# Malware and Encryption

David A. Wagle

School of Business, Northcentral University TIM-8301: Principles of Cybersecurity

Dr. Bill Souza May 9,2021

# Malware and Encryption Malware

Malware is nearly as old as the internet itself. In 1988, the internet consisted of only a few 10s of thousands of hosts (Zimmermann & Emspak, [2016),](#_bookmark23) the htttp protocol and the World Wide Web did not yet exist, and most users still were associated to academic institutions. On November 2, 1988, roughly 10% of those hosts began to act strangely.

Robert Morris, Jr., who is now a respected computer science professor at MIT but was then a graduate student, had either accidentally or on purpose released the first internet “worm” a program that replicated itself, then sought out new hosts to infect, spreading its way across the nascent network (Zittrain, [2008).](#_bookmark24)

The worm was able to spread easily because controls where weak. Indeed, only three controls existed as a practical matter. First, there were ethical norms to not harm other people’s equipment. Second the systems were built and staffed by professionals tho tended to keep them patched and configured properly. Third, malware lacked a business model (Zittrain, [2008).](#_bookmark24) Today,as Zittrain notes, all of this is no longer the case. Most devices connected to the network are owned by average people with no formal training in system maintenance and management. Malware developers have found multiple routes to profitability from directly scamming people to engaging in corporate espionage for hire. Finally, black-hat hacking has developed a following where the ethics to not harm others equipment is not a primary motivator of behavior. For these reasons, organizations have become aware of the need to have tools and techniques and trained professionals ready to prevent and respond to malware attacks.

# Snort

One tool that is used quite frequently by large organizations to address the concern

of malware is Snort. Snort is an open-source intrusion detection system that is maintained by Cisco SYstems, Inc. As an open source project, anyone in the world can contribute to

Snort development. What makes Snort so powerful is that it uses rules rather than signatures to detect intrusion attempts. A signature looks for the specific behavior of a particular piece of malware. A rule, by contrast, looks for characteristic behaviors of malware. This allows Snort to detect 0-day attacks that do not yet have signatures developed (Cisco, [20](#_bookmark3)21).

Because Snort can both log network packets as well as perform rules based analysis on the packets, it is also possible to connect machine learning systems to the Snort logs to enhance the detection of intrusion attempts on the network. Complex analytical tools such as n-gram analysis and clustering algorithms can combine with other methods to achieve detection rates of 90% or better, even for new attacks (Arra & Rekha Devi, [2021;](#_bookmark0) Khammas et al., [2019).](#_bookmark8)

Snort thus provides several capabilities to an organization. A company can use Snort to prevent intrusions in the first place for the vast majority of malware attacks. Secondly, the company can use Snort to generate an alert to a security team when a suspected attack is initiated successfully. This will allow IT security experts to begin work on remediation as early as possible. Finally, by logging network traffic and classifying that traffic, Snort allows forensic investigations after the fact to determine how an attack was initiated and proceeded. This provides the organization the ability to learn from each successful attack and to improve the organizations ability to both prevent and respond to similar threats in the future.

# Solarwinds Patch Manager

Along with human engineering, poorly patched machines are one of the top ways attackers can obtain unauthorized access to a system (Security Intelligence, [2021).](#_bookmark17) Poor patching practice is such an important attack vector the third and fourth most exploited vulnerabilities in 2020 where Apache Struts exploits where patches have been available for 15 and nine years respectively. Part of the difficulty of patch management lies in the fact

that our networks are built on a heterogeneous collection of vendor products. Collecting and analyzing the information necessary to determine which patches are needed from multiple vendors is a complex and thankless task.

To address this problem several companies, including Solarwinds have introduced patch management tools that make the job easier (Solarwinds, [2021).](#_bookmark18) This product allows an administrator to easily identify critical patches based on the actual environmental configuration from a dashboard. The necessary patches can be automatically located and downloaded from the various vendors securely. Patching can often be automated and scheduled based on the criticality of the vulnerability the patch addresses. The important difference compared to services like Windows Server Update is that Solarwinds can know what third-party software is being used on a system and can patch those vulnerabilities as well.

This system allows a network administrator to ensure that servers and workstations using Microsoft Windows as the base OS are patched consistently. Further, patch histories can be recorded, reports can be created, and the data can be integrated into other IT Service Management tools such as the rest of the Solarwinds products.

# Review of Encryption

Cryptography is an important component of the IT security stack. In a more and more connected world, it is important to not only understand best practices with regard to encryption, but to recognize that many devices are being marketed and sold without adhering to these practices. For example, researchers have found that some hubs in the IoT space do not encrypt device messages, violating best practices (Momenzadeh et al., [2020).](#_bookmark13) When selecting systems to integrate into the IT environment of our company, it is necessary to fully examine if devices adhere to best practices, including cryptography.

While cryptography is becoming less important over the years due to the rise in the success of malware attacks (Green, [2014),](#_bookmark7) and will likely cease to be a major consideration at some

future point (Leetaru, [2019;](#_bookmark9) Leyden, [n.d.),](#_bookmark10) that time is not here yet. However, it should be remembered that encryption is only part of the security environment, and by itself is not likely to provide much in the way of protection to an organization (Dingman et al., [2018).](#_bookmark5)

Confidentiality is an important internal and external security requirement.

Encryption is central to confidentiality as it ensures that people who do not have the access key to view data are not able to see that same data (Xu & Zhou, [2021).](#_bookmark21) It is important to note that encryption is not free, and while it would be ideal to have all data encrypted, it is the case that encryption has a performance cost that can impact user experience (Fujdiak et al., [2019).](#_bookmark6) Therefore it is important to use cryptography prudently to both ensure confidentiality and the user experience. There is ample advice available on how to consider the trade-offs between encryption and performance (Martin, [n.d.).](#_bookmark11)

# Types of Encryption

There are primarily four types of encryption which exist on two dimensions. These dimensions are binary “yes/no” conditions and are not sliding scales.

The first dimension is the one of symmetry. An encryption algorithm is symmetric if the same key is used to both encrypt and decrypt the content. An encryption algorithm is asymmetric if different keys are used to both encrypt and decrypt the content (Cloudfalre, [n.d.).](#_bookmark4)

Asymmetric algorithms are useful for allowing someone else to initiate an encrypted conversation. The key-pair can be thought of as a private key component that must be kept secret and secure, and a public key component that can be broadly shared. Anyone with the public key can encrypt a message that the holder of the private key can read.

This is an extremely important property for things such as messaging systems or web traffic. However, it is un-necessary complexity for things like storage systems where the same entity will be both encrypting and decrypting the data.

The second dimension is the one of directionality. An encryption algorithm is

bidirectional if data can be both encrypted and decrypted. An algorithm is uni-directional if data can only be encrypted, but not the process is not reversable. This latter condition has come to be known as “hashing” and is often thought of as separate from encryption.

However, we still talk about “encrypting passwords” and most password storage is uni-directional (SSL Store, [2018).](#_bookmark19)

# Where to use Encryption

***Data Storage***

Data at rest, that is, on storage medium such as disk or tape, should be encrypted at least once, and often twice. The first level of encryption should be device level encryption. Full disk encryption ensures that all of the data on the device is encrypted, and can only be read by someone who has the password to decrypt the device (Mateaki, [n.d.).](#_bookmark12) This helps ensure the security of data even if a device is lost and physically ends up in an attackers hands. Full disk encryption can be symmetric and obviously must also be reversable.

Data should be encrypted on the system, even if the system is utilizing device encryption when the data is not considered public data. This allows control of confidentiality by ensuring only those with proper access credentials can view the data.

One example of this is system passwords. System passwords are often stored on a device either in cache memory or on disk so that access rights can be checked. It is important that anytime a password is stored it is stored encrypted. Password encryption is generally symmetric and one-way. That is, there is not a separate decryption key, but the algorithm is not always reversable (TLDP, [2021).](#_bookmark20) An entered password need only be checked against the resulting hash value, and if they match, then the password entered is likely the same as the true password.

Database data should also be encrypted in storage to ensure that confidentiality is retained. Only people with proper access to the data should be able to read it, not just anyone with access to the system the data is stored on. Database encryption should be

asymmetric and reversable. It should be asymmetric so that distribution of the public key will allow different data owners to enter data into the system without reading other people’s entries into the same system. And it generally must be reversable as a typical database includes situations where data needs to be read from the database and displayed to the user (netlib Security, [2016).](#_bookmark15)

Due to the rise in cloud computing use, which often means data is duplicated around the globe, database column level encryption is more and more important. Data should be decrypted at the point of use and not in-transit. This is because the company can not always control the routing of data around the globe, and man-in-the-middle attacks may be possible at any routing point in transit. All data that the company uses must be categorized for an appropriate level of encryption for this reason.

# Data Transit

Data in motion over the internet should also be encrypted for security (Bahri et al., [2018).](#_bookmark1) Again, there are multiple levels of encryption. All network communication streams should be encrypted, just as devices are encrypted. This is especially true for any communication streams that will exist external to the company. This includes company owned cloud assets that are stored or accessed via a cloud provider.

Typical connection level encryption is achieved through the SSL/TLS protocol utilized by web services like HTTPS (Oltsik, [2015).](#_bookmark16) This security protocol is an asymmetric and reversable protocol. The asymmetry allows anyone with the public key to attempt to connect to the web service and it must be reversable so that the systems can understand the data flows involved.

More secure communication channels can add on-top of this encryption. For encryption between corporate owned systems that traverse outside of the company and which carry highly sensitive data, hardware based encryption devices should be considered (Zybersafe, [n.d.).](#_bookmark25) These devices provide encryption at the layer-2 of the network stack,

which is below the TCP/IP protocol. This makes it extremely difficult for man-in-the-middle attacks to succeed.

As noted in the discussion about data storage, data that should be encrypted in the database or files should be decrypted at the user-end of the application stack and not in transit. This can complicate web-client design, but is an important aspect of secure communications.

# International Data

The European Union’s General Data Protection Regulation (GDPR) was updated in 2018. This set of regulations impose significant penalties on companies that are shown to fail to adhere to best practices for protecting user data. The compliance requirements include addressing legacy systems that may be utilizing no or very weak cryptographic functions to protect user data and user access credentials (Blue & Furey, [2018).](#_bookmark2) Companies that will be doing business in the European Union must consider the demands of the GDPR on system architecture. Failure to do so upfront can have severe financial impacts on the company, either in the form of fines and penalties or in the form of costly

re-architecture efforts (Yuan & Li, [2019).](#_bookmark22)

# Implementation Considerations

Following best practices for when to encrypt data and which data to encrypt is only part of a solid cryptographic strategy. Companies need to be aware of what specific libraries and tools are used to provide their cryptographic solutions. Not all implementations of cryptography are robust. Doing cryptography well is often complex and errors or omissions in implementation details can result in serious weaknesses of the system. For example, the “heartbleed” bug in the OpenSSL library’s TLS/DTLS implementation allowed the leakage of primary key, secondary key, and protected content from the connection. Any organization utilizing the vulnerable version had to upgrade all

systems which were built against those libraries. Failure to do so would result in a continuing on-going vulnerability (NA, [n.d.).](#_bookmark14)

# Actions

In light of the current state of cybersecurity, staying on top of best practices is a critical step in ensuring both compliance to legal standards such as the GDPR as well as compliance to internal policies and corporate data strategy. Both the legal and technical framework of cybersecurity are ever-evolving. As such it is recommended that the following steps be implemented.

1. Establish policies for documenting corporate data collection and properly categorizing data for encryption standards
2. Establish policies for auditing system and network compliance to encryption standards and best practices
3. Establish policies for collecting and documenting what encryption tools and libraries are used in all applications
4. Establish policies for ensuring patching and updating of all encrypt tools and libraries used in all applications
5. Establish regular reviews of encryption policies to ensure continued adherence to both legal standards and best practices

# References

Arra, S., & Rekha Devi, K. (2021). Evaluation, prediction and implementation patterns of network traffic malware using machine learning. *Materials Today: Proceedings*. <https://doi.org/10.1016/j.matpr.2021.01.795>

Bahri, L., Carminati, B., & Ferrari, E. (2018). Privacy in web service transactions: A tale of more than a decade of work. *IEEE Transactions on Services Computing*, *11* (2), 448–465. <https://doi.org/10.1109/TSC.2017.2711019>

Blue, J., & Furey, E. (2018, June). A novel approach for protecting legacy authentication databases in consideration of gdpr, In *2018 international symposium on networks, computers and communications (isncc)*. 2018 International Symposium on Networks, Computers and Communications (ISNCC). <https://doi.org/10.1109/ISNCC.2018.8531022>

Cisco. (2021). *Snort - network intrusion detection & prevention system*. Retrieved May 8, 2021, from <https://www.snort.org/>

Cloudfalre. (n.d.). *What is encryption? | types of encryption*. Cloudflare. Retrieved May 9, 2021, from <https://www.cloudflare.com/learning/ssl/what-is-encryption/>

Dingman, A., Russo, G., Osterholt, G., Uffelman, T., & Camp, L. J. (2018). Poster abstract: Good advice that just doesn’t help. *2018 IEEE/ACM Third International Conference on Internet-of-Things Design and Implementation (IoTDI),*

*Internet-of-Things Design and Implementation (IoTDI), 2018 IEEE/ACM Third International Conference on, IOTDI*, 289–291. <https://doi.org/10.1109/IoTDI.2018.00044>

Fujdiak, R., Blazek, P., Apvrille, L., Martinasek, Z., Mlynek, P., Pacalet, R., Smekal, D., Mrnustik, P., Barabas, M., & Zoor, M. (2019). Modeling the trade-off between security and performance to support the product life cycle. *2019 8th Mediterranean Conference on Embedded Computing (MECO), Embedded Computing (MECO),*

*2019 8th Mediterranean Conference on*, 1–6. <https://doi.org/10.1109/MECO.2019.8760043>

Green, A. (2014, January 21). *Cryptography may not be dead, but it is on life support*.

Inside Out Security. Retrieved May 9, 2021, from <https://www.varonis.com/blog/cryptography-may-dead-life-support/>

Khammas, B. M., Ismail, I., & Marsono, M. N. (2019). Pre-filters in-transit malware packets detection in the network. *Telkomnika*, *17* (4), 1706–1714. <https://doi.org/10.12928/TELKOMNIKA.v17i4.12065>

Leetaru, K. (2019, July 26). *The encryption debate is over - dead at the hands of facebook*.

Forbes. Retrieved May 9, 2021, from [https://www.forbes.com/sites/kalevleetaru/2019/07/26/the-encryption-debate-is-](https://www.forbes.com/sites/kalevleetaru/2019/07/26/the-encryption-debate-is-over-dead-at-the-hands-of-facebook/) [over-dead-at-the-hands-of-facebook/](https://www.forbes.com/sites/kalevleetaru/2019/07/26/the-encryption-debate-is-over-dead-at-the-hands-of-facebook/)

Leyden, J. (n.d.). *Prepare for ’post-crypto world’, warns godfather of encryption*. Retrieved May 9, 2021, from <https://www.theregister.com/2013/03/01/post_cryptography_security_shamir/>

Martin, L. (n.d.). *Encryption won’t affect app performance—if you do it right*. TechBeacon.

Retrieved May 9, 2021, from [https://techbeacon.com/security/relax-good-](https://techbeacon.com/security/relax-good-encryption-practices-wont-affect-app-performance) [encryption-practices-wont-affect-app-performance](https://techbeacon.com/security/relax-good-encryption-practices-wont-affect-app-performance)

Mateaki, G. (n.d.). *Securing mobile devices with mobile encryption*. SecurityMetrics.

Retrieved May 9, 2021, from

<https://www.securitymetrics.com/blog/securing-mobile-devices-mobile-encryption> Momenzadeh, B., Dougherty, H., Remmel, M., Myers, S., & Camp, L. J. (2020). Best

practices would make things better in the iot. *IEEE Security Privacy*, *18* (4), 38–47. <https://doi.org/10.1109/MSEC.2020.2987780>

NA. (n.d.). *Heartbleed bug*. Retrieved May 9, 2021, from <https://heartbleed.com/> netlib Security. (2016, January 21). *Differences between whole database and column*

*encryption*. NetLib Security. Retrieved May 9, 2021, from

[https://netlibsecurity.com/white-papers/differences-between-whole-database-and-](https://netlibsecurity.com/white-papers/differences-between-whole-database-and-column-encryption/) [column-encryption/](https://netlibsecurity.com/white-papers/differences-between-whole-database-and-column-encryption/)

Oltsik, J. (2015, February). *Network encryption and its impact on entrprise security*.

Enterprise Security Group. Retrieved May 9, 2021, from [https://docs.broadcom.com/doc/esg-report-network-encryption-and-its-impact-on-](https://docs.broadcom.com/doc/esg-report-network-encryption-and-its-impact-on-network-security) [network-security](https://docs.broadcom.com/doc/esg-report-network-encryption-and-its-impact-on-network-security)

Security Intelligence. (2021, March 10). *Top 10 cybersecurity vulnerabilities of 2020*.

Security Intelligence. Retrieved May 8, 2021, from <https://securityintelligence.com/posts/top-10-cybersecurity-vulnerabilities-2020/>

Solarwinds. (2021). *Patch management software - it patching guide*. Retrieved May 8, 2021, from <https://www.solarwinds.com/patch-manager/patch-management-software>

SSL Store. (2018, December 19). *The difference between encryption, hashing and salting*.

Hashed Out by The SSL Store™. Retrieved May 9, 2021, from <https://www.thesslstore.com/blog/difference-encryption-hashing-salting/>

TLDP. (2021). Password security and encryption. *The Linux Documentation Project*.

Retrieved May 9, 2021, from

<https://tldp.org/HOWTO/Security-HOWTO/password-security.html> Xu, J., & Zhou, J. (2021). Strong leakage-resilient encryption: Enhancing data

confidentiality by hiding partial ciphertext. *International Journal of Information* *Security*, *20* (2), 141–159. <https://doi.org/10.1007/s10207-020-00487-7>

Yuan, B., & Li, J. (2019). The policy effect of the general data protection regulation (gdpr) on the digital public health sector in the european union: An empirical investigation. *International journal of environmental research and public health*,

*16* (6). <https://doi.org/10.3390/ijerph16061070>

Zimmermann, K. A., & Emspak, J. (2016). *Internet history timeline: Arpanet to the world wide web*. livescience.com. Retrieved May 8, 2021, from <https://www.livescience.com/20727-internet-history.html>

Zittrain, J. (2008). Protecting the internet without wrecking it: How to meet the security threat. *Boston Review*, *33* (2), 7–13. Retrieved May 8, 2021, from [http://proxy1.ncu.edu/login?url=https:](http://proxy1.ncu.edu/login?url=https)

//search.ebscohost.com/login.aspx?direct=true&db=ofs&AN=509901577&site=eds- live

Zybersafe. (n.d.). *Zybersafe trafficcloak - network encryption hardware portfolio*. ZyberSafe.

Retrieved May 9, 2021, from <https://zybersafe.com/solutions/>