INF FAKULTÄT FÜR INFORMATIK

PaymentTraces:
gone but not forgotten!

SMKITS/IFOR
26.04.2023

Bernhard Birnbaum
Tobias Heitmüller
Pascal Heiroth
Glenn Diebetz
Sönke Otten

Inhalt

1. Team-Organisation
2. Motivation
3. Aufgabenverständnis
4. Fortschritte und Probleme bei der Umsetzung
5. Tabellarische Zusammenfassung als Wissensbasis mit Referenzen
6. Tabellarische Zusammenfassung für Tool-Auswahl
7. Bezahlmethoden
8. Nächsten Schritte

1. Team-Organisation

• Tobias Heitmüller	Informatik	IT-Forensik
• Sönke Otten	Informatik	IT-Forensik
• Glenn Diebetz	Informatik	SMKITS
• Pascal Heiroth	Ingenieurinformatik	SMKITS
• Bernhard Birnbaum	Informatik	IT-Forensik

Organisation:

- Wöchentliches Team-internes Meeting sowie Meeting mit S. Kiltz
- Bei Bedarf: Absprachen mit S. Kiltz für Sondertermin
- Dynamische Aufgabenteilung

2. Motivation

- App-basierte Zahlungssysteme benötigen netzbasierte Zugriffe auf Systeme von Zahlungsdienstleistern
- Datensicherheit und Datenschutz sind von großer Bedeutung
  - oftmals werden nicht notwendige, datenschutzrelevante Daten übermittelt
  - auch Drittanbieter können kontaktiert und Informationen transferiert werden
- IT-Sicherheitsaspekte werden verletzt: Vertraulichkeit, Authentizität
- forensische Untersuchung von App-basierten Bezahlvorgängen kann potentielle Bedrohungen aufdecken

3. Aufgabenverständnis

- **Ziel: Forensische Untersuchung von App-basierten Bezahlvorgängen im Rahmen eines Demonstrators***
  - Dokumentation der kompletten Bearbeitungskette (Eingangsdaten, Konfigurationsdaten, Ausgangsdaten) nach existierendem Modell
  - Einrichtung eines virtualisierten Ökosystems für App Payments, das diesen Anforderungen genügt
  - App-basierte Zahlungsvorgänge durchführen begleitet mit live+post mortem IT-forensischen Methoden auf den Datenströmen Haupt-, Massenspeicher und Netzwerk
  - Beschreibung des gesamten Untersuchungsverlaufs als Kette von Untersuchungsmethoden und deren Ein- und Ausgabedaten
  - Ergänzung/Erweiterung der existierenden Ontologie “Mitre Att@ck Schema”

*Dieses Thema wurde uns bereitgestellt von der Arbeitsgruppe AMSL.

4. Fortschritte und Probleme bei der Umsetzung

Fortschritte

- Jeder hat eine lauffähige Android-VM zur Untersuchung
- Jeder hat Zugang zu den benötigten Analyse-Tools

Probleme

- Testerstick hat nicht richtig gebootet
- Mit Rufus erstellte Sticks waren nicht bootfähig

→ individuelle Lösungen wurden umgesetzt

5. Tabellarische Zusammenfassung als Wissensbasis mit Referenzen

Titel	Link	Beschreibung
[Kil20] Data-Centric Examination Approach (DCEA) for a qualitative determination of error, loss and uncertainty in digital and digitised forensics	http://dx.doi.org/10.25673/34647	zu verwendendes forensisches Datenmodell
[EBE+22] Revisiting Online Privacy and Security Mechanisms Applied in the In-App Payment Realm from the Consumers' Perspective	https://dl.acm.org/doi/abs/10.1145/3538969.3543786	vorangegangene Arbeit zum Thema In-App-Payment mit Fokus auf Privacy und Security
[Mit23] Mitre Att&ck	https://attack.mitre.org	zu erweiternde Ontologie
How to Install Android x86 on Virtual Machine using VMware Player	https://www.youtube.com/watch?v=nFtNKY1g6Lc	Android x86 - Installation
How to convert .img to usable VirtualBox format	https://superuser.com/questions/554862/how-to-convert-img-to-usable-virtualbox-format	Umwandlung Testerstick-Image in VBox-Format
Bootfähigen Linux USB stick in Mac erstellen	https://www.youtube.com/watch?v=42KWq0OBY1k	Testerstick mit Android Umgebung lauffähig machen auf macOS

6. Tabellarische Zusammenfassung für Tool-Auswahl

Titel	Link	Beschreibung
Testerstick der Uni	https://cloud.ovgu.de/s/Pk4RfzFEKzCoMc5	rauscharme Untersuchungsumgebung mit Android-Image
VM Ware	https://www.vmware.com/de.html	Virtualisierungslösung
VirtualBox	https://www.virtualbox.org/	Virtualisierungslösung
Wireshark	https://www.wireshark.org/	Tool zum Analysieren des Netzwerkdatenstroms
Volatility	https://github.com/volatilityfoundation/volatility	Tool zum Analysieren des Speichers
(Genymotion)	https://www.genymotion.com	Non-OpenSource (eventuelle Paywall)

7. Bezahlmethoden

giropay

Klarna.

amazon pay

~~PayPal~~

G Pay

8. Nächste Schritte

- Android VM intern vorbereiten (App(s) installieren, Konten einrichten)
- Bezahlvorgänge auf Teammitglieder verteilen
- Analyse-Tools vorbereiten und konfigurieren (Parameter festlegen, etc.)
- Analyse-Methodik entwickeln (Was wird wann wo und wie analysiert?)
- Erste Probedurchläufe
- Draft erstellen
- Vertrautmachen mit: Ontologie “Mitre Att@ck Schema”

Danke für Ihre Aufmerksamkeit!