Why Should We Analyse Security Ceremonies?

Jean Everson Martina[1⋆] , Marcelo Carlomagno Carlos[2⋆⋆]

[1] University of Cambridge
Computer Laboratory
William Gates Building
15 JJ Thomson Avenue
Cambridge – CB3 0FD – United Kingdom
Jean.Martina@cl.cam.ac.uk

[2] Royal Holloway University of London
Information Security Group
Egham, Surrey – TW20 0EX – United Kingdom
marcelo.carlos.2009@rhul.ac.uk

Abstract. The concept of ceremony as an extension to network/security protocols was introduced by Ellison. No methods or tools to check correctness or the properties in such ceremonies are currently available. The applications for security ceremonies are vast and normally fill gaps left by strong assumptions in security protocols, like provisioning of cryptographic keys and or correct human interaction. The key issue in this extended abstract is the formalisation of the human cognitive processes in security ceremonies taking them into account when designing or verifying protocols. We intend to survey a possible formal approach for analysing ceremonies by combining existing proposals.
Keywords : Security Ceremonies, Security Protocols, Formal Methods, Cognitive Human Formalisation

1 Introduction

Protocols has been analysed for a long time now. Since Needham and Schroeder's[1] has introduced the idea, methods have been researched to prove protocols' correctness and claims. We have seen a lot of research in this field, in particular in developing formal methods and logic to check and verify its claims. We must cite Burrows et al.[2] for their belief logic, Abadi for spi-calculus[3], Ryan[4], Lowe[5] and Meadows[6] for works on state enumeration and model checking, and Paulson and Bella[7,8] for their inductive method as the principal initiatives. We have been also seing the creation of a large number of tools to verify and check security protocols. These techniques and tools have evolved in such a way that, nowadays, we can check and analyse complex and extensive protocols, varying from classic to complex, well-established and deployed ones.

Meadows [9] and Bella et al.[10] gave us a broad coverage of the maturity in this field. We also see in these papers trends followed by methods, pinpointing their strong and weak points. They give propositions for research ranging from open-ended protocols, composability and new threat models; something that has changed very little since Dolev and Yao's proposal[11]. These problems seem very well covered nowadays. Research in general is just trying to optimise the actual methods in speed and coverage.

However, recent research[12,13] shows us that even the most deployed, tested and analysed protocols, such as SSL/TLS or Kerberos, can have security problems. This normally happens when a user acts in an unexpected, but cognitively predictable way. Since protocols operate at the computer level, we tend just to verify them for computer interaction. Nevertheless, they are built to accomplish a human task and we must design and also verify protocols (in this case ceremonies) also against human

⋆ Supported by CAPES Foundation/Brazil on grant #4226-05-4
⋆⋆ Supported by CNPq/Brazil

interaction. We must take into account human cognitive processes when designing computer security protocols. Corroborating the idea that verification of protocols should include more environmental assumptions, Bella et al.[10] state that "it is unwise to claim that a protocol is verified unless the environmental assumptions are clearly specified. Even then, we can be sure that somebody will publish an attack against this protocol".

Ceremonies and ceremony analysis were introduced by Ellison[14,15]. His description states that "ceremonies extend the concept of protocols by including human beings, user interfaces, key provisioning and all instances of the workflow". This idea can give a broader coverage of the protocols' point of view, extending what can be analysed and verified by protocol techniques. Ellison gives an overview and establishes the basic building blocks for ceremony description. Although he states the possibility of using the formal methods available for security protocol analysis, no major work is found today in the ceremony formal-analysis field. This point creates a weak spot, and leads to empirical analysis, which can be difficult and error-prone, as protocol analysis history shows us.

An important advance that can enable us to reason about ceremonies was introduced by Rukšėnas et al.[16,17]. They developed a human error cognitive model, initially applied to interaction on interfaces. They show that, normally, security leaks come from mistakes modelling interfaces, not taking into account the cognitive processes and expectations of human beings behind the computer screen. They successfully verify problems on an authentication interface and a cash-point interface. They showed the normal lack of consideration in the human peers cognitive processes, the weakest factor in these systems. Their modelling comes with a powerful implementation using a model-checker to assist the state verification. This makes the approach reasonable to integrate with actual protocol verification ones.

To try to achieve this complex task of verifying security ceremonies, we need to first understand what the major differences and features of ceremonies are when compared to security protocols (Section 2), then we will explore the propositions of Ellison's and Rukšėnas et al. proposals focusing on human peers and cognitive causes of security leaks (Section 3). We will conclude with some thoughts on what is achievable and the limitations we can have.

2 Ceremony Analysis versus Protocol Analysis

Security ceremonies are a superset of security protocols. They can be seen as an extension of security protocols, by including out-of-bounds operations of protocols. These out-of-bounds operations are normally the assumptions we have to make when trying to check or analyse claims for protocols. They can include a safe key distribution scheme for symmetric key protocols, the confidence we must have that the computer executing the protocol is trusted and that the users will behave as expected, among other things.

Inclusion of human interaction, and consequently, behaviour and cognitive processes, is a characteristic of ceremonies as human peers are out of bounds for protocol verification. They are normally the most error prone peer in any process, and their inclusion can enrich in details and coverage any analysis done so far. The inclusion of this new piece can lead us to understand better how and why correctly implemented and deeply verified protocols still fail for some set of users.

Protocol descriptions tend to be easier to transcribe as mathematical notations, due to the intrinsic computational characteristics present in them. Much of this comes from their being targeted to computers. Ceremonies modelling is a much more subtle approach, since the possibilities involved in modelling human behaviour and/or cognition are immense. The environmental coverage ceremonies brings to security protocols is another property worth verifying. This can gives us better insights into the problem of the composability of protocols. The composability problem normally happens because of clashes between environmental assumptions embedded into protocols. By not being able to model the environment, we also cannot predict what will happen with two protocols designed with their own environment in mind, and put to work together.

There is also the idea of breaking down assumptions of protocols, by taking them as variables in security ceremonies. An example is the key distribution phase. It is not clear if it will give us better

insights in the protocols analysis, since some methods in the past[8] already modelled the loss of keys and the compromise of peers by a spy. This feature of security ceremonies seems to add complexity without bringing better results, thus it seems the least likely extension to research.

3 A Proposed Method

By Ellison's modelling, every computer connected to the network has a human that has its expectations and cognitive factors relying on the execution of protocols. As humans don't explicitly send messages in a protocol run, but interact with the computer using an interface, Rukšėnas' modelling seems very attractive for analysing ceremonies.

Taking into account Bella's goal availability[8] and the idea that guarantees should be present in each peers' point of view, we should produce independent verification models based on Rukšėnas approach for each human peer. Every human peer represented will have its own mental and physical actions, pre-determined goals, reactive behaviour, salience, voluntary task completion and forced task completion attributes. This human peer will "interface" with the protocol taking his point of view from the execution.

We will model the interaction by representing the protocols as the devices.This will keep protocols as black boxes, thus being analysed separatly, and enable us to test user interpretation of protocol messages, as well as possible inputs and outputs the user can create with his computer node in the scope of the ceremony.

Each human peer should be modelled following its possible cognitive aptitudes and in the presence of an attacker. This will give us insights on which pitfalls the user is more likely to go into. By tuning the human peer attributes we will be able in the future to grade protocols and ceremonies with scales representing the possibility of attacks depending on user experience and its pre-determined goals for example. This will give us a better tool to design and test protocols against real scenarios and user specifications.

As Rukšėnas et al. don't explore yet the environment model proposed in their approach, we will opt now for tackling just the user model for the security ceremonies. We must emphasise that the environment modelling can be a key issue to understand protocol composability in the future. This makes the approach even more appealling.

4 Final Considerations

The idea of modelling ceremonies and applying formal methods to them seems promising. The knowledge acquired by the protocol analysis community can be used to boost ceremony analysis. Such analysis can help us to detect scenarios where protocols are more prone to fail. By understanding better these issues we will be able to design more user centric and less-likely to fail protocols.

We don't want to change the way we analyse protocols today, since the formal methods available are mature and powerful for their intended purposes. We want to approach the problem from a different point of view.

The idea of defining an interface between humans and protocols seems a good approach to achieve a reasonable cognitive verification of ceremonies. Keeping with the addition of the human peers in ceremonies, and targeting their cognition as our primary objective seem logical and an easier task to accomplish. The proposal also uses the idea of an environment, which can help us to understand composability, a still open area in security protocols.

The next step is testing this proposal in an already modelled ceremony, and to try to create a method to establish interfaces between protocols and human peers. This will give us the data not available right now to decide if the current proposal is as promising as it looks like.

References

1. Needham, R.M., Schroeder, M.D.: Using encryption for authentication in large networks of computers. Commun. ACM **21**(12) (1978) 993–999
2. Burrows, M., Abadi, M., Needham, R.: A logic of authentication. In: Proc. 12th ACM Symposium on Operating Systems Principles, Litchfield Park, Arizona (December 3-6 1989)
3. Abadi, M., Gordon, A.D.: Reasoning about cryptographic protocols in the spi calculus. In: CONCUR '97: Proceedings of the 8th International Conference on Concurrency Theory, London, UK, Springer-Verlag (1997) 59–73
4. Ryan, P., Schneider, S.: The modelling and analysis of security protocols: the csp approach. Addison-Wesley Professional (2000)
5. Lowe, G.: Breaking and fixing the needham-schroeder public-key protocol using fdr. In: TACAs '96: Proceedings of the Second International Workshop on Tools and Algorithms for Construction and Analysis of Systems, London, UK, Springer-Verlag (1996) 147–166
6. Meadows, C.: Language generation and verification in the nrl protocol analyzer. In: CSFW '96: Proceedings of the 9th IEEE workshop on Computer Security Foundations, Washington, DC, USA, IEEE Computer Society (1996) 48
7. Paulson, L.C.: The inductive approach to verifying cryptographic protocols. Journal of Computer Security **6**(1-2) (1998) 85–128
8. Bella, G.: Formal Correctness of Security Protocols. Volume XX of Information Security and Cryptography. Springer Verlag (2007)
9. Meadows, C.: Formal methods for cryptographic protocol analysis: Emerging issues and trends. IEEEJSAC: IEEE Journal on Selected Areas in Communications **21** (2003)
10. Bella, G., Longo, C., Paulson, L.C.: Is the verification problem for cryptographic protocols solved? In Christianson, B., Crispo, B., Malcolm, J.A., Roe, M., eds.: Security Protocols Workshop. Volume 3364 of Lecture Notes in Computer Science., Springer (2003) 183–189
11. Dolev, D., Yao, A.: On the security of public key protocols. Information Theory, IEEE Transactions on **29**(2) (Mar 1983) 198–208
12. Gajek, S.: Effective protection against phishing and web spoofing. In: Proceedings of the 9th IFIP TC6 and TC11 Conference on Communications and Multimedia Security (CMS 2005), Springer-Verlag, LNCS 3677. (2005) 32–41
13. Jakobsson, M.: The human factor in phishing. In: In Privacy & Security of Consumer Information '07. (2007)
14. Ellison, C.: Ceremony design and analysis. Cryptology ePrint Archive, Report 2007/399 (2007) http://eprint.iacr.org/.
15. Ellison, C.: Improvements on conventional pki wisdom. In: Proceedings of the First Annual PKI Research Workshop, Gaithersburg, MD (April 2002)
16. Ruksenas, R., Curzon, P., Blandford, A.: Modelling and analysing cognitive causes of security breaches. Innovations in Systems and Software Engineering **4**(2) (June 2008) 143–160
17. Ruksenas, R., Curzon, P., Blandford, A.: Detecting cognitive causes of confidentiality leaks. In Cerone, A., Curzon, P., eds.: Proceedings of the First International Workshop on Formal Methods for Interactive Systems (FMIS 2006). Volume 183 of Electronic Notes in Theoretical Computer Science. (July 2007) 21–38