RUHR-UNIVERSITÄT BOCHUM

RUB

RUHR-UNIVERSITÄT BOCHUM

Insert title here

Insert your name here

Master's Thesis – June 12, 2018.
Chair for Network and Data Security.

Supervisor: Prof. Dr. Jörg Schwenk
Advisor: Dipl.-Ing. Max Mustermann

hgi Lehrstuhl für Netz- und Datensicherheit

Abstract

Insert abstract here.

Official Declaration

Hereby I declare, that I have not submitted this thesis in this or similar form to any other examination at the Ruhr-Universität Bochum or any other Institution of High School.

I officially ensure, that this paper has been written solely on my own. I herewith officially ensure, that I have not used any other sources but those stated by me. Any and every parts of the text which constitute quotes in original wording or in its essence have been explicitly referred by me by using official marking and proper quotation. This is also valid for used drafts, pictures and similar formats.

I also officially ensure, that the printed version as submitted by me fully confirms with my digital version. I agree that the digital version will be used to subject the paper to plagiarism examination.

Not this English translation, but only the official version in German is legally binding.

Eidesstattliche Erklärung

Ich erkläre, dass ich keine Arbeit in gleicher oder ähnlicher Fassung bereits für eine andere Prüfung an der Ruhr-Universität Bochum oder einer anderen Hochschule eingereicht habe.

Ich versichere, dass ich diese Arbeit selbstständig verfasst und keine anderen als die angegebenen Quellen benutzt habe. Die Stellen, die anderen Quellen dem Wortlaut oder dem Sinn nach entnommen sind, habe ich unter Angabe der Quellen kenntlich gemacht. Dies gilt sinngemäß auch für verwendete Zeichnungen, Skizzen, bildliche Darstellungen und dergleichen.

Ich versichere auch, dass die von mir eingereichte schriftliche Version mit der digitalen Version übereinstimmt. Ich erkläre mich damit einverstanden, dass die digitale Version dieser Arbeit zwecks Plagiatsprüfung verwendet wird.

Date	author

Erklärung

Ich erkläre mich damit einverstanden, dass meine Bachelorarbeit am Lehrstuhl NDS dauerhaft in elektronischer und gedruckter Form aufbewahrt wird und dass die Ergebnisse aus dieser Arbeit unter Einhaltung guter wissenschaftlicher Praxis in der Forschung weiter verwendet werden dürfen.

Date	author

Contents

1 Introduction

Always start a chapter with a short but informative text about the following sections. Point out the relevance of the sections and create interconnections between them. Never ever just write a single sentence here. Furthermore, you are strongly advised to respect the hints given in this template.

1.1 Motivation

What is your motivation to deal with this subject? Which interesting problems do you expect? Do not abbreviate "e. g." within a sentence, always write "for example". However, within in parentheses you are allowed to abbreviate and use, e. g., and, i. e., as shown here: with a comma right before and after it. In addition to that, ensure correct spacing by using `\,` in between.

1.2 Related Work

List related work *and* the result of this work! What is the relevance of this work concerning your thesis? If necessary, *emphasize* some words in your text, for example words like *not* or *and* are sometimes crucial for understanding.

1.3 Contribution

What is your contribution?

1.4 Organization of this Thesis

Please give a general overview on how your thesis is divided into sections and chapters ...

2 Background

Lorem ipsum dolor sit amet consectetuer parturient ac pulvinar magna porttitor. Accumsan vel ac eros laoreet Nulla leo Nulla vel Pellentesque Quisque. Adipiscing penatibus Phasellus egestas leo id neque nec quis est orci. Porta tellus ligula ut ridiculus eros eget ut Vivamus dictum nulla. Dui wisi enim vitae nulla Fusce Curabitur congue consectetuer urna Quisque. Felis Vestibulum Quisque sed Vestibulum et malesuada ac id tristique vitae. Aliquam Suspendisse mattis et libero et tincidunt quis tellus eget consectetuer. Libero Morbi cursus augue eget dapibus tincidunt nunc parturient id arcu. ...

2.1 Some text

Quis convallis fermentum accumsan Ut Nulla libero Morbi quis Nam at. Mi suscipit cursus mus eu Curabitur elit commodo at volutpat turpis. Tristique Sed orci id Aenean tempus quis Nunc ligula lacinia sagittis. In vitae ipsum quis tincidunt id Vivamus tincidunt volutpat ut venenatis. Nullam Nunc accumsan pellentesque et augue sem Integer auctor Nam ac. Hendrerit laoreet tellus urna faucibus pellentesque Nulla turpis wisi pede porta. Felis malesuada Vestibulum amet Curabitur lacinia wisi cursus habitasse Nam massa. Porttitor consequat Sed tempus interdum Donec Vestibulum a Curabitur ante eget. ...

2.2 Even more text

Quis convallis fermentum accumsan Ut Nulla libero Morbi quis Nam at. Mi suscipit cursus mus eu Curabitur elit commodo at volutpat turpis. Tristique Sed orci id Aenean tempus quis Nunc ligula lacinia sagittis. In vitae ipsum quis tincidunt id Vivamus tincidunt volutpat ut venenatis. Nullam Nunc accumsan pellentesque et augue sem Integer auctor Nam ac. Hendrerit laoreet tellus urna faucibus pellentesque Nulla turpis wisi pede porta. Felis malesuada Vestibulum amet Curabitur lacinia wisi cursus habitasse Nam massa. Porttitor consequat Sed tempus interdum Donec Vestibulum a Curabitur ante eget. Et nec et Nullam nunc non ligula dignissim sit velit Curabitur. Rhoncus wisi et pretium vestibulum metus fringilla pede nibh volutpat vel. ...

3 Implementation

3.1 Duties and Agreements

To successfully write your thesis, you should definitely respect some rules. They are explained in the following sections.

3.1.1 Rules for Students

At the beginning of your thesis, estimate the complexity of the work you are going to have. Take into account that you will have problems with certain aspects of your thesis that will consume a lot of time. Consider times for recreation and delays you can not influence, for instance, asking your supervisor, waiting for orders to be shipped, complex problems during the implementatuon phase, and so on ...

For some students it is a good idea to agree upon a rough plan (with their supervisor) on how to make progress on their thesis and what goals to achieve. Milestones might help to control your progress. If you fail to meet a milestone in time, contact your supervisor on why this happened or when to expect it to be fulfilled.

If you have a problem, try to solve it on your own twice over. Some things just take time. In case you fail to solve it on your own, write an email to your supervisor and tell him about your problem and what you did to solve it. Make an appointment if necessary. Please do not jump right into his office, supervisors have other stuff to do, too.

For quotations, either use “quotation” or “quotation”. For some words, you should use a tilde to link them, for example, when referring to chapter 5 you should use it. Or use chapter 5. This prevents words from being separated by a line break or some other rare circumstances. Use BibTeX within your thesis and learn the different citation options [3, 1].

One last piece of advice. Do not try to attend courses in parallel to your thesis. You should take this seriously and not think that writing a thesis is done quickly.

3.1.2 Rules for Supervisors

"With great power comes great responsibility" :-)

- It is very important, that if you want specific things to be done that you send these important instructions by mail. Your student might be in a moment of confusion when telling him.
- Attend the "Diplomandenseminar" and give your student the feeling, that this is important to you, too.
- Offer your students the opportunity to talk to you right after the "Diplomandenseminar". While discussing things, tell your student to write down the results of this discussion and tell him to send you this summary by mail to ensure (if necessary), you did not talk at cross purposes.
- Last but not least: Please be gentle to your students :-)

3.2 Hints on Typesetting

To get this template running, you need at least

- either TeXLive 2010 (use update utility and install the most recent packages!)
- or MikTeX (IMPORTANT: install the cm-super font package manually!)

This template is confirmed to work in both situations. In case it does not work for you, there is something wrong with your LaTeX environment :-)

You can use `pdflatex` or `latex` to typeset this template.

3.2.1 Structuring Text, English Hints

Another text about the following sections ...

3.2.1.1 Text

Always try to structure your text in a manner that makes sense. Either use indentations, itemize or enumeration environments.

This sentence will have an indentation at the beginning. Now an enumeration starts:

1. One.
2. Two.
3. Three.

Sometimes you do not want an indentation. Use the `noindent` command in such a case.

One Is the first number.

Two Is the second number.

Glossary Use the glossary package for acronyms. In addition, the glossay package can help you to avoid typing the same word in different ways. For example students tend to mix-up the writing of the word *User-Agent* in different ways: user-agent, User-Agent, user agent, User agent. This inconsistency can be avoided by just using the glossary entry: User-Agent (UA).

3.2.1.2 English Hints

- Use an active voice and avoid using passive wherever possible.
- *Always* use the present tense (especially when you refer to content that occurs later in your text). For example:
  - *wrong*: The next chapter *will* explain ...
  - *correct*: The next chapter explains ...
- Either use American English or British English, but do not mix (e. g. summarize vs. summarise, analyze vs. analyse, ...). American English is preferred.
- Do not use filler words.
  - omit: “some kind of” and others ...
- Never use a comma before “that”.

- For enumerations, always use a comma before "and": "... module 1, module 2, and module 3.".
- The title of your thesis is capitalized except for words like and, or, with, the, a ...
- *Always* address the reader using the third person: "As one can see from ..." and not "As you can see ...".
- All tables, figures have to be explained very briefly in the text itself.
- Always use correct quantifications:
  - *wrong*: ... a small amount of runs ...
  - *correct*: ... at most three runs ...
- Never use "I". Depersonalize your sentences or use "we" if necessary.
- Read *The Elements of Style* by William Strunk, Jr., which is for example available at `http://www.crockford.com/wrrrld/style.html`. The (short) book provides an overview of typical errors and helps you to significantly improve your English.

3.2.1.3 General Hints

- Use non-breaking small space for some abbreviation
  - z. B.
  - u. a.
  - e. g.
- Use a non-breaking space just before references, parentheses and so which shall not begin at the beginning of a new line. This sentence will not break here (and here).
- Did you notice the overfull horizontal box (hbox)? You should avoid these! Underfull boxes are not that bad. But only fix them when most of the section, paragraph etc is ready. Otherwise you have to fix them more than once. You can tell LaTeX when to break a word if it does not do it correctly. Just put a \- at the corresponding position in the world. Vertical overfull boxes (vbox) occur if the document uses `\flushbottom` instead of `\raggedbottom`. That way, LaTeX ensures that each page ends with the last sentence in the last line (except for the final line in a section). To enforce this, LaTeX sometimes has to add extra vertical space between, e. g., paragraphs. Overfull vertical boxes are hard to fix, as additional content needs to be added or even has to be removed sometimes. Keep in mind that any changes to the type area (Satzspiegel)

might produce many additional over- or underfull boxes (and of course it will fix other boxes).

- Read `ftp://ftp.dante.de/tex-archive/info/german/l2tabu/l2tabu.pdf`. Really, read it.
- You can find many more good information at `http://www.dante.de/CTAN/info/lshort/german/l2kurz.pdf`
- The KomaScript guide is very useful: `ftp://ftp.dante.de/pub/tex/macros/latex/contrib/koma-script/scrguide.pdf`

3.2.2 Formulas, Figures, Tables, Definitions

3.2.2.1 Formulas

Define abbrevations with the `\acro{...}` command, use them in the text mostly with `\ac{...}`. (Yes, in this example there are still a lot of wrong abbrevations. Make it better :)

So, testing abbrevations the Advanced Encryption Standard (AES) is written in different form. Lets see, when using the AES again, what will happen :D .

Using the method shown in Table XX for all three functions yields.

$$f_a^4 = \texttt{0x2C79} = \mathrm{abc} + \mathrm{ac} + \mathrm{ad} + \mathrm{bc} + \mathrm{a} + \mathrm{b} + \mathrm{d} + 1 \tag{3.1}$$

$$f_b^4 = \texttt{0x6671} = \mathrm{abd} + \mathrm{acd} + \mathrm{bcd} + \mathrm{ab} + \mathrm{ac} + \mathrm{bc} + \mathrm{a} + \mathrm{b} + \mathrm{d} + 1 \tag{3.2}$$

$$f_c^5 = \texttt{0x7907287B} = \mathrm{cde} + \mathrm{abde} + \mathrm{ade} + \mathrm{de} + \mathrm{abce} + \mathrm{bce} + \mathrm{ce} + \mathrm{be} + \mathrm{bcd} + \mathrm{acd} + \mathrm{bd} + \mathrm{d} + \mathrm{bc} + \mathrm{ab} + \mathrm{b} + 1 \tag{3.3}$$

When typesetting formulas, pay special notice on constants, variables, and units:

$$\mathcal{F}_\omega\{x(t)\} = \int_{-\infty}^{\infty} x(t)\, \mathrm{e}^{-\mathrm{j}\omega t}\, \mathrm{d}t \qquad \text{(Fourier-Transformation)}$$

The use of constants, variables and units is explained by “Rohde & Schwarz” in their famous document “Der korrekte Umgang mit Größen, Einheiten und Gleichungen” [2]. These rules are in compliance with ISO-31. Consequently, always typeset the following in italics:

- Variables like k, x, ...
- Functions like $f(x)$,...
- Physical constants like c_0, ...

- Indices that are variables or physical units, like $a_{i,j}$ or c_V.

Always typeset the following upright:

- Functions with fixed name like $\sin(x)$ or $\Gamma(x)$.
- Mathematical constants like π, i or e.
- Units and their prefixes, like $\lambda = 0.56\,\mu\mathrm{m}$, alternatively $\lambda = 0.56\,\mu\mathrm{m}$.
- Indices that represent names or identifiers, like $x_{\max}$ or μ_{B}.

In case it is necessary to make heavy use of user defined functions, one should use `\DeclareMathOperator` to define the corresponding function. Finally, a good example how it should *not* look like.

$$Throughput = 30mbit/s$$

In case you need some extra symbols: `http://mirror.ctan.org/info/symbols/comprehensive/symbols-a4.pdf`

3.2.2.2 Figures

Figures and tables are important to explain things. Here are some rules that apply, when using figures:

- Whenever possible use vector graphics (eps, pdf, svg, ...) instead of bitmap graphics (jpg, gif, ...).
- All figures should have the same font and size (do not scale them or the size will change) and "style" (line strength, arrow heads, ...).
- Some employees of the chair need all figures in `.eps`. However, do *not* convert your `.jpg` and `.png` to `.eps`, instead use a *wrapper* program to wrap these file types into the `.eps` format. As a consequence, you are forced to use `latex` to typeset your document instead of `pdflatex`. Appropriate wrapper programs can be found here:
  - Windows: click
  - Linux/Mac: click
- **Always** try to use your own figures, so you do not run into copyright problems and it is easier for us, to reuse these figures for papers. You might want to have a look at these tools to create your own figures:
  - Windows: MS Visio (available via MSDNAA), Graphviz, Gnuplot ...
  - Linux: xfig/jfig, IPE, Graphviz, Gnuplot ...

– Mac: IPE, Graphviz, Gnuplot, OmniGraffle (commercial, academic licensing available) ...

There are many possibilities on how to include figures, here is just one example on how to do it. In case you need further assistance, please google for `l2picfaq`.

3.2.2.3 Tables

There are many possibilities on how to create and include tables. From a typographic point of view, *one should avoid any vertical lines*, cf. Table 3.1.

Table 3.1: Captions for tables are *always above* the table and give a short but informative description of the table. Always use full sentences here and end them with a full stop.

		Component	
Amount[a]	Price	Description	Role
23	1.234 $	good stuff	important
multirow example the other row	x	y	XXX
42	43.123,13[b]	good stuff	important

[a]This is a footnote inside a table, you need a minipage for this to work.
[b]This is another footnote inside a table.

3.2.2.4 Definitions

This is a definition. You can of course make a reference to it 3.2.

Definition 3.2 (A name) *A really good definition. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.*

3.2.3 Listings, Algorithms

3.2.3.1 Listings

For source code listings, three options are available:

- the `verbatim` environment,
- the `listings` package,
- and the `lgrind` package.

The verbatim environment is the most simple environment and not suited for large code listings (due to different limitations). Only use it for single

```
$ important shell commands
```

Otherwise, either use the `listings` or `lgrind` packages. The listings package is easier to use, therefore we present it here. *Important* advice: Only explain important functions and/or structures of your program in your thesis..Especially point out the big picture of your program, for instance, how different modules interact and which important input limitations to respect. Please note: Using special language characters (ê, ü, ä, ...) in your source code is strongly discouraged, as they may cause problems using the `listings` package.

```
1  /*!
2   * This is a Doxygen comment for a function.
3   * \param first operand
4   * \param second operand
5   * \returns a+b
6   */
7  int  sum(int a, int b)
8  {
9    return (a + b);
10 }
```

Listing 3.3: A sample listing of a C function. Description of the function is here. Please note that different languages are available.

```
1  entity InterLeavedMul is
2    generic(wide : natural :=8); -- highest bit
3    port(clk : in std_logic;
4         rst  : in std_logic;
5         x    : in std_logic_vector(wide-1 downto 0);
6         y    : in std_logic_vector(wide-1 downto 0);
7         N    : in std_logic_vector(wide-1 downto 0);
8         start: in std_logic;
9         done : out std_logic;
10        xyN  : out std_logic_vector(wide-1 downto 0));
11 end  InterLeavedMul;
```

Listing 3.4: A sample listing of a VHDL entity. Description of the entity is here. Please note that different languages are available.

You should thoroughly document your code using comments and (best case) by using a documentation system like Doxygen. Please ask your supervisor for additional rules (e. g. which repository system to use, etc.). Regularly commit your changes and backup your data!

3.2.3.2 Algorithms

For many theses, typesetting algorithms is necessary. There are at least four packages available that allow easy typesetting of algorithms.

- `program` offering the environment `program`.
- `algorithm` offering the environment `algorithm`.
- `algorithmic` offering the environment `algorithmic`.
  - This package sometimes has compatibility problems with `hyperref`.
- `algorithm2e` either offering the environment `algorithm` or `algorithm2e`.

Students are advised to use only *one* of these packages and not mix them. The author of this template suggests to use the package `algorithm2e` with the option `algo2e`. This prevents conflicts with other packages, just in case it is ever required to mix `algorithm` or `algorithmic` with `algorithm2e`.

Algorithm 3.5: INSERTION-SORT

Data: unsorted array $A[1 \dots n]$
Result: array $A[1 \dots n]$ with $A[1] \leq A[2] \leq \dots \leq A[n]$

```
1 begin
2     for j ← 2 to length[A] do
3         key ← A[j];
          /* Insert A[j] into the sorted sequence A[1...j-1]   */
4         i ← j − 1;
5         while i > 0 and A[i] > key do
6             ;
7             A[i + 1] ← A[i];
8             i ← i − 1
9         A[i + 1] ← key
```

3.2.4 Protocols

3.2.4.1 2-Party Protocol Sessions

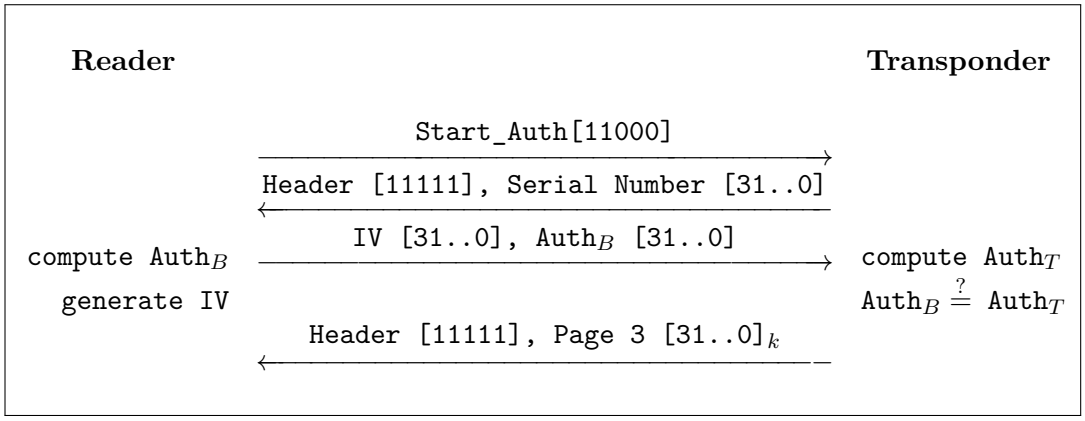

Figure 3.6: Mutual authentication of the HITAG 2 protocol in crypto mode.

3.2.4.2 Protocol Headers

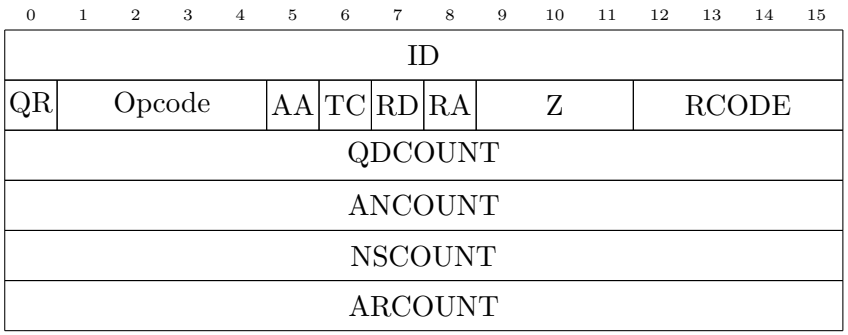

Figure 3.7: DNS Request

4 Results

Lorem ipsum dolor sit amet consectetuer parturient ac pulvinar magna porttitor. Accumsan vel ac eros laoreet Nulla leo Nulla vel Pellentesque Quisque. Adipiscing penatibus Phasellus egestas leo id neque nec quis est orci. Porta tellus ligula ut ridiculus eros eget ut Vivamus dictum nulla. Dui wisi enim vitae nulla Fusce Curabitur congue consectetuer urna Quisque. Felis Vestibulum Quisque sed Vestibulum et malesuada ac id tristique vitae. Aliquam Suspendisse mattis et libero et tincidunt quis tellus eget consectetuer. Libero Morbi cursus augue eget dapibus tincidunt nunc parturient id arcu. Donec sapien enim Aenean convallis Donec elit tincidunt dolor vitae tellus. Ac consectetuer at tortor malesuada ac dui ligula habitant habitasse congue.

5 Conclusion

Lorem ipsum dolor sit amet consectetuer parturient ac pulvinar magna porttitor. Accumsan vel ac eros laoreet Nulla leo Nulla vel Pellentesque Quisque. Adipiscing penatibus Phasellus egestas leo id neque nec quis est orci. Porta tellus ligula ut ridiculus eros eget ut Vivamus dictum nulla. Dui wisi enim vitae nulla Fusce Curabitur congue consectetuer urna Quisque. Felis Vestibulum Quisque sed Vestibulum et malesuada ac id tristique vitae. Aliquam Suspendisse mattis et libero et tincidunt quis tellus eget consectetuer. Libero Morbi cursus augue eget dapibus tincidunt nunc parturient id arcu. Donec sapien enim Aenean convallis Donec elit tincidunt dolor vitae tellus. Ac consectetuer at tortor malesuada ac dui ligula habitant habitasse congue.

List of Figures

List of Tables

List of Algorithms

List of Listings

Bibliography

[1] J. Newsome and D. Song. Dynamic Taint Analysis for Automatic Detection, Analysis, and SignatureGeneration of Exploits on Commodity Software. In *Symposium on Network and Distributed System Security (NDSS)*, 2005.

[2] Rohde & Schwarz. Der korrekte Umgang mit Größen, Einheiten und Gleichungen. `http://www.rohde-schwarz.de/ps/rus/tools/show_8437_document/Der_korrekte_Umgang.pdf`, as of June 12, 2018.

[3] Y. Xie, F. Yu, K. Achan, R. Panigrahy, G. Hulten, and I. Osipkov. Spamming Botnets: Signatures and Characteristics. *ACM SIGCOMM Computer Communication Review*, 38(4), 2008.

A Java Code