A Security Analysis of the Lenel BlueDiamond

Quintin Walters[1], Joshua Niemann[1], Connor Leavesley[1], Daniel Capps[1], and Jacob Ruud[1]

[1]Computing Security, Rochester Institute of Technology

March 8, 2020

Abstract

The abstract is in a sense the most important part of your paper, since many readers will scan an abstract first before deciding to invest effort in reading the paper.

An abstract should be about 300 words long at most, and should act as a clear summary of the paper. It should state the aim and scope of the research, methods, results and conclusions, and the implications of the paper's finding. The abstract should be broadly accessible (i.e. able to be understood by as many people as possible - even those outside the field) and communicate the importance of the work being done.

Structure the abstract as follows: background and aims, methods, results and conclusion.

Examples of some decent abstracts can be found here, with the main ideas highlighted.

Keywords

Select keywords with care, because they will help users discover your paper. To determine appropriate keywords, put yourself in the position of someone who is trying to search for a paper like yours. What search terms would you use? From those terms, select a list of at least three and no more than five words. Include these words in the text of the abstract and if at all possible, in the title of the paper.

1 Introduction

Before we get to the actual introduction, welcome to Overleaf, as well as LaTeX itself! Although LaTeX certainly has its quirks, we hope that by contrasting the template you see here with the compiled document on the right side, you can get an intuitive sense of how to work with it.

Another thing before the introduction; here, I'm going attach a citation to this sentence [1]. Scroll on down to the bibliography section of the LaTeX code if you'd like to see the other end of the built-in references system. The numbering is all handled in-house – you just have to assign each reference a key, and Overleaf takes care of the rest.

On with the actual introduction! The introduction should provide context and background information appropriate for an academic audience. It should state a focused research question, define the variables being studied, and make clear the objective, importance, and relevance of the work.

Here is where you'd introduce the context surrounding your study. What led you to the question you ended up asking? Why is it relevant? Which fields of science is your question based around? What has previous literature demonstrated?

While the structure of the previous parts of the introduction can be relatively variable, you must make sure to provide a brief overview of the study itself, and the methods you used to accomplish it. Obviously, excessive detail is not necessary (that's what the next section is for). Lastly, be sure to make mention of the potential implications of your findings, but once again remember that you'll be going into more detail about that in the discussion.

For your Auth Paper: treat your introduction as the initial pitch of an idea or a thorough examination of the significance of a research problem. After reading the introduction, your readers should not only have an understanding of what you want to do, but they should also be able to gain a sense of your passion for the topic and to be excited about the study's possible outcomes.

Think about your introduction as a narrative written in **two to four paragraphs** that succinctly answers the following four questions:

1. What is the central research problem?
2. What is the topic of study related to that research problem?
3. What methods should be used to analyze the research problem?
4. Why is this important research, what is its significance, and why should someone reading the paper care about the outcomes of the proposed study?

2 Background & Significance

This is where you explain the context of your paper and describe in detail why it's important. It can be melded into your introduction or you can create a separate section to help with the organization and narrative flow of your paper. Approach writing this section with the thought that you can't assume your readers will know as much about the research problem as you do. Note that this section is not an essay going over everything you have learned about the topic; instead, you must choose what is most relevant in explaining the aims of your research.

To that end, while there are no prescribed rules for establishing the significance of your proposed study, you should attempt to address some or all of the following:

- State the research problem and give a more detailed explanation about the purpose of the study than what you stated in the introduction. This is particularly important if the problem is complex or multifaceted.

- Present the rationale of your proposed study and clearly indicate why it is worth doing; be sure to answer the "So What? question [i.e., why should anyone care].

- Describe the major issues or problems to be addressed by your research. This can be in the form of questions to be addressed. Be sure to note how your proposed study builds on previous assumptions about the research problem.

- Explain the methods you plan to use for conducting your research. Clearly identify the key sources you intend to use and explain how they will contribute to your analysis of the topic.

- Describe the boundaries of your proposed research in order to provide a clear focus. Where appropriate, state not only what you plan to study, but what aspects of the research problem will be excluded from the study.

- If necessary, provide definitions of key concepts or terms.

3 Related Work

Connected to the background and significance of your study is a section of your paper devoted to a more deliberate review and synthesis of prior studies related to the research problem under investigation. The purpose here is to place your project within the larger whole of what is currently being explored, while demonstrating to your readers that your work is original and innovative. Think about what questions other researchers have asked, what methods they have used, and what is your understanding of their findings and, when stated, their recommendations.

Since a literature review is information dense, it is crucial that this section is intelligently structured to enable a reader to grasp the key arguments underpinning your proposed study in relation to that of other researchers. A good strategy is to break the literature into "conceptual categories" [themes] rather than systematically or chronologically describing groups of materials one at a time. Note that conceptual categories generally reveal themselves after you have read most of the pertinent literature on your topic so adding new categories is an on-going process of discovery as you review more studies. How do you know you've covered the key conceptual categories underlying the research literature? Generally, you can have confidence that all of the significant conceptual categories have been identified if you start to see repetition in the conclusions or recommendations that are being made.

NOTE: Do not shy away from challenging the conclusions made in prior research as a basis for supporting the need for your paper. Assess what you believe is missing and state how previous research has failed to adequately examine the issue that your study addresses. For more information on writing literature reviews, go to: https://libguides.usc.edu/writingguide/literaturereview.

To help frame your paper's review of prior research, consider the "five C's" of writing a literature review:

- Cite, so as to keep the primary focus on the literature pertinent to your research problem.

- Compare the various arguments, theories, methodologies, and findings expressed in the literature: what do the authors agree on? Who applies similar approaches to analyzing the research problem?

- Contrast the various arguments, themes, methodologies, approaches, and controversies expressed in the literature: describe what are the major areas of disagreement, controversy, or debate among scholars?

- Critique the literature: Which arguments are more persuasive, and why? Which approaches, findings, and methodologies seem most reliable, valid, or appropriate, and why? Pay attention to the verbs you use to describe what an author says/does [e.g., asserts, demonstrates, argues, etc.].

- Connect the literature to your own area of research and investigation: how does your own work draw upon, depart from, synthesize, or add a new perspective to what has been said in the literature?

4 Research Design & Methods

To provide a well rounded analysis of the device we expect three primary areas of research. First, we expect to perform attacks against the physical security of the device. Second, we will analyze the firmware for vulnerabilities. Finally, we plan on testing the application and Bluetooth implementation.

The phyisical security of the lock, particularly the magnetic antitamper switch, is what protects it from well known attacks against the Wiegand protocol. If the physical security can be bypassed than attackers could take advantage of these other attacks to bypass the lock entirely.

Firmware analysis is necessary to discover underlying vulnerabilities. The vulnerabilities discovered here may include hardcoded credentials, service backdoors, and poorly implemented authentication methods. These vulnerabilites would not be obvious or easily detectible without dissecting the firmware.

The application and Bluetooth implementation are the primary means which users will be interacting with the device. Any vulnerabilities here will be exposed to outside attackers on a daily basis. Any attacker within 30ft of the device can snoop on the Bluetooth traffic. The application is also downbloadable on the Google Play Store for free, any vulnerabilities in it would be easily accessible to an attacker.

4.1 Firmware Analysis

- Search for hard-coded credentials.
- Search for vulnerabilities such as buffer overflows, default certificates, debugging services, open ports, etc.
- Search for improperly implemented authentication and cryptographic methods.
- Search for any unpatched vulnerabilities in dependencies and base code such as BlueBorne.

Firmware analysis is a solid foundation for the research to build upon. The firmware is the software that runs on and controls the device as a whole, vulnerabilities evident in it reduce the security of the device as a whole and can lead to vulnerabilities in other areas. The firmware analysis will be performed with automated tools at first, followed by manual analysis to confirm any discoveries. A final pass through with manual analysis will then be done to spot any missed or overlooked vulnerabilities. The methods of analysis will vary, depending on if we are supplied with the firmware or if we have to extract it from the device ourselves. If we are provided with the firmware source code we can do analysis directly on that, if we need to extract it ourselves we will have to disassemble it and spend a large amount of time reverse engineering in order to find any vulnerabilities.

4.2 Bluetooth and Application Analysis

- Perform Generic Attribute Protocol (GATT) attacks to gather data about the device and conduct Man-in-the-Middle (MITM) attacks.
- Perform known cryptographic attacks against Bluetooth Low Energy (BLE) to decrypt intercepted traffic, perform replay attacks and command injection.
- Search for hard-coded credentials, buffer overflows, and other application vulnerabilities.
- Search for abusable edge cases in the authentication scheme.

BLE is a major part of this research. BLE is a Bluetooth protocol variant designed for low energy operations and such has a limited set of computing resources available. BLE does not need manual pairing to a device, meaning an application with the correct authentication data can pair automatically. Automated tools will gather preliminary data about the device by examining the GATT and Generic Access Profile (GAP) . The tool will copy he GATT over to an intermediary device and MITM all communications between the device and the application. With the device communication being intercepted, an Injection Free Attack can force a re-pairing and the intermediary device will intercept the Short Term Key. With the Short Term Key, we can derive the Long Term Key. We can then use the Long Term Key to decrypt communications and send commands on the behalf of the application. Automated tools will scan the application to discover hard-coded credentials and vulnerabilities. Finally, edge cases in the authentication scheme will be manually explored to see if an attacker could exploit permissions.

5 Preliminary Suppositions & Implications

Just because you don't have to actually conduct the study and analyze the results, doesn't mean you can skip talking about the analytical process and potential implications. The purpose of this section is to argue how and in what ways you believe your research will refine, revise, or extend existing knowledge in the subject area under investigation. Depending on the aims and objectives of your study, describe how the anticipated results will impact future scholarly research, theory, practice, forms of interventions, or policymaking. Note that such discussions may have either substantive [a potential new policy], theoretical [a potential new understanding], or methodological [a potential new way of analyzing] significance.

When thinking about the potential implications of your study, ask the following questions:

- What might the results mean in regards to challenging the theoretical framework and underlying assumptions that support the study?
- What suggestions for subsequent research could arise from the potential outcomes of the study?
- What will the results mean to practitioners in the natural settings of their workplace?
- Will the results influence programs, methods, and/or forms of intervention?
- How might the results contribute to the solution of social, economic, or other types of problems?
- Will the results influence policy decisions?
- In what way do individuals or groups benefit should your study be pursued?
- What will be improved or changed as a result of the proposed research?
- How will the results of the study be implemented and what innovations or transformative insights could emerge from the process of implementation?

NOTE: This section should not delve into idle speculation, opinion, or be formulated on the basis of unclear evidence. The purpose is to reflect upon gaps or understudied areas of the current literature and describe how your proposed research contributes to a new understanding of the research problem should the study be implemented as designed.

6 Conclusions

The conclusion reiterates the importance or significance of your paper and provides a brief summary of the entire study. This section should be only one or two paragraphs long, emphasizing why the research problem is worth investigating, why your research study is unique, and how it should advance existing knowledge.

Someone reading this section should come away with an understanding of:

- Why the study should be done,
- The specific purpose of the study and the research questions it attempts to answer,
- The decision to why the research design and methods used where chosen over other options,
- The potential implications emerging from your proposed study of the research problem, and
- A sense of how your study fits within the broader scholarship about the research problem.

7 Acknowledgements

In the Acknowledgements section, the author(s) acknowledge or thank any persons or institutions who helped support the work in any way. In particular, this section must disclose any funding for the research completed, including the grant number (if a grant was awarded).

Anyone to thank/credit for helping your team along the way? This is the place to do it.

8 Appendix

Appendices are optional sections that should include additional tables, figures, or other data beyond what is included in the results section. An appendix should be able to stand separately from the prinicpal article. Therefore, no references (callouts) to appendix figures or tables should be made in the principal article. If required, the appendix should have its own bibliographic reference list with citations to that list confined to the appendix. [1]

9 References

[1] M. Goossens, F. Mittelbach, and A. Samarin. *The LaTeX Companion*. Addison-Wesley, Reading, Massachusetts, 1993.

[2] test. test, Dec. 1998. Accessed blah.