Jacob Ellis

I.T. JEllisy, Inc.

Technological Consulting firm

7/25/11

Self-checkout Kiosks in general have many different types of vulnerabilities, some that are physical (hardware) and some that are logical (networking capabilities or software programs). Beginning with the physical aspect, a basic vulnerability would be the chance of service degradation, dealing with electric power to run the kiosk, Internet to allow for transactions, and communications. If these utilities were to go out then the whole system and physical components would not be able to function correctly. The reason this is physical even though none of these resources are tangible, is because of the power cords, Ethernet cords, as well as any telephone or other wires that may be connected to the kiosk; if any these physical connections where to go bad or disconnect, then the whole kiosk would suffer.

Another large vulnerability of the self-checkout Kiosk is the use of self-scanning technology. This means each customer scans and operates the unit personally with limited security from the store employees, leaving each individual ample time and ability to adjust some minor physical component. If a threat agent adjusted a component such as the cash dispenser or credit card reader, it may result in stolen credit card numbers or loss of cash from dispensing too much or too little. A similar way to collect credit card information would be, if a threat agent were to plant video cameras within the store in order to catch the customer’s credit card information. Multiple video cameras could catch the front and back of the card, as well as the pin number they type into the keypad before giving their signature. This technique would allow the criminal to access all of the customer’s credit card information while they use the self-checkout kiosk.

A different type of physical tampering may be, fooling the kiosk by switching the tags on the products that the threat agent is scanning, so that the computer believes it scanned a different item than was actually purchased. If the customer switches out the barcode tag on one product for a cheaper but similar product, then the computer wouldn’t know the difference and the customer would be able to pay less for a more expensive product. Lastly, a kiosk has the obvious weakness of being completely stolen although it may be very difficult and unlikely. Every physical object has a chance of being stolen even thought this kiosk is inside of a protected store with employees, video cameras, and is probably very large.

Now that all of the vulnerabilities have been identified, there must be some type of security to prevent issues from occurring. To begin, each organization should have a policy implemented for each and every employee to agree to and follow. If this is understood and appreciated it should minimize many errors and physical tampering. The employees have the responsibility of monitoring the kiosk to protect it from illegal video surveillance, credit card readers, and theft. In order to protect the kiosk from service degradation, the organization should have a contract with the service provider that will commend the SLA; as well as having back-up generators, protective coverings over the physical connections to the kiosk, and an emergency plan practiced and ready to implement at a moments notice. To protect the organization from theft by switching barcode tags, the kiosk should be able to detect the weight of a certain product so that if the price tags were to be switched, the computer would notice a difference. Also the employee that is monitoring the kiosks should notice if the handheld computer says something different than what was placed into the cart.

Moving from the physical aspect over to the logical aspect, a self-checkout kiosk has very complex software components that deal with a large number of information systems. If any vulnerability is found and exploited, an unknown amount of data could possibly be accessed such as customer credit card numbers, SSN of employees, as well as other personal information that could cause harm if released. One possible attack is using a packet sniffer in order to see all of the information passed through the data connection. Most of the time this would consist of credit card information and maybe points based rewards cards depending on the grocery chain. Although it may be able to gather information being transmitted off of the employee’s hand held device that is used to control the kiosks. These handheld machines have access to parts of the kiosk that normally a customer would not be able to control; if the sniffer could trap those signals and find a way to use those signals or recreate the handheld machine, a threat agent could create his/her own device and use it to steal items or disable security features.

One of the more common Vulnerabilities of the software system would be a general hack of the system that controls all of the information systems for the grocery store chain. If a hacker could access the system, they would have all of the information processed and saved in the store. This would allow them to gather information from the self-checkout kiosks, as well as the employee-operated computers. This can also consist of hackers implementing malware such as a virus, worm, Trojan horse, logic bomb, or accessing a back door to the system.

Some ways this can be protected are similar to ways that most information systems protect any software and data. Security features such as firewalls for all Internet access, information and access on need-to-know basis, keeping software and security features up to date, and policy agreements. All of these components are essential to securing a system, although it is extremely difficult to balance every aspect. Firewalls will protect the system from unauthorized access and malware trying to enter the network. Information on a need-to-know-basis will protect the integrity of the data by disallowing any single person the knowledge to a large component of the organization. This means that the system cannot be hacked or modified by one single person; it would need multiple people with different types of information. Software updates are crucial in protecting a system, due to the fact that hackers break into new versions of security software every year, so updating the software forces them to adapt and learn new techniques that may keep them out. Lastly, policies are one of the easiest and most important security features because the way the company handles themselves, can determine how well the organization protects their assets. This includes the actions and attitudes of the employees that are dealing with the kiosk, all the way to the IT professionals working on the system. If the policy states that the software is required to update every six months then it has a greater chance of being secure than one that would update every twelve months.

Environmental hazards are always a large component of physical security and the design of the machine itself. The hardware should be made of a combination of hard metal and plastics to protect it from physical damage along with wear and tear. Since it will be used in a grocery store, we may want to consider adding metal guards on the corners of the machine, two or three feet high, to protect it from accidental collisions with shopping carts or baskets. Also any exposed area that will be used for direct contact with the user should be sealed tight to protect from liquid spills and damages, in order to protect the wires and other internal components from damage. Assuming that the machines will be placed inside of the actual grocery store we shouldn’t have to be too critical about the threat of weather protection. Although to protect if a flood were to occur, the machine should be placed on a “Riser” to lift it and all components such as wires, off of the floor to protect it from getting wet.

In order to protect the cost of the kiosk machine, the grocery chain should take steps to require some type theft or damage insurance in the contract from the supplier that states, if the kiosk were to have issues or malfunctions while under normal working conditions then they must diagnose the problem and take all measures to ensure the organization receives proper maintenance or replacement. Also, the grocery chain could possibly claim an external insurance agency so they would be liable to cover the loss instead of the store. Although this may be considered as adding additional security for the system due to the fact that the chain is paying for this service in case something were to happen to the kiosk.

Moving into the legal organization’s perspective. What if it was found that the system software was equipped with a backdoor or other vulnerability that was planned by a software engineer? There would be plausible cause to investigate for criminal acts due to the violation of the Computer Fraud and Abuse Act (CFA Act), Criminal Law, as well as the Federal Privacy Act. The CFA Act formalizes laws to counter threats from computer-related acts and offenses such as this one. This applies to the insertion of a back door in a system for exploitation and in result, should be taken into consideration for charges on the author of the code. Criminal Law regulates activities deemed harmful to society and is enforced by the state. The reason why this law is involved is because the backdoor could lead to theft of personal information with intent to steal monetary assets or identification, in order to gain from someone else’s loss. The Federal Privacy Act prohibits unauthorized access to personal information, even though the only way that this back door would infringe on the Federal Privacy Act is if the software allowed someone to gain access to information and the information was obtained.

If the self-checkout kiosk were to go down at any time for any reason, it would become a priority to get it up and running again. The reason this is so important is because while the kiosk is down, the grocery store is not collecting in on the $4000 worth of items that are sold per day, by using that system. Not only would they be losing out on the profits of the machine but they would possibly have to hire more employees to compensate for the down machines, which would cause in increase in labor costs by approximately 1000$ per day.

If the organization wanted to add extra security measures to protect this kiosk we must ask questions like; how much money is this worth? Is it worth paying for extra security rather than just buying a new one? The machine itself holds about $500 at any given time, so if it were to be stolen, the initial loss would be the $500; although, if the machine was compromised beyond repair then the only loss would be the purchasing price of a new kiosk. The cost of a brand new kiosk is approximately $20,000, so the total loss if stolen would be $20,500 and $20,000 if out of order. Now the question is; would we have to pay more than the cost to replace the kiosk in additional security to protect this machine? If the price of adding significantly better security is less the amount of the loss, then the protection is feasible. But, if the cost of protecting the machine is more than the value of the machine itself, then it might be better to just let it go and purchase a new one. The machine’s value is determined on the basis of the number of years it has been depreciated, the machine’s benefits, and current condition. If the machine was originally worth $20,000 but due to the depreciation and current condition, was only worth $1000 when it was stolen. Then the company may decide it was a good time to replace the machine any way, if it was beneficial to the organization.

Jacob Ellis

Exam 1 part 2

Points: 20

<http://www.ibtimes.com/articles/184607/20110721/fake-apple-store-china.htm>

In China’s Yunnan province, the city Kunming, was found with a fake Apple store fully equipped with the Apple symbol on the door, wooden tables, and the famous “genius bar” employees to finish off the legitimate look. The employees of the “fake” store even believed they were working for apple as if they didn’t know the store was a fraud. The store was selling counterfeit or stolen Apple products claiming they were real; even promoting such items with large banners and posters.

The false Apple store provides a look at the security flaws that must be addressed by the Apple Corporation. I believe that Apple must be able to protect its image as well as products with a strict governing policy. In this policy, every store is required to register the new location with the national headquarters prior to opening; as well as registering the products that they sell. By registering the location, it will legally notify the organization that a new store is being developed. The location of the new store must receive the registered paperwork prior to being allowed to move in. This policy will prevent the unauthorized openings of Apple stores as well as minimizing the amount of illegally sold products.

Secondly, Apple must update and manage the security of their copyrights, patents, and Trademarks. The store’s use of the signature Apple symbol as well as numerous advertisements was likely illegally duplicated. If the legal aspect of this were to intervene then the false store would have had a much more difficult time opening its doors. Increasing the legal actions taken on by the company would increase the security.

Thirdly, Apple could develop new security software that prevents unauthorized users from hacking into the device. The software would minimize the ability to use stolen devices, which in return would reduce the amount of illegal sales such as the fake. Also, the software could prevent the possibility of stolen personal information that is kept on hacked devices. This security feature allows the organization to protect the physical security of devices as well as security of the system from being hacked.

Sun Tzu’s Art of war says, “Know yourself and know your enemy”. This correlates with this article because if Apple were to know “themselves” as an organization, they would know the amount of stores that they have in operation as well as ones that are not. Knowing your enemy would mean that Apple would know the intensions of their consumers and competitors. The enemies in this case were the thieves that managed to find their way around Apple policies as well as physical security. Apple should assume that people are going to steal their products in order to produce some type of profit. So they should be ready to prevent or end that type of attack, if they knew their enemy.

<http://voices.washingtonpost.com/fasterforward/2011/03/google_activates_kill_switch_t.html>

Google’s Android platform has been “attacked” from a series of Trojan Horse viruses in their Android Marketplace which existed as applications available for download that were not doing what they were intended. The virus was said to have downloaded other unidentified code in the background of the OS, as well transmit the phone’s electronic ID number. Google is actively researching ways to correct and prevent this from happening again.

In order to monitor the possessed applications, Google has decided to use its control of the Android market to perform a mass removal of all violations on the network. This procedure has never been performed on such a large scale, which showcases the lack of security control that Android has on its application market. For those users whom do not carefully exam each app before downloading or purchasing, there must be some type of security measure to prevent the access of malicious applications.

I believe Google should implement a new policy stating the requirements of each application before it is permitted onto the Android market. This policy should require a safety certification that proves the application wishing to enter the market, is secure in all software aspects. This would be achieved in steps, beginning when the author submits an application for the developed app to be added to the market. This application is essentially a resume for the app, explaining why it deserves to be used publicly. Once the application was received and if accepted by Google, the author would be required to send the source code of the app in for inspection by Google professionals. This process would take long periods of time and possibly extra manpower, although it will be providing excellent security for each Android user.

The new policy, in the business aspect, would potentially attract new customers to the Android marketplace in their search for the latest and greatest applications. It would give their brand an improved reputation among the communities of interest as the most reliable and secure location to download apps. On the contrary, it could also deter some application developers because of how slow it takes to process each new application. With a slow acceptance rate, the developers may choose to work towards other OS such as iphone apps instead, which could possibly hurt the value of the Android market.

Secondly Google should require all phones and other devices to upgrade to the newest version of the OS, 2.3. This version does not have the same vulnerability of exploits as the previous version, which protects users from malware such as the one recently infecting Google phones. Essentially, updating the version of the phone is software security because the user is using a new and improved system that will prevent hackers or malware from entering the system.

Sun Tzu’s Art of war says, “Know yourself and know your enemy”. In this case, Google needs to understand the Android marketplace and all of the applications available. Knowledge of all of the applications includes the purpose of use, as well as the code used to perform that purpose. If the code of the app is malicious, then Google should know that before allowing it on the network. Knowing the enemy means knowing the possibility of what they can do. Assuming that everyone app created has the potential to do harm to an individual or organization. By understanding this, Google would be able to effectively protect their market and users.