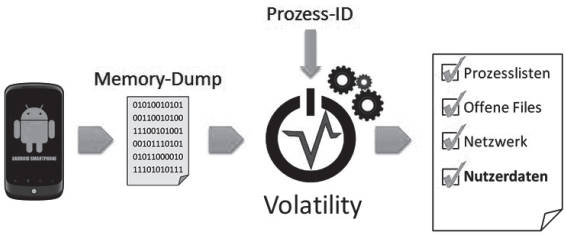
Android Memory Forensik

Fachgebiet: Informatik
Betreuer: Dr. Endre Bangerter
Experte: Armin Blum (BAKOM)

Bei Ermittlungen in Straftaten oder beim Reverse-Engineering von Malware stellen mobile Geräte wie Smartphones oder Tablets aufgrund ihrer Allgegenwärtigkeit heutzutage eine wichtige Informationsquelle dar. Dabei sind sowohl die Daten im Speicher, wie auch eine Analyse des RAM sehr aufschlussreich. Trotz des grossen Marktanteils von Android (75% im dritten Quartal 2012) steckt die Memory-Forensik bei Android-Geräten jedoch noch in den Kinderschuhen.



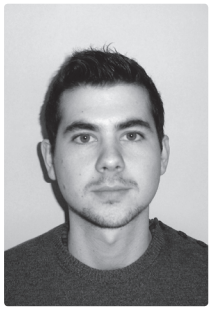
Generischer Analyseprozess nach unserer Arbeit

Mit bestehenden Werkzeugen ist es heute bereits möglich, Systemdaten wie Netzwerkverbindungen oder Prozesslisten aus einem Memory-Dump von Android-Geräten zu rekonstruieren. Das Opensource Framework Volatility ist der bekannteste Vertreter dieser Tools, bietet aber nur begrenzte Unterstützung für Android-Systeme. Insbesondere die Analyse und Wiederherstellung von Userdaten wie SMS, Browser-History oder Passwörter lassen zu wünschen übrig. Bruchteile dieser Informationen können zwar wiederhergestellt werden, was allerdings mit grossem Aufwand verbunden ist und umfassende Kenntnisse der Materie erfordert. Dadurch ist die Anwendbarkeit in der Praxis nicht gegeben.

Mit unserer Arbeit zeigen wir auf, wie die automatisierte Auswertung von beliebigen Useranwendungen – den Android-Apps – in Memory-Dumps durchgeführt werden kann. Unsere Lösung stellt eine Erweiterung des Volatility-Frameworks dar. Unabhängig vom Aufbau der zu analysierenden App werden sämtliche wiederherstellbaren Datenstrukturen im Memory-Dump identifiziert, ausgewertet und für die weitere Verwendung aufbereitet. Als Input wird lediglich die Prozess-ID der entsprechenden App benötigt. Danach läuft der Prozess vollständig automatisch ab und verlangt keine weitere Benutzerinteraktion.

Da Android-Apps in Java umgesetzt sind, wird ihr Zustand zur Laufzeit dementsprechend durch Java-Objekte repräsentiert. In unserem Prozess wird dieser Zustand so weit als möglich wiederhergestellt. Dies beinhaltet einerseits die effektiven Inhalte der Objekte wie beispielsweise Zahlen oder Strings und andererseits die Verknüpfung der Objekte untereinander. Dadurch können die wiederhergestellten Informationen in den richtigen Kontext gebracht werden. Über ein GUI werden die Resultate visualisiert. Die übersichtliche Darstellung der Objekt-Inhalte und -Verknüpfungen ermöglicht so eine exakte Interpretation der rekonstruierten Daten. Zusätzlich stehen Such- und Filtermechanismen zur Verfügung. Um die Ergebnisse unseres Prozesses weiteren möglichen Verarbeitungsschritten zugänglich zu machen, werden diese in einem gängigen Format abgelegt.

Durch den generischen Ansatz haben wir erreicht, dass für den Analyse-Prozess kein tiefgehendes Fachwissen mehr erforderlich ist. Dies macht die forensische Auswertung von Android-Geräten einem grossen Benutzerkreis zugänglich und ermöglicht eine Anwendung in der Praxis.



Alex Joss

Dario Schwab

ObjID	Name	Value	Descriptor
▽ 226820	mMessageItem		Lcom/android/mms/ui/MessageItem;
▷ 226838	mAddress	0798189470	Ljava/lang/String;
▷ 226815	mType	sms	Ljava/lang/String;
▷ 226856	mBody	hello agent xy. this is a secret message. please delete	Ljava/lang/String;
226905_226820_0	mTimestamp	4:56PM	Ljava/lang/String;
226820_1	mCachedFormattedMessage		
199892_226820_2	mContact	0798189470	Ljava/lang/String;
226820_3	mContext		
221200_226820_4	mDeliveryStatus		Lcom/android/mms/ui/MessageItem$DeliveryStatus;
226820_5	mTextContentType		

Ausschnitt zeigt eine gelöschte Kurznachricht inkl. Absender und Sendezeit