secure
sba-research.org

COMET
Competence Centers for
Excellent Technologies

Aktuelle Forschungsergebnisse

Edgar Weippl

SBA Research

bmvit
Bundesministerium
für Verkehr,
Innovation und Technologie

bmwfj
Bundesministerium für
Wirtschaft, Familie und Jugend

Christian Doppler
Forschungsgesellschaft

FFG

wirtschafts
agentur
wien

zit
Die Technologieagentur
der Stadt Wien

Aktuelle Forschungsergebnisse

secure
sba-research.org
COMET
Competence Centers for Excellent Technologies

- Dropbox (Usenix 2011)
  - Sichere Software-Entwicklung
  - Vertrauen dem Client
- Facebook (ACSAC 2011)
  - Unklare Privacyeinstellungen und Zugriffskontrolle
  - Social Engineering
- WhatsApp (NDSS 2012)
  - Protokollsicherheit, “eigene” Erfindungen

Datenspeicherung

secure sba-research.org

COMET Competence Centers for Excellent Technologies

Einfache Systeme

- FTP, WebDAV, NFS

Ein wenig komplexer

- Delta sync
- P2P

Komplexe Systeme

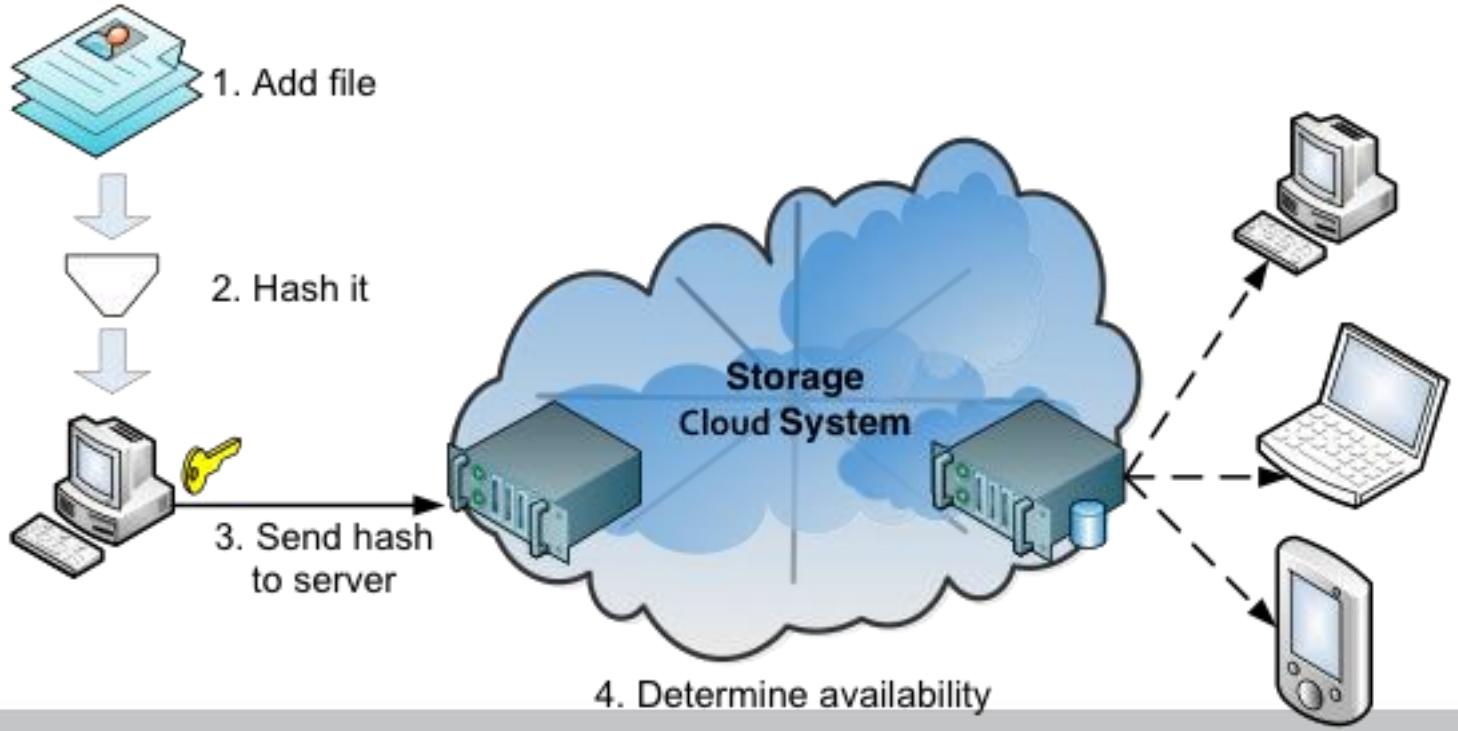
Name	Protocol	Encrypted transmission	Encrypted storage	Shared storage
Wuala	Cryptree	yes	yes	yes
SpiderOak	proprietary	yes	yes	yes
Ubuntu One	u1storage	yes	no	yes
Dropbox	proprietary	yes	no	yes

- Amazon Simple Storage System (S3)
- Data Deduplication, SHA-256
- Datei 4 MB Blöcke geteilt
- (server-seitiger) AES-256

- 25 Millionen Benutzer
- >100 Milliarden Files
- 1 Million neue Files alle 5 Minuten

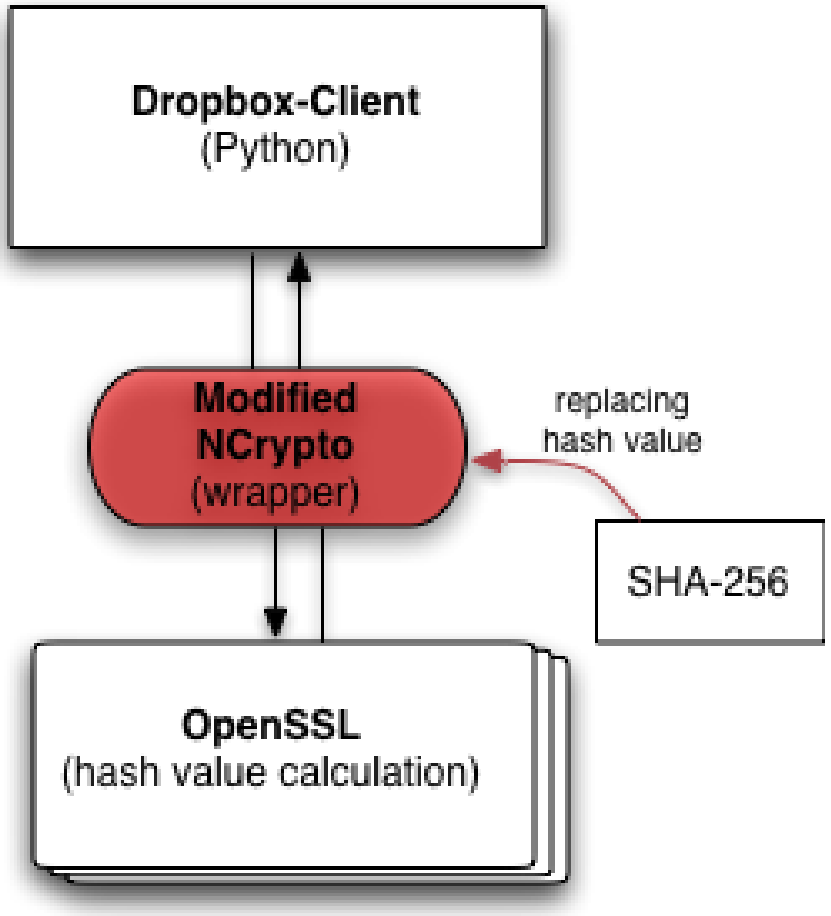
Data Deduplication

- Auf dem Server
  - Datei nur einmal gespeichert
  - Spart Speicherplatz
- Auf dem Client
  - Hash-Wert
  - Minimiert Datenübertragung



Angriffe

- Hash Manipulation
- Stehlen der Host ID
- Direkte Up-/Download
  - Uploads ohne Linking
  - Einfache HTTPS Anfragen https://dl-clientXX.dropbox.com/store



Evaluierung

secure sba-research.org

COMET Competence Centers for Excellent Technologies

Löschen von Chunks

- Zufallsdaten
- Versteckter Upload: min 4 Wochen
- Regulärer Upload: > 6 Monate

Beliebte Dateien auf Dropbox:

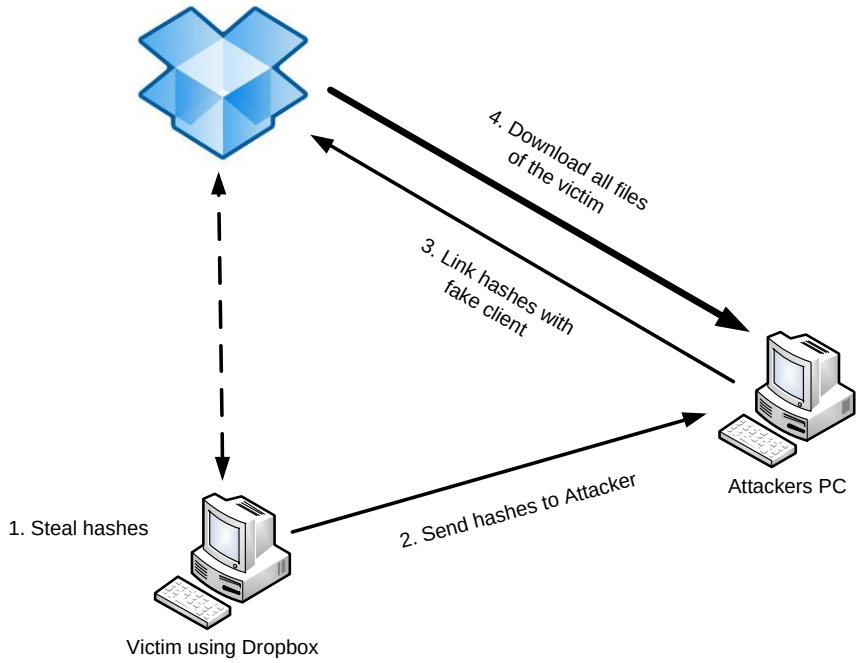
- thepiratebay.org Top 100 Torrent Dateien
- Download “legaler” Inhalte (.sfv, .nfo, ...)
- 97 % (n = 368) waren verfügbar
- 20 % der Torrents waren jünger als 24

Interpretation:

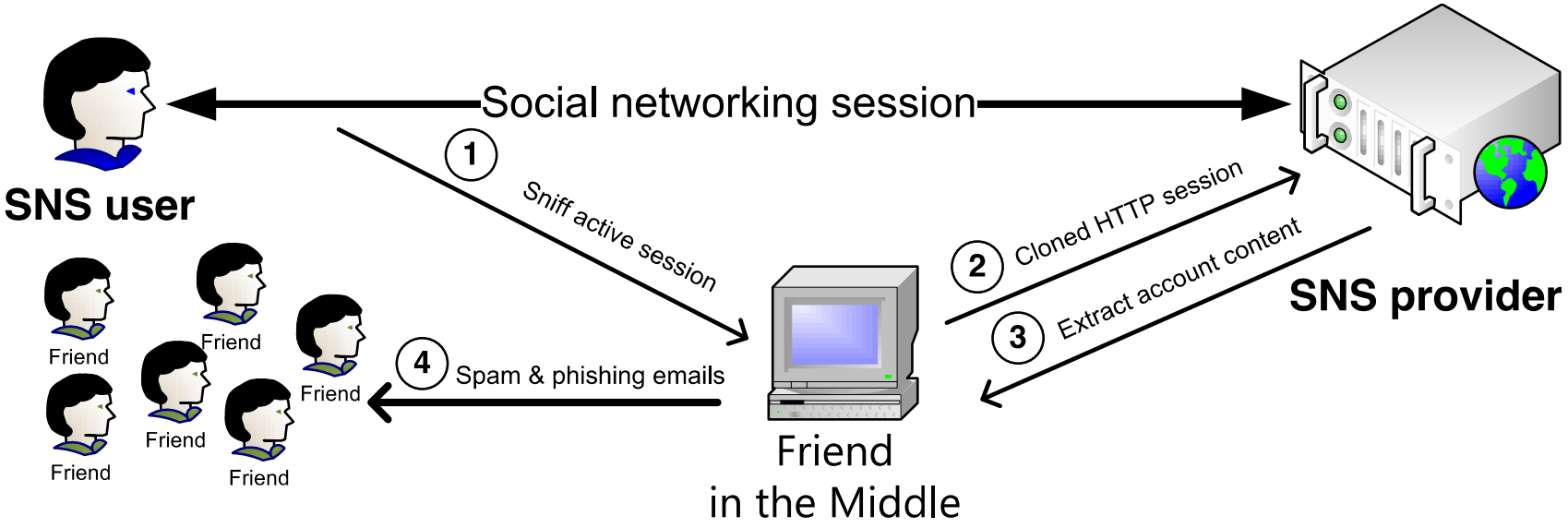
- Zumindest eine Kopie liegt auf Dropbox

Lösung

- Dropbox behebt Schwachstellen
  - HTTPS Up-/Download Angriff
  - Host ID verschlüsselt
  - Keine accountübergreifende Deduplication
    - Proof of ownership
    - Take down notice

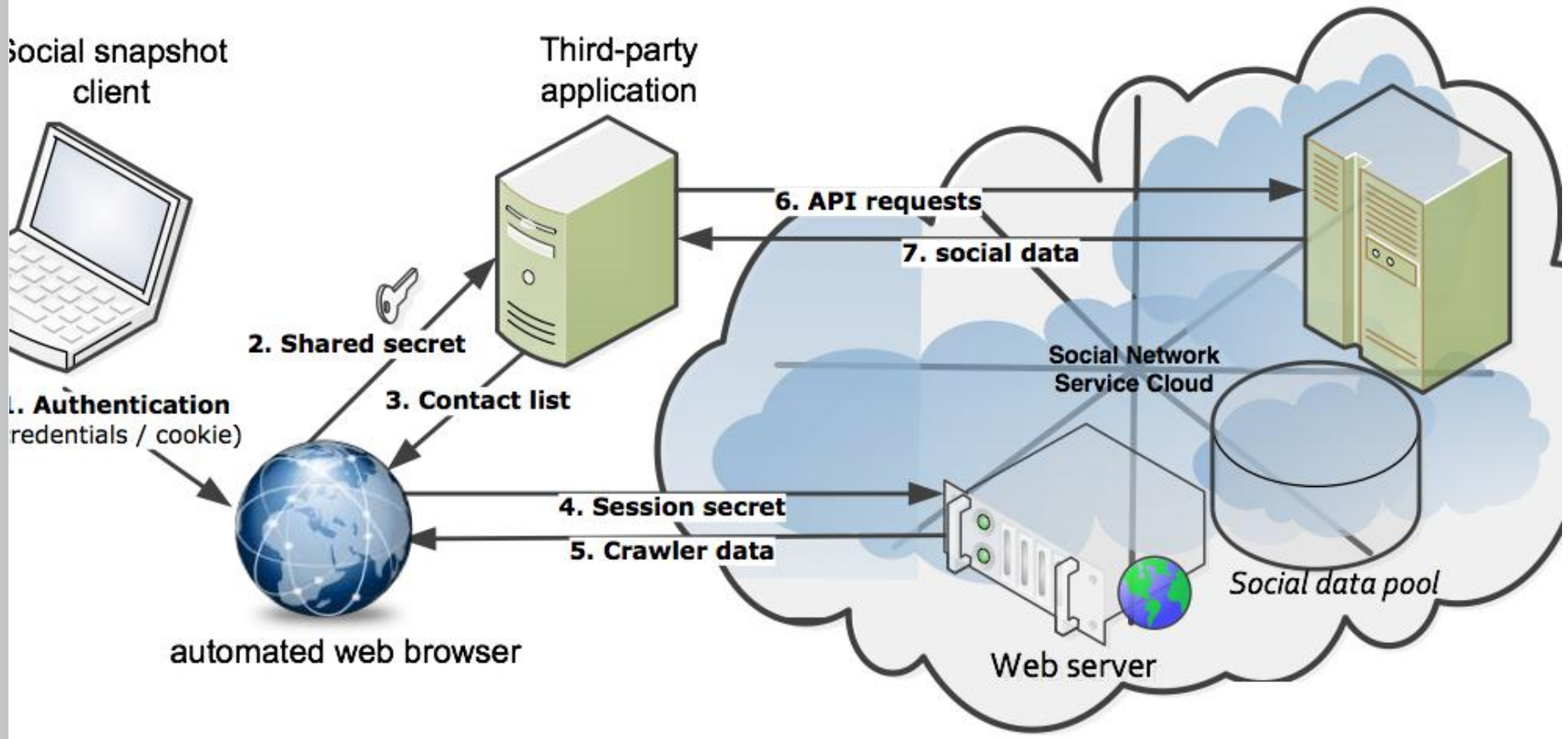


Friend-in-the-middle (FITM) Angriffe

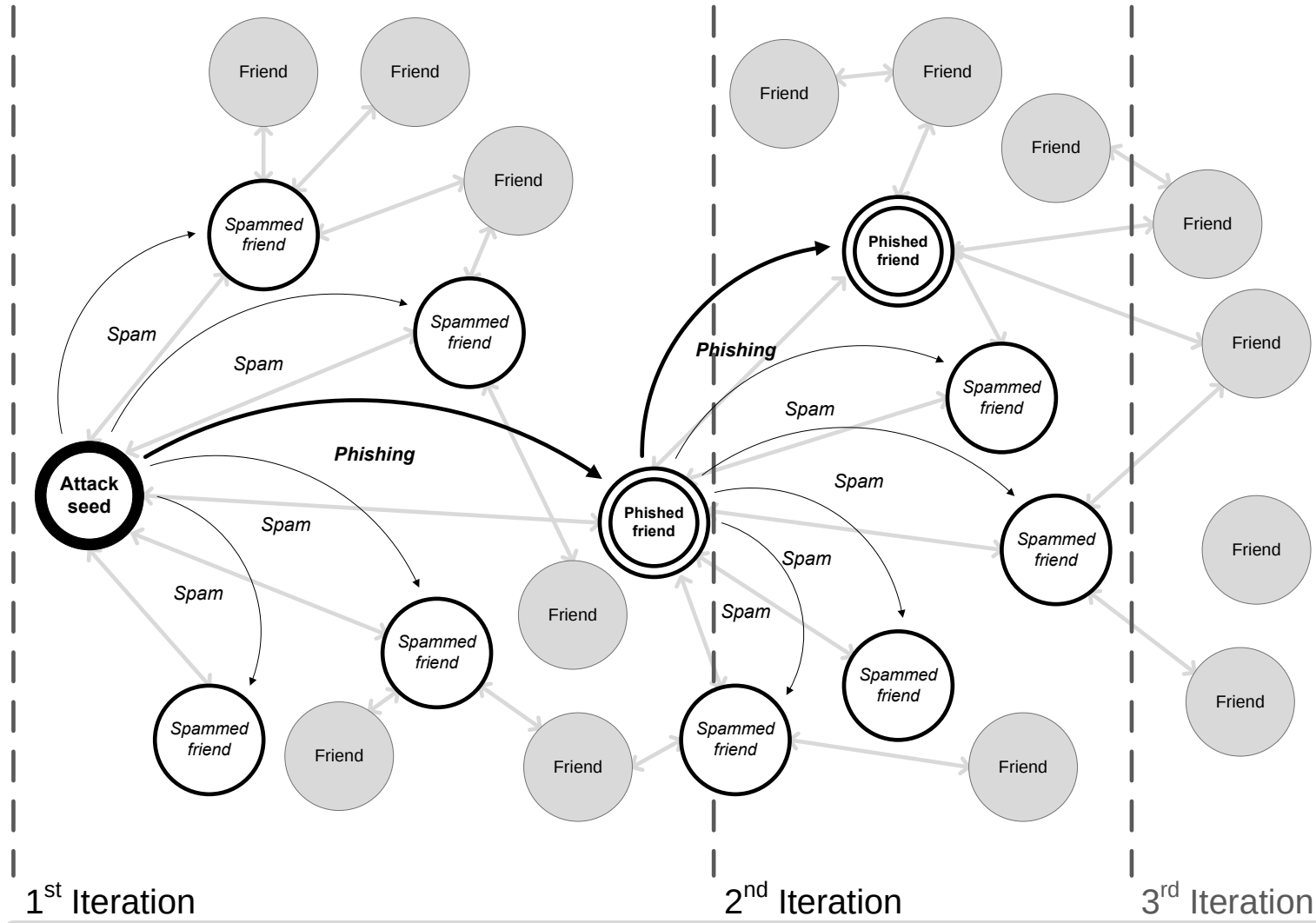


- Übernehmen von Sessions
- Unverschlüsseltes WLAN, Router bei LAN

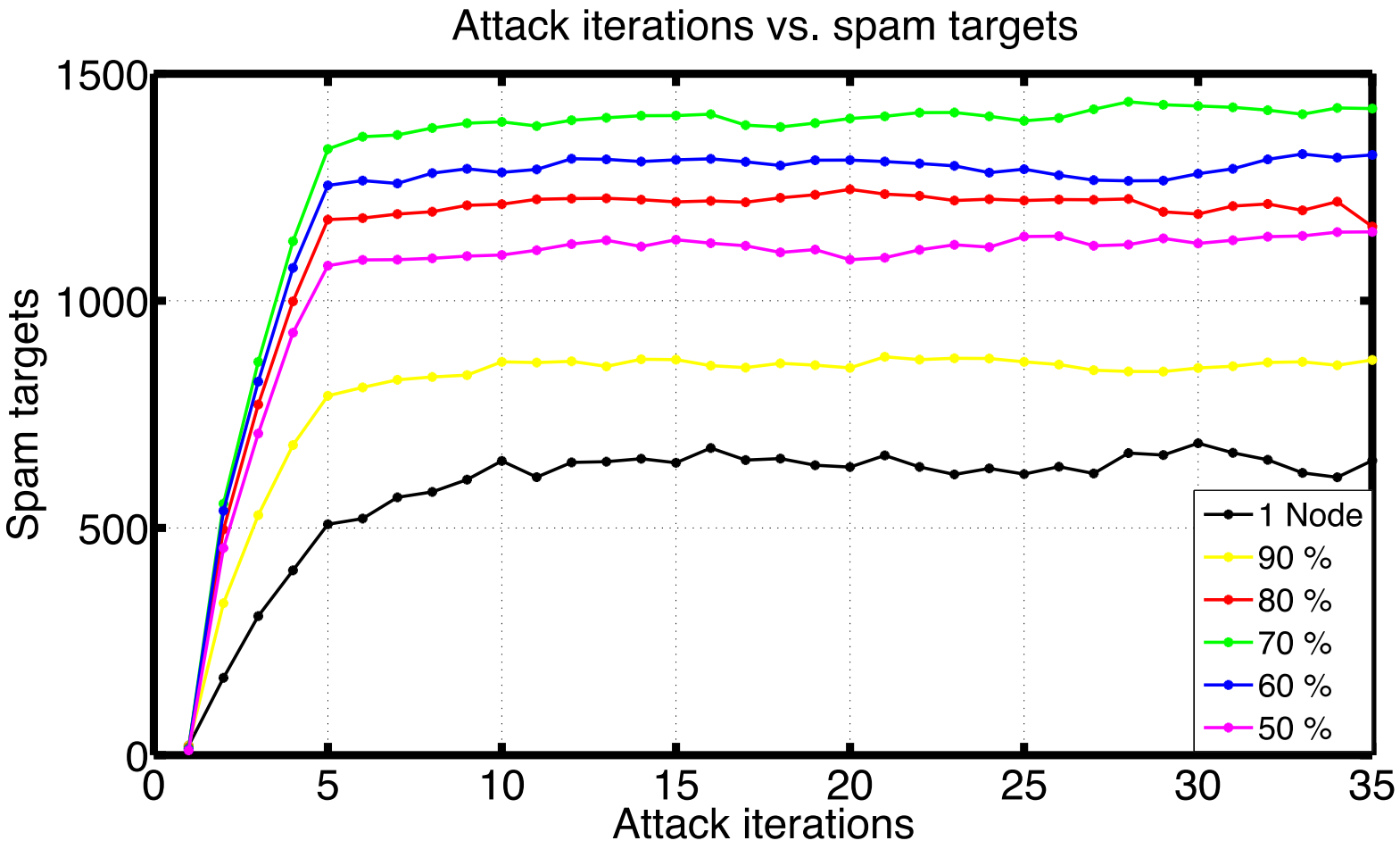
Schneller Zugriff auf viele Daten



Angriffsszenario



Ergebnisse der Simulation



Forschungsgebiete

secure
sba-research.org
COMET
Competence Centers for Excellent Technologies

Area 1 (GRC): Governance, Risk and Compliance	P1.1: Risk Management and Analysis P1.2: Secure BP Modeling, Simulation and Verification P1.3: Computer Security Incident Response Team P1.4: Awareness and E-Learning
Area 2 (DSP): Data Security and Privacy	P2.1: Privacy Enhancing Technologies P2.2: Enterprise Rights Management P2.3: Digital Preservation
Area 3 (SCA): Secure Coding and Code Analysis	P3.1: Malware Detection and Botnet Economics P3.2: Systems and Software Security P3.3: Digital Forensics
Area 4 (HNS): Hardware and Network Security	P4.1: Hardware Security and Differential Fault Analysis P4.2: Pervasive Computing P4.3: Network Security of the Future Internet

secure
sba-research.org

COMET

Competence Centers for
Excellent Technologies

Edgar Weippl
www.sba-research.org