2020

AP® CollegeBoard

AP® Research Academic Paper

Sample Student Responses and Scoring Commentary

Inside:

Sample J

☑ Scoring Guideline

☑ Student Samples

☑ Scoring Commentary

AP Central is the official online home for the AP Program: apcentral.collegeboard.org.

The Response…				
Score of 1 **Report on Existing Knowledge**	**Score of 2** **Report on Existing Knowledge with Simplistic Use of a Research Method**	**Score of 3** **Ineffectual Argument for a New Understanding**	**Score of 4** **Well-Supported, Articulate Argument Conveying a New Understanding**	**Score of 5** **Rich Analysis of a New Understanding Addressing a Gap in the Research Base**
Presents an overly broad topic of inquiry.	Presents a topic of inquiry with narrowing scope or focus, that is NOT carried through either in the method or in the overall line of reasoning.	Carries the focus or scope of a topic of inquiry through the method **AND** overall line of reasoning, even though the focus or scope might still be narrowing.	Focuses a topic of inquiry with clear and narrow parameters, which are addressed through the method and the conclusion.	Focuses a topic of inquiry with clear and narrow parameters, which are addressed through the method and the conclusion.
Situates a topic of inquiry within a single perspective derived from scholarly works **OR** through a variety of perspectives derived from mostly non-scholarly works.	Situates a topic of inquiry within a single perspective derived from scholarly works **OR** through a variety of perspectives derived from mostly non-scholarly works.	Situates a topic of inquiry within relevant scholarly works of varying perspectives, although connections to some works may be unclear.	Explicitly connects a topic of inquiry to relevant scholarly works of varying perspectives **AND** logically explains how the topic of inquiry addresses a gap.	Explicitly connects a topic of inquiry to relevant scholarly works of varying perspectives **AND** logically explains how the topic of inquiry addresses a gap.
Describes a search and report process.	Describes a nonreplicable research method **OR** provides an oversimplified description of a method, with questionable alignment to the purpose of the inquiry.	Describes a reasonably replicable research method, with questionable alignment to the purpose of the inquiry.	Logically defends the alignment of a detailed, replicable research method to the purpose of the inquiry.	Logically defends the alignment of a detailed, replicable research method to the purpose of the inquiry.
Summarizes or reports existing knowledge in the field of understanding pertaining to the topic of inquiry.	Summarizes or reports existing knowledge in the field of understanding pertaining to the topic of inquiry.	Conveys a new understanding or conclusion, with an underdeveloped line of reasoning **OR** insufficient evidence.	Supports a new understanding or conclusion through a logically organized line of reasoning **AND** sufficient evidence. The limitations and/or implications, if present, of the new understanding or conclusion are oversimplified.	Justifies a new understanding or conclusion through a logical progression of inquiry choices, sufficient evidence, explanation of the limitations of the conclusion, and an explanation of the implications to the community of practice.
Generally communicates the student's ideas, although errors in grammar, discipline-specific style, and organization distract or confuse the reader.	Generally communicates the student's ideas, although errors in grammar, discipline-specific style, and organization distract or confuse the reader.	Competently communicates the student's ideas, although there may be some errors in grammar, discipline-specific style, and organization.	Competently communicates the student's ideas, although there may be some errors in grammar, discipline-specific style, and organization.	Enhances the communication of the student's ideas through organization, use of design elements, conventions of grammar, style, mechanics, and word precision, with few to no errors.
Cites **AND/OR** attributes sources (in bibliography/ works cited and/or in-text), with multiple errors and/or an inconsistent use of a discipline-specific style.	Cites **AND/OR** attributes sources (in bibliography/ works cited and/or in-text), with multiple errors and/or an inconsistent use of a discipline-specific style.	Cites **AND** attributes sources, using a discipline-specific style (in both bibliography/works cited **AND** in-text), with few errors or inconsistencies.	Cites **AND** attributes sources, with a consistent use of an appropriate discipline-specific style (in both bibliography/works cited **AND** in-text), with few to no errors.	Cites **AND** attributes sources, with a consistent use of an appropriate discipline-specific style (in both bibliography/works cited **AND** in-text), with few to no errors.

Academic Paper

Overview

This performance task was intended to assess students' ability to conduct scholarly and responsible research and articulate an evidence-based argument that clearly communicates the conclusion, solution, or answer to their stated research question. More specifically, this performance task was intended to assess students' ability to:

- Generate a focused research question that is situated within or connected to a larger scholarly context or community;
- Explore relationships between and among multiple works representing multiple perspectives within the scholarly literature related to the topic of inquiry;
- Articulate what approach, method, or process they have chosen to use to address their research question, why they have chosen that approach to answering their question, and how they employed it;
- Develop and present their own argument, conclusion, or new understanding while acknowledging its limitations and discussing implications;
- Support their conclusion through the compilation, use, and synthesis of relevant and significant evidence generated by their research;
- Use organizational and design elements to effectively convey the paper's message;
- Consistently and accurately cite, attribute, and integrate the knowledge and work of others, while distinguishing between their voice and that of others; and
- Generate a paper in which word choice and syntax enhance communication by adhering to established conventions of grammar, usage, and mechanics.

Threats, Vulnerability, & Legality

An infosec analysis of RFID and Wiegand manipulation in a modern light

Word Count: 4355

ABSTRACT

This article delves into multiple lenses of RFID fraud (Wiegand data flow IoT, MAS as well as Datakey encryption), these technologies show extensive reports of criminal and malicious use. Nefarious opportunities are present and the extensibility and accessibility of MAS pertaining to said developmental tech needs to be limited. Looking into system functionalities and augmentation towards firmware development for necessary improvement, shown in a multitude of workplace environments. Not only developmental machines and crowdsource script management tend to be used, this article outlines the different usages and expands upon the current ideology. This paper intends to explore and highlight replicable examples of how RFID technology is used in industry and daily life in order to further explain vulnerabilities.

INTRODUCTION

RFID fraud, unlike other means of fraud is untouched upon and rarely brought to the light. Although Banks and the governments release data on fraudulent cases. This particular instance of fraud is used excessively daily with little repercussions and still goes unnoticed. This is due to the digital imprint, it's hard to prove connections. Wiegand data is the primary target of individuals with malicious intent. Not only is it an easy target, its public and everywhere. Traditional Wiegand data in the form of cards has 26 bits of data. Out of the 26 bits two are for error checking while the other 16 are facility and ID bits. These bits can be manipulated and decrypted with ease. Wiegand data can be manipulated through hardware, software, and even physically. There can be over 65,000 card id numbers within each facility code brining difficulty especially due to the possible 254 other facility codes. This was an attempt at fixing fraudulent behavior through RFID devices, but to not avail as malware can directly target both the reader as well as the card or chip. Facility identifiers also known as FIN’s were assigned by the Federal Communications Commissions, the government issued IDs can be abused and a new system is in dire need. A clear representation of RFID vulnerability as well as needed fixes will be facilitated through multiple forms of data, and is desperately needed in the cyber security community.This is due to little to no attention being drawn toward RFID behaviors.

To fully encompass RFID fraud many perspectives are needed, Social, Legal, etc. RFID Fraud comes in many shapes and forms, so victims can be hard to sample. With this smaller pool in mind data can be faulty or limited. Not only is it hard to gather a pool due to victims diverse cases, most events of RFID fraud goes unreported or noticed. This is primarily due to it being pseudo-physical fraud, essentially a digital pickpocket perpetrators tend to fly under the radar. According to the U.S yearly fraud reports 80% of RFID fraud cases are suspected to be unreported. Even large scale cases are rarely escalated to the anything over 7 years, the typical sentence is 3 years. A prime example of this would be the arrest of Joel Narvaez at the age of 19. It took years for him to get caught, starting at the age of 15 Joel stole millions through many RFID based methods. In the end he faced very little legal repercussions and even gained large media attention, which allowed him to get a multitude of job opportunities. Not only is the technology flawed the penalties aren't monumental enough to cause any distraught in a attacker.

Review of Literature

To fully encompass RFID fraud, many aspects of fraud as a whole had to be looked over. When looking into US Census released fraud data (2010-2018) many gaps in knowledge arise. To further be in tune with the current fraud means and methods alternative sources were a must. Delving into the realm of fraud is very complex, as current methods are kept very secretive. The initial focus on government data quickly shifted to convention data. Defcon, ShmooCon, ToorCon, and THOTCON where the clear choices for consultants. Not only do these four conventions feature the leading experts in infosec they allow for a multitude of knowledge not accessible to the public. Previously attending these events allowed for multiple security professionals to weight in on this paper, including Bryce Case Jr, otherwise known as YTCracker. Bryce is well known for hacking many government websites. He is well regarded in the community and has a tremendous wealth of knowledge. The main source used was Defcons Research forum, which is a professionally released column on Fraud, including many papers written about RFID fraud. After consulting with professionals and reading plenty of papers the clear gap and lack of knowledge was apparent. Cryptography and public awareness was lacking. This lead to the conclusion of ex post facto analysis and drove to many unique conclusions. This gap in cryptography lead me to delving deeper into how RFID mechanics and wiegand data functions, which showed how vulnerable machine functions and IoT style connections actually are. There is a clear need for additional research upon both cryptography of local RFID nets as well as RFID vulnerabilities as a whole. Due to the general lack in research already, the key way to obtain data was through my consultants, primarily Bryce. He was a very valuable asset throughout the research process as he was able to give an in depth analysis on both the legal repercussions and how penetrable wiegand data is. As a security professional he was able to use penetration tools for educational purposes to illustrate these vulnerabilities (Also known as Pen Points) and manipulate them in a controlled environment. Without access to these tools in depth analysis would not have been plausible. The primary focus throughout the paper was identifying the issues, and than addressing the repercussions. In a sense it is a view into the mind of a criminal, the process of how its carried out, how it affects the victim, and the seemingly inevitable legal repercussions. Yet when looking into the legal repercussions there's a clear lack in consequences. This is what influenced the decision to include legality of RFID fraud within the paper both minor and serious offenses. As a whole RFID fraud isn't touched upon very much especially in the eyes of the public. This raised the question how many high school students know about RFID penetration? To answer this question a brief survey with a controlled sample size was conducted. When interviewing 100 High school students only one student knew about what RFID even was. Once a lack of knowledge was seen it was clear that public education was sub-par. Although new interpretation of material was the focus of the paper, public education quickly became a factor as well. This is due to current research not being well released. To fulfill new conclusions many questions had to be answered that. Scouring current research to no avail lead to the idea of a bulletin release, which finally pushed toward crowd source security and how needed it is within RFID tech. Crowd-source security isn't a new concept but it hasn't been incorporated at all with RFID tech, or wiegand data. This was a conclusion reached independently and was the final puzzle piece for a firm solution.

Legality

Delving deeper into the legal aspect of this type of fraud you can clearly see how its so popular. With little repercussions and ease of access to tools, criminals jump to RFID based fraud. Most RFID cases get dismissed as misdemeanors or dismissed instantly. Although most cases of fraud are simplistic, large scale RFID Heist’s also referred to as licks on many forums do have legal repercusssions. Yet the legal system is clearly lacking, less cases tie directly to profit and risk ratios. Criminals have very similar tendencies especially when it comes to profit margin ratios. To get a firm grasp on the legal implications of certain fraudulent cases. Many court issued trial results provide vast insight into cyber-criminal behavior.

The threat of “RFID Skimming” gets waved off constantly by law enforcement and is seen as a non follow up case. The majority of local police stations don’t follow through with procedures or even have them. When interviewing miami-dade cyber detectives such as Charles Nanney they had very little to no response on the subject. The main victims that follow through with these instances are Banks as well as freelance security experts. The cyber security field as a whole is diverse, many experts contribute to the problem themselves. Not only is it diverse its corrupt this is proven in many instances such as major database leaks, ssn breaches, etc. This is why the only thing that can be taken seriously for research purposes is either government data, or con investigative data. Con investigative data is data gathered first hand at conventions by leading professionals, and is recorded live. It's tested for bias as well as many other factors such as ping radius and authenticity. In recent events conventions have focused their media panels primarily on RFID fraud, data is used from these panels in order to properly conduct individual facility code research. Recently panel data has shown vulnerability within four major portions of RFID Behavior. This would include MHz (Mid Range), Scanner, Port, and Client side breaches. This is all very similar to looking into a IoT location or agent platform in terms or connectability and ease of access.

Vulnerability can be broken down in many ways, but in this instance “Open Source Vulnerability” will be the only way to accurately gauge the dilemma. This is due to Non Open Source scripts and many projects being highly exclusive and illegal to own depending on its usage. When looking into OSV (Open Source Vulnerability), github or similar project development sites/forums you can see clear access points. New bugs and entry keys are being uploaded every minute. These High pentested data numbers are the primary concern, new exploits are being released at an exponential and alarming rate, while current publicly used technology sits by. Individual bit protection is a long term solution yet is taking ages in its developmental stages. Facility MD5 Hashing and Temporary bit scramblers, or data shields are the only option for users but can range upwards of thousands of dollars. While this isn't a problem for banks and or retailers, individual users face the damage. Large crowds as well as internet cafe style areas are the most susceptible. Non tech savvy individuals fall into these traps every day without realizing it, not all data theft is large scale either. Attacks can range from data for advertisement, to identity theft. Even physical fraud is a possibility because many “High tech” ID scanners run through RFID Ports, or use Wiegand data this is shown in the Defcon research release (2015). Yet its relatively easy to pinpoint when an attack is caused by RFID bruting or injection. The real issue is finding how it was done and patching it. This feat is nearly impossible without a fully dedicated team as data its such large scale data analysis. Luckily most methods get leaked. This is due to the tensions between “Hacking” groups. Rivals are very common in the cyber security world. When gathering leaked public access vulnerability points, both unpatched and patched it's easy to see why it is so hard to substantially decrease the number of infects. Especially when looking over a large scale data set. Even in 1983 when there was only 2 million personal computers in the United states the issue would be hard to control. Let alone tablets, phones, and other common devices using this data flow method. Most everything connected to Wiegand data is flawed, especially RFID cards and chips. With hundreds and thousands of potential vantage points a clear cycle of information is needed.

Although there is a wealth of knowledge on how to manipulate RFID chips and cards for educational purposes, there is very little developed by security professionals to stop the problem. Penetration testing and RFID security as a whole tends to bring in alot of money to the community. It is seen as taboo to speak of permanent solutions. The primary reason conventions even have media panels on the subject is to raise media awareness in turn increasing their pay check. Rather than helping the greater good the majority of the people sit by in order to reap the benefits and leave it to governmental agencies which have shifted their attention to larger scale crimes such as Sim Swapping. Government data is still large scale yet took hours to pick down into groups. These groups include Local, Physical, and Global. Using transcriptome style analysis and a venn diagram it's easy to how Local smaller scale attacks are the most prevalent, and in this instance dangerous. The highest risk to profit ratio was displayed in the Global data set, yet the most damage was caused by the local data. Running a python based script to run the data sets allowed for bulk checking of multiple variables within these groups. The main factor was Damage which was gauged by Time, and economic loss. The script was analyzed and deemed opertable for the task by “Red Team”, a notable group within the community which released over 40,000 patches and is still currently releasing more ID fixes.

Commercial and Media Usage

Another large issue with RFID tag data is its commercial usage. Looking at a media perspective this is where all the hate spawns. Companies use this data to catalog movement buying trends etc, this is where the nickname Spy tags came from. Not only are companies monitoring and manipulating data trends legally individuals with malintent have this same information at their fingertips. This crucial detail tends to be left out of many news outlets. Through personal analysis there isn't a real reason behind this other than a fear of media hype. A notable point to bring up is that any reader can pick up a tags details. There isn't a variety of readers even for government usage, all tags and readers remain the same. With this in mind data tracking on both a commercial and malicious manner is an ease. Combined with constant breaches and port reconfigurations a possible media storm is brewing. Continuing on the little media coverage path is a must. If it becomes a known to the public, companies will lobby money, experts will be upset, and the community will turn against each other. A similar trend was seen when Sim swapping first became a big ordeal. These trends have formed crowd-sourced security which has proven to be very prosperous for both the hackers and companies. To entice hackers to not exploit errors “Bug bounties” are placed offering large lump sums of cash for reported bugs. Hackerone does a superb job in keeping these RFID breaches under check, yet there is a still a large gap of knowledge on the subject as a whole as not all vulnerabilities have been outlined yet, and little to no consequence is set in stone. With this in mind it's easy to see why further research on both commercial grade penetration testing and local RFID network traffic vulnerabilities.

When looking into the social aspects of RFID fraud the first thing to delve into is the victims. Millions of hard working innocent people are subjected to attacks. Their data is being constantly manipulated, read, and even physically altered. Millions of victims and billions of dollars are at stake. Over 19 Million Americans had their identity stolen last year according to the U.S Cybercrime yearly release 58% was through RFID means. The major reason why cyber based identity theft happens is rarely brought to light. 31.8 Million credit cards are stolen as well through RFID technology yearly. These statistics are just a small glance at the dangers of RFID manipulation. Looking into all the other possible ways information and data is stolen especially Wiegand data generates the question, How many people are taken advantage of yearly? This number is impossible to gauge without private and commercial help, which is isn’t going to happen due to consumerism. The pool size is massive and can have a harsh social impact. Florida is the highest per capita rate of RFID based identity theft, and is currently the state leading in development and widespread acknowledgement of the problem. Identity theft is seen as fairly common to the public eye but why should it be? Technological advances are in place, yet not for a long time at the current rate of development. Decreased developmental rates are caused primarily by large companies and lobbying. It’s seen socially unacceptable to manipulate an individual and their data is the same way. Companies hide behind brittle RFID technology in order to gain quick capital without properly looking into consequences, as most of the blame has been shifted to the government. Typically data is regulated and protected by consumer privacy law and maintains on a sectoral basis. Yet the U.S does not have any formal data protection laws, only the Privacy Act, Safe Harbor Act, As Well as the Portability and Accountability Act. These are seemingly in the favor of the average joe yet in actuality oppose common moral privacy beliefs of many individuals. A survey conducted by Yale on privacy of data in 2016 concluded that 89% of a 50,000 participant pool said they would want their data to be secure and in their own hands only. The other popular option was data release with consent, yet only 8% chose this option. The public's opinion on data doesn't seem to matter much though in the long run, as no effort has been put toward protecting privacy.

Public education is a must, not only is the public unaware it's also misinformed. Although tags are seen as harmless, because they are. The malintent behind their practices is truly shocking. Cyber-criminals can take crowds of people's information in a breeze. Small things can help, public awareness and key signs to look out for such as Public wifi. If everyone kept their wifi off in public unless it was trusted, auto loggers and other RFID phishing techniques would be completely useless. This is why education is a key component, but just to a needed extent. Media breaks and technology have a past of not linking well. An inevitable crime “bubble” bursts typically after these news articles, and new methods and manipulation are created at a intense rate. This increases government interest but decreases the infosec community engagement. When patches run ramped with little reward laborers won't waste their time. Although a public awareness approach is needed, a lot more data will need to be gathered before any real sort of publicity is brought to the subject. Crowd-sourced security comes into play with public awareness, if more people knew about how pressing the issue was more individuals, including industry professionals on all fronts would be able to contribute. Crowd-sourced security works best on a large scale, the more eyes on a project or concept the better. Companies need to be informed individually about the potential risks and have solutions in place.

It can be difficult to gain a background on data manipulation in general as there is very little to no historical evidence. Although the first RFID chip was invented in 1948 it became more popular in recent years. The first case of RFID manipulation was reported in the 80’s and the rate of fraud has increased exponentially each year. It really became a pressing problem in the early two thousands and has escalated even more since. Not only is more technology with both Wiegand data processing and RFID tags present, penetration is seemingly common knowledge to entry level hackers. Looking into the future it's still a sharp incline as no monumental solution is predicted in the distant future. It is shown to be statistically more likely for RFID to become obsolete before a final patch is produced. Although there is a multitude of negative features of RFID Tech, there are some positive ones. It's an easy way to track as well as identify objects, and rapidly stores information electronically. Another helpful feature is the passive tag communication and energy efficiency. It can be helpful in a controlled environment and does help in security to an extent. To a regular user RFID tech is perfect, and can withstand a lot of pressure, yet it cuts some necessary corners.

The best possible solution would be an automated bulletin style application, with a locked RDP (Remote desktop protocol), and locally secured data flow. This app would transmit data to a professional hub automatically based on census data.Running a complex python script to target an identify possible and ongoing attacks by using strategically placed RFID readers on theft hotspots would be ideal. In a sense it would be able to change the data back on a global scale resetting it to default before any damage is able to be done. Removing the need for shields or scramblers entirely. The root of the problem is taken down directly through the automation. The main driving force in the script is its compatibility to locally manipulate the locked RDP data. Since the script is automated and private all that would be needed is a high ranking government employee to hold possession. The main problem with RFID technology is its variety and public appearance. The bulletin would take this and transform the cracked key into something entirely different with the same function. The data flow would still be transmitted fully, just active onboard support would be needed. If RFID distributors provided support through this application it would disrupt the need for old RFID tags. It would allow for the distributors to guarantee astronomically better security and public credibility. Not only would this be an economic boost for the RFID companies, consumers could acquire the setup for much cheaper without the need for scramblers. This would cut down on server costs by over 60% allowing for many more security improvements on top of the Remote Desktop server space.

Throughout the paper many limitation were met on many fronts. For one how large scale the issue truly is, not everyone can be protected from such a large problem. The populus as a whole forced big picture ideas upon the research, in the end working out for the better. The primarily limitation included the lack of knowledge, lack of data, and lack of government interference. This as a whole is what cut down on the idea of creating a survey, or selecting a sample size. With little to no public awareness it's hard to telegraph how large the issue truly is. Not only are most cases unreported, most are conducted with unknown variables such as connection methods (IoT, RDP, etc). The average user may use the technology without knowing they have even used it. Another concern raised was the cyber-security community and how it is in a constant siege. Without united fronts there is no possible way to create a solution without serious economic influence. In this case it's not going to happen once again due to government involvement. The “Bigger fish to fry” mentality is seen time and time again. Uniting the community is a must in order to take on such a large task. Local changes need to start before a such a large project is even considered. Work with the public as well as professionals to actively warn and prevent individuals from facing these riskys. Small steps at first would be optimal, informing small business owners, the youth, and once a solid team is united than media can be released. This plan is relatively similar to how Sim Swapping and Mirai nets were first approached after they became a widespread attack method. It has been proven time and time again to work. The only thing needed is time, dedication, Government and Corporation cooperation.

References

www.usa.gov/scams-frauds

www.grants.gov/fraud

www.ftc.gov/identity/data

www.sas.com/en_us/software/detection

Weis, Stephen A. (2007), RFID (Radio Frequency Identification): Principles and Applications, MIT CSAIL, CiteSeerX 10.1.1.182.5224

"RFID and Rail: Advanced Tracking Technology – Railway Technology". 16 March 2008. Retrieved 14 March 2018.

Daniel M. Dobkin, The RF in RFID: Passive UHF RFID In Practice, Newnes 2008 ISBN 978-0-7506-8209-1, chapter 8

John R. Vacca Computer and information security handbook, Morgan Kaufmann, 2009 ISBN 0-12-374354-0, page 208

Bill Glover, Himanshu Bhatt ,RFID essentials, O'Reilly Media, Inc., 2006 ISBN 0-596-00944-5, pages 88–89

“Ants' home search habit uncovered". BBC News. 2009-04-22. Retrieved 2013-09-03.

"Hitachi RFID powder freaks us the heck out". Engadget. Retrieved 2010-04-24.

TFOT (2007). "Hitachi Develops World's Smallest RFID Chip". Archived from the original on 2009-04-16. Retrieved 2009-03-27.

Martein Meints (June 2007). "D3.7 A Structured Collection on Information and Literature on Technological and Usability Aspects of Radio Frequency Identification (RFID), FIDIS deliverable 3(7)". Retrieved 2013-09-22.

Paolo Magrassi (2001). "A World Of Smart Objects: The Role Of Auto Identification Technologies". Retrieved 2007-06-24.

Silva, S., Lowry, M., Macaya-Solis, C., Byatt, B., & Lucas, M. C. (2017). Can navigation locks be used to help migratory fishes with poor swimming performance pass tidal barrages? A test with lampreys. Ecological engineering, 102, 291–302.

Pete Harrison (2009-07-28). "EU considers overhauling rules for lost air luggage". Reuters. Retrieved 2009-09-09.

[Miles, Stephen Bell (2011). RFID Technology and Applications. London: Cambridge University Press. pp. 6–8]

"Benefits of RFID in Theft Protection – CONTROLTEK". Controltek. 14 February 2014. Retrieved 11 October 2017.

Rohrlich, Justin (15 December 2010). "RFID-Tagged Gaming Chips Render Hotel Bellagio Robbery Haul Worthless". Minyanville Financial Media. Retrieved 16 December 2010.

Booth-Thomas, Cathy; Barnes, Steve; Cray, Dan; Estulin, Chaim; Israely, Jeff; Mustafa, Nadia; Schwartz, David; Thornburgh, Nathan (September 22, 2003),

Weston, Liz Pulliam (2007-12-21), "New Credit Cards Allow Hands-Free Theft", *Money central*, MSN, retrieved 2009-03-14.

Heydt-Benjamin, Thomas S; Bailey, Daniel V; Fu, Keven E; Juels, Ari; O’Hare, Tom (October 22, 2006), *Vulnerabilities in First-Generation RFID-enabled Credit Cards* (PDF) (draft study)

Amherst, MA; Bedford, MA; Salem, MA: University of Massachusetts; RSA Laboratories; Innealta, retrieved 2009-03-14. Newitz, Annalee (May 2006), "The RFID Hacking Underground", *Wired* , 14(5).

Gannsle, Daniel J (December 2008), "How to Protect Yourself from High-Tech RFID Identity Theft", *How To Do Just About Everything*.

Academic Paper

Note: Student samples are quoted verbatim and may contain spelling and grammatical errors.

Sample: J
Score: 1

Threats, Vulnerability, & Legality: An Infosec of RFID and Wiegand Manipulation in Modern Light

The paper earned a score of 1. The paper presented an overly broad topic (page 2) of the "many perspectives" on RFID fraud. While the paper uses the term survey on page 4, it does not provide any details, let alone a non-replicable research method or an oversimplified description of a method. Furthermore, the mentioned method is not germane to the topic of inquiry.

The paper didn't earn a score of 0 because there is a report on existing knowledge, both scholarly and non-scholarly.

The paper didn't earn a score of 2 because there is no description of method and the topic does not have a narrowing scope.