PeerJ Preprints NOT PEER-REVIEWED

Internet of Things Security: A review on the RFID contactless security protocols

Natalie Outteridge

Faculty of Science & Engineering

Manchester Metropolitan University, Manchester, UK

natalie.outteridge@stu.mmu.ac.uk

Abstract

The advancement of technology that have been produced for Internet of Things (IoT) security has grown significantly and exponentially over the years. This has caused a major impact in the world of IoT security as technological companies have to keep up with the ever-changing security protocols. The Radio Frequency Identification (RFID) technology has recently gained popularity in the world of IoT, this is due to the RFID chips involvement within credit and debit cards to allow them to become contactless. This survey will produce an in-depth discussion about the background of RFID, the relevance of RFID in today's society, related work, the advantages and disadvantages of RFID and finally a solution to the RFID contactless.

Keywords—Internet of Things (IoT), RFID, Contactless, Security, Sensor Networks, ECC-based authentication, Dual chip, chipless.

I. Introduction

Wireless Sensor Networks revolutionized the way that humans perceive and interact with their environment [1], [2]. However, this technology introduced a wide range of security threats that has not been addressed in the classical information and network security research [3], [4], [5], [6], [7], [8], [9]. Radio Frequency Identification (RFID) has exponentially and increasingly become more in-demand with major companies now incorporating RFID into their technology. RFID depends on radio waves as a communication method between the tags incorporated to the object/technology such as RFID readers to obtain or transmit data such as bank account details, names, addresses and many more. RFID was first introduced

PeerJ Preprints | https://doi.org/10.7287/peerj.preprints.26504v1 | CC BY 4.0 Open Access | rec: 11 Feb 2018, publ: 11 Feb 2018

PeerJ Preprints NOT PEER-REVIEWED

to society in the recent few years therefore becoming the most recent advancement in technology.

The first RFID technology that was created would be a pre-war listening device, this involved using antennas as a way of communicating and transmitting audio radio-waves into a small electronic device mainly used for spies in the war time. After that time the potential of RFID was spotted and more RFID technology became prevalent, the most recent ones being EAS tags which protect the merchandise in shops by using a plastic covering with an EAS tag adjusted to the top to be a deterrent to thieves, these can only be taken off by a member of staff working at the establishment. Other recent RFID technologies would be micro-chipping used to track pets locations when they have gone missing and contactless cards that have recently become a lot more popular due to the increase of RFID readers being introduced.

The rest of the paper is organised as follows: Section II presents recent advances in RFID technology. Section II reviews recent related work in the RFID domain. Section IV concludes the paper and gives future research directions.

II. Recent RFID Technology

RFID technology recently has become a major technological advancement for electronic devices produced to create an easier access to data. RFID has three important specifications that need to be encoded, these would-be RFID tags, RFID reader and back-end server [10], [11], [12], [13]. RFID tags are generally implanted into an electronic device in which contains specific numbers, this helps to clarify the details of a specific user when transmitting the data to an RFID Reader. RFID readers are mainly used as transmission device to capture the data from the tags and send them to the back-end server. The back-end server retrieves the data from the RFID reader and manages the information [10], [14] by storing it in the server. Technology in recent times depend on the three specifications due to micro-chips now being incorporated in RFID devices. Micro-chips are essentially the same as RFID tags, they both contain and transmit data to the RFID reader. However due to the costs and implementation it was decided that micro-chips would be better fitting and easier to implement rather than RFID tags. New RFID technology created with micro-chips are mainly used in society for different purposes such as micro-chipping for pets, contactless credit and debit cards to help

PeerJ Preprints | https://doi.org/10.7287/peerj.preprints.26504v1 | CC BY 4.0 Open Access | rec: 11 Feb 2018, publ: 11 Feb 2018

easy and secure payment, smart-watches and much more. This survey paper will mainly be focused on the uses of contactless credit and debit cards within society and the disadvantages and advantages to the design implementation of the RFID.

A. Contactless Cards

Contactless Cards have become the most successful and recent implementation of advanced RFID technology integrated into society. It has become so successful that every bank or shop have now implemented RFID readers into their technology as a way of retrieving data that is transmitted from the debit or credit card when contact is made with the RFID reader. The problem with contactless cards is that the RFID technology implemented proposes some very serious security vulnerabilities in which a potential hacker could take advantage of. One very serious security vulnerability would be that RFID can be read by any RFID reader at close range, this means that the card does not necessarily have to be in contact with the machine, but the machine would have to be at a close enough range to read the data. RFID readers can be easily bought from any online websites such as Amazon or eBay, therefore it is easy for a hacker to buy an RFID reader and to be close enough to a person's wallet or card to obtain their details. RFID blocking wallets have been produced to prevent any RFID tags being accessed, however can we trust that this solution will last for long due to the vulnerability issues that it poses to contactless cards.

Contactless cards are the pinacle of today's society with banks now handing them out for free with varying results. Sure it does become easier with them around as you can easily swipe the card against an RFID reader provoking an transaction to take place but what happens when contactless cards display a more sinister side to them. Hackers are now able to figure out ways in which to combat the security and privacy of data and that can be potentially a very serious problem. New and more adapted techniques can be used on contactless cards to provide an overall better quality of service and also to provide users with the security that they need.

III. Related Work

Security and privacy issues are a major vulnerability to any technology, this can become quite serious if not treated correctly by adopting the appropriate methods [15], [16], [17],

PeerJ Preprints NOT PEER-REVIEWED

[18], [19], [20]. It has been known in recent years that RFID contactless cards have one of the most serious vulnerabilities due to the accessibility of RFID readers that can be bought online. RFID readers are known for transmitting and obtaining data, therefore it's only logical that hackers have now found a way to gather users bank details just by standing near them with an RFID reader. RFID blocking wallets have been constructed and sold for cheap prices however there is no evidence that they do truly block out RFID signals. It has now become the time where security of data needs to be highly addressed with contactless cards becoming more available by the minute. Researching into encryption types and techniques that could potentially fix the security issues was the top priority, therefore this section will be dedicated to the research that has been carried out by several journal articles on different techniques that could be adapted and implemented to create a better and more secure contactless cards.

A. PSP Protocol

PSP bases around the security and privacy of payment through RFID technology such as contactless debit and credit cards. PSP protocols structure is based around cash as it stores already paid for virtual coins, this would be acceptable to the RFID as real money therefore making the transactions safe and legitimate [21]. There are quite a few advantages of implementing a protocol such as PSP within RFID technology. These would be that hackers can not re-invent the currency of virtual coins as they are already paid for through a bank company [21]. RFID tags are also incorporated into the design and structure of this protocol as the data they provide will always remain undetected and details will remain anonymous [21]. Although there are many advantages to using a PSP protocol, there can be disadvantages as well such as the issue of although stated that the details will remain undetected how can they be sure that the RFID reader will not show the data accidentally to the banks because of a mistake with the coding of the protocol or any hardware issues. Another disadvantage of PSP protocol will be the fact that virtual coins already have to be paid for, therefore the data that the user provides will already be with the bank. If the bank gets hacked by an unknown hacker will there details be as safe with PSP protocol or will they also release the details of the user to the hacker revealing the virtual currency that could always be copied to imitate the real virtual currency. Virtual currency has lately been on

PeerJ Preprints NOT PEER-REVIEWED

the news as they are the most vulnerable and also confusing technique that has also become popular recently, therefore would it be prudent to this protocol as a way of essentially using monopoly money. Buying virtual currency could also become a big disadvantage as users could begin to get irritated by the fact that they have to keep purchasing virtual coins just so they can use the contactless credit or debit card, this could potentially revert the technology to just chip and pin again.

B. ECC Based Authentication

Elliptic Curve Cryptography (ECC) focuses on the security and privacy of data from potential hackers [3], [22], [23], [24]. ECC incorporates an RFID privacy model within the structure of authentication, this produces 4 new methods to be abided by to ensure safety and privacy of information stored. Step one would be where the server decides a random number which it then assigns to an RFID tag, the tag is then assigned to a RFID reader which then decides to transmit the random number [25]. Step two states that when the tag is received, another tag is implemented in which uses the same random number but implements a hash function to scramble the data and then sends that data back to the server [25]. The final step then goes back to the server which has received the other tag with the hash function and supplies the tag with a private key, the server then researches the tag to see if a specific feature [25]. If the server does not find the feature then the message will be deleted, where else if the message was found they will be provided with the tag's random number which will then be accepted by the server [25].The advantages of implementing an ECC based authentication into an RFID technology would be the sophistication of the cryptography, the steps state that as well as incorporating an ECC, they also incorporate a hash function to protect the safety and data of the user. However the only drawback to this would be that if the hacker is familiar with ECC then they would be able to recognise the pattern and the coding, therefore it will be easier to hack. Another drawback would be security vulnerabilities, if the ECC is not coded properly and efficiently a security vulnerability can be found and that could lead the hacker to access vulnerable data.

PeerJ Preprints NOT PEER-REVIEWED

C. Chipless RFID tags

Chipless RFID tags have become the most trending solution to the problems that contactless debit or credit cards face. Chipless RFID tags was based around the idea of a radar which it shows some similarities when looking at the research produced on the subject. Chipless RFID tag stores information or data that would be encoded in a specific section of the RFID tag, this eliminates the need of using micro-chips inside the contactless cards [26]. Chipless RFID tags have to rely on the signal strength produced by the RFID rather than the electromagnetic fields it usually relies on [27]. This would be because Chipless RFID technology need a lot more bandwidth which in return drastically reduces the signal stemmed from the RFID tag [10]. The advantage of having a Chipless RFID tag implemented into a contactless debit or credit card would be that the risk of any data being exploited would be significantly lower than having a Chipped RFID tag. However, the drawback of this would be the drastic drop in bandwidth reducing the signal, therefore the product could have faults when trying to connect with an RFID reader for a transaction. This could lead to a lot more money being spent to try to fix the problem rather than having the problem already fixed. Another potential drawback to chipless RFID tags would be the way that it could be more of a problem than a potential benefit as data can be easily accessed the same way as contactless cards could be. Without any form of encryption or algorithm to merge with this technique, it could become more troublesome than it's worth. This means that hackers still have the chance to access your data by using RFID readers near the wallet of the user or by essentially being in close contact. Chipless RFID tags could have the potential to become the next hot topic to research when thinking of ways to improve the security and privacy of users data when making a transaction with an contactless credit and debit card however it would be highly suggested that both the chipless RFID tags and encryption be merged together due to the complexity and urgent nature of the privacy of data.

D. RC4 and 3DES Algorithm Encryption

1) RC4 Stream Cipher: The implementation of an RC4 Stream Cipher provides a lot of safety for any information being stored in the RFID tag implanted on a debit or credit card. A crypto key must be used as a way of maintaining and masking any dubious vulnerabilities that may crop up, if a crypto key was not used then the percentage of a hacker breaching the system and obtaining information will be high [28]. There are seven steps in coding an RC4 encryption method within an RFID technology. Step one would be finding the information that needs to be encrypted and finding the perfect key to produce the highest quality encryption [28]. The second step then splits this data into two arrays ready for step three [28]. Step three changes the array so the range of numbers stem from 0 to 255 [28]. Step four fills the same array that was arrange in step three with the crypto key [28]. Step five finds the first array and randomly re-arranges it [28]. Step six produces the finalised key [28] and the final step uses XOR to encrypt the data to cipher text [28]. The advantages of using RC4 stream cipher within RFID technology would be that it can be the simplest and fastest method to ensure safety within the technology without comprising the data, however the drawback would be that some of the methods used may not be suitable for using within RFID technology therefore causing errors and complications when coding [28]. Another drawback would be that the methods are far too complex to think about implementing to contactless cards and also the time it might take to code this on each individual card before a hacker decides to use a new attack, therefore putting the plan back to square one.

2) 3DES Algorithm: 3DES Encryption also known as triple DES encryption has become one of the most well-known encryption methods due to the fast way it can be implemented and the security it can bring to information or data provided [28]. 3DES is a block cipher in which obtains plain text, encrypts it with one key, decrypts it with another key and then encrypts the text again with one last final key to produce highly secure cipher text [28]. The advantages to using 3DES encryption would be that due to the immense popularity and high praise for it because the safest and fast acting encryption type it seems a lot more reliable to use it based on feedback. Another advantage would be that the three keys used as encryption, decryption and then again encryption again provides a better and safer way of encrypting data without worrying about the integrity of the data as it would be well protected. A drawback would be that due to the immense popularity a lot of hackers would have been looking for security vulnerabilities, therefore the system will always be scoped and will become even more vulnerable when hackers do find a loophole in the system. Another drawback to 3DES encryption would be the cost and time of having to encode the encryption, this could potentially hinder the progress and speed of the advancements of contactless cards if the encryption takes too long to implement. The cost could also be exceptionally high with many workers having to work on each individual card to ensure the encryption is perfect for each card otherwise they face having to deal with another hacking situation. Other drawbacks include the long process of retrieving plain text just to encrypt it then decrypt it and then to encrypt it again just to receive cipher text, this could become quite the nuisance when coding the encryption due to it's repetitive nature.

E. Dual Chip with Touch Switch

Dual Chip with touch switch in a contactless card depends on using two chips as a way of determining when the user wants to use the contactless card. A standard micro-chip is used as well as another microchip named transport card [29]. The transport micro-chip is used for determining whether the card has been touched by the user to activate or deactivate the radio-waves within the RFID technology to ensure that all data has been protected. The advantages to implementing dual chips with a touch switch would be that the data can be protected easily from any intruders by allowing the user to manually activate the function(contactless) on their card by a simple touch and then after they have gone through with a transaction they can touch the card again to deactivate so that there is no need for any RFID blocker wallets. Another advantage to this would be the simple design of involving two antennas to have a high strength signal when testing out the wireless communication with the RFID reader. A drawback of this would be that if the user accidentally touches the card without realising and activating the dual chip contactless card, they could essentially intruders to obtain their information or data without any problems. It was not specified if any encryption techniques would be used in also helping protect the data within the card therefore it cannot fully protect the data. Another drawback to having dual chips would be that if the switch accidentally broke then it would be the same as having a normal contactless card, therefore is it really prudent to involve incorporating a touch switch into a contactless card without the thought that it might break through some accident.

IV. Conclusion

Wireless sensing technologies present an unprecedented opportunity for a broad spectrum of applications [30], [31], [32], [33]. New applications, such as smart cities [34], [35], intelligent transport, and digital health services make use of the low-cost RFID technologies to achieve

PeerJ Preprints NOT PEER-REVIEWED

seamless interaction between humans and their environment. In conclusion it has been within no doubt proven that while RFID contactless cards are quite useful for society, there are serious issues that must be addressed with the security and privacy of data and this action must be taken as soon as possible before any serious problems happens. By researching different journal articles it has become evident that the most trending solution to this problem would be by adopting a chipless RFID tags. The drawbacks however are very concerning with the drastic drop in bandwidth meaning slower signals and slower reactions when placed on an RFID reader. The solution however that could be proposed would be to merge both the idea of having chipless RFID tags with 3DES encryption types ensuring that the data has the protection it really needs without the hassle of using touch switches or any other technique. Another hot topic to research into when considering the idea of updating the security and privacy of a contactless card would be the merging both the dual chip with touch switch with also 3DES encryption as it has been proven that it is the best encryption for the security of information.

References

[1] T. Alsboui, A. Abuarqoub, M. Hammoudeh, Z. Bandar, and A. Nisbet, "Information extraction from wireless sensor networks: System and approaches," *Sensors & Transducers*, vol. 14, no. 2, p. 1, 2012.

[2] M. Hammoudeh, "Applying wireless sensor networks to solve real-world problems," in *Proceedings of the International Conference on Intelligent Information Processing, Security and Advanced Communication*. ACM, 2015, p. 1.

[3] S. Moffat, M. Hammoudeh, and R. Hegarty, "A survey on ciphertext-policy attribute-based encryption (cp-abe) approaches to data security on mobile devices and its application to iot," in *Proceedings of the International Conference on Future Networks and Distributed Systems*. ACM, 2017, p. 34.

[4] S. Belguith, N. Kaaniche, M. Laurent, A. Jemai, and R. Attia, "Phoabe: Securely outsourcing multi-authority attribute based encryption with policy hidden for cloud assisted iot," *Computer Networks*, vol. 133, pp. 141–156, 2018.

[5] J. Mohsin, L. Han, M. Hammoudeh, and R. Hegarty, "Two factor vs multi-factor, an authentication battle in mobile cloud computing environments," in *Proceedings of the International Conference on Future Networks and Distributed Systems*. ACM, 2017, p. 39.

[6] P. Dibb and M. Hammoudeh, "Forensic data recovery from android os devices: an open source toolkit," in *Intelligence and Security Informatics Conference (EISIC), 2013 European*. IEEE, 2013, pp. 226–226.

[7] I. Ghafir, V. Prenosil, M. Hammoudeh, L. Han, and U. Raza, "Malicious ssl certificate detection: A step towards advanced persistent threat defence," in *Proceedings of the International Conference on Future Networks and Distributed Systems*. ACM, 2017, p. 27.

PeerJ Preprints | https://doi.org/10.7287/peerj.preprints.26504v1 | CC BY 4.0 Open Access | rec: 11 Feb 2018, publ: 11 Feb 2018

PeerJ Preprints NOT PEER-REVIEWED

[8] Y. Atwady and M. Hammoudeh, "A survey on authentication techniques for the internet of things," in *Proceedings of the International Conference on Future Networks and Distributed Systems*, ser. ICFNDS '17. New York, NY, USA: ACM, 2017. [Online]. Available: http://doi.acm.org/10.1145/3102304.3102312

[9] A. Aloraini and M. Hammoudeh, "A survey on data confidentiality and privacy in cloud computing," in *Proceedings of the International Conference on Future Networks and Distributed Systems*, ser. ICFNDS '17. New York, NY, USA: ACM, 2017, pp. 10:1–10:7. [Online]. Available: http://doi.acm.org/10.1145/3102304.3102314

[10] N. C. Karmaker, "Tag, youre it radar cross section of chipless rfid tags," *IEEE Microwave Magazine*, vol. 17, no. 7, pp. 64–74, 2016.

[11] M. Hammoudeh, J. Shuttleworth, R. Newman, and S. Mount, "Experimental applications of hierarchical mapping services in wireless sensor networks," in *Sensor Technologies and Applications, 2008. SENSORCOMM'08. Second International Conference on.* IEEE, 2008, pp. 36–43.

[12] M. Hammoudeh and T. A. AlsbouвЃЄi, "Building programming abstractions for wireless sensor networks using watershed segmentation," in *Smart Spaces and Next Generation Wired/Wireless Networking.* Springer, 2011, pp. 587–597.

[13] S. Belguith, N. Kaaniche, A. Jemai, M. Laurent, and R. Attia, "Pabac: a privacy preserving attribute based framework for fine grained access control in clouds," in *13th IEEE International Conference on Security and Cryptography(Secrypt)*, 2016, pp. 133–146.

[14] M. Hammoudeh, S. Mount, O. Aldabbas, and M. Stanton, "Clinic: A service oriented approach for fault tolerance in wireless sensor networks," in *Sensor Technologies and Applications (SENSORCOMM), 2010 Fourth International Conference on.* IEEE, 2010, pp. 625–631.

[15] A. Carlin, M. Hammoudeh, and O. Aldabbas, "Intrusion detection and countermeasure of virtual cloud systems-state of the art and current challenges," *International Journal of Advanced Computer Science and Applications*, vol. 6, no. 6, 2015.

[16] I. Ghafir, V. Prenosil, and M. Hammoudeh, "Botnet command and control traffic detection challenges: A correlation-based solution," *International Journal of Advances in Computer Networks and Its Security (IJCNS)*, vol. vol. 7, no. Issue 2, pp. 27–31, 2015.

[17] I. Ghafir and V. Prenosil, "Proposed approach for targeted attacks detection," in *Advanced Computer and Communication Engineering Technology.* Springer, 2016, pp. 73–80.

[18] D. Q. Bala, S. Maity, and S. K. Jena, "Mutual authentication for iot smart environment using certificate-less public key cryptography," in *Sensing, Signal Processing and Security (ICSSS), 2017 Third International Conference on.* IEEE, 2017, pp. 29–34.

[19] S. Belguith, N. Kaaniche, M. Laurent, A. Jemai, and R. Attia, "Constant-size threshold attribute based signcryption for cloud applications," in *SECRYPT 2017: 14th International Conference on Security and Cryptography*, vol. 6, 2017, pp. 212–225.

[20] I. Ghafir and V. Prenosil, "Malicious file hash detection and drive-by download attacks," in *Proceedings of the Second International Conference on Computer and Communication Technologies.* Springer, 2016, pp. 661–669.

[21] E.-O. Blass, A. Kurmus, R. Molva, and T. Strufe, "Psp: private and secure payment with rfid," in *Proceedings of the 8th ACM workshop on Privacy in the electronic society.* ACM, 2009, pp. 51–60.

PeerJ Preprints NOT PEER-REVIEWED

[22] I. Ghafir, V. Prenosil, J. Svoboda, and M. Hammoudeh, "A survey on network security monitoring systems," in *IEEE International Conference on Future Internet of Things and Cloud Workshops (FiCloudW)*. IEEE Xplore Digital Library, 2016, pp. 77–82.

[23] S. Belguith, A. Jemai, and R. Attia, "Enhancing data security in cloud computing using a lightweight cryptographic algorithm," in *ICAS 2015 : The Eleventh International Conference on Autonomic and Autonomous Systems*. IARIA, 2015, pp. 98–103.

[24] I. Ghafir, J. Svoboda, and V. Prenosil, "A survey on botnet command and control traffic detection," *International Journal of Advances in Computer Networks and its security (ICJNS)*, vol. vol. 5, no. Issue 2, pp. 75–80, 2015.

[25] Y. Chen and J.-S. Chou, "Ecc-based untraceable authentication for large-scale active-tag rfid systems," *Electronic Commerce Research*, vol. 15, no. 1, pp. 97–120, 2015.

[26] M. Jalil, M. K. A. Rahim, N. A. Samsuri, and R. Dewan, "Flexible printed chipless rfid tag using metamaterial–split ring resonator," *Applied Physics A*, vol. 122, no. 4, p. 348, 2016.

[27] M. Forouzandeh and N. C. Karmakar, "Chipless rfid tags and sensors: a review on time-domain techniques," *Wireless Power Transfer*, vol. 2, no. 2, pp. 62–77, 2015.

[28] P. R. Sharma, "The simulation and analysis of rc4 and 3des algorithm for data encryption in rfid credit card," *International Journal of Applied Engineering Research*, vol. 10, no. 2, pp. 4265–4273, 2015.

[29] B. Shin, J. Yum, S. Kim, J. Lee, and J. Jang, "Secure dual-chip contactless card with an integrated complementary touch switch," *Microwave and Optical Technology Letters*, vol. 55, no. 3, pp. 529–533, 2013.

[30] R. Newman and M. Hammoudeh, "Pennies from heaven: A retrospective on the use of wireless sensor networks for planetary exploration," in *Adaptive Hardware and Systems, 2008. AHS'08. NASA/ESA Conference on*. IEEE, 2008, pp. 263–270.

[31] M. Hammoudeh, R. Newman, S. Mount, and C. Dennett, "A combined inductive and deductive sense data extraction and visualisation service," in *Proceedings of the 2009 international conference on Pervasive services*. ACM, 2009, pp. 159–168.

[32] M. Hammoudeh, "Modelling clustering of sensor networks with synchronised hyperedge replacement," in *International Conference on Graph Transformation*. Springer, 2008, pp. 490–492.

[33] I. Ghafir and V. Prenosil, "Blacklist-based malicious ip traffic detection," in *Global Conference on Communication Technologies (GCCT)*. IEEE Xplore Digital Library, 2015, pp. 229–233.

[34] O. Jogunola, A. Ikpehai, K. Anoh, B. Adebisi, M. Hammoudeh, H. Gacanin, and G. Harris, "Comparative analysis of p2p architectures for energy trading and sharing," *Energies*, vol. 11, no. 1, p. 62, 2017.

[35] O. Jogunola, A. Ikpehai, K. Anoh, B. Adebisi, M. Hammoudeh, S.-Y. Son, and G. Harris, "State-of-the-art and prospects for peer-to-peer transaction-based energy system," *Energies*, vol. 10, no. 12, p. 2106, 2017.

PeerJ Preprints | https://doi.org/10.7287/peerj.preprints.26504v1 | CC BY 4.0 Open Access | rec: 11 Feb 2018, publ: 11 Feb 2018