

Information Security Challenges: Camera Phones

By Michael R. Grimaila and Abhijit S. Kulkarni

mgrimaila@cgsb.tamu.edu, kulkarni-a@bizlab.tamu.edu

Abstract

The explosive surge in camera phone usage presents tremendous opportunities for cell phone manufacturers to boost their sales for mobile devices and take mobile telephony into the next generation (3G). These devices combine a number of features including a telephone, a digital camera, a computing platform, and a wireless transceiver in a small, lightweight package which makes them extremely attractive to consumers. Their ubiquity, ease of use, and ability to be easily concealed presents serious new challenges for information security experts in terms of information compromise and privacy issues. In this article, we present a brief overview of the problems identified with camera phones; discuss factors that one should consider when developing policies, procedures, and technology to mitigate the risk induced by their use; and present a simple model that identifies some key elements one should consider when developing strategies to address their use.

Introduction

Currently, camera phones are a rage around the world, with consumers vying for these gadgets. Manufacturers like Nokia, SonyEricsson, and Samsung are generating record sales from these devices. In Japan, NEC DoCoMo technology "Freedom of Mobile Multimedia Access" (FOMA) has enabled the surge of cellular telephony to the 3G-network topology from the existing 2.5G. According to a report by Visiongain, camera-phone sales are forecast to grow at 50 per cent annually for the next four to five years. Camera phones were only introduced in the market towards the end of 2002, but have seen remarkable sale figures with estimated 55 million devices sold worldwide in 2003, accounting for 14 per cent of total shipments¹. More than a quarter of all mobile phones expected to be sold globally in 2004 will also function as cameras².

Handheld devices (such as mobile phones) present unique security challenges for organizations that want to control, limit, or monitor their usage. Unlike traditional Ethernet devices which reside within a limited geographical network, mobile phones travel freely from one zone to the other without restrictions. Their small size, mobility, storage and processing power, and architectural diversity make it extremely difficult to mitigate risk generated by their use. Further, one must consider the security of end-to-end communications system to properly identify possible source of risk. For example, the Wireless Transport Layer Security (WTLS) protocol which is used for secure transmission of wireless data over mobile networks, suffers from limitations; a hacker can easily capture all the data of the user if he is able to compromise the Wireless Application Protocol (WAP) gateway, because the WTLS encrypted data is decrypted

and translated to Secure Sockets Layer (SSL) that is widely used for secure HyperText Transfer Protocol (HTTP) requests, when it hits the gateway³. Special attention must be given to information interfaces when measuring the aggregate risk of a given communications system. Technology aside, the ethics of the user plays a significant role in determining if an individual will use the camera phone for inappropriate or illegal uses.

The Pros and Cons of Camera Phones

It is only after camera phones have become popular that reports from across the world have started filtering in regarding the benefits and security hazards generated by the use (or misuse) of these gizmos. There have been reported misuses of the technology where people have used camera phones to take pictures in locker rooms or spas to capture nude images that get posted on the Internet. Even more serious threats like corporate espionage, stealing confidential information by capturing visual details, taking pictures of a competitor's new retail setup and selling it at a price in the market, etc. have created corporate security concerns that demand attention. Many high tech organizations have addressed the issue by banning camera phones from their sensitive facilities⁴. Although similar gadgets like spy cameras and laptops with cameras have been a threat to security for decades, it is the ease of use, convenience and popularity of camera phones that make them more susceptible for information security compromise, thus increasing an already-existing risk.

However, camera phones do carry a host of advantages that present barriers to their immediate ban. For example, there have been instances when camera phones resulted in a surgeon getting help during an operation because he was able to send a picture of the patient's X-Ray to other specialists across the world and receive a solution referral⁵. Camera phones have helped capture criminals; for example, in Italy, alert bystanders quietly took a picture of a robber holding up a bank with the help of which police were able to track down the criminal⁶. An indecent stripper who dared to undress himself in front of a woman in a parking lot in Atlanta had his picture snapped by her camera phone that provided the evidence to convict him. The images captured on her camera phone led police to his arrest⁷. In New Jersey, a 15-year-old boy foiled an abduction attempt when he took pictures of a man trying to lure him into a car. In Pittsburgh, several basketball players of St. John's University were cleared from a rape accusation because of some pictures of the incident taken by a camera phone. In Japan, an 18-year-old woman took a photo of a 38-year-old man who was fondling her on a commuter train, and police arrested him at the next stop. In Sweden, a

convenience store owner took a picture of a robber that was used to help identify and arrest the criminal⁷. Many such examples exist that tend to give an extremely favorable opinion about the utility of camera phones. Added to these factors, the tremendous popularity of camera phones, their amazing technological capabilities and their contribution to ever-increasing sales for mobile phone manufacturers pose further barriers to their ban. Moreover, camera phones are the stepping-stone towards migration from 2.5G to 3G networks due to video and Multimedia Messaging Service (MMS) capabilities built in their upgrades. *Banning such phones would mean a reverse transition from technological progress in telecommunications.*

Developing Strategies to Mitigate Camera Phone Risk

As with most other information security topics, the risk arising from the proliferation of camera phones should be tackled on three fronts: People, Policy and Technology. People are always the weakest link as their behavior dramatically affects the overall outcome of any security program. We must remember that information security is a distributed responsibility because everyone can impact the security of the organization, both positively and negatively. For this reason, a structured security education, training, and awareness program is essential to minimize security risk. Certainly, one component of this program should address issues of mobile computing and communication devices. Policies should be written carefully to insure that their content and delivery is neat, concise, and customized to the intended audience. A well-written and implemented set of policies will define your organizational culture and ideally evolve as your organizational infrastructure and operational requirements change. Make sure that you clearly address 'acceptable use' policies for mobile computing and communication devices and implement sanctions for improper use. This policy must be well understood, supported by management and colleagues, and enforceable. On the technology front, a British company called Iceberg Systems is on the verge of launching a product called *Safe Haven*, a combination of hardware, which resides on the network in the form of transmitters, and software that is installed in these phones during their manufacture⁸. This technology blocks the imaging facility in camera phones when the user enters a secure wireless network, thus preventing misuse. The company is currently in talks with manufacturers to have this technology implemented in camera phones. Although there are many benefits to this type of solution, it remains to be seen if camera phone manufacturers will incorporate this technology.

Consider the People-Process-Technology Solution Triangle as shown below in Figure 1. We proposed that ideally the triangle should be balanced, with equal importance given to each of these factors to achieve optimum security. We call this value for the three factors as 'critical value'. If either of these factors is given lesser critical value (i.e. less than 1/3 of the metric score), we conjecture that more security loopholes will exist. We recognize that other factors may also influence the validity of the solution triangle. A more detailed analysis of the model should be conducted to insure completeness⁹. However, we believe that this represents a good initial representation of the approach we have outlined.

What follows is a discussion of each of these component areas and salient factors, which should be considered when developing strategies to mitigate the organizational risk induced by the use of camera phones.

Metrics & Industry Standards of Security

The levels of security awareness and implementations across countries are amazingly different. Countries like the US and UK have strong security

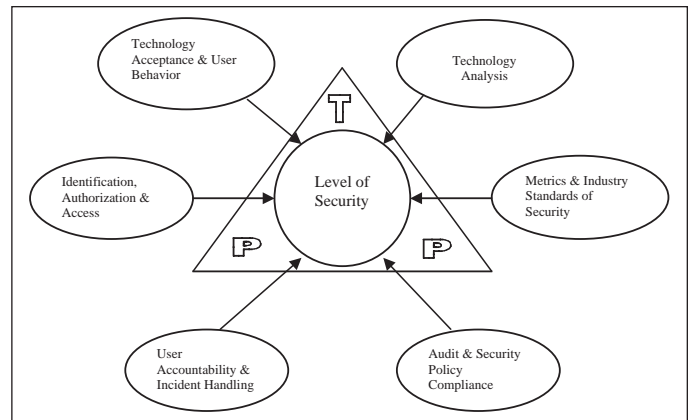


Figure 1: The People-Process-Technology Solution Triangle

policies at all levels, whereas many countries in Africa do not even know what security is. Developing nations like India, which realize the importance of information security, face problems like infrastructure and political issues for implementing a solid security policy for mobile telephony. Also, different countries have different Telecom Regulatory bodies, which implement policies that govern the use of mobile devices. It is difficult to implement a uniform policy across nations. If this were implemental only in a few nations, then the whole purpose of creating a uniform secure technology for prevention of camera phone misuse would be defeated. Moreover, it is extremely difficult for a multinational corporation to implement a Security Policy that covers camera phone usage restrictions across all locations throughout the world, because of disparity in security awareness and legal policies of regulatory bodies.

More research is needed to develop objective information security metrics programs that organizations will adopt. Few organizations take the time to quantify their information security capability over time. Without assessment, how can we possibly know "Where are we now?", "Where are we going?", and "Where were we last year?" Metrics also provide the inputs for decision support tools. It has been demonstrated that lack of decision support tools can lead to subjective assessment and biased resource allocation. A well-designed metrics program will account for new threats created by use of camera phones and other mobile communications devices. However, the rapid technological development in handheld devices and availability of newer features in upcoming phones make quantification and definition of metrics even more difficult. So, it would be a challenging exercise to incorporate a technology like *Safe Haven* in the security policy, allocating metrics that would measure the level of security attained by the use of such a solution.

Identification, Authorization & Access

The issue of identifying users of camera phones and knowing whether they are misusing these devices is quite difficult. Unlike conventional computers and other hardware devices that can be easily identified to their network through their IP and MAC addresses, camera phone identification is easier to manipulate, like their other handheld counterparts. Moreover, camera phones are the most dangerous of the lot—they are efficient in terms of transmission of data with speed, secrecy and ease; as well as the rapid technological development they are subjected to in terms of compatibility with other devices, processing power and size. It should be noted that with all the advanced development in camera phone capability, the network used by the device is still the same—conventionally built for simple mobile hand-helds. Security hazards that could arise due to a camera phone were unrecognized when these mobile networks were built.

The other crucial factor that becomes an impediment for implementing a foolproof authentication process is limitations with respect to identifying and authorizing the 'non-business user' of a camera phone. Would Telcos install *Safe Haven* transmitters across their networks to make this possible? The answer cannot be 'yes' without many conditions. The other problem with building identification & authorization capability within a mobile network is investment. There is no incentive for telecom service providers to invest in more security equipment just because users can misuse camera phones over their networks; moreover, its implementation would involve complex regulatory issues.

User Accountability & Incident Handling

Due to factors like small size, mobility, and lack of established regulations concerning their use, it is a challenge for the incident response teams of security departments to effectively report malicious incidents. The attacker always seems to be ahead of the security expert, thus resulting in many security incidents in information infrastructures, which are not detected or reported. Due to the fact that camera phones are used as personal as well as official data storage and transmission devices, it is very difficult for an organization to audit a user accountability clause in the security policy. The success of implementing such a clause depends to a great extent on the robustness of the technology used and policy procedure defined by the organization.

An example that could be cited is the famous unethical strategy implemented by hotels in the UK to increase their revenue from long-distance calls⁹. These hotels installed mobile phone jamming devices, which disabled the mobile phones customers carried on the hotel premises. Customers started using the hotel telephones for placing calls, thinking that there was a signal problem. Since camera phones have affected digital camera sales a great deal, it would be prudent to anticipate similar strategies implemented to thwart camera phone sales; unethical business practices could result in a technology like *Safe Haven* being used to block camera phones in locations of photographic interest.

Audit & Security Policy Compliance

Many countries in the world have camera phones sold through grey markets; it is very difficult to stem the demand for camera phones even though the government issues a legal ban on such phones. Countries like Saudi Arabia have banned camera phones due to reasons that defy the strict laws in the country³; this may result in the increase of illegal sales of such phones in countries that implement such regulations.

There are many security issues related to handheld wireless devices, which don't yet have solid solution. Hacking is easier in mobile devices than stationary computers within a network due to their mobility, as well as their limited battery storage that prevents implementation of a complex, secure operating system. Visual data transferred by camera phones thus can be easily hacked into; it thus puts forth the same amount of risk that a transfer of textual data does. As a matter of fact, it is much more difficult to trace misuse of camera phones because of the dangerous facility of imaging that a camera phone offers—Al Qaeda members used steganography to transmit digital images of the World Trade Center before the attacks¹¹—camera phones make such acts much easier. The pressing question that arises about security policy and compliance is: How does an organization get its employees to comply with a policy? A more difficult question is: How does the legal framework prevent users from misusing these devices? Currently, the only way to deal with security defiance using camera phones would be through a legal suit; however, by the time the judgment is passed, the damage would have already been done—through the Internet.

Auditing is a crucial process that is needed to verify policy compliance; but, it is interesting to note the methodology which organizations adopt for such a process. Usually, the process has two stages—an internal audit is carried out first, and then an external agency is invited for the main audit. It is not surprising that in many organizations, the internal audit is a 'dress rehearsal' for the external audit; many employees are unaware of most of the ideal processes that are defined in the policy which need to be followed. The internal auditors go around 'educating' employees about the procedure and the way they need to present their answers to the external audit team—in effect, the results analyzed by the external auditors is based on results derived not from awareness and compliance but from last minute preparation and manipulation. This issue poses another impediment to compliance with a policy that accommodates restrictions on camera phone usage in organizations.

Technology Acceptance & User Behavior

There is a crucial factor that stands against the extreme clause of a security policy of issuing a ban on a certain device that is a threat to information CIA (Confidentiality, Integrity and Availability) model¹⁴, which is technology acceptance. Camera phones stand among those devices that have had tremendous success in markets because of their large acceptance rates by users. Their simplicity and convenience of usage along with technology capabilities have lead to a high extrinsic and intrinsic motivation levels with respect to buyer behavior¹². It is interesting to note that the camera phone stands among the very few devices, which is well accepted across user demographics, occupation, status, utility, and availability.

Added to this factor is the difficulty in segregating a camera phone as a personal or an official device, since it is well suited for both categories. However, a camera phone used by an employee of an organization is more likely to be perceived as a personal device than an official one, as compared to other IT devices like laptops and computers. An interesting observation that supports this conclusion is a security check done on employees as they leave an organizations' facility. Employees are checked for floppy disks, CD's, authority passes for their laptop computers; but there is usually no check done whatsoever on their mobile phones. The perception that a security guard has about a handheld device creates a loophole in the physical aspect of security.

Technology Analysis

Safe Haven is a solution that uses a combination of transmitters which are installed in a secure network and software that is loaded on camera phones⁸. The product is still in testing phase, and it remains to be seen whether it is compatible with all types of camera phones. If there are compatibility issues, the amount of changes that need to be made in the design of these phones needs to be evaluated, that would affect cost as well as the interests of manufacturers.

The solution blocks image capture when the camera phone is inside the secure network where the *Safe Haven* transmitters are installed. Once the user goes beyond the boundary of the network, the imaging facility is restored. If the technology disables imaging immediately after a *Safe Haven* enabled camera phone enters the secure network, a question that arises is, what mechanism can be incorporated which would prevent a user carrying a non-*Safe Haven* camera phone into the secure area? Thus, a malicious user carrying such a phone can transmit an image captured by his camera phone after he goes outside the limits of *Safe Haven* protection. All across various networks, it remains to be seen whether this technology would work. Because of roaming facilities available with mobile phones, it is worth noting whether this has a consistent result across networks.

The *Safe Haven* technology is relatively new and there is little public information available on its system architecture, capabilities, or limitations. One can envision a number of different technical approaches to implement such a system— one, in which the transmitter would continuously transmit inhibiting signals that disable imaging in the camera phone the moment it enters the secure zone; and the other, in which a camera phone is detected first upon its entry in the secure zone, and the phone is then requested to disable its imaging capability. There are advantages as well as disadvantages with these options. In the first case, the solution is: simple and cost-effective, since the communication between the transmitter and the phone is simplex; does not offer authentication; does not accommodate permission levels for security; consumes more transmitter power; and may pose possible health hazards to users because of continuous radiation. The second option is: more complex, since it involves handshaking between the transmitter and the phone, which is duplex mode of communication; offers authentication and authorization levels, which increase customization options; consumes less transmitter power; and can be exploited to gather confidential user data that may violate privacy rights, since user recognition levels are established in the system and users store official as well as personal information on their camera phones.

Thus, an important issue about successful implementation of such a technology is scalability and customization. A solution could start off being a low-cost, simple solution, but get increasingly complex as attackers find means of compromising the latest security technology, as they always have. It would be a challenge to incorporate security permission levels in the *Safe Haven* technology that would allow certain, influential users of camera phones within an organization take pictures in a secure zone during an emergency or an urgent need. Moreover, it is worth researching the probability of an attacker compromising a *Safe Haven* secure network by cracking the software code inside his camera phone. It would also be crucial to implement a proper authorization process, which could be done in two ways—recognize and authenticate a user when he enters a *Safe Haven* network, or conduct an authorization check only if a user tries to use the camera inside his phone in the secure network.

It would be interesting to understand more about certain hidden issues like battery consumption of a camera phone due to switching transitions of its imaging capabilities. A camera phone user, within a *Safe Haven* network, has his imaging facility cut off once he is inside the network; as soon as he steps out of the zone, the facility is enabled again. Would the continuous transition between the unprotected zone and the *Safe Haven* network affect battery consumption and its life? Also, since the *Safe Haven* transmitters would be transmitting radio waves, what kind of RF protection equipment would be required to prevent health hazards or interference with adjacent equipment? We do not know the answers yet.

With technology making seemingly impossible things possible, it wouldn't be outrageous to claim a possibility of phony devices using technologies similar to *Safe Haven* created for unethical purposes; under the guise of security, such devices could act as information capture receptors and collect personal information from users of *Safe Haven* enabled camera phones, leading to privacy violation. Further, criminals could carry a *Safe Haven* transmitter to prevent camera phones from being able to capture their images during the commission of a crime.

Security vs. Piracy: Conflict

There have been solutions proposed to address privacy issues in handheld devices, such as the Logical Borders Mechanism and the Anonymous User Identity (UID)¹³. These solutions, if implemented in camera phones,


would result in users taking advantage of the privacy provided. There are two ways in which malicious users can exploit the situation.

Logical Borders Mechanism—In this technique, the advertising of the camera phone on the network would be allowed up to the limit specified by the user, thus giving the user liberty to decide on the definition of the logical border. Misuse of camera phones becomes very easy, because visual information can be trapped in a certain mobile zone and the user's identity (the camera phone used) would be captured in that zone alone. Once the user leaves that zone, the capture information is lost. Thus, it would be extremely difficult for security teams to trace these snoopers capturing confidential information through camera phones from a network. Because a visual image captures more information than textual data, is easy to interpret and is capable of displaying more information on a small screen, the damage inflicted by a camera phone is much more than a simple mobile phone.

Anonymous User Identity—In this technique, the real identity of the user is kept confidential; hackers using camera phones would be able to easily capture visual information from a network without being identified.

Thus, addressing privacy issues of users pose threats to security of confidential data, since it gives leeway to hackers to use camera phones more easily to steal information. The serious question is—how do policy makers draw a line between security and privacy protection? Technology continues to stretch the limits of expectation of privacy.

Conclusion

Although the capabilities of small cameras and their ability to inflict security hazards are not new, camera phones have, with their unique feature of an integrated package with imaging features and ease of use, exploded this risk. Considering all the above issues about camera phones, it should be an endeavor to present a balanced solution to mitigate risk based on policy, technology and feasibility. Initiatives undertaken by enterprising companies like Iceberg Systems do offer one dimension of a solution, but do not encompass issues like piracy. It remains to be seen as to how quickly security experts are able to expand existing security policies addressing handheld devices to accommodate camera phones. However, it makes little sense to develop policies if they are not enforced. It is obvious that taking critical steps in combating camera phone misuse, such as banning these devices or cutting down on its features and capabilities would result in objections from users and an increase in illegal sales of these devices. A more thought-out solution is advisable which considers the rights and privacy of individuals, the regulations and laws of different localities, use of new technologies, and the enforcement of organizational policy. 

Michael Russell Grimaila, B.S., M.S., Ph.D. is a Research Scientist and Visiting Assistant Professor of Management of Information Systems (MIS) and a member of the Center for Information Assurance and Security at Texas A&M University. His research interests include critical infrastructure protection, enterprise risk management, and the economics of information security. He is an active member of the IEEE, ACM, AIS, CSI, ISSA, and SANS Institute. Contact him at mgrimaila@cgsb.tamu.edu.

Abhijit S. Kulkarni, B.S., M.B.A., is a Master's candidate in Information Systems with a specialization in Data Communications and Security in the Mays Business School at Texas A&M University. He has had more than 3 years experience in consulting for IT and Telecom solutions. His research interests lie in Disaster

Recovery, Security Policy Management and Wireless Security. Contact him at kulkarni-a@bizlab.tamu.edu.

¹ "Camera phone sale increase could boost 3G phone sales," 3G Newsroom, available at http://www.3gnewsroom.com/3g_news/feb_04/news_4162.shtml, February 7, 2004.

² "Global sales of camera phones shoot up," ZDNet UK News, available at <http://news.zdnet.co.uk/hardware/mobile/0,39020360,39148306,00.htm>, March 12, 2004.

³ "Saudi Arabia bans camera phones," Annova, available at http://www.ananova.com/news/story/sm_681800.html, March 1, 2004.

⁴ "Camera Phone makers ban own products," CNet Asia, available at <http://news.zdnet.co.uk/hardware/mobile/0,39020360,2137192,00.htm>, July 8, 2003.

⁵ "Picture phones save doctors time," BBC news, available at http://news.bbc.co.uk/2/hi/uk_news/wales/2995518.stm, June 17, 2003.

⁶ "Nokia picture phone IDs lurking villains," The Register, available at <http://www.theregister.co.uk/content/59/29346.html>, February 17, 2003.

⁷ "Smile! I'm calling police: Camera phones help nab crooks," CNN, available at <http://www.cnn.com/2004/LAW/03/19/crime.fighting.camphones.ap/index.html>, March 19, 2004.

⁸ "Safe Haven", Iceberg Systems, available at <http://www.icebergsystems.co.uk/>, January 14, 2004.

⁹ "Information Security Metrics, an audit-based approach" by Jennifer L. Bayuk, NIST Security Metrics Workshop, available at <http://csrc.nist.gov/ispab/june13-15/Bayuk.pdf>, June 13 and 14, 2000.

¹⁰ "Scottish Hoteliers jam mobiles," CNET Asia, available at <http://news.zdnet.co.uk/communications/wireless/0,39020348,39116039,00.htm>, September 1, 2003.

¹¹ "Al Qaeda members used Steganography," Eight Links, available at <http://www.eightlinks.com/archives/000245.html>, May 10, 2003.

¹² "A Test of the Technology Acceptance Model—The Case of Cellular Phone Adoption," by H. S. Kwon and L. Chidambaram, Proceedings of the 33rd Hawaii International Conference on System, available at <http://csdl.computer.org/comp/proceedings/hicss/2000/0493/01/04931023.pdf>, January 4-7, 2000.

¹³ "Security and privacy issues of handheld and wearable wireless devices" by R. Di Pietro and L.V. Mancini, Communications of the ACM, September 2003, Vol. 46, No. 7.

¹⁴ "Principles of Information Security" by M. Whitman and H. Mattord, ISBN #0-619-06318-1, Thompson Course Technology, 2003.

