SY401 Annotated Bibliography

***"Vulnerabilities of Near-Field Communication (NFC) Technology" By McKenzie Eshleman, Caitlynn Stringer, Ben Mclellan, Jon Robinson***

## Tag Duplication

**Saeed, Muhammad Qasim, and Colin D. Walter. "Off-line nfc tag authentication." 2012 International Conference for Internet Technology and Secured Transactions. IEEE, 2012.**
This article features the protocol for the off-line authentication of NFC tags and provides a framework, based on NFC Forum specifications, to support the authentication. The article proposes that it is based on a challenge-response protocol using public key cryptography and a PKI. In order to make the framework compatible with existing NFC Forum devices, a new tag authentication record, designed according to the NFC Data Exchange Format (NDEF), is introduced. The proposed framework successfully differentiates between legitimate and cloned tags which have sufficient resources to perform the required cryptography.

**Francis, L., Hancke, G., Mayes, K. and Markantonakis, K., 2010. On the security issues of NFC enabled mobile phones. International Journal of Internet Technology and Secured Transactions, 2(3/4), p.336.**
This article focuses on widespread security issues that are seen with NFC on enabled smartphones, which can be useful for further research of other vulnerabilities. The potential misuse of both the token emulation and the contactless reader functionality provided by NFC mobile phones. It also mentions Cloning and Skimming Attacks, which are described as two of the most prominent attacks on contactless systems. The articles goes into detail about how to accomplish such attacks are often impractical and cost a lot in terms of the hardware required. Nevertheless, this is still a vulnerability and still does occur regardless of what it takes to carry out an attack. I think this article will be extremely useful in terms of cloning attacks, because of the extent it goes into for smartphones.

**Lehtonen, Mikko & Ostojic, Daniel & Ilic, Alexander & Michahelles, Florian. (2009). Securing RFID Systems by Detecting Tag Cloning. 5538. 291-308. 10.1007/978-3-642-01516-8_20.** Cloning of RFID tags can lead to financial losses in many commercial RFID applications. There are two general strategies to provide security: prevention and detection. The security community and the RFID chip manufacturers are currently focused on the former by making tags hard to clone. This paper focuses on the latter by investigating a method to pinpoint tags with the same ID. This method is suitable for low-cost tags since it makes use of writing a new random number on the tag's memory every time the tag is scanned. A back-end that issues these numbers detects tag cloning attacks as soon as both the genuine and the cloned tag are scanned. This paper describes the method and presents a mathematical model of the level of security and an implementation based on EPC tags. The results suggest that the method provides a potentially effective way to secure RFID systems against tag cloning.

**Tesoriero, Ricardo, and Jose A. Gallud 2018. "Software Architecture and Framework to Develop NFC-Based Applications" Sensors 18, no. 8: 2654. https://doi.org/10.3390/s18082654**
This article addresses a range of varying kinds of architectures to implement NFC technology. An application specific model is proposed to help developers secure their NFC technology. It is mentioned that tag identification can be duplicated depending on their production. A comparison is drawn between ISO 14443 Type A 4-byte tags, ISO 14443 Type A 7-byte tags, and ISO 15693 tags and how they can be duplicated depending on their purpose, memory size, and encryption.

**Zanata Omayr. "How I Finally managed to clone a NFC TAG." *Medium*, Medium, 20 Dec. 2018, https://medium.com/@omayrzanata/how-i-finally-managed-to-clone-a-nfc-tag-4a9f64ef49c5**
In this article Omayr goes over how they were able to clone an NFC tag by manipulating the tag's memory.

**A, Jeremie. "The DIY Portable NFC Cloner." *Medium*, Medium, 25 Mar. 2019, https://medium.com/@lp1/the-diy-portable-nfc-cloner-1ebdecfe5f66.**

This article and video resource shows us how to create an NFC tag cloner and how to build one ourselves.

**Kassim, Jafar, and Yurii Maslyiak. *SOFTWARE FOR OBJECT IDENTIFICATION USING NFC TECHNOLOGY*. West Ukrainian National University, http://dspace.wunu.edu.ua/bitstream/316497/39130/1/4.pdf.**

The purpose of the study is to develop software for object identification using NFC Technology as an easy, fast, accurate and secure method of object identification. The purpose of the inclusion of this source is to study the research implementation that has been done with respect to tag authentication to have a better understanding of the software trying to be cloned and how to improve it to better defend against the vulnerability of tag duplication.

## Tag Erasure Retrieval Attack

**Saeed, D, Iqbal, R, Sherazi, HHR, Khan, UG. Evaluating Near-Field Communication tag security for identity theft prevention. Internet Technology Letters. 2019; 2:e123. https://doi.org/10.1002/itl2.123**

Near-Field Communication (NFC) applications are growing at a rapid pace due to their user-friendly nature and cost effectiveness. The growth of NFC applications has caught the attention of attackers who can target NFC entities (eg, tags and readers) to gain access to any stored information. NFC is a nascent technology that offers ease of use and secure communication. However, this technology can act as a doorway for major hacks, such as skimming and other identity theft problems. This article presents a technique that can still read the erased data from an NFC tag even if the tag has been erased employing conventional techniques. Furthermore, a set of recommendations is provided for the proper erasure of NFC tags to avoid leaving any traces of the erased data.

**Kamaludin, Hazalila. "Clone Tag Detection in Distributed RFID Systems." PlosOne.Org, 22 Mar. 2018, journals.plos.org/plosone/article?id=10.1371/journal.pone.0193951**.

Although Radio Frequency Identification (RFID) is poised to displace barcodes, security vulnerabilities pose serious challenges for global adoption of the RFID technology. Specifically, RFID tags are prone to basic cloning and counterfeiting security attacks. A successful cloning of the RFID tags in many commercial applications can lead to many serious problems such as financial losses, brand damage, safety and health of the public. With many industries such as pharmaceuticals and businesses deploying RFID technology with a variety of products, it is important to tackle RFID tag cloning problem and improve the resistance of the RFID systems. To this end, we propose an approach for detecting cloned RFID tags in RFID systems with high detection accuracy and minimal overhead thus overcoming practical challenges in existing approaches. The proposed approach is based on consistency of dual hash collisions and modified count-min sketch vectors. We evaluated the proposed approach through extensive experiments and compared it with existing baseline approaches in terms of execution time and detection accuracy under varying RFID tag cloning ratio. The results of the experiments show that the proposed approach outperforms the baseline approaches in cloned RFID tag detection accuracy.

## Replay Attacks

**Thammarat, Chalee, et al. "A secure lightweight protocol for NFC communications with mutual authentication based on limited-use of session keys." *2015 International conference on information networking (ICOIN)*. IEEE, 2015.**

This paper introduces new authentication techniques for NFC communication that provides mutual authentication. The mutual authentication will be between connecting devices. Mutual Authentication is a security property that prevents replay and man-in-the-middle attacks. The proposed protocols deploy limited-use offline session key generation and distribution techniques to enhance security and importantly make our protocol lightweight.

**Lu, He-Jun, and Dui Liu. "An improved NFC device authentication protocol." *Plos one* 16.8 (2021): e0256367.**

This paper focuses on the technology of asymmetric encryption algorithms, symmetric encryption algorithms, and hash functions, timestamp and survival period to improve the confidentiality, performance and security of the protocol. The symmetric encryption algorithm encrypts the transmission content, while the asymmetric encryption algorithm encrypts the shared key. By using this encryption scheme then it can help prevent replay attacks from occurring.

**Mitrokotsa, A., Rieback, M. R., & Tanenbaum, A. S. (n.d.). "Classification of RFID Attacks." 86. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.143.9601&rep=rep1&type=pdf**

This paper classifies RFID attacks, expresses their features, and offers countermeasures. The paper categorizes attacks by the layers of RFID communication: strategic layer, application layer, network-transport layer, and physical layer. Replay attack is defined and categorized as a multilayer attack. Simple yet inconvenient countermeasures include the use of timestamps, one-time passwords, and challenge response cryptography. Alternatives include RF shielding and distance restricting.

**Dafalla, Yousif & Liu, Bo & Hahn, Dalton & Wu, Hongyu & Ahmadi, Reza & Bardas, Alexandru. (2020). “Prosumer Nanogrids: A Cybersecurity Assessment.” IEEE Access. PP. 1-1. 10.1109/ACCESS.2020.3009611.**
This article is an assessment of Nanogrids or licensed platforms located in locations owned by customers that can generate and inject electricity into the power grid. In the cybersecurity assessment of the system the differences are drawn between a replay attack and a man-in-the-middle attack.

## Man in the Middle

**Akter. (2020). Man-in-the-Middle Attack on Contactless Payment over NFC Communications: Design, Implementation, Experiments and Detection. *IEEE Transactions on Dependable and Secure Computing.*, 1–1. https://doi.org/10.1109/TDSC.2020.3030213**

This article focuses on a new technique of a man in the middle attack. The new attack focuses on using a malicious card and a normal card, this malicious card can be used to change information such as payment details, personal information, and the price of payment. The only downside is that the adversary must be able to physically emplace the MITM card in between the legitimate card and the terminal, while also being able to read and communicate with both the legitimate card and the terminal throughout the communication process.

**Dreyer, Julian, Marten Fischer, and Ralf Tönjes. "NFC Key Exchange-A light-weight approach to authentic Public Key Exchange for IoT devices." *2021 IEEE 7th World Forum on Internet of Things (WF-IoT)*. IEEE, 2021.**

This article focuses on the use of digital signatures to help combat man in the middle attacks. The use of a key exchange can help with authentication, without this exploitation of the cards are simple. The article proposes a useful algorithm with a public and private key to encrypt the data and ensure secure transfers of data or payment.

## Denial of Service

**F. Fahrianto, M. F. Lubis and A. Fiade, "Denial-of-service attack possibilities on NFC technology," *2016 4th International Conference on Cyber and IT Service Management*, 2016, pp. 1-5, doi: 10.1109/CITSM.2016.7577582.**

This article focuses on the uses of denial of service attacks to exploit the vulnerabilities of NFC technology. The article uses two methods for denial of service, the first method is attacking an application technique used to make a NFC-enabled mobile phone browser could not handle when the opening a single URL which contain infinite loop, for a moment the browser opened one hundred page more and appear dialog box “browser isn't responding.” The second exploit is a developed simple app .apk which sets appname 500000+ chars in a strings.xml file. This application gives a serious impact for NFC enabled phones, where for a moment they can not respond.

***“Vulnerabilities of Near-Field Communication (NFC) Technology” By McKenzie Eshleman, Caitlynn Stringer, Ben Mclellan, Jon Robinson***

This research is to study the vulnerabilities that are present within Near-Field Communication (NFC) Technology. This stems from NFC technology becoming a growing part of today's society. With the growing industry, there exists an increasing dilemma of signals being scanned, duplicated, and collided. Our research is to help discover potential exploitable vulnerabilities that are common with NFC technology and offer suggestions for improved security.

Our research is aimed to educate and offer suggestions to improve the use of NFC technology used everyday by Civilians, Sailors, and Marines to make our fighting force more secure from the ground up. By focusing on Eavesdropping, Man in the Middle, Replay Attacks, and Tag Duplication, our goal is to provide as much information to the NFC field with suggestions on improving technology to help combat these vulnerabilities.

“***Off-Line Tag Authentication” by Muhammed Saeed and Colin Walter***

Near Field Communication (NFC), a short range wireless technology, has recently experienced a sharp rise in uptake because of its integration with smart phones. Smartphones that are enabled with NFC capabilities can retrieve information in a single touch. The tags can be used in a variety of applications, for example “smart posters, product identification, access control, etc.” The integrity of these tags are ensured by digital signatures, but this does not guarantee the legitimacy of the tags. They can be replaced with counterfeits. Our capstone focus on tag duplications is to help combat the use of counterfeit tags in the Off-Line environment.

Currently there is not a mechanism for detecting duplicated tags. In an offline environment, when there is not any shared secret between the tag and the reader, it can be extremely difficult to differentiate between a legitimate and counterfeit tag. For Off-Line Authentication there are occasions when there is no shared secret between the tag and the reader. Any reader can access the tag and read its contents. The process of authentication the tag or the reader or both in such scenarios is called off-line authentication. Normally it is just the tag that needs to be authenticated. Off-Line authentication becomes challenging in an RFID environment owing to the low computational power of RFID tags. The typical low cost tag is currently unable to perform any useful public key cryptography.

Tag authentication requires a framework that distinguishes a legitimate tag from a counterfeit tag. The counterfeit may or may not store the same data as the original. A duplicate with the same data is not desirable either. We describe such tags as a cloned tag. Examples of such scenarios are ePassports, product identification, access control, etc. A suggested approach would be to add a simple private key encryption with the tags to help with authenticating that the tag has not been duplicated.

**"Countermeasure of NFC relay attack with jamming" by S. Oh, T. Doo, T. Ko, J. Kwak and M. Hong**

Recently released smartphones are equipped with support for Near Field Communication. Near Field Communication (NFC) is a short-range contactless technology allowing smartphones to act primarily as either a reader or a token. NFC on mobile phones presents new opportunities and threats. NFC provides convenient and easier payment service. However, it is vulnerable to relay attacks. Some countermeasures are known, but there are drawbacks. In this paper we introduce NFC technology, relay attack, well-known countermeasure and relay attack case. This research proposed countermeasures to prevent NFC relay attack.

**"Secure Inductive-Coupled Near Field Communication at Physical Layer" by R. Jin and K.Zeng**

Near field communication (NFC) is widely used today in many useful applications, such as contactless payment, identification, and file exchange. Due to the limitations on computation, power, and cost of NFC devices, NFC systems often lack encryption or are weakly encrypted, leaving them exposed to security attacks. One solution for this problem is to install strong cryptographic protocols on NFC devices. However, it involves upgrading and revoking deployed NFC devices, which is costly and impractical. Moreover, encryption algorithms are usually considered expensive for resource constrained NFC devices in terms of computation overhead and energy consumption. Aiming at a solution to tackle the security threat without revoking or changing the insecure NFC devices, this paper investigates whether the recent advance of physical layer security can be applied as a means to secure NFC. A detailed analysis is performed to reveal two unique challenges brought by NFC's data transmission mechanism. A practical solution, SecNFC, through special waveform design at the initiator is proposed. Extensive simulations and concept-proof experiments are conducted to evaluate the performance of our solution. Both simulation and experimental results show that SecNFC can efficiently prevent NFC from eavesdropping with a slight and tolerable decoding performance degradation at the initiator.

## References

Saeed, Muhammad Qasim, and Colin D. Walter. "Off-line nfc tag authentication." 2012 International Conference for Internet Technology and Secured Transactions. IEEE, 2012.

S. Oh, T. Doo, T. Ko, J. Kwak and M. Hong, "Countermeasure of NFC relay attack with jamming," *2015 12th International Conference & Expo on Emerging Technologies for a Smarter World (CEWIT)*, 2015, pp. 1-4, doi: 10.1109/CEWIT.2015.7338165.

R. Jin and K. Zeng, "Secure Inductive-Coupled Near Field Communication at Physical

Layer," in *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 12, pp. 3078-3093, Dec. 2018, doi: 10.1109/TIFS.2018.2832983.