

ATTRIBUT Phase II

Teilprojekt Standard Internetprotokolle

Sebastian Zillien¹ Steffen Wendzel¹ Denis Petrov¹ Jana Dittmann² Christian Krätzer²
Stefan Kiltz² Robert Altschaffel² Claus Vielhauer³ Sandro Wefel⁴ Holger Nitsch⁵

¹University of Applied Sciences Worms ²Otto-von-Guericke Universität, Advanced Multimedia and Security Lab
³Technische Hochschule Brandenburg ⁴Martin-Luther-Universität Halle-Wittenberg ⁵Hochschule für den öffentlichen Dienst in Bayern

Motivation

- Mehr und mehr Schadsoftware nutzt **Steganographie** für:
 - Unterstützung beim Einschleusen von Schadcode auf das Zielsystem
 - Exfiltration gestohlener Daten
 - Kommunikation mit Command & Control Server (C2-Server)
- Bekannte Beispiele
 - **Stuxnet**, verdeckte Ausführung
 - **SynCrypt**, Einschleusen von Schadcode
 - **Duqu/Duqu2**, Datenexfiltration & C2-Kommunikation
- Bestehende Sicherheitsmechanismen verlieren durch Steganographie an Wirksamkeit
- Einfache Verfügbarkeit von Stego-Modulen in Foren oder auf GitHub

Steganographie

- Verstecken geheimer Daten in anderen, legitimen Daten
- Keine Kryptographie – Kryptographie verschleiert den *Inhalt* der Nachricht, Steganographie das *Vorhandensein* der Nachricht
- Kleine, unscheinbare Veränderungen dienen als Signale
- Verschiedenste Methodiken bekannt und bereits “in the wild” zu finden: Digitale Medien (Bild, Audio und Texte), Industrielle Steueranlagen, Netzwerk Kommunikation.

Netzwerk-Steganographie

- Geheime Kommunikation in harmlos erscheinendem Netzwerkverkehr versteckt
- In der Forschung unterteilt in “Hiding Patterns” [7]
 - **Storage Pattern** – Ausnutzen von Protokollfunktionen zum Einbetten der Daten
 - **Timing Pattern** – Manipulation zeitlicher Abläufe zur Repräsentation der Daten
- Vertreten auf allen Netzwerkschichten

Warum Attribution?

- Um sinnvoll auf Sicherheitsbedrohungen zu reagieren, sind zahlreiche Informationen aus diversen Blickwinkeln nötig. Darunter auch, wer den Vorfall ausgelöst hat [6] – also die **Attribution**.
- Bei Falschattribution können schwerwiegende Folgen drohen.
 - In [2] nennen Egloff und Smeets die “Certainty” im Bereich der Attribution und unterstreichen die **Schwierigkeit**
- Fokus für das Projekt **ATTRIBUT** ist es, einem Angriff ein “System-of-Origin” [5] zuzuordnen und entsprechende Angreifersignaturen zu erkennen
- Speziell bei der Steganographie ist es von Interesse, die beteiligten **Kommunikationspartner** zu identifizieren [4]

Acknowledgement

Teile dieses Posters basieren auf [1] (under review), in dem das Gesamtprojekt vorgestellt wird. Projektleitung: Univ. Magdeburg.

Förderung des Projekts

Beauftragung d. die Agentur für Innovation in der Cybersicherheit GmbH: Forschung zu „Existenzbedrohenden Risiken aus dem Cyber- und Informationsraum – Hochsicherheit in sicherheitskritischen und verteidigungsrelevanten Szenarien“ (HSK) - <https://www.cyberagentur.de/tag/hsk/>.

Attribution bei StegoMalware

- Strukturelle Grundlage bilden sog. “Hiding Patterns” [7] als abstrakte und generische Beschreibung Strganographischer Methoden.
- Hierauf aufbauend werden zwei Attributierungen angestrebt:
 - Einbettmuster Attributierung (EMA) – Basierend auf den Charakteristika der genutzten Stego-Methoden
 - Szenario/Protokoll-Attributierung (SPA) – Basierend auf dem Ablauf der Kommunikation von Initialisierung über Datenübertragung hin zu Abbau des Kanals.

Standard Internetprotokolle

Die Kernaufgabe in diesem Projektteil liegt in der grundlegenden Erforschung von Attributionsmethoden für StegoMalware im Kontext des TCP/IP Protokollstacks. Hierfür arbeiten wir an mehreren Punkten:

- Analyse des Datenverkehrs bestehender und bekannter StegoMalware
 - Untersuchen, Verstehen und Kategorisieren von genutzten Methoden
 - Konzeption und Aufbau eines Netzwerktestbeds zur Beobachtung von Schadsoftware
- Simulation von StegoMalware-Datenverkehr
 - Erweiterung der Analysedaten mit weiteren Methoden
 - Abwandlung bestehender Methoden
- Erweiterungen und Entwicklung von Attributionsmodulen für WoDiCoF+ [3]
 - Zentralisierte Verarbeitung von Netzwerkmitschnitten
 - Filterung, Gruppierung und Extraktion von relevanten Daten zur Attribution
 - Attributionsmodule implementieren tiefere Logik

Erste Analysen zeigen, dass StegoMalware oft auf HTTP(S) und DNS zurückgreift, um geheime Daten zu übertragen. Diese zwei Protokolle stehen im Fokus unserer initialen Analysen und Simulationen.

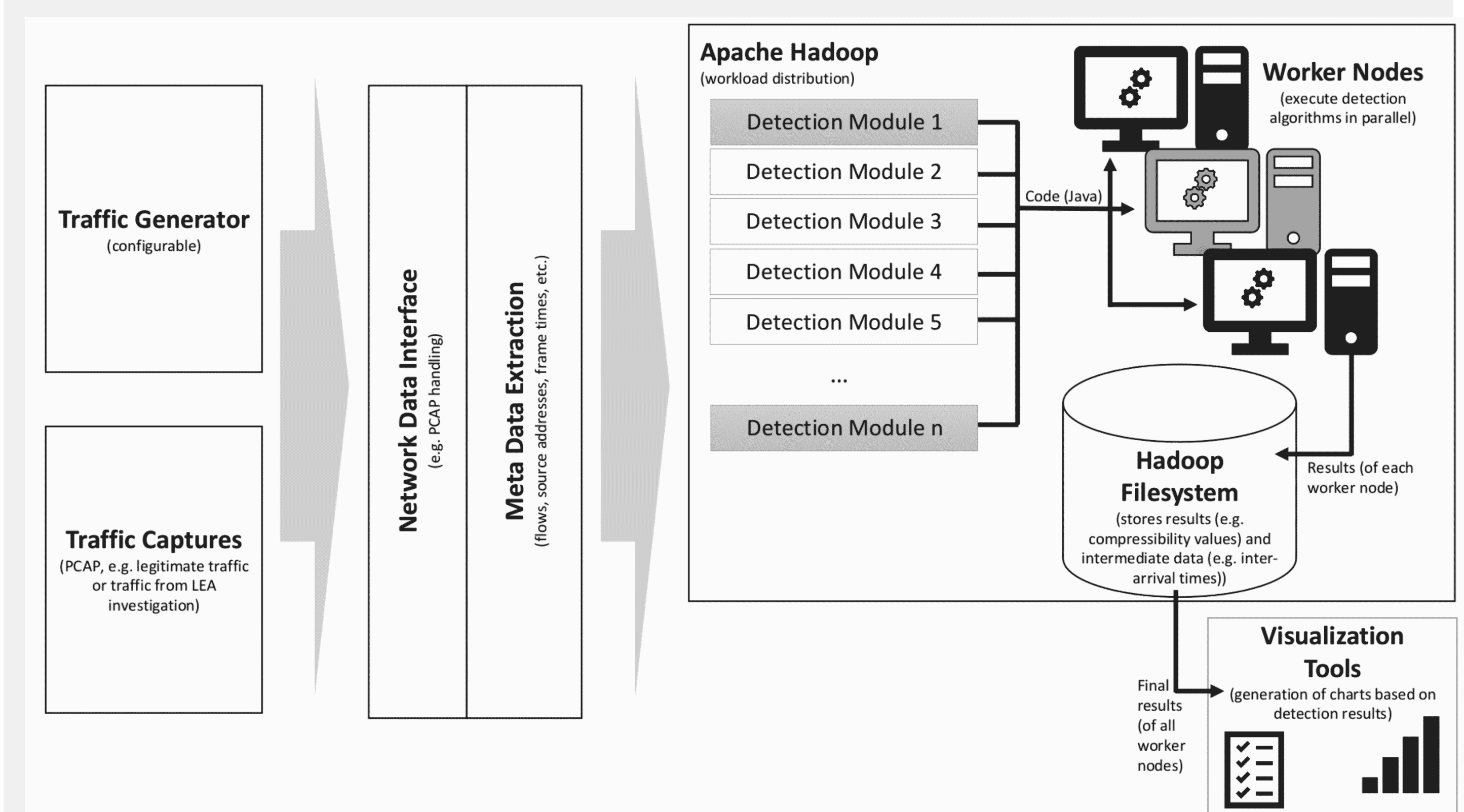


Figure 1. Urspr. WoDiCoF Architektur aus [3] (aktuell in Revision)

Referenzen

- [1] J. Dittmann, Ch. Krätzer, S. Kiltz, R. Altschaffel, C. Vielhauer, S. Wendzel, S. Wefel, and H. Nitsch. Attribution von verdeckten (Informations-)Kanälen im Bereich kritischer Infrastrukturen und Potentiale für Prävention und Reaktion (ATTRIBUT). 2023. under review.
- [2] F. J. Egloff and M. Smeets. Publicly attributing cyber attacks: A framework. *Journal of Strategic Studies*, pages 1–32, 2021.
- [3] R. Keidel, S. Wendzel, S. Zillien, E. S. Conner, and G. Haas. WoDiCoF - A testbed for the evaluation of (parallel) covert channel detection algorithms. *JUCS - Journal of Universal Computer Science*, 24(5):556–576, 2018.
- [4] Ch. Krätzer and J. Dittmann. Früherkennung von verdeckten Kanälen in VoIP- Kommunikation. *Proceedings of the BSI-Workshop IT-Frühwarnsysteme*, 2006.
- [5] N. Müller, F. Diekmann, and J. Williams. Attacker attribution of audio deepfakes. *Proc. Interspeech 2022*, pages 2788–2792, 2022.
- [6] F. Skopik, A. Bonitz, V. Grantz, and G. Göhler. From scattered data to actionable knowledge: flexible cyber security reporting in the military domain. *In International Journal of Information Security*, 21:1323–1347, 2022.
- [7] S. Wendzel, L. Caviglione, W. Mazurczyk, A. Mileva, J. Dittmann, C. Kraetzer, K. Lamshöft, C. Vielhauer, L. Hartmann, J. Keller, and T. Neubert. A revised taxonomy of steganography embedding patterns. 2021.

