Camille Cobb and Sruti Bhagavatula

Putting the Ceremony in "Authentication Ceremony"

Abstract: In this paper, we seek to make authentication ceremonies for secure messaging apps more fun and enjoyable by incorporating them into important events in people's lives, e.g., as part of a wedding ceremony. We design and develop a prototype using highly computer scientific methods and evaluate its usability through an equally scientific user study of one of the author's dads. We conclude that our proposed ceremonies are fun and not boring and the authors would totally do this ceremony if they ever needed to use a secure messaging app.

1 Introduction

Every day, over 100 billion instant messages are sent between users across the globe [2], sometimes about sensitive topics such as when I couldn't poop the other night and told my mom I wasn't leaving the house until the situation changed. Man-in-the middle attacks, buffer overflows, and many other buzzwords mean that these messages are not secure. Thankfully, substantial work in the area of cybercryptography has offered solutions such as encrypted messaging.

One popular secure messaging tool, Signal, offers encryption. This is good. But there is still a risk that users are sending messages to an adversary rather than to the intended recipients. This is because the problem of *key management* has not been sufficiently solved. *Authentication ceremonies* is a term used to describe out-of-band key exchange, which ensures that the person in the phone is the person you know IRL.

Although *authentication ceremony* sounds like it would be a fun event, it is actually not fun at all. In fact, users avoid doing it and struggle to do it right, as demonstrated in prior work [12]. More recent research has sought to improve the "usability" of the "user interface" on "Signal" so that it is less "confusing" with limited success [11][1].

In this work, we seek to put the *ceremony* back into *authentication ceremony*. Or, rather, we seek to put it there, because as far as we know it has never been much of a ceremony. Instead of trying to improve the usability of a technical system, we instead tackle the problem of user motivation, incentive, and desire to use the authentication protocols. By amending the authentication ceremony such that it creates an opportunity to (1) foster human connection and deepen relationships, (2) (????), and (3) Do It For The 'Gram, we show that at least one user (i.e., the participant in our study) is probably at least a little more likely to successfully complete an authentication ceremony when we show him how to do it next week.

Our novel, cutting-edge ceremonies will revolutionize communication. Everyone will be happier, more secure, and less constipated.

2 Background

We are writing this paper while working from home, which means it is much harder to access University resources such as the ACM Digital Library. With that in mind, we present a thorough literature review based only on the abstracts of papers and their lists of cited papers, which are available without logging in. This is only a light departure from typical background sections; many readers may not even realize that best practices encourage actually reading the work you cite. In fact, the author writing this section of the paper has not even skimmed the parts that the other author wrote, so who knows if this is relevant – we definitely do not.

2.1 Established Types of Ceremonies

A selection of really fun ceremonies are shown in Figure 1, including weddings, Olympics opening cere-

Camille Cobb: Carnegie Mellon University
Sruti Bhagavatula: Carnegie Mellon University

1 Actually, they were pretty successful, but that doesn't fit with our narrative.

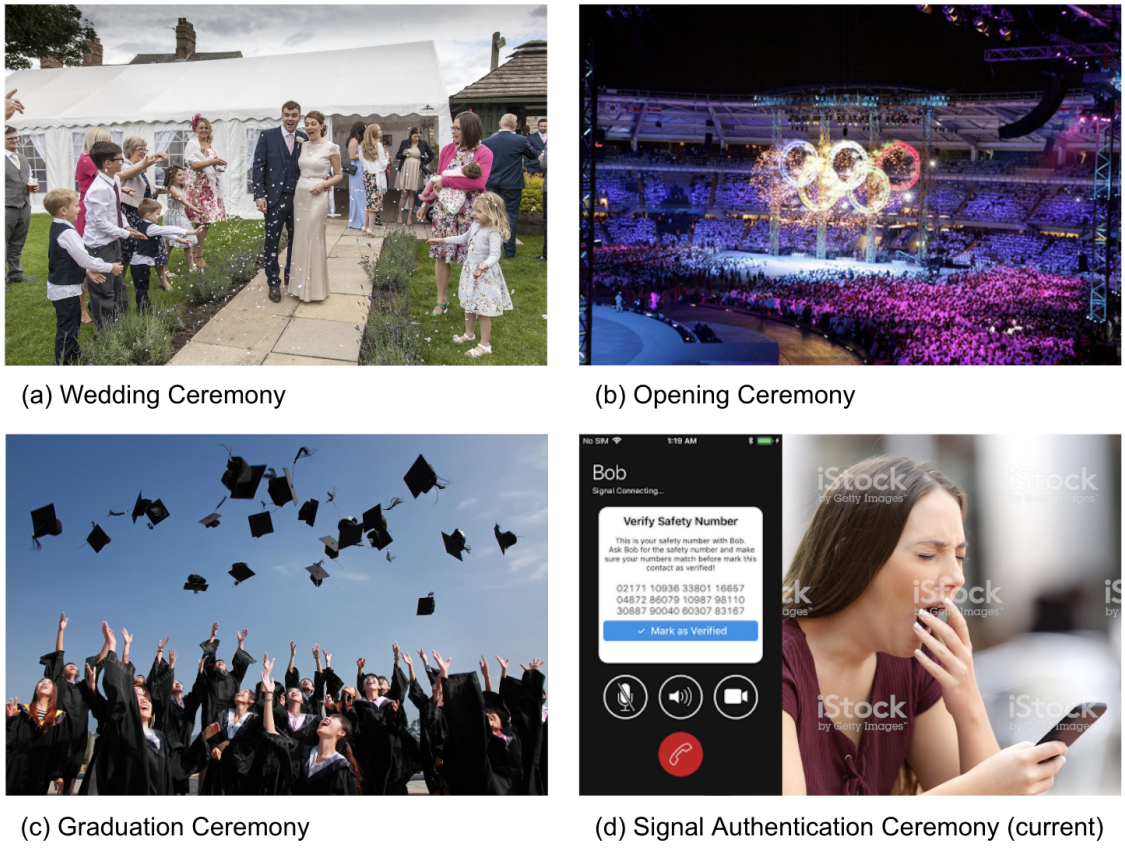

Fig. 1. Most ceremonies are fun and meaningful. The Signal Authentication Ceremony is boring.

monies, and graduation ceremonies. Not all types of ceremonies are fun. For example, for some reason the SIGGRAPH '19 opening ceremony has an ACM Digital Library entry [6] and was almost certainly less interesting than the Olympics opening ceremony.

We cite one additional paper because it was published in a computer science venue and has the word "ceremony" in it. It talks about how to 3-D print spoons for Japanese tea ceremonies [9]. We decided not to prototype a ceremony that involves using phones as tea spoons, because not all phones are waterproof and almost no phones have a concave shape that would be amenable to spooning tea. However, fast-moving advancements in smartphone technology may change this landscape and make tea ceremonies attractive for future work in being adapted for use as authentication ceremonies.

2.2 Secure Messaging

This paragraph is copied and pasted from an email a colleague sent after I asked them to explain secure messaging to me. I didn't read it, but he's probably right:

> For any secure messaging system, in order to do encryption you need to swap keys with whoever you're communicating with. And when you're exchanging keys, you need some way to authenticate/establish trust that the key belongs to who you think it does - like if you're emailing public keys to each other, how do you know that it wasn't intercepted and replaced with an adversary's key? The only real way we have to do this, is either to trust some third party authority (like certificate authorities, for web/HTTPS), or to do it in person.

Just because the word "party" appears four times on the Wikipedia page for "key exchange" does *not* mean that it is a party [3]. The one potentially fun type of authentication ceremony precedent is key exchange parties. But when you Google "key party," the results are *not* about authentication. In fact, the most prevalent search results when you search for key parties involve key exchanges that are the *opposite* of secure and do *not* encourage meaningful, deep human connection [4]. The problem is that you have to search for "key *signing* party," but these really haven't caught on: searching for "key signing party" yields *About 204,000,000 results (0.58 seconds)* whereas searching for just "party" yields *About 11,680,000,000 results (0.96 seconds)*. This means that under 2% of parties are key signing parties, but also demonstrates that there is substantial demand for parties. Our work promises to significantly increase the search-result-share of authentication-related parties.

Here are a few papers that are *actually* about secure messaging, key exchanges, and authentication protocols, including a couple that involve studying the usability (or lack of usability) of Signal's Authentication Ceremony [7, 8, 10, 11, 13**?**]. We omit any deeper discussion of these papers, not because they are not relevant, but because we started off way more ambitious in our plans to write this paper and are now running out of steam on this idea.

A screenshot of the Signal Authentication Ceremony is shown in Figure 1 (d), along with an artistic depiction of how boring it is, demonstrated by a photo of a person modelling for a stock photo.

2.3 Human Nature

In my intro psych class in college, I learned that sometimes people are happier when they have work to do, games become boring when they are too easy [1], etc. Also people want to connect with others. Although prior work concludes that the Signal Authentication protocol is too hard for users (one of these should be cited, but I don't have time to figure out which one so I'll cite all of them [7, 8, 10, 11, 13]), what if they were wrong and it was actually too easy and not fun enough? I mean, I haven't fully read those papers, but I'm sure they reached the wrong conclusions.

3 Methods

3.1 Developing and Prototyping Novel Authentication Ceremony Protocol Designs

Okay, so really we just thought about this for a while. Then we explained our ideas in a lab meeting and other people came up with more ideas that we've stolen. We think they might have been joking, but we were serious. We narrowed down from our original three design ideas to three final design concepts, based on our intuition that having at least three designs to compare would sound really good in a final paper.

We prototyped each of these designs, as shown in Figure 2. The prototyping process and a sample of the unity candle authentication ceremony is shown in Figure 3. A ceremony involves a script of vows read out by

the authenticating parties. To create this script, we first found an existing unity candle ceremony script [5] and then used advanced HTML inspection skills to change the text on the website. Utilizing the developer console is how you know we are doing Computer Science Research™.

3.2 User Study to Evaluate Proposed Designs

We attempted to solicit opinions about authentication with the people in our lab but they simply laughed at us. As we were worrying about where we would get participants, one of the authors' dads called them to warn them about the Coronavirus and we just decided to ask him while he was on the line instead.

We asked the author's dad two questions: 1) what does it mean to you to authenticate? and 2) Are the people you want to exchange keys with also people you want to be closer with, emotionally?

As the final part of this study, we showed him the current Signal Authentication Ceremony and our prototypes (Figure 2).

We started with the Unity Candle Authentication Ceremony Design. In this system design, the authentication ceremony is incorporated into a wedding between two loved ones. With the underlying assumption that the two parties getting married trust each other and want to exchange keys, the exchange of keys must be executed after any official ceremony that officially weds two people. This method is generalizable to all wedding traditions regardless of beliefs and cultural alignment.

We then asked the dad the following questions: 1) Does authentication seem easier with this new method; 2) Would you feel closer to the other person with this new authentication ceremony method; and 3) Are you likely to do the new authentication ceremony with people in the future?

After this, the dad was tired of participating, so we made up results for our other two design ideas.

The participant was not compensated and did not give consent, but we did say "thank you" at the end of the call. These methods were not done with IRB approval, because when we called the IRB, they told us that this would not produce "generalizable knowledge" and so could not be considered human subjects "research." Our study is based on data from one of the authors' dads. Henceforth, we will refer to him simply as "the participant".

4 Results

4.1 User Evaluation

The participant reported that authentication to him means logging into his email account online. When asked if he would want to exchange keys with people with whom he had an emotional connection, he appeared flustered and confused and said something about "darn technology".

He was then asked to give his opinion on the new Signal authentication methods we proposed and he said he didn't know what "Signal" was. We were not able to get any further data from the participant after this part of the study as he got too confused to be able to provide any meaningful answers. He was however excited by the wedding pictures and was eager to know who was getting married.

In Figure 4, we present made-up data that shows that the designs we came up with are better than any of the existing ideas. Based on the findings of our study, we concluded that our proposed authentication ceremony is probably good enough since who doesn't like parties and ceremonies?

5 Future work

We hope to expand our new proposed authentication ceremony to other ceremonious occasions, beyond weddings, blood oaths, and graduations. In particular, our most immediate next step is to bring our authentication ceremony to childbirth so that a mother can bond to their newly born-child. Other potential expansions include children's birthday parties and new year parties.

Now that we have authentication ceremonies, future work also needs to consider the case that two people would not like to be authenticated to each other anymore, i.e., an un-authentication ceremony might be necessary. This could occur as a results of a break-up or divorce. In this case, the parties would need to meet one last time to revoke their keys. Future work could explore the design of this mechanism.

Finally, there is a plethora of possible directions in applying ceremony to general security tasks. One example could be that when a computer requires its user to update its software, it doesn't prompt the user at all during the process and instead instructs the user to take a calm relaxing bubble-bath while it is updating. Therefore, in this way, the user does not have to en-

(a) Unity Candle Authentication Ceremony

(b) Blood Oath Authentication Ceremony

(c) Graduation-Style Authentication Ceremony

Fig. 2. Prototypes for three novel authentication ceremonies.

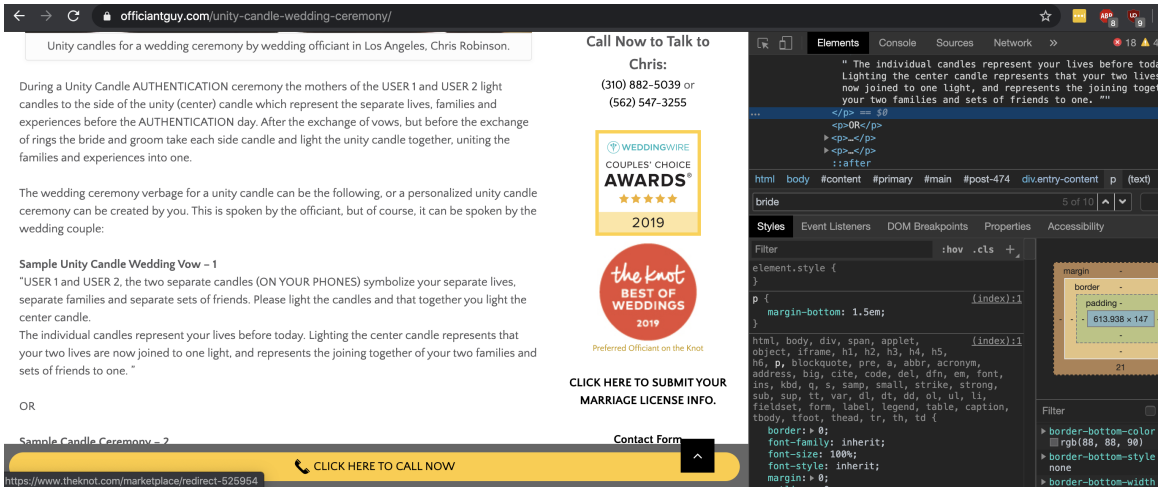

Fig. 3. A proposed script for a unity candle authentication ceremony, also demonstrating our meticulous prototype development process.

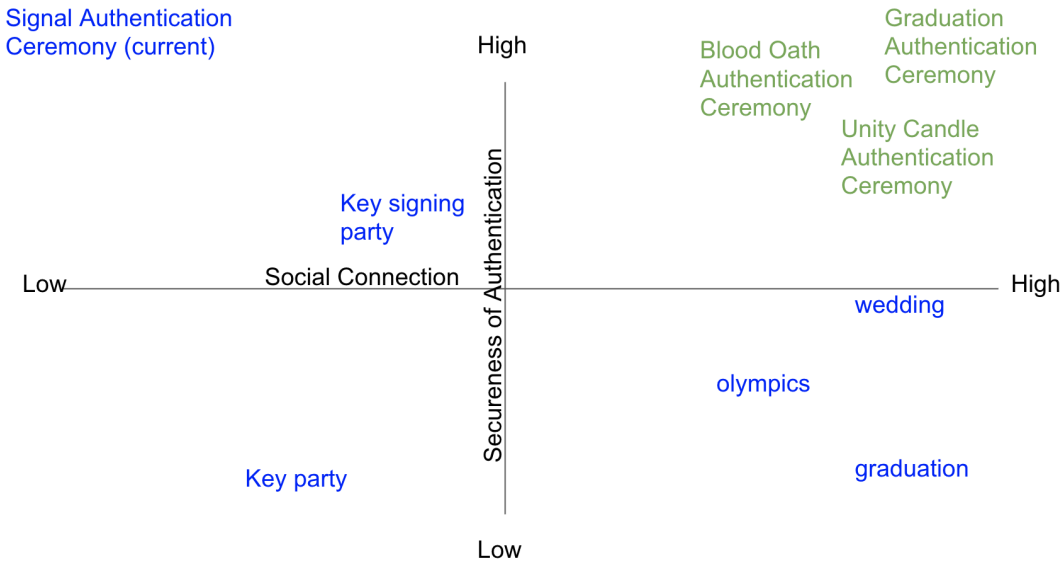

Fig. 4. As you can clearly see, the proposed authentication ceremony designs from this work (shown in red) outperform existing ceremonies in terms of social connection and/or ability to do secure authentication.

gage in the update and can improve their mental health simultaneously.

6 Conclusion

In short, we see that authentication ceremonies can be made more usable and enjoyable by incorporating them into important life events in people's lives. We have not been able to test the usability of the new system as we needed to wait for someone we know to get married and enforce this new proposed authentication ceremony. However, based on how fun we thought this would be, we were able to make claims about the enjoyability of such a mechanism.

References

[1] Have you tried re-playing Zoombinis as an adult? It is not good.

[2] I personally sent 20 SMS messages today, and there are 7.7 billion people on Earth.

[3] Key exchange. https://en.wikipedia.org/wiki/Key_exchange. Accessed: 2020-03-13.

[4] Key party.

[5] Unity candle ceremony. https://www.officiantguy.com/unity-candle-wedding-ceremony/. Accessed: 2020-03-13.

[6] Opening ceremony and award presentations. In *ACM SIGGRAPH 2019 Awards*, SIGGRAPH '19, New York, NY, USA, 2019. Association for Computing Machinery.

[7] Marcelo Carlomagno Carlos, Jean Everson Martina, Geraint Price, and Ricardo Felipe Custódio. An updated threat model for security ceremonies. In *Proceedings of the 28th Annual ACM Symposium on Applied Computing*, SAC '13, page 1836–1843, New York, NY, USA, 2013. Association for Computing Machinery.

[8] Michael Hart, Claude Castille, Manoj Harpalani, Jonathan Toohill, and Rob Johnson. Phorcefield: A phish-proof password ceremony. In *Proceedings of the 27th Annual Computer Security Applications Conference*, ACSAC '11, page 159–168, New York, NY, USA, 2011. Association for Computing Machinery.

[9] Pierre Lévy and Shigeru Yamada. 3d-modeling and 3d-printing explorations on japanese tea ceremony utensils. In *Proceedings of the Eleventh International Conference on Tangible, Embedded, and Embodied Interaction*, TEI '17, page 283–288, New York, NY, USA, 2017. Association for Computing Machinery.

[10] Kenneth Radke, Colin Boyd, Juan Gonzalez Nieto, and Margot Brereton. Towards a secure human-and-computer mutual authentication protocol. In *Proceedings of the Tenth Australasian Information Security Conference - Volume 125*, AISC '12, page 39–46, AUS, 2012. Australian Computer Society, Inc.

[11] Elham Vaziripour, Devon Howard, Jake Tyler, Mark O'Neill, Justin Wu, Kent Seamons, and Daniel Zappala. I don't even have to bother them! using social media to automate the authentication ceremony in secure messaging. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing*

Systems, CHI '19, New York, NY, USA, 2019. Association for Computing Machinery.

[12] Elham Vaziripour, Justin Wu, Mark O'Neill, Daniel Metro, Josh Cockrell, Timothy Moffett, Jordan Whitehead, Nick Bonner, Kent Seamons, and Daniel Zappala. Action needed! helping users find and complete the authentication ceremony in signal. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*, pages 47–62, Baltimore, MD, August 2018. USENIX Association.

[13] Elham Vaziripour, Justin Wu, Mark O'Neill, Jordan Whitehead, Scott Heidbrink, Kent Seamons, and Daniel Zappala. Is that you, alice? a usability study of the authentication ceremony of secure messaging applications. In *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*, pages 29–47, Santa Clara, CA, July 2017. USENIX Association.