ULB UNIVERSITÉ LIBRE DE BRUXELLES

Cryptographic protocols in the real world

Jens Hermans

Topic : Security

Julien Baudru - 000460130

March 20, 2022

Contents

1 Introduction

This document the synthesis of the seminar given by Jens Hermans during which he briefly presented the different steps necessary to implement, develop and standardize a security protocol in a presentation entitled : **Cryptographic protocols in the real world**.

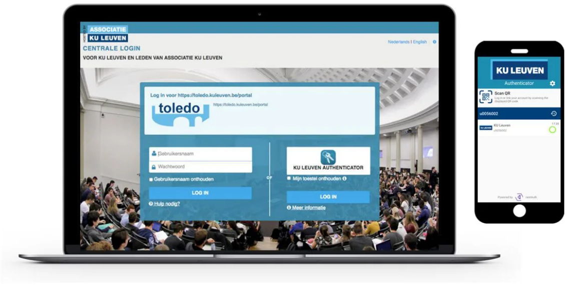

Figure 1: Illustration taken from the speaker's slides

In computer security, one of the most recurrent problems when we wish to create and share a new cryptographic system lies in the accomplishment of the following steps: The theoretical proof of the correctness of this system, the development, the standardization i.e. the acceptance of the newly created protocole by the NIST organization (National Institute of Standards and Technology) and of course the implementation of the newly created protocol and how to produce accurate documentation to avoid security breaches by allowing the future developer to use this protocol as intended by its creators. During this seminar, the presenter went through each of these different steps, giving concrete examples each time, including many comparisons with the TLS (Transport Layer Security) protocol. He also shared his personal experience in developing such a protocol as well as the difficulties he and his team had to face during this period. The presenter's approach to the topic was more like a roadmap to follow in order to finalize the deployment of a new security protocol, hence the presence of the words *real word* of the title, rather than on how to develop them in practice. He explained the different good practices to be followed as well as the requirements that a new protocol should absolutely follow.

(1524 characters)

2 Biography

Jens Hermans, the presenter of the seminar, is an expert in cryptographic protocols, provable security and authentication. He is currently CEO of nextAuth, a company that grew out of KU University Leuven and is dedicated to secure mobile authentication and making security accessible to as many people as possible. During his scientific career the presenter of the seminar published around 34 papers from 2009 to 2019 and gave talks at various conferences such as the Annual Computer Security Applications Conference (ACSAC) or the European Conference on ePassports (FIDELITY event). Before the nextAuth adventure, Jens Hermans was a part-time web developer, then from 2008 to 2012 he joined the COSIC group (Computer Security and Industrial Cryptography group) of the electricity department of the KU Leuven as PhD researcher, this research laboratory has as main objective to provide expertise in digital security. Then, until 2019, he was a post-doctoral researcher in this same laboratory. On the academic side, he obtained his Master in mathematical engineering in 2008 for which he received an award from Jos Schepens Memorial Fund and his PhD in 2012 with his thesis entitled Lightweight Public Key Cryptography, both at KU Leuven. In addition, he has also held various academic committee posts such as member of the Academic Council and member of the Executive Committee Science. Finally, he is also in charge of teaching the *Advanced methods in cryptography (H03G5A)* course at the KU Leuven. During his career he has mainly focused on creating security protocols for practical application case such as template protection, electronic voting, models for RFID privacy, lightweight public key protocols for RFID, ePassports or biometric databases.

3 The major points discussed

The main points discussed during this seminar are listed and detailed below.

- **Security goals of a protocol:** In a first instance, the presenter insisted on the fact that it was important to know in which field we evolve, it is indeed important not to lose sight of the fact that there is the communication protocol on one side and the human on the other. Then, he explained the different security goals that protocols should reach, such as data authenticity or data confidentiality. Then, for a protocol to be usable in practice, it must be efficient and low on resources to be for example executed on a smartphone for which the battery is a limiting factor thus requiring a light and simple protocol. Finally, he explain that the best way to prove the robustness of a protocol is to do it mathematically, a security protocol must be theoretically verifiable even it's a difficult task. Indeed, one of the most common mistakes is trying to prove the security of a protocol by assuming that an attacker will follow a well-defined pattern for his attack. Moreover, the more assumptions we make about how the protocol will be used and/or attacked, the more we increase the risk of breaches.

- **Standardization:** In order to make the protocol usable by all the systems it is necessary to pass by a phase of standardization. This phase of verification is carried out by the National Institute of Standards and Technology (NIST), the latter established a set of guidelines that must be respected by the protocols, these are known under the name of Federal Information Processing Standards (FIPS). This phase can take several years due to the multiple exchanges between the experts who analyze if the protocol respects the guidelines and the resulting modifications by the developers of the protocol. Moreover this time can also vary according to the country by which this new protocol is analyzed, there are indeed several instances of NIST in different countries. However, and that's an important point, the presenter indicated that it was not because a protocol was standardized that it was totally secure, indeed it happens that some large organizations force the hand to keep protocols which one proved that they were broken. Indeed, there seems to be a political implication behind this phase and the importance of it also varies according to the country. Moreover, it is possible that a protocol that has been standardized turns out to be broken with time, for example, this case occurred with the following protocols: RC4, MD5 or SHA-1.

- **Putting the protocol into practice:** Jens Hermans then indicated that having a nice paper describing the protocol is all well and good, but it is also essential to describe precisely how to use it. Indeed, as this protocol will be used by different parties for mutliple purposes, it is essential to be precise about what the developers using it will have to respect in order not to compromise security. Thus, in the documentation it is better to be strict about how to use the differents part of this protocol, for example what form the messages should take or how the sessions should be established. Here the presenter took the example of TLS for which the documentation on how to implement connections is very informal. Finally, it is also important to try to keep this protocol as easy as possible to implement in order to avoid making the life of developers too complicated. A good counter example to this practice was given by the protocol used for ePassports. However this protocol is indeed complicated by the will to leave many possibilities open given the number of possible uses.

4 Other papers

Unlike previous seminars we have attended, this one was not based on a paper written by the author, so the papers that follow are related to the topics discussed by the presenter without being strictly quoted by him.

4.1 Closely related papers

Among the various papers closely related to the subject presented during this seminar we can retain the paper written by Ling Dong and Kefei Chen entitled *Security Analysis of Real World Protocols*[2]. In this paper the authors analyze real world security protocols using the trusted freshness method, the main goal of this paper is to allow the reader to understand this last method but also to allow him to evaluate the security level of the protocols he would use. The two authors analyze different communication protocols on the web and in particular the TLS protocol often quoted as an example during this seminar, this is why this paper is related to the subject presented in these pages.

Another paper that can be cited is *Model Checking Security Protocols*[1] co-authored by David Basin, Cas Cremers and Catherine Meadows in 2018. In this paper, the three authors present different models and techniques for checking security protocols. Through this article, they also detail the main concepts of protocol security analysis, namely, the abstraction of messages, protocols as role automata, the adversary model, and property specification. This article is closely related to the subject treated by the presenter of the seminar, indeed he insisted on the importance of the formal verification of security protocols and on the complexity of carrying out this task by hand.

4.2 Related papers

Given the growing importance of connected objects in our daily lives and their many security flaws often reported in the media, the first paper will deal with the Internet of Things (IoT). This paper was written by Kim Thuat Nguyena, Maryline Laurent and Nouha Oualhaa and is entitled *Survey on secure communication protocols for the Internet of Things*[4]. In the latter, the three authors apply themselves to demonstrate the various security problems related to the IoT as well as to show the limits of existing solutions. Moreover, they focus on new security protocols and techniques proposed by different authors, on the specific security properties needed for the IoT and on the cryptographic primitives used by these systems. Although the presenter does not focus specifically on the IoT, this paper is clearly related to the topic of this seminar as it focuses on security protocols and more specifically how they are designed and used.

A second paper related to the topic discussed here that can be chosen is *Secure Communication Protocol for Mobile Multimedia Applications*[3] by Komninos, Honary and Darnell. In these the authors present a secure communication protocol for mobile multimedia applications. The main innovation brought by the protocol presented here is that both parties, receivers and senders, are involved in the generation of the keys used for the communication session. Moreover, this protocol identifies the mode used by the cryptographic algorithm, thus allowing to reduce the time and energy needed to process the data. This paper is indeed related to the topic of the seminar as it deals with a new concrete proposal for a real-world communication protocol. In addition, the company netxAuth, of which the presenter is the CEO, is also involved in providing security for mobile devices.

5 Other groups

The main research groups in the field of computer security seem to be mainly linked to various universities, apart from the presenter's group, we can mention among others the following groups: the iCSS (Interdisciplinary Research Centre in Cyber Security) of the University of Kent in England, the CSRG (The Cyber Security Research Group) of the King's college of London or the COSIC (The Computer Security and Industrial Cryptography group) of the KU Leuven. Furthermore, it seems important to mention The European Cyber Security Organisation (ECSO), which is an organisation working closely with the European Commission in the public and private sectors.

6 Open science

The author of the conference as well as the colleagues with whom he co-authored his various papers seem to practice open science. Indeed, on the website of the presenter, a list of these different articles is available and a digital version of the majority of them are downloadable for free. However, concerning in particular the protocols for the real world, and more particularly everything that revolves around the algorithms developed by the company nextAuth, there does not seem to be any trace of code on the internet. This is quite logical for a private company, but it goes against the principles of open science regarding the protocols related to the different scientific papers published by the presenter.

7 Two scientific questions

During the first part of the seminar, the presenter emphasized the importance of formally verifying the security of a protocol as well as the inherent difficulty of solving this problem by hand. **I wondered if there was no automatic way to check this type of property?** Wouldn't there be a language developed for this purpose?

My second question is not strictly scientific but rather the continuation of the approach taken by the presenter in his talk. Given the various fastidious steps and the huge amount of time and energy needed to develop such a protocol : **I was wondering how companies developing security protocols manage financially?** Do they have access to subsidies? What if the protocol is never accepted by the standardization authority? This question makes sense to me since Jens Hermans is himself CEO of such a company.

8 Criticism(s) about the seminar

One small criticism that could be made to this presentation is the fact that, although it is not the main purpose of this seminar, there is a certain lack of technical details about the cryptographic algorithms created by the presenter and his team. In my opinion, it would have been interesting to discuss some of the details of the algorithm's implementation in more depth as most of the audience has followed courses explaining the fundamentals of cryptography. Another criticism/question that comes to mind is why the slides were not made available for this seminar? Was it for educational purposes or for intellectual property reasons?

References

[1] David Basin, Cas Cremers, and Catherine Meadows. "Model Checking Security Protocols". In: *Handbook of Model Checking*. Ed. by Edmund M. Clarke et al. Cham: Springer International Publishing, 2018, pp. 727–762. ISBN: 978-3-319-10575-8. DOI: 10.1007/978-3-319-10575-8_22. URL: https://doi.org/10.1007/978-3-319-10575-8_22.

[2] Ling Dong and Kefei Chen. "Security Analysis of Real World Protocols". In: *Cryptographic Protocol: Security Analysis Based on Trusted Freshness*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 153–213. ISBN: 978-3-642-24073-7. DOI: 10.1007/978-3-642-24073-7_5. URL: https://doi.org/10.1007/978-3-642-24073-7_5.

[3] Nikos Komninos, B. Honary, and M. Darnell. "Secure Communication Protocol for Mobile Multimedia Applications". In: *3rd International Symposium on Wireless* (Jan. 2000). URL: https://www.academia.edu/511635/Secure_Communication_Protocol_for_Mobile_Multimedia_Applications.

[4] Kim Thuat Nguyen, Maryline Laurent, and Nouha Oualha. "Survey on secure communication protocols for the Internet of Things". In: *Ad Hoc Networks* 32 (2015). Internet of Things security and privacy: design methods and optimization, pp. 17–31. ISSN: 1570-8705. DOI: https://doi.org/10.1016/j.adhoc.2015.01.006. URL: https://www.sciencedirect.com/science/article/pii/S1570870515000141.