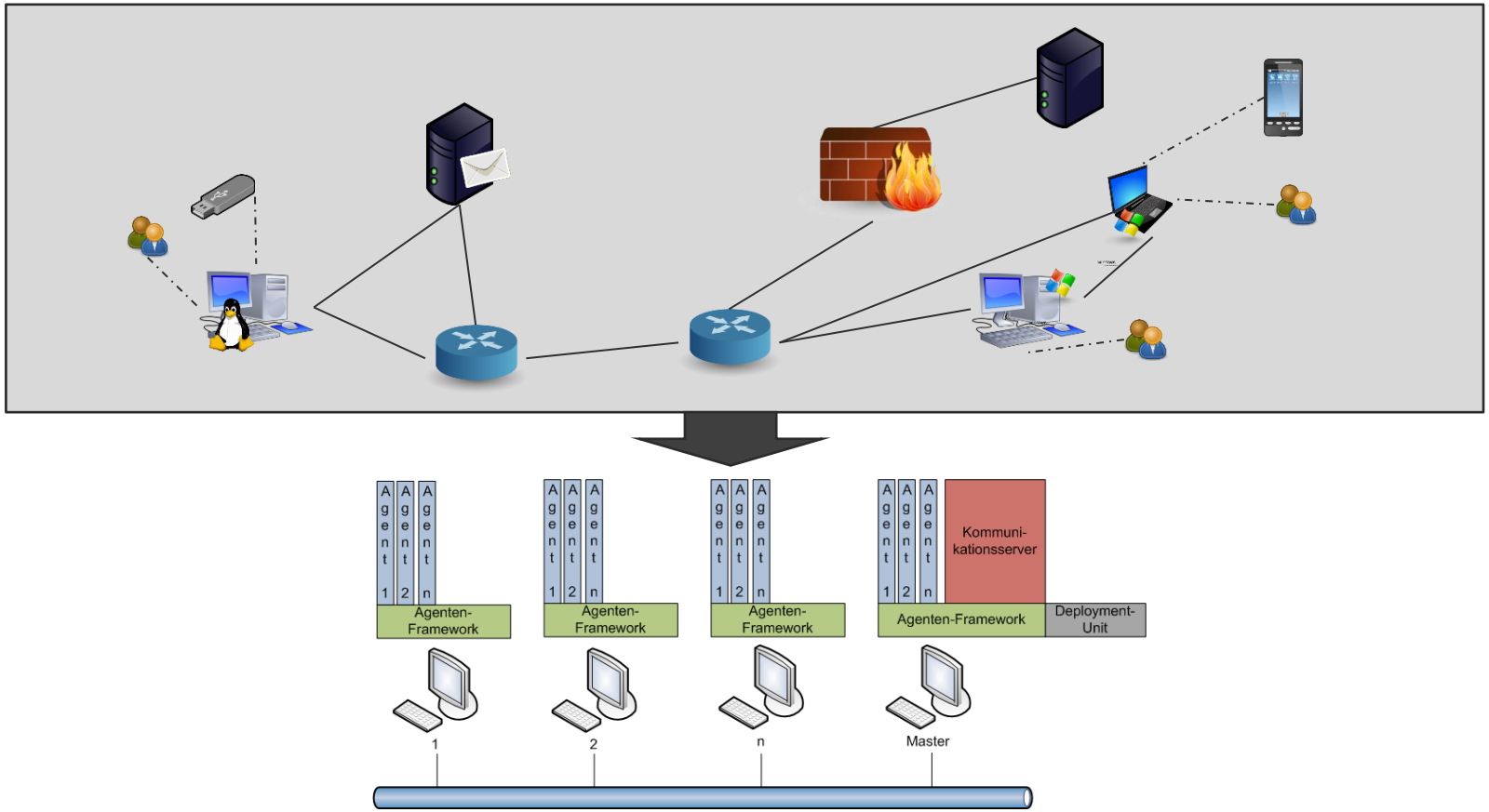


→ OSI Layer 3+4 sind relevant, müssen allerdings nicht detailliert betrachtet werden

Rückblick

Projekt 1 - Ausbreitungssimulation von Schadsoftware

- Berücksichtigung relevanter Kommunikationsknoten



Rückblick

Projekt 1 - Ausbreitungssimulation von Schadsoftware

- Sinnvolle Vorgehensweise -> Simulation in 3 Schritten:

1. Information Gathering

   Möglichst automatisches Sammeln nötiger Informationen

   (Bachelorarbeit Robert Krauß, Schnittstellen bestehen)

2. Simulation

   Ausbreitung in simulierter Umgebung beobachten

3. Auswertung

   Ereignisse auf Kausalität und Wirkung untersuchen

Aktuell

Projekt 2

Aktuell

Projekt 2

- Experimentierumgebung
  - Umsetzung von Agenten und Verhalten abschließen (insbesondere Cloudstorage)
  - Routingprotokoll für virtuelle Umgebung

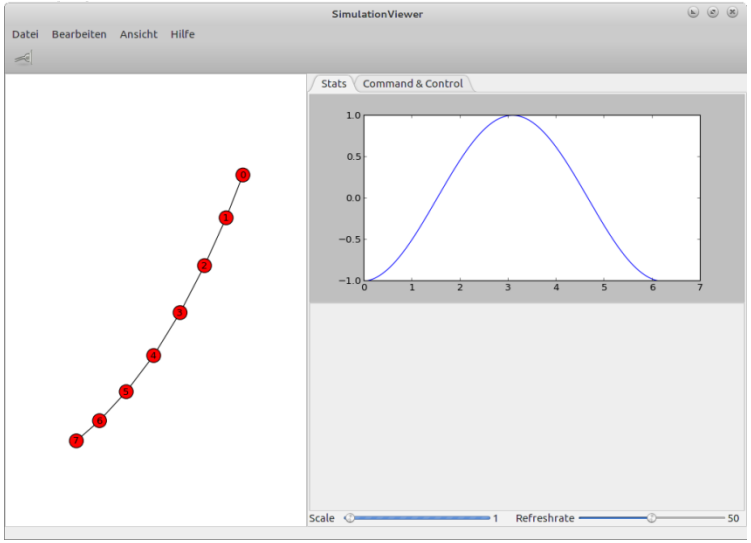
- Visualisierung und Steuerung laufender Simulation
  - Darstellung von Infektionsraten, Aktivitäten, etc.
  - Pausieren der Simulation, Geschwindigkeitssteuerung, etc.
  - Ändern der Simulationsumgebung zur Laufzeit

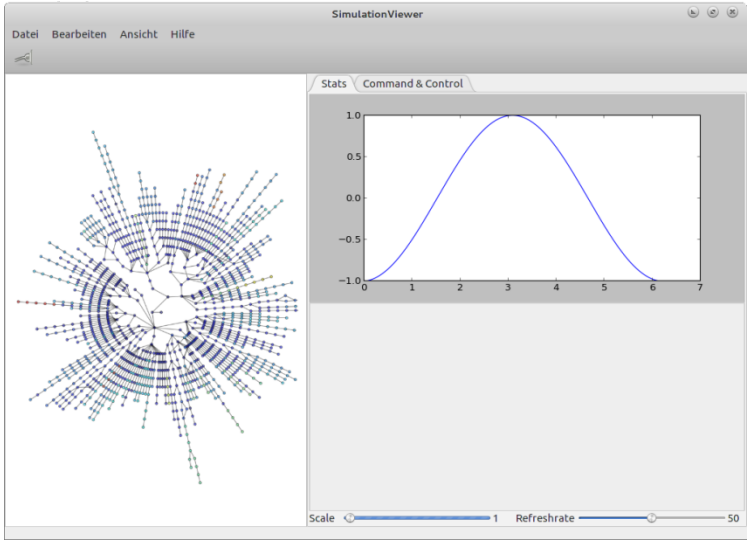
Aktuell

Projekt 2

Visualisierung und Steuerung laufender Simulation *(Work in Progress)*

Darstellung von Infektionsraten, Aktivitäten, etc.





Aktuell

Projekt 2

- Persistieren von Ereignissen zum nachträglichen Auswerten
  - Zentral vs. dezentral
  - GUI?

- Plausibilisieren der Simulation:

  Vergleich von Simulationsergebnissen mit empirischen Daten

  (Zusammenarbeit mit AV-Herstellern, Verwenden bekannter Daten – z.B. W32.Stuxnet Dossier [2])

Masterarbeit

Ziele

Masterarbeit

Ziele

„Impact of connectivity density on malware propagation“

Genaue Fragestellung

- Wie beeinflusst Dynamik das Ausbreitungsverhalten?
  - Nutzung von Cloudspeicher
  - Wechseldatenträger
  - BYOD (Bring Your Own Device)
- Welchen Einfluss hat die Valenz von Knoten?
- Welchen Einfluss hat der Knotentyp?
- Kann man praktische Empfehlungen ableiten?

Masterarbeit

Vorgehen

Masterarbeit

Vorgehen

- Empirisches Vorgehen
  - Abbilden eines Unternehmens mit mehreren Standorten (>500 Knoten)
    Aus realen Daten
    (Fallback: nach Watts and Strogatz model; Graph mit Small-World-Eigenschaften [2])
  - Malwareagenten entwerfen mit verschiedenen Ausbreitungsvektoren
    (beispielsweise: Mail, Binary Planting, Drive-by Download)
  - Mehrere Simulationsdurchläufe mit unterschiedlichen Einstellungen
    - Dynamik reduzieren/entfernen
    - Cloudfunktionen deaktivieren

Masterarbeit

Vorgehen

- Metriken
  - Infektionsrate (Neu-Infektionen/*t*)

    Wie viele neue Infektionen finden pro Zeiteinheit statt
  - Replikationshäufigkeit

    Wie viele Infektionen gehen von einem Knoten aus
  - Durchsetzung

    Prozentuale Bestimmung der Gesamtinfektionen
  - Infektions-Distanz

    Über wie viele Knoten breitet sich Malware im Mittel aus

Masterarbeit

Vorgehen

- Metriken
  - Valenz

    Anzahl Nachbarknoten
  - Zusammenhangszahl

    Kleinste Anzahl von zu entfernenden Kanten, um Zusammenhang zu zerstören (Inselbildung → Bottlenecks)

Masterarbeit

Risiken

Masterarbeit

Risiken

- Daten für Plausibilisierung unzureichend

- Ergebnisse lassen sich u.U. nicht generalisieren
  (Repräsentativität der simulierten Umgebung?)

Literaturverzeichnis

[1] Microsoft:
Microsoft Security Intelligence Report Volume 11, 2011

[2] Nicolas Falliere, Liam O Murchu, and Eric Chien - (Symantec Corp.)
W32.Stuxnet Dossier, 2011

[3] Watts, Duncan J.; Strogatz, Steven H.:
Collective dynamics of `small-world' networks*, in Nature, Volume 393, Issue 6684, 440-442,* 1998

Vielen Dank für die Aufmerksamkeit