Six Characters in Search of a Security Problem: Pirandellian Masks for Security Ceremonies

Taciane Martimiano[1], **Jean Everson Martina**[1]

[1]Universidade Federal de Santa Catarina (UFSC) – Florianópolis – Brazil

Abstract. *For the Italian play-writer and 1934 Nobel-Prize winner Luigi Pirandello, a fictional mask is either self-imposed or, in most cases, forced on by society, being what makes life possible. Drawing from that, we believe that due to the non-deterministic nature of the human being, the only way to specify and verify human-tailored security protocols (known as security ceremonies) is by the specification of masks that users wear in order to interact with ceremonies. In the current paper, we review further this literary inspiration and propose six possible masks: the Attentive, the Naive, the Careless, the Fearful, the Busy, and the Elder. We then discuss an example of how we can reason about security involving human beings, and present what still needs to be done.*

1. Introduction

Nowadays, one of the problems of the security community is that even massively deployed protocols which are proved secure by automated protocol analysis tools still fail [Bella et al. 2015]. Most of these failures are related to assumptions taken by the protocol designer that are not fulfilled when the protocol is implemented (for instance, errors occurred due to unexpected user behaviour). Such problems call for a new approach that better describes protocol assumptions by taking the human role into account. We then see the appearance of the socio-technical area of security ceremonies [Martina and Carlos 2010].

Security ceremonies are defined as a sequence of interactions among entities, designed to achieve a given security goal (such as entity authentication, key distribution, secrecy, etc). The distinction between ceremonies and protocols, as described in [Ellison 2007], is that ceremonies are a super-set of protocols. Ceremonies can include as explicit interactions all assumptions considered out-of-scope in protocols, e.g. interactions between humans and devices, and between humans and other humans [Ellison 2007].

Ellison also says that "A secure ceremony is secure against both normal attacks, and social engineering. However, some secure protocols imply ceremonies that cannot be made secure. [...] The problem comes with modelling a human node. Like a computer protocol node, the human node has state, and a state machine. It receives and emits messages which cannot be programmed as done with device nodes. We must instead learn the human state machine empirically, by observing actual human behaviour" [Ellison 2007]. So, differently than in protocols, human behaviour is not considered to be predictable or deterministic in ceremonies.

Bella et al. argue that security measures should become invisible or beautiful/dictatorial to stimulate the user to participate more willingly [Bella 2020]. They bring to attention that a security analysis should account for other socio-technical facets of the task that the user is trying to accomplish as well, for example when surfing the Internet

[Giustolisi et al. 2018]. With all this in mind, we adhered to Bella and Coles-Kemp's approach for specifying and verifying security ceremonies, comprised of five layers, which can be folded or unfolded to focus on specific details one would like to assert [Bella and Coles-Kemp 2012]. Their approach is called Security Ceremony Concertina, and its layers are: Informational (layer I), Operating System (layer II), Human-Computer Interaction (layer III), Personal (layer IV), and Communal (layer V). Most of the work conducted in their framework is related to layers I and II, while our work focuses on layers III and IV (given that the first two layers are more related to security protocols, while layer V is out of our scope).

The difficulty of addressing the verification and specification of layers IV and V lies in the non-deterministic nature of the human being that is troublesome to grasp [Bella and Coles-Kemp 2012]. To fulfill this gap between technical methods and the socio-technical nature of layers IV and V of the Security Ceremony Concertina, we borrow our inspiration from the 1934 Nobel Prize winner and Italian play writer Luigi Pirandello and his characters' masks, which are used to define his classical meta-theatre plays.

Pirandello's work is recognised by his meta-theatrical play "Sei personaggi in cerca d'autore" (Six characters in search of an author) [Pirandello 2006]. In this play, Pirandello discusses the relations between authors, their characters, and theatre practitioners (which in our parallel will become protocol designers, users, and protocol implementers). The play demonstrates the problems involved in translating the reality conceived by six characters into the reality of staging the behaviour without complete knowledge of the author's thoughts. The story of the six characters is only incidental to the more important aspect of the play, the clash and exchange between the two worlds of art and life (for us, designing and using ceremonies).

It is not uncommon for computer security gurus to find themselves in the role of designing security systems (or protocols, in our case) that do not account for the real world and also do not take in the shortcomings of the users, since their focus is security for security itself. In this sense, we then find computer security practitioners trying to understand what was happening inside the guru's head while making that design an actual product that can be consumed by the user. Our idea in this paper is to explore the parallel of this scenario with Pirandello's masterpiece, trying to foster some ideas that can help us better understand the relation between computer security design, verification, implementation, and use.

In the rest of this paper, we present some of the work by Pirandello that bases our masks proposal, and review parallel work to ours in section 2. In section 3, we describe the six masks we believe can be used to start reasoning about security ceremonies as socio-technical problems. Following, we discuss how our Pirandellian masks can be used to verify layer IV of security ceremonies and how different user personas influence the whole ceremony execution (section 4). Finally, Section 5 brings our final considerations.

2. Related Work

In this section, we bring more insights on Luigi Pirandello's work, since it will drive some of our strategies in how to take humans into account for the specification and verification of security ceremonies. Following that, we present and discuss parallel work to ours by

showing the reader our contributions in context.

2.1. Luigi Pirandello's Work Synthesis

Luigi Pirandello was an Italian play-writer to whom was awarded the 1934 Nobel Prize in Literature "for his bold and ingenious revival of dramatic and scenic art" [Nobel Media AB 2018 2022]. His work was always considered analytic in nature with little action, but focused on the investigation between dichotomies, such as essence and appearance or illusion and reality. He produced 43 plays in all, being known for his meta-theatrical interventions, publishing some novels, poetry and short stories as well. His most known plays are published as a collection of plays called "Maschere Nude" (Naked Masks) [Pirandello 1952].

Important to our computer security discussion is a trilogy of plays that starts with "Sei personaggi in cerca d'autore" (1921; Six Characters in Search of an Author) [Pirandello 2006]. This first meta-theatrical play shows the problems involved in translating the "ideal reality" of six characters of a play into the casual reality of the stage, represented by the actors. The story itself is only incidental, as usual in Pirandello's work, to more important aspects, such as the clash and exchange between the two worlds of art and life. In this play, he introduced the concept of the fictional mask, where actors are required to wear their characters' masks of imposed reality to the staging.

In the second play, "Ciascuno a suo modo" (1924; Each in His Own Way) [Pirandello 2022a], this analytic preoccupation is even more pronounced. Instead of action and ensuing reflection on the stage, after each of the acts there follows coral interludes, in which the preceding action is discussed, bringing more reasoning to the outcome of the meta-theatrical endeavour. Although we are initially interested in defining the masks for security ceremonies, this second play already hints at us further ideas on how to analyse such masks, what we plan to explore in the future.

In the last play of the trilogy, "Questa sera si recita a soggetto" (1930; Tonight We Improvise) [Pirandello 2022b], is another meta-theatrical play where we see actors having to improvise, in an attempt to allow the work to stage itself, with characters rather than actors. Actors become frustrated at the conflict to completely become their characters, but also to come when they are called and adapt themselves. This play also gives us hints of how to follow up with the way masks should be defined in order not to frustrate users, by taking out their freedom on executing the ceremonies.

Most of Pirandello's work past the trilogy is concerned with the concept of masks. For Pirandello, a mask can be self-imposed or, in most cases, forced on by society. According to him, the mask is what makes life possible. If this mask is taken off, willingly or by force, we loose our identity and cannot function anymore. This is how security protocols and ceremonies work today. If our users get out of our scripted security ceremony they end up in a limbo, where security cannot be asserted anymore.

Pirandello also brings up the concept of a society based upon the law of common masks. In this society, if you do not wear your mask you choose death or insanity, and you are excluded from society. Some of the characters also exercise their freedom to wear specific masks, as does the protagonist of Enrico IV (1922; Henry IV) [Pirandello 1952]. He chooses to wear the mask of insanity in full consciousness. In that mask he committed a murder; and, ironically, society — the world of masks — cannot hold him responsible

because he has taken refuge behind a mask and beaten society at its own game. We see that choice as a means of how to use a mask from the user's point of view is paramount for the acceptability of the security ceremony, and also for understanding how users can try to defeat what was designed.

In the present paper, we plan to parallel Pirandello's work for the presentation of layers III and IV of the Security Ceremony Concertina. In summary, we would like to describe usual personas in security ceremonies as Pirandellian masks. This will be done in order to reuse them in the specification and verification of security ceremonies as framework, and allow for mechanisation strategies to be drawn on top of masks instead of the human behaviour itself. We also want to draw from his meta-theatrical exercise to devise a set of meta-design strategies for security ceremonies, so that we can convey the thinking of the designers to ceremony implementers and ultimately to users.

2.2. Parallel work

The first approach to human modelling we want to present is the one seen in [Johansen and Jøsang 2014]. We generally see works that model human agent interaction with a user interface as a non-deterministic process. In their paper, they propose a probabilistic model where the model of the human peer and that of the user interface are separate and, as such, they have a "compilation" operation as a means of putting the two together.

The authors base their modelling on the Security Ceremony Concertina methodology as well, making use of the notion of "personas". A persona can be understood as an abstract representation of a physical user in the digital world. Johansen and Josang then defined the persona in their model with a finite set of social and cognitive attributes of a human being, including their emotions, senses, and memory [Johansen and Jøsang 2014]. For their user interface model, they simply have a deterministic state machine with labels on its transitions to denote the options offered by the interface to the user in each particular state.

In [Johansen and Jøsang 2014], they even describe how an attack on the intersection between layers III and IV could happen, that being in the form of an intentional change of user behaviour from one persona to another (from being cautious to trusting, for instance) due to a trick on the user interface (through the clever use of colours, logos or symbols, etc).

Johansen and Josang's approach is different from our Pirandellian masks because they focus on the user interface (layer III) instead of on the modelling of the human nature characterised by layer IV of the Concertina.

In [Pedersen et al. 2018], they argue that to design and use technology one needs to develop and use models of humans and machines in all their aspects - including cognitive and memory models as well as social influence and emotions. This wider discipline is what they call Behavioural Computer Science (BCS). The authors believe that empirical studies can be one effective way to constantly update the behavioural models, instead of only making inferences about human behaviour based on rational models.

Pedersen et al. also use the Concertina methodology as a basis for defining BCS concepts in their work. They analyse how events, memories, and change of emotion affect

the user during the interaction with ceremonies. For example, people tend to remember their experience with a given system by how they felt by the end of their interaction, and that can get humans to choose options in a biased way when dealing with protocols in general.

They see the persona as a filter for the user himself (the human with feelings and thoughts interacting with the system), and they acknowledge that attacks can be transmitted from the user interface to the user through the persona (that is, the user's state of mind in a particular time of the interaction), where the users may be induced to click on insecure links, etc.

Pedersen et al. state that behavioural models can be used by system developers to incorporate knowledge about human actual behaviour in their designs. In summary, their proposal is "to take the perspective of the individual when building user interfaces that take into consideration human behavioural tendencies, with the aim of designing systems that empower individuals to make more correct judgements when interacting with an automated system" [Pedersen et al. 2018].

Our work differentiates from theirs because we focus not only on the user behaviour, rather also on describing it with an interchangeable formal definition which can be easily applied to any ceremony that can be described with the Security Ceremony Concertina.

Basin et al. propose a formal modelling of the human limitations and errors with Tamarin in [Basin et al. 2016]. As human peers are the weakest link in a security ceremony, their understanding is that social engineering attacks are a much easier entry point to today's systems than direct attacks on the involved machines or their underlying cryptography. For them, a human error is any deviation of a human from the protocol/ceremony specification.

In their modelling, they keep track of the human agents' knowledge which can be updated over time. Besides, they do not limit human memory (that is, the number of terms humans can remember) and they do not take into account intentions or reasons when defining human errors, only their behaviour.

This way, Basin et al. classify human peers as fallible (those that execute their roles in the protocol differently than expected) and infallible (those who do not deviate from their role specification). From that, the authors are able to test protocols with respect to their resilience to different kinds of human errors in their case studies [Basin et al. 2016].

Note that Basin et al. focuses on the human error in [Basin et al. 2016], while our work focuses on other human characteristics other than error alone. We plan to include error as part of our model, but we are not limited to that.

The next work we want to mention presents an intuitive graph-theoretic model called communication topology [Basin et al. 2015]. It is a labelled graph where the vertices and edges represent the actors and their communication channels. The assumptions about the actors go on the vertex labels, while the edge labels assign channel assumptions (such as confidential, authentic, or insecure) to communication links. They use these assumptions to determine whether it is possible to have secure communication between any

two nodes in the topology.

The authors propose a complete characterisation of necessary and sufficient conditions for the existence of security protocols that provide secure channels between humans and a remote server using an insecure network and a dishonest platform [Basin et al. 2015]. Such protocols are called Human-Interaction Security Protocols (HISPs). With this characterisation, they are able to indicate which secure or insecure communication channels must be available in HISPs for a secure communication to be established. They demonstrate the feasibility of their proposal with the Tamarin tool [tam 2022].

In more recent works, such as [Sempreboni and Viganò 2020], the authors model the mistakes that humans make when participating in a security ceremony through mutation rules. Such rules model possible human behaviours, automatically adjusting the behaviour of the other agents of the ceremony as well.

Sempreboni and Viganò consider the mutations provoked by human users to be of the following natures: skipping one or more of the actions that the user was supposed to perform, switching/replacing messages, or adding an unforeseen action to the ceremony execution [Sempreboni and Viganò 2020]. To automate their proposal, they have developed a prototype tool that extends Tamarin, called X-Men.

Another relevant recent work is seen in [Bella et al. 2022a], where the authors propose a formal modelling of human threats imposed on the ceremony using the Tamarin tool [tam 2022].

They state that the ceremony is directly affected by its users' behaviours, mentioning as an example of this that "a train ticketing system can become insecure if passengers are dishonest and controllers are lazy" [Bella et al. 2022a]. More serious scenarios would involve the disclosure of information that was supposed to be kept private by the users of the ceremony, or even the forging of physical elements that aim to exploit the system. In this light, they discuss three different personas: the chatty (the user who reveals information), the cocky (a user who gives out objects), and the forger (for those who fabricate objects).

Their approach diverges from ours as the basic behaviours we cover with our masks are more focused on the interaction of the user with the system rather than on the interaction between the user and the other users and the potential harm it could bring to the ceremony in question.

Extra motivation for modelling human peers in security systems can be found in [Radke et al. 2014], [Radke and Boyd 2017], [Jacomme and Kremer 2018], and [Bella et al. 2022b]. In the next section, we start talking about the masks we are proposing in the present paper and what are their characteristics in finer detail.

3. The Six Masks in Search of a Security Goal

The creation of personas to whom a security goal must be fulfilled, as Pirandello did his Characters' definition, is one of our strategies. As in Pirandello's initial approach in Six Characters in Search of an Author [Pirandello 2006], we aim at creating the first sketches of the Pirandellian masks that could be reused in several different security ceremonies in the future.

We start with our "default" behaviour, represented by our Attentive mask, that considers more aware users who are actively seeking a successful ceremony outcome. Apart from the Attentive, there are those who, although understanding the risks involved, do not care for the security mechanisms in place, thinking that such mechanisms are there just to protect others (thus, the Careless mask). Another persona we can mention stands for those who would rather not engage with the security system at all as they believe that their shortcomings will be noticed and alarmed by such systems (the Fearful).

We have drawn the setting of the three masks above from the work of [Johansen and Jøsang 2014], where they analyse the aware, indifferent, and cautious personas. These personas are the equivalent of our Attentive, Careless, and Fearful masks, respectfully.

Apart from the three masks just presented, we too draw from experience as we have seen security protocols designed, verified, and implemented only to fail when put into practice. As already mentioned by the related works reviewed in the previous section, much can be perceived by empirical observation, especially when we regard human behaviour. As such, we designed a separate mask for people not aware of the real dangers of engaging with certain systems, the Naive mask. The idea here is to also target first-timers with this mask, helping them through the correct use of the system and its functionalities.

On the other hand, we generally see people who simply do not have time to properly engage with the security system (the Busy). This mask seeks to bring a simplified version of the ceremony for a faster approach to its execution as a whole.

In [Johansen and Jøsang 2014], they also hint at the possibility of introducing more personas to the model by the combination of the ones already in there (for example, being both cautious and aware). Following along these lines, we suggest the Elder mask, which is a practical case of those personas that can be understood as the composition of other personas.

Lastly, as Ebner et al. say, "usually a target for attacks into systems is to explore characteristics of the persona such as their age" (EBNER et al., 2018), we have the Elder mask. This mask considers users who may not be properly trained to use security systems (as in the Naive case) and they may be afraid of making something stupid (as seen with the Fearful mask).

Following, we have a subsection for each of the six briefly mentioned masks, where we discuss in more detail their unique characteristics. We also describe in what kind of circumstances they can be perceived in real life.

3.1. The Attentive

The Attentive mask is the mask a ceremony designer expects the users to be wearing when interacting with the security ceremony. Here, the user is considered to be mindful of each step they are taking in the ceremony, rechecking their credentials whenever they need to enter personal information for authentication or similar operations. In this case, the attentive user is probably more familiarised with the interaction with the system, performing the required tasks more accurately when compared to the other masks.

Attentive users will also usually read very carefully all the instructions provided

by the user interface, most for completeness than for guidance (as seen with the Naive mask). We usually have successful ceremony outcomes when the user is wearing the Attentive mask, as a result of their responsible behaviour.

The user wearing the Attentive mask is playing their part actively in the ceremony execution and is willing to help the ceremony achieve its goals, as intended by the ceremony designers, and that is why it is the "default" mask of our proposal.

3.2. The Careless

The Careless mask is designed for users who, although possibly understanding the risks involved, simply do not care about the security mechanisms in place. They are not concerned whether the ceremony execution will be successful or not, as they will just proceed in whichever way best suits them.

Careless users will press any of the options in the interface without attentively reading the instructions or rechecking of credentials they have entered into the system for correctness. This kind of behaviour can affect the users themselves and the ceremony as a whole given they will most likely need to redo some of the ceremony steps due to their own lack of compromise with the ceremony's outcome, resulting in an unnecessarily greater amount of time spent to conclude it.

A relevant aspect to mention for this mask is the higher probability of the Careless users leaving their device(s) unattended during the ceremony execution, given they do not tend to prioritise their own privacy and security.

A Careless mask could just as well be the result of someone having to interact with the system because they are obliged to do so or maybe because they are performing it for somebody else, and thus they do not take the steps so seriously and personally as they would otherwise.

3.3. The Fearful

The Fearful mask is intended for those users who would rather not engage with security systems whatsoever. However, this mask also includes those who are familiar with ceremonies and computational systems in general, but simply do not trust their personal data to digital devices.

It is important to notice that this mask can be worn by anyone despite of age, as both young and old people alike may be suspicious of entering their credentials and other private information to the system.

In addition to that, the Fearful mask refers to the cases where users do not feel secure in their own ability in recognising social engineering attacks, thus avoiding participation in security protocols whenever possible. Examples of such services are the purchase of tickets online instead of directly in a physical store (e.g. for flights or bus trips), mobile banking, etc.

3.4. The Naive

The Naive mask is designed for a very beginner user in a security ceremony. Perhaps it is the case that the naive person is not much familiarised with the ceremony in question or with computers and technology altogether.

This mask assumes that the protocol should guide the user as they do not know how to proceed in advance. In every step of the user interface flow, the naive user will be looking for signs and instructions on what they are expected to do in order to move forward with the ceremony.

With the Naive mask, we see the importance of a user interface with proper usability so that users are able to perform all the ceremony steps with no major concerns.

Leaving devices unattended is also an expected behaviour for this mask. Such behaviour can be extremely dangerous, especially in a work or public environment, where potential eavesdroppers can obtain private information of the users without them noticing.

If the Naive user leaves their computer unblocked in their work station to go to the restroom, for instance, they may be facilitating the interaction of a coworker or someone just passing by. In this case, they could check which tabs they have open, which programs they are using, email contents, and so on.

The attack scenarios we describe here illustrate the point we want to make about how crucial the users are to the ceremony execution and in reaching its conclusion safely. Both the ceremony should help the user get through all necessary steps but, also, the user should commit to being careful when entering critical information into the system, by protecting their devices from external tempering at the very least.

3.5. The Busy

The Busy mask was thought out for those users who do not have the time to do a thorough reading of instructions in a ceremony or to recheck personal information entered. This may lead to an unsuccessful ceremony end, as in the case of the Careless mask. Nonetheless, here it is not so much a misdemeanour of the user, but rather a not-so-fine use of the available resources as considered ideal.

The errors that may occur for the users wearing this mask include information misinterpreting, the user skipping a character when typing their password or passport number, etc. Scenarios much more serious than these would be, for example, if the user ends up signing documents without cautiously reading them and, consequently, compromising themselves in any way because of that.

3.6. The Elder

The Elder mask is specifically designed for elderly people, who have difficulty in understanding and following the steps of a ceremony. It can be quite similar to the Naive one (if the user has no familiarity with the process), and to the Fearful mask (for those users who fear doing something wrong during the ceremony execution).

As elders are gaining more attention from brain and computer sciences lately, we intentionally chose this mask as our example of a combination of other Pirandellian masks. For this mask, we take into account their more limited mobility and probable greater time of response during the interaction with the ceremony as well, such as scenarios where elders hit an option by mistake and proceed through an unwanted user interface flow, for instance.

It is our desire that ceremony designers could plan and conceptualise new masks as a combination of previously existing ones or even propose brand new masks from sketch

accordingly to their needs. The idea with our masks proposal is to offer an approach easy enough while just as flexible and malleable to accompany society's changing behaviours over time.

4. Human Analysis in Security Ceremonies

In this section, we reinforce the importance of our proposal and the mechanisation techniques we envision for the six Pirandellian masks we are proposing.

To formalise a human peer in a security ceremony is a very challenging task and still an open issue in the security community. It is infeasible to represent each human being's particular behaviour, and that is why we propose masks to more accurately describe those behaviours that can most commonly be seen among the users of a ceremony.

Our proposal consists of designing Pirandellian masks instead of targeting each user individually. Our idea is to have general common behaviours characterised by a group of masks where the user needs only to wear one of them while interacting with the ceremony. Note that the wearing of a mask is our way to express the state of mind of the user while they attempt to perform the steps of the ceremony.

4.1. The Banking Example

The simplest example we can use is that of a routine use of an ATM machine. With this example we can show how the same ceremony scenario can yield to different outcomes depending on the mask the user is wearing.

Suppose an elderly person reaches the ATM machine after a very long time without using it. At first, they will probably try to read all the instructions showing up on the ATM screen to try and figure out under which interface option lies the service that suits their needs.

Consider it is the particular case that they want to do a bank transfer, for instance. Then, they need first to enter every bit of information correctly (account number, transfer amount, the date they want to set the transfer to, and so on), which can take more than one attempt to get right. In this particular scenario, if they take too much time rechecking the credentials entered into the machine, the session could even expire before they confirm it is safe to move forward with it. Here we already notice that the ceremony should consider the extra time needed for elderly people to take action in comparison to younger and more familiarised ones.

From this, it is possible that either they need to perform the ceremony once again or they can feel rushed by the ATM remaining session time and end up proceeding half-heartedly, fearing they could have made a mistake and compromised the transaction or their own accounts. Given that, we see that we should seek ways for the ceremony to help the sense of security and reliability the user experiences through their persona at all times.

Let us now suppose the possibility of our elder user deciding not to interact with the ATM machine by themselves, thus seeking further assistance from a person nearby. Ideally, such person should be a trustworthy bank assistant who would be perfectly capable to help such user. On the contrary, if the elder user asks for any other bank user for help instead, they may end up exposing private information accidentally. As this other person helps the elder user, it is possible that they could start collecting data on the elder's

account, such as their balance and recent transactions, probably without the elder user even realising it.

When we compare the presented example above to our default Attentive mask, we observe that they would perform all steps of the transfer ceremony neatly, rechecking all info entered and only proceeding once they were absolutely sure of the operation's correctness. They would not leave the ATM machine unattended and would make sure the machine has logged out of their accounts before moving away from it.

Now, consider how a Busy user would act in the same scenario. The user enters the bank to use the ATM machine. They know exactly how to perform the wanted transactions on the ATM machine, as they are very familiar with the procedure. However, as a Busy user is always in a rush, it could be inconvenient for them if the system happens to malfunction or have constant delays during the transactions.

Bearing that in mind, the Busy user starts interacting with the machine and it goes just as expected when, at the very end, the user is prompted by the machine about whether or not they wish to perform another operation. Suppose that the Busy user just takes their card out of the ATM and walks away, thus leaving a gap for the next user of the machine to proceed in an attempt to impersonate the Busy user who just left. Of course, the session will automatically expire in just a couple of seconds, but it could open up a margin for some information about the Busy user's account leak to the next user due to an internal error, for example, leaving some extra time for an intruder to continue interacting with the screen.

Another behaviour we can notice from a Busy user is that if they do not recheck their credentials before completing a transaction, we still might have a circumstance where they would have to redo the whole process (as well as with the Elder scenario). In this case, it could be misinterpreting/misreading of the information on the ATM screen or just too much anxiety to get it done, rather than a lack of skill or knowledge about how the ceremony works, as previously mentioned.

With this example, we were able to compare three of our six masks' distinct behaviours for the very same security ceremony of interacting with a bank's ATM machine. We see that each mask has dealt with the ceremony accordingly to their inner characteristics, making it clear that the personas (here represented by our masks) are the driving force behind the user's actions.

For the Attentive mask, no further steps apart from the originally designed were needed to reach a successful outcome of the ceremony. The ceremony was executed in a secure way and presented no potential attack risks to the user. Nevertheless, we started seeing possible entry points for attacks, potentially leading to insecure ceremony runs, with the Busy mask.

Similarly happens with the Elder mask, presenting a greater probability of information leak and attacks from both eavesdroppers around the user in the bank line and/or the person helping them use the ATM machine. This mask also represents an insecure execution of the very same bank ceremony. Namely, the ceremony is most significantly impacted by the particular mask the user is wearing while interacting with it. This way, we can conclude that it is not the ceremony that is in itself secure or insecure, it rather depends on the user's persona.

4.2. Reasoning about our Masks Proposal

Our mask approach is of practical importance to symbolic evaluation of security goals in a ceremony due to the fact that it can restrict the necessary amount of states needed to validate a ceremony scenario.

If we think about every decision point in a ceremony, where the user has to choose to follow through one path or another, we would have several options in total to evaluate. From each of these decisions can come a secure or an insecure action depending on whether the decision was secure or not from the user part. In this sense, we can assume that a ceremony has 2^n possibilities of execution, where n is the number of binary choices the human peer makes.

Notice that a previous decision taken by the user does not alter the probability of their next decision being more assertive. Each decision is independent of the ones that came before them on the execution of the ceremony and is, in fact, highly influenced by the state of mind of the user (namely, their persona - here represented by a Pirandellian mask) and the environment they are inserted in by the time they are interacting with the ceremony.

If we would take into account all possible decisions a user can make to be able to establish a ceremony as secure or insecure, that would demand a vast search space, rendering not useful most of the tools available today due to search space explosion. What we offer, with our masks approach, is a simpler and shorter way of validating a ceremony, where each mask is validated in turn.

In other words, for each mask, the ceremony needs only to be validated considering the decisions the user wearing that particular mask would take. This way, regarding the user decision-making process while interacting with the ceremony, we can see our masks proposal as a guide or heuristic to simplify the evaluation of whether a ceremony is secure or insecure for each of those particular masks.

5. Conclusions

One of the problems of the security protocols' community is that even massively verified protocols still fail. With security ceremonies, we are able to take the human user as a node of the system and try to minimise such problem. After all, we now have more interactions (those of humans and humans, and humans and devices) that can be accounted for.

In this context, we see that attacker models are quite well established and developed for security ceremonies. However, user modelling is still an open issue. Given the non-deterministic nature of human behaviour, we decided to work with the concept of masks (borrowed from Luigi Pirandello). The choice for Pirandello's work is due to the fact of the philosophical effort to conceive the elaborate relation between the designer, the implementer and the user of a security ceremony. As it is very difficult to model the ideal human peer to engage in a security ceremony, or to model each individual user that we may believe would interact with our security ceremony, we resorted to conceiving Pirandellian masks we could use to represent the most common user personas in a ceremony.

With our proposal, we aimed to have more secure ceremony executions and users more aware of the inner threat models they are subject to while interacting to ceremonies.

The contributions of this paper are 2: the fostering of the relation between the meta-theatrical discussion of Pirandello and the meta-security protocol discussion of security ceremonies, and the proposal of six basic masks to start reasoning about human interaction with security ceremonies, along with an ATM example to demonstrate that different masks yield different results in terms of security goals for a ceremony.

All that said, we understand that the work presented here is just the beginning. Our plan for future work is to develop the implementation of a security verification framework with our reusable masks that automates security ceremonies testing. We intend to mechanise our masks approach with a formal tool such as the Tamarin prover, combining it with the Security Ceremony Concertina so we can reason about layers I through IV of any security ceremony against each mask to see how well they would perform considering the classic Dolev-Yao [Dolev and Yao 1983] and its more versatile derivations, the Multi-Attacker [Arsac et al. 2011] and the Distributed Attacker [Martimiano and Martina 2016].

References

(2022). The tamarin user manual. [Online; accessed June-2022].

Arsac, W., Bella, G., Chantry, X., and Compagna, L. (2011). Multi-attacker protocol validation. *Journal of Automated Reasoning*, 46(3-4):353–388.

Basin, D., Radomirovic, S., and Schläepfer, M. (2015). A complete characterization of secure human-server communication. In *2015 IEEE 28th Computer Security Foundations Symposium*, pages 199–213. IEEE.

Basin, D., Radomirovic, S., and Schmid, L. (2016). Modeling human errors in security protocols. In *2016 IEEE 29th Computer Security Foundations Symposium (CSF)*, pages 325–340. IEEE.

Bella, G. (2020). Out to Explore the Cybersecurity Planet. *Emerald Journal of Intellectual Capital*, 21(2):291–307.

Bella, G. and Coles-Kemp, L. (2012). Layered analysis of security ceremonies. In Gritzalis, D., Furnell, S., and Theoharidou, M., editors, *Information Security and Privacy Research*, pages 273–286, Berlin, Heidelberg. Springer Berlin Heidelberg.

Bella, G., Curzon, P., and G.Lenzini (2015). Service Security and Privacy as a Socio-Technical Problem. *IOS Journal of Computer Security*, 23(5):563–585.

Bella, G., Giustolisi, R., and Schürmann, C. (2022a). Modelling Human Threats in Security Ceremonies. *IOS Journal of Computer Security*, 30(3):411–433.

Bella, G., Ophoff, J., Renaud, K., Sempreboni, D., and Viganò, L. (2022b). Perceptions of Beauty in Security Ceremonies. *Springer Philosophy & Technology*.

Dolev, D. and Yao, A. C. (1983). On the Security of Public Key Protocols. *IEEE Transactions on Information Theory*, 29(2):198–208.

Ellison, C. (2007). Ceremony design and analysis. Cryptology ePrint Archive, Report 2007/399.

Giustolisi, R., Bella, G., and Lenzini, G. (2018). Invalid Certificates in Modern Browsers: A Socio-Technical Analysis. *IOS Journal of Computer Security*, 26(4):509–541.

Jacomme, C. and Kremer, S. (2018). An extensive formal analysis of multi-factor authentication protocols. In *2018 IEEE 31st Computer Security Foundations Symposium (CSF)*, pages 1–15. IEEE.

Johansen, C. and Jøsang, A. (2014). Probabilistic modelling of humans in security ceremonies. In *Data Privacy Management, Autonomous Spontaneous Security, and Security Assurance*, pages 277–292. Springer.

Martimiano, T. and Martina, J. E. (2016). Threat modelling service security as a security ceremony. In *Availability, Reliability and Security (ARES), 2016 11th International Conference on*, pages 195–204. IEEE.

Martina, J. E. and Carlos, M. C. (2010). Why should we analyse security ceremonies? First CryptoForma workshop.

Nobel Media AB 2018 (accessed June 2022). The nobel prize in literature 1934. https://www.nobelprize.org/prizes/literature/1934/summary/.

Pedersen, T., Johansen, C., and Jøsang, A. (2018). Behavioural computer science: an agenda for combining modelling of human and system behaviours. *Human-centric Computing and Information Sciences*, 8(1):7.

Pirandello, L. (1952). *Naked masks, five plays*. Everyman's library: Drama. Dutton.

Pirandello, L. (2006). *Sei personaggi in cerca d'autore*. Gutemberg Project, ebook #18457 edition. Original publication in 1921.

Pirandello, L. (Integral text accessed June 2022a). Ciascuno a suo modo - commedia in due o tre atti con intermezzi corali. https://www.pirandelloweb.com/il-teatro-di-pirandello/ciascuno-a-suo-modo/.

Pirandello, L. (Integral text accessed June 2022b). Questa sera si recita a soggetto – commedia in tre atti ed un intermezzo. https://www.pirandelloweb.com/il-teatro-di-pirandello/questa-sera-si-recita-a-soggetto/.

Radke, K. and Boyd, C. (2017). Security proofs for protocols involving humans. *The Computer Journal*, 60(4):527–540.

Radke, K., Boyd, C., Nieto, J. G., Manulis, M., and Stebila, D. (2014). Formalising human recognition: A fundamental building block for security proofs. In *Proceedings of the Twelfth Australasian Information Security Conference - Volume 149*, AISC '14, pages 37–45, Darlinghurst, Australia, Australia. Australian Computer Society, Inc.

Sempreboni, D. and Viganò, L. (2020). X-men: A mutation-based approach for the formal analysis of security ceremonies. In *2020 IEEE European Symposium on Security and Privacy (EuroSP)*, pages 87–104.