By: Erik Buschardt, Summer 2016 Term

Introduction: The Evolution of Cryptography

The study of codes or secret messages (Greek: "kryptos"), and the art of writing and solving them ("graphein", per Merriam Webster), has intrigued humankind for millennia, and remain a vital part of communication when keeping information classified from others as appropriate, and in any relative context.

This paper will explain various topologies, technologies and techniques used both in the past as well as present for military and civilian use, advantages and disadvantages of each, in addition to any best-practices arising therefrom.

Differences between Encryption from the 1930's vs. today

Qualitatively speaking, principal differences between how messages were encrypted in the 1930s and 1940s vs. how messages are encrypted for transmission today, vary only in the technologies used, not necessarily in the techniques. As the mathematics became more sophisticated, computers were of course put into use upon their initial invention and development, to assist in the development of higher-end mathematics for the sophistication of the encryption process.

With the invention of the Enigma machine, the German war machine went into full throttle, overconfident of their abilities until their successful decryption by Allied forces during World War II. The mathematical techniques used are fascinating still to this day, and various emulators

demonstrating the technology are widespread and available for public examination and enjoyment.

In contrast, as for the techniques used, one similarity between the WWI and WWII era that I have noticed is the language barrier. As notable as the Navajo effort was between 1942 and the Vietnam Era, linguistic barriers between lesser-known dialects around the world remain, (Eastern African, Slavic, Nordic or Mesoamerican to name but a few examples). As the Navajo example set precedent with the linguistic aspects of encryption used in a major world war, so can we expect our next world war to include any number of these lesser known dialects and languages as part of the encryption process for military strategy and success. (Singh, 191-201)

FIPS

The Federal Information Processing Standards are a set of criteria developed by the National Institute of Standards for Technology (NIST), the most important of which is FIPS 140 because that is the standard used as a benchmark for encryption products for sale to the United States Government. Other FIPS standards include #140-2, "Security Requirements for Cryptographic Modules", #186-2, "Digital Signature Standard including Elliptic Curve Digital Signature Algorithm (ECDSA)" and #190 "Guideline For The Use Of Advanced Authentication Technology Alternatives". (FIPS Validation: What is it?)

For encryption purposes, the standard bearer remains FIPS 140-2, introduced in May of 2001 (FIPS 140-1 was introduced in January of 1994 and the working draft of FIPS 140-3 is still under

consideration as of September of 2009). Therefore the current production version of 140-2 has four levels of protection requirements. Level 1 imposes minimal requirements with regards to production-grade software. Level 2 includes a requirement for role-based authentication methods and evidence for physically tampering with the product. Level 3 goes beyond this, adding identification-based authentication. Finally, Level 4 adds a final layer of physical security requirements as well as a robustness against environmental threats. (Storage for Spies)

However, unless you are using a government computer, or designing an encrypted system for sale or use by the federal government, it is not recommended to use this FIPS standard on standalone or enterprise-level machines unless required. The reasoning for this is because enabling FIPS mode in Windows forces Windows to utilize only FIPS-validated cryptography, and disregard all else. In fact, some retail-level applications will require switching off or disabling FIPS mode in order to function properly. (Margosis, A)

DES

The Data Encryption Standard, first published in May of 1973, was developed by IBM for use government-wide for the purpose of encrypting and storing unclassified, sensitive information. During this development process, it is disputed that the NSA tampered with what are called "S-boxes" or substitution boxes, where the module to implement the substitution algorithm is housed. Eventually, an agreed-upon key length of 56 bits was agreed upon. (Johnson, p.232)

With the DESCHALL Project, breaking DES is now not hard to do, and as such, Triple-DES or 3DES is the current successor to DES (as of 1998), applying the DES standard three times for each block of data of 64 bits each. As a matter of interest, the RIVYERA parallel architecture project broke 56-bit DES in less than one day. (Break DES)

AES

The symmetric Advanced Encryption Standard, (or "Rijndael" as it was first known as), was based on an encryption standard of 128 bits per block size, with a key length of up to 256 bits. Developed by Vincent Rijmen and Joan Daemen (hence the wordplay for the original nomenclature) and first published in 1998, it became a successor to DES in 2002, after becoming approved for use by the Department of Commerce. (Singh, 250-1)

Full Drive Encryption

The theory behind Hardware-based Full Disk Encryption (FDE) includes a tamper-resistant case wherein the drive is housed, as well as an encryptor bridge and chipset (BC) placed between the CPU and drive, encrypting the stream of data for each sector written. This FDE approach is transparent to the user, but will appreciably slow the bootup process.

Vulnerabilities to FDE encryption include the sleep mode, where it has been demonstrated that as the drive powers down, the encryption password remains in memory so that the drive can be resumed without requesting the password. A hacker need only gain access to the memory via extension cables to the drive. Additionally, the drive's firmware needs to be verified authentic

from the Original Equipment Manufacturer (OEM), otherwise any data sent to that drive, encrypted or not, will be sent to the third party - a classic middleman attack. (Zetter, Kim)

Other encryption methods and technologies

Other encryption methods include a factorization of a product of two large prime numbers, as developed by Ron Rivest, Adi Shamir, and Leonard Adleman (RSA, 1977), as well as OpenPGP (and it's open-source equivalent entitled GNU Privacy Guard (GnuPG) for use with the GNU General Public License with respect to secure email messaging.

Various wireless standards have come and gone over the years, including Wired Equivalent Privacy (WEP, 1997), superseded by Wi-Fi Protected Access (WPA, 2002), in addition to the FIPS government standard as previously mentioned.

Conclusions

As we can see from the above, various methods of securing information and data exist, from wireless means to network topologies to the hard drive itself, to the encryption of the data itself, or a combination of any of these methods. It will of course be up to the organization to determine cost and resource factors when implementing a customized solution, however one fact remains clear: the trendline of complexity used in the encryption will only increase going forward.

References

Break DES in less than a single day. (n.d.). Retrieved June 28, 2016, from http://www.sciengines.com/company/news-a-events/74-des-in-1-day.html?eab1dd0ce8f296f6302f76f8761818c0=0b59c5b91984fe01986ef3bbc6de9871

cryptography. 2016. In Merriam-Webster.com. Retrieved June 30, 2016, from http://www.merriam-webster.com/dictionary/cryptography

FIPS Validation: What is it? (n.d.). Retrieved June 28, 2016, from https://www.certicom.com/index.php/fips-validation-what-is-it

Johnson, Thomas R. (2009-12-18). "American Cryptology during the Cold War, 1945-1989.Book III: Retrenchment and Reform, 1972-1980, page 232" (PDF). National Security Agency. Retrieved 2016-06-16

Margosis, A. (2014, April 7). Why We're Not Recommending "FIPS Mode" Anymore. Retrieved June 28, 2016, from https://blogs.technet.microsoft.com/secguide/2014/04/07/why-were-not-recommending-fips-mode-anymore/

Navajo Code Talkers: http://navajocodetalkers.org/ (Accessed 2016-06-23)

Singh, S. (2000). *The Code Book: The Science of Secrecy From Ancient Egypt to Quantum Cryptography*. Anchor Books.

Storage for spies: How the FIPS standard makes data extremely hard to steal. (n.d.) *PC World*. Retrieved June 28, 2016, from http://www.pcworld.com/article/2846653/storage-for-spies-how-the-fips-standard-makes-data-extremely-hard-to-steal.html

Zetter, Kim (2015-02-22). *"How the NSA's Firmware Hacking Works and Why It's So Unsettling"*. Wired.