CSC 845 ADVANCED COMPUTER NETWORKS

Group Project: Proposal

I. Names of Team Members

Leslie Zhou (team lead)
Khanh Nguyen
Warren Singh

II. Background and Motivation

In 2013, Edward “Ed” Snowden, a 29 year old government contractor who was a former technical assistant for the CIA and current employee of defense contractor Booz Allen Hamilton came forward with startling revelations: the United States government was indiscriminately collecting and spying on the internet communications of a huge majority of the English speaking world [4].

While security concerns are part of network engineering, major service providers and technology companies did not typically prioritize security at the time. Due to the revelations, securing their services and communications became a top priority, as the scope and extent of the ‘bulk collections’ programs that were being run by the NSA shocked even industry insiders.

Within six months, prominent companies such as Facebook, Twitter, and Google began implementing upgrades to both internal and external systems [5], and according to some, greatly sped up the adoption of stronger security and end-to-end encryption protocols [6]. Millions of Americans, and others around the world learned of government spying programs as well as the importance of encryption and privacy in the face of mass surveillance as an added aftereffect of Snowden’s whistleblowing activities.

One open source cryptography project [7] developed into an industry leading standard [8] for end-to-end encryption in the wake of these developments: the Signal Protocol.

The Signal Protocol [3] is a non-federated cryptographic protocol which is most widely used to ensure end-to-end encryption for communication applications (i.e. text-based messaging and VoIP). Applications which implement the Signal Protocol include Google’s Messages, Facebook Messenger, Whatsapp, and Skype [8], meaning the number of users whose messages are secured by the Signal Protocol potentially number in the billions.

Due to its widespread use, broad influences, intended effect, and open sourced approach, examining the protocol thoroughly is crucial in understanding how industry leaders secure both internal and external network communications, as well as providing a foundation for apprehending and developing further iterations and applications, since developers working on applications continue to use the Signal Protocol as foundation and inspiration for further encryption protocol development.[9][10][11][12]

III. Goals

The Signal Protocol is such a widely used and industry standard protocol for end-to-end encryption precisely because it has been open sourced for years, meaning that thorough analyses and audits on it have been able to be performed (and that those audits themselves are also peer reviewed and scrutinized) [1][2]; there is a very high degree of confidence in the protocol as a result.

Our main goal is to understand, analyze, and implement the Signal Protocol [3] for end-to-end encryption. A secondary goal (time permitting) is to use this implementation to cryptographically secure communications between users of a text-based chat application, and to develop and understand new protocols based on aspects of this industry standard encryption.

The scope of this project focuses on the cryptographic security protocols implemented for networking communications, but encompasses the (possible) development of a web-based application which makes use of said cryptographic encryption implementation, as well as potential further iteration, as deadlines and workflows allow.

IV. Activities and Methods

a) Protocol:
   i) Double Ratchet algorithm [3]
   ii) Pre-keys [3]
   iii) Triple elliptic-curve Diffie-Hellman handshake [3]
   iv) Cryptographic Primitives
      1) Curve25519
      2) AES256
      3) HMAC-sha256

b) Backend:
   i) Node.JS / Express.JS
   ii) Socket.IO (messaging)

c) Frontend:
   i) React.JS
   ii) Socket.IO (messaging)

d) Analysis Tools:
   i) Wireshark
   ii) Binwalk
   iii) Foremost
   iv) Tcpdump

V. Timeline and Responsibility of Each Member

Timeline:

Project Proposal: February 27, 2022
Midterm Presentation: March 28,2022
Final Presentation and Demo: May 8, 2022

Roles & responsibilities:

- Leslie Zhou (team lead)
  - Double Ratchet algorithm
  - Backend
  - Analysis
- Khanh Nguyen
  - Triple elliptic-curve Diffie-Hellman handshake
  - Frontend
  - Analysis
- Warren Singh
  - Pre-keys
  - Cryptographic Primitives
  - Documentation
  - Analysis

VI. References

1. Nadim Kobeissi, Karthikeyan Bhargavan, Bruno Blanchet. Automated Verification for Secure Messaging Protocols and Their Implementations: A Symbolic and Computational Approach. *2nd IEEE European Symposium on Security and Privacy*, Apr 2017, Paris, France. pp.435 - 450, ?10.1109/EuroSP.2017.38. Hal-01575923
2. K. Cohn-Gordon, C. Cremers, B. Dowling, L. Garratt and D. Stebila, "A Formal Security Analysis of the Signal Messaging Protocol," *2017 IEEE European Symposium on Security and Privacy (EuroS&P),* 2017, pp. 451-466, doi: 10.1109/EuroSP.2017.27.
3. Signal Technical Information. *Signal*. https://signal.org/docs/
4. Edward Snowden: the whistleblower behind the NSA surveillance revelations. *The Guardian.* https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance
5. Miller, C. C. (2013, November 4). Angry Over U.S. Surveillance, Tech Giants Bolster Defenses. *The New York Times Company*. https://web.archive.org/web/20131106015230/https://www.nytimes.com/2013/11/01/technology/angry-over-us-surveillance-tech-giants-bolster-defenses.html
6. Cuthbertson, A. (2016, June 8). Snowden "Sped Up Encryption" by Seven Years. *Newsweek*. https://www.newsweek.com/snowden-sped-encryption-seven-years-452688
7. Garling, C. (2011, December 20). Twitter Open Sources Its Android Moxie. *WIRED*. https://web.archive.org/web/20111222010355/http://www.wired.com/wiredenterprise/2011/12/twitter-open-sources-its-android-moxie/
8. Signal partners with Microsoft to bring end-to-end encryption to Skype. (2018, January 11). *Signal*. https://web.archive.org/web/20200202152037/https://signal.org/blog/skype-partnership/
9. Canada, Germany, and Australia are getting e2e encryption, Viber Blog https://web.archive.org/web/20161005083000/http://www.viber.com/en/blog/2016-05-03/canada-germany-and-australia-are-getting-e2e-encryption
10. Viber Encryption Overview, Viber https://web.archive.org/web/20160711035838/http://www.viber.com/en/security-overview
11. Forsta developer AMA (interview) https://web.archive.org/web/20180502045526/https://www.reddit.com/r/crypto/comments/8b1m6n/forsta_signal_based_messaging_platform_for/
12. Forsta codebase, (Github repository) https://web.archive.org/web/20180613054634/https://github.com/ForstaLabs/libsignal-node