INF FAKULTÄT FÜR INFORMATIK

PaymentTraces:
gone but not forgotten!

SMKITS/IFOR
14.06.2023

Bernhard Birnbaum
Tobias Heitmüller
Pascal Heiroth
Glenn Diebetz
Sönke Otten

Inhalt

1. Fortschritte/Projektentwicklung
2. Konzept
   - Methodikdiagramm
   - Tabellarische Zusammenfassung für Tool-Auswahl
3. Umsetzung
4. Probleme
5. Aussicht
   - Draft
   - Nächsten Schritte

1. Fortschritte/Projektentwicklung

Teammitglied	Aufgaben
Bernhard	Vorbereiten der Untersuchungsumgebung, Konzept, Draft
Glenn	Konzept und Analyse des Haupt- und Massenspeichers
Pascal	Bezahlvorgang Amazon
Tobias	MitrAtt@ck Ontologie
Sönke	Vorbereitung Draft

1. Fortschritte/Projektentwicklung

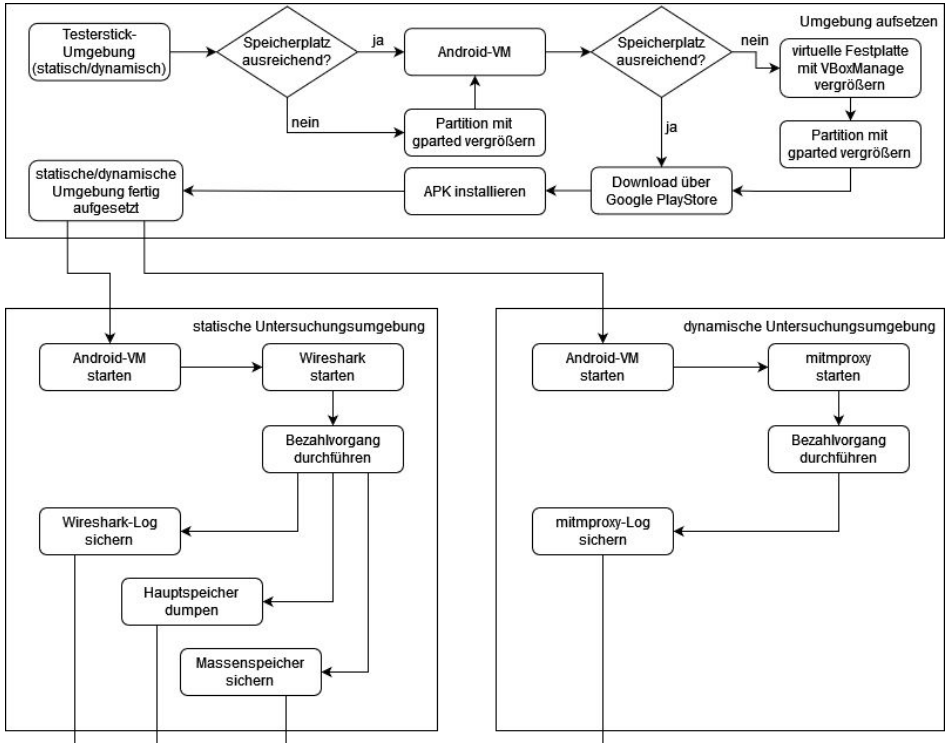
Fortschritte

- 2 PaymentApps installiert und fertig für Analyse
- erster Bezahlvorgang durchgeführt
- theoretische Analyseverfahren geschaffen

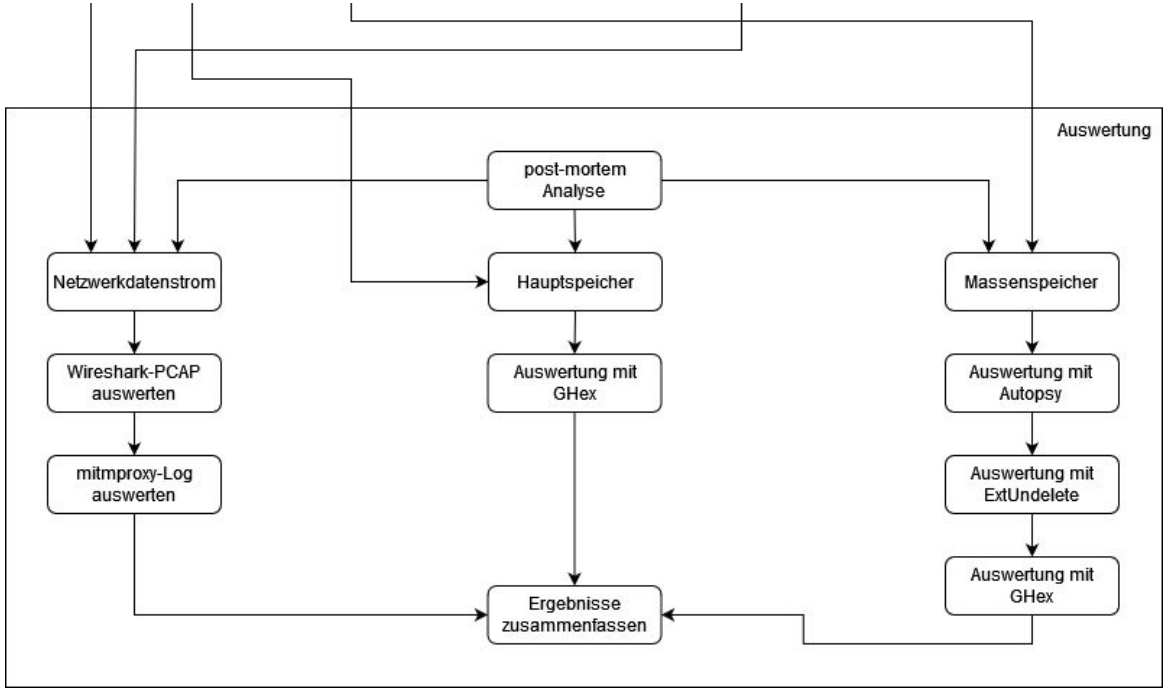
Projektentwicklung

- Hauptproblem: Testumgebung unzureichend vorbereitet für PaymentApp-Analyse:
  - Speicherplatz unzureichend für Installationen sowie Analysen
  - Analyse von Payment Apps auf gerootetem Android erfordert Verbergen des Rooting-Umstands (nötige Frameworks nicht installiert)
  - (zu) altes Android-System hat Probleme bei der Verbindung mit modernen Web-Diensten (TLS 1.3)

2. Konzept


Umgebung aufsetzen
Testerstick-Umgebung (statisch/dynamisch)
Speicherplatz ausreichend?
ja
Android-VM
Speicherplatz ausreichend?
nein
virtuelle Festplatte mit VBoxManage vergrößern
nein
Partition mit gparted vergrößern
ja
Partition mit gparted vergrößern
statische/dynamische Umgebung fertig aufgesetzt
APK installieren
Download über Google PlayStore
statische Untersuchungsumgebung
Android-VM starten
Wireshark starten
Bezahlvorgang durchführen
Wireshark-Log sichern
Hauptspeicher dumpen
Massenspeicher sichern
dynamische Untersuchungsumgebung
Android-VM starten
mitmproxy starten
Bezahlvorgang durchführen
mitmproxy-Log sichern

2. Konzept


Auswertung
post-mortem Analyse
Netzwerkdatenstrom
Hauptspeicher
Massenspeicher
Wireshark-PCAP auswerten
Auswertung mit GHex
Auswertung mit Autopsy
mitmproxy-Log auswerten
Auswertung mit ExtUndelete
Auswertung mit GHex
Ergebnisse zusammenfassen

2. Tabellarische Zusammenfassung: Tool-Auswahl

Titel	Link	Beschreibung
Testerstick der Uni	https://cloud.ovgu.de/s/Pk4RfzFEKzCoMc5	rauscharme Untersuchungsumgebung mit Android-Image
VirtualBox	https://www.virtualbox.org/	Virtualisierungslösung
Wireshark	https://www.wireshark.org/	Tool zum Analysieren des Netzwerkdatenstroms
mitmproxy	https://mitmproxy.org/	MITM-Proxy zum entschlüsseln des Netzwerkdatenstroms
SleuthKit/Autopsy	https://www.sleuthkit.org/autopsy/	Wiederherstellung von gelöschten Dateien, Extrahieren von Metadaten, etc.
ExtUndelete	https://extundelete.sourceforge.net/	Wiederherstellung von gelöschten Dateien
GHex	https://github.com/GNOME/ghex	Hex-Editor
Volatility	https://github.com/volatilityfoundation/volatility	Tool zum Analysieren des Speichers

3. Umsetzung der Analyse/erste Ergebnisse

- Amazon
  - Wireshark: 12 einzigartige DNS-Anfragen, darunter u.a. “api.amazon.de”, “cloudfront.net”, “device-metrics-us-ud.amazon.com” sowie “m.media-amazon.com”
  - GHex: Suche nach Passwort/IBAN in Massen- und Hauptspeicher keine Ergebnisse

  → auf den ersten Blick sind dort nur Amazon Dienste verzeichnet, jedoch fehlt uns hier noch eine Vergleichsanalyse um zu sehen welche Dienste bereits auf der Android-VM vorhanden sind und welche nicht.
- Limitierungen und mögliche Verbesserungen:
  - gestellte Untersuchungsumgebung ist für App-Analyse geeignet, allerdings nicht für PaymentApps optimiert (durch Safety-Check wird Rooting-Umstand bemerkt)

  → vor neuer Untersuchung aktuelle, auf PaymentApps zugeschnittene Umgebung aufsetzen, wo bereits zwingend nötige Frameworks und Apps installiert sind

  → evtl. Alternativen wie GenyMotion in Erwägung ziehen

4. Probleme

- Speicherplatz-Knappheit der Untersuchungsumgebung [gelöst]
  - Partition-Resize des Testersticks
  - Partition-Resize des Android-Images
- Installation von Apps [gelöst]
  - AuroraStore erst nach mehreren Versuchen und Neuinstallation überhaupt lauffähig
  - kein Download von Apps über AuroraStore möglich

  → verwendete APKs über Stefans GooglePlay-Account bezogen
  - finale Lösung: Installation von Apps m.H. von ADB anstatt der “DynamischenAppAnalyse”-Software
- Wiederholter Absturz von PayPal und giropay [ungelöst]
  - Versuch der Installation von openGApps schlug nach mehreren Versuchen fehl
  - Problem vermutlich auf Rooting-Umstand des Android-Systems zurückzuführen
  - aktuell: Versuch des Verbergens des Rooting-Umstands m.H. Xposed-Framework, allerdings ist Installation des Frameworks weiterhin problematisch

5. Draft

- erster Entwurf der Struktur
- Tabelle mit Datenarten
- Referenzen bereits alle in Draft eingebunden

5. Nächste Schritte

- PayPal und giropay lauffähig aufsetzen/analysieren
- Analyse des bereits erfolgten Bezahlvorgangs ausweiten
- Draft zu Bericht schreiben
- Ontologie erweitern
- SMKITS: Management Report verfassen

Danke für Ihre Aufmerksamkeit!