Designing and building a 5G security learning platform

www.simply5gsecurity.com

Pien van den Abeele
s1044362

March 20, 2023

First supervisor/assessor:
dr. K.S. (Katharina) Kohls

Daily supervisor:
D.J.H. (David) Rupprecht

Second assessor:
dr. ir. E. (Erik) Poll

Radboud University

Abstract

This thesis elaborates on the implementation risks of the 5th generation (5G) mobile network and how to create a better solution. The 5G network, with its cloud-based solution, supports a wide range of new applications, including the Internet of Things (IoT), remote surgery, and self-driving cars. However, this also requires increased complexity and creates a larger attack surface. The cloud-based implementation increases the accessibility of deploying a 5G network. The high accessibility of deploying a 5G network and the complexity of its specifications may lead to mistakes in network implementations, making the network more vulnerable to security threats.

The 5G specifications are written by the 3rd Generation Partnership Project (3GPP), which has over a thousand specification papers describing 5G. However, the overwhelming amount of specifications and the language and formulation used in these papers make it difficult to know where to start when deploying a 5G network. Websites explaining 5G in a simpler way exist, but they lack the depth needed to offer support when implementing a 5G network and do not focus on the security aspect of a 5G implementation.

To fill the gap between the 3GPP specifications and the simpler websites, this paper proposes creating a website called "Simply 5G Security," which supports programmers who need to implement their own 5G network. The website provides a starting point for programmers and information on the security aspects of 5G, bridging the knowledge gap and helping to design a safe 5G network. With this thesis, we elaborate on the process of creating Simply 5G Security.

Contents

Chapter 1

Introduction

Everyone uses mobile networks, whether it is to call a loved one or to do online banking. Besides human usage of the mobile network with a smartphone, most devices exchanging data (e.g. a smart thermometer or sensors in a nuclear power plant) also use the mobile network. The collective of all devices which communicate through the mobile network is also known as the Internet of Things (IoT). As the need for mobile networks keeps growing, the mobile network needs to keep evolving [1, 2]. The number of devices in the IoT is ever-expanding, which means that the network needs to keep evolving. The result of this need for improvement is the 5th generation (5G) of mobile networks which has become the new standard.

5G introduces a faster and more reliable network compared to previous generations. With these improved features, there is better support for a wide range of (new) applications, some of which include the IoT, remote surgery, and self-driving cars. Whereas previous network generations' core networks were hardware-based, the 5G cloud-based solutions revolutionised the core network, enabling these (new) applications. These changes lead to lower latency of the network traffic and a higher capacity for devices [3, 4].

The introduction of (new) improved features in 5G, requires more complexity to the system architecture. More complexity leads to more possible security risks [5] since more complexity increases the attack surface. The complexity of 5G is easily observed when looking at, for example, the 572 pages long general 5G architecture specification [6]. Ahmad et al. (2019) show an excessive list of security threats found in 5G security [7]. One of the risks comes from the move from hardware to cloud-based infrastructure. With a cloud-based infrastructure, in theory, all who are interested or need to can deploy their own 5G network.

This introduces a problem that can be explained as follows; The high complexity of the system architecture is directly related to a complex specification. This complexity combined with the high accessibility of deploying

a 5G network inherently leads to an increased possibility of mistakes in network implementations. Not all who implement a 5G network will have the necessary expertise to properly follow the specifications. One such result of this effect can be seen in research by C. Leuverink which shows how many 5G networks still use the default login credentials [8].

1.1 Related work

1.1.1 3GPP specifications

The 5G specifications are written by the 3rd Generation Partnership Project (3GPP). 3GPP is a global partnership project which combines national Standards Development Organizations (SDOs) to create specifications for the mobile networks [9]. They have specifications on the general 5G architecture, which describe how the 5G network behaves and how the components should interact [6]. The 3GPP has also released a paper for each component describing in detail how the component should behave and be implemented [10, 11]. Besides the papers describing the functions, the 3GPP has papers on the security aspects of 5G [12]. There are over a thousand specification papers describing 5G made by the 3GPP [13]. This is overwhelming and makes it difficult to know where to start when deploying a 5G network. Besides the vast amount of specification papers, the language and formulation used in these papers are difficult to follow for those who do not yet have any prior knowledge or experience.

1.1.2 Websites about 5G

Besides the 3GPP specifications, there are websites explaining 5G in a simpler way [14, 15]. The focus of these websites is explaining how the 5G network works. When learning about 5G and what it brings, they can be useful. However, if one needs to implement their own 5G network, these websites do not contain enough details. There are no specifications explaining exactly how each component relates to another. Besides the lack of details, there is no mention of how to make a secure 5G network. These websites do not focus on the security aspect of a 5G implementation.

1.2 Simply 5G Security

There is a lot of information about 5G out there. The 3GPP introduces the specifications but in such complexity and quantity, it is difficult to navigate [13]. Then there are websites explaining 5G but lack the depth to offer support when implementing a 5G network [14, 15]. There are programmers who need to implement a 5G network or people who configure 5G networks or pen-testers who analyse 5G networks. We assume they often do not have

4

sufficient knowledge yet to understand the 3GPP specifications. This creates a gap in the information that is out there. There is no middle ground for the programmers who need the details on specifications but lack the knowledge to understand the 3GPP specifications alone. As mentioned before, the lack of knowledge in the programmers leads to 5G networks being not secure [8]. Therefore a way is needed of giving these programmers more knowledge and help them design a safe 5G network. With this thesis we propose the following solution to fill in this gap:

We create a website called "Simply 5G Security"[1], which supports programmers who need to implement their own 5G network. With Simply 5G Security, there is a starting point for those programmers. On top of that, it also contains information on the security aspects of 5G. Then besides the general information about 5G, Simply 5G Security offers more detailed information. It contains details on the different components of the 5G network and how they communicate. Combining the simplicity used in websites about 5G and the detailed specifications of the 3GPP, we create an accessible website for the programmers who need it.

With our thesis we contribute as follows:

- We show how to make the complexity of 5G easier to understand. Presenting the information in split-up parts makes it more comprehensible to the reader.

- In order to understand the security aspects of 5G, the reader needs a basic understanding of 5G itself. However, for the reader to understand 5G security, it is not necessary to know all the details of 5G. Therefore we explain the basics of 5G a reader needs to understand the security aspects.

1.3 Outline

In this thesis, we walk through the process of creating Simply 5G Security. Firstly, we discuss the technical background in Chapter 2, explaining which framework and languages we use to create the website. In this chapter, we also talk about why we chose certain frameworks over others. Secondly, we discuss the methodology in Chapter 3, where we determine what we should and should not display on the website. We explain design and content choices and substantiate these. Thirdly, in Chapter 4 we have the discussion where we elaborate more on the content of our website. Alongside this, we discuss the limitations of our work and what future work can be done. Lastly, Chapter 5 summarises all work and concludes the thesis.

---

[1]www.simply5gsecurity.com

Chapter 2

Technical background

In this chapter, we elaborate on the technical details of our website. To develop the website we use certain programming languages which we elaborate on. We explain the framework we use for our website. Lastly, the deployment steps we take to deploy the website will be explained.

2.1 Languages

The languages we use to create Simply 5G Security, are HTML, CSS, Markdown, and JavaScript.

- HTML: HyperText Markup Language is the standard markup language for files displayed on the web browser. The focus of HTML is on the functionality of the website [16].

- CSS: Cascading Style Sheets is a style sheet language used for designing files made in HTML. The focus of CSS is on the design of the web page [17].

- Markdown: MarkDown is a lightweight markup language which can be used together with HTML or standalone. The focus of MarkDown is on the functionality of the website [18].

- JavaScript: JavaScript is a programming language used in web-based files. JavaScript gives functionality to a web page, making it dynamic [19].

2.2 Framework

For the website's framework, we use Jekyll in combination with Bootstrap-sass and Bootwatch. Jekyll is a static website generator. It lets the programmer of the website use their favourite markup language, and turns it

into a static website [20]. We use MarkDown and HTML for Simply 5G Security. Bootstrap-sass is a CSS framework to create front-end websites which also work on mobile devices [21]. Bootwatch is a free open-source project with layout themes for Bootstrap websites [22].

In Jekyll, there are *layout* and *include* files.

- *Layout:* Layout files are HTML files using CSS layout. In each new HTML file there will be a layout defined on top of the page, like so:

  ```
  ---
  layout: default
  ---
  ```

  When the site is compiled, this layout is loaded into the HTML file. An example of a layout file can be found in A.1.

- *Include:* An include file is made in HTML. In an HTML file, it is possible to refer to an include file. This include file then includes the HTML code inside the file. The reference to an include file can be done in a div like so:

  ```
  <div class="col-md-3">
      {% include docs_nav.html %}
  </div>
  ```

  When the site is compiled, the HTML code from the include file will be included in the HTML file it is in. An example of an include file can be found in A.2.

Jekyll provides templates that can be freely used [23]. These themes offer a layout that can be changed to preferences. The Jekyll template we use is Jekyll Docs Template [24], which uses Bootstrap-sass and Bootwatch themes. The pages inside the website can be made in HTML or in Mark-Down, or a combination of both.

2.3 Deployment

Simply 5G Security is deployed through GitHub pages. We use GitHub pages, a website hosting platform that uses the files straight from the GitHub repository to turn them into a website [25]. Jekyll allows easy deployment with GitHub pages. If the Jekyll-based website repository is in a GitHub repository, all that needs to be done is enable GitHub pages in the repository settings and the website is live.

We have our own bought domain, www.simply5gsecurity.com. We need to change the DNS settings to make our GitHub page go to the said domain. We have configured the DNS server to redirect our own domain[1] to our GitHub page[2].

---

[1]www.simply5gsecurity.com

[2]https://pienvandenabeele.github.io/Simply5GSecurity/

Chapter 3

Methodology for creating Simply 5G Security

In this chapter, we explain the choices we make to create Simply 5G Security. Firstly, we establish the target audience for our website. Secondly, we elaborate on the creation of the website flow. Thirdly, we explain how we generate the content. Lastly, we discuss the use of Jekyll as the framework for the website.

3.1 Who is the target audience?

The first step in the process of designing and creating a platform for 5G Security, is to decide who the website is for. We decide to create a website aimed at programmers with some network knowledge, but not yet anything specific about 5G. For example knowledge from courses like *Networks and Security* or related books [26, 27]. The reasoning for the decision is that most information on 5G networks (e.g. 3GPP [28]) is aimed at people which already have a deep understanding of how mobile networks work. We want to give programmers who are just starting, the opportunity to learn and be able to implement a secure network.

With the target audience already having some network knowledge, we do not explain every single aspect of mobile networking. For example, we assume the audience knows what networking protocols are and that they have some basic understanding of what a cryptographic algorithm is. Knowledge gained from bachelor courses like *Introduction to Crypography* or *Web Security*, is expected. The reason for this assumption is so we can focus on the main aspect of the learning platform: the security of 5G.

3.2 The website flow

With the audience established, we decide to build a website called Simply 5G Security. For a website the flow is just as important as the content of the website itself. If there is well-explained information on a website but no way to easily navigate to said information, the information is mostly lost [29]. Therefore, we first think about what the flow of the website should be before creating the content.

To create the flow from scratch, we take pen and paper and draw the landing page. From that point, we think about the different pages we need on the website. For Simply 5G Security there needs to be some explanation of the 5G Basics, thus a *5G Basics* page and also the main feature, which is the security of 5G, a *5G Security* page. See Figure 3.1 for the total website flow.
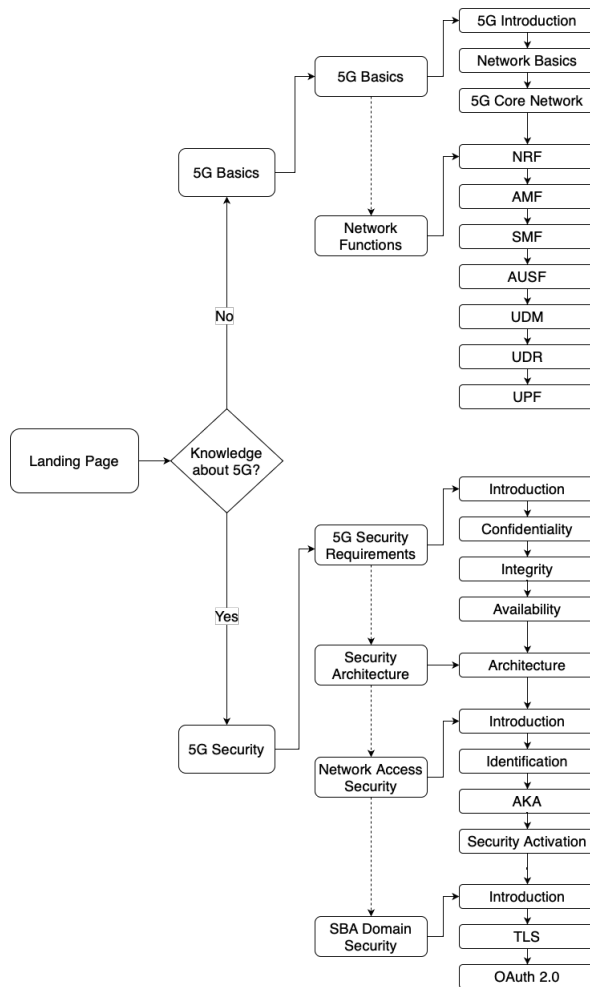

Figure 3.1: Website flow.

Both *5G Basics* and *5G Security* are tabs in the navigation bar on the top of the website, see Figure 3.2. 5G Basics and 5G Security both have a navigation bar on the left side, to show the user on which topic page they are currently.

Figure 3.2:   The navigation bar of Simply 5G Security.

3.2.1   5G basics

As established before, we have a target audience who do know some things about networking but do not necessarily have knowledge about 5G. Therefore we need a 5G Basics page, explaining the general concept of 5G. To have a more clear overview of the information, we have different pages under the 5G Basics tab.

- 5G Introduction
  The reason we start with an introduction is to inform the user about which aspects will be discussed and explained in this section. It also provides a nice starting point, to avoid the user becoming overwhelmed with new information.

- Network Basics
  Here we explain the concepts like User Equipment (UE) and Radio Access Networks (RAN). The reason we have a separate page for these concepts is that they are needed for the overall understanding of the network but they are not part of the 5G Core.

- 5G Core Network
  Before we can explain the Network Functions (NF) of the 5G network, the user needs an explanation of the layout of the 5G network. We explain what Service-Based Architecture (SBA) and Referenced-Based Architecture (RBA) are and the difference between the control and user plane. This gives the user a picture of how the 5G network looks.

- Network Functions
  We decide to only focus on the most essential NFs of the 5G Core. There are more NFs than the ones we explain. The reason for this decision is the focus of the learning platform, as our focus is on the security aspect of 5G. For the user to understand the security aspects, it is not needed to know every detail of the 5G network. Therefore, only the basic concepts are needed to further focus on the security aspects. We explain the following network functions:

- Network Repository Function (NRF)
- Access and Mobility Management Function (AMF)
- Session Management Function (SMF)
- Authentication Server Function (AUSF)
- Unified Data Management (UDM)
- User Data Repository (UDR)
- User Plane Function (UPF)

With the separation of these different concepts, we achieve a clear overview of what 5G is. With the knowledge obtained in 5G Basics, the user can continue to the 5G Security tab.

3.2.2 5G security

The flow for 5G security is comparable to that of the 5G basics.

- 5G Security Requirements
  To define the security of a system, the Confidentiality, Integrity and Availability (CIA) triad is often used [30], so we also include it in the security of 5G. The 3GPP defines security aspects in these terms as well. Therefore, we explain the CIA triad to the user and how they relate to 5G security, in the following order:

  - CIA Introduction
  - Confidentiality
  - Integrity
  - Availability

- Security Architecture
  The security architecture 5G can be shown in Service Based Architecture (SBA) or Reference Based Architecture (RBA). We use RBA as this shows all the dependencies and references NFs have with each other. We focus on two aspects of communication in 5G, Network Access Security, and SBA Domain Security, as those are the most used.

- Network Access Security
  This protocol is used in (almost) all communication in 5G and thus it is important the user knows what it means and how it works. We elaborate by explaining the following concepts:

  - Introduction
  - Identification
  - Authentication and Key Agreement

11

– Security Activation

- SBA Domain Security
  SBA Domain Security is used in the communication between the NFs.
  If the user wants to implement their own 5G Core, it is important
  they make the internal communication secure. To help the user achieve
  this, we explain the SBA Domain Security. The main concepts of SBA
  Domain Security are addressed in the following order:

  – Introduction
  – TLS
  – OAuth 2.0

To keep a clear overview of the different aspects of security, we split up
different levels. The user should go from top to bottom to get the clearest
understanding of the security, as this is the flow of the website. However,
the reader can follow the website flow or create their own flow. This way
the user keeps their freedom but is guided as well.

3.3 Generation of the content

Once we know what the flow of the website is, we start to create the content
of the website. Content can be split up into two sections, the text and the
images, which is what we do as well. We want the user to understand the
concepts we explain, and thus we use images and text combined. This is
proven to be more efficient, in the sense that learners will understand and
remember information better [31].

3.3.1 Text

To write the text of the website we first collect information about the topics
mentioned in section 3.2. We use the 3GPP specifications to create text
explaining the different concepts. We leave out details and instead refer to
the specific specifications if needed. The purpose of this is to not overwhelm
the user with information. If the user needs more details, they can easily
look it up with our provided references.

3.3.2 Images

We first design the images in draw.io, to know what they will look like. As
references, we use images from the 3GPP specifications but also images from
lecture slides provided by D. Rupprecht and K. Kohls. Once we have the
layout, we design the images with visually pleasing icons compared to static
black-and-white images. This improves the visuals of the website, making

it more attentive to users and improving their learning abilities [31]. We design the final images with Microsoft PowerPoint.

3.4   Jekyll

The first reason for using Jekyll as the framework is that with a Jekyll theme, we have a good starting point. Jekyll provides static website templates, you can use and modify to easily create a website or blog to your liking. The Jekyll Docs Template provides us with a working website template [24]. This template comes with an introduction page on Jekyll and the template itself. It already has a navigation bar and different tabs for different topics. We alter the template to our needs and use these components to display our content on 5G and its security. The second reason to choose Jekyll is that it saves us time on website design. This leaves more time to create and define the website's content.

We decide to pick Jekyll over other frameworks like Django or stand-alone Bootstrap, for its simplicity. Django is a python based web framework. The focus of Django is on templates filled with data from databases [32]. However, we do not need this for Simply 5G Security. Therefore we pick Jekyll over Django as we do not need to extra features Django offers.

Jekyll uses Bootstrap in its framework which gives us both advantages. The reason we pick Jekyll over stand-alone Bootstrap is the advantages Jekyll gives us. For example with the Jekyll Docs Template, we already have a working website we can then change to how we want it.

Chapter 4

Discussion

In the discussion, we elaborate on the concepts of Simply 5G Security and future work. Firstly, we explain the two major decisions we make in terms of content. Secondly, we discuss the limitations of Simply 5G Security. Thirdly, we reflect on the use of Jekyll as our framework. Lastly, we suggest possible future work to be done.

4.1   Content discussion

Two big decisions we make in terms of content are about the network functions (NF) and the security protocols. We explain why we focus on certain NFs instead of all of them. In 4.1.2 we elaborate on why we focus on Network Access Security & SBA domain security.

4.1.1   Network functions

The 5G Core has 14 different network functions, see Figure 4.1 (the UE, (R)AN and DN are not network functions).

All these network functions have their own functionality. When implementing a 5G network, they are all needed for the network to work. However, it is possible to explain how 5G works without having to mention every single NF.

By limiting the information provided to the user, the user can focus on the main concepts. Our goal is to teach the user about the security of 5G. A basic understanding of 5G is necessary but it is not necessary to know every single detail about 5G. Therefore, we limit the information about 5G, so we can focus on the security aspect of 5G.

As our target audience does not yet know anything about 5G, we decide to use a simplified explanation of 5G. As shown in our Figure 4.2, we use the NFs that are needed for a successful flow of traffic over the network. The NFs AMF, SMF, AUSF, UDM, UDR and UPF, are all used in a successful

traffic flow. In Figure 4.3 an example of the AMF representation on the website. On top of that, we include the NRF which is responsible for the security aspects.
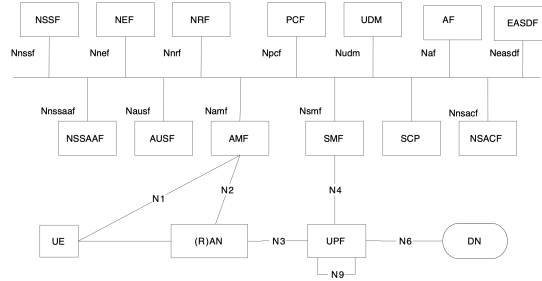

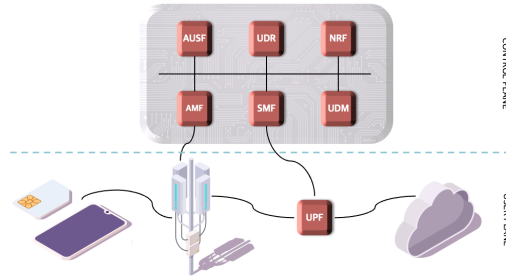Figure 4.1: 3GPP specification of the 5G Network Service Based Architecture.

Figure 4.2: Our specification of the 5G Network Service Based Architecture.
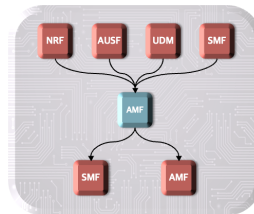

Figure 4.3: The representation of the AMF on Simply 5G Security.

4.1.2 Security protocols

The 5G Security architecture is built up of six communication protocols, which can be seen in Figure 4.4. Just as with the NFs, the security domains all have their own purpose and functionality. These domains define the security of communication. To build a secure network, all security domains are needed to ensure security.

However, as our target audience is programmers who need to implement their own 5G core network, we decide to not include everything seen in Figure 4.4. Instead, we focus on two of the six protocols. We decide to do this to not overwhelm the user and because of time limitations.

Firstly, Network Access Security (I) is used in (almost) all communication. Therefore we decide to explain this protocol on our platform. When implementing a 5G core, it is important that communication is secure and Network Access Security ensure this.

We also elaborate on SBA Domain Security (V) because this is the communication between NFs. The user is making a 5G core, which consists of the NFs. Therefore a secure communication protocol is necessary for a secure network core.
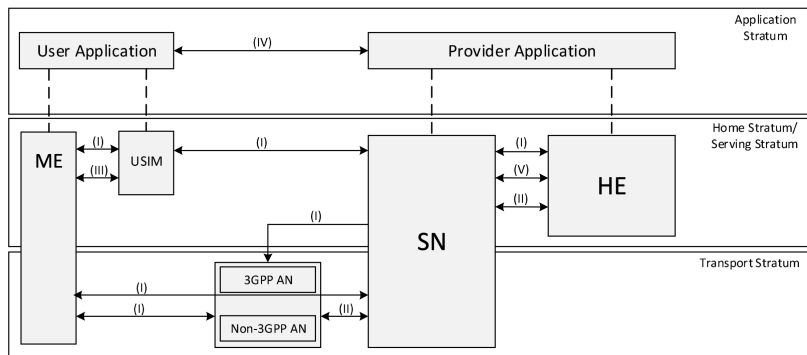

Figure 4.4: 3GPP specification of the security architecture of 5G.

4.2 Jekyll

While using Jekyll saves us time, it also consumes time. We have to learn a new tool and read the documentation. With Jekyll Docs Template, this can all be found in one place, which helps us. However, picking the right template also takes time. There are paid and free Jekyll themes one can use [33]. Deciding which theme fits the needs of the programmer is a time-consuming process, in our experience.

Jekyll can also be limiting when the programmer has very specific needs for their website. Most Jekyll themes are blog or business-based websites. If that is not the goal of the website, Jekyll might not be the best framework choice.

4.3 Limitations and future research

While Simply 5G Security covers the basics and contains information on 5G, there is much more to 5G than what is on our website. On multiple occasions, we decide to exclude information, see Appendix B.1 and B.2 for the lists. Two motivations are time and the focus on the main features. However, this does give a limitation to Simply 5G Security. The details about 5G we exclude are still part of the 5G network. Future work could add these parts to guide the user further in implementing a 5G network.

On top of excluded content, another improvement could be to include a place on the website explaining attack models. With the attack models explained, the user can better envision the need for security. However, there is already information on attacker models out there [34]. It could also be a decision for future work to refer to said information instead of adding it to the website.

The goal of Simply 5G Security is to teach users about 5G Security in a structured way. However, testing whether our platform is making people learn better has not been done. Future work would therefore be to investigate if our website in fact does help users to learn about 5G Security in a successful way. Possibly by having an evaluation of the users' knowledge after using the website. Having 2 groups, one which uses the website to learn about 5G security and one group that does not use the website. Then afterwards a survey about 5G security could be done on both groups to determine if the website helped to learn or not.

A limitation of our work is the basic images provided. According to the multi-media learning principles [31], interactive content improves learning. Future work should include upgrading the images of the website. These images or even videos should be as interactive as possible. Exercises supported with images will improve the learning of the user.

Chapter 5

Conclusion

The increase in the Internet of Things (IoT) has led to the need for a new generation of mobile networks. In the past few years, 5G has become the new standard. One of the major changes 5G has made is the move from a hardware-based core network to a cloud-based core network. This change has led to more accessibility for creating a 5G network. It also increases the complexity of the 5G network and its specifications. While this can be a positive feature, it also introduces security risks. With more accessibility, more people can implement their own 5G network. Together with more complexity it increases the chance of implementation issues, as not everyone has the knowledge to create a secure network.

The 3GPP specifications give a detailed explanation of how to implement a 5G network. However, not everyone is able to follow these specifications. Other websites on 5G, either lack depth or do not focus on security aspects of the network. Therefore, we decide a new solution is needed.

Simply 5G Security offers a well-structured learning point for users who want or need to know more about 5G Security. With the use of media and text, we achieve a better learning platform. Moreover, we focus only on the essential parts the user needs to understand 5G and its security. This prevents the user from getting overwhelmed and lost in all the details.

Compared to websites which contain information on 5G, we also explain the basics of 5G [14, 15]. The difference between them, and Simply 5G Security, is the focus on the security aspect. With the explanation of each network function (NF), we also mention the security aspect of said NF. We also specifically mention which NF consumes and provides functions to other NFs. This information can not be found on other websites on the basics of 5G.

We use methods that allow us to focus on the content instead of development. Tools like Jekyll and Bootstrap let us avoid unnecessary web development and let us focus on the content. Using Jekyll has advantages

and disadvantages in our experience. As mentioned, using Jekyll gives us an already functioning website. However, by using the templates provided by the Jekyll community, we give up a part of the design freedom. By using the template, we follow the layout of the template. This saves us time but also limits us in terms of website design.

Creating Simply 5G Security was challenging in some parts. The most difficult choice was deciding on what information to put on the website and how to present the information. It is difficult finding a balance between providing enough details for the user to work with, and not overwhelming them with too many details at once. However, we think we found the middle ground to provide the user with detailed information.

Looking back, something we spend too much time on was making designs of how the website should look like. In the end, it changed completely because we decided on Jekyll templates. It would have been better to have a general design idea and focus on the content.

In conclusion, with this thesis, we explain our process of creating Simply 5G Security and by doing so, contribute to a more secure mobile network. Simply 5G Security gives information on 5G and its security to anyone who wants or needs to learn. There is still future work to be done but we fill the gap between the 3GPP specifications and more general websites on 5G. Therefore, in the future, we will continue working on Simply 5G Security with improvements mentioned in section 4.3. It will also become a part of Radix Security [35]. In terms of research, Simply 5G Security can be used to introduce new researchers to 5G.

Bibliography

[1] J. Harkin, *Mobilisation: The growing public interest in mobile technology.* Demos, 2003. [Online]. Available: http://www.demos.co.uk/files/Mobilisation.pdf

[2] F. Dahlqvist, M. Patel, A. Rajko, and J. Shulman, "Growing opportunities in the internet of things," *McKinsey & Company*, pp. 1–6, 2019.

[3] J. A. Adebusola, A. A. Ariyo, O. A. Elisha, A. M. Olubunmi, and O. O. Julius, "An overview of 5G technology," in *2020 International Conference in Mathematics, Computer Engineering and Computer Science (ICMCECS)*, 2020, pp. 1–4.

[4] D. Wubben, P. Rost, J. S. Bartelt, M. Lalam, V. Savin, M. Gorgoglione, A. Dekorsy, and G. Fettweis, "Benefits and impact of cloud computing on 5g signal processing: Flexible centralization through cloud-ran," *IEEE Signal Processing Magazine*, vol. 31, no. 6, pp. 35–44, 2014.

[5] M. Alenezi and M. Zarour, "On the relationship between software complexity and security," *arXiv preprint arXiv:2002.07135*, 2020.

[6] 3GPP, "5g; system architecture for the 5g system (5GS) (3GPP TS 23.501 version 17.6.0 Release 17)," Sep 2022. [Online]. Available: https://www.etsi.org/deliver/etsi_ts/123500_123599/123501/17.06.00_60/ts_123501v170600p.pdf

[7] I. Ahmad, S. Shahabuddin, T. Kumar, J. Okwuibe, A. Gurtov, and M. Ylianttila, "Security for 5G and beyond," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 4, pp. 3682–3722, 2019.

[8] C. Leuverink, "Detecting vulnerable 5G mobile networks exposed to the internet," Master Thesis. Radboud University, 2022.

[9] 3GPP, "The 3rd generation partnership project (3GPP)," 3GPP. [Online]. Available: https://www.3gpp.org/about-us

[10] ——, "5G; NR; user equipment (UE) radio transmission and reception; part 1: Range 1 standalone (3GPP TS 38.101-1 version 16.5.0 Release

16),” Nov 2020. [Online]. Available: https://www.etsi.org/deliver/etsi_ts/138100_138199/13810101/16.05.00_60/ts_13810101v160500p.pdf

[11] ——, “5G; 5G security assurance specification (SCAS); access and mobility management function (AMF) (3GPP TS 33.512 version 16.3.0 Release 16),” Aug 2020. [Online]. Available: https://www.etsi.org/deliver/etsi_ts/133500_133599/133512/16.03.00_60/ts_133512v160300p.pdf

[12] ——, “5G; security architecture and procedures for 5G system (3GPP TS 33.501 version 17.7.0 Release 17),” Sep 2022. [Online]. Available: https://www.etsi.org/deliver/etsi_ts/133500_133599/133501/17.07.00_60/ts_133501v170700p.pdf

[13] ——, “5G system overview,” Aug 2022. [Online]. Available: https://www.3gpp.org/technologies/5g-system-overview

[14] M. Ivezic, “Introduction to 5g core service-based architecture (SBA) components,” 5G Security, Aug 2020.

[15] S. Brown, “5G, explained,” MIT Sloan, Feb 2020. [Online]. Available: https://mitsloan.mit.edu/ideas-made-to-matter/5g-explained

[16] W3Schools, “HTML tutorial.” [Online]. Available: https://www.w3schools.com/html/

[17] ——, “CSS tutorial.” [Online]. Available: https://www.w3schools.com/css/

[18] J. Gruber, “Daring fireball: Markdown,” Daringfireball.net, 2019. [Online]. Available: https://daringfireball.net/projects/markdown/

[19] W3Schools, “Javascript tutorial.” [Online]. Available: https://www.w3schools.com/js/

[20] J. Team, “Jekyll • simple, blog-aware, static sites,” Jekyll • Simple, blog-aware, static sites. [Online]. Available: https://jekyllrb.com

[21] M. Otto, “Bootstrap,” Getbootstrap.com, 2019. [Online]. Available: https://getbootstrap.com

[22] T. Park, “Bootswatch: Free themes for bootstrap,” bootswatch.com. [Online]. Available: https://bootswatch.com

[23] J. Team, “Themes,” Jekyll • Simple, blog-aware, static sites. [Online]. Available: https://jekyllrb.com/docs/themes/

[24] C. Güney Aksakalli, “Jekyll doc theme,” Jekyll Doc Theme. [Online]. Available: https://aksakalli.github.io/jekyll-doc-theme/

[25] GitHub, "Github pages," GitHub Pages. [Online]. Available: https://pages.github.com

[26] J. F. Kurose and K. W. Ross, *Computer networking: a top-down approach.* Boston: Pearson, 2017.

[27] M. T. Goodrich and R. Tamassia, *Introduction to computer security*, ser. Always learning. Harlow: Pearson, 2014.

[28] "5g system overview," 3GPP, 08 2022. [Online]. Available: https://www.3gpp.org/technologies/5g-system-overview

[29] E. Cho and K. Youn-Kyung, "The effects of website designs, self-congruity, and flow on behavioral intention," *International journal of Design*, vol. 6, no. 2, 2012.

[30] K. Fenrich, "Securing your control system: the "CIA triad" is a widely used benchmark for evaluating information system security effectiveness," *Power Engineering*, vol. 112, no. 2, pp. 44–49, 2008.

[31] R. E. Mayer, "Multimedia learning," *Psychology of Learning and Motivation*, vol. 41, pp. 85–139, 2002. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0079742102800056

[32] D. S. Foundation, "Django." [Online]. Available: https://www.djangoproject.com/

[33] J. Themes, "Jekyll themes – a curated directory," 2023. [Online]. Available: https://jekyllthemes.io/

[34] M. Rocchetto and N. O. Tippenhauer, "On attacker models and profiles for cyber-physical systems," in *Computer Security–ESORICS 2016: 21st European Symposium on Research in Computer Security, Heraklion, Greece, September 26-30, 2016, Proceedings, Part II 21.* Springer, 2016, pp. 427–449.

[35] K. Kohls and D. Rupprecht, "Radix security." [Online]. Available: https://radix-security.com/about_us/

Appendix A

Code examples

A.1   Layout

An example of the HTML and CSS code of a *layout* file in Jekyll.

```
<!DOCTYPE html>
<html lang="{{ page.lang | default: site.lang | default: "en" }}">

{% include head.html %}

<body>

    {% include topnav.html %}

    <div class="page-content">
        <div class="wrapper">
            {{ content }}
        </div>
    </div>

    {% include footer.html %}
    {% include js_files.html %}
</body>

</html>
```

A.2   Include

An example of the HTML code of an *include* file in Jekyll.

```
<footer class="footer">
```

```
    <div class="container">

        <p class="text-center">
            {{ site.title }} {{ site.time | date: '%Y' }} |
            Part of <a href="https://radix-security.com">Radix Security</a>
        </p>
    </div>
</footer>
```

Appendix B

List of excluded content

B.1   Network functions

- Network Slice Selection Function (NSSF)
- Network Exposure Function (NEF)
- Policy Control Function (PCF)
- Application Function (AF)
- Edge Application Server Discovery Function (EASDF)
- Network Slice-Specific Authentication and Authorization Function (NSSAAF)
- Service Communication Proxy (SCP)
- Network Slice Access Control Function (NSACF)

B.2   Protocols

- Network domain security (II)
- User domain security (III)
- Application domain securit (IV)
- Visibility and configurability of security (VI)