INF FAKULTÄT FÜR INFORMATIK

PaymentTraces:
gone but not forgotten!

SMKITS/IFOR
05.07.2023

Bernhard Birnbaum
Tobias Heitmüller
Pascal Heiroth
Glenn Diebetz
Sönke Otten

Inhalt

1. Aufgabenverteilung
2. Konzept
   a. finale Werkzeugauswahl mit Datenarten
   b. Aufbau der Untersuchungsinfrastruktur
   c. Untersuchungsmethodik
3. Evaluierung der Untersuchungsergebnisse
4. MITRE ATTACK: Ontologie
5. Aussicht

1. individuelle Teamaufgaben

Teammitglied	Aufgaben
Bernhard	Konzept zum Aufbau der Untersuchungsinfrastruktur, Datenströme und -arten, Bezahlvorgang In-App-Kauf
Glenn	Konzept und Analyse des Haupt- und Massenspeichers, Bezahlvorgang Anton-App
Pascal	Bezahlvorgang Amazon, Vorbereitung Draft
Tobias	Konzept und Implementierung der MitrAtt@ck Ontologie
Sönke	Bezahlvorgang Google Play Store, Vorbereitung Draft

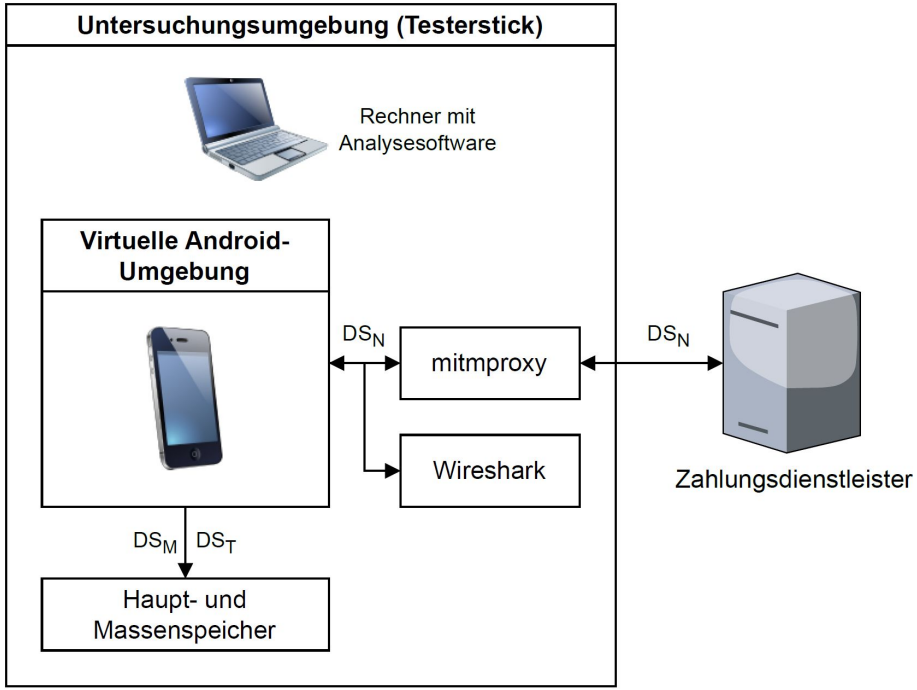
2. Konzept: finale Werkzeugauswahl mit Datenarten

Werkzeuge	Datenströme	Datenarten		Umgebung
		Eingang	Ausgang	
VirtualBox	DS_T, DS_M	n.a.	DT_1	s, d
Wireshark	DS_N	DT_5	DT_5	s, pm
mitmproxy	DS_N	DT_5	DT_5, DT_7	d, pm
strings	DS_M	DT_1	DT_6, DT_7	pm
GHex	DS_M	DT_1	DT_6, DT_7	pm
Autopsy	DS_T	DT_1	DT_3, DT_4, DT_8	pm
ExtUndelete	DS_T	DT_1	DT_3, DT_4, DT_8	pm

Legende:

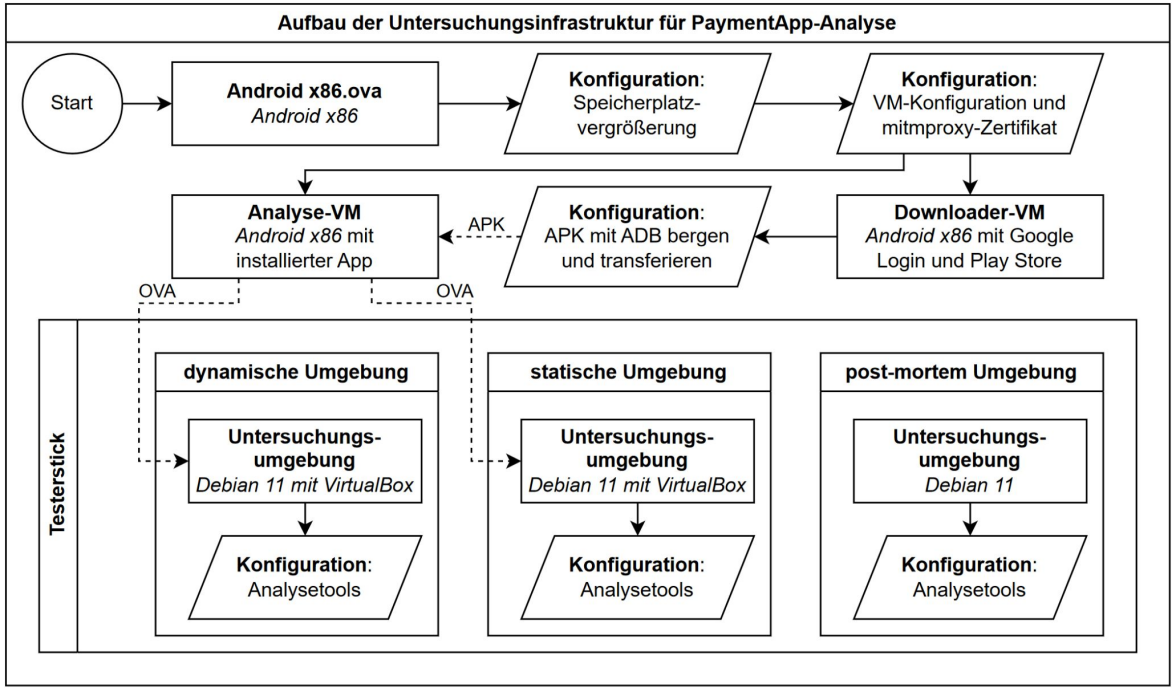
DS_N: Netzwerkdatenstrom
DS_M: Hauptspeicher
DS_T: Massenspeicher
DT_1: Rohdaten
DT_3: Metadaten
DT_4: Konfigurationsdaten
DT_5: Kommunikationsprotokolldaten
DT_6: Prozessdaten
DT_7: Sitzungsdaten
DT_8: Nutzerdaten
s: statische Umgebung
d: dynamische Umgebung
pm: post-mortem Umgebung

2. Konzept: Aufbau der Untersuchungsinfrastruktur

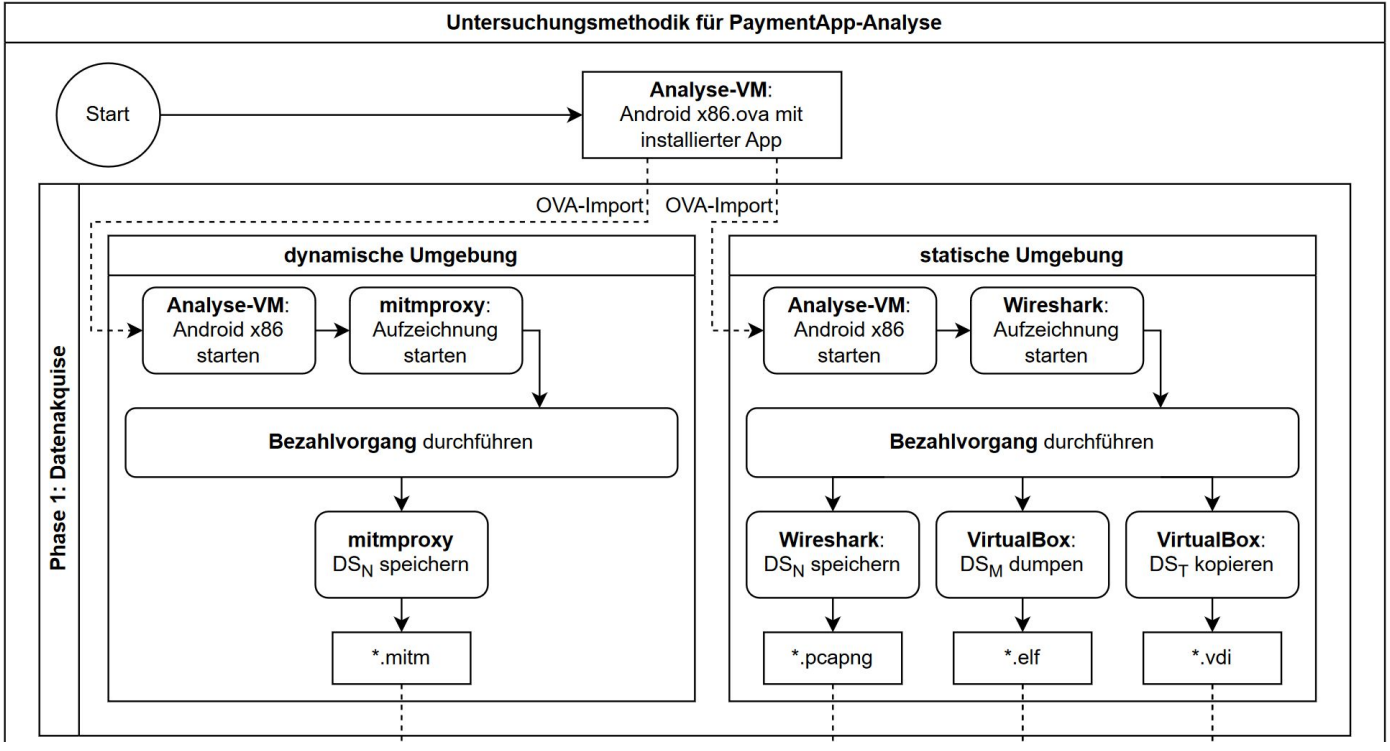


IT-Systemlandschaft

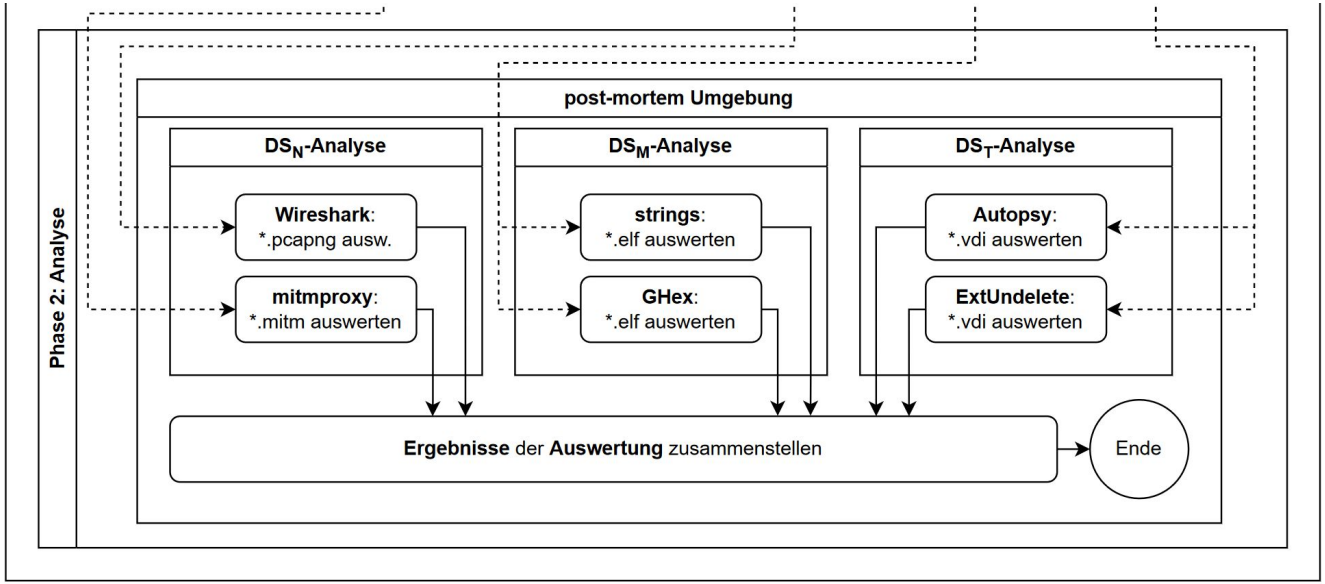
2. Konzept: Aufbau der Untersuchungsinfrastruktur



2. Konzept: Untersuchungsmethodik / Phase 1



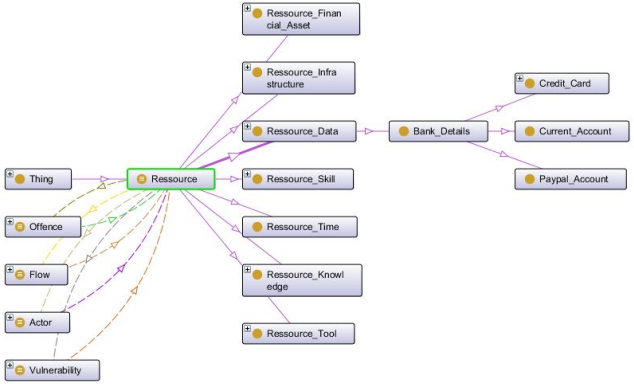
2. Konzept: Untersuchungsmethodik / Phase 2

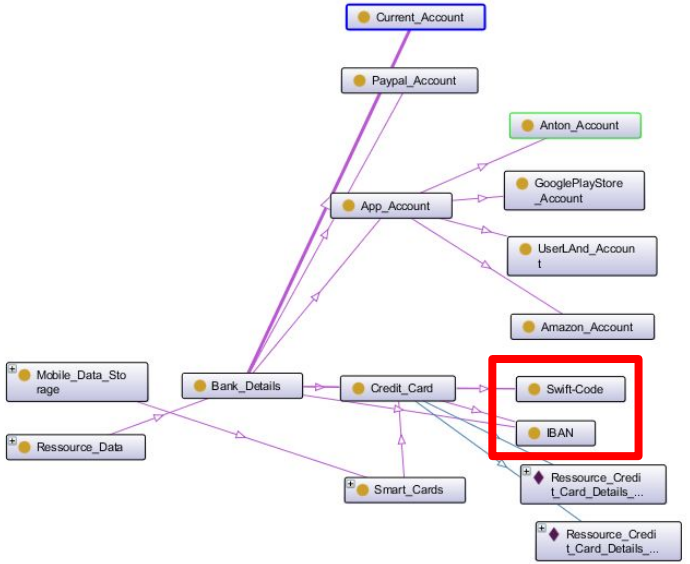


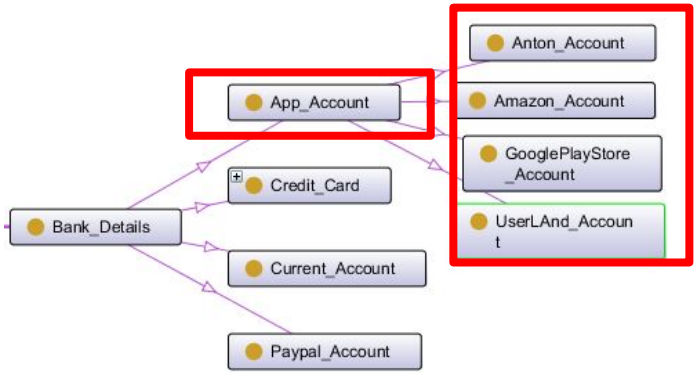
3. Evaluierung der Untersuchungsergebnisse

Bezahlvorgang	Ergebnisse (Auswahl)
Amazon App Store: App-Kauf	DS_N: 12 einzigartige DNS-Anfragen z.B. device-metrics-us-ud.amazon.com - personalisierte Werbung nach Gerätemetriken, DS_M: Suche nach Passwort/IBAN, keine Ergebnisse - keine Zwischenspeicherung, DS_T: 26 Ergebnisse zu SSL/TLS, Certificate Transparency, Content Delivery Network, Frameworks, Certificate Operations
Google Play Store: In-App-Abo ANTON-App	DS_N: 9 einzigartige DNS-Anfragen z.B. logger-lb-4.anton.app, Server in Deutschland , Account Token im Klartext, E-Mail Adresse im Klartext DS_M: Suche nach E-Mail Adresse lieferte ein Ergebnis, DS_T: E-Mail Adresse und Bearer-Auth-Token
Google Play Store: App-Kauf	DS_N: 18 einzigartige DNS-Anfragen z.B.Tracker ‘app-measurement.com’ und ‘region1.app-measurement.com’ , E-Mail Adresse sowie Passwort im Klartext im entschlüsselten Datenstrom DS_M: Im Dump E-Mail Adresse im Klartext gefunden DS_T: E-Mail Adresse sowie Bearer-Auth-Tokens
Google Play Store: In-App-Kauf UserLAnd	DS_N: Server in USA, CNAME-Tracking ‘app-measurement.com’ schreibt den Kaufvorgang mit (Anzahl, Artikel, Währung, …), **vollständige Login-Daten im Klartext** im entschlüsselten Datenstrom, Bearer-Auth-Tokens; DS_M: vollständige Login-Daten im Klartext im Dump gefunden; DS_T: E-Mail-Adresse sowie Bearer-Auth-Tokens

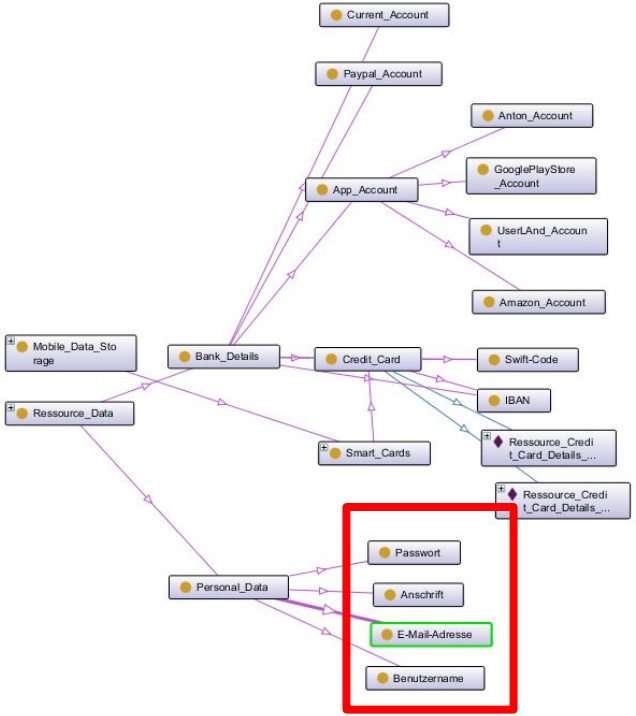
4. MITRE ATTACK: Ontologie

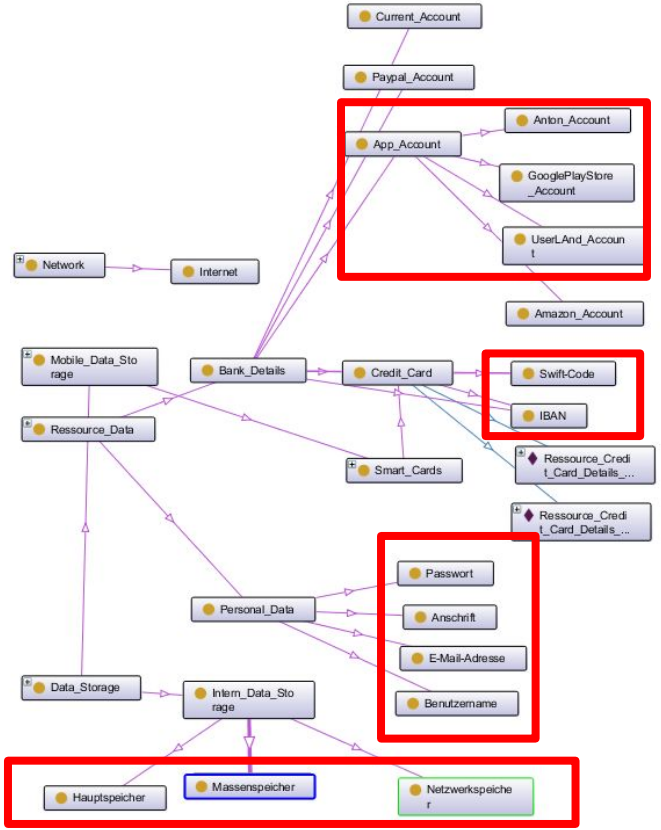




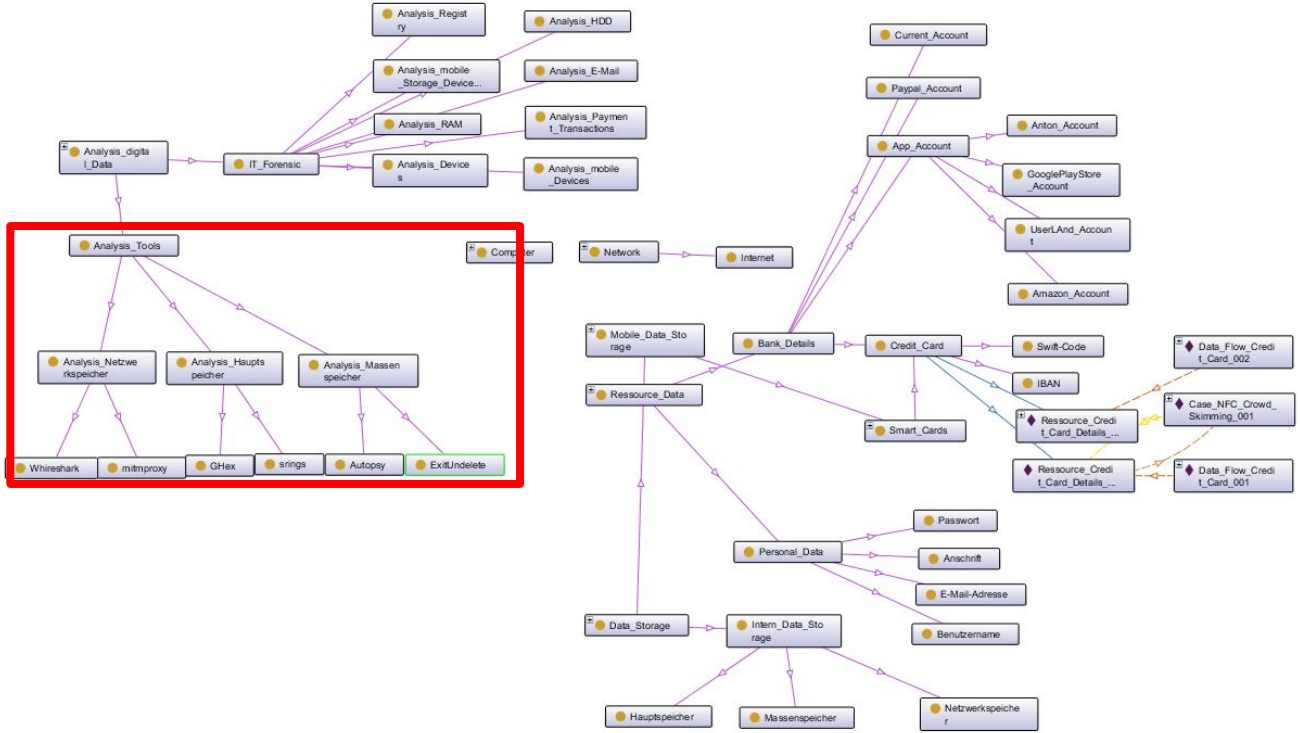


4. MITRE ATTACK: Ontologie

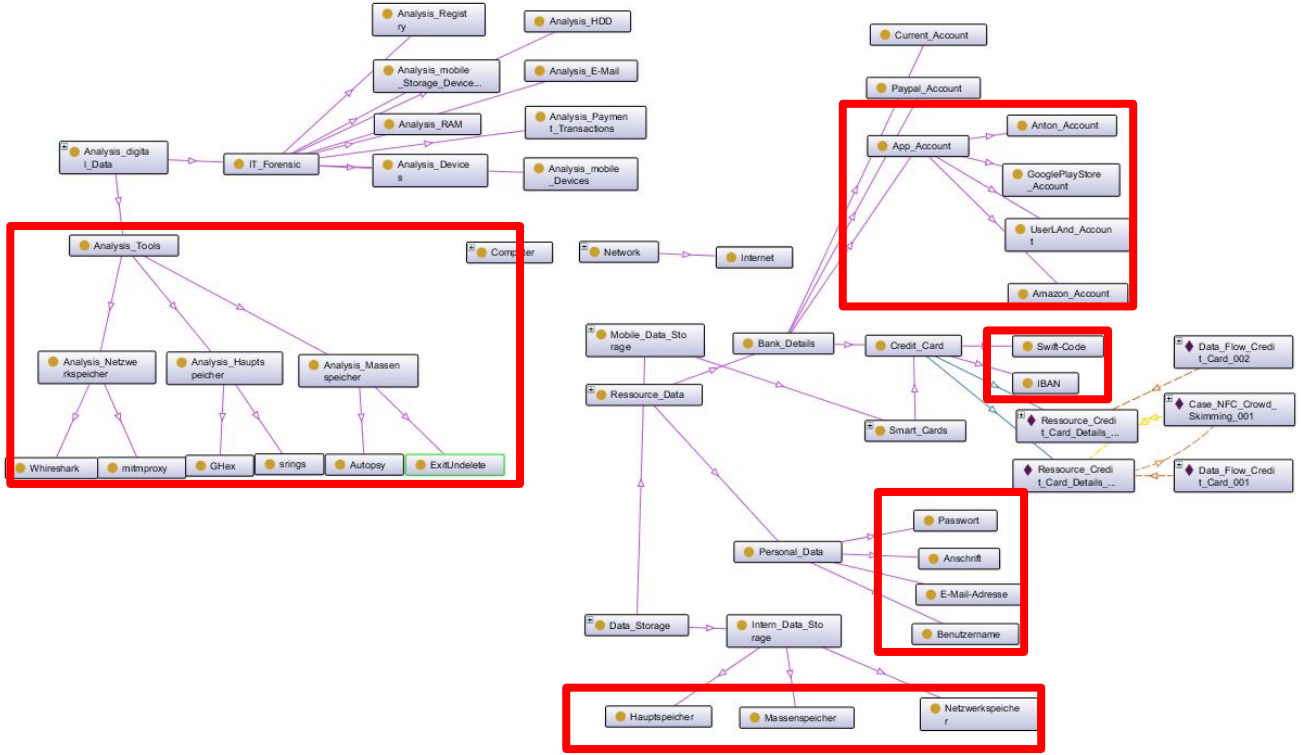




4. MITRE ATTACK: Ontologie



4. MITRE ATTACK: Ontologie



5. Aussicht

- Bericht fertig schreiben
- Ausblick für zukünftige Arbeiten
  - Vereinigung der statischen und dynamischen Untersuchungsumgebung
  - Volatility-Profil für Android-x86-RAM-Analyse
  - GenyMotion als alternative VM, um App-Kompatibilität zu verbessern
  - Frameworks wie Xposed oder Magisk verwenden, um Rooting zu verbergen bzw. Safety-Check zu bestehen
- SMKITS: Management Report abschließen

Danke für Ihre Aufmerksamkeit!

Ergebnistabelle - Amazon App Store

Datenstrom	Werkzeug	Ergebnisse
DS_N	*Wireshark*	• 12 einzigartige DNS-Anfragen, darunter `api.amazon.de`, `cloudfront.net`, `device-metrics-us-ud.amazon.com` sowie `m.media-amazon.com`
DS_N	*mitmproxy*	• Analyse, aufgrund fehlender/alter Zertifikate nicht möglich
DS_M	*strings*	• Suche nach Passwort/IBAN - keine Ergebnisse
DS_T	*Autopsy*	• 26x verschiedene E-Mail Adressen zu Kategorien: SSL/TLS, Certificate Transparency, Content Delivery Network, Frameworks und Certificate Operations

Ergebnistabelle - UserLAnd

Datenstrom	Werkzeug	Ergebnisse
DS_N	*Wireshark*	• Server in Kalifornien, USA lokalisiert • CNAME-Tracker `app-measurement.com` identifiziert
DS_N	*mitmproxy*	• weiteren Tracker `ssl.google-analytics.com` identifiziert • nur Google-Dienste involviert → PayPal-Passwort muss auf Google-Server gespeichert sein • vollständige Login-Daten des verwendeten Google-Accounts: E-Mail und Passwort im Klartext • Bearer-Auth-Tokens werden verwendet und können u.U. zur Umgehung der 2FA genutzt werden
DS_M	*strings*	• 27263x Google-E-Mail-Adresse • Suche nach „`"password","credential":`“ liefert Google-Passwort im Klartext
DS_T	*Autopsy*	• 637x Google-E-Mail-Adresse • Bearer-Auth-Tokens

Ergebnistabelle - GooglePlayStore

Datenstrom	Werkzeug	Ergebnisse
DS_N	*Wireshark*	• Server in Kalifornien, USA lokalisiert • Server in Hamburg, Deutschland lokalisiert • tracker `app-measurement.com` identifiziert • tracker `egion1.app-measurement.com` identifiziert
DS_N	*mitmproxy*	• Einzige involvierte Patei ist Google -¿ MYPaySafe muss auf Google gespeichert sein • E-Mailadresse und Passwort in Klartext • Bearer-Auth-Tokens können ausgelsen werden
DS_M	*strings*	• Stichprobensuche: E-Mailadresse im Klartext
DS_T	*Autopsy*	• Bearer-Auth-Tokens

Ergebnistabelle - Anton App

Datenstrom	Werkzeug	Ergebnisse
DS_N	*Wireshark*	• Server in Deutschland lokalisiert, IP Adressen von Hetzner Online Gmbh werden genutzt
DS_N	*mitmproxy*	• nur Google Dienste involviert → PayPal Passwort muss auf Google Server gespeichert sein • Account Token ist im Klartext • E-Mail Adresse ist im Klartext
DS_M	*strings*	• E-Mail Adresse ist im Klartext zu finden
DS_T	*Autopsy*	• E-Mail Adresse auslesbar • Bearer-Auth-Tokesn