

Running head: THE DANGERS OF MOBILE COMPUTING

## The Dangers of Mobile Computing

Joshua J Sawyer

East Carolina University

## Abstract

In today's world of fast-paced communications, the need to access data while physically away from the workplace or home has greatly increased. This has given rise to the practice of mobile computing, which is often taken for granted by many users. While mobile computing is often seen as an efficient, alternative way of completing tasks, it can also be used by attackers as an avenue through which to steal and manipulate data. Solutions to common problems are discussed, as well as practical steps users can take in order to minimize the risks resulting from mobile computing. In addition to the technical solutions, emphasis is also placed on user awareness and education. Imaginary scenarios as well as actual incidents are presented to assist in the retention of the information presented. The primary target of this paper is the corporate / business user. However, the analysis given will certainly apply in the home setting as well, especially to users that frequently access data from home remotely, or use portable computing devices of any type to store important data. Current trends and statistics are also provided in order to show which areas are often overlooked, and which areas users should focus on. The concepts discussed here should be considered mandatory knowledge for anyone who uses a laptop, pda, or other portable device to access or store important data.

## The Dangers Of Mobile Computing

Easy, fast and convenient: these are attributes commonly associated with mobile computing. All too frequently, however, they disguise the many dangers created by this common practice. Performing seemingly simple tasks from a remote device, such as checking email, working on business documents, or even discussing sensitive issues via VOIP (Voice Over Internet Protocol), can enable attackers to monitor and access everything accessed, if the mobile computing device and the remote systems are not properly secured. This can enable almost anyone: business competitors, restrictive governments, hackers, and others, to build a profile of the user's activities, and possibly even their identities. Alternatively, attackers can perform DOS (Denial Of Service) attacks, in an effort to disconnect legitimate users from working remotely altogether.

Although these attacks are used by many malicious users, they can be avoided by using mobile computing securely. A common fallacy is that encryption is the solution to all problems, and that, when using it, the user is invulnerable to these types of attacks. This could not be further from the truth. Although today's headlines are increasingly filled with businesses losing data to criminals due to not using any encryption whatsoever, it is becoming more and more evident that encryption alone is not enough. If not properly implemented, encryption can be easily bypassed, cracked or breached by using tactics such as: keylogging, physical media analysis, social engineering, wireless monitoring, electromagnetic interception, use of trojans, among numerous other tactics. It should be evident that encryption, although extremely helpful when correctly implemented, cannot be relied upon solely to solve all the problems created by mobile computing. In order to combat these vulnerabilities, a complete approach must be adopted. This should include an educational approach as well as a technological one. The true

degree of security is the users' ability to recognize and thwart malicious attacks, and this can only be accomplished via a combination of both knowledge as well as technological tools.

Mobile computing, like any other type of remote communications medium, frequently uses insecure media to provide connectivity to the user's target network. The medium used can include: fiber cables, traditional copper cables, wireless links, satellite links, and other types of connections, which carry the users' information. (Figure 1). In addition to using numerous and diverse methods of delivery, the insecure internet network frequently travels through numerous countries, each having different standards of how information should be handled, if any. This allows data monitoring or loss to easily occur without the user's knowledge. For example, a business professional using a laptop to access her email via a normal website (without SSL enabled) may be giving her login credentials, as well as any emails read / sent during her session to anyone who may be monitoring traffic on any one of the many stops her data passes through to reach her email provider. The average online connection travels through many different countries. This may include satellite links being transmitted to space and back, intercontinental cables, wireless links, and many other types of links. SSL alone is not the ultimate solution, but it does assist in preventing data disclosure while accessing information online. In addition to monitoring her data via network components located in various countries around the world, an attacker could easily monitor the data being sent / received directly from her laptop if operating wirelessly. Compared to their wired counterpart, wireless networks are prone to security attacks ranging from passive eavesdropping to active interfering (Kong, J., Lu, S., Luo, H., Zerfos, P., Zhang, L., 2001, ¶1). Even if she is using WPA or a similar relatively secure method of access, the attacker could perform a wireless DOS attack by transmitting on the same frequency as her wireless link. This would deny her access to email and any other network-based services being

accessed. In this way, while using remote systems to perform tasks, users must be alert to these possibilities before solely relying upon mobile computing. Regardless of the different methods available for monitoring and modifying data on each of the different types of media, the entire network used to carry information from the users' machine to their target devices is an untrusted Internet zone. Therefore, in addition to securing the devices themselves, the users must also ensure that they are using a secure communications medium as well as be aware of the common methods used by attackers in order to thwart them. It has been said that an attacker's job is easier than the legitimate user's, because the user must constantly ensure that all systems and related devices are as secure as possible, while an attacker must only find one weakness and exploit it. In this way, users must be trained and knowledgeable about current tactics in order to stand any chance of securely defending mobile computing against attacks.

To begin, one must first concentrate on the most vulnerable area attackers can target while attacking a system: the user. Regardless of how secure any hardware / software security measures may be, all can be bypassed and rendered ineffective if an attacker can convince or trick the user into giving them access. The best way to defend against this method of attack is to educate the user about computer security and common tactics used by attackers, such as: theft of mobile computing devices (such as Laptops, PDAs, cellphones, electronic organizers, etc., enabling the possibility of divulging any data presently on or ever placed on the device), phishing (creating emails / websites that look similar to a legitimate bank or company in an attempt to steal the user's financial information or identity), shoulder-surfing (watching everything the user is doing on his/her computer, and trying to determine their passwords, etc), DOS, Denial Of Service attacks (overpowering a network or computers in order to prevent users from sending/receiving legitimate traffic), network monitoring (watching all data passing

through a specific device or part of the network in order to glean passwords and other personal information), exploiting vulnerabilities (such as open ports, clients without firewalls on high-speed connections, unpatched operating systems, devices infected with spyware, malware, viruses, etc.), using social engineering (calling the user and posing as a senior member of the company, demanding the user's logon credentials in order to solve an 'urgent' problem), and many others. If users are unaware of these methods of attack, it is very likely that they will fall victim to them. Now that these major scenarios have been discussed, some solutions are presented.

To combat these types of attacks, technological solutions are required, but the most important solution is educating the user. Once informed, the user will be aware of and prepared for these exploits. The alternative is comparable to sending soldiers into battle who have had no basic training. The majority of effective solutions are not necessarily technologically involved, but are rather very simple. When combined with technological solutions, the mobile computing user can be nearly invulnerable to the majority of attacks.

Perhaps the simplest and oldest technique used by attackers on computing devices as well as any device, is that of physical theft. A survey found an indication that people are more concerned about their privacy online than offline (Osback, P., Ryan, N., 2004, p. 4). Perhaps this yields the key as to why so many thefts of computing devices, and also the personal information contained therein, are occurring today. Users are constantly being reminded about the dangers of the Internet while the physical threat fades into the background. The old adage is definitely true: Without physical security, there is no security. An example of this technique being used by attackers is the case of the laptop which was stolen from Ameriprise Financial, a recent spin-off of American Express. The laptop was stolen from a parked car and contained 158,000

Ameriprise users' internal account numbers and the names and Social Security numbers of 68,000 Ameriprise advisers (ConsumerAffairs.Com, 2006, ¶7). The data on the laptop was not encrypted, so an attacker would be able to access this data with little effort. Although most laptops and other devices are often stolen for their physical value alone, this incident should illustrate that more frequently, attackers are becoming smarter and are targeting the data contained on the devices as well as the physical devices themselves. Encrypting the sensitive data on the laptop would have helped greatly in discouraging the theft of the data. However, if not properly implemented, it could be easily bypassed or cracked. While this incident involved the data present on the laptop, once an attacker has a device in his/her physical possession, they can gather most of the data that was ever written to the drive (deleted data) as well as the data currently on the drive, if secure deletion tools were not employed by the user. This gives the attacker a much more rewarding target: the data currently on the disk, and any deleted data which is intact, in addition to the physical device itself. The knowledgeable attacker will often copy any data presently on the device, try to recover any deleted data, then resell the device. The attacker can then sell the personal information or transfer it overseas to assist in identity theft and other financial crimes.

A recent theft of enormous magnitude occurred when a US Veterans Affairs employee's laptop and external hard drive were stolen from his residence. The devices contained the personal information of more than 26 million veterans (Smith, S.D., 2006, ¶1). The devices were eventually recovered, and the data is not believed to have been accessed, but this cannot be determined for certain, as a knowledgeable attacker would be able to mirror both drives without altering the contents of the original drives in any way. From this example it should be evident that one of the oldest methods used by attackers, physical theft, is still profitable, if not more so,

than in previous years. This increases the incentive to prevent this type of attack from occurring to begin with. To do this, users must ensure that they have any devices assigned to them in their possession at all times. Thoughtless practices such as leaving them in parked cars, airplane storage areas, etc., should never be allowed. A company training program which addresses this will also help in preventing these risky behaviors. The devices should also have all data on them properly secured via encryption or similar means which complies with the business' data policies. These protections should be implemented properly and tested to ensure they are performed correctly and securely. This is comparable to a database administrator who regularly backs up his/her data. Without checking the backups to ensure they aren't corrupted, there can be no assurance of their quality or usefulness. To ensure security measures are effective, they must be tested.

Another attack commonly used by attackers is 'phishing'. This is the practice of creating a fraudulent email which looks identical to a legitimate email from a bank or other company such as Suntrust, etc., in order to capture the user's login credentials. Often the attacker will include an 'all too convenient' link in the body of the email which will appear to go to the legitimate website, but will actually redirect the user to a website owned and created by the attacker. The website will look identical to the real website, and will ask the user to login with their username and password, and often also request their Social Security number, credit card numbers, etc. As soon as the user enters this information, it is stored in an online database or emailed to the attacker, who can now use it for identity theft or resell it for profit. This type of attack has become fairly common, and needs to be described to users as part of their security training program. Users can defeat this type of attack by monitoring their email closely to ensure it is really from who it says it is. If an email seems to be out of the ordinary, or is asking for the user

to update his/her information as soon as possible under the threat of account termination or something similar, it is most likely a fraudulent email. To be safe, users should be trained to read the contents of the email. Once this is done, they should open a new browser window and type in the link to the website the email maintains it was sent by. For example, if a user receives an email from Suntrust asking for personal information, the user should open a new browser and type in "<http://www.suntrust.com>". If the email is legitimate, the website will mirror the email's content. Users should never click on any links in emails. Always go directly to the legitimate website, and go from there. By doing this, users can avoid falling victim to this trap. A helpful tool to help users visualize what site they are truly on at any given time is "SpoofStick". This tool lists the website they are currently on, showing any fake websites for what they are if the user is on a fraudulent site. For example, if the user accidentally clicks on a link appearing to take them to: <https://www.suntrust.com/login.cgi?ID=344374&pass=x4Vr4E>, SpoofStick will show the actual domain they are on. If they are on a fraudulent site, SpoofStick may show something similar to: <http://suntrust.com.cn.info/login.cgi>. This will alert the user that they are not on the legitimate Suntrust website. However, if the user opens a new browser window and types in the web address for the legitimate site, SpoofStick will mirror this and show: <http://www.suntrust.com>. This is a helpful tool and is available from <http://www.spoofstick.com>.

Shoulder-surfing is a practice commonly used by attackers in mobile settings as well as in any location where users are in close proximity to one another. Essentially, an attacker observes a user while he/she is using a device. The attacker intends to catch any passwords or other personal information being entered. This attack can occur with any device, portable or fixed, as long as an attacker is within close proximity of the user, or is using optics to observe their actions. They will monitor the device's screen, keyboard, and any other medium which may

provide sensitive information. One way for users to prevent this attack is to maintain as much distance as possible between themselves and their neighbors, making it difficult for them to monitor their actions. Also, users may wish to use privacy filters if using a laptop in an airplane or similar close proximity environment. The privacy filter simply limits the viewing angle of the laptop screen to the user's view only, preventing neighboring individuals to the left or right from observing the screen. However, the best way to avoid this attack is to train the user to always be aware of their surroundings. They should be trained to never enter passwords or other sensitive information in the presence of an attacker. If necessary, they should cover their typing with one hand while entering their password with the other. This will prevent nearby users from observing their keystrokes. This is especially true in the rare event that a user must use a public computer, such as in a library, to check their email, etc. This is not recommended, as the systems most likely will have spyware and malware resident, which can steal the user's username and password, as well as track all activities accessed. However, in the rare event this is necessary, the user should use a preset 'one time use' password, which enables the user to use this password once, after which the email system discards it and enables an alternate password the user knows. If this is done, then the only risk in using the public computer is any tracking of the content accessed. Although extremely simple, this attack can be extremely dangerous if used on the unsuspecting user, and therefore they should be trained to be aware at all times.

DOS (Denial Of Service) attacks are another type of attack which can be performed on mobile as well as normal users. This attack basically seeks to deny legitimate users service by sending large amounts of data to the server, network, or both. Websites such as Ebay and Amazon were attacked using this method. The attack didn't involve breaking into the target Web site but simply overloaded it (Williams, M., 2000, ¶2). Such a large amount of data is sent

either directly to the target machine, or to a critical network device, such as a router. This enormous amount of data overloads the connection of the network device, blocking legitimate users from accessing the device as well as the target machine (Figure 2). While this often occurs with traditional websites, if the user is using a wireless connection while working remotely, they are vulnerable to a more concentrated and localized DOS attack. Wireless connections depend on a link between the network device serving the clients and the client devices themselves. If an attacker is within range of either, they can transmit on the same frequency which the network is operating on, thereby disrupting any communications and severing the link. This will deny users access to network resources. The best way to defend against this type of attack is to update the firmware in any network devices the user administers, if any. For the majority of mobile computing users, the best course of action is to be aware of who is on the network. While it may not be possible to know every user who is physically connected to the network, those connected in close proximity to the user can certainly be observed. If a user is experiencing problems with their wireless connection, they should readjust their antenna and / or move to another channel if necessary. Most newer wireless devices will do this automatically. Denial of service attacks also occur for non-malicious reasons, such as atmospheric conditions, other wireless devices close by, etc. Once again, maintaining a good survey of their surroundings is the best way for mobile computing users to combat this problem.

Network monitoring is a preferred method commonly used by attackers, both on mobile as well as normal computing users. This method of attack involves using a sniffer utility to monitor the users' network traffic, in an attempt to glean personal data such as surfing habits, usernames and passwords, ip addresses and other information. Packet sniffers are designed to intercept network traffic in shared communications channels (such as WiFi, ethernet, etc.).

Packet sniffing is primarily used in intrusion detection, network management, wiretapping, and hacking (Davis, L., Hale, J., Manes, G., Meehan, A. & Sheno, S., 2001, ¶1). The default nature of wireless communication includes that any two nodes within the wireless communication range may interact with each other over the shared wireless channel (Lu, S., Meng, X., & Yang, H., 2002, ¶23). While it can prove to be very effective, the attacker must somehow connect to a point on the network the user is presently on or a network connected to that network. If the user is utilizing a wireless connection, then this makes it even simpler for the attacker, as they need only monitor the airwaves for the users' data, as opposed to physically connecting to a network via cables. One example of this is a mobile user working on a pda to check his/her schedule while on a train enroute to their destination. While checking his/her schedule, the user logs into an email account via the Internet. Administrators often do, but attackers can also sometimes monitor all data transferred through specific network devices on the Internet as well, especially if they have previously compromised those devices (Figure 3). Even if no devices were compromised, the path the user's data takes to get to its' destination may include more wireless links, any of which could be easily monitored. This provides the attacker with any communications received / sent from the user while he/she is connected to the network. Depending on the network settings used and the website type visited, the attacker may be able to glean anything from usernames and passwords to entire email contents, or just ip addresses. This attack can also be performed, with perhaps even greater results, by monitoring the users' wireless connection. If an attacker is within range of the client's wireless device or the access point, they can monitor and record all traffic being sent / received wirelessly. Although this is the case, users can make their traffic much harder to analyze even if an attacker is listening. It is widely known that any traffic sent wirelessly can be intercepted and cracked at a later time. However, if setup properly, the user's

device can make this very difficult if not practically impossible. Most newer networking devices can support relatively secure network settings such as WPA2, etc. These standards should be enabled and utilized whenever possible to minimize the threat of network monitoring. Weak encryption standards such as WEP should only be used if no stronger encryption standards are supported by the users' hardware. Although this encryption standard is easily compromised, it is slightly better than the alternative of using no encryption whatsoever. Any WLAN should be considered a hostile environment, which means an end-to-end encryption protocol (e.g., SSH and SSL/TLS) or a secure VPN (Virtual Private Network) must be used for remote access over WLANs (Nakao, K., Nogawa, H., Rikitake, K., Shimojo, S., & Tanaka, T., 2004, ¶22). Users should utilize VPNs whenever possible to encapsulate their data while performing mobile computing tasks. In addition, using SSL enabled websites will assist in protecting any data transmitted / received during that session. The best protection will occur when users utilize all of these solutions together. For example, if a mobile employee uses her pda to access her corporate email, she may first access a VPN, login, then login to her email account via her company's email software. All this should be performed via a WPA2 or stronger wireless encrypted connection. Doing so will protect any data sent / received from network monitoring, provided her mobile device isn't infected with spyware or malware. In this case, the only logs available to the wireless network administrator or attacker hacking in at this level will be those of her wireless device contacting the VPN. Everything from there on will be encrypted inside the VPN tunnel. While this layering technique is the optimum solution, there are others, depending on business' needs and capabilities. If the user's transmissions are properly encrypted, this will greatly decrease the chances that an attacker will devote the time necessary to crack the encryption, and increase the likelihood that the attacker will move to an easier target.

Another variant of the network monitoring attack is to monitor and record wireless emissions from mobile devices, then modify and replay this data at a later time. One similar test was performed on a rfid security system used by an Internet security company located north of Boston, Massachusetts (Newitz, A., 2006, ¶2). Outside the company's offices, a 23-year-old, Jonathan Westhues, planned to use a cheap, homemade USB device to swipe the office key out of the company leader's back pocket. "I just need to bump into him and get my hand within a few inches of him," Westhues says. As the company official walked from the parking lot, Westhues quickly brushed past him. After the official entered the company building, Westhues took a device, and, using a USB cable, connected it to his laptop and downloaded the data from the company official's card for processing. Then, Westhues switched the cloning device from Record mode to Emit mode. He waved the cloner's antenna in front of a black box attached to the wall beside the building's main entrance doors. The single red LED blinked green. The lock clicked. He walked in and found the company official waiting (Newitz, A., 2006, ¶2) (Figure 5). This was a planned hack, designed to test the ease at which the company employees' RFID cards could be compromised, and exactly how it could be done. This attack required no physical contact between the attacker's cloning device and the employee's RFID card. The attacker simply had to be close enough in proximity to 'monitor' the signal being emitted by the RFID card in order to clone it. Then, the attacker switched the mode on his device from Record to Emit, and replayed the data he had wirelessly captured. After replaying this signal in close proximity to the card reader installed at the business' entrance, he was allowed access into the building as if he were the company official with the original RFID card. In this way, users must be aware of their surroundings, as the official should certainly have known that something was amiss if he observed an individual coming that close to his person for no apparent reason. As opposed to

relying upon a single mechanism such as RFID authentication, multiple systems should be used in order to strengthen security. If this was implemented, even if the attacker successfully cloned the RFID card, he/she would have to know a passcode or other information in addition to the RFID card itself. To guard against this specific method of attack, users should use encryption whenever possible when using portable devices which emit wireless signals, and always turn the devices off when not in use. In this case, the user could have also put the card in a grounded, shielded metal case when not in use if extra security was needed. This would lower the already short distance which the attacker would have to move into in order to read the RFID's contents wirelessly.

One of the major ways attackers gain unauthorized access to systems today is almost solely by way of exploiting vulnerabilities in those systems. When an attacker first probes a target, they will seek to find what operating system is running, what updates, if any, are installed, etc. In this way, they can build a profile of the device and its weaknesses. They can then exploit a specific vulnerability based on their profile of the device. No device is completely immune to this type of attack. However, all devices can be made nearly immune by keeping security updates and fixes up to date and running updated antispymware / antimalware and antivirus software. Most newer company VPN connections and equipment now require client devices to at least have a specific level of active protection against spyware and viruses before they are even allowed to connect to the network. Teleworking systems should maintain adequate security compliance. Otherwise, the systems may become the weakest points of failure in security incidents (Hamai, T., Kikuchi, T., Nagata, H., & Rikitake, K., 2001, ¶8). Even with WPA2 or similar encryption mechanisms present on laptops and other mobile devices, if the devices are infected with malware, then they can now be securely controlled by an attacker, and any data on the device can be easily

compromised. Both the mobile as well as the traditional user must be proactive in preventing these infections, as spyware will infect mobile devices regardless of their type or model. For example, malware now exists which, after infecting a mobile phone, will cause it to dial 900 numbers which use up all the user's minutes and generate hefty bills, another blocks certain plugins from running, and still another actively seeks nearby Bluetooth devices and sends infected files to them (Figure 4), as long as the target phone is in range (Naraine, R., 2005, ¶6). Bluetooth is a technology which is aimed at supporting wireless connectivity among cell phones, handsets, PDAs, digital cameras, and laptop computers. It is a frequency hopping system which defines multiple channels for communication (each channel defined by a different frequency hopping sequence) (Bhagwat, L., LaMaire, R., Salonidis, T. & Tassiulas, Leandros, 2001, ¶6). In addition, researchers have recently shown that malicious neighbor discovery attacks can be performed against Bluetooth devices (Buttayan, L., Capkun, S., & Hubaux, J.P., 2001, ¶16). This implies that these attacks could possibly be compatible with a much wider range of devices which employ Bluetooth technology, such as MP3 Players, PDAs, etc. Needless to say, this malware could wreak havoc if turned loose on a personal device, and even more so if turned loose on business devices needed for day to day operations. To combat this threat, users should be familiar with their device's security settings and keep them up to date with the latest firmware and updates. If using a computer, they should ensure that they have the latest updates and have a firewall with updated and active antispysware and antivirus software. In using another mobile device such as a pda, personal organizer, cellphone, etc., users should use the security settings available to lock down the devices as much as possible, turning off features such as bluetooth that are not being used. Leaving options activated that are not being used may introduce an additional avenue of attack for an intruder. Firewalls must be used on computing devices

whenever possible. This will prevent an attacker from successfully entering via an unused port, or relying upon a trojan or similar malware to open a backdoor for him/her to utilize. Normally, without a firewall, the user would not be alerted if a trojan program were placed on their pc, then proceeded to open specific ports for the attacker to connect to. With a firewall installed, it would block these actions, and only allow specific programs access as set by the user or administrator.

A free firewall for home use called ZoneAlarm is available from <http://www.zonelabs.com>.

There are also many other firewalls available. By being vigilant in ensuring their devices are kept patched and up to date with the latest firmware, service packs, antivirus and antispyware products, users can eliminate the majority of vulnerability risks. For more in-depth vulnerability utilities for Windows systems, visit the Gibson Research website at <http://www.grc.com>

Often the most lethal and successful type of attack is the social engineering attack. This method involves attacking the most vulnerable part of any system: the user. Attackers know that security is only as good as its weakest link. Regardless of the encryption or other safety measures deployed to protect the systems and information, the user can override this by giving information to an attacker, thus bypassing the entire security mechanism altogether. Social engineering uses very low cost and low technology means to overcome impediments posed by information security measures (Dealy, B., & Winkler, I. S., 1995, ¶1). These attacks reveal vulnerabilities in security policies and awareness that cannot be detected through other means (Dealy, B. & Winkler, I.S., 1995, ¶24). This is why social engineering is perhaps the most lethal method of attack today. One typical example is that of a senior business official who calls the business' helpdesk and has reportedly forgotten his login information. He requests that his login information be provided immediately or there may be consequences, as he is in a hurry to access some information needed for a high-level meeting. The helpdesk employee, fearing he may

cause problems if he doesn't comply, provides the requested information to the senior official. The phone call is then terminated. This may seem to be a normal, everyday scenario in some businesses, but in fact, it isn't. The senior business official isn't really a senior business official, but rather an attacker who used little pieces of information learned via social engineering to persuade the helpdesk employee to comply with his request. Beginning with seemingly insignificant details, an attacker can build an impressive amount of data on the target. Eventually the attacker works his/her way into higher and higher levels of access, until they have full access to their original target. This attack can best be averted by educating users. Once trained about what to look for, the user can recognize that 'out of the ordinary' phone call as a social engineering attack and forward it to the appropriate department for tracking, as opposed to handing over sensitive information. As user awareness increases, the chances of the user falling victim to this type of attack will proportionately decrease.

In conclusion, defending against all threats to users utilizing mobile computing requires user education to play a central role in these efforts. Without this, all technological countermeasures can be easily rendered useless. Technological best practices no doubt play a vital role in preventing data loss, low productivity and attacks. However, the ultimate solution to counteract the dangers of mobile computing is to employ a balanced, comprehensive solution which combines technological solutions with solid user education. If these concepts are presented to the user clearly, in an understandable manner, then they will see the need for the technological tools and will become self-aware of the best practices required when employing mobile computing, as opposed to simply following a list of rules written in stone with no reasoning required. One would not send a soldier to war without training. Similarly, any competent plan for securing mobile computing must include a thorough training aspect. By empowering the user to be alert,

aware, and thorough, most of the dangers of mobile computing can be averted, and it can become a secure way to communicate while in a mobile environment.

## References

- Bhagwat, Pravin, LaMaire, Richard, Salonidis, Theodoros & Tassioulas, Leandros, (2005). *Distributed Topology Construction of Bluetooth Personal Area Networks*, Proceedings of INFOCOM 2001, Anchorage, April 2001, pp. 1577-1586
- Buttayan, Levente, Capkun, Srđan, & Hubaux, Jean-Pierre (2001). *The Quest for Security in Mobile Ad Hoc Networks*, in the Proceedings of the ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC 2001)
- ConsumerAffairs.Com Inc. (2006). *Ameriprise Loses Customer Data*. Retrieved July 10, 2006 from [http://www.consumeraffairs.com/news04/2006/01/ameriprise\\_data.html](http://www.consumeraffairs.com/news04/2006/01/ameriprise_data.html)
- Davis, L., Hale, J., Manes, G., Meehan, A., & Shenoi, S. (2001). *Packet Sniffing for Automated Chat Room Monitoring and Evidence Preservation*, Proceedings of the 2001 IEEE Workshop on Information Assurance and Security, United States Military Academy, West Point, NY, 5-6 June 2001
- Dealy, Brian, & Winkler, Ira S. (1995). *Information Security Technology? ...Don't Rely on It: A Case Study in Social Engineering*, Proceedings of the 5<sup>th</sup> USENIX UNIX Security Symposium, Salt Lake City, Utah, June 1995
- Hamai, Tatsuaki, Kikuchi, Takahiro, Nagata, Hiroshi, & Rikitake, Kenji (2001). *Security Issues on Home Teleworking over Internet*, IEICE Technical Report IA2001-20, Vol. 101, No. 440, pp. 9-16 (2001)
- Kong, Jiejun, Lu, Songwu, Luo, Haiyun, Zerfos, Petros, & Zhang, Lixia (2001). *Providing a Robust and Ubiquitous Security Support for Mobile Ad-Hoc Networks*, In 9<sup>th</sup> International Conference on Network Protocols (ICNP '01), pp. 251-260, November 2001
- Lu, Songwu, Meng, Xiaoqiao, & Yang, Hao (2002). *Self-Organized Network-Layer Security in Mobile Ad Hoc Networks*, Proceedings of ACM MOBICOM Wireless Security Workshop (WiSe '02), Atlanta, Georgia, USA, September 2002
- Nakao, Koji, Nogawa, Hiroki, Rikitake, Kenji, Shimojo, Sinji, & Tanaka, Toshiaki (2004). *Internet Security Management on Teleworking Environment*, Proceedings of the 6<sup>th</sup> Japan Telework Society Conference, Japan Telework Society, pp. 85-90 (2004)
- Naraine, Ryan (2005). *New Cell Phone Malware Packs Double Punch*. Retrieved July 10, 2006 from <http://www.eweek.com/article2/0,1895,1750109,00.asp>
- Newitz, Annalee (2006). *Wired 14.05: The RFID Hacking Underground*. Retrieved July 11, 2006 from <http://wired.com/wired/archive/14.05/rfid.html>
- Osbakk, Patrik & Ryan, Nick (2005). *The development of a privacy-enhancing infrastructure: Some interesting findings*. Ubicomp Privacy: Current Status and Future Directions

Workshop, UbiComp 2004, Nottingham, UK

Smith, Steven Donald (2006). *Stolen Veteran's Affairs laptop turned in to FBI*. Retrieved July 11, 2006 from <http://www.blackhillsbandit.com/articles/2006/07/10/news/news04.txt>

Williams, Martyn (2000). *EBay, Amazon, Buy.com hit by attacks*. IDG News Service, Retrieved July 10, 2006 from <http://www.networkworld.com/news/2000/0209attack.html>

### Figure Captions

*Figure 1.* JPEG image of a typical internet network path.

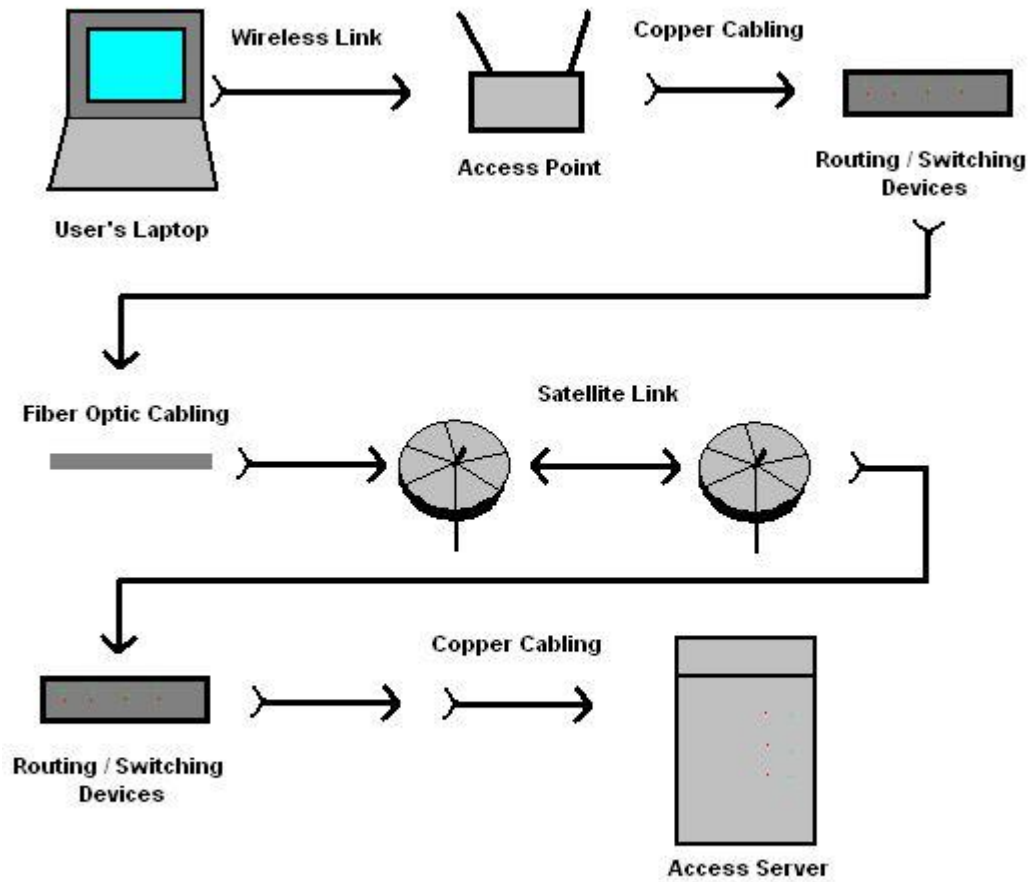
*Figure 2.* JPEG image of a typical DOS attack.

*Figure 3.* JPEG image of network monitoring by an attacker.

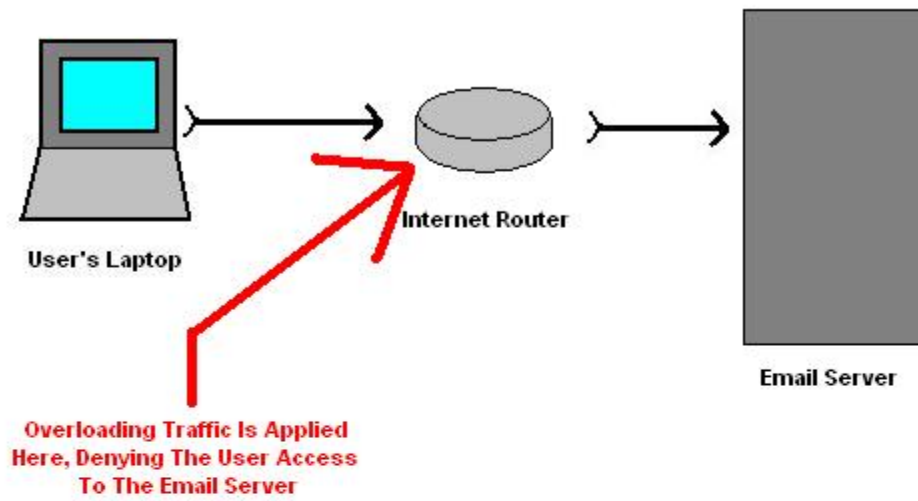
*Figure 4.* JPEG image of infected phone infecting nearby phones.

*Figure 5.* JPEG image of wireless RFID card cloning process.





*Figure 1. JPEG image of a typical internet network path.*



*Figure 2.* JPEG image of a typical DOS attack.

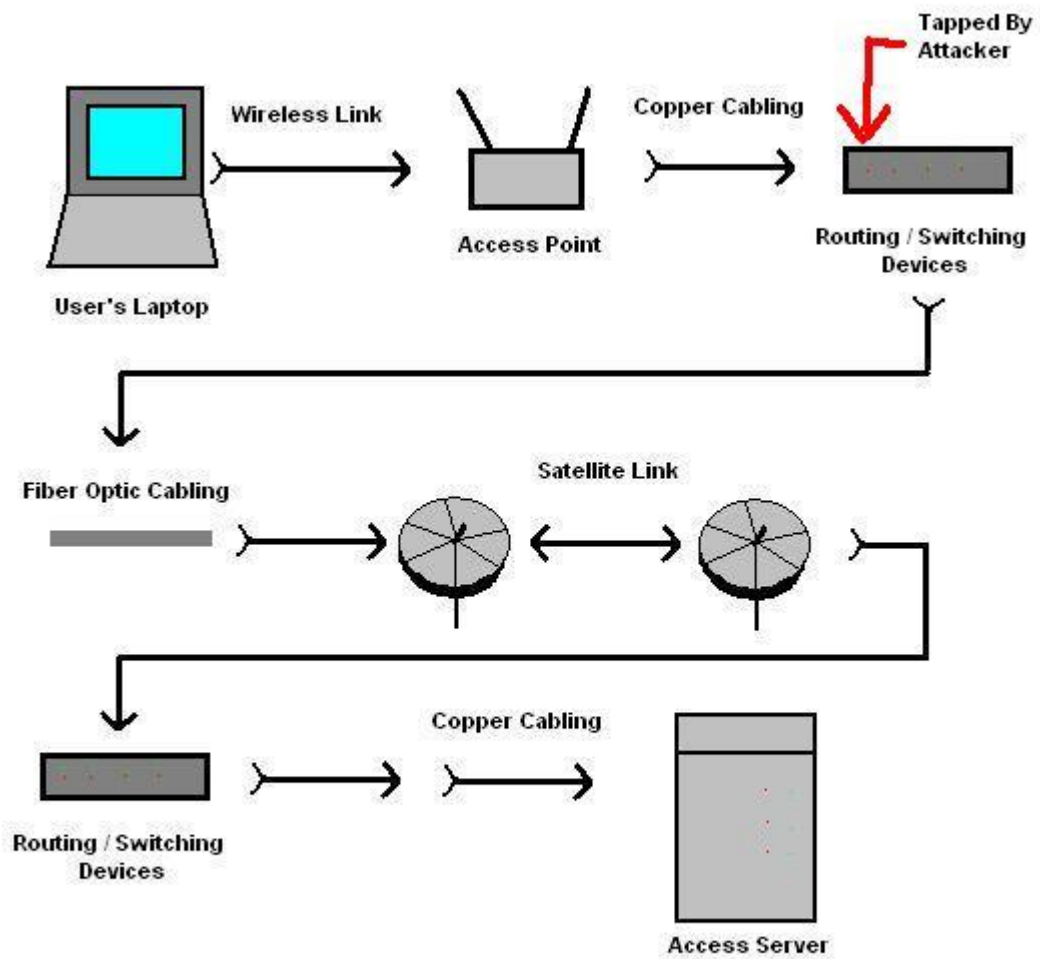
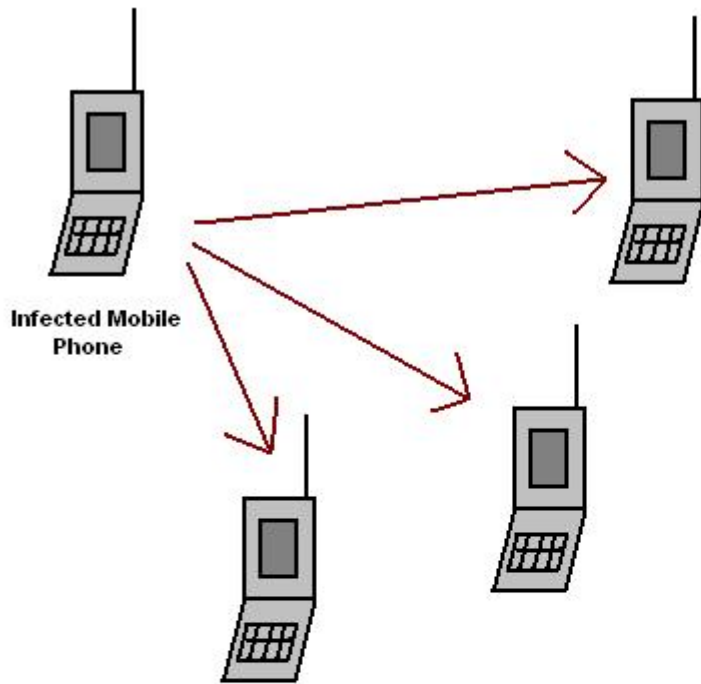


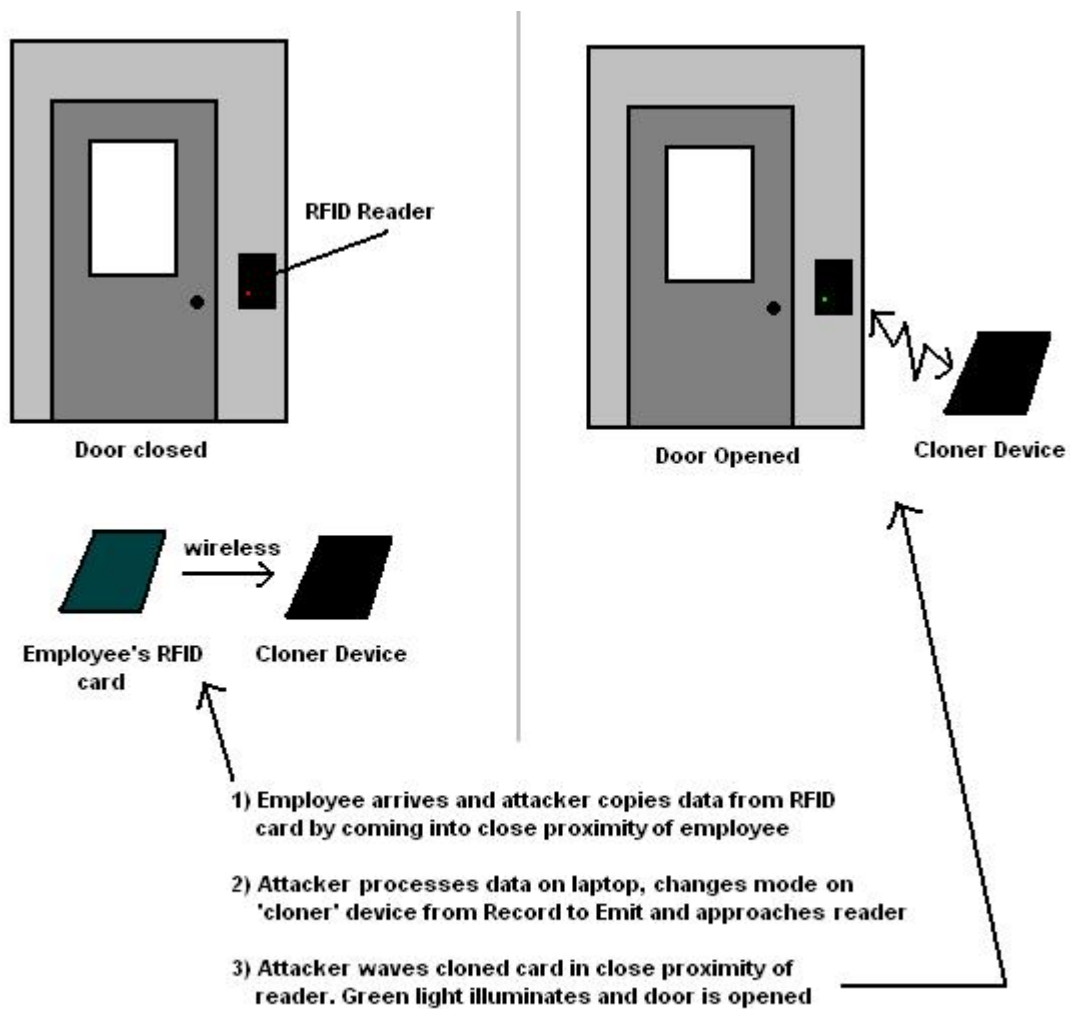
Figure 3. JPEG image of network monitoring by an attacker.



**The malware searches for nearby phones and transmits itself via Bluetooth. This helps to spread the malware to other nearby devices.**

**It spreads via the Bluetooth frequency, and not via the frequency used to call other phones via phone towers**

***Figure 4. JPEG image of infected phone infecting nearby phones.***



**Figure 5. JPEG image of wireless RFID card cloning process**