Cryptography in Modern Times

Urmila Das

Department of Computer Science, Fordham University

CISC – 3580 – Cybersecurity and Applications

Dr. Abdullah Saleh Al-Hayajneh

5/2/24

Cryptography in Modern Times

Cryptography is the practice of writing and solving codes in order to hide the true meaning of information, it is also one the strongest defenses in the arsenal of computer security protection. An important element of many computer security services and applications is the use of cryptographic algorithms. As discussed in Lecture 2, AES which stands for advanced encryption system is a symmetric algorithm meaning the sender and receiver uses the same key for encryption and decryption. AES is the standard for encrypting sensitive U.S. government data. Cryptography and cryptographic algorithms are used in real life, for example encryption can be used for emails, bank accounts, transferring money, and more. More specifically though do these encrypted algorithms keep data safe. Banking information is very sensitive and unique to every person because it is not just the account that needs safe keeping, but there are also social security numbers as well. Using online banking was a concern for people since all of that information can be at risk. This concern was surrounding the effectiveness of current cryptographic algorithms against modern cyber attacks. The effectiveness of modern cryptographic algorithms in securing sensitive information on digital platforms, for example, smartphones and banking systems, assessing their strength against evolving cyber threats and potential vulnerabilities in their implementation to determine overall security efficiency.

Literature review

There are many kinds of mobile banking applications and this is for convenience to make things easier and for the environment as well. Banks suggest for people to go paperless and it could be easier for people to have access to their important information. “However, M-banking is often conducted via unsecure wireless networks on which adversaries can use available techniques to hack into systems to steal sensitive financial information including money. From this study, we show that Advanced Encryption Standard is the most preferred standard for M-banking because there are no specific attacks against it so far. However, since technology is changing fast, Advanced Encryption Standard might not provide security in M-banking for long” (Orucho, 2023). Many cyber attacks have occurred since people have their finances online now. According to BBC “Losses from online banking fraud rose by 48% in 2014 compared with 2013 as consumers increasingly conducted their financial affairs on the internet. The rise is due to increased use of computer malware and con-artists tricking consumers out of personal details. Overall losses on UK cards from fraud totaled £479m in 2014, up 6% on 2013, according to Financial Fraud Action. The total amount of fraud is down 21% from the peak of £609.9m in 2008” (More, et al, 2015). Not only did the BBC report these findings of increased malware and attacks, but Business Insider India, Business Standard and more had similar findings.

Protection and Challenges in Banking and Messaging

Encryption and cryptographic algorithms have beneficial aspects to them as well because of data the customers have, transactions, protection against data breaches and more. The research done by Islam, Ciganek, and McCoy (2019) delves into the security landscape of mobile banking applications through a meticulous examination of academic articles, conference papers, and industry reports spanning the decade. They shed light on the critical aspects of mobile banking security, including encryption protocols, authentication mechanisms, and vulnerabilities inherent in app design and deployment. They discuss the strong algorithms such as AES and RSA that are commonly used to encrypt sensitive information between phones or tablets and the bank servers. There is also MFA which is multi factor authentication that is used heavily for anything that has sensitive data including Fordham University and other colleges for students and faculty for logging into their school accounts. However, passwords that unlock more than just one account or activity can be very dangerous and make it easier for hackers. For example, a student's Fordham account can be used to unlock their email, Blackboard, financial aid, e-bill suite which includes bank information and more. However, challenges persist in the seamless integration of these mechanisms, with usability concerns and susceptibility to social engineering attacks remaining prevalent. In addition, the adoption of tokenization and secure enclave technologies are also discussed as promising avenues to improve the security posture of mobile banking apps against evolving cyber threats.

In text messaging, there is also protection and challenges in protecting people’s information when messaging each other. One of the strongest applications in this is WhatsApp and this is due to their end to end encryption. Abdelaty, Al-Khazragy, and Fathy (2018) took surveys into the security landscape of messaging applications, mainly focusing on WhatsApp and Messenger, within the context of Egypt. They found that people trust the apps especially WhatsApp due to their end to end encryption or known as E2EE. However, many people didn’t know about encryption technologies and why it is important to people for it to be known. Moreover, there was concern among users regarding potential risks of government surveillance and interception, which alludes to the complex issue between user trust, state surveillance, and individual privacy. This is always a concern even in the United States of America due to companies like Meta and TikTok. Additionally, the study identifies potential vulnerabilities within WhatsApp's security infrastructure, highlighting the ongoing need for robust security measures and proactive efforts to address emerging threats.

Discussion

Although there is no way to know whether the encryption of certain applications and information is completely safe or unsafe. With more time, comes more technology to help with protecting users' data. The study done in 2018 led to discussion about the intricate relationship between user trust, encryption technologies, and messaging security. This is a huge debate within the technology field right now because of how data is being used against people. It is not just whether users get hacked and their information gets to one person, but people have a concern on how the government can have people's information. It is interesting that this study was done in another country, more specifically Egypt (Abdelaty, 2018). In other countries such as China, there are parts of it where many people's every move gets tracked and there are security cameras everywhere, and there is not much privacy. This happens in Palestine as well where there are checkpoints to keep track of people. The tracking makes people trust less in their government.

Work Cited

Aljawarneh, S. A. (Ed.). (2020). Online Banking Security Measures and Data Protection. Jordan University.

Wong, D. (Year of publication). Real-World Cryptography. Publisher.

Islam, M. R., Ciganek, A. P., & McCoy, S. (2019). Security of Mobile Banking Apps: A Systematic Literature Review. Journal of Financial Services Marketing.

Abdelaty, M., Al-Khazragy, H., & Fathy, N. (2018). WhatsApp and Messenger Users in Egypt: Are Their Messages Secure? Information & Computer Security

Orucho, D. O., Awuor, F. M., Makiya, R., & Oduor, C. (2015). Review of Algorithms for Securing Data Transmission in Mobile Banking.