Jessica Showers

10/02/2019

ISSC431

Week 5

Database Security Research Paper - DRAFT

**Applied Cryptography**

**Table of Contents:**

Abstract

Introduction

iOS 13 ‘Find My’ Location Services

Google’s Private Join and Compute

Example: Private Data Intersection

Example: Homomorphic Encryption

Digital Signatures and Certificates

Conclusion

**Abstract:**

Cryptography is as much art as science. Encryption is the process of converting data using cryptographic techniques to prevent unauthorized access. These techniques are used to secure information both in transit and when securely stored on a server. This paper takes an in depth look at modern cryptographic techniques used with iOS 13 Find My location services, Googles ‘Private Join and Compute’, and the commonly used Digital Website Certificate.

**Introduction:**

Cryptography can be described as an art form which obscures the meaning of information in such a way that only the intended recipient can decipher. It has existed as a form of information security since well before the computer era and the principles behind message encoding are similar today to the ones used in the ancient past. Both modern computers and manual cryptographic techniques rely on an algorithm to convert a message into a secure code. The algorithm is used to transform a legible message known as plaintext into cyphertext, which is an indecipherable code to anybody who does not possess the algorithmic key required to transform it back into plaintext. This cryptographic process was originally applied to coded text messages printed on leather or parchment but the same premise can apply to any batch of digital information including text, photo, audio, video, or any other file type.

Modern cryptographic technics are necessary to shield information while in transit and at rest. These can be simple such as password hashing, or more complicated such as those used to shield location services on mobile devices. Data encryption is crucial for data both at rest on a secure server as well as data in transit from device to device. Many modern mobile devices include location services which must be shielded from interception. Business communications need to utilize secure channels to insure that partners have access to the data required to complete a task, without putting connected data sets into unauthorized hands. Businesses and organizations working with confidential data sets may require secure collaboration protocols to analyze information from multiple secure data sets. Multi-party computation involving secure data poses a risk of data exposure without proper security and encryption. Even simple web page access poses numerous points of vulnerability to users, hosts, and data access. Hosting a secure website requires the use of a digital certificate. Secure websites have a url which begins with HTTPS rather than HTTP and present on load with a closed padlock usually located in the address bar. Secure websites use encryption and are backed by the authority of a certificate authority. Cryptography effects all aspects of digital activity by securing communications such as location services, protecting confidential data being stored on a server, and even basic website navigation.

**iOS 13 ‘Find My’ Location Services:**

iOS 13 introduced changes to the find my iPhone application. Both find my iPhone and find my friends have been merged into a new ‘Find My’ application. This application is currently available on iOS 13 devices and will be introduced to MacOS when Catalina is released. This new find my feature will introduce offline location finding. Should a device be lost in an area without connection to wifi or cellular data it is able to interact with other nearby apple products via bluetooth to pass location data to the iCloud server. It uses a type of encryption by which a devices location can be anonymously passed by other Apple users to the iCloud server and made available only to the authorized Apple ID account holder. The location data is not accessible to the devices passing it, nor will it be available to Apple either despite being hosted on the iCloud server.

This iOS 13 feature allows a verified user in a supported application to locate a lost device even when that device is not connected to wifi or cellular data. This feature poses some unique challenges because it uses near field communications to pass the devices location data through the devices of untrusted users in a way that does not impact security. This is an example of using cryptography to secure communications in transit. According to Apple, when MacOS Catalina is released it will introduce activation lock to the Mac operating system for the first time. Activation lock enables remote locking, erasing, and reactivating of MacOS and presents as a firmware lock which prevents device access even if an erase is attempted. This process is made secure thanks the Mac T2 Security Chip which ensures you are running trusted software and automatically encrypts stored data. In addition to find my location encryption, activation lock, and the T2 security chip, MacOS Catalina is designed to be more secure than ever by running the operating system in a secure read-only volume. Cryptographic techniques are used for data in transit with the passing of location data through nearby devices via near field communications, data at rest on the users hard drive, and the MacOS operating system is protected through encryption on a read-only volume.

**Google’s ‘Private Join and Compute’:**

Google’s ‘Private Join and Compute’ software: Private join and compute allows for secure multi-party computation (MPC). This software is open-source and is designed to allow organizations to collaborate using confidential data sets while allowing for cryptographically secure privacy protection. Private Join and Compute uses the cryptographic techniques of private set intersection and homomorphic encryption. Private set intersection is a security technique by which set of confidential data A. can be compared with set of confidential data B. and correlations can be drawn from the two data sets without exposing either set of data to the other.

**Example: Private Data Intersection**

Jane and John are going into business together. They are using confidential data sets to design the website homepage of their joint business venture. They each have their own separate business and want to only share the data sets which they have in common and which are relevant to the business needs. Neither Jane nor John known the contents of the others data sets.

Janes Favorite Colors: Purple, Green, Yellow

Johns Favorite Colors: Blue, Purple, Red

Output: Website background should be Purple.

Googles private join and compute provides multi-party collaboration which allows multiple parties to gain insights from their private data sets without providing the entire data set to all parties involved. This software also uses homomorphic encryption to further protect confidential data. This type of encryption protocol allows for working with confidential data while it is encrypted in cyphertext. The benefit is that calculations can be performed on the data without first converting it to plaintext. The idea of homomorphic encryption has been around since the late 1970s however was not fully realized until 2009. This method allows one party to provide confidential encrypted data to a second party and the second party is able to perform computational analysis on the data without ever having full access to it. An example of where this may be useful would be in the providing of a confidential data set to an analysis firm which generates useful results without ever having to be decrypted.

**Example: Homomorphic Encryption**

Jane has created a website for her business and has accumulated a large number of log files which require analysis. She intends to hand the log files over to a digital security company which will provide her with weekly reports on the results of log file analysis. She is concerned about handing the log files over to a third party entity as they could pose a point of vulnerability for her website. The security firm uses a secure file sharing service which uses homomorphic encryption.

* Jane uses an application provided by the security firm which lets her set permissions, encrypt the data, and upload it to a secure file server.
* The security firm receives securely encrypted files which appear in cyphertext as gibberish to any human analyst.
* Those files are opened within a secure application which can run designated tests and create automatically generated reports of the results.
* A security analyst reviews the reports, highlights key details, and creates a list of suggestions based on the results.
* Jane receives a customized list of suggestions for improving her websites security while the security firm is unable to make use of the log files in any manor beyond the permissions set by Jane.

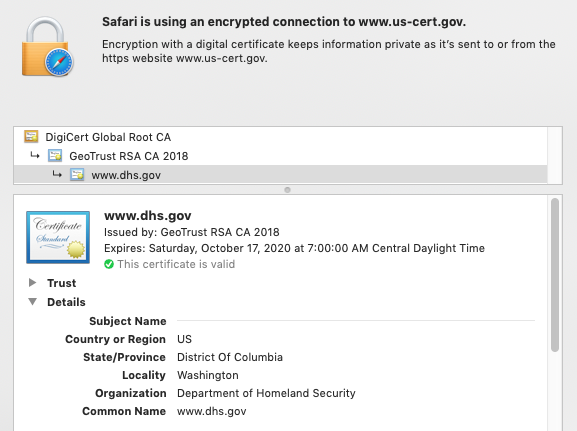
Googles Private Join and Compute service combines these two methods of digital security, private data intersection and homomorphic encryption to create a secure digital platform for collaboration between multiple parties using private data sets. By using Private Join and Compute John and Jane can safely share data with neither party being exposed to the full data set. Jan can gain insights from seeing where Johns data intersects with her own and John can analyze the data that Jane provides him without fully viewing the data itself. This package could be used to analyze voter data, or population data, without exposing vulnerable vulnerable or resident information to the analysis tools being used. It could also be used to monitor healthcare trends without exposing HIPPA protected data to third parties. There are many situations in which confidential data may need to be analyzed by an expert who is not authorized to directly interact with the data. For security purposes, it allows working with third parties without ever fully handing your data over to those third parties.

**Digital Signatures and Certificates:**

Digital signatures and certificates are one of the major backbones of online security. Secure websites use SSL (Secure Sockets Layer) to establish encrypted communications with a web server. To be secure a website or web application must be backed by the legitimacy of a Certificate Authority. A website certificate includes a digital signature which authenticates that its origins are valid and recognized. The value of a digital certificate can be found through a web search using a browser which is set to validate digital certificates.

Should a developer issue a web application called “Best App Ever” that developer may want to distribute it over the internet using a digital signature. The digital signature is encrypted using the Certificate Authorities private key. A second developer, seeing that “Best App Ever” is quite popular decides to make a malicious application called “Best Appp Ever” and attempt to direct users searching for the original application toward the modified version of the app. Users visiting the original developers site with a signed certificate with no obstacles. Visitors using secure browser setting visiting the malicious “Best Appp Ever” site receive a notice in their browser that the website is not trusted and receive a recommendation to go back to search results.

Website certificates are issues by a certificate authority. There are many certificate authorities. It is important to insure that a website url matches the address listed on the website certificate. By clicking the padlock icon on a secure website, you can view a websites certificate.



This certificate, issued to [www.dhs.gov](http://www.dhs.gov) indicates the the certificate was issued by DigiCert Inc and uses a 256 byte Public key. A website certificate is a security protocol. The certificate itself holds data which links a cryptographic key to a websites server or address. This is important for websites which transmit sensitive data such as user information, medical records, financial data, or other data requiring protection. Encryption protocols may use 128 or 256 bit encryption. The process of obtaining an SSL Certificate starts with the generation of Certificate Signing Request (CSR). This request contains information that identifies your organization and domain. It is generated using encrypted text and contains the information which is sent to the Certificate Authority. Once a CSR and key are generated and paired by the server that CSR and key are sent to a Certificate Authority. The Certificate Authority verifies the identification contained in the CSR and once verified issues the digital certificate with the electronic signature of the Certificate Authority. This certificate binds with the Certificate authorities trusted root certificate. Once this process is complete the secure website is able to function using the secure SSL/TSL transportation layer.

**Conclusion:**

Cryptography encompasses some of the most important protocols required to keep digital information secure. The exploitation of secure data such as mobile device location services, shared confidential data sets, and secure communications over the SSL/TSL transport layer can lead to devastating consequences capable of effecting a users physical security, health, identity, ad financial information, and device security. Cryptography effects personal, corporate, and national security and encrypting data is an absolute must for secure communications and the protection of data at rest. In some cases, as with iOS 13 location services, exact cryptographic protocols are not publicly available. The shielding of specific encryption details makes it more difficult for attackers to exploit known vulnerabilities and even more difficult for them to probe for new ones. In other cases such as with Googles Private Join and Compute software, security details may be open source yet still designed to exclude known vulnerabilities allowing for secure communications. With regards to webpage certificates, there is a combination of known and unknown information. A webpage certificate contains a public key however the certificate itself links with the Certificate Authorities private trusted root certificate. These various techniques combined allow for securely traversing a dangerous digital environment.

**Resources:**

(n.d.). Retrieved from <https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_71/rzahu/rzahudigsig.htm>

(n.d.). Retrieved from <https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_71/rzahu/rzahurzahu02mcertificateauthority.htm>

Google. (2019, August 5). google/private-join-and-compute. Retrieved from <https://github.com/google/private-join-and-compute>

Greenberg, A. (2019, June 6). Apple's 'Find My' Feature Uses Some Very Clever Cryptography. Retrieved from <https://www.wired.com/story/apple-find-my-cryptography-bluetooth/>

Helping organizations do more without collecting more data. (2019, June 19). Retrieved from <https://security.googleblog.com/2019/06/helping-organizations-do-more-without-collecting-more-data.html>

Home. (n.d.). Retrieved from <https://www.ssh.com/pki/>

Introduction. (n.d.). Retrieved from <https://homomorphicencryption.org/introduction/>

macOS Catalina. (n.d.). Retrieved from <https://www.apple.com/macos/catalina/>

Pinkas, B. (2015). Private Set Intersection. Retrieved October 4, 2019, from <https://cyber.biu.ac.il/wp-content/uploads/2017/01/15.pdf>

Set up Find My on your iPhone and other devices. (2019, September 19). Retrieved from <https://support.apple.com/en-us/HT210400>

TucakovDejan, D., & Dejan. (2019, September 15). OpenSSL Tutorial: How Do SSL Certificates, Private Keys, & CSRs Work? Retrieved from <https://phoenixnap.com/kb/openssl-tutorial-ssl-certificates-private-keys-csrs>

Understanding Website Certificates: CISA. (n.d.). Retrieved from <https://www.us-cert.gov/ncas/tips/ST05-010>

What Is Cryptography? (n.d.). Retrieved from <https://www.livescience.com/65648-cryptography.html>