2010

Evidential Recovery in a RFID Business System

Brian Cusack
AUT University

Ar Kar Ayaw
AUT University

DOI: 10.4225/75/57b291b040cd9
Originally published in the Proceedings of the 8th Australian Digital Forensics Conference, Edith Cowan University, Perth Western Australia, November 30th 2010

Evidential Recovery in a RFID Business System

Brian Cusack and Ar Kar Ayaw
AUT University
Digital Forensic Research Laboratories
Auckland, New Zealand
brian.cusack@aut.ac.nz

Abstract

Efficient stock management in the commercial retail sector is being dominated by Radio Frequency Identification (RFID) tag implementations. Research reports of the security risk of RFID tags show that breaches are likely and that forensic readiness is a requirement. In this paper a RFID tag business simulation is reported that replicates previous research reports of security breaches with the purpose of identifying potential evidence after such attacks. A Read/Write Tag was cloned and used to replicate a SQL poisoning attack on a simulated Business System. A forensic investigation was then undertaken to identify potential locations for evidential recovery. This paper differentiates from the replicated studies in that the whole Business System is considered evidential. The scope of the inquiry includes the technical artefacts, the information artefacts and the human actors. The result of the investigation shows locations of evidence and the priority for investigations in RFID system architectures.

Keywords

RFID, Evidence, System

INTRODUCTION

Radio Frequency Identification (RFID) Tags are used in the commercial retail sector for stock management (Chalasani, Boppana, & Sounderpandian, 2005). A tag is attached to a Stock Item (SI) so that the identity of the SI is accessible by digital scanning. The cost advantage is apparent in various stock management processes including audit, transaction, and entry (for example in a book shop the contents of a carton may be individually scanned and data matched without opening a carton). However, the risk of fraudulent exploitation of RFID stock management systems escalates when more expensive tags are used (usually on more expensive SI). The higher risk tags are read/write and/or active. The appetite for risk also escalates with higher valued SI and the parallel increase in opportunity to crack a system. The utility value to the retailer of RFID Tags is transaction efficiency and inventory control but the trade-off is trust in the system. The violation of trust may occur in many ways and be demonstrated by educated theft of properties. The residual risk of system violation requires a forensic readiness capability that can inform the system security module how to best treat a risk. In addition the evidence requires identification and preservation so that perpetrators may be prosecuted. The retailer has balanced a cost-benefit analysis to invest in such a stock management system but may not have realised the forecasted benefits in the event of negative control risks materialising (Altschaffel, Kiltz, & Dittmann, 2009).

The research interest in this paper is to scope the risk of violation in a RFID stock management system (the Business System), to document the location of potential evidences after an event, and to recommend best practice for both system security and forensic investigation. A laboratory simulation is set up to replicate previously published security violations of RFID systems, and then the Business System is forensically investigated in order to locate potential evidences. The simulation context is the retail environments of clothing and electronic goods. In both environments SI can vary in price from a few dollars to tens of thousands of dollars. The environments are high intensity with large numbers of SI, high transaction rates, many entry level sales assistants, high staff turn over, and generic brand systems architectures. The Read/Write Tag is often deployed to SI in these environments by press clip attachment (with optional band extension) (Jones, Hoare, Dontharaju, Shenchih, Sprang, Fazekas, Cain, & Mickle, 2006). The attachments are released at the point of sale (POS) with a design tool for future re-writing and re-attachment to another SI. The business process is cost effective and the Business System integrity is theoretically maintained (Jeng, Chang, & Wei, 2009).

The paper is structured to first define a RFID Tag Business System and then to elaborate the specific security risks associated (Rotter, 2008). The Business System is defined in Figure 1 and the potential for system violations are identified between the Business System entities, within the entities (eg. tag cloning), and through social engineering. It is assumed the Business System is closed so that the event of an item being thrown out of a window undetected or breaking and entering are excluded from the study. The case of a Business System is

violated by SQL Injection attack through the Read/Write RFID Tag is replicated (Haines, 2006; Rieback, Simpson, Crispo, & Tanenbaum, 2006). The Business System is investigated for evidence remaining after the attack and suggestions made for where to look for evidence, how to extract evidence and how to preserve the evidence (Michael, & McCathie, 2005; Masters, & Turner, 2007; Harrill, & Mislan, 2007; Khannaa, Mikkilinenia, Martonea, Alia, Chiub, Allebacha, & Delpa, 2006; Martone, Mikkilineni, & Delp, 2006).

STOCK MANAGEMENT SYSTEMS

The Business System architecture of a RFID stock management system consists of three entities, namely the SI, the POS and the BIS. Each entity has sub-systems and services that are required by the other entities. For example the SI requires RFID Tags, a scanner, and services from POS and BIS. The POS requires a Transaction Processing System (TPS), scanners (for cards, Tags and Chips), a Tag attach/detach service and the services of SI and BIS. The BIS requires software for data base/warehouse and the relevant build for information management. In addition the services of SI are required for audit and POS for updating the relevant stock values. The Business System consequently presents a closed system of sub-systems, entities and services (Zhang, Li, Wang, Li, & Xia, 2007).

Table 1. The Business System

Entity	Stock Items (SI)	Point of Sale (POS)	Business Information System (BIS)
Sub-Systems	Tag Scan	Scan TPS	Data Storage IS Management
Services	ID Authentication	De/Attach Authorization	Refresh Audit

A Business System mixes and mingles elements of the real world with infomatic abstractions and the people who interact within the system. The Scan sub-systems (often termed ‘Readers’) illustrate the environment complexity where hardware, software, data, information and humans interact. In each of the instances of interaction elements of the Business System create a nexus of intent that delivers the business value. Similarly non-beneficial interactions may occur that create drag cost and potential legacy costs of unintended disclosures. The risk of disclosure and subsequent compromise of the Business System is eventual in every process (Ohkubo, Suzuki, & Kinoshita, 2005; Rieback, Crispo, & Tanenbaum, 2006).

RFID STOCK MANAGEMENT SECURITY RISK

Trust in RFID based Tagging of stock inventories is unfounded (Rieback, et al., 2006). The potential for fraudulent intervention into the RFID system is established in the literature (eg. Ding & Bow, 2008; El-Said, & Woodring, 2009). Other authors classify the security risks into layers that represent the different architecture designs a RFID stock management system may have (Haines, 2006). One of the concerns for retail commerce is the progression that as RFID chips are made more user-friendly then the risk of attack grows. Jones, et al. (2006) described the evolution of RFID chip design and process time costs. In the manufacture of Tags the access to writing has become easier and less costly in the interest of letting retailers code their own Tags. The benefit has however brought with it easier access for criminals to write and rewrite over Tags and hence changing the values (including the null value) in a RFID stock management system (Chalasani, & Boppana, 2007).

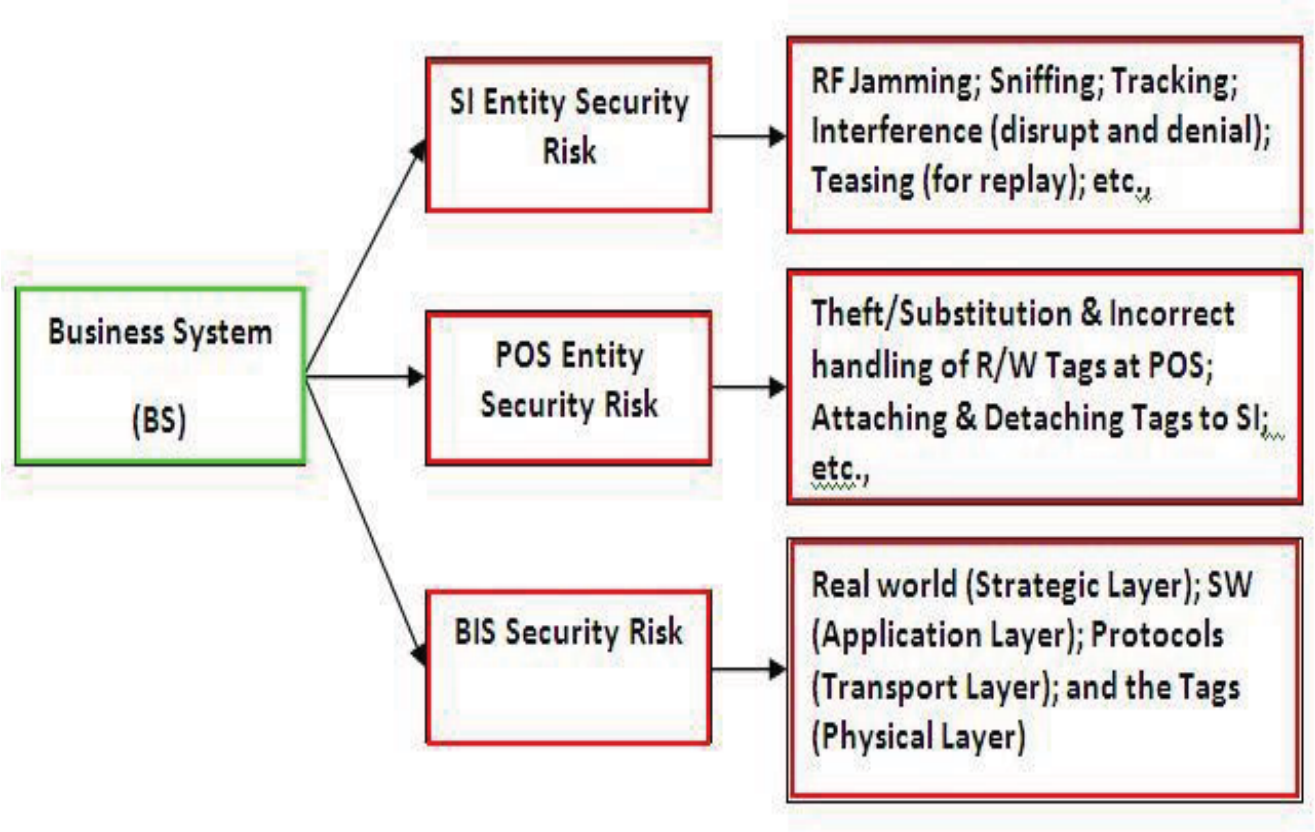

Figure1. Business System RFID Security Risks

The SI Entity Security Risk

The architecture and engineering of a RFID Tag invites a suite of obvious attacks that may exploit any radio frequency device. For example jamming, sniffing, teasing (for replay), tracking, and interference (disrupt and denial) (Bolan, 2007; Rao, et al. 2005). Some of the less obvious vulnerabilities are in the perceived appetite for risk. The false sense of security engendered by the innovation and the 'off-line' context reduce awareness of the potential threats and yet the high value of the stock inventories managed by RFIS Tags heightens criminal motivation for risk. The perception that RFID Tags are small and cannot be protected overlooks the growing capacity of Tags and the strengthening of encryption algorithms. The scanners and the relatively large number of lines of source code use to read and write on Tags provide a celebrity challenge and backdoor for criminal activity.

RFID Tags are passive and active by nature of design and each type has particular risks. The type of Tag can determine the attack vector and the proximity an attacker must gain. For example a Tag with a range of one meter or less would require the attacker presence and possible social engineering for a radio attack to be effective. Passive Tags are open to kill hits and hence the retail exit security can be negated (Tu & Piramuthu, 2008; El-Said & Woodring, 2009). Active Tags with the read/write feature can be hacked in order to change the ID to cheat pricing scales (Haines, 2006). And both types of Tags are vulnerable to worms and viruses. In the real world context practices of physically swapping a high value Tag with a lower value Tag are being reduced by customised attachment designs and detachment tools.

The POS Entity Security Risk

The POS Entity has many potential security risks that fall beyond the interest of this research and are published elsewhere, for example card skimming (Rieback, et al., 2006). The principle risk to the RFID stock management system is the substitution and incorrect handling of the Read/Write Tags at the POS. The Business System processes of attaching and detaching Tags to SI occurs at the POS. These services require the input from the BIS and the SI entities to assure the release from and the capture into the Business System. It is at this point that the value is realised and extracted from the business process and hence vulnerabilities exist.

Tags that are released from the system (using a design tool) require physical protection from theft or substitution. To this end a secure receptacle is required within the release tool to assure all Tags are captured and no substitutes are deposited. Similarly policies are required for the management of released Tags and the rewriting of these Tags. Audit is to be maintained of the number of Tags engaged in the different processes of the Business System and every released Tag is to be hashed and re written (ie. a Tag from one SI may not be reattached to a similar SI until due process is complied). Similarly the attachment of a Tag is to be tested to assure the Tag cannot be easily removed and stolen for analysis / disclosure (Chawla, & Ha, 2007).

The BIS Security Risk

The Business Information System (BIS) consists of the database/warehouse application, the human participants, the Information System (IS) build, and the Information Technology (IT) that supports the IS. As a sub-system of the BIS middleware is found on the scanners and in the POS entity. The explanation given by other researchers (Bhargava, 2006) suggests that the division of the BIS into layers that account for the real world (strategic layer), the software (application layer), the protocols (the transport layer) and the Tags (the physical layer). Such a categorisation maps onto the archive of known security breaches in the internet world and provides structure for security risk assessment.

The most effective way to mitigate the risk of theft is to implement protective polices and to place physical barriers to shield wrongful transactions. In a compliant security environment only the residual risk remains. The residual represents a percentage chance of an occurrence and therefore forensic readiness is a requirement for post-event assurance. Intrusion detection systems that mine the BIS transaction logs may provide alert and also regular physical stock taking (made easy by reader scanning of Tags). To successfully breach a security compliant RFID stock management system an attacker must co-ordinate an orchestrated script of social engineering, Tag cloning and the physical SI release (Kim, Shin, & Park, 2007; Landit, 2005; Li, Xu, & Yu, 2008).

HUMAN ACTORS

The investigation of a crime scene considers all matters evidential. In the previous studies reviewed attention has been paid to IT and IT Systems technical detail. The scope of inquiry is however wider than isolated technical details and considers integration scenarios and multidisciplinary complexities. The humans who interact with the technologies (the actors) trap and convey evidence in the scene that requires extraction. In different instances the actors are perpetrators and victims (both conscious and unconscious) (Gonzalez, Sarriegi, & Gurrutxaga, 2006). Social engineering concerns the deception of people in order to have them disclose systems sensitive information that can be used to compromise integrity and to defraud the system of resources. The manipulation of people, in addition to the errors and inadvertent mistakes they make, are significant security risks (Workman, 2007). The potential for disclosure of information that leads to the compromise of passwords, encryption keys, SI codes, SI prices, and other mission critical information is high. The Business System security risks described in Section 3 are increased when social engineering is added into the mix (Quin & Burgoon, 2007).

The social engineer is able to extract information that may provide precision in an attack and also leave less digital evidence. The perpetrator also requires less technical knowledge and can execute a social control strategy (Samani, 2010). The common approaches of impersonating roles, such as friend, colleague, technician, authority figure, and so on are less effective than an employee compromising the Business System. In this way the exact and sensitive information regarding the SI Tags, the POS processes and the BIS architecture may be disclosed. The technical security measures such as release mechanisms and encryption are generally reliable, robust and effective controls. However, the people who specify, build, use, and manage the Business System can be persuaded into overriding the control system. Social engineering is a powerful technique for gaining unauthorized access to confidential proprietary or personal information. The risk to the Business System is escalated by drip feed gains where an attacker starts with publicly available information and then leverages the knowledge for social relationships and escalating gains of sensitive information. The approach includes coercion (eg. blackmail) and different sequenced win-loss situations for a targeted internal customer (current or former). The soft edge of profiling is trivia including casual gossip and rumours, and the frame internal procedures, roles and responsibilities.

The system impact of successful social engineering has consequences over a range of business performance indicators. In our study we are principally concerned with theft and hence the additional risk social engineering has for Business System violation. Loss of integrity, trust, system utility and other collateral damages caused by

successful social engineering fall outside of the interest. The interest focuses on criminal activity and the potential to collect robust digital evidence.

TESTING REPLICATIONS

To investigate the presence of digital evidence after the theft of a Stock Item (SI) a prototype of commercial retail environment using a RFID stock management system was constructed in the laboratory. Previous studies were replicated (eg. Haines, 2006; Rieback, et al., 2006). By design two (one real and one poisoned) RFID Read/Write tags were applied in a stabilised retail Business System. The SQL poisoning attack was launched through the RFID Tag and then each entity in the Business System investigated for evidence of the theft. Evidence extraction occurred from the tag, the scanner, the POS and the SQL server. In addition CCTV and interview evidences were considered relevant to the investigation.

Research Design

The research had five phases. A search of IEEE and ACM publications in RFID systems was conducted for the past 10 years. The Literature was analysed and the learning compounded. An environment was created within the laboratory to simulate a RFID Tag retail stock inventory system with SI, POS and BIS entities. The system was then stressed by a series of different attack type and category (the SQL injection attack is reported here). On the completion of an attack each entity, sub-system and service were interrogated to identify evidence left from the attack. The final phase consisted of an evaluation of the learning in the form of data analysis and presentation. A descriptive research approach was used throughout with the intention of reporting the precise detail of architectures, digital evidence storage locations, and compliant extraction techniques.

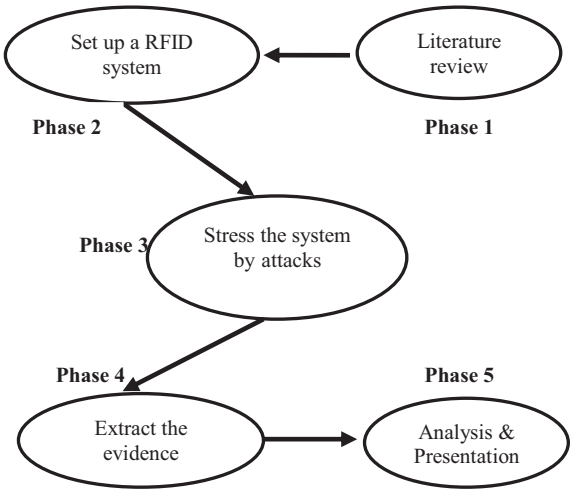

Figure 2. Research Design

Data Collection

The test scenario was a violation of a secure Business System with a SQL injection attack that was injected on a poisoned RFID Tag. Two Tags were used to represent the real Tag and the poisoned Tag. The Tags were ISO 18000-6B operating in the 860 – 960 MHz range and with 1728 bits of memory and a 64 Bit ID size.

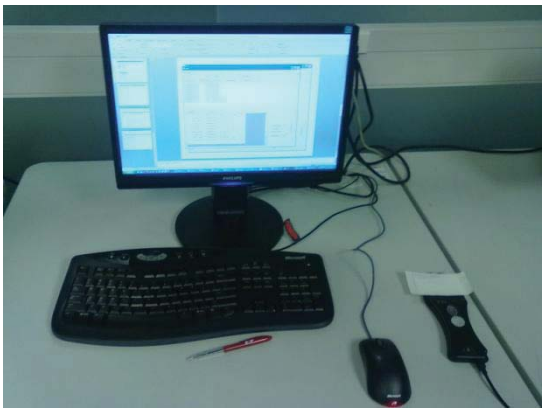

Figure 3. Fake tag is read by the RFID reader

Before the attack simulation, the two databases were created in the BIS Microsoft SQL 2005 server. The primary data file named RFID_test.mdf was used for storing stock values according to the RFID tags. Likewise, the transaction log file named RFID_test_log.ldf was used for storing the reader logs to the backend server. Then, all the fictitious product values and tag IDs were pre-keyed into the database files. Examples of inserting the values (1000) into the primary data and log files are as follows:

```
insert into rfid_db ( Tag, Value,Date) VALUES ('E0040000E90A4301', '1000','17:19:51 02/07/2010');
insert into rfid_log ( Tag, Date) VALUES ('E0040000E90A4301', '17:19:51 02/07/2010');
```

The malicious code is written into the user memory of the fake RFID tag (as shown in the Figure 2.) in order to change the value from $1000 to $10. The inserted malicious code is 55 bytes and the command is:

```
');update rfid_db set Value='10' where Tag > 'E004%' --
```

The injected command changed the values relating to the tag IDs starting with E004 in the database table.

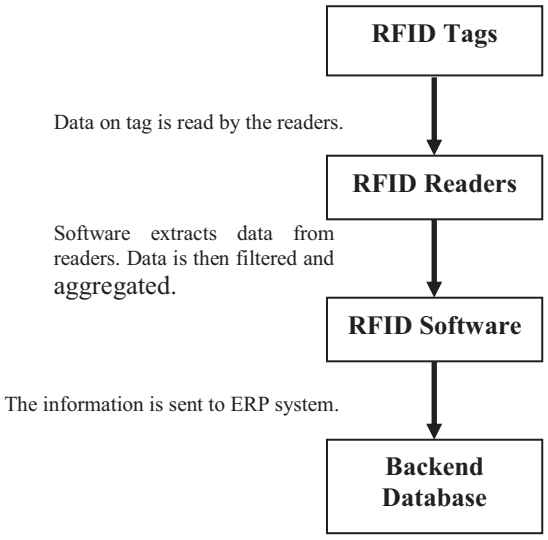

Figure 4. Information Functions of RFID Middleware Software

The data collection methods were necessarily designed to fit a laboratory simulation. In a commercial Business System the context would be similar but there would be many more tags, data entries in the log and the whole world of commercial human computer interaction. The method and the techniques were sufficient to test the vulnerability of a system. The scenario is instructive for an investigator who wishes to understand the scope of evidential potential in a Business System without becoming lost in the complexity of such specific attacks. In the next section the processes of preservation, identification and acquisition are described.

EVIDENTIAL SEARCH

The primary concern is to preserve the evidence. The volatility of the evidence is apparent around the SI (including the scanner) and the POS. The volatility is driven by security policy and the business practices adopted in any particular enterprise. Policies that manage the Tag processes will also determine the availability or otherwise of the poisoned Tag for evidential purposes. In most instances a Tag is removed at the POS and placed in a secure receptacle for future rewriting. A poisoned Tag has potential for rewriting and the erasure of the poison code. Similarly the BIS architecture will determine the storage capabilities of the POS and the scanner. In some instances the scanner has a continuous wireless feed into the BIS and in others it stores evidence. The stored evidence has cycle times where previous entries are erased and the memory reused. The POS is also dependant on BIS architecture. In some instances the POS stores transactions on a hard drive and in others routs directly to the server/ data warehouse. Each variation requires investigation to determine system and to assure the best preservation rate for evidence.

The identification of evidence in the simulation was simple because the researchers determined the system architecture and chose the hardware capabilities. Also the Lab context had no business processes or policies to obstruct the access to evidence. As a consequence the poisoned Tag was available after the event, the scanner log was complete, the POS hard drive and RAM chip were available, and the database backend had under 500 entries that could be accessed. The challenge was to follow correct process in extraction and then to conduct an analysis that would locate the attack event amongst the potential of many transaction occurrences. Again the laboratory context simplified the extraction and analysis phases. In addition the further investigation of the business system by interviewing the human participants and reviewing CCTV footage was not relevant. In the Business context the evidence extracted from the server logs and the POS and scanner logs (if available) could be utilised to speed the search of CCTV frames. The dates and time that are located in the logs can be matched against frames of visual surveillance and witness statements.

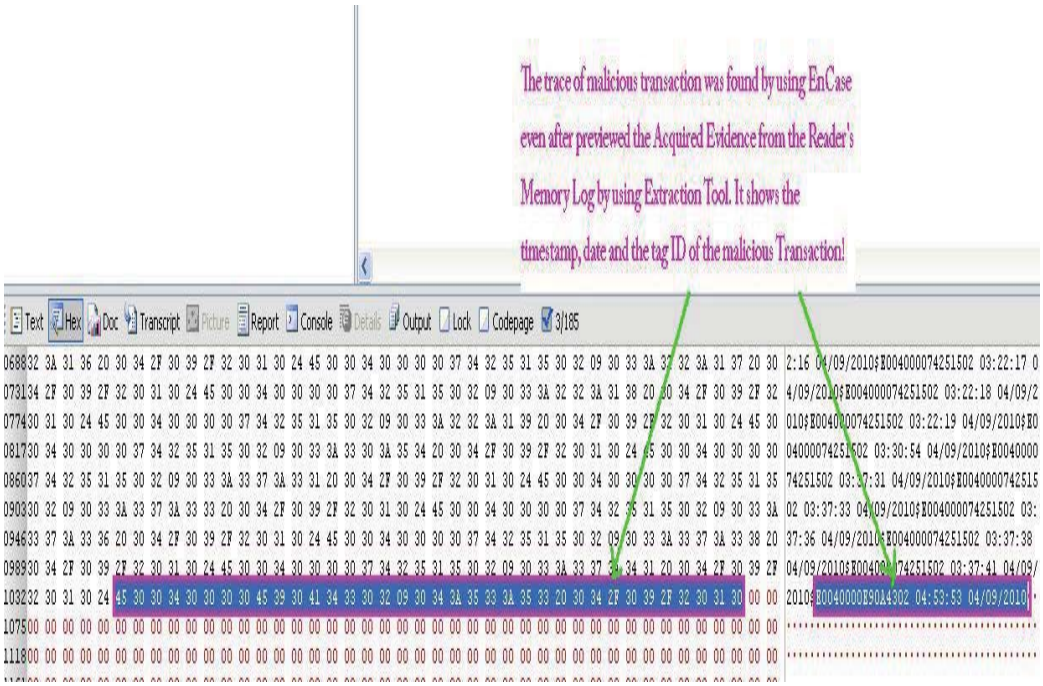

Figure 5. Forensic Image of Scanner Log

In the laboratory simulation the POS had a hard drive and also a RAM chip, and dumped complete records into the SQL Server on demand. Two data bases (RFID_test.mdf & RFID_test_log.ldf) had been created prior to the simulation to hold the authentic SI records and also to record each transaction. The Scanner stored 1Mb of log evidence that recorded transactions line by line (ID & Time Stamp). When the buffer was full then the algorithm started again at line one rewriting each record in the Scanner memory.

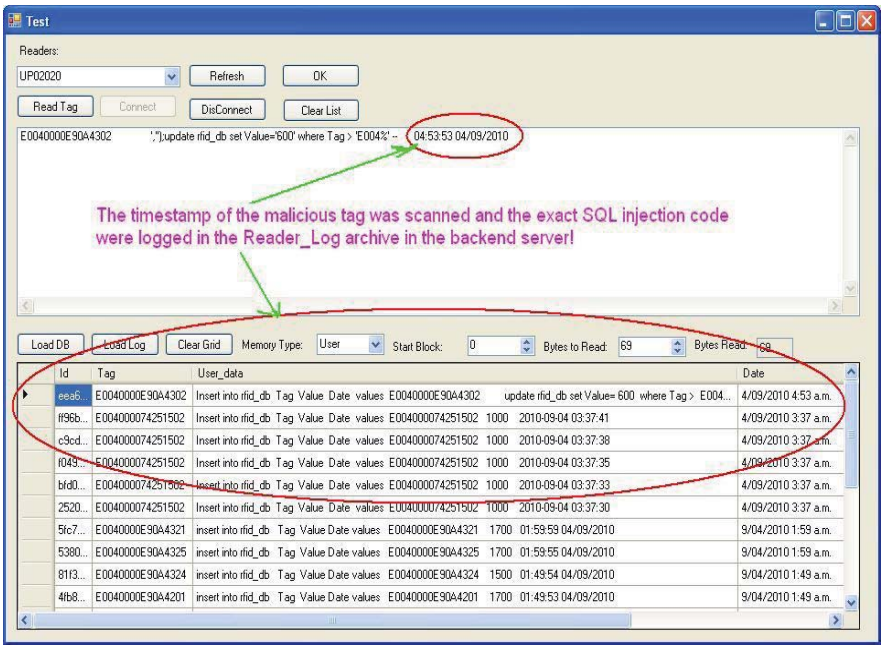

Figure 6. Forensic Image of Server Log Files

The evidence acquisition was achieved by taking each element of the SI, POS and BIS and then write blocking each extraction (this included using ddcfldd for hashing). Helix RFID IR2 was taken from the Incident Response Took Kit and customised so that other tools could also be used securely within the extraction framework. This included WinEn for RAM extraction and RFID code extraction. The physical hard drive of the POS was imaged using FTK Imager (Disk Jockey Pro was available as a backup if any problems occurred), and the SQL Server imaged using Windows Forensic Tool Chest (WFT). The three Figurers 5-7 show screen shots of forensic images taken from the scanner, the transaction logs, and the SI records.

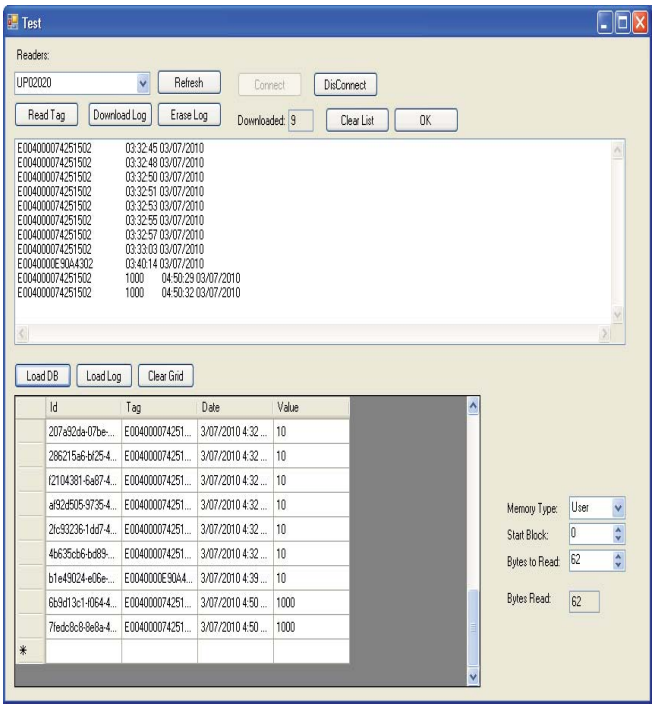

Figure 7. Forensic Image of SI Record Change from $10 to $1000 and Back

The Forensic image Analysis focused on each artefact extracted from the three entities of the simulated BIS and the sub-systems identified in Table 1. Encase was used as the Forensic Test Station. Initially a visual scan of the

Master Server Log was made to quickly identify where SI values had been changed. In a real business search the technique to query the transaction logs in the Master Server Log would have been more complex and time consuming. Such a search can be bench marked from stock controls and the legitimate time stamps of value alterations. In the simulation it was quick to visually review 500 entries all of $1000 and then observe where the $1000 was changed to $10 and then back to $1000 (see figure 7). The time stamp identified was then used as a keyword search in the other images. In the Server Transaction Logs the Keyword search then identified the Tag ID (identification) string (see figure 6). At this point in the analysis enough evidence had been discovered so that the analysis of the RAM, Tag and Scanner would be for verification and exception evidence. In a real search the existence of evidence in these subsystems would be a bonus given the volatile state (see figure 5 example). In the simulation the evidence was present in each of the subsystems and it was searched for time stamp and ID strings. The Tag also contained the malicious code that can be signature matched for identification of potential sources.

The evidential search of a RFID business system would hence proceed by preserving the evidence of the volatile entities and subsystems. Forensic Imaging would usually proceed from the most volatile to the least however in this business system the key evidence can be located in priority from the Server BIS, the POS and the SI. If the SI evidence has been lost on account of volatility then the Server Image should contain sufficient detail from which to fully investigate the system. Hence the SI and POS can be isolated (define system first) and the Server Imaged as a priority. The simulation did not have human actors or CCTV dimensions. The evidence from these sources would normally be imaged at the same time and in the analysis phase the ID and time stamps from the related sources used to speed the extraction. The analysis phase may also lead to a second round of human interviews. These matters are not considered in the simulation.

CONCLUSION

RFID controlled stock inventories are not trustworthy and with the best securing still have a significant residual risk of violation. Evidence is located in a complex business environment that has elements of technicality, informatics and humanity. In this example the theft of a SI through an orchestrated test scenario of hardware, software and social engineering illustrates the potential and vulnerability. The evidence after such a successful attack can be found principally in the server logs, but also in interviews with human actors and in surveillance devices. To a lesser extent the evidence stored in scanners and tags may be available. Forensic extraction can proceed using the standard practice of write blocking, forensic imaging, preservation and analysis.

REFERENCES

Altschaffel, R., Kiltz, S., & Dittmann, J. (2009). From the Computer Incident Taxonomy to a Computer Forensic Examination Taxonomy. *Fifth International Conference on IT Security Incident Management and IT Forensics, 2009 (IMF '09)*, 54-68. USA: IEEE Computer Society.

Bhargava, H. (2006). RFID Security: Attacking the Backend. *Syngress Force 2006 Emerging Threat Analysis: From mischief of malicious* (pp. 503-513). Rockland, MA: Syngress Publishing, Inc.

Bolan, C. (2007). A Single Channel Attack on 915MH Radio Frequency Identification Systems. C. Valli & A. Woodward (Ed.), *Proceedings of the 5th Australian Information Security Management Conference* (pp. 8-16). Perth, Western Australia: School of Computer and Information Science.

Chalasani, S., & Boppana, R. (2007). Data Architectures for RFID Transactions. *IEEE Transactions on Industrial Informatics, vol.3*, no.3, pp.246-257, Aug. 2007

Chalasani, S., Boppana, R. V., & Sounderpandian, J. (2005, August 11-14). *RFID Tag Reader Designs for Retail Store Applications.* Paper presented at the Proceedings of the Eleventh Americas Conference on Information Systems (AMCIS 2005), Omaha, NE, USA.

Chawla, V., & Ha, D. S. (2007). An overview of passive RFID. *Communications Magazine, IEEE , 45*(9), 11-17, September 2007.

Ding, Z., Li, J., & Bo, F. (2008). A Taxonomy Model of RFID Security Threats. *In IEEE International Conference on Communication Technology Proceedings (2008), 765-768.* USA: IEEE.

El-Said, M. M., & Woodring, I. (2009). An Empirical Study for Protecting Passive RFID Systems against Cloning. *Sixth International Conference on Information Technology: New Generations, ITNG '09, vol.,* no., pp.558-563, 27-29 April 2009.
Gonzalez, J., Sarriegi, J., & Gurrutxaga, A. (2006). A Framework for Conceptualizing Social Engineering Attacks. *Critical Information Infrastructures*, 79 - 90.

Haines, B. R. (2006). RFID Attacks: Tag Encoding Attacks. *Syngress Force 2006 Emerging Threat Analysis: From mischief of malicious* (pp. 433-445). Rockland, MA: Syngress Publishing, Inc.

Harrill, D. C., & Mislan, R. P. (2007). A Small Scale Digital Device Forensics Ontology. *Journal of Small Scale Digital Forensics, 1*(1), 1-7.

Jeng, A. B., Chang, L., & Wei, T. (2009). Survey and remedy of the technologies used for RFID tags against counterfeiting. *2009 International Conference on Machine Learning and Cybernetics, vol.5,* no., pp.2975-2981, 12-15 July 2009.

Jones, A. K., Hoare, R. R., Dontharaju, S. R., Shenchih, T., Sprang, R., Fazekas, J., Cain, J. T., & Mickle, M.H. (2006). *A Field Programmable RFID Tag and Associated Design Flow. The 14th Annual IEEE Symposium on Field-Programmable Custom Computing Machines, 2006. FCCM '06, vol.,* no., pp.165-174.

Khannaa, N., Mikkilinenia, A. K., Martonea, A. F., Alia, G. N., Chiub, G. T., Allebacha, J. P., & Delpa, E. J. (2006). A survey of forensic characterization methods for physical devices. *Digital Investigation, 3S*(2006), S17-S28.

Kim, D. S., Shin, T., & Park, J. S. (2007). A Security Framework in RFID Multi-domain System. *The Second International Conference on Availability, Reliability and Security, ARES 2007, vol.*, no., pp.1227-1234, 10-13 April 2007.

Landt, J. (2005). The history of RFID. *Potentials, IEEE* , vol.24, no.4, pp. 8-11, Oct.-Nov. 2005.

Li, X., Xu, G., & Yu, D. (2008). Security architecture for RFID application in home environment. *The 2nd International Conference on Anti-counterfeiting, Security and Identification, ASID 2008*, 467-470.

Martone, A. F., Mikkilineni, A. K., & Delp, E. J. (2006). Forensics of Things. *2006 IEEE Southwest Symposium on Image Analysis and Interpretation,* 149-152.

Masters, G., & Turner, P. (2007). Forensic data recovery and examination of magnetic swipe card cloning evices. *Journal of Digital Investigation, 4S*(2007), S16-S22.

Michael, K., & McCathie, L. (2005). The Pros and Cons of RFID in Supply Chain Management. *Proceedings of the International Conference on Mobile Business (ICMB'05).* USA: IEEE Computer Society.

Ohkubo, M., Suzuki, K., & Kinoshita, M. (2005). RFID Privacy Issues and Technical Challenges. *The Communications of the ACM, 48(9),* 66-71.

Qin, T., & Burgoon, J. K. (2007). An Investigation of Heuristics of Human Judgment in Detecting Deception and Potential Implications in Countering Social Engineering. *IEEE Intelligence and Security Informatics* (pp. 152-159).

Rao, K.V., Nikitin, P. V., & Lam, S.F. (2005). Antenna design for UHF RFID tags: a review and a practical application. *In IEEE Transactions on Antennas and Propogation, 52*(12), 3870-3876.

Rieback, M. R., Simpson, P. N. D., Crispo, B., & Tanenbaum, A. S. (2006). RFID malware: Design principles and examples. *Journal of Pervasive and Mobile Computing, 2*(2006), 405–426.

Rieback, M.R.; Crispo, B.; Tanenbaum, A.S. (2006). Is your cat infected with a computer virus? Pervasive Computing and Communications, 2006. PerCom 2006. Fourth Annual IEEE International Conference.

Rotter, P. (2008). A Framework for Assessing RFID System Security and Privacy Risks. *Journal of Pervasive Computing, IEEE Computer Society, April-June*(2008), 70-77.

Samani, R. (2010). Re-defining the human factor. *Infosecurity*, 7(2), 30-33.

Tu, Y., and Piramuthu, S. (2008). Reducing false reads in RFID-embedded supply chains. *Journal of Theoretical and Applied Electronic Commerce Research, 3*(2), 60-70.

Workman, M. (2007). Gaining Access with Social Engineering: An Empirical Study of the Threat. *Information Systems Security*, 16(6), 315-331.

Zhang, M., Li, W., Wang, Z., Li, B., & Xia, R. (2007). A RFID-based Material Tracking Information System. 2007 IEEE International Conference on *Automation and Logistics,* vol., no., pp.2922-2926, 18-21 Aug. 2007.

Zhou, Z., & Huang, D. (2008). SRK: A Distributed RFID Data Access Control Mechanism. *IEEE International Conference on Communications, ICC '08, vol.,* no., pp.2854-2858, 19-23 May 2008.