TECHNISCHE UNIVERSITÄT DRESDEN

Faculty of Computer Science Institute of Systems Architecture, Chair of Privacy and Data Security

Bachelor-Arbeit

Thesis title

Student name

Geboren am: 25. Dezember 1999 in Dresden
Matrikelnummer: 4803900
Immatrikulationsjahr: 2018

Betreuer
Supervisor

Betreuender Hochschullehrer
Prof. Dr. Professor

TECHNISCHE UNIVERSITÄT DRESDEN

Fakultät Informatik • Institut für Systemarchitektur • Professur für Datenschutz und Datensicherheit

AUFGABENSTELLUNG FÜR DIE BACHELORARBEIT

Name, Vorname des Studenten: Köllner, Tobias
Immatrikulationsnummer: 4803900
Studiengang: Bachelor Informatik
E-Mail: tobias.koellner@mailbox.tu-dresden.de

Thema: Kontextsensitivität für Netzwerk-Sicherheits-Monitoring

Zielstellung:

Zur Erhöhung der Sicherheit von Netzwerken werden häufig Techniken wie Network security monitoring (NSM) sowie intrusion detection (IDS) verwendet. Inbsesondere die Menge an falsch-positiven Meldungen stellt hierbei eine große Herausforderung dar. Um dieses Problem sowie die generelle Interpretierbarkeit der Beobachtungsdaten zu verbessern können zusätzliche Informationen gesammelt werden, die man als Netzwerkkontext bezeichnen kann.

Der erste Teil der Arbeit soll untersuchen, wie solche Kontextinformationen sowohl während des Betriebs von NSM-Systemen als auch während der Signatur/Modell-Erstellung im Rahmen von IDS gesammelt und verwendet werden können. Ziele hierbei sind, solche Möglichkeiten auf theoretischer Ebene wie auch von open-source Implemntierungen zu sichten und hierbei einen kritischen Kontextbegriff im Vergleich zu etablierten Kontextbegriffen in der Literatur in Bezug auf Netzwerke zu entwickeln.

Aufbauend auf diesen Resultaten kann eine einfache praktische Auswertung verfügbarer Implementierungen mit explizitem Hinblick auf die kontextsensitiven Fähigkeiten durchgeführt werden. Hierfür ist ein Plan für eine minimale Testumgebung sowie das Design von geignetem Netzwerkverkehr erforderlich.

In der Arbeit sollen schwerpunktmäßig folgende Teilaufgaben bearbeitet werden:

- Überblick und Analyse existierender NSM-Ansätze in Bezug auf Kontext- und Umgebungsbewusstsein. Hierbei sollen mindestens folgende Forschungsfragen bearbeitet werden:
  - Lassen sich generelle Kategorien von Kontext im Rahmen von NSM formulieren?
  - Welche Kontextinformation kann während der Regelgenerierung im Unterschied zu generell verfügbaren Regel aus öffentlichen Quellen berücksichtigt werden?
  - Welche Techniken wurden vorgeschlagen, um Kontextinformation während des regulären Betriebs zu sammeln und wie werden diese dann genutzt?
  - Inwifern gibt es Möglichkeiten der Anpassungen an Änderungen der Netzwerkumgebung, etwa der Topologie oder der genutzen Protokolle?
  - Wie stark trägt Kontextinformation zur Reduktion von falsch-Positiven bei?
- Es soll eine Evaluation der Fähigkeit von Kontextnutzung von verfügbaren open-source-Implementierungen (etwa Plugins in Zeek oder Netzdefinitionen in Suricata) durchgeführt werden.

Verantwortlicher Hochschullehrer: Dr. Stefan Köpsell
Institut: Systemarchitektur
Beginn am: 3.6.2022 Einzureichen am: 19.8. 2022

3.6.22, T. Köllner .....
Datum, Unterschrift der/des Studierenden

.....
Unterschrift des betreuenden Hochschullehrers

Kopie: Sekretariat + elektronische Datei

Selbstständigkeitserklärung

Hiermit versichere ich, dass ich das vorliegende Dokument mit dem Titel *Thesis title* selbstständig und ohne unzulässige Hilfe Dritter verfasst habe. Es wurden keine anderen als die in diesem Dokument angegebenen Hilfsmittel und Quellen benutzt. Die wörtlichen und sinngemäß übernommenen Zitate habe ich als solche kenntlich gemacht. Während der Anfertigung dieses Dokumentes wurde ich nur von folgenden Personen unterstützt:

Supervisor name

Zusätzliche Personen waren an der geistigen Herstellung des vorliegenden Dokumentes nicht beteiligt. Mir ist bekannt, dass die Nichteinhaltung dieser Erklärung zum nachträglichen Entzug des Hochschulabschlusses führen kann.

Student name

Zusammenfassung

The abstract serves as a summary of the work. It should concisely (around half a page) answer the following questions:

- What is the problem tackled in this thesis?
- Why is this problem relevant?
- What contributions does this thesis contain with regards to the problem?
- Which scientific method(s) was/were used and what were their results?

Inhaltsverzeichnis

1 Einführung

1.1 Analyse/Beschreibung des Ausmaßes der Mängel bestehender nicht-kontextsensitiver IDS-Systeme

2 Hintergrund

2.1 Definition eines Kontextbegriffs im Rahmen der Zugriffskontrolle

Kontext ist ein Begriff unter dem sich die meisten Menschen zwar etwas vorstellen, aber nur schwer erläutern oder gar korrekt und vollständig definieren können [6]. Auch herrscht in verschiedenen Fachbereichen, jede davon mit anderen Sachverhalten und Problemen die die jeweiligen Autoren versuchend zu lösen, eine andere Auffassung darüber welche Ansprüche eine Definition erfüllen muss . Das erschwert eine allumfassende, konkrete Definition zusätzlich [4]. Ich will in diesem Kapitel also nicht versuchen Kontext abschließend zu definieren, da dies in Anbetracht der vielen verschiedenen Definitionen und dem fehlenden Konsens wie Kontext zu definieren ist [16, 3] schlicht nicht möglich ist bzw. den Rahmen dieser Arbeit übersteigen würde. Stattdessen werde ich versuchen mithilfe, meiner Ansicht nach relevanter Definitionen für den Bereich der Informatik bzw. der Zugriffskontrolle, die historische Entwicklung des Kontextbegriffs darzustellen. Das soll dem Leser ermöglichen nachzuvollziehen auf welcher Grundlage ich mich für die von mir gewählte Definition entschieden habe.

2.1.1 Historische Entwicklung des Kontextbegriffs

Eine der frühesten Definitionen von Kontext [14] bestimmt als 3 Hauptaspekte von Kontext an welchem Ort, mit welcen Personen und in der Nähe welcher Ressourcen man sich befindet.
Des weiteren beinhaltet laut [14] Kontext Attribute wie Beleuchtung, Lautstärke, den Grad der Netzwerkverbindung, Kommunikationskosten, Kommunikationsbandbreite und die soziale Situation.
Nach der Definition von Dey et al. [6] ist "Kontext jede Information die genutzt werden kann um die Situation einer Entität zu charakterisieren. Eine Entität ist eine Person, ein Objekt oder ein Ort mit Relevanz für die Interaktion zwischen Nutzer und Anwendung. Das schließt auch Nutzer und Anwendung selbst mit ein". Sie wird allgemein hin von den meisten anderen Autoren als Quasikonsens akzeptiert [16, 3, 2] oder als Ausgangspunkt für ihre eigene Definition genutzt [18, 9].
Kaltz et al. [17] versteht Kontext als ein Kontextraum also eine Kombination aus Kontextparametern, und Dienstleistungsbeschreibungen in Form von $C = \{U; P; L; T; D; I; S\}$ definiert. Dabei ist U das Set aus Nutzern und den dazugehörigen Rollen, P die Prozesse und Aufgaben, L der Ort, T der Zeitfaktor, D beschreibt das Gerät, I die verfügbaren Informationen und

S die verfügbaren Dienstleistungen. Ein spezifischer Kontext ist somit ein Punkt in diesem Raum.
Bazire und Brézillon [4] haben 150 Kontextdefinitionen analysiert und sind dabei zu der Erkenntnis gekommen das Kontext wie eine Begrenzung fungiert welche das Verhalten eines Systems, Nutzers oder Computers in einer bestimmten Tätigkeit beeinflussen. Allerdings herrscht ihrer Ansicht nach kein Konsens darüber ob Kontext extern oder intern, ein Set aus Informationen oder Abläufen, statisch oder dynamisch ist.

Kayes et al.[9] definieren Kontextinformationen in Bezug auf Zugriffskontrollentscheidungen als relevante Informationen über den Zustand einer Entität (Nutzer, Ressource, Ressourcenbesitzer) und deren Umgebung oder die Beziehung zwischen Entitäten.

2.1.2 Kontextdefinition mit Zugriffskontrollbezug

2.2 Kontextkategorisierung

Das Hauptanliegen

2.2.1 Analyse bereits vorgeschlagener Kategorien

Abowd et al.[1] haben einen der führenden Mechanismen zur Definition von Kontexttypen vorgeschlagen. Sie identifizierten Ort, Zeit, Identität, und Aktivität als primäre Kontexttypen. Weiterhin wird sekundärer Kontext als Kontext definiert der durch Nutzung von Primärkontext erschlossen werden kann.

Schilit et al. [14] kategorisieren Kontext basierend auf 3 Fragen, die genutzt werden können um den Kontext zu bestimmen, in 3 Kategorien:

1. Wo man sich befindet: Enthalt alle Informationen die sich auf einen Ort beziehen, beispielsweise GPS-Koordinaten, Namen von Institutionen oder Gebäuden (ein Café, ein Krankenhaus, eine Universität), spezifische Namen (z.B.: Technische Universität Dresden) spezifischen Adressen(z.B.: APB Nöthnitzer Str. 46) oder Nutzerpräferenzen (z.B. das Lieblingsrestaurant eines Nutzers)

2. Mit wem man sich zusammen aufhält: Information über die Personen die um einen herum anwesend sind

3. Welche Ressourcen sich in der Nähe befinden: Informationen darüber welche Ressourcen (Maschinen, technische Geräte, Betriebsmittel) sich im direkten Umfeld eines Nutzers befinden

Henricksen et al.[8] ordnet Kontext basierend auf der betrieblichen Katergorisierungstechnik in 4 verschiedene Kategorien:

1. Messbar: Informationen die aus direkt messbaren Werten bestehen. Diese ändern sich oft oder gar kontinuierlich.

2. Statisch: Informationen die sich während der Lebenszeit eines Systems gleich bleiben.

3. Profiliert: Informationen die sich selten ändern.

4. Abgeleitet: Informationen die unter Verwendung anderer Daten gewonnen wurden.

Van Bunningen et al. [15] ordnen Kategoriesungsversuche in zwei übergeordnete Gruppen: Betrieblich und Konzeptionell.

1. Betriebliche Kategorisierung: Einordnung anhand dessen wie der Kontext akquiriert, modelliert und behandelt wird.
2. Konzeptionelle Kategorisierung: Einordnung anhand der Bedeutung des Kontextes und der konzeptionellen Beziehungen

Chong[5] schlägt Historie als Kontextkategorie vor. Dabei werden die Werte die eine bestimmte Messgröße in der Vergangenheit angenommen hat als Kontext definiert. Das erlaubt die Festlegung eines Standardzustandes dieser Werte und unter Umständen eine Vorhersage darüber welche Werte die Messgrößen zukünftig erwartung

2.2.2 Notwendigkeit einer Taxonomie

Die Evaluation verschiedener Kategorisierungsschemata zeigt das keine Kategorisierung allen Ansprüchen gerecht werden kann[12].

2.3 Erstellung einer Kontexttaxonomie

Im folgenden möchte ich meinen Versuch einer Kombination der bereits vorgeschlagenen Kategorisierungsschemata erläutern. Dazu lege ich zuerst die Definition der einzelnen Kategorien im Bezug auf kontextsensitive Zugriffskontrolle fest. Die Kategorien müssen dafür, abhängig davon mit welchem Fokus sie der jeweilige Autor konstruiert hat, mehr oder weniger stark angepasst werden. Danach definiere ich in welcher Form die Kontextinformationen in den einzelnen Kategorien vorliegen müssen und wie man Informationen aus unterschiedlichen, teils analogen Quellen auf für Netzwerkverkehr anwendbare

2.3.1 Betrieblich

Primär

Kontextinformationen die gesammelt werden können ohne bereits vorhandene Daten zu verwenden oder zu kombinieren. [12]

Sekundär

“Kontext der durch das verarbeiten von Primärkontext erschlossen werden kann. Dies kann durch die Kombination einzelner Datenpunkte einer oder mehrerer Kategorien oder durch Abfragen weiterer Informationen mithilfe der Primärinformationen geschehen.

2.3.2 Konzeptionell

Zeit

Wann etwas geschieht.

Ort

Wo sich etwas befindet.

Identität

Wer etwas macht.

Aktivität

Was jemand macht.

Grund

Warum jemand etwas macht.

2.3.3 Historie/Zeitliche Entwicklung

Historie früherer Verbindungen/Verbindungsanfragen einer Entität (Annahme das Netzwerkteilnehmer eindeutig identifizierbar sind)

Statisch - Dynamisch

Änderungsrate

Wie häufig sich Werte/Attribute ändern

Abtastrate

Wie oft Werte/Attribute im Netzwerk aktualisiert werden

Anfrage-rate

Wie oft Werte/Attribute im Netzwerk von Netzwerkteilnehmern angefragt werden

2.3.4 Logisch

Protokoll nach dem OSI-Schichtmodell

Anwendung

Transport

Netzwerk

Entität

Gerät

Nutzer

Anwendung

2.3.5 Physisch

Gerät

Umgebung

2.4 Kontextgewinnung

- network (open ports) | Nessus - devices in network | Configuration Management Database (CMDB), nmap - cve reference - yes/no - protocol header

2.5 Werte einer Kategorie

Historie =======

3 Voraussetzungen und verwandte Arbeiten

3.0.1 Kontextsensitivität

Ein System ist kontextsensitiv wenn es Kontext verwendet um dem Nutzer mit für ihn relevanten Informationen und/oder Dienstleistungen zu versorgen. Die Relevanz hängt dabei von der Aufgabe des Nutzers ab [6].

3.0.2 Situation

3.0.3 Umgebung

3.0.4 Netzwerk-Sicherheits-Monitoring

3.0.5 Policy

3.0.6 Intrusion Detection

Angriffserkennung ist "der Prozess des Überwachung von Ereignissen in einem Computersystem oder Netzwerk, und die Analyse dieser Ereignisse auf Anzeichen eines möglichen Zwischenfalls. Gemeint sind damit Verstöße oder unmittelbare Bedrohungen von Sicherheitsrichtlinien, Akteptanzrichtlinien oder Standardsicherheitspraktiken"[13].

3.0.7 IDS

Auf Grundlage der Definition von Intrusion Detection, ist ein IDS somit Software die den Prozess, einen Eingriff zu erkennen, automatisiert [13].

4 Design

4.1 Kontextkategorisierung

Das Hauptanliegen

4.1.1 Analyse bereits vorgeschlagener Kategorien

Abowd et al.[1] haben einen der führenden Mechanismen zur Definition von Kontexttypen vorgeschlagen. Sie identifizierten Ort, Zeit, Identität, Zeit und Aktivität als primäre Kontexttypen. Weiterhin wird sekundärer Kontext als Kontext definiert der durch Nutzung von Primärkontext erschlossen werden kann.

Schilit et al. [14] kategorisieren Kontext basierend auf 3 Fragen, die genutzt werden können um den Kontext zu bestimmen, in 3 Kategorien:

1. Wo man sich befindet: Enthalt alle Informationen die sich auf einen Ort beziehen, beispielsweise GPS-Koordinaten, Namen von Institutionen oder Gebäuden (ein Café, ein Krankenhaus, eine Universität), spezifische Namen (z.B.: Technische Universität Dresden) spezifischen Adressen(z.B.: APB Nöthnitzer Str. 46) oder Nutzerpräferenzen (z.B. das Lieblingsrestaurant eines Nutzers)

2. Mit wem man sich zusammen aufhält: Information über die Personen die um einen herum anwesend sind

3. Welche Ressourcen sich in der Nähe befinden: Informationen darüber welche Ressourcen (Maschinen, technische Geräte, Betriebsmittel) sich im direkten Umfeld eines Nutzers befinden

Henricksen et al.[8] ordnet Kontext basierend auf der betrieblichen Katergorisierungstechnik in 4 verschiedene Kategorien:

1. Messbar: Informationen die aus direkt messbaren Werten bestehen. Diese ändern sich oft oder gar kontinuierlich.

2. Statisch: Informationen die sich während der Lebenszeit eines Systems gleich bleiben.

3. Profiliert: Informationen die sich selten ändern.

4. Abgeleitet: Informationen die unter Verwendung anderer Daten gewonnen wurden.

Van Bunningen et al. [15] ordnen Kategoriesungsversuche in zwei übergeordnete Gruppen: Betrieblich und Konzeptionell.

1. Betriebliche Kategorisierung: Einordnung anhand dessen wie der Kontext akquiriert, modelliert und behandelt wird.

2. Konzeptionelle Kategorisierung: Einordnung anhand der Bedeutung des Kontextes und der konzeptionellen Beziehungen

Chong[5] schlägt Historie als Kontextkategorie vor. Dabei werden die Werte die eine bestimmte Messgröße in der Vergangenheit angenommen hat als Kontext definiert. Das erlaubt die Festlegung eines Standardzustandes dieser Werte und unter Umständen eine Vorhersage darüber welche Werte die Messgrößen zukünftig erwartung

4.1.2 Notwendigkeit einer Taxonomie

Die Evaluation verschiedener Kategorisierungsschemata zeigt das keine Kategorisierung allen Ansprüchen gerecht werden kann[12].

4.2 Erstellung einer Kontexttaxonomie

Im folgenden möchte ich meinen Versuch einer Kombination der bereits vorgeschlagenen Kategorisierungsschemata erläutern. Dazu lege ich zuerst die Definition der einzelnen Kategorien im Bezug auf kontextsensitive Zugriffskontrolle fest. Die Kategorien müssen dafür, abhängig davon mit welchem Fokus sie der jeweilige Autor konstruiert hat, mehr oder weniger stark angepasst werden. Danach definiere ich in welcher Form die Kontextinformationen in den einzelnen Kategorien vorliegen müssen und wie man Informationen aus unterschiedlichen, teils analogen Quellen auf für Netzwerkverkehr anwendbare

4.2.1 Konzeptionell

Primär

Kontextinformationen die gesammelt werden können ohne bereits vorhandene Daten zu verwenden oder zu kombinieren. [12]

Sekundär

“Kontext der durch das verarbeiten von Primärkontext erschlossen werden kann. Dies kann durch die Kombination einzelner Datenpunkte einer oder mehrerer Kategorien oder durch Abfragen weiterer Informationen mithilfe der Primärinformationen geschehen.

4.2.2 Betrieblich

Grund

Aktivität

Zeit

Ort

Identität

4.2.3 Historie/Zeitliche Entwicklung

Historie früherer Verbindungen/Verbindungsanfragen einer Entität (Annahme das Netzwerkteilnehmer eindeutig identifizierbar sind)

Statisch - Dynamisch

Änderungsrate

Wie häufig sich Werte/Attribute ändern

Abtastrate

Wie oft Werte/Attribute im Netzwerk aktualisiert werden

Anfrage-rate

Wie oft Werte/Attribute im Netzwerk von Netzwerkteilnehmern angefragt werden

4.2.4 Logisch

Protokoll nach dem OSI-Schichtmodell

Anwendung

Transport

Netzwerk

Entität

Gerät

Nutzer

Anwendung

4.2.5 Physisch

Gerät

Umgebung

4.3 Kontextgewinnung

- network (open ports) | Nessus - devices in network | Configuration Management Database (CMDB), nmap - cve reference - yes/no - protocol header

4.4 Werte einer Kategorie

Historie

4.5 Umwandlung der Taxonomie in IDS-Signaturen

Um die im Abschnitt Kontexttaxionomie festgelegten Kategorien in Signaturen für ein Intrusion Detection System umzuwandeln zu können gilt es gewisse Dinge zu beachten:

Die Kontextsensitivität eines Computers unterscheidet sich drastisch von der eines Menschen. Rechensysteme sind sehr gut darin Daten zu erfassen und zu sammeln, aber Menschen sind immer-noch nötig um verschiedene Kontexte zu erkennen und zu entscheiden welches Handeln in einer bestimmten Situation angemessen ist [6].
Der limitierende Faktor des Potenzials eines kontextsensitiven Systems ist das Maß an Kontext das ein Entwickler vorhersehen und kodieren kann.
Es ist aber weder beim Design noch später bei der Implementierung unmöglich alle Zusammenhänge vorherzusehen.
Dementsprechend schwer wird ist es ein in sich geschlossenes und allumfassendes Regelset festzulegen [12].

Nach Greenberg et al. [7] gibt 3 non-triviale Hauptaspekte die man beim Entwerfen eines kontextsensitiven Systems beachten sollte:

1. Spezifizieren aller möglichen Kontextzustände
2. Wissen welche Informationen einen konkreten Kontextzustand akkurat festlegen.
3. Welche Aktion im jeweiligen Zustand ausgeführt werden sollen.

4.5.1 Festlegung auf bestimmte IDS-Implementierungen

Es steht eine Vielzahl an Software- und Hardwareimplementierungen zur Entscheidung von Zugriffskontrollentscheidungen zur Verfügung. Je nachdem welche Kriterien auf welche Art und Weise erfüllt werden müssen hängt vom spezifischen Anwendungsfall ab.

4.5.2 Analyse der Regel-Syntax eines IDS

Wie arbeiten die einzelnen IDS? Wie einfach lassen sich die Zustände die auftretender Kontext annehmen kann in Regeln festlegen?

4.5.3 Abgleich zwischen Taxonomie und den in der Praxis zur Verfügung stehenden Informationen

Wie gut lässt sich bestimmter Kontext in verfügbaren Informationen finden bzw. sind die verfügbaren Informationen in die Taxonomie einsortierbar?

4.6 Anspruch an das IDS

Um die Performance eines IDS verbessern zu können, muss man festlegen welche Kriterien die Leistung beeinflussen bzw. bestimmen. Mell et al.[10] nennen in ihrer Übersicht verschiedene Charakteristiken zur quantitativen Bestimmung der Erkennungsgenauigkeit eines IDS und erläutern zusätzlich die Wechselwirkungen zwischen einzelnen Kriterien, die beim Vergleich verschiedener IDS-Lösungen beachtet werden sollten.

Abdeckung

Gibt an welche Typen von Angriffen ein IDS unter idealen Bedingungen feststellen kann.

Wahrscheinlichkeit falscher Alarme

Gibt die Wahrscheinlichkeit das durch ein IDS ausgelöste Alarme durch gutartigen bzw. nicht-schädlichen Netzwerkverkehr verursacht wurden an.

$$\textit{Rate an falsch – Positiven Meldungen} = \frac{\textit{Anzahl falscher Alarme}}{\textit{Anzahl aller Alarme}}$$

Wahrscheinlichkeit einer Erkennung

Gibt die Rate der durch das IDS korrekt erkannten Angriffe an.

$$\textit{Erkennungswarscheinlichkeit} = \frac{\textit{Anzahl korrekt erkannter Angriffe}}{\textit{Anzahl aller Angriffe}}$$

Resistenz

Ein signatur-basiertes IDS bzw. der menschliche Administrator hinter dem System weisen Probleme auf die nicht direkt beim Umgang mit verarbeitetem Netzwerkverkehr, sondern schon bei der bewussten, unbewussten, oder erzwungenen Entscheidung welcher Netzwerkverkehr überhaupt in Frage kommt, entstehen:

1. Ein zu große Menge an zu verarbeitendem Netzwerkverkehr die die Verarbeitungskapazität eines IDS übersteigt kann dazu führen das Netzwerkpakete verworfen und Angriffe nicht erkannt werden
2. Pakete die zwar nicht bösartig sind aber so konstruiert das sie möglichst viele IDS Signaturen auslösen, überfordern den Administrator oder stören eventuell sogar die Verarbeitung von Paketen generell.
3. Ein Angreifer könnte eine Vielzahl "harmlosereräber trotzdem noch als schädlich zu deklarierende Pakete senden um einen größeren Angriff im Netzwerkverkehr zu verschleiern.
4. Pakete die möglicherweise vorhandene Fehler im IDS selbst ausnutzen.

Korrelation zwischen Einzelereignissen

Demonstriert wie gut ein IDS eine Korrelation zwischen einzelnen Ereignissen, möglicherweise verschiedenen Ursprungs herzustellen. Die Ereignisse können dabei aus Routern, Firewalls, Anwendungen, dem IDS selbst oder einer großen Bandbreite anderer Quellen stammen.

Unbekannte Angriffe vorhersehen

Gibt an wie gut ein IDS einen Angriff erkennt der so noch nicht aufgetreten ist. Signaturbasierte IDS sind allgemein, mit wenigen Ausnahmen, nicht in der Lage solch einen Angriff zu erkennen. Normalerweise erhöht die Fähigkeit eines Systems einen noch unbekannten Angriff zu erkennen, im Vergleich zu Systemen die dies nicht versuchen, zusätzlich die Rate an falsch-positiven Meldungen.

Identifizieren von Angriffen

Wie gut ein IDS einem Angriff den es erkennt, einen Namen oder eine Kategorie, beispielsweise ein CVE-Nummer, zuordnen kann.

Beurteilung eines Angriffs

Indikator dafür ob ein IDS den Erfolg und die Auswirkungen eines Angriffes korrekt beurteilen kann. In aktuellen Netzwerkumgebungen schlagen viele Angriffs(-vesuche) fehl. Die meisten IDS unterscheiden allerdings nicht zwischen erfolgreichen und fehlgeschlagenen Angriffen. Für den selben Angriff können manche IDS die Anzeichen dafür ob ein Angriff erfolgreich war erkennen, andere lediglich das ein Angriff stattgefunden hat, allerdings ohne feststellen zu können ob er erfolgreich war. Die Fähigkeit, den Grad zu dem ein Angriff auf das überwachte System erfolgreich war zu beurteilen ist essenziell. Eine Vorfilterung der Meldungen durch das IDS vereinfacht die Arbeit des Netzwerkadministrators bzw. Analysten stark, da so eine Analyse des Angriffsszenarios und der Korrelation einzelner Angriffe vereinfacht wird. Diese Fähigkeit bei einem gegebenen IDS messen zu können setzt das Wissen, darüber welche Angriffe erfolgreich sind und welche nicht, voraus.

4.6.1 Einordnung der Kriterien

Die Wahrscheinlichkeit einen Angriff zu erkennen variiert mit der Rate an falsch-positiven Meldungen. Bei der Konfiguration eines IDS kann entweder die Falsch-positiv-Rate oder die Erkennungsrate optimiert werden.

4.6.2 •

[11] In dieser Arbeit beschäftige ich mich ausschließlich mit sicherheitsrelevanten Leistungsmetriken. Dabei will ich hauptsächlich den Einfluss von Kontextsensitivtät auf die Abdeckung, die Erkennungswahrscheinlichkeit, die Wahrscheinlichkeit falscher Alarme und die Interpretierbarkeit von Meldungen durch einen menschlichen Nutzer betrachten. Zusätzlich will ich beleuchten inwiefern Kontext die Korrelation zwischen Einzelereignissen und das Identifizieren von Angriffen ermöglicht bzw. verbessert.

4.7 Kontextsensitivität

5 Implementierung

5.0.1 Umsetzung/Implementierung der Taxonomie in IDS-Signaturen

5.1 Test der kontextsensitiven Signaturen

5.1.1 (Auswahl eines bereits existierenden/ Erstellung eines eigenen) Datensatzes + dazugehörige Label

5.1.2 Aufbau eines oder mehrerer Netzwerke

5.1.3 Setup der verschiedenen IDS

5.1.4 Grundlage mit non-kontextsensitiven Signaturen auf Datensatz

5.1.5 Test der kontextsensitiven Signaturen auf Datensatz

6 Evaluation

This chapter is usually expected to present which experiments you did as part of your thesis, what results came out of them and what these results tell us about to which extent your design improves the state of the art with regards to the requirements specified in chapter As a rough outline, this chapter should address the following questions:

6.1 Auswertung der Testergebnisse

6.2 Vergleich der IDS-Alerts mit Datensatzlabeln

6.2.1 Baselineauswertung

6.2.2 Vergleich der Performance gemäß der in 1.1 festgelegten Kriterien zwischen non-kontextsenitiven und kontextsenitiven Signaturen

6.2.3 Vergleich der unterschiedlichen getesteten Kontextkategorie(kombinationen)

6.3 “Bewertung” der theoretischen Mächtigkeit einzelner Kategorien

6.4 Beurteilung/Einschätzung der tatsächlichen Verfügbarkeit von Kontext im Netzwerk

6.5 Urteil/Ranking der Kontextarten hinsichtlich der Erhöhung der Netzwerksicherheit

7 Konklusion/Schlussfolgerung

In this chapter, you summarize the conclusions that can be drawn from your thesis with regards to solving the problem explained in the introduction section. Furthermore, you should concisely explain further experiments or design options that may be interesting to pursue in future work.

Literatur

[1] Gregory D. Abowd u. a. “Towards a Better Understanding of Context and Context-Awareness”. In: *Handheld and Ubiquitous Computing*. Hrsg. von Hans-W. Gellersen. Bearb. von Gerhard Goos, Juris Hartmanis und Jan van Leeuwen. Bd. 1707. Series Title: Lecture Notes in Computer Science. Berlin, Heidelberg: Springer Berlin Heidelberg, 1999, S. 304–307. ISBN: 978-3-540-66550-2 978-3-540-48157-7. DOI: 10.1007/3-540-48157-5_29.

[2] Jose Aguilar, Marxjhony Jerez und Taniana Rodríguez. “CAMeOnto: Context awareness meta ontology modeling”. en. In: *Applied Computing and Informatics* 14.2 (Juli 2018), S. 202–213. ISSN: 22108327. DOI: 10.1016/j.aci.2017.08.001.

[3] Unai Alegre, Juan Carlos Augusto und Tony Clark. “Engineering context-aware systems and applications: A survey”. en. In: *Journal of Systems and Software* 117 (Juli 2016), S. 55–83. ISSN: 01641212. DOI: 10.1016/j.jss.2016.02.010.

[4] Mary Bazire und Patrick Brézillon. *Understanding Context Before Using It*. en. Hrsg. von David Hutchison u. a. Bd. 3554. Series Title: Lecture Notes in Computer Science. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005, S. 29–40. ISBN: 978-3-540-26924-3 978-3-540-31890-3. DOI: 10.1007/11508373_3.

[5] Suan Khai Chong u. a. “Context-Aware Sensors and Data Muling”. In: (), S. 15.

[6] Anind K Dey. “Understanding and Using Context”. In: (2001), S. 4.

[7] Saul Greenberg. “Context as a dynamic construct”. In: *Human–Computer Interaction* 16.2-4 (2001), S. 257–268.

[8] Karen Henricksen. “A framework for context-aware pervasive computing applications”. In: (2003).

[9] A S M Kayes, Jun Han und Alan Colman. “ICAF: A Context-Aware Framework for Access Control”. en. In: (2012), S. 8.

[10] Peter Mell u. a. “An overview of issues in testing intrusion detection systems”. In: (2003).

[11] Aleksandar Milenkoski u. a. “Evaluating Computer Intrusion Detection Systems: A Survey of Common Practices”. en. In: *ACM Computing Surveys* 48.1 (Sep. 2015), S. 1–41. ISSN: 0360-0300, 1557-7341. DOI: 10.1145/2808691. URL: https://dl.acm.org/doi/10.1145/2808691 (besucht am 27. 05. 2022).

[12] Charith Perera u. a. “Context Aware Computing for The Internet of Things: A Survey”. In: *IEEE Communications Surveys & Tutorials* 16.1 (2014), S. 414–454. ISSN: 1553-877X. DOI: 10.1109/SURV.2013.042313.00197.

[13] Karen Scarfone, Peter Mell u. a. “Guide to intrusion detection and prevention systems (idps)”. In: *NIST special publication* 800.2007 (2007), S. 94.

[14] Bill N Schilit, Norman Adams und Roy Want. “Context-Aware Computing Applications”. In: (1994), S. 7.

[15] Arthur H Van Bunningen, Ling Feng und Peter MG Apers. “Context for ubiquitous data management”. In: *International Workshop on Ubiquitous Data Management*. IEEE. 2005, S. 17–24.

[16] Wei Liu, Xue Li und Daoli Huang. “A survey on context awareness”. In: *2011 International Conference on Computer Science and Service System (CSSS)*. 2011 International Conference on Computer Science and Service System (CSSS). Nanjing, China: IEEE, Juni 2011, S. 144–147. ISBN: 978-1-4244-9762-1. DOI: 10.1109/CSSS.2011.5972040.

[17] J. Wolfgang Kaltz, Jürgen Ziegler und Steffen Lohmann. “Context-aware Web Engineering: Modeling and Applications”. In: *Revue d’intelligence artificielle* 19.3 (1. Juni 2005), S. 439–458. ISSN: 0992499X. DOI: 10.3166/ria.19.439-458.

[18] Andreas Zimmermann, Andreas Lorenz und Reinhard Oppermann. “An Operational Definition of Context”. In: *Modeling and Using Context*. Hrsg. von Boicho Kokinov u. a. Bd. 4635. Series Title: Lecture Notes in Computer Science. Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, S. 558–571. ISBN: 978-3-540-74254-8. DOI: 10.1007/978-3-540-74255-5_42.