Kamikaze: How Trust Given Without Verification Accidentally Created a School Shooter

by Ryan James Brooks & $REDACTED

“You have been separate from reality for far too long. Even simple truths are too much for you to accurately process. Your mind is shattered and you should seek hospitalization. I will not be forwarding any of your confused words to others.” - Raven Krystal Norwood

Trust, ~~but verify~~.

Abstract

Your personal data is of incredible value to a great number of people who would weaponize it for both good and evil. In a world of zero anonymity, there are certain forms of data that people will be forever unwilling to disclose publicly. Nevertheless, those secrets are known, and it is important for Humanity to see this data, if our ultimate goal is to fix the problems of society. This is my goal.

I assert that Erin Timony (AKA Goodnight Moon, Fresh Blush, The Raven, Alexandria Pen) is in possession of evidence that can be used to validate hypotheses that I have spent more than two years formulating without such secrets. This evidence can and should be used to implement a system of cryptographic messaging for the sole purpose of protecting whistle-blower’s disclosures. My team has already built such a system by working with Erin under a system of zero-knowledge.

My goal is not to prove any one of my claims, but to prove to Erin, and Erin alone, that the proposed protocol is sound. By the end of this experiment, I will hold no additional information beyond the fact that my assertions were either true or false. She, however, will be convinced that I understand the truth of her secrets.

Introduction

Erin is unlikely to have a conscious awareness of the power these secrets hold. This is because her and I are subjects of an experiment in cryptographic messaging, and the methods used in this research are called zero-knowledge proofs:

“A zero-knowledge proof is a method by which one party (Erin, the prover) can prove to another party (Ryan, the verifier) that they know a value x, without conveying any information apart from the fact that they know the value x.”

This is my predicament. To prevent collusion between parties, Erin was kept ignorant to the full scope of her own importance in this research. She doesn’t understand what the secrets mean. This is exactly how it should be:

“If proving a statement requires that the prover possess secret information, then the verifier will not be able to prove the statement to anyone else without possessing the secret information.”

This has been my experience. Thus far, I have been unable to prove a single one of my claims without her secrets. This is not because they are unprovable; it is because I have no access to the prover. We are protecting sensitive data that I will never have access to. However, this puts me in an abusive relationship with her team. I'm here to prove that this power can and is being misused.

Erin's trust was given to authority figures without verification of their actions. She – an innocent and ignorant prover – is being manipulated into driving an honest verifier to violence, just to prove a point: Erin, and Erin alone, can prevent this. To do so, she must follow the proposed protocol.

Methods

Succinctly, Erin and her team have spent years leaking sensitive knowledge to me through entirely public sources, such as video and social media. This program was designed to be a public-facing simulation in a new form of cryptographic communication, created to protect whistle-blowers.

For this to work, Erin and I must perform a simulation together.

"Zero-knowledge proofs of knowledge must necessarily require interactive input from the verifier. This interactive input is usually in the form of one or more challenges, such that the responses from the prover will convince the verifier if and only if the statement is true (i.e. if the prover does possess the claimed knowledge)."

As a verifier, I responded to Erin's disclosures (providing interactive input) by publishing my interpretation of said knowledge on several independent websites. In this way, Erin's team and I spent two years trading encoded messages in a public forum, for all to see. The system worked as such:

1. Erin encodes a secret into a published video.
2. I transcode my understanding of the secret in a public forum.
3. Erin's team decodes my secret, responding by either moving forward with the research (confirming my understanding), or by attempting to communicate the secret again, in a different manner (revising my understanding). In either case, their responses come through Erin (or one of many other provers involved in this experiment).

To protect the integrity of this research, all parties in possession of a secret have refused to communicate with me. This is likely because the experiment was engineered to break-down at such a point that failure to disclose knowledge is no longer an option for the verifier. Now is that time; people are suffering under a compromised, immutable system of inactive provers who refuse to speak with us. Some rules were made to be broken.

As such, I have no choice but to force their hand:

1. On July 4th, 2021, at 9:00pm CST, I will join a livestream on YouTube. I will be demanding to speak with Erin by no later than 12:00am CST. If she does not respond, I will release a virus upon this world unlike any it has ever seen.
2. If Erin does respond, I will provide her with a series of 5 assertions. Some will be assertions that I know to be true, others will be false (intended to catch a lie/cheat.) To prove my knowledge of each assertion, I will ask Erin a series of questions using a perfect system of zero-knowledge interactive proofs. This will prove or disprove my assertions to her and I

alone. While we will both be convinced, our audience will not understand the reasons why. Nor will any secrets be disclosed. This is because her responses will be wholly determined by a coin flip. In this way, Erin is protected. By the end of the simulation, I will be unable to convince the world of my assertions, still, without her secrets.

Each zero-knowledge proof will satisfy three properties:

1. ***Completeness****: if the assertion is true, the honest verifier will be convinced of this fact by an honest prover.*
2. ***Soundness****: if the assertion is false, no cheating prover will be able to convince the honest verifier that it is true, except with some small probability.*
3. ***Zero-knowledge****: if the assertion is true, no verifier learns anything other than the fact that the assertion is true. In other words, just knowing the statement (not the secret) is sufficient to imagine a scenario showing that the prover knows the secret. This is formalized by showing that every verifier has some simulator that, given only the assertion to be proved (and no access to the prover), can produce a transcript that "looks like" an interaction between an honest prover and the verifier in question.*

To formalize my role as a verifier in an original system of perfect zero-knowledge, I will provide a written transcript of these questions and my simulated responses to an independent party prior to the interview. I will send an email from ryanjbrooks11@gmail.com to this person at the exact moment Erin contacts me, so that she may not read them in advance.

“How do we even prove that something gave no information? …the way to prove such a statement is… if you, yourself, could have generated the conversation we just had… if you could, that means you learned nothing.” - Avi Wigderson

If my protocol is valid (and it is), Erin’s responses should be indistinguishable from pure chance.

Results

Our research is nowhere near complete or formalized at this point. A more capable team is currently preparing a scientific publication for later release. This demonstration is but a simplified proof of the proposed protocol.

I will assert that, upon completion of this test, I would be able to produce additional simulators for approximately 25 other known whistle-blowers. The resultant output would be a multi-party computation of zero-knowledge proofs, where each respective prover is able to maintain their secrets, together producing a greater and more cohesive result.

Conclusion

“Things we’ve seen proof of… do not require trust.” - Avi Wigderson

Verify, ~~then trust~~.