2011

Seeing the full picture: the case for extending security ceremony analysis

Giampaolo Bella
De Montfort University, UK

Lizzie Coles-Kemp
Edith Cowan University

Originally published in the Proceedings of the 9th Australian Information Security Management Conference, Edith Cowan University, Perth Western Australia, 5th -7th December, 2011

SEEING THE FULL PICTURE: THE CASE FOR EXTENDING SECURITY CEREMONY ANALYSIS

Giampaolo Bella[1] and Lizzie Coles-Kemp[2]
[1]Dipartimento di Matematica e Informatica, Università di Catania, Italy
Software Technology Research Laboratory, De Montfort University, UK
[2]Information Security Group, Royal Holloway University of London, UK
School of Computer and Security Science, Edith Cowan University, Australia
giamp@dmi.unict.it; lizzie.coles-kemp@rhul.ac.uk

Abstract

The concept of the security ceremony was introduced a few years ago to complement the concept of the security protocol with everything about the context in which a protocol is run. In particular, such context involves the human executors of a protocol. When including human actors, human protocols become the focus, hence the concept of the security ceremony can be seen as part of the domain of socio-technical studies. This paper addresses the problem of ceremony analysis lacking the full view of human protocols. This paper categorises existing security ceremony analysis work and illustrates how the ceremony picture could be extended to support a more comprehensive analysis. The paper explores recent weaknesses found on the Amazon's web interface to illustrate different approaches to the analysis of the full ceremony picture.

Keywords
Technical perspective; practice perspective; socio-technical; human-computer; Amazon; security protocol, security ceremony

INTRODUCTION

The enormous literature about security protocol analysis has taught a great deal about threats for, attacks to, and properties of modern protocols. It has ultimately contributed to the development and deployment of more robust protocols.

More recent research (Karloff et al., 2009; Gunawardena, 2007;Radke et al., 2011; Martina et al., 2009) has pointed out that yet more insights are derived from putting a protocol in context, which turns out to be so multi-faceted as to involve profound technical and social elements. For example, protocols involving public-key cryptography cannot be generally used in contexts where certification authorities cannot be relied upon, such as over mobile networks. Similarly, the protocol users cannot be assumed to always act as anticipated by the protocol designers. This demonstrates the context sensitive nature of technology. It also indicates that it is more than context at work – in addition to the circumstances of technology use, cultural belief systems, demographic factors and emotions play a substantial role in shaping protocol user responses.

It has been realised that whatever a protocol leaves "out-of-band" and neglects defining or clarifying cannot be dismissed during practical use. Hence, the definition of *ceremony*, introduced by Walker and elaborated further by Ellison, explicitly expands that of a security protocol to include whatever was left out-of band (Ellison, 2007) . In particular, a ceremony recognises the role played by the human, who is "likely to do incomplete comparisons of values, for example" (Ellison, 2007). Introducing the role of the human introduces considerable complexity into the analysis. There are essentially two perspectives when the human is introduced: viewing the human from the perspective of the technology (the perspective that is typically adopted in security protocol analysis) or viewing the technology from the perspective of the human (the perspective that is typically adopted in technology practice analysis). Whilst the technology perspective gives us robust analysis of how technology behaves, it does not have the analytical tools to account for the different ways in which humans engage with technology. The technology practice perspective enables analysis of different types of human interaction with technology and allows for a richer picture of the security ceremony. Current ceremony literature acknowledges technology practice but does not present the analytical tools to develop that perspective. This paper addresses the problem of ceremony analysis lacking the full view of human protocols. In addressing this problem, this paper identifies where analytical tools are necessary to form this fuller ceremony picture and concludes with a discussion of how a formal analysis approach may be used to explore both perspectives.

CURRENT ANALYSIS FOCUS

This section outlines the development of security ceremony thinking and introduces our running example.

Security Ceremonies

Social engineering teaches us that formal correctness of the technology in use does not necessarily imply *security* for its users. We are now aware that humans cannot always be expected to make the choices anticipated in technology design. For example, they cannot be expected to remember a very long password and to type it in without mistakes within a bounded number of attempts just because this meets an expectation of secure authentication. Hence, traditional security protocol analysis has clear limitations as its assumptions about human behaviour are often flawed.

The first publication on ceremonies (Ellison, 2007) was made in 2003. Although the definition of ceremony was rather vague, to account for "messages among computers, people and possibly the environment" [6], it meant a real breakthrough. It acknowledged for the first time that computer security cannot be treated as a purely theoretical-then-technical issue because the nodes it involves are not all computer programs and human nodes need to be included in the picture of the protocol.

In particular, the notion of ceremony indicates that the classical protocol picture must be expanded with a representation of humans and the extra exchanges within the social protocol. This current view of the security ceremony is represented in *Figure 1*.

The exchange between humans and their computers is termed "prot'" and refers to a protocol in the common understanding. However, the protocol between technological nodes, the protocol between human nodes and the protocol between human and technological nodes has very different properties and leads us to challenge what we understand by the term protocol (Wikipedia, 2011). Alexander Galloway (Galloway, 2004) emphasizes this point when he explains how social protocols are fluid and non-deterministic and technical protocols are deterministic. Yet, the use of the term “protocol” is common to all three exchanges and results in abstraction away from the social.

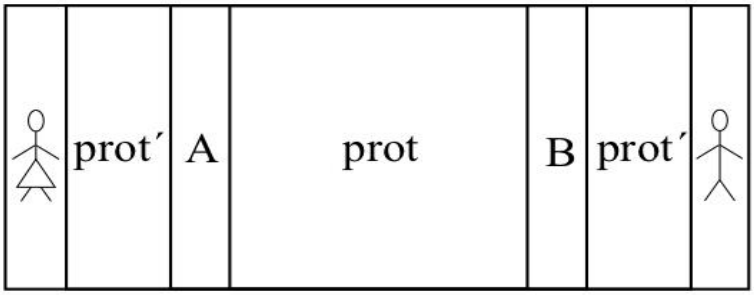

Figure 1 The Current Ceremony Picture

Ceremony literature argues that the concept of “protocol” needs to be extended to include humans in a way that retains rather than reduces human complexity. This need was first documented in Ellison’s 2007 work. The 2009 work by Karlof et al explored the difficulties in making these extensions and the challenges in meeting the needs described by Ellison. The 2011 work by Radke et al identify areas that ceremony analysis must address for it to truly model the human interaction with security technologies., thereby characterizing the needs described by Ellison in 2007.

There is a discernable shift through the literature in terms of the positioning of the analysis of human actions within the overall ceremony analysis. Ellison pioneers that a ceremony must be shown to be secure not only against classical protocol attacks but also against social engineering threats. For example, he draws a clear sequence of interaction steps that would lead the user to unwittingly engage with a spoof website. Ellison acknowledges the need for modelling the human actions and describes the human as a state machine. He acknowledges that the building of such a state machine requires empirical research. Ellison also concludes that modelling human behaviour would need to be probabilistic in nature to account for the variable ways in which

users respond to technology. However, it is noticeable that Ellison refers to the empirical research as if it is outside of, and not a part of, the ceremony analysis. In contrast to this position, Karlof et al undertake empirical research as part of ceremony analysis to establish whether a particular group of participants are susceptible to a phishing attack. The findings of Karlof's work show that humans are not state machines and that even if modelled probabilistically, their behaviour is not easily predictable. Karlof's work shows that users reason in many ways about how they should interact with technology. Radke et al enumerate how ceremony analysis needs to be extended in order to encompass analysis of human interaction with security technologies.

These works qualify as the most notable extensions from protocols into ceremonies, however they do not provide a frame through which unified technology and social analysis can take place. This paper develops this quest by presenting a more complete picture of ceremony analysis. This paper argues that ceremony analysis is in fact the union of human technology practice with an underlying security protocol. We argue that the current ceremony perspective must be widened to include at least patterns of technology practice *in general* and the analysis must be able to identify where the goals of human technical practice are misaligned with the goals of the security protocol; for it is where there is this mismatch that the social engineers of Ellison's paper carry out their exploits.

RUNNING EXAMPLE

Amazon is the world's largest e-shopping site, with its market capitalization having just passed 100 billion (Techchrunch, 2011). Therefore, the motivation to study the users' engagement with it is high. Amazon offers two ceremonies to its users: one for registration and one for purchase (Bella and Coles-Kemp, 2011). As services, they are rather complicated as there are many points at which they can be used. For example, registration can be interleaved with almost any task.

The two ceremonies are analysed in previous work (Bella and Coles-Kemp, 2011) using the HCI cognitive walkthrough method (Wharton et al., 20114) to give an idea of technological practice and compare the outcomes of technological practice analysis with security protocol analysis of the same ceremonies. The analysis resulting from the HCI cognitive walkthroughs showed that registration and purchase services are separate ceremonies and can happen independently of each other. The analysis in Bella and Coles-Kemp's 2011 paper shows that the user continuously faces a registration invitation on each page but if the user defers registration, then they will be compelled to register to finalise the purchase, as the interface illustrated in Figure 2. Analysing the walkthroughs showed that, in terms of security, this separation can result in the Amazon user not realizing the significance of the password and setting a weak one even though it is used to protect the user's credit card number while it is stored with Amazon. The walkthrough analysis also showed that the privacy issues are related to Amazon storing not only the shopping preferences of registered users and thus effectively profiling them, and also through the storing of the preferences of unregistered users by linking click patterns to IP addresses.

Figure 2 Amazon's Checkout Window

The conclusion of Bella and Coles-Kemp's analysis is that the design of services contributes to the context in which users develop security and privacy ceremonies. In order to understand the interaction between technology practice and the goals of the security protocol in contexts such as the one described above, some method has to be found to link the patterns of technical practice with the underlying security protocol so that analysis can take

place on the complete picture without reducing the human complexity. One possible approach to this integrated analysis is outlined in the next section.

A MORE COMPLETE CEREMONY PICTURE

In reality, security ceremonies are far more complex than shown in the current ceremony literature. The work of Whitworth (Whitworth, 2009) points out that the human-computer interface (HCI) surrounds the software running on modern computers which in turn is surrounded by a socio-technical layer which is the societal setting in which the HCI interaction takes place. We use this approach to refine the protocol picture and extend the ceremony as shown in Figure 3. As the ceremony literature shows, there are essentially two perspectives when the human is introduced: viewing the human from the perspective of the technology (the perspective that is typically adopted in security protocol analysis) or viewing the technology from the perspective of the human (the perspective that is typically adopted in technology practice analysis). Figure 3 shows a unified approach that enables analysis from both perspectives and in so doing, enables analysis which links the patterns of technical practice with the underlying security protocol.

It is important to note that even a robust security protocol will not benefit its executors should its goals fail to reach the outermost layer, where the humans are positioned, through the various intermediate layers that are described below. To obtain the full ceremony picture about *two humans* who interact through the ceremony, Figure 3 should be mirrored around the vertical axis, producing a protocol which stretches peer B and back again. If only A is a human and B for example is a web site, then the protocol stretches to Layer II and back again, its outermost peer being a server root process, which is an instance of a computer program running within an operating system – the term process will always be used with this meaning below. In this scenario the human element is absent on B's side, the layers external to II are therefore empty on that side. In the Amazon example, Layer II can be informally thought of as the main Amazon program that responds to customer queries.

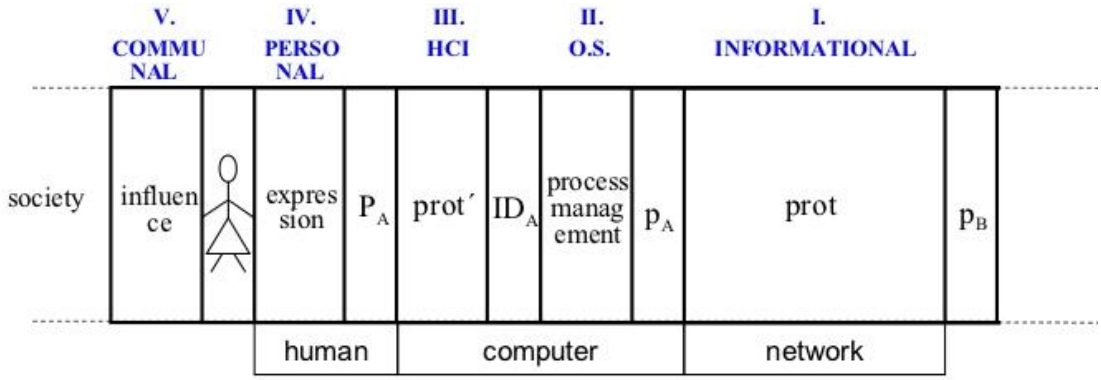

Figure 3 A More Complete Ceremony Picture

Layer I is the *informational layer*, and is where traditional protocol analysis focuses. Its actors are the computer processes running on behalf of the users. Each process is denoted by p indexed with the letter indicating the process owner. This layer hides Layer 0, which indicates the hardware on which the protocols run.

In the Amazon example, Layer I reduces to Secure Socket Layer (SSL), the most widely used security protocol over the Internet. Existing protocol analysis literature shows that it robustly achieves its stated security goals. However, this as such does not imply that its goals will reach the Internet users, as demonstrated with the Amazon example (Bella and Coles-Kemp, 2011).

Layer II is the *operating system layer*, which manages the computer processes that run on behalf of a user. This layer is where malware attacks might come, for example. This layer hosts the inter-process communication between a root process, denoted by *ID* indexed with the letter indicating the process owner, and running on behalf of a user, and the child process that executes the security protocol.

In the Amazon example, Layer II consists of the customer's operating system and of Amazon's commercial system. The former is often notoriously vulnerable because of insufficient or outdated maintenance. The latter is a hardened software system that may possibly run in the cloud. While extra details on the actual architecture lie

beyond our focus, our layering captures the essence of a complex computer program that, with the Amazon example, manages various registration/purchase requests, each by means of a computer process.

Layer III is the *human-computer interface layer*. It contains interfaces that need to communicate the service's security goals in an accessible manner; otherwise, users derive a false sense of security that is not supported by the underlying technology. For example, Radke et al pointed out an interface limitation of the OperaMini system for the smartphone, where the user erroneously believes that nobody intercepts their traffic with a server when in fact a third party acts as a proxy, receiving traffic from one peer and sending it to the other, and vice versa (Radke et al, 2011).

This layer therefore sees user personas interacting with a root process through a graphical interface. This is easy to envisage in the traditional "Alice and Bob" setting, where the ends of the communication indeed are humans. In contrast, in the Amazon example, as noted above, Layer III is empty on Amazon's side, while it faithfully features the customer's persona on the other side.

Layer IV is the *personal layer*. While they interact with technology, users may have different behaviours with different services. For example, users who are cautious when they interact with their on-line bank may exhibit a very relaxed persona while they participate in a social network. Also, a user cannot be assumed to always exhibit the same behaviours with the same peer over time.

There are various examples of user behaviour patterns. For example, the *click-whirr* user, who learns by heart the sequence of steps to reach his goal once, and then repeats them mechanically every time he seeks the same goal (Karloff et al., 2009). While this appears to save some of the user's effort, it is risky because the working context may have changed, such as with an updated webmail interface following a system upgrade. The *rushing user* is a persona that embodies both the previous ones with additional elements of non-determinism resulting from variable constraints on a user's ability to engage with the interface.

Studying the various combinations of layers III and IV is challenging and important. For example, a cautious and skilled persona may make up for the deficiencies of a poor interface. Arguably, a network administrator will choose a strong password to access his bank account, while the general public needs an appropriate interface to guide them to do so. However, we advocate ceremonies to be secure for all of their users.

In the Amazon example, Layer IV pictures the Amazon customer on one side, while it is empty on the other side. The walkthrough analysis is used to identify these different behaviour patterns and analyse how they form different patterns of technological practice.

Layer V is the *communal layer*, which represents the diverse influence of society on the human user. Influence may come from people, from publicity, etc. For example, the communal layer plays an important role for humans who engage with a mass-phenomenon such as Amazon. A human can therefore be seen as the end point of the ceremonies they engage with – each time via a potentially different persona. Humans are influenced through society, and as well as through the internal influences through the ceremonies they execute. Layers III through to V can be seen as our specification of Whitworth's external, socio-technical layer.

Analysing and Verifying the Layers

There are many ways in which the layers could be analysed and verified. Potentially, hierarchical verification approaches found in hardware analysis (Gordon, 1986) could be used. In this approach, firstly the functionality of a device is specified as a black box; secondly, the device is opened and the interaction of its internal devices is specified too; finally, the two specifications are showed to provide the same result. Using the layered model described in the previous section, we could apply this to the more complex case of ceremony analysis, thus:

- a specification at Layer I should handle *cryptographic messages* between processes;
- a specification at Layer II should handle *inter-process communication data* between root processes;
- a specification at Layer III should handle *signals* between personas;
- a specification at Layer IV should handle *expressions* between humans;
- a specification at Layer V should handle *influences* between society and humans.

In this categorization the appropriate analytical tools could be used for each kind of exchange.

An alternative approach could be to analyse the ceremony “end to end” from the perspective of the user. For example, such an end-to-end analysis of the full Amazon picture would require a specification of the customer behaviour patterns, analysis of the societal context in which those patterns are exhibited, then of the senses of security and privacy that the human-computer interface transmits, through to the operating system's management of its processes, down to the security goals derived from a cryptographic protocol.

DISCUSSION – ADVOCATING THE USE OF FORMAL METHODS IN CEREMONY ANALYSIS

Many security analysts advocate the use of formal methods to tackle the ceremony picture and yet, as analysis in the previous sections shows, this is challenging because of the different interpretations of security at each layer.

Formal methods provide a means of abstracting the ceremony whilst preserving the diversity of the context and the influence of the belief systems and cultural values. For example, by taking an approach of an inductive nature to the analysis, it becomes possible to articulate many such contexts and promote the consideration of how the influences of different perceptions and values result in different behaviours. The inductive approach provides a powerful means of expressing a range of worlds with different norms and memes.

Formal methods could help in evaluating the technologies in terms of the technical practice, namely they help to produce a baseline of expected behaviour and a means of predicting whether a given technology will result in a particular ceremony. It does not matter whether the prediction is 100% accurate. Rather, it is the approach of looking at a range of possible worlds, regardless of their likelihood, that enables a wider range of security responses and makes the technology deployment more effective. This is an extension of the probabilistic modeling approach put forward by Ellison in the 2007 paper.

Furthermore, formal methods used in this way enable a modelling approach that provides a picture of the social and technical protocols at the same time. It can be argued that the articulation of personas on-line is at once both a social and technical protocol and this approach allows the analyst to look at this fuller picture removing the distinction between "in-band" and "out-of-band".

It finally becomes clear that a full security analysis of a ceremony should account for threats arising at each of the layers seen above, from the informational to the communal. This appears to require significant extensions to the current formal analysis approaches, which are mostly limited to the informational layer only.

CONCLUSION

As the ceremony literature shows, there are essentially two perspectives when the human is introduced: viewing the human from the perspective of the technology (the perspective that is typically adopted in security protocol analysis) or viewing the technology from the perspective of the human (the perspective that is typically adopted in technology practice analysis). Current ceremony literature acknowledges technology practice but does not present the tools to develop that perspective. This paper has proposed a model for integrated technical and technology practice analysis and exemplified its use using the Amazon service and consideration as to how such a model may be evaluated. The paper concludes with considerations as to how formal methods may be used in this integrated analysis approach.

ACKNOWLEDGEMENTS

This work was supported by the Technology Strategy Board; the Engineering and Physical Sciences Research Council and the Economic and Social Research Council [grant number EP/G00255/X].

REFERENCES

Abadi, M. and Needham, R. M. (1996). Prudent engineering practice for cryptographic protocols. IEEE Transactions on Software Engineering, 22(1) 6–15

Armando, A. Carbone, R., Cuellar, J., Tobarra, L. and Compagna, L. (2008). Formal analysis of saml 2.0 web browser single sign-on: Breaking the saml-based single sign-on for google apps. Proceedings of FMSE 2008. ACM Press.

Bella G. and Coles-Kemp, L. (2011). Internet users' security and privacy while they interact with amazon, in Proc. of IEEE International Workshop on Trust and Identity in Mobile Internet, Computing and Communications (TrustID'11). IEEE Press

Coles-Kemp, L. and Kani-Zabihi, E. (2010). On-line privacy and consent: A dialogue, not a monologue, in Proc. of the New Security Paradigms Workshop (NSPW'10). ACM Press.

Ellison, C. (2007). Ceremony design and analysis, Technical report, Cryptology ePrint Archive, Report 2007/739

Galloway, A. (2004). Protocol — How Control Exists After Decentralisation. MIT Press

Gollmann, D. (1996).What do we mean by entity authentication? In Proc. Of the 15th IEEE Symposium on Security and Privacy (SSP'96), pages 46–54. IEEE Press

Gordon, M.J.C. (1986). Why High-Order Logic Is a Good Formalism for Specifying and Verifying Hardware?, Formal Aspects of VLSI Design: Proc. 1985 Edinburgh Conf. VLSI, G.J. Milne and P.A. Subrahmanyam, eds., North-Holland Publishing, Amsterdam, 153-177.

Gunawardena, D., Scott, J., Zugenmaier, A. and Donnelly, A. (2007),.Countering automated exploits with system security captchas, in B. Christianson, B. Crispo, J. Malcolm, and M. Roe, editors, Proc. of the 18th InternationalWorkshop on Security Protocols (IWSP'10), LNCS 4631, Springer,162–169

Karlof,C., Tygar, J. D. and Wagner, D. (2009). Conditioned-safe ceremonies and a user study of an application to web authentication, in Proc. of the 16th Network and Distributed System Security Symposium (NDSS'09)

Martina, .J. E.. de Souza, T. C. S. and Custdio, R. F. (2009). Ceremonies design for PKIs hardware security modules, in Proc. of the 9th Brazilian Symposium on Information and Computer System Security (NDSS'09), SBC Press, 115–128

Radke, K., Boyd, C., Nieto, J. G. and Brereton, M. (2011). Ceremony analysis: Strengths and weaknesses, in Proc. of the 26th IFIP International Information Security Conference (IFIP SEC'11), LNCS. Springer

Ryan, P. Y. A., Schneider, ., S., Goldsmith, M., Lowe, G. and Roscoe, A. W. (2001). Modelling and Analysis of Security Protocols. Addison-Wesley

URL. Amazon's market cap passes $100 billion. http://techcrunch.com/2011/07/27/amazons-market-cap-passes-100-billion, last accessed September 2011

Wharton, C., Rieman, J., Lewis, C. and Polson, P. (1994). The cognitive walkthrough method: a practitioner's guide, John Wiley & Sons, Inc.,New York, NY, USA, 105–140.

Whitworth, B. (2009). Socio-technical Design and Social Networking Systems, chapter The Social Requirements of Technical Systems, IGI Global, 3–22.

Wikipedia (2011). http://en.wikipedia.org/wiki/Process_(computing) last accessed November 2011