KAMAS Usability Study

Allgemeines

Die Systemtests werden voraussichtlich im Zeitraum zwischen 04.10.2015 und 20.10.2015 durchgeführt. Es werden voraussichtlich 5-6 ProbandInnen getestet wobei diese alle aus der IT-Security Domäne kommen. Hierbei streben wir an, 3 ProbandInnen aus der Forschung und 2-3 ProbandInnen aus der Wirtschaft zu haben.

Methode

Um eine gute und aufschlussreiche Evaluierung des KAMAS Prototypen zu garantieren, werden mehrere verschiedene Testansätze zeitgleich bzw. hintereinander durchgeführt.

- Erhebung der persönlichen Daten
- Usertest (Aufgabenbasiert) + Logging + Video
- System Usability Scale (SUS)
- Semi-strukturiertes Interview

Basierend auf den Erkenntnissen dieser Tests werden verschiedene Auswertungen durchgeführt und dokumentiert.

Vorgehensweise

JedeR ProbandIn wird auf einem Handelsüblichen PC den Test durchführen Der Test dauert ca. eine Stunde und wird von einem Testleiter begleitet. Neben den Aufzeichnungen die durch den Testleiter erstellt werden, wird während dem Systemtest auch noch ein Logfile mitgeschrieben und auch ein Bildschirmvideo erstellt (gegebenenfalls kann auch der Proband gefilmt werden um die Gesichtsausdrücke während der einzelnen Aufgaben festzuhalten).

- Testdauer: ca. 1 Stunde
- Anwesende Personen: TestleiterIn und ProbandIn
- System: Notebook 15‘‘ Monitor full HD
-

Forschungsfrage

1. Profitiert der Analyst von extern gespeicherten Wissen bei der Analyse von Behavior Based Malware Analysedaten?
2. Ist die Art der Wissensspeicherung verständlich und nachvollziehbar?
3. Ist die Visualisierung des externen Wissens verständlich für den Probanden / die Probandin?

Ziele

- Testen des Forschungsprototypen auf seine Funktionalität.
- Testen der Visualisierungstechniken auf Verständlichkeit in Bezug auf die Domäne.
- Testen der Effektivität der Wissensspeicherung und Repräsentation im System.

Nicht Ziele

- Vergleich des Prototypen mit einem anderen Analysesystem.
- Performancetests

KAMAS Usability Study: Road Map

Willkommen (ca. 5 min)

Hallo, mein Name ist <NAME> und ich werde Sie heute durch den etwa ein stündigen Test unseres Systems begleiten. Vor dem Beginn des Tests werde ich Ihnen nähere Informationen zum Testablauf vorlesen. Diese Maßnahme ist insofern notwendig, da ich sicherstellen möchte, dass alle Testpersonen die gleichen Informationen erhalten.

Bei diesem Test wird ein interaktives Tool zur Exploration von System- und API-Calls sowie zum Analysieren von Call-Sequenzen (werden auch Regeln genannt) auf seine Nutzbarkeit getestet. Wichtig ist an dieser Stelle anzumerken dass nicht Sie als Person getestet werden sondern das System. Ich möchte Sie bitten ehrliche Aussagen zu dem System zu tätigen, sei es positiv oder negativ, beides ist für uns sehr hilfreich, um die Entwicklung des Systems bestmöglich fortzusetzen.

Zu Beginn werde ich Ihnen ein paar Fragen zu Ihrer Person, Ausbildung, beruflichen Werdegang und der Erfahrung in Bezug auf Malware Analyse stellen. Anschließend werde ich Ihnen 5 Aufgaben vorlesen und Sie werden versuchen diese zu lösen. Lassen Sie sich bei den Aufgaben so viel Zeit wie sie benötigen und sprechen Sie ihre Gedanken einfach laut aus.

Ich werde Sie während des Tests beobachten und dazu Notizen machen. Während der Testphase unseres Systems werden die Interaktionen aufgezeichnet (protokolliert), so dass wir diese im Nachhinein genau analysieren können. Ebenso wird von diesem Test ein Video aufgenommen. Dieses Video hilft uns bei der Testanalyse und der Verbesserung der Applikation. Alle Aufzeichnungen dieses Tests werden vertraulich für Forschungszwecke in diesem Projekt behandelt und nicht an außenstehende Personen weitergegeben. Diesbezüglich möchte ich Sie bitten unsere Einverständniserklärung zu unterzeichnen.

Einverständniserklärung von Probandin oder Probanden unterzeichnen lassen!

Falls während des Tests Fragen auftreten, lassen Sie es mich bitte sofort wissen. Um die Testanalyse zu vereinfachen, möchte ich Sie bitten, bei den Aufgaben Ihre Gedankenweg und jeden Schritt den Sie unternehmen werden, laut auszusprechen (Bspw. Ich klicke jetzt auf <XY> um eine Sortierung der Daten nach <YZ> vorzunehmen …).

Gibt es noch Fragen?

<Starten der Kamera für den Test>

Ich werde nun die Kamera für die Aufzeichnung des Tests starten.

Personenbezogene Fragen

1. Als erstes beginnen wir mit den zuvor besprochenen Personenbezogenen Fragen:

Name: _____

Geschlecht: _____

Alter: _____

Ausbildung: _____

Beruf: _____

Tätigkeit: _____

2. Wie viele Jahre Berufserfahrung haben Sie in der IT?

◯ 0 – 4 ◯ 5 – 9 ◯ 10 – 14

◯ 15 – 19 ◯ 20 – 24 ◯ 25 – 29

◯ 30 – 34 ◯ 35 – 39 ◯ 40 - 44

3. Haben Sie Erfahrung in der verhaltensbasierten Malwareanalyse?

◯ Ja

◯ Nein

4. Wie würden Sie sich selbst in Bezug auf Ihre / deine Fertigkeiten in diesem Feld einstufen?

◯ Anfänger ◯ Fortgeschritten ◯ Erfahren ◯ Experte

5. Mit welchen Interfaces arbeiten Sie bei der Malwareanalyse (mehrere Möglichkeiten)

◯ Konsolenprogramme (z.B.: Shell, CMD)

◯ Texteditoren (z.B.: VI, VIM, NANO, Notepad++)

◯ Interaktive Interfaces (z.B.: Interfaces die die Analysedaten als Text darstellen und weitere Optionen zur Analyse zur Verfügung stellen.)

◯ Grafisch aufbereitete Interfaces (z.B.: Interfaces die auch grafisch aufbereitete Statistiken oder ähnliches in Bezug auf die Analysedaten zur Verfügung stellen.)

◯ Grafisch aufbereitete interaktive Interfaces (z.B.: Interfaces die eine Interaktion mit den grafisch aufbereiteten Daten zulassen um weitere Einsichten über die Analysedaten zu gewinnen)

6. Können Sie mir ein paar Programme nennen?

Besten Dank für die Informationen. Beginnen wir nun mit den Aufgaben in unserem zu testenden System. Bitte sprechen Sie alle Gedankengänge laut aus während der Lösung der Aufgaben.

Test der Software (ca. 30 min)

Kennenlernen des KAMAS-Systems zur interaktiven Exploration von behavior based Malware Analysedaten.

Vor ihnen sehen Sie nun das Interface des Analysesystems. Bitte sehen Sie sich das Interface einmal an um einen ersten Eindruck zu gewinnen.

Was ist der erste Eindruck?

Danke für die erste Einschätzung des Systems. Sehen wir uns nun das System einmal in Detail bezüglich der gebotenen Optionen und Funktionalitäten an.

Welche Funktionalitäten können Sie nach ihrem ersten Eindruck ableiten?

<!!! NICHT SAGEN!!!: Auf der rechten Seite sehen Sie eine Tabelle mit 3 Spalten in der die einzelnen System- und API-Calls dargestellt werden die im Analyse File vorkommen. Darunterliegend sind einige verschiedene Filter zu sehen.>

Aufgabe 1:

Bitte versuchen Sie alle Calls die zwischen 5 und 30 mal in dem Analysefile vorkommen und in denen der Wortlaut „file“ vorkommt zu filtern. Wie viele Einträge haben Sie gefunden?

◯ 9 Stk. (richtig gelöst) ◯ Falsch Antwort Anzahl Versuche: _____

Welche 3 der 9 gefundenen Calls kommen am häufigsten vor?

◯ SetFilePointer ◯ NtQueryInformationFile ◯ NtSetInformationFile

Welche Features haben Sie benutzt um die 3 häufigsten Calls zu finden?

◯ Balken ◯ Sortieren der Spalte ◯ Nummern

Welcher Call kommt am Häufigsten vor und wie oft?

◯ NtSetInformationFile ◯ 23 mal

Woran haben Sie das erkannt?

◯ Balken ◯ Sortieren der Spalte ◯ Nummern

Bitte versuchen Sie nun alle Calls zu finden die zwischen 5 und 30 in dem Analysefile vorkommen und in denen der Wortlaut „Open“ vorkommt. Wir wollen nur die großgeschriebenen finden.

Wie viele Calls haben sie gefunden?

◯ 1 Stk. (richtig gelöst) ◯ Falsche Antwort Anzahl versuche:_____

Haben Sie Auswirkungen der Selektionen auf der rechten Seite in der Mitte des Bildschirms bemerkt?

◯ Ja ◯ Nein

Warum?

Aufgabe 2:

Nachdem Sie nun alle Regeln in der Mitte des Bildschirmes gefiltert haben die den zuvor gesuchten Call „NtOpenFile“ beinhalten (rechter Bildschirm). Werden wir nun in diesem Bereich weitere Filteroptionen benutzen.

Wie viele Regeln werden derzeit in der Mitte des Bildschirmes (Regelvisualisierung) angezeigt?

◯ 9 Stk. (richtig gelöst) ◯ Falsche Antwort Anzahl versuche:_____

Was können Sie in der Tabelle alles Ablesen?

◯ Occurrence ◯ Verteilung ◯ Regel ◯ Länge der Regel

Bitte filtern Sie nun nach Regeln die eine Auftrittshäufigkeit zwischen 30 und 90 haben und eine Länge zwischen 3 und 5. Wie viele Regeln sind nun sichtbar?

◯ 5 Stk. (richtig gelöst) ◯ Falsche Antwort Anzahl versuche:_____

Wie viele Samples sind in diesem grafisch dargestellten Analysefile zusammengepackt?

◯ 16 Stk. (richtig gelöst) ◯ Falsche Antwort Anzahl versuche:_____

Welche weiteren Optionen können Sie unter der Sample Anzahl erkennen.

◯ multiples only ➔ nur Regeln anzeigen deren Anzahl ein Vielfaches der Sampleanzahl ist.

◯ equal only ➔ nur Regeln anzeigen deren Calls gleichmäßig auf alle Samples verteilt sind.

Anmerkungen:

Aufgabe 3:

<RESET DER FILTER> Bitte filtern Sie nun nach allen Calls die zwischen 1 und 50 mal vorkommen. Jeder der Calls soll den Wortlaut „file“ enthalten.

◯ Sofort geschafft ◯ herumprobiert und geschafft ◯ nicht geschafft

Nachdem Sie das nun erledigt haben, möchten Sie nun auch nur die Regeln betrachten deren Auftrittshäufigkeit ein Vielfaches der Sampleanzahl ist.

◯ multiples only sofort angekreuzt ◯ herumprobiert und geschafft ◯ nicht geschafft

Im nächsten Schritt wollen Sie nur die Regeln sehen deren auftreten gleich in allen Samples verteilt ist.

◯ equal only sofort angekreuzt ◯ herumprobiert und geschafft ◯ nicht geschafft

Wie würden Sie die Grafik im Bereich der Spalte „Rule“ interpretieren?

◯ Zusammenfassung des Textes ◯ Eine Art Fingerprint ◯ Sonstiges

Anmerkungen zu Sonstiges:

Klicken Sie nun eine der gefilterten Regeln an. Welche Informationen können Sie jetzt ablesen?

◯ Occurrence ◯ Verteilung ◯ Rule Image ◯ Length ◯ ID

◯ Die einzelnen enthaltenen Calls in einer eigenen Tabelle.

Welche Bedeutung können Sie aus dieser Verbindungslinie zwischen den beiden Tabellen ablesen?

Sonstiges:

Hätten Sie eine andere Form der Darstellung erwartet?

◯ ja ◯ nein

Sonstiges:

Aufgabe 4:

Bitte versuchen Sie nun eine Regel in die Wissensdatenbank einzufügen ***(<Hinweis: Drag & Drop>).***

◯ Sofort geschafft ◯ herumprobiert und geschafft ◯ nicht geschafft

War es für Sie klar, dass Sie gerade erfolgreich ein Element in die Wissensdatenbank eingefügt haben?

◯ ja ◯ nein

Anmerkung:

Nachdem Sie nun eine oder mehrere Regeln zu der Struktur hinzugefügt haben, ist ihnen da etwas in der Visualisierung aufgefallen?

◯ Regeln werden in unterschiedlichen Farben angezeigt ◯ nichts aufgefallen

Aufgabe 5:

<SYSTEMNEUSTART> Versuchen Sie bitte nach allen Calls zu suchen die mit „Nt“ beginnen. Nun grenzen Sie bitte noch alle Regeln aus die nicht ein Vielfaches der Sampleanzahl sind und über keinerlei Gleichverteilung der Calls verfügen. Im nächsten Schritt wollen Sie nur noch alle Regeln sehen mit einer Auftrittshäufigkeit von max 64.

Wie viele bekannte und teilweise bekannte Regeln finden Sie hier?

◯ Bekannte: <_____> ◯ Teilweise bekannte <_____>

Ist das Farbschema für Sie passend oder haben Sie etwas anderes erwartet?

◯ ja ◯ nein

Anmerkung:

Filtern Sie nun noch nach Regeln die mindestens 10 Calls enthalten müssen. Wählen Sie eine dieser Regeln aus und versuchen Sie in dieser Regel ein Muster zu erkennen. Sie können auch gerne verschiedene Regeln betrachten um sich einen besseren Überblick zu verschaffen.

Wie haben Sie die Muster in den Regeln erkannt?

◯ Gedanklicher Abgleich der Namen ◯ Selbst nach Muster basierend auf den Strings gesucht

◯ Die Bögen an der Seite zeigen die Muster automatisch auf

Würden sie diese Bögen als hilfreich einstufen?

◯ ja ◯ nein

Warum?:

Herzlichen Dank dass sie sich für den Test der Software zeitgenommen haben. Im nächsten Schritt wollen wir nun noch in einem kurzen Gespräch die Ihre Eindrücke zu unseren Forschungsprototypen reflektieren.

Fragebogen zum Softwarehandling → SUS (max 2 min)

Bitte füllen sie diese Fragebogen schnell nach ihrem 1. Eindruck nach aus.

1. Ich denke, dass ich das System gerne häufig benutzen würde.

Stimme überhaupt nicht zu 1	2	3	4	Stimme voll zu 5
○	○	○	○	○

2. Ich fand das System unnötig komplex.

Stimme überhaupt nicht zu 1	2	3	4	Stimme voll zu 5
○	○	○	○	○

3. Ich fand das System einfach zu benutzen.

Stimme überhaupt nicht zu 1	2	3	4	Stimme voll zu 5
○	○	○	○	○

4. Ich glaube, ich würde die Hilfe einer technisch versierten Person benötigen, um das System benutzen zu können.

Stimme überhaupt nicht zu 1	2	3	4	Stimme voll zu 5
○	○	○	○	○

5. Ich fand, die verschiedenen Funktionen in diesem System waren gut integriert.

Stimme überhaupt nicht zu 1	2	3	4	Stimme voll zu 5
○	○	○	○	○

6. Ich denke, das System enthielt zu viele Inkonsistenzen.

Stimme überhaupt nicht zu 1	2	3	4	Stimme voll zu 5
○	○	○	○	○

7. Ich kann mir vorstellen, dass die meisten Menschen den Umgang mit diesem System sehr schnell lernen.

Stimme überhaupt nicht zu 1	2	3	4	Stimme voll zu 5
○	○	○	○	○

8. Ich fand das System sehr umständlich zu nutzen.

Stimme überhaupt nicht zu 1	**2**	**3**	**4**	**Stimme voll zu 5**
○	○	○	○	○

9. Ich fühlte mich bei der Benutzung des Systems sehr sicher.

Stimme überhaupt nicht zu 1	**2**	**3**	**4**	**Stimme voll zu 5**
○	○	○	○	○

10. Ich musste eine Menge lernen, bevor ich anfangen konnte das System zu verwenden.

Stimme überhaupt nicht zu 1	**2**	**3**	**4**	**Stimme voll zu 5**
○	○	○	○	○

Semi-strukturiertes Interview (ca. 15 min)

Waren die Filtermöglichkeiten verständlich?

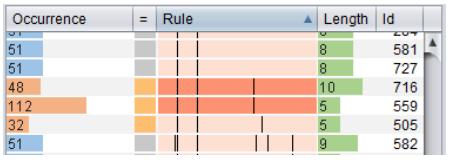
Haben die verschiedenen Visualisierungsmöglichkeiten zum Verständnis beigetragen?

Haben Sie die Verwendung der Knowledge Datenbank verstanden?

Haben Ihnen die verschiedenen Möglichkeiten der Wissensrepräsentation bei der Findung ihrer Entscheidungen geholfen?

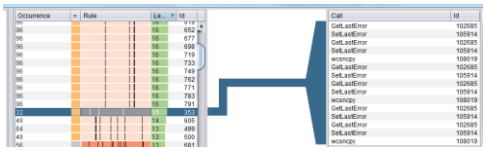
Wie wurde das Expertenwissen im System repräsentiert?

Waren die Balkendiagrame in den Tabellen hilfreich? Wofür?

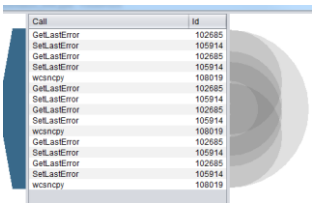


Waren die Histogramme bei den Regeln hilfreich? Wofür?

War die Verbindungslinie zwischen den Tabellen hilfreich? Wofür?



Waren die Bögen (Arc-Diagram) neben der Detailtabelle hilfreich? Wofür?



Wie ist ihr Gesamteindruck zu der Software?

Herzlichen Dank dass sie an diesem Softwaretest teilgenommen haben.

Software Testaufgaben zum Nachlesen

Aufgabe 1:

Bitte versuchen Sie alle Calls die zwischen 5 und 30 mal in dem Analysefile vorkommen und in denen der Wortlaut „file“ vorkommt zu filtern.

- Wie viele Einträge haben Sie gefunden?
- Welche 3 der 9 gefundenen Calls kommen am häufigsten vor?
- Welche Features haben Sie benutzt um die 3 häufigsten Calls zu finden?
- Welcher Call kommt am Häufigsten vor und wie oft?
- Woran haben Sie das erkannt?

Bitte versuchen Sie nun alle Calls zu finden die zwischen 5 und 30 in dem Analysefile vorkommen und in denen der Wortlaut „Open“ vorkommt. Wir wollen nur die großgeschriebenen finden.

- Wie viele Calls haben sie gefunden?
- Haben Sie Auswirkungen der Selektionen auf der rechten Seite in der Mitte des Bildschirms bemerkt?
- Warum?

Aufgabe 2:

Nachdem Sie nun alle Regeln in der Mitte des Bildschirmes gefiltert haben die den zuvor gesuchten Call „NtOpenFile“ beinhalten (rechter Bildschirm). Werden wir nun in diesem Bereich weitere Filteroptionen benutzen.

- Wie viele Regeln werden derzeit in der Mitte des Bildschirmes (Regelvisualisierung) angezeigt?
- Was können Sie in der Tabelle alles Ablesen?
- Bitte filtern Sie nun nach Regeln die eine Auftrittshäufigkeit zwischen 30 und 90 haben und eine Länge zwischen 3 und 5. Wie viele Regeln sind nun sichtbar?
- Wie viele Samples sind in diesem grafisch dargestellten Analysefile zusammengepackt?
- Welche weiteren Optionen können Sie unter der Sample Anzahl erkennen?

Aufgabe 3:

Bitte filtern Sie nun nach allen Calls die zwischen 1 und 50 mal vorkommen. Jeder der Calls soll den Wortlaut „file“ enthalten.

Nachdem Sie das nun erledigt haben, möchten Sie nun auch nur die Regeln betrachten deren Auftrittshäufigkeit ein Vielfaches der Sampleanzahl ist.

Im nächsten Schritt wollen Sie nur die Regeln sehen deren auftreten gleich in allen Samples verteilt ist.

- Wie würden Sie die Grafik im Bereich der Spalte „Rule“ interpretieren?
- Klicken Sie nun eine der gefilterten Regeln an. Welche Informationen können Sie jetzt ablesen?
- Welche Bedeutung können Sie aus dieser Verbindungslinie zwischen den beiden Tabellen ablesen?
- Hätten Sie eine andere Form der Darstellung erwartet?

Aufgabe 4:

Bitte versuchen Sie nun eine Regel in die Wissensdatenbank einzufügen ***(<Hinweis: Drag & Drop>).***

- War es für Sie klar, dass Sie gerade erfolgreich ein Element in die Wissensdatenbank eingefügt haben?
- Nachdem Sie nun eine oder mehrere Regeln zu der Struktur hinzugefügt haben, ist ihnen da etwas in der Visualisierung aufgefallen?

Aufgabe 5:

<SYSTEMNEUSTART> Versuchen Sie bitte nach allen Calls zu suchen die mit „Nt“ beginnen. Nun grenzen Sie bitte noch alle Regeln aus die nicht ein Vielfaches der Sampleanzahl sind und über keinerlei Gleichverteilung der Calls verfügen. Im nächsten Schritt wollen Sie nur noch alle Regeln sehen mit einer Auftrittshäufigkeit von max 64.

- Wie viele bekannte und teilweise bekannte Regeln finden Sie hier?
- Ist das Farbschema für Sie passend oder haben Sie etwas anderes erwartet?

Filtern Sie nun noch nach Regeln die mindestens 10 Calls enthalten müssen. Wählen Sie eine dieser Regeln aus und versuchen Sie in dieser Regel ein Muster zu erkennen. Sie können auch gerne verschiedene Regeln betrachten um sich einen besseren Überblick zu verschaffen.

- Wie haben Sie die Muster in den Regeln erkannt?
- Würden sie diese Bögen als hilfreich einstufen?