Computer Science

Opponent(s):

Mats Persson and Rickard Karlsson

Respondent(s):

Zak Blacher and Anja Fischer

An Ontological Approach to SIP DoS Attack Detection

Opposition Report, C-level

2010:01

1 A General Evaluation of the Project

The project seems to be a good start of the ontology described in the thesis. It deals with an important topic, since the packet switched networks are growing and will most probably replace the now used public switched telephone networks. Therefore a secure way of communication is needed.

2 Comments on the Project in Relation to the Dissertation

The dissertation describes the project in a good and understandable way.

2.1 Title

The title reflects the key subjects in the project.

2.2 Dissertation Layout

The dissertation layout has a good flow, it describes the whole project in a chronological order.

2.3 Scientific Method

The scientific method used for this project is the Constructing Models method and the techniques used is Reading and referencing, Statistical Material and Observation through Participation.

2.4 Argumentation and Conclusions

The argumentations are stated in an understandable way in the introduction and connects well with the answers given in the conclusion.

2.5 The Abstract

The abstract summarizes the project in a good way, it gives a broad background and describes the project.

2.6 Language Aspects

The language used in the thesis is good overall with only a few grammatical errors. It is however written in a first-person narrative view(“we”, “our”) which does not suit a technical report.

We think that “First order logic” should be “First-order logic”, but we are unsure.

2.7 References and Sources

The references stated in the dissertation are explanative. However there are too few references and the [2] reference need to be finished. Suggestions on where to add references are stated in each chapter.

Some of the references are written without a title when referred to, it looks better with a title.

2.8 General Comments on the Project

This project covers an interesting area.

3 Chapter by Chapter Evaluation of the Dissertation

3.1 Chapter 1

This chapter gives a good background, explains the goals for the project and describes the thesis structure in a good way.

One negative thing is that there is no description of voice messages, it could be good with a short explanation but state that it is not important for this thesis.

Suggestions for references:

- PSTN
- VoIP

- IDS
- DoS attacks
- Explanation of ontologies
- First-order logic

3.2 Chapter 2

This chapter gives a good explanation of SIP, how it works(with nice figures) and a rough overview of ontologies.

It would be nice with a small example on what a “further contact information” can be, on the bottom of page 7.

On page 10, the first sentence of section 2.3, what are the attacks against?

Suggestions for references:

- Instead of ref [7] on page 10, it would be nice with a reference to a more general explanation of ontologies.
- SIP URI, page 9.

3.3 Chapter 3

This chapter gives an understandable overview of the five different attacks.

A definition of *“hard-to-resolve domains”* and *“hard-to-connect domains”* would be appreciated since it is the first time mentioned.

On the bottom of page 15, explain *“it is set back down”*.

On page 17, section 3.3, instead of “...and so on.” write something like “...includes for example First-Line, Headers...” because “and so on” is unspecific.

The first sentence in section 3.2 *“Denial of Service attacks are numerous”*, do you mean that there are many attacks being made or that there are many different types of attacks? If you mean many different types of attacks the sentence should be rewritten to something like “The types of Denial of Service attacks are numerous”.

In the last sentence on page 13, maybe define “major types” to something like “major types of attacks”.

Suggestions for references:

- References to all countermeasures.

3.4 Chapter 4

This chapter gives a good explanation of the threat model and the ontology. Figure 4.1 is a good explaining picture.

However, section 4.4 needs to be explained more. The operators used in the attacks needs a description. It would also be nice with a detailed description of the five attacks.

Suggestions for references:

- A reference to where the explanation of the First-order logic used in this chapter is from.

3.5 Chapter 5

This chapter gives a good technical explanation of how the tests are set up, the figures in this section is good and shows what is described.

One point of interest is the names for the servers and clients in the experiments. We think they are distracting and thus have a hard time understanding the experiments.

Be more specific on:

- "...we monitor all incoming..." on page 28 and page 31, how is this monitored?
- "...only fractions of a second..." on page 30, how long time is that?
- "...system with fast Internet access." on page 29 and page 32, how fast is that?

3.6 Chapter 6

This chapter gives a good presentation of the results, but the quality of the figures could be improved, it is very hard to see what they represent. They could also need more detailed explanations.

This chapter is too unspecific at several places, for example "...below the baseline..." and "...at least some seconds...".

A good idea could be to define what a *peak* and a *valley* is.

3.7 Chapter 7

This chapter summarizes the project and the results from the experiments well. It concludes the thesis in a good way, but the future work could have been more extensive.

3.8 General Comments on the Dissertation

Overall it is a good dissertation. The red thread is easy to follow and is a SIP DoS detection ontology. But it could be more detailed on several places. Suggestions on spelling and grammatical corrections are in chapter 4 of this document.

4 Spelling and Grammatical errors

4.1 Chapter 1

- *"However, since there are many papers about possible countermeasures..." page 2,* maybe split this sentence into two sentences, because it is too long.
- "it's" on page 1, line 4, should be "its".
- "chose" on page 2, line 4, should be "choose".

4.2 Chapter 2

- *"...different types is difficult since many research papers are about the detection mechanisms ..." page 10,* "are about" should be changed to "deal with".
- "it's" on the bottom of page 5, should be "its".
- "login" on page 6, should be "log in".
- "down time" on page 10, should be "downtime".

4.3 Chapter 3

- In *"This can be seen in [12] where a Non-Blocking Cache is introduced to avoid this new problem.* " on page 14, maybe remove "new".
- "it'll" on page 16, should be "it will".
- "droping" on page 16, should be "dropping".

4.4 Chapter 4

- "As always" should be removed from page 19.
- On page 24, *"Requests generated by our User Agent would be defined as A. Responses to these requests would be A. Requests received by User Agent would be A' and responses to these requests would be A' . Standard traffic flow would be represented by α.*

", replace all "would be" with "is" or "are".

- *"A lot more difficult, but not entirely impossible, would it be for an attacker to make..."* on page 20, could be replaced by "It would be more difficult for an attacker to make...".
- *"We have not mentioned those AAA servers before"* on page 22, "those" should be removed.
- *"networking flow" on several places, should be "network flow".*

4.5 Chapter 5

- The sentence *"We set up our legal traffic for 10 seconds before we started the attack sending one, three or 5 attack messages per second." on page 32*, should maybe be rephrased as something like "Legal traffic was sent for 10 seconds before the attack was started, sending one, three or 5 attack messages per second."
- The second sentence of the summary starts with "Of course", this should be removed.
- *"...an open source tool that allows to generate SIP traffic." on page 29 and page 31,* should be "...an open source tool that can generate SIP traffic."
- *"(see also figure 5.3)" on page 31,* should be "(also shown in figure 5.3)"
- *"sesions" on page 29,* should be "sessions"
- *"machinen" on page 29,* should be "machines"
- *"operationg" on page 29 and page 32,* should be "operating"
- *"atack" on page 32,* should be "attack"

4.6 Chapter 6

- *"However, this characteristics..." on page 35,* "this" should be "these".
- *"...illustrates amounts of requests and..." on page 36,* "amounts" should be "the amount"
- *"...and forwarded by a proxy server." on page 37,* "a proxy" should be "the proxy"
- *"...were received while it has been under attack." on page 38,* "has been" should be "was"
- *"...increased average value for the DNS response time." on page 42,* remove "value for the"
- *"So, to distinguish between those attacks..." on page 42,* remove "So"

– *“Of course, that’s only the case for...” on page 43*, “that's” should be “that is”

4.7 Chapter 7

– *“...representation and sharing to be used by distinct systems...*“ on page 45, should be “*...representation and sharing. This could be used by distinct systems...*”

– “...performance loss, implementing of all measures...” on page 45 should be something like “...performance loss. The systems performance might be drastically reduced by implementing all these countermeasures at once.”