Ceremonies Formal Analysis in PKI's Context

Jean Everson Martina
University of Cambridge
Computer Laboratory
15 JJ Thomson Avenue
Cambridge – United Kingdom
Email: Jean.Martina@cl.cam.ac.uk

Túlio Cícero Salvaro de Souza, Ricardo Felipe Custódio
Laboratório de Segurança em Computação
Universidade Federal de Santa Catarina
Caixa Postal 476 – 88040-900
Florianópolis – SC – Brasil
Email: {salvaro,custodio}@inf.ufsc.br

***Abstract*—Ceremonies are a useful tool to establish trust in scenarios where protocols operate. They describe a greater range of issues not taken into account by protocol designers. We take an already-designed protocol and ceremony for a key management protocol operating in a Public-Key Infrastructure environment and test it using a formal method. The ceremonies were analysed to test human peers' cognition pitfalls using formal methods. The analysis came up with a potential cognitive slip in one early design. This directly affects trust in the protocol.**

***Keywords*-Key Management Protocols, Ceremony Design, Ceremony Analysis**

I. Introduction

Despite being important to safe protocol operation, ceremonies are not often seen in research. Recently, ceremony design and analysis were introduced by Ellison [1], [2]. He states: "ceremonies extends the concept of protocols by including human beings as nodes in the network", this can be extended even further to the environment and the relations between subjects and security targets, dealing directly with their capacity for trust establishment. This kind of description gives a broader coverage of *out of bounds* operations which arise from day-by-day protocol usage. We also note that human peers are often mentioned in protocol designs, since a protocol is commonly defined as a system of rules used during a ceremony, but normally their expected behaviour is not tested against the protocols' goals. We adopt the idea of ceremonies as extensions of protocols, taking into account environmental variables and by extension human peers.

Ellison establishes the basis on ceremony description. He describes the important *out of bounds* operations that we should consider in ceremony analysis. Although he states the possibility of using formal methods available for security protocol analysis, no major work is found today. This lead to empirical analysis, which proved to be hard and error-prone. Our idea is to use Ellison's approach and to survey in the, until now untouched, area of formal ceremony verification.

Jean Everson Martina is supported by the CAPES Foundation/Brazil on grant #4226-05-4

Taking Ellison's ideas on security ceremonies requires a vast amount of things to be covered to declare a ceremony secure and trusted. One reasonable approach is breaking the problem into small parts and try to verify them separately. By dividing the approach we can find two different classes of problems to deal with when analysing ceremonies: The first regards humans peers interaction/expectation and the second regards environmental conditions which the ceremony is subject to. The problem regarding human peers - choice of the current work - can be understood as how adapted the protocol is to cope with limitations of humans behind the computer screens. Especially how this affects the security and trust in a systematic manner. The second class is broader, and can include almost anything that is not included in the ceremony as a protocol or a human peer. Furthermore, the representation and verification of environmental conditions in ceremonies, and, by extension, protocols, can be a key to understand better problems on protocols' composability, making them trustworthy.

The work of Rukšėnas et al. [3], [4] can answer part of the first class of problems. They developed a human error cognitive model, which was applied to interaction with interfaces. This model can be directly applied to a human-protocol interface. Furthermore, taking recent Rukšėnas et al. [3] extensions, cognitive slips can be easily verified in protocols in the presence of attackers. Their model supports a description of any human peer in protocols, taking its point of view, describing its interpretation, the effects it can cause in security and it's impressions on the protocol run (trust). Another important feature of Rukšėnas et al. is the support of environmental descriptions. Although not yet developed, it shows potential to model the second class of interactions. Rukšėnas et al. does not formalise the environment due to its complexity, but leaves an input to add it later.

An approach to embrace Rukšėnas et al. method and use it in ceremonies is by applying it using Bella's [5] goal availability ideas. By this principle, we must take into account each peers point of view and work towards guarantees available to each human peer. The approach requires that the guarantees must be checkable only by what is visible to the peer during its participation. This correlates

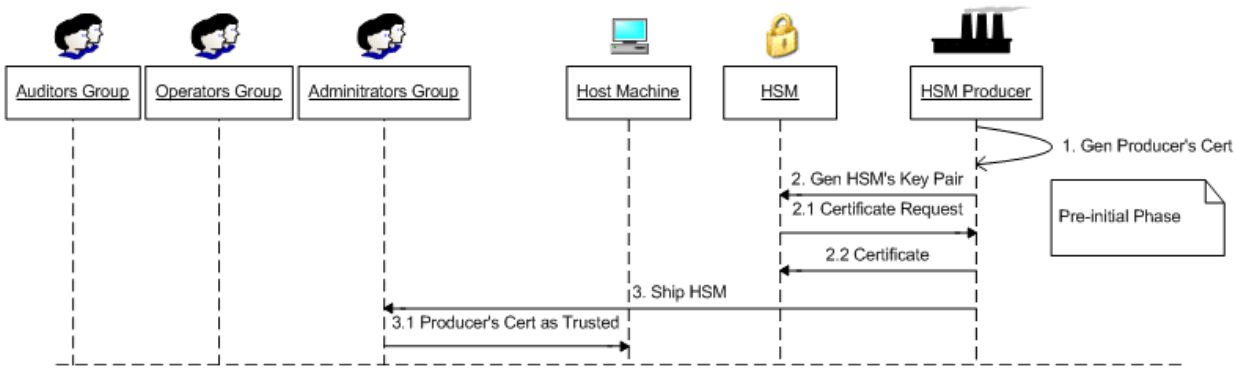

Figure 1. Ceremony to initialise the OpenHSM - Pre-initial Phase

with the human idea of trust, where we build up trust over facts that can be verified.

This work shows concepts of ceremonies and related work stressing the importance of this area. Section III shows a formal analysis method applied to verify cognitive slips of human peers on one of the security ceremonies introduced in Section II. It combined a series of approaches to achieve this goal. Finally Section IV discusses the outcomes of ceremony analysis. Some future research is proposed.

II. HSM Ceremonies

Martina and Salvaro [6], [7] proposed the creation of an open HSM software architecture called OpenHSM, where key life cycle can be controlled under a generic environment. The next challenge is to establish basic ceremonies to the OpenHSM. This should be done to address environmental and procedural threats in the proposed protocols.

The OpenHSM is an environment where PKI keys can be created and managed. It includes protocols to create keys based on threshold cryptography and heavy auditing. Thus, keys' consequent usage can be controlled. The focus will be in the narrative regarding the ceremony description in a system that will enable to create witnessed ceremonies. All ceremony processes will finish with a written act which will help to describe the key life cycle. The creation of such records is seen as part of the environmental procedures needed to establish trust in the HSM, and to satisfy human peer expectations on controlled and audited execution.

In PKI ceremonies the presence of auditors is mandatory and often mentioned in standards [8]. Works in Management and Governance shows the importance of auditing and tracking. Spira [9] states that the importance of auditing and ceremony in corporate governance standards is because they validate the legitimacy of operations and enable access to the history of procedures. It can also detect the roots of problems, thus making the governance standards higher. We should also mention that such PKI related ceremonies must be already documented somewhere by the big companies that operate in the Digital Certification market, but due to industrial and security concerns - such as the lack of correctness analysis tools - they remain secret. This work should not be compared with those ceremonies, but seen as an open proposal to drawn attention to its importance. Other work that corroborates the usage of witnesses was recently published by Brainard [10], where he emphasises the importance of people's relations to give security to authentication processes and the threats that can be avoided when other parties are involved in a collaborative security process.

The initialisation ceremony is an important step towards a secure HSM. A ceremony starts even before an HSM is bought, when it is still under production, since that to included an HSM in the any process it should come from a trusted source and in a trusted, or at least verifiable, path.

Ceremonies are used to establish trust anchors allowing actions to be traced to something that is trusted. The difference between protocols and ceremonies is that the trusted assumptions are generally weaker in ceremonies if compared to protocols. Thus, without evidence that the process was strictly followed, there is no basis for trusting a ceremony. Also, a design that is not secure against human inherent problems can be subject to vulnerabilities. The initialisation ceremony starts with a Pre-initial Phase as illustrated in Figure 1. In this phase it is proposed that the HSM's producer issue its own certificate (Step 1) that will be used as its identity and to sign HSM's certificate and software.

As part of the fabrication process, the producer requests the generation of the HSM's internal key pair during its first run (Step 2). Thus, the HSM issues a certificate request and returns it to the HSM's producer (Step 2.1). Using the HSM's serial number which is unique and is marked on the HSM's chassis, the producer issues the HSM's certificate. The producer and HSM's certificates are uploaded to the HSM (Step 2.2). The OpenHSM software is also signed and included in the HSM shipment (Step 3). Therefore, the HSM certificate and the software signature will guarantee the origin of the HSM and will be anchored to the HSM's producer certificate. The last step of this phase consists in the recipient of the HSM to trust the producer's certificate.

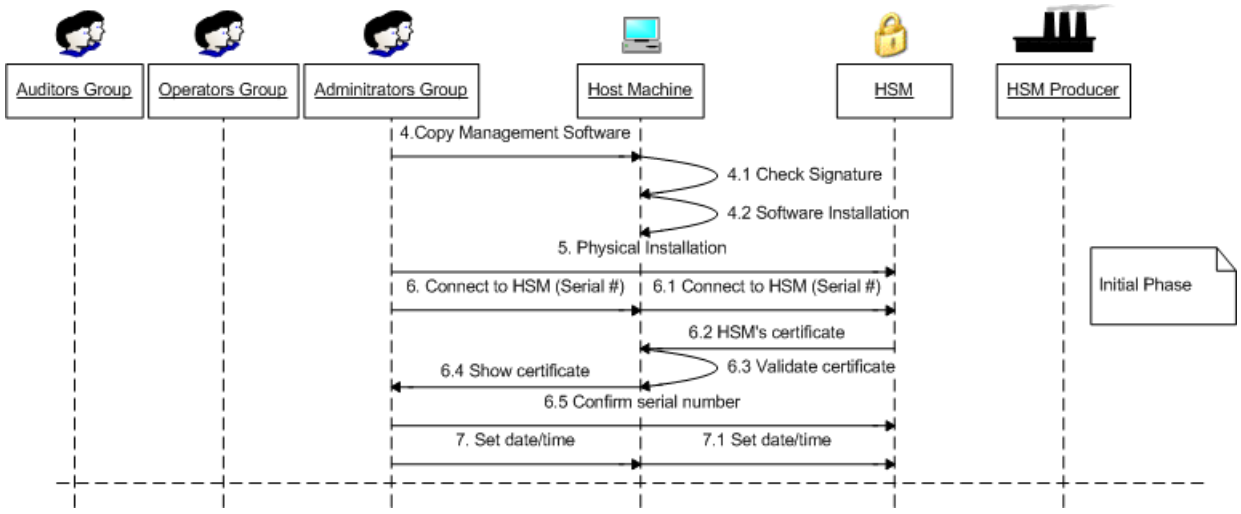

Figure 2. Ceremony to initialise the OpenHSM - Initial Phase

To do this, the recipient copies the producer's certificate, verifies and installs it into the host machine. After this, the host machine can verify the integrity of the HSM's software and communications channels.

The producer certificate will be distributed to its clients, assuring the virtual anchor already existent in the real world: The customer must trust the HSM producer, since that without this trust it can be assumed that the HSM is compromised by default. The transfer of this certificate to the HSM user will happen in a human-to-human data channel in a form that gives enough confidence to the other human counterpart. This channel will be considered a high security channel under the Rukšėnas et al. model, and therefore, out of scope of the human cognition verification. This is justifiable because it embeds much more than cognitive issues from the human peer.

It is difficult to establish what is a good human-to-human channel. Some humans require face to face contact with a company representative, receiving the digital version of the certificate together with a signed letter containing the certificate digest, while for others, just receiving the letter by post in a signed-for letter could be enough to give the required assurance. This analysis is beyond from what is achievable today with the current method.

The producer is now able to create a Cryptographic Identity for the HSM, binding it physically. He ties the logical contents of the HSM with its physical instance, using the protections in the security perimeter of the HSM to avoid tampering in this process. An important objective achieved by this Pre-initial Phase is to reduce the strong assumption that the HSM is not compromised before it arrives in the destination. It is reduced to the security of the human-to-human interaction that exist with the HSM producer. The steps that are in between can be reproduced and checked to give confidence. Additionally, errors and misconduct can be easily detected by an auditing process. No cognitive issues were taken into account so far because the first and only human-to-human channel exceeds the verification capacity of the method by including more than just cognitive issues.

The second phase starts with the HSM and software installation, shown in Figure 2. In this phase, management software is uploaded to the host machine (Step 4). Before installing software, the installation procedure verifies the signature of the management software (Step 4) validating its signature and certificate (Step 4.1). If the signature is verified then the management software is installed (Step 4.2).

With the software installed, HSM's physical installation can be proceed (Step 5). From this point on, we establish the first connection to the HSM. The administrators group request the Host Machine to connect to the HSM (Step 6) and the Host Machine forwards this request to the HSM (Step 6.1). As the HSM is being connected by the first time - even if the HSM has already been used it can reach this state[6] - the connection uses an encrypted channel, through which, the HSM will send its certificate to the Host Machine (Step 6.2). The Host Machine will then check the certificate's validity, using the previously trusted producer's certificate (Step 6.3), and upon validation, the certificate will not be shown to the user (Step 6.4). The user enters the HSM serial number marked on the HSM chassis (Step 6.5). If the number entered by the user - the user does not have access to the content of the HSM certificate before - is equal to the value in the certificate extension, the HSM sends a message to the computer, that it will forward the user, stating that the firmware in the HSM is original, was created by the expected producer and that it is the expected HSM (Confirms the HSM identity).

Once this phase is run, the user can be prevented to use a tampered or unexpected HSM. By blindly asking the user for information and letting the system deal with the

comparison we solve a possible human peer's weakness point. After being assured that they are connected to the right and trusted equipment, the Administrators Group must set the date and time in the Host Machine (Step 7), which will then synchronise its clock with the HSM's (Step 7.1). This step is important to guarantee further auditing steps, since clock de-synchronisation can lead to severe problems in auditing processes.

III. Ceremony Analysis Strategies

Inclusion of human interaction, behaviour and cognitive processes, is a characteristic of ceremonies as human peers are out of bounds for protocol verification. They are the most error prone peers in any process, and their inclusion can enrich in details any analysis done so far. Inclusion of this can lead us to understand how and why correctly implemented and deeply verified protocols still fail for some set of users. This approach has never been tried due to the intrinsic complexity of human cognition and behaviour, and also because of the lack of a formal model for such properties.

Ellison's idea [1], [2] give a broader coverage of the protocols' point of view, extending what can be verified by protocol techniques. He establishes the basis at 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 leads to empirical analysis, which can be difficult and error-prone, as protocol analysis history shows.

Formally analysing ceremonies is a difficult task. It should include all interactions with the protocols working within the HSM and cover the points of interaction between equipment and environment and equipment and human peers. Due to the intrinsic difficulty of analysing ceremonies it was opted for dividing interactions in two classes: those environmental, and those regarded to human behaviour. A good method should be able to represent such distinction and also to be able to tackle one at a time.

Ellison focuses on describing ceremonies as a sequence of steps that demonstrate the existence or not of attacks. Although concise and straightforward, sequential description is not ideal when it is tried using a formal method or a formal tool. It captures the problem but does not allow for properties to be checked precisely. The dualism of right and wrong ceremony scripts creates problems too. When choosing a scope and a formal tool to verify ceremonies, we realised that the translations of ceremonies to a state diagram was a good approach because it is possible to use a range of verification tools such as model checkers. We opted to represent ceremonies in the correctness perspective, using violations in this model to detect problems.

An important advance that enables one to start reasoning about a fraction of ceremony problems was introduced by Rukšėnas et al. [3], [4]. They developed a human-error cognitive model applied to interaction on interfaces. They showed that confidentiality leaks come from mistakenly modelling interfaces, not taking into account the cognitive processes of human beings behind the computer screen. Rukšėnas et al. successfully verified problems on cash-point interfaces, also showing the normal lack of consideration in the weakest link: the human peers. The modelling comes with an implementation using a model-checker to state verification. This makes the approach appropriate to integrate with the actual protocol verification ones.

Rukšėnas et al. support environmental descriptions. Although not yet formalised, their approach shows potential to model the first class of interactions as well. They do not formalise the environment due to its complexity, but leave an input to add it later. It will be for now focused in the human peers interaction within the OpenHSM ceremonies. It is not planned to set a definite answer on ceremonies verification, but we start taking out empirical test and start in an automated and formal fashion. The model also supports the inclusion of active or passive attackers. The passive attacker describes an attacker just observing the human peer execution and trying to extract information in the form of confidentiality leaks. The active attacker can participate together with the human peer, trying to introduce traps or to distract the user deliberately causing a security fault.

Taking Bella's goal availability approach [5] where guarantees should be present in each peers' point of view, we decided to produce independent verification models for each human peer. Every human peer will have its mental and physical actions, pre-determined goals, reactive behaviour, salience, voluntary task completion and forced task completion attributes. This human peer will *interact* with the protocol taking his point of view from execution. The attacker has been modelled using the same cognitive infrastructure as the users.

Using Ellison's adapted description allied to Rukšėnas verification method and in the perspective of Bella's remarks, the description of how to address the verification of cognitive issues in ceremonies is addressed. This is done by analysing what was proposed in Section II. Due to the hyper-exponential detailing carried out in the ceremony cognitive verification process, we will describe the approach applied to the Initial Phase of the first ceremony in Figure 2. Even though we already carried out the experiments in other phases, this stretch shows the richest example in terms of cognitive pitfalls.

A. Proposed Method

By Ellison's modelling, every computer connected to the network has a human relying on the execution of protocols. Assuming that humans do not explicitly send messages in a protocol run, they actually interact with the computer using an interface.

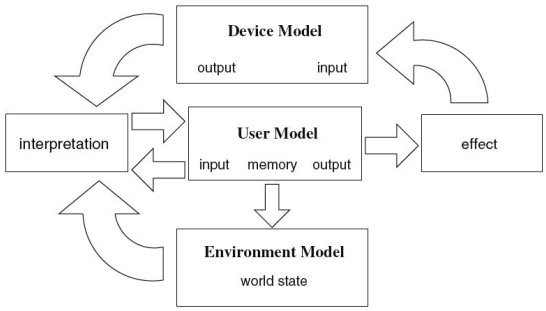

Figure 3. Interaction model by Rukšėnas et al.[8]

Rukšėnas' verification method describes a dynamic interaction as shown in Figure 3. It is easy to understand the choice on modelling a device and to try to map user interpretation and effect inside an environment, since the main goal was verifying the usability. Within this structure we can easily distinguish between user perception (input signal to the human peer), consequences of user's actions (output signals) and the user's internal state (in this case his memory). The cognitive architecture built is a higher-order formalisation of plausible cognitive behaviour. This tries to map standard user behaviour but it is unable to detect those who act outside the cognitive standard. It can be targeted to find general pitfalls in ceremonies.

In terms of user modelling, the user description enables the creation of users with different capabilities, enabling us to specify an attacker. The different characteristics represented in the standard user model that can be instantiated are:

- Non-determinism of user actions;
- The difference between mental and physical actions;
- Pre-determined goals;
- Reactive behaviour;
- Salience;
- Voluntary task completion;
- Forced task completion.

This proposal will make usage of just 4 of the 7 different user parameters. As the interest in this first stage is identifying user bypass of security measures, it will be just focused on the parameters of pre-determined goals, reactive behaviour, salience, and force task completion. The pre-determined goal parameter enables to test achievability of commitments made by the user when starting the ceremony. Reactive behaviour shows how the user can react to an attacker action and test the safety of his commitments. Salience enables to work over the user knowledge of task enabling to test things that appear due to lack of knowledge in the purpose of his actions. Forced task completion tries to map where the user can be forced by the attacker to leave the ceremony process with complete or incomplete goals.

It is proposed to build of one device model for each human peer point of view, making use of Bella's ideas, where the guarantees should be present to each peer. If it cannot be verified that the ceremony is safe for all users then it is considered unsafe. The approach also keep protocols as black boxes, thus analysed separately, and enables the testing of user interpretation of protocol messages, as well as possible inputs and outputs the user can create in the scope of the ceremony.

Each human peer is modelled following their cognitive aptitudes in the presence of an attacker. This gives insights into which pitfalls the user is more likely to fall. By tuning human peer attributes it will be possible in the future to grade protocols and ceremonies representing the possibility of attacks depending on user experience and pre-determined goals. This will give a better tool to design and test protocols against scenarios and user specifications.

As Rukšėnas et al. do not explore the environment model, we opt for tackling just the user model for the ceremonies. It must be emphasised that environment modelling can be a key issue to understand protocol composability, but is not a main issue in the OpenHSM case. This makes the approach appealing.

B. Implementation

The implementation was done in three steps. The first was changing the representation of the ceremonies. It was converted from a sequential description to a state description. As shown in Figure 4, part of the first ceremony - Initial Phase - was described on term of the point of view of the lead administrator within the OpenHSM architecture. This ceremony phase was chosen as the first target of evaluation because its success is crucial to the OpenHSM since it is not protected yet by the auditing scheme. Figure 4 shows what the leading administrator can achieve in the ceremony. It starts at the initial state, then it has the transition copy software. In this transition the leading administrator gives the control over the execution to the Host Machine, which before the installation proceeds will verify the software signature. At this point, we captured part of the decision tree in the ceremony, where the Host Machine will reset the state machine in case of failure or will proceed to the state *Software Installed*. Control of the ceremony goes back to the human peer, which will receive the appropriate perceivable message. The human peer will then fire the *execute Mgmt SW* transition and go to *Mgmt Software Running* state. The human peer will then request a connection to a specific HSM calling the transition *Connect to HSM*, passing the serial number engraved in the HSM as a parameter. The control will go to the *Management software*, which proceeds to connect to the available HSM and retrieve its X509 certificate. It comes to a decision point where the state machine will be reset in case of failure verifying the serial number extension match with the informed by the user, otherwise it will move to state *X.509 Accepted* showing

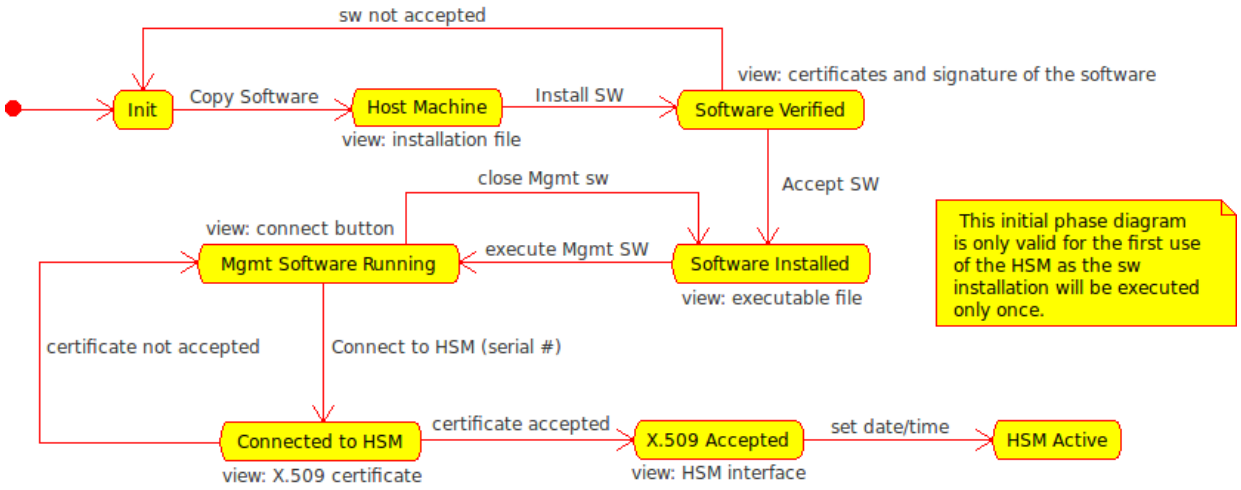

Figure 4. Translation from Ellison's Sequence Diagram to State Diagram taking the lead Administrator point of view

the certificate to the user. After this point, when the lead administrator sets the date and time in the HSM, the final stage is reached, *HSM Active*.

The second step was the translation of the above state machine to the SAL Model-checker implementation. This is straight forward, since we create the state machine composed of all the states and transition described in Figure 4. This comes to Rukšėnas et al. model as the device implementation. Next we instantiated the user model, where we took into account the settings described in Section III-A. We created the lead administrator model and an active attacker with a simple state machine attached to it: two states (Waiting for attack, and Attack succeeded) and a single transition (Switch HSM). After that, the Interactive system was created.

The third step was the interactive testing using the model. SAL model-checker has its own nuances and some of the key properties are proved using different binaries, making the process a bit painful. The outcome of these experiments is described in part on Section III-C.

Figure 5 represents the ceremony using Ellison's description before testing it using the formal model, and Figure 2 represents the corrected version of the ceremony. The difference between both sequence diagrams is the parameter in the firing of Connect to HSM transition, taking the serial number.

C. Results

In a first version of initial phase ceremony, few problems happened during the verification of safety properties, as well as in the attempt of proving that the ceremony was safe in the presence of an active attacker. The property regarding user perception of using the right HSM was not satisfied in the presence of an attacker that could deliberately switch the correct HSM by a rogue one. So the following assertion is defined:

```
IntruderGoal = λ( in, mem, env):
env.switchHSM ≥ 1 ∧ rightHSMCommitment =
λ( in, mem, env): TRUE
```

The assertion states that the intruder has a goal of switching the HSM by a rogue one he controls, and due to the lack of a specific binding between the serial number of the HSM and its certificate, and the fact that this check was performed by the user in an out-of-band human-only fashion, led to the possibility of the user being fooled by the attacker into believe his received a non tampered HSM from the Producer.

Although not very likely to happen, the attacker can get another HSM and switch its identification number tag, making the administrators initialise the wrong HSM. By doing this he creates a Denial-of-Service-like attack, since he may be able to leave the ceremony environment with the now initialised ceremony HSM once he removes the fake identification tag number.

With the correction introduced in the ceremony in Figure 5, a check on serial number consistency is done by the device in co-operation with the user in the ceremony, and it is possible to prove that the intruder cannot foul the user in switching the HSM, since the system will do the comparison in order to proceed.

An interesting outcome from this formalisation process was that it clearly obligates the user to do the checking in every connection. As stated before, the user should not be forced into a specific kind of action, but in this case, it seemed the right choice to avoid a cognitive problem of post-completion error. A post-completion error here is characterised by the cognitive slip that happens when completing the desired goal (connect to the HSM) and forgetting to accomplish an intermediary goal (check on the serial number).

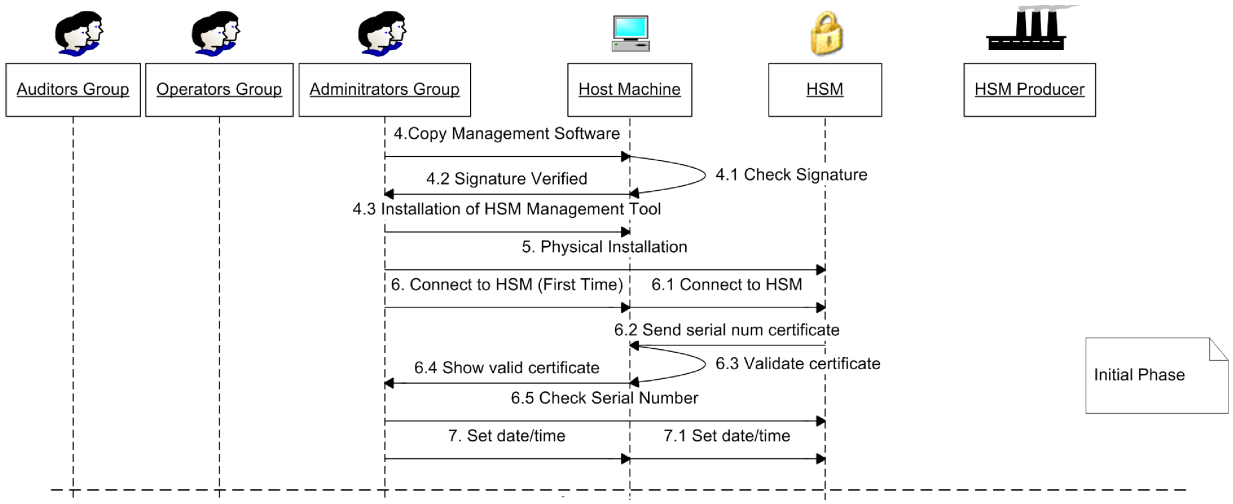

Figure 5. First version of ceremony OpenHSM - Initial Phase

IV. Final Considerations

Recent work on the area of ceremonies was taken into account and applied to the OpenHSM protocols. The ceremony set was stated to give assurance and guarantees in the usage of the module. It was tried to describe the ceremonies by sketching real scenarios where the OpenHSM would be introduced.

During the process of ceremony design, an open problem was faced regarding to the verification of ceremonies. It was aimed to scope the cognitive verification of human peers slips that could lead them into security pitfalls.

A new description to ceremonies was introduced using states instead of sequences, thus enabling the usage of modern formal tools to help in the verification of goals for ceremonies more specifically to test human peer cognitive slips. It was possible to verify a very subtle attack that could be corrected at user interaction level.

As future work, in the ceremony design area, it is being proposed to expand such ceremonies to cover all HSM operations, and to extend to a complete Certification Authority operation. In the ceremony verification area, it is being proposed to extend which characteristics can be verified in human peers, as well as introduce environmental constrains to enrich the ceremony design/analysis process.

Acknowledgments

We would like to acknowledge Giampaolo Bella for discussions about goal availability, Paul Curzon and Rimvydas Rukšėnas for explaining their method to us and Nik Sultana for proof-reading the final version of this paper.

References

[1] C. Ellison, "Ceremony design and analysis," Cryptology ePrint Archive, Report 2007/399, 2007, http://eprint.iacr.org/.

[2] ——, "Improvements on conventional pki wisdom," in *Proceedings of the First Annual PKI Research Workshop*, Gaithersburg, MD, April 2002.

[3] R. Ruksenas, P. Curzon, and A. Blandford, "Modelling and analysing cognitive causes of security breaches," *Innovations in Systems and Software Engineering*, vol. 4, no. 2, pp. 143–160, June 2008.

[4] ——, "Detecting cognitive causes of confidentiality leaks," in *First International Workshop on Formal Methods for Interactive Systems*, ser. ENTCS, vol. 183, 2007, pp. 21–38.

[5] G. Bella, *Formal Correctness of Security Protocols*, ser. Information Security and Cryptography. Springer Verlag, 2007, vol. XX.

[6] J. E. Martina, T. C. S. de Souza, and R. F. Custódio, "Openhsm: An open key life cycle protocol for public key infrastructures hardware security modules." in *Fourth European PKI Workshop: Theory and Practice*, ser. LNCS, vol. 4582. Springer-Verlag, 2007, pp. 220–235.

[7] T. C. S. de Souza, J. E. Martina, and R. F. Custódio, "Audit and backup procedures for hardware security modules," in *Proceedings of the 7th Symposium on Identity and Trust on the Internet*. New York, NY: ACM, 2008.

[8] S. Chokhani, W. Ford, R. Sabett, C. Merrill, and S. Wu, "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework," RFC 3647 (Informational), Nov. 2003. [Online]. Available: http://www.ietf.org/rfc/rfc3647.txt

[9] L. F. Spira, "Ceremonies of governance: Perspectives on the role of the audit committee," *Journal of Management and Governance*, vol. 3, pp. 231–260(30), 1999.

[10] J. Brainard, A. Juels, R. L. Rivest, M. Szydlo, and M. Yung, "Fourth-factor authentication: somebody you know," in *Proceedings of the 13th Conference on Computer and Communications security*. New York, NY: ACM, 2006, pp. 168–178.