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

Zusammenfassung 4

1 Hintergrund 7
1.1 Definition eines Kontextbegriffs im Rahmen der Zugriffskontrolle 7
1.1.1 Historische Entwicklung des Kontextbegriffs 7
1.1.2 Darlegung/Erläuterung meiner Kontextdefinition 8
1.2 Kontextkategorisierung 8
1.2.1 Analyse bereits vorgeschlagener Kategorien 8
1.2.2 Erstellung einer Kontexttaxonomie 8

2 Voraussetzungen und verwandete Arbeiten 9
2.0.1 Kontextsensitivität 9

3 Design 10
3.1 "Übersetzung"/Transfer der Taxonomie/Kategorien in IDS-Signaturen 11
3.1.1 Festlegung auf bestimmte IDS-Implementierungen 11
3.1.2 Analyse der IDS-Regel-Syntax 11
3.1.3 Abgleich zwischen Taxonomie und den in der Realität zur Verfügung stehenden Informationen 11
3.1.4 Umsetzung/Implementierung der Taxonomie in IDS-Signaturen 11

4 Implementierung 12
4.1 Test der kontextsensitiven Signaturen 12
4.1.1 (Auswahl eines bereits existierenden/ Erstellung eines eigenen) Datensatzes + dazugehörige Label 12
4.1.2 Aufbau eines oder mehrerer Netzwerke 12
4.1.3 Setup der verschiedenen IDS 12
4.1.4 Baseline mit non-kontextsensitiven Signaturen auf Datensatz 12
4.1.5 Test der kontextsensitiven Signaturen auf Datensatz 12

5 Evaluation 13
5.1 Auswertung der Testergebnisse 13
5.2 Vergleich der IDS-Alerts mit Datensatzlabeln 13
5.2.1 Baselineauswertung 13
5.2.2 Vergleich der Performance gemäß der in 1.1 festgelegten Kriterien zwischen non-kontextsenitiven und kontextsenitiven Signaturen 13
5.2.3 Vergleich der unterschiedlichen getesteten Kontextkategorie(kombinationen) 13

5.3 “Bewertung” der theoretischen Mächtigkeit einzelner Kategorien 13
5.4 Beurteilung/Einschätzung der tatsächlichen Verfügbarkeit von Kontext im Netzwerk 13
5.5 Urteil/Ranking der Kontextarten hinsichtlich der Erhöhung der Netzwerksicherheit 13

6 Konklusion/Schlussfolgerung 14

1 Hintergrund

1.1 Definition eines Kontextbegriffs im Rahmen der Zugriffskontrolle

Kontext ist ein Begriff den die meisten Menschen zwar etwas vorstellen, aber nur schwer erläutern oder gar korrekt und vollständig definieren können [4]. Auch herrscht in verschiedenen Fachbereichen, mit unterschiedlichen Auffassungen darüber was Kontext eigentlich ist und welche Ansprüche eine Definition erfüllen muss . Das erschwert eine allumfassende, konkrete Definition zusätzlich [3]. Ich will in diesem Kapitel also nicht versuchen Kontext abschließend zu definieren da dies in Anbetracht der vielen verschiedenen Definitionen und dem fehlenden Konsens [7, 2] schlicht nicht möglich ist bzw. den Rahmen dieser Arbeit übersteigen würde. Stattdessen werde ich versuchen mithilfe, meiner Ansicht nach relevanten Definitionen für den Bereich der Informatik bzw. der Zugriffskontrolle, die historische Entwicklung des Kontextbegriffs darzustellen und so zumindest darzulegen wieso ich mich für die von mir gewählte Definition entschieden habe und worauf diese Definition aufbaut.

1.1.1 Historische Entwicklung des Kontextbegriffs

Eine der frühesten Definitionen von Kontext [6] 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 [6] Kontext Attribute wie Beleuchtung, Lautstärke, den Grad der Netzwerkverbindung, Kommunikationskosten, Kommunikationsbandbreite und die soziale Situation.

Nach Dey [4], die von den meisten anderen Autoren akzeptierte Definition [7, 2, 1] oder als Ausgangspunkt für ihre eigene Definition [9, 5], 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".
In [8] wird Kontext als ein Kontextraum also eine Kombination aus Kontextparametern, domain ontology elements 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 [3] 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 [5] definiert Kontextinformationen in Bezug auf Zugriffskontrollentscheidungen als relevante Informationen über den Zustand einer Entität (Nutzer, Ressource, Ressourcenbesitzer) und deren Umgebung oder die Beziehung zwischen Entitäten.

1.1.2 Darlegung/Erläuterung meiner Kontextdefinition

1.2 Kontextkategorisierung

1.2.1 Analyse bereits vorgeschlagener Kategorien

1.2.2 Erstellung einer Kontexttaxonomie

2 Voraussetzungen und verwandete Arbeiten

In this section, you should point out which requirements a good solution to the problem addressed in your thesis should fulfill. It makes sense to state functional as well as non-functional requirements.

When it comes to the related work, you should then point out to which extent the existing works / proposed solutions already fulfill the requirements you introduced previously.

2.0.1 Kontextsensitivität

"A system is context-aware if it uses context to provide relevant information and/or services to the user, where relevancy depends on the user's task."

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.

3 Design

In this chapter, you should present your solution in detail but at a conceptual level. This means that you explain the overall design including your motivation for this design but you do not provide details on the actual implementation of your design (e.g., in which programming language you wrote it, how the software is structured and so on). This means that you should also point out the aspects where you had different design options and in which points they differ. A good approach to write this chapter is to make yourself aware of the different aspects and design problems that need to be addressed in your design. To do so, you can then proceed repeatedly in three steps:

1. Explain a design problem that needs to addressed by the solution (e.g. to enable anonymous communication over the internet, participants need to be able to send messages to each other without revealing identifying to the corresponding receiver).

2. Discussion of design choices (e.g. Mix Networks, DC-Networks, etc.) with regards to the requirements from the previous chapter and identification of the most promising choices.

After the second step, you start the next iteration by identifying design problems that arise when you want to use the most promising design choice. For example, if Mix networks turn out to be the most promising approach for your requirements, you then need to address the question how the mix network should be designed (e.g. how are mix nodes chosen by the users of the anonymization network? How do mix nodes process messages?). Once you identified the most promising solutions to that, you can then start the next iteration and so on until there are no more open design questions that you are aware of.

What is important for the reader is to understand that the contextual awareness of machines is from a radically different nature than the one of humans. Also, that computational systems are good at gathering and aggregating data, but humans are still better at recognizing contexts and determining what action is appropriate in a certain situation [2]. On the other hand, positivism looks at context as a representational problem, considering it as a "form of information, delineable, stable and separable from activity" [5]. The definitions made in the context-aware field, naturally adopt this point of view. For instance, Dey's definition [10] allows designers to use the concept for determining why a situation occurs and use this to encode some action in the application [26], making the concept operational in terms of the actors and information sources [17]. Nevertheless, since the definition inherently has a positivist view, the potential of C-AS remains limited to the context that developers are able to encode and foresee. [2]

3.1 “Übersetzung”/Transfer der Taxonomie/Kategorien in IDS-Signaturen

3.1.1 Festlegung auf bestimmte IDS-Implementierungen

3.1.2 Analyse der IDS-Regel-Syntax

3.1.3 Abgleich zwischen Taxonomie und den in der Realität zur Verfügung stehenden Informationen

3.1.4 Umsetzung/Implementierung der Taxonomie in IDS-Signaturen

4 Implementierung

In this chapter, you should provide technical details on how you actually implemented the design that you derived in the previous chapter.

4.1 Test der kontextsensitiven Signaturen

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

4.1.2 Aufbau eines oder mehrerer Netzwerke

4.1.3 Setup der verschiedenen IDS

4.1.4 Baseline mit non-kontextsensitiven Signaturen auf Datensatz

4.1.5 Test der kontextsensitiven Signaturen auf Datensatz

5 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:

5.1 Auswertung der Testergebnisse

5.2 Vergleich der IDS-Alerts mit Datensatzlabeln

5.2.1 Baselineauswertung

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

5.2.3 Vergleich der unterschiedlichen getesteten Kontextkategorie(kombinationen)

5.3 “Bewertung” der theoretischen Mächtigkeit einzelner Kategorien

5.4 Beurteilung/Einschätzung der tatsächlichen Verfügbarkeit von Kontext im Netzwerk

5.5 Urteil/Ranking der Kontextarten hinsichtlich der Erhöhung der Netzwerksicherheit

6 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] 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. URL: https://linkinghub.elsevier.com/retrieve/pii/S2210832717301643 (besucht am 08. 06. 2022).

[2] 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. URL: https://linkinghub.elsevier.com/retrieve/pii/S0164121216000467 (besucht am 08. 06. 2022).

[3] 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. URL: http://link.springer.com/10.1007/11508373_3 (besucht am 28. 07. 2022).

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

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

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

[7] 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. URL: http://ieeexplore.ieee.org/document/5972040/ (besucht am 28. 06. 2022).

[8] 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. URL: http://ria.revuesonline.com/article.jsp?articleId=5984 (besucht am 06. 06. 2022).

[9] 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. URL: http://link.springer.com/10.1007/978-3-540-74255-5_42 (besucht am 01. 06. 2022).