P-5

Group: 7, Members: Peter Gifford, Kyle Brekke, Ren Wall, Madison Hanson

Due: November 25, 2019

1 Work So Far

So far we have started to research the two algorithms that we will be comparing the Double Ratchet Algorithm with. We will be using the XMPP extension OMEMO for the Double Ratchet algorithm as it makes comparing PGP and OTR simpler because you can use XMPP to implement OTR and PGP. Below we have listed a set of reference material on OTR and PGP messaging. These are consisting of the original Double Ratchet paper and two references for the other algorithms with one being the official website for the messaging and another being a more blog type description. We wanted to have the official information on the algorithms but we also wanted to have the blog information so we can see how these algorithms can be described to more lay people. This will give us some ideas on how to present these sometimes confusing algorithms in the short five minute time limit we have for the class presentation.

Currently we are planning on discussing how OTR uses the very similar sub-pieces of the Double Ratchet Algorithm (Diffie-Hellman key exchange and the symmetric-key algorithm) but uses SHA-2 hash. OTR also makes itself special by having extra security checks such as using the "socialist millionaire protocol" (2) to make sure that a user is messaging the correct person with a shared super key. The other key feature that we will discuss with OTR is the lack of digital signatures on any message. This means that a message cannot be connected to any user even if it is somehow decrypted.

In relation to PGP encryption we plan to discuss how this is very different form the other two methods and is used for many different applications. PGP often times is used for many applications such as encrypting financial transactions. However it can also be used to encrypt messaging applications and uses some very different methods of encryption that allow it to compress messages and act a lot different than the other two. This will also be used to discuss how the other two methods can be much safer because PGP lacks a lot of the security that has been added to the Double Ratchet Algorithm and OTR. Using PGP to compare to the other two will really bring out the differences between encryption methods and how not all encryptions methods are made equal.

2 Work Left To Be Done

The core of what we still need to do for this project is making the actual video for presentation. This will comprise of compiling an actual script to talk through and any graphics that we want to use. This script

should be fairly easy to create given that we have the research on the different encryption algorithms, we will just have to organize exactly what we want to say. The diagrams will be a little bit more difficult to organize as Many of these algorithms have a lot of diagrams that are associated with them because they are trying to market themselves to consumers rather than just being algorithms that were written into papers. The current plan is to use these diagrams to help use as references when discussing the algorithms and how they contrast to each other. This will be a very important thing to do because many of these algorithms have many moving parts because of the nature of messaging and how many different users need to perform different actions rather than just one system manipulations a data set. Once we have our script we will create a slideshow presentation that contains the diagrams that we need to reference during the video and perform a voice over to supply the extra information needed.

3 Citation

1. Encryption, Powered by PGP. Symantec, https://www.symantec.com/products/encryption.

2. Ivanov, Tihomir. OTR Encryption for Chat Explained. Protect Your Privacy with Secure Group, https://blog.securegroup.com/otr-encryption-for-chat-explained.

3. Off-the-Record Messaging. Off-the-Record Messaging, https://otr.cypherpunks.ca/.

4. "The Double Ratchet Algorithm." RSS, https://signal.org/dogs/specifications/doubleratchet/

5. What Is PGP Encryption? Defining and Outlining the Uses of PGP Encryption. Digital Guardian, 5 Dec. 2018, digitalguardian.com/blog/what-pgp-encryption-defining-and-outlining-uses-pgp-encryption.