A Comparison of Modern Symmetric and Asymmetric Cryptographic Protocols

CSIS 463

Professor Schall

James Riley Dorough

Liberty University

January 21st, 2021

**Introduction**

Securing information has been a critical need for humanity since the birth of stored information. Conflict, malintent, and theft are just a few of the major proponents that drive the need for the privacy of information. An added layer of this is the transportation of data. While the information may be safe in human-readable plaintext form if it is locked away from prying eyes. The need to transport information between entities makes the challenge of securing this information much harder. The advent of digital infrastructure provides yet another challenge to keeping data safe as malicious actors attempt to breach all current security methods. Using modern capabilities such as better processing power, faster arithmetic logic units (ALU) on central processing units (CPU), and optimized mathematic algorithms allows for much more complex security algorithms to be created and commercially available.

Of the modern systems of security, none are as well-known and universally implemented as encryption systems. While they originally were created in mechanical form, modern technology allows for highly advanced, digital, mathematical systems to encrypt and decrypt data efficiently. There are two main standards of encryption protocol accepted as standard practice today. These are symmetric and asymmetric encryption. They are vastly different in operation, complexity, speed, and application. This document outlines the basis of encryption, the differences between symmetric and asymmetric protocols, how these protocols are used today to improve security, a brief outline of the history of how these systems evolved to their current standard, and some rising threats to cryptography.

**Symmetric Overview**

Symmetric encryption is a relatively lightweight protocol to implement in a system. Symmetric encryption protocols are far faster than asymmetric protocols. This is due to the symmetric algorithm being much less complex than asymmetric. The math to encrypt and decrypt information using a single secret key is much simpler than the math required to compute and agree on shared keys. Thusly the symmetric protocol can execute faster (Cyware Hacker News, 2020). Because of symmetric encryption’s lower overhead, we often find it coupled with asymmetric encryption software. You can imagine this as an aspect to authentication for a live session where gaining initial validation would require a process to securely start the asymmetric protocol while guaranteeing security from the beginning. There are many protocols currently employed today. Some commonly well-known and used symmetric encryption algorithms are the Advanced Encryption Standard (AES), Blowfish, Twofish, Rivest Cipher (RC4), and Data Encryption Standard (DES) (Encryption Consulting, 2021). These protocols are often used for initial validation to hand off to an Asymmetric Protocol.

**Asymmetric Overview**

Asymmetric encryption is much more complex and recourse intensive than symmetric. It requires two entities to compute and share encrypted keys in a way that an outside, third party is unable to view. The problem of authentication is mitigated by implanting pairs of keys per user to be encrypted by another user’s public key, such that the receiving user can decrypt the incoming message with their secret key (Farah, 2012, p. 121). Asymmetric encryption is one of the most used encryption frameworks. Some commonly well-known and used asymmetric encryption algorithms are the Elliptic Curve Digital Signature Algorithm (ECDSA), Rivest-Shamir-Adleman (RSA), Diffie-Hellman, and Pretty Good Privacy (PGP) (Encryption Consulting, 2021).

**Encryption’s Role in Security**

As has been made clear by now, encryption is heavily for digital security methods. One frequently used, but unknown by most of its users is the Windows authentication utility Kerberos. Kerberos uses both Symmetric and Asymmetric encryption in its authentication services (Walker, 2019, p. 214). Of these services, a few commonly implemented ones are Secure Shell (SSH), Post Office Protocol (POP), Simple Mail Transfer Protocol (SMTP), Samba, and Active Directory. The main reason for Kerberos’ prevalence is its use of a layered authentication approach. The client requests a ticket from the key distribution center (KDC). The AS responds to the client system with a hashed version of the user’s stored password known as the ticket-granting ticket (TGT). Since the TGT is the client’s hashed password, there should be no problem decrying the remaining secret. This is an example of symmetric encryption in this stage of Kerberos (Walker, 2019, p. 214). The client then sends the previously extracted session key (SK1) and TGT back to the ticket-granting service (TGS). This authenticates the user after the TGS validates that the same client that made the initial request is the same client that sent the TGT back to the system with the same timestamp (Simplilearn, 2021). If all previous steps have been completed, the TGS will send a second session key to both the client and the requested server for the client to interact with. The client receives a packaged network address, timestamp, and new session key (SK2). All these information points are encrypted using the original SK1. The target server uses its secret key to decrypt the service ticket and recover the SK2 the target server then uses the SK2 to decrypt the authenticator and perform validation checks against the client (Simplilearn, 2021). These final steps between the TGS and the requesting client are initially symmetric. However, after enough information has been securely shared, the system can use asymmetric encryption to encode the other system’s information without requiring the initial pre-shared key.

**A Brief History of Encryption**

Understanding the birth and evolution of cryptographic protocols, tools, and implications is useful for understanding how the current stands came to be. While the need for data encryption methods has remained persistent since the invention of long-term information storage the algorithms and systems to accomplish this security have continuously been improved. In Simmons’ work, he outlines three major phase changes of cryptographic operations. These classifications are manual cryptography, electromechanical cryptography, and digital cryptography. Of these, modern methods are the most optimal and provide the highest complexity. The path which led to this ability today is critical to understand when focusing on the logic and math that supports such encryption. Originally, systems relied on primary algebra to alphabetically shift information. As their development progressed, humanity began improving methods to strengthen the security of information. This eventually took the form of mechanical tools used to produce scrambled messages which required a key to decode the info (Simmons, 2016). From here as electronics improved, chips using more advanced math were able to secure information at the speed of light and thusly encrypt much larger datasets than ever before. In the technology boom, new standards of encryption were born. This includes the symmetric and asymmetric methods we commonly use today which can encrypt entire data centers with ease (Simmons, 2016).

**Threats to Encryption**

The rise of quantum computing becoming feasible to scale has proved a threat to cryptographic functions as we understand them today. However, I first must explain that the buzz or interest surrounding quantum is grossly misguided and uninformed. Quantum computing is not the end-all-be-all to all computing problems. It is not just a leap in performance for all problems. Instead, quantum computing applies to a different realm of problems. The delineation is known as classical problems which current computers can solve and quantum problems which operate on different physical properties allowing solutions to specific problems should a quantum algorithm exist for that problem (Bayerstadler). Because of this, a specific quantum algorithm can crack some encryption protocols within a reasonable timeframe.

**Conclusion**

Encryption is immensely important for data security in today’s industry. It has progressed through three various stages of evolution to become a highly efficient digital product included in nearly all digital and information systems. Both symmetric and asymmetric protocols offer vastly different benefits to security and operate at different levels of complexity. Symmetric encryption is simple but allows for third-party interference. Asymmetric is more secure and allows data to remain encrypted from an outside perspective.

**References**

Bayerstadler, A., Becquin, G., Binder, J., Botter, T., Ehm, H., Ehmer, T., Erdmann, M., Gaus, N., Harbach, P., Hess, M., Klepsch, J., Leib, M., Luber, S., Luckow, A., Mansky, M., Mauerer, W., Neukart, F., Niedermeier, C., Palackal, L., . . . Winter, F. (2021). Industry quantum computing applications. *EPJ Quantum Technology*, *8*(1), 1–18. https://www.proquest.com/docview/2597014462?pq-origsite=summon&accountid=12085

Cyware Hacker News. (2020, February 22). *Exploring the Differences Between Symmetric and Asymmetric Encryption*. Cyware Labs. Retrieved January 21, 2022, from https://cyware.com/news/exploring-the-differences-between-symmetric-and-asymmetric-encryption-8de86e8a

Encryption Consulting. (2021, May 20). *Symmetric vs Asymmetric Encryption*. Encryption Consulting | Education Center. Retrieved January 22, 2022, from https://www.encryptionconsulting.com/education-center/symmetric-vs-asymmetric-encryption/

Farah, S., Javed, Y., Shamim, A., & Nawaz, T. (2012, December). An experimental study on performance evaluation of asymmetric encryption algorithms. In *Recent Advances in Information Science, Proceeding of the 3rd European Conf. of Computer Science,(EECS-12)* (pp. 121-124).

Simmons, G. J. (2016, August 17). *cryptology*. Encyclopedia Britannica. Retrieved January 22, 2022, from https://www.britannica.com/topic/cryptology

Simplilearn. (2021, December 15). *What Is Kerberos, How Does It Work, and What Is It Used For?* Https://Www.Simplilearn.Com/What-Is-Kerberos-Article. Retrieved January 23, 2022, from https://www.simplilearn.com/what-is-kerberos-article

Walker, M. (2019). *CEH Certified Ethical Hacker All-in-One Exam Guide, Fourth Edition: Vol. 1.0* (4th ed.). McGraw Hill.