TRUDIE
Trust Relations in Underground IT Economies

Gilbert Wondracek, gilbert@seclab.tuwien.ac.at , 18.10.2011

Worum geht es?

Cybercrime, Hacker, Malware & Co.

- Themen ständig präsent
- Bisher nur wenig wissenschaftlich untersucht
- Es gibt z.B. Online-Marktplätze für
  - Gestohlene Kreditkartendaten
  - Gestohlene Identitäten
  - Schadsoftware (Bots, Würmer)
  - Dokumente, Drogen, Waffen, …
  - Durch Suchmaschinen leicht zu finden
  - Eigene Währungen, eigene „Polizei“, Treuhand, ...

Ziele

- Untersuchen von Foren & Chats
- Was wir wissen wollen:
  - Modus operandi der Verbrecher
  - Güter, Preise, etc. (automatisch) ermitteln
  - Welche Aktoren und Rollen gibt es überhaupt?
  - Wie sehen die Businessmodelle aus?
  - Wie kann man „stören“, wo sind Schwachstellen?

Milestones

- Start im Oktober 2009 mit Industriepartner Ikarus Software GmbH als FIT-IT Projekt
- Intelligente Crawler zum Sammeln von Daten erstellt (IRC, Foren)
- Machine Learning und AI zum Klassifizieren und Sortieren der Daten
  - z.B. „Ist Kreditkartenbetrug? Ja / Nein“
- Disruption Framework in Entwicklung

Ergebnisse

- Akademische Auswertung
  - >10 wissenschaftliche Publikationen
  - 4 Diplomarbeiten / Dissertationen
- Auch Projektpartner profitiert von Ergebnissen (neue Produkte usw.)
- Kooperationen / Einladungen diverser Partner (Polizeiorganisationen, Industrie)
  - → Neue Möglichkeiten für Forschung

Resümee

- FIT IT Projekt TRUDIE
- Untersucht Underground Economy
- Wissenschaftlich erfolgreich, Impulse für Industriepartner
- Freiheiten im Projekt erlauben uns flexible Forschung, bessere Ergebnisse
- Geringer bürokratischer Overhead → effektive Forschung

Gilbert Wondracek, gilbert@seclab.tuwien.ac.at