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

zur Erlangung des akademischen Grades

Bachelor of Science (B.Sc)

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

Supervisor name

Weitere Personen waren an der geistigen Herstellung der vorliegenden Arbeit 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 General notes

This chapter is not part of the typical outline of written thesises and only serves the purpose of providing more general advice that is not specific to any of the following chapters.

- Citations can be done using the cite command. It is possible to place multiple references in the cite command, e.g.
- In general, it might not be the best approach to write the texts of the chapters in the same order as the chapters appear (e.g. first write introduction, then background, and so on. Instead, you can also consider to start writing the introduction chapter first to check how good your understanding of your own contribution is, as during writing, you are likely to discover gaps in your argumentation or implicit assumptions that you made.
- To get into writing mode, you may just start to write down your thoughts freely first without being to critical about your argumentation, grammar and so on and incrementally improve your text.
- When you write your thesis or any other scientific text, it is recommended that you think about what the target audience of your work is and following from that, what you can assume about their prior knowledge. When it comes to a thesis, you should assume the reader to have the same knowledge about the topic as your fellow students may have.

2 Einführung

The introduction serves the purpose of educating the reader about the broader context or research problem that your work addresses and its relevance as well as the relevance of your work towards solving this problem. As a rough guideline, this section should be written to answer the following questions:

1. What is the problem your work addresses?
2. Why is it desirable to solve this problem? (e.g. which new possibilities/use cases become possible if the problem is solved)
3. Roughly, what contribution towards solving the problem will you present to the reader in this thesis?

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

2.1.1 Festlegung der IDS-Performancekriterien(bspw. Erkennungsrate/Rate der falsch-positiven Meldungen)

2.2 Verbesserung bestehender IDS-Lösungen(bessere/weniger Zugriffskontrollentscheidungen)

2.3 Erläuterung der Vorteile eines kontextsensitiven IDS

3 Hintergrund

The background chapter aims to give a more detailed introduction into the context of your work and provides additional information that enables the target audience to understand the argumentations and motivations that you explain in the following chapters. This chapter is typically read on demand, if in the following chapters, the reader encounters a term or argumentation that is not immediately clear from the corresponding chapter alone.

3.1 Definition eines Kontextbegriffs im Rahmen der Zugriffskontrolle

3.1.1 Historische Entwicklung des Kontextbegriffs

Eine der frühesten Definitionen von Kontext [2] bestimmt als 3 Hauptaspekte von Kontext an welchem Ort, mit wem und in der Nähe welcher Ressourcen man sich befindet. Desweiteren beinhaltet laut [2] Kontext Attribute wie Beleuchtung, Lautstärke, den Grad der Netzwerkverbindung, Kommunikationskosten, Kommunikationsbandbreite und die soziale Situation. Nach Dey [1], eine der am meist akzeptiertesten, wenn nicht sogar die akzeptierteste, Definition, 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".
[3]

3.1.2 Darlegung/Erläuterung meiner Kontextdefinition

3.2 Kontextkategorisierung

3.2.1 Analyse bereits vorgeschlagener Kategorien

3.2.2 Erstellung einer Kontexttaxonomie

4 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.

4.0.1 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.

5 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.

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

5.1.1 Festlegung auf bestimmte IDS-Implementierungen

5.1.2 Analyse der IDS-Regel-Syntax

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

5.1.4 Umsetzung/Implementierung der Taxonomie in IDS-Signaturen

6 Implementierung

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

6.1 Test der kontextsensitiven Signaturen

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

6.1.2 Aufbau eines oder mehrerer Netzwerke

6.1.3 Setup der verschiedenen IDS

6.1.4 Baseline mit non-kontextsensitiven Signaturen auf Datensatz

6.1.5 Test der kontextsensitiven Signaturen auf Datensatz

7 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 4. As a rough outline, this chapter should address the following questions:

- Which questions did you want to answer or which hypothesises did you want to test with the experiments?
- Which metrics did you measure and how does their value relate to the questions you want to answer?
- Which system parameters exist that may have an influence on the value on the metric? Which ones did you vary in your experiments? Intuitively, what are your expectations with regards to the relationship between the system parameters and the metrics?
- How did the experiments that you did actually looked like, or how did you actually measure the chosen metrics?
- What are the actual values that you measured in your experiments? Do they match your intuition about the relationship between the system parameters and the metrics?

7.1 Vergleich der IDS-Alerts mit Datensatzlabeln

7.1.1 Baselineauswertung

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

7.1.3 Vergleich der unterschiedlichen getesteten Kontextkategorie(kombinationen)

7.2 “Bewertung” der theoretischen Mächtigkeit einzelner Kategorien

7.3 Beurteilung/Einschätzung der tatsächlichen Verfügbarkeit von Kontext im Netzwerk

7.4 Urteil/Ranking der Kontextarten hinsichtlich der Erhöhung der Netzwerksicherheit

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

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

[3] 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).