Technische
Hochschule
Rosenheim
Technical University of Applied Sciences

Fakultät für Informatik

Studiengang Informatik

Attack surfaces and security measures in enterprise-level Platform-as-a-Service solutions

Bachelor Thesis

von

Lukas Grams

Datum der Abgabe: tt.mm.jjjj TODO
Erstprüfer: Prof. Dr. Reiner Hüttl
Zweitprüfer: Prof. Dr. Gerd Beneken

Erklärung

Ich versichere, dass ich diese Arbeit selbständig angefertigt, nicht anderweitig für Prüfungszwecke vorgelegt, keine anderen als die angegebenen Quellen oder Hilfsmittel benützt sowie wörtliche und sinngemäße Zitate als solche gekennzeichnet habe.

Rosenheim, den tt.mm.jjjj TODO

Lukas Grams

Kurzfassung (deutsch)

TODO

Kurzfassung (englisch)

The increasing amount of Platform-as-a-Service (PaaS) solutions, cloud-hosted environments and microservice architectures introduces new attack scenarios. This creates the need for new defense strategies in both Development and Operations. Especially solutions providing (Kubernetes conformant) container orchestration are identifiably different and in high demand compared to long established solutions. This calls for a more detailed, focused examination. This thesis aims to answer the following questions:

- What generic security risks emerge when providing or using a multi-tenant PaaS solution, with each tenant developing, deploying and running their own applications?

- How can a PaaS provider (serving internal and/or external users) mitigate those risks?

- In this scope and from a PaaS provider viewpoint, how does an on-premise solution compare to a public cloud solution?

Another goal is to recommend security measures for different implementation use cases. If achievable within the provided time frame, it will additionally try and answer this question:

- Does a cloud-hosted, self-managed solution (buy IaaS, provide PaaS) offer benefits in contrast to the solutions compared above? (In case there are sufficient differences, another set of security measures will be recommended for this solution)

Examples for widely used PaaS solutions in different environments include OpenShift as an on- premise solution, Azure Kubernetes Service as a public cloud solution. To include a cloud-hosted, self-managed solution, OpenShift running on self-managed instances in Azure could serve as an example.
To achieve these goals, the thesis will first limit the view on the problem to a manageable scope by focusing on specific components of a few (2-3) commonly used PaaS solutions, specifically Certified Kubernetes solutions. Components providing Kubernetes conformity will be the main focus, as these bear the most significance across all Kubernetes Certified solutions.
Looking at three common attack scenarios, it will then determine vulnerabilities and attack vectors, as well as their potential damage and rate those risks:

- Malicious third party attacking the underlying infrastructure from within the LAN and/or the internet

- Malicious third party attacking from inside a hijacked container, i.e. remotely executing code or commands

- Bad User, i.e. a negligent, hijacked or malicious developer (account) risking compromise

of his own and/or other applications

Possible measures to mitigate those risks will also be explored, evaluated and (if possible) put to use in practical examples, leveraging the PaaS solutions within scope. With the results gathered, the thesis will compare different best practice implementations for different use cases and recommend measures for each.

Schlagworte:

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1 Introduction

TODO

1.1 Motivation

TODO

1.2 Objective

TODO

1.3 Scope limitation

TODO

2 Theory

TODO

2.1 Platform-as-a-Service

TODO

2.2 Containers

TODO

2.3 Orchestration

TODO

2.4 TODO

TODO

3 Potential attack scenarios

TODO

3.1 Defining procedures and approach

TODO

3.2 Scenario 1: Third party over network

TODO

3.2.1 TODO: Vector one

TODO

3.2.2 TODO

TODO

3.3 Scenario 2: Third party inside container

TODO

3.3.1 TODO: Vector one

TODO

3.3.2 TODO

TODO

3.4 Scenario 3: Bad user

TODO

3.4.1 TODO: Vector one

TODO

3.4.2 TODO

TODO

4 PaaS solution risk analysis

TODO

4.1 Differentiating on-premise and public cloud environments

TODO

4.2 OPTIONAL: Comparison of cloud-hosted, self-managed environments

If this is omitted, the section above will become the chapter TODO

5 Best-Practice implementations

TODO

5.1 On-premise environment

TODO

5.2 Public cloud environment

TODO

5.3 OPTIONAL: cloud-hosted, self-managed environment

TODO

6 Summary

TODO

7 Wichtige Hinweise

Hier sind einige wichtige Hinweise zur Verwendung dieser Vorlage zusammengefasst, die erfahrungsgemäß oft falsch gemacht werden. Fehler bitte an jochen.schmidt@fh-rosenheim.de melden.

7.1 Abbildungen und Tabellen

Da dies leider immer wieder falsch gemacht wird (mit erheblichen Auswirkungen auf das Layout), hier einige Hinweise zur Positionierung von Bildern und Tabellen. Im professionellen Textsatz werden diese als Gleitobjekte behandelt. Wie der Name impliziert, bedeutet dies, dass Abbildungen (und Tabellen) relativ unabhängig vom Text platziert werden. Insbesondere sollten Sie Latex *niemals* dazu zwingen, Bilder genau an der von Ihnen vorgegebenen Stelle zu positionieren (z. B. mit Positionsangaben wie [h] oder schlimmer [h!]). Es gibt dann für Latex keine Freiheit mehr, den Text richtig zu setzen, was unschöne Lücken zur Folgen hat. Zudem wird durch ein Platzieren mitten im Text der Lesefluss unterbrochen.

> Gleitobjekte sollten daher immer mit [t] oder [tb] positioniert werden, oder bei großen Bildern auf Einzelseiten bzw. wenn mehrere Objekte auf einer textfreien Seite gesammelt werden sollen mit [p], alternativ mit [tbp].

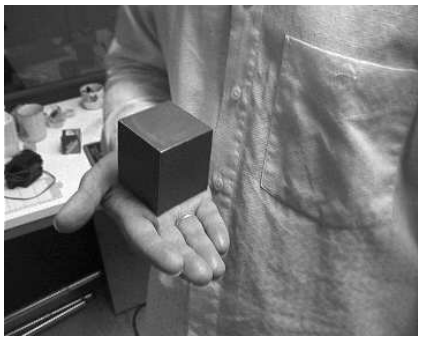
Falls dadurch Bilder immer weiter vom eigentlichen Text wegrutschen, dann ist das ein Hinweise darauf, dass Sie im Verhältnis zu den Bildern zu wenig erläuternden Text geschrieben haben ...

Jede Abbildung erhält eine Abbildungsnummer und eine Bildunterschrift. Diese sollte kurz beschreiben, was in der Abbildung zu sehen ist und zu verstehen sein, ohne dass man den gesamten Text gelesen hat. Jede Abbildung wird im Text beschrieben und referenziert, und zwar über die Abbildungsnummer, also z. B. „Wie in Abb. 3.1 zu sehen ist ... “. Nicht zulässig ist z. B. „Wie in der folgenden Abbildung zu sehen ist ... “ – es gibt keine „folgende“ Abbildung! Ferner sollte darauf geachtet werden, dass alle Abbildungen/Tabellen gut lesbar sind.

Ein Beispiel wird in Abb. 7.1 gezeigt, mit zwei Teilen bestehend aus Abb. 7.1a und 7.1b. Und ein Beispiel für das Einbinden einer Tabelle, zu sehen in Tabelle 7.1.

Bei Bildern verwendet man üblicherweise eine Bildunterschrift (also caption unter dem Bild), bei Tabellen steht die Beschriftung üblicherweise über der Tabelle, da diese von oben nach unten gelesen werden.

Sind die Bilder/Tabellen schmal, kann die Beschriftung stattdessen auch neben dem Bild stehen. Dies ist in Abb. 7.2 zu sehen (für ein Bild), verwendet wurde der Befehl fcapside. Entsprechend funktioniert dies für Tabellen mit tcapside. Die Einstellungen wurden so gewählt, dass die Beschriftung immer an der Innenseite ist (für doppelseitigen Druck). Für eine korrekte Darstellung sind evtl. mehrere Latex-Läufe nötig.



(a) Originalbild

(b) erweitertes Bild

Abbildung 7.1 Beispiel für Bilder, mit Beschreibung. Für nicht selbst erstellte Bilder, die nicht Public Domain sind, ist eine Quellenangabe erforderlich. Bilder aus [Sch01]

Tabelle 7.1 Datenselektion für verschiedene Testdatensätze

Sequence	ARTS	wman	stcams	ARTVZ	ARTSUZ
# Frames	190	40	400	270	190
# relative movements	17955	780	79800	36315	17955
# movements after pre-sel.	14336	623	37915	21788	14343
min. angle in seq.	0.233°	5.95°	0.154°	0.00000171°	0.0388°
max. angle in seq.	81.7°	180°	47.3°	80.3°	80.9°
min. angle after pre-sel.	12.9°	21.1°	17.3°	16.3°	12.9°
max. angle after pre-sel.	81.7°	161°	47.3°	80.3°	80.9°

7.2 Seitenumbrüche

Überlassen Sie Seitenumbrüche Latex, verwenden Sie kein newpage oder pagebreak. Diese Befehle sind nur in sehr wenigen Ausnahmefällen erforderlich. Wenn Sie diese verwenden müssen ist dies eher ein Hinweis darauf, dass etwas anderes mit Ihrem Layout nicht stimmt.

7.3 Schriftart

Als Schriftart für den Haupttext ist Palatino voreingestellt. Dies hat in erster Linie zwei Gründe:

1. Die Schrift ist etwas breiter als z. B. Times und daher gerade für den A4-Druck (zur besseren Lesbarkeit) noch am besten geeignet.

2. Es gibt einen passenden Mathematikzeichensatz dazu, d. h. Ziffern und Buchstaben (wenn beide gerade bzw. kursiv gedruckt werden) sehen im Text und im Mathemodus gleich aus – alles andere wäre unschön.

Passende Mathematikzeichensätze gibt es auch für Times und Computer/Latin Modern, die stattdessen verwendet werden können. Kommentieren Sie in diesem Fall das Paket mathpazo (durch ein %) aus, und dafür lmodern (für Latin Modern) oder mathptmx (für Times) ein.

Weitere Hinweise zu den Themen Seitenlayout/Einfluss der Schriftart findet man z. B. in der Dokumentation zu KomaScript[1].

1 `http://www.komascript.de`

Abbildung 7.2 Beschreibung neben dem Bild mit fcapside. Für Tabellen wird tcapside verwendet

Abbildung 7.3 Beschreibung neben dem Bild mit fcapside. Für Tabellen wird tcapside verwendet

7.4 Druck

Die Vorlage ist für doppelseitigen Druck eingerichtet, den Sie auch verwenden sollten. Wenn (aus welchem Grund auch immer) ein einseitiger Druck erwünscht ist, schalten Sie die Vorlage bitte um: Ganz oben in thesis.tex muss dann aus twoside=true ein twoside=false werden. Wird dies nicht beachtet erscheinen die Seitenzahlen einmal innen und einmal außen, zudem entstehen komplett leere Seiten (die beim doppelseitigen Druck Rückseiten wären, die dazu dienen, dass ein neues Kapitel auf einer rechten Seite anfängt). Wenn Sie die Arbeit nicht selbst drucken, denken Sie daran, den Dienstleister auf den doppelseitigen Druck hinzuweisen.

7.5 Dokument Richtlinien

Beachten Sie bitte auch die Hinweise im separaten Dokument „Hinweise zur Erstellung von Abschlussarbeiten“.

7.6 Diverse Beispiele

Verwenden Sie für Querverweise den Befehl label und ref (Bilder und Tabellen), eqref (Formeln), pageref (Seitenzahlen) damit diese automatisch erzeugt werden. Beachten Sie vor der Abgabe der Arbeit, dass evtl. mehrere Latexläufe erforderlich sind, bis alle Querverweise korrekt sind, da Latex diese während eines Laufs erzeugt und beim nächsten wieder einliest. Durch Verschiebungen können je nach verwendeten Paketen auch drei oder vier Läufe erforderlich sein, bis alles passt.

Beispiel für eine Formel

$$f(x) = \frac{1}{3}x + 5, \quad x \in \mathbb{R}. \tag{7.1}$$

Und noch eine:

$$\boldsymbol{M} = \boldsymbol{A}\boldsymbol{x}\pi, \quad \boldsymbol{A} \in \mathbb{R}^{2\times 2}, \boldsymbol{x} \in \mathbb{R}^2. \tag{7.2}$$

Eine Referenz auf eine Formel: (7.1).

Und eine Literaturreferenz: [Aue00]. Verwenden Sie auf jeden Fall Bibtex (oder etwas äquivalentes), Referenzen sollten auf keinen Fall manuell eingefügt werden.

Gedankenstriche entstehen durch zwei Minuszeichen – und sind länger als ein Bindestrich -.

Und wenn es ganz besonders schön aussehen, dann beachten Sie zusätzlich

- Der Leerraum nach eine Punkt am Satzende ist größer als der nach einer Abkürzung (wie evtl.). Um Latex zu sagen, dass der Punkt kein Satzende ist, wird dieser bei Abkürzungen durch einen Backslash markiert, also so: evtl.\, ohne Leerzeichen zwischen Punkt und Backslash.
- Leerräume zwischen zwei Teilen einer Abkürzung (wie z. B.) sind kleiner als zwischen einzelnen Wörtern, außerdem sollten diese beiden Buchstaben nicht getrennt werden. Dies erreicht man durch: z.\,B.\, wieder ohne Leerzeichen.

Noch ein Hinweis zur Silbentrennung von Wörtern mit Bindestrichen: Diese werden nur direkt am Bindestrich getrennt (so soll es eigentlich sein), was insbesondere im Deutschen oft dazu führt, dass Wörter in den Rand hineinragen (man bekommt auch eine Overfull Box Warnung). Möchte man, dass die Wörter selbst auch getrennt werden dürfen, so kann man

- entweder bei Problemfällen manuelle Trennpunkte durch \- in das Wort einfügen,
- oder statt des Bindestrichs - die Zeichenfolge "= verwenden, also wort"=wort statt wort-wort.

In vielen Fällen sollte man sich zudem fragen, ob das Wort nicht eher zusammen geschrieben werden sollte (statt des Bindestrichs).

A Erstes Kapitel des Anhangs

Wenn Sie keinen Anhang benötigen, dann bitte einfach rausnehmen.

Literaturverzeichnis

[Aue00] T. Auer. *Hybrid Tracking for Augmented Reality*. Dissertation, Technische Universität Graz, Graz, Austria, 2000.

[Sch01] J. Schmidt, I. Scholz und H. Niemann. Placing Arbitrary Objects in a Real Scene Using a Color Cube for Pose Estimation. In B. Radig und S. Florczyk, Hg., *Pattern Recognition, 23rd DAGM Symposium*, Bd. 2191 von *Lecture Notes in Computer Science*, S. 421–428. Springer-Verlag, Berlin, Heidelberg, New York, 2001.