A DISCUSSION ON THE SECURITY AND PRIVACY CONCERNS IN A WIRELESS HANDHELD ENVIRONMENT

R Gururajan & D Roberts
Department of Information Systems
The University of Southern Queensland
Toowoomba, QLD, Australia
Correspondence: gururaja@usq.edu.au

ABSTRACT

The wireless handheld devices are a new communications channel for access to data and people at a global level. These devices are, perhaps, the first electronic medium to allow every user to reach others despite geographic, social, and political barriers, due to their mobility and flexibility. Recognizing this potential, government agencies and other business entities started delivering information to users through these devices. As these devices are Internet ready, the usage of these devices is growing. This Internet capability combined with office applications has made these devices an essential component of future information exchange.

However, it remains to be seen as to whether the anticipated benefits of these devices will be delivered as governments are concerned about the security and privacy aspects of the communication channels facilitated by these handheld devices. In a wireless environment, devices needed to be 'polled' in order to send and receive messages and hence the physical location of these devices should be known to service providers. When a technology called 'location identification technology' is engaged, it is possible to remotely locate users of these devices with about 10 meter precision. Further, with the implementation of GPS systems on these devices, it is possible to monitor users from a distant location. Therefore, users who are not conversant with emerging technologies, while using these wireless handheld devices, may inadvertently expose themselves to physical threats, instead of threats approaching them. This discussion paper investigates these security threats arising from the use of wireless handheld devices, with specific attention paid to privacy issues. The investigation covers recent changes to privacy policies and the difficulty in the implementation of these policies in a wireless environment.

KEYWORDS: Wireless, Security

INTRODUCTION

Succeeding the advent of the Internet Technology, wireless has dominated the Information Technology for the past two years. Worldwide, cellular and personal communication service providers are upgrading their networks to meet the demand experienced from consumers. Third Generation (3G) services are being offered in many countries and customers are able to combine voice, data and graphics into one communication channel using devices facilitating 3G services. While the wireless technology is growing at a rapid speed, individual security and privacy issues associated with wireless technology are also assuming prominence due to the

difficulties encountered in managing information related to individuals. For example, in Australia, some pharmaceutical companies accessed prescription information through pharmacy service providers without prior consent from patients, violating privacy regulations. Similarly, a city council in Australia 'sold' the details of residents either building or upgrading their houses to a private security firm, that enabled the firm to market security products. This has violated some of the regulations associated with marketing in Australia. When wireless handheld devices become prominent, the issues of privacy invasion will also become prominent, as controlling data collection and distribution becomes difficult using these devices (Fitzgerald, 2003).

Privacy issues have received considerable attention all over the world over the past several months. The range of issues vary from the United States congressional inquiry into the usage of red-light cameras at traffic signals through to the use of face recognition software at major airports concerned with potential criminal activity. Recent terrorist attacks have definitely toned down the public views on privacy, but there is little indication that these events have changed public attitudes about privacy. With the facilities available in wireless technology domain to locate users, privacy of individuals is threatened. This would increase the level of privacy intrusion by employers (Atwal, 2001). Because of the remarkable level of intrusion that has become possible with wireless devices and remote monitoring devices using wireless technology, legitimate organizational interests in employee activities is questioned by many employees .

The number of commercial applications that have been developed in the past five years to locate and track inanimate objects such as vehicles have increased (Andrews, 2001; Schiller, 2000). In countries like Australia, taxis and buses are fitted with wireless positioning devices for monitoring purposes as well as for security and safety reasons. While the objectives of these developments are improved efficiency in production, logistics and the security of assets, these software applications do not address various issues associated with privacy regulations. For instance, some software development projects that have been contracted to educational institutions by the Australian Government track endangered species of animals, in order to identify their location and movement, to study their habits and to protect them, by attaching an electronic tag to the animal. When the animals cross a predefined location, the electronic tag is read and its new location is established. While these projects are currently research oriented, annexing such tags to human beings may lead to controversy. Some Departments of Justice in Australia conceived the idea of attaching an 'electronic bracelet' to prisoners who are kept in minimum security level to enable them staying in society in order to reduce costs involved in maintaining them. However, the idea was abandoned at conceptual stages because of the adverse impact it can have due to privacy laws in Australia.

Using wireless technology, it is possible to identify individuals based on specific parameters such as financial transactions. For instance, cases have been reported in the literature of how some law enforcement authorities have been able to identify the locations of individuals based on visa card transactions[1] as stated by Budhwani (2000).

[1] An American-Thai Buddhist monk was arrested in Sydney while using his Visa Card. His arrest was initiated by the IRS of the United States and completed in Australia.

While some of the cases reported involve physical cards, current attempts to mimic such cards on a mobile telephone terminal may result in undesired outcomes.

As long as these location identification technologies identify only objects and not humans, they are not controversial. However, with wireless applications, it is possible to identify precisely individuals who use mobile devices such as mobile telephones and PDAs. When this identification is activated, the privacy of individuals is compromised leading to concern (Warrington et al., 2000). Further, this breach of privacy may lead to potential security problems. These issues are discussed in this paper.

TERMINOLOGY

The location of an entity is usually described in terms of certain reference points (Schiller, 2000), the location being ascertained with varying degrees of precision and varying degrees of timeliness. Tracking refers to the plotting of a trail or a sequence of locations within a space over a period of time (Dornan, 2001). The space is generally physical space or geographical space. A real-time trace refers to the identification of an object or person at any particular point in time, with a degree of precision (Smith & Andrews, 2001).

The above terms show that, by tracking a person at varying time intervals, it is possible to observe his/her behaviour. When multiple persons are tracked, then it is possible to observe group behaviour. In certain circumstances, using location identification technologies, it is possible to analyse employee behaviour such as where a particular employee went to conduct business activities, how much time was spent on each activity etc. These details may be used for employee performance without realization that there could be external forces having an impact on certain business activities and hence resulting in delays. While, analyses are not properly tested by organisations, logical decisions are not made and this may adverse employees adversely. Therefore, location identification technologies provide the power to make decisions about subjects and hence to exercise a certain amount of control over these subjects.

INFLUENCES OF LOCATION IDENTIFICATION TECHNOLOGIES

Location identification technologies were initially used in homes and community areas. Examples are meter boxes for electricity readings and post boxes. Telephone books also come under this category. However, in recent years, location identification devices have been used to capture the movements of individuals to generate transactional data (Hulme, 2000). For instance, for security purposes, the movements of the police are identified using a form of location identifier such as a wireless phone. Credit cards and debit cards also identify the location of financial transactions.

However, with the advent of emerging technologies such as intelligent cards, identification techniques have improved. These cards provide identification based on the characteristics entered in a ‘chip’ and, in conjunction with a location, may allow entry to a secure environment by the person who possesses the card. Security features are usually incorporated into these smart cards to avoid any unauthorised use (Deise

et al., 2000). These security features may include biometrics such as finger prints and face recognition.

Telecommunication advancement also assisted in locating certain characteristics of identification such as telephone numbers. For instance, when a caller telephones, it is possible to identify that caller by the number displayed on the telephone panel (provided one is available) and then to choose whether to respond to the call. The recently introduced radio frequency based systems can identify individuals based on the devices they are carrying (Anonymous, 2000). For instance the Global Positioning System (GPS) identifies positional reference points using satellite signals. Closed Circuit TV (CCTV) monitors the movement of individuals in certain environments (McConnel, 2000). But not many of the above systems intrude into the privacy and security of individuals.

Recent mobile devices such as portable computers and mobile telephones can assist in the identification of individuals and this may become an intrusion into their privacy because such identification can lead to personal data stored on these devices. Once these devices are located, using infrared technologies, it is possible to transfer information to another device without the knowledge of the user of these devices. For instance, location of buses, taxis and the number of people in the bus or taxi etc can be transmitted to a central location in order to optimise transport logistics. In specific instances, this data could be used in order to identify a specific entity and this is a potential threat to security or privacy.

RISKS IN A WIRELESS DOMAIN

Location identification technologies, using wireless technology, have raised four major areas of concern (McCullagh et al., 1998). They are (i) Individual danger; (ii) Social dangers; (iii) Organisation danger; and (iv) Privacy invasion. While there are other dangers involved, these four appear to be impacting on the security and privacy of individuals on a large scale. A discussion on these four aspects is provided below.

Individual dangers

Prior studies have indicated that it is possible to locate an individual using a mobile device through a mobile telephone number or the IP address in a wireless device (Hayes, 2001). When such identification is successful, approaching the user of the wireless device becomes possible and this may lead to potential security problems. Even if the individual cannot be identified, it is possible to steal data from a mobile device, such as a mobile computer, leading to potential data security risks. Further, people entering a wireless network (also known as WAP zone) can be targeted with notices or messages containing viruses, effectively paralysing the various functions of their computer. Even if viruses cannot be passed on, it is possible to send unwanted information and simply drain the battery of the mobile device. When individuals communicate using mobile devices, it is also possible to steal data in a WAP zone as the security protocols are not strong on these devices (Dornan, 2001).

By using location identification technologies, it is possible to discover an individual's behaviour patterns and governments can use this in order to generate suspicion. Organisations can use this sort of data to classify individuals in order to capitalise on consumer behaviour. Further, once identified, individuals can be blackmailed. In

addition, these location identification technologies can be used as 'evidence' in criminal cases.

Social dangers

Social dangers assume greater significance because when identified, individuals involved in the act are subject to being exposed and assumed to have performed the act. The accusation may be right or wrong, but the very fact that the person has been associated with the crime, influences public perception and leads to social action against that individual. For instance, the identity of a person associated with a murder case in New Zealand in June 2001 was published on a local Internet site, leading to accusations against that person by the public. However, this individual was only in the vicinity of the murder and in no way associated with it, nonetheless suffered irreparable damage. While this example is pertinent to the Internet, in this situation is not far away with wireless applications.

Another situation where wireless technology can have adverse impact on specific society related problems is the usage of RF tags. RF tags are becoming popular to track and monitor inventories currently. The concept of Smart Trolleys is trialled at the moment, where consumers can fill up a trolley with goods, identified by RF Tags. When these goods pass through a reader (instead of a check out counter), the RF tags are read. Then, this information is communicated to the store database and the amount to be paid is automatically computed. One social danger is the possibility of reduction in employment. As these tags can store only limited information, it is difficult to build security features onto these tags and privacy information of members of society can be compromised.

Organisational danger

Organisations may also encounter problems associated with wireless data. For instance, if the use of mobile devices lacks proper authentication procedures, then it is possible for an intruder to get access to these devices and make use of the service facilities (Deise et al., 2000). Such abuses may put organisational data at risk. Further, the intruder may send the wrong data to organisations using mobile communication technologies, thereby negatively influencing their decision making processes. Such an act would create bad publicity for an organisation and could possibly end up with a legal battle. Therefore organisations have to protect themselves against such risks in a wireless environment.

Privacy invasion

In a wireless environment, location identification devices also generate concerns with regard to privacy. According to Green (2000), reports indicate that consumers are worried about their privacy and the potential intrusion when mobile devices are used. With certain financial transactions, consumers like to be anonymous, but this anonymity can be revealed in a mobile commerce environment because of location identification devices. In areas such as health, revealing patient details may violate privacy regulations in certain countries. While some governments are in the process of modifying their privacy laws, more work is needed to tighten the various loopholes caused by modern technologies.

POTENTIAL SECURITY THREATS ARISING FROM WIRELESS TECHNOLOGY

Security threats in a wireless domain can range from passively eavesdropping into others' message to actively stealing user's data (Loney, 2000). In a radio frequency operated mobile commerce, with minimum difficulty it is possible to listen to one's conversation. This has an impact for users because they are concerned about their data and voice messages from unauthorised access. At the other end of the problem is the inherent security risk involved in transferring information over the networks. This problem consists of two components: identification integrity, and message integrity. Identification integrity refers to the signature elements found in the messages in order to establish where the message is originating. Message integrity refers to details to establish that the message is received as sent and no third party has attempted to open, modify or alter the contents. According to Zhang (2000), these two items appear to cause a lot of concern to both sender and receiver in a wireless environment. While the sender risks theft or misuse of personal information such as account and bank details, the receiver risks repudiation of the transaction.

In addition to the above two, additional security concerns in a wireless domain arise due to the new development in technology itself (Zhang & Lee, 2000). The mobile technology is envisaged in such a way that the services offered will eventually warrant payment for the type of services offered. This is already emerging in the domain of mobile telephones. For instance, when mobile telephone users access other network carriers, a special charge is levied on the users. Therefore, it is safe to assume that there will not be any "free services" in the future. The technology is developing in such a way that the payment for such services will be through some form of "smart cards". Current development indicates that these smart cards will be in the form of an 'electronic card' stored in mobile devices. The details stored in the smart cards need to be transmitted via wireless networks for validation and verification in order to determine service levels. If these networks are not fully secure, there are possibilities for security breaches to occur.

One major security breach that can happen in wireless environment is when the user details are transmitted from one mobile network to another (Hulme, 2000). When this transformation occurs, any encrypted data needs to be decrypted for transparency. In a wireless environment, when mobile devices make requests to web pages of a network server, a four-stage process is followed. First, the requests arise from the originating Wireless Transport Security Layer (WTSL) protocol. Second, the requests are translated at the originating Wireless Application Protocol (WAP) gateway. Third, they are sent to the standard Session Security Layer (SSL) protocol of the destination network. Fourth, the translated information reaches the Hyper Text Transfer Protocol (HTTP) modules in the new network in order for the requests to be processed. In the process of translating one protocol to another, the data is decrypted and then re-encrypted. This process is commonly known as the "WAP Gap". If an attacker is able to have access to the wireless network at this point, then simply capturing the data when it is decrypted can compromise the security of the session.

Data in the wireless environment is secured using encryption technology. According to Ghosh (2001), it has already been proven that the technology is vulnerable to attacks. Hackers have broken some of the existing algorithms for encryption. So,

there is nothing like complete security. Further, there is no international regulatory framework available to enforce certain security related standards (Fitzgerald, 2003). For example, in the current climate, no individual organisation or government can guarantee security to consumers. When the security breach appears in an international transaction, no one country will be able to assume responsibility to prosecute the vandals. While these problems have been recognised and solutions are being proposed, organisations tend to lose consumer confidence. This could potentially impact an organisation in an adverse way. One example[2] that comes to mind is Verisign.

Trust is central to any commercial transaction and more so using wireless networks (Fink, 2000). Trust is normally generated through relationships between transacting parties, familiarity with procedures, or redress mechanisms. In the case of wireless technology, the need for creating the trust in the consumer assumes extreme importance because of its virtual nature. It hinges on assuring consumers and businesses that their use of network services is secure and reliable, that their transactions are safe, that they will be able to verify important information about transactions and transacting parties such as origin, receipt and integrity of information, and identification of parties dealt with. Therefore the challenge is not to make wireless technologies fool proof but to make the system reliable enough so that the value greatly exceeds the risk.

Any new development in consumer' minds create both curiosity as well as reluctance. The informality and lack of overall control creates the perception that the Internet is inherently insecure (Schiller, 2000). This inherent perception can trigger business risks and technological risks using mobile devices on the Internet (Shroeder, 1999). Business risks involve products and services, inadequate legal provisions, reliability of trading partners, behaviour of staff and demise of Internet service provider. Technological risks involving hacker attacks, computer viruses, data interception and misrepresentation could all arise. To achieve satisfactory levels of trust, organisations have to think about managing both business and technological risks. Currently Mobile Commerce relies mostly on knowledge-based trust that is useful for Business-to-Business commerce (Fink, 2000). However, there is a big surge in the need for identification-based trust to satisfy consumer concerns about their transaction details. In wireless environment, any compromise to identity based threat could lead to 'identity theft'. Identity theft is an emerging problem in the IT industry, where identities of individuals are stolen for various reasons, resulting in both financial losses and unauthorised entry into restricted locations. In addition, current architectures for mobile communications do not provide full security measures in terms of transaction integrity. Some of the models envisaged for mobile commerce are based on a smart cards oriented approach and hence the issue of financial transaction security needs greater examination in mobile commerce.

[2] The site of Verisign, a company that certifies trust worthiness of web sites, was hijacked a few years ago. Verisign noted this incidence after considerable delay. When this information was made public, Verisign lost its credibility.

POTENTIAL PRIVACY THREATS ARISING FROM WIRELESS TECHNOLOGY

When mobile devices are connected to the Internet, privacy threat increases as the general expectation of anonymity is not guaranteed by the combination of mobile devices and the Internet (Freeman, 2003). In a physical world, if an individual has not actively disclosed information about him/herself, then he/she believes that no one knows who he/she is or what he/she is doing. But using the mobile devices for a transaction using the Internet or any other online medium generates an elaborate trail of data detailing every activity of a transaction (Freeman, 2003). This data trail may be captured, stored and analysed using software technologies such as 'agent' technologies to understand the pattern of individual habits (Morger et al., 1997). Further, an employer may be able to monitor an employee's behaviour. Transactional data, click stream data, or "mouse-droppings," can provide a "profile" of an individual's online life. This may intrude into the privacy of individuals. Using mobile devices, individuals need to disclose their personal details to establish communication.

Technologies such as "cookies" enable Web sites to surreptitiously collect information about online activities and store it for future use. While these technologies were initially designed for the benign purpose of enabling Web sites to recognize a repeat visitor and respond accordingly, (initially developed by Netscape), cookies were quickly adopted for the purpose of customizing content and advertising (adopted by Microsoft). The surreptitious activities gained the attention of policy makers in order to protect consumers and to safeguard their privacy. There are examples of companies using and disclosing personal information for purposes well beyond what the individual intended (Clarke, 2003). For example, recent news stories[3] have alerted the public on misuses of personal health information by the private sector, particularly when it is digitized, stored and manipulated. Public outrage and the concern expressed by politicians on the issue of health privacy, appear to have halted the growth of this process. It appears that the sale and disclosure of personal health information is a big business, which is evidenced by a recent advertisement by an American company which stated that it had 7.6 million names of people suffering from allergies, 945,000 suffering from bladder-control problems, and 558,000 suffering from yeast infections.

These incidents prompt for strong privacy legislations to safeguard sensitive information such as health and financial records. While legislations are yet to become stronger, consumers have protested against services that appear to infringe on their privacy. For example, public uproar forced Lexis-Nexis to withdraw a service known as P-Trak, which granted easy online access to a database of millions of individuals' Social Security numbers in America; Yahoo faced a public outcry over its People Search service, which jointly run with a marketing list vendor, would have allowed Net searchers to put an instant finger on 175 million people, all culled from commercial mailing lists[4]; American Online ("AOL") announced plans to disclose its subscribers' telephone numbers to business partners for telemarketing and

[3] The Washington Post reported that CVS drug stores and Giant Food were disclosing patient prescription records to a direct mail and pharmaceutical company.
[4] After hearing the complaints, Yahoo deleted 85 million records containing unlisted home addresses.

encountered loud objections from subscribers[5]; the report in Washington Post about the unsuccessful attempt by American States to sell state drivers' license photos to Image data for a profit. It is encouraging to note that the general public is serious about their privacy and this seriousness has forced governments and big organisations to change their attitude while dealing with consumer details.

REMEDIAL ACTIONS TO ALLEVIATE USERS FROM SECURITY AND PRIVACY THREATS

Emerging technologies will assist in the surveillance capacity to collect, aggregate, analyse and distribute personal information coupled as these processes help the current business practices to target customers who indulge in commercial transactions. However, these technologies have left individual privacy unprotected (Freeman, 2003). While recent surveys and public pressure have raised the privacy consciousness, particularly those operating with emerging technologies, individuals' information is frequently used and disclosed for purposes well beyond what the individual provided it for. Therefore, individuals need to take necessary action to protect their information.

As consumers, it is recommended that we encourage technologies that limit the collection of personally identifiable data. This is important because due to the hardware limitations placed on mobile devices, it may be difficult to implement various security features found on the desktop computers. Therefore, collectively we must promote applications of technology that limit the collection of transactional information that can be tied to individuals. There are tools available to protect privacy by limiting the disclosure of information likely to reveal identity. These tools remove the identity information of an individual from any actions conducted using these wireless devices on the Internet by exploiting the decentralized and open nature of the Internet. Example of such a tool is ‘Crowds’ that provides anonymity to individuals by mingling their requests for access to Web sites with those of others. This tool, by routing access requests in a series of unpredictable paths, hides the identity of the requester. A similar tool to the Crowds, passes the communications through a series of routers before reaching the recipient. The message is encircled in a series of layers, resembling an onion and each router is able to peel one layer of the onion enabling it to learn only the next stop in the messages path. Passing messages in this fashion protects an individual's identity by obfuscating the originator and recipient of the message from points in the network. These technical advances, if adopted by users, can provide protection for privacy.

It is the responsibility of consumers and individuals to establish rules and use technologies that control personal information during commercial interactions as there will be limits to the effectiveness of regulation and self-regulation. Governments can also help us by generating enforceable standards, both self-regulatory and regulatory, to ensure that information provided for one purpose is not used (or disclosed) for other purposes. We must recognize that in this freewheeling, open marketplace, technological tools are needed to empower individuals to control their personal information.

[5] Subscribers opposed to this unilateral change in the "terms of service agreement" covering the use and disclosure of personal information and in response, AOL decided not to follow through with its proposal.

CONCLUSION

While the future of wireless application is bright, various important issues need to be addressed before consumers fully accept the technology. Combined with location identification technology, wireless applications make some impressive applications realised. But security and privacy of individuals appear to be major issues with these technologies. While there have been some recent changes to privacy laws associated with information technology, organisations appear to have difficulty in implementing them. The four risk areas mentioned in this paper are being investigated further in order to assess the awareness of privacy and security issues with a focus on regulatory frameworks. The subjects of the investigation include industries, consumers and government agencies in order to determine the general awareness of privacy and security issues in a wireless application domain.

While privacy on the Internet is in a fragile state, there is new hope for its resuscitation as business community has recently begun serious efforts at self-regulation. Further, a growing number of advocacy organizations, ranging from consumer to civil liberties to libertarian organizations, have begun to focus on privacy. The public voice is being heard more clearly than ever, more often than not weighing in strongly in support of privacy protections through law and technology over the Internet and this reaches a larger audience. This would, hopefully, trigger new developments in the privacy and security regulatory framework.

REFERENCES

Andrews, W. (2001). *Portals and E-Commerce: Different Goals, Parallel Projects* (No. COM-13-6391): Gartner.

Anonymous. (2000). Wireless technology reaches behind the firewall. *Informationweek.com* (June), 30.

Atwal, R. (2001). *The wireless office: Evolution, Revolution or Bust* (No. PCIS-EU-DP-0101): Gartner Research.

Budhwani, K. (2000). Becoming part of e-Business. *CMA Magazine,* 24-27.

Clarke, R. (2003). *Identification and Authentication Fundamentals*. Retrieved 10 Feb 2004, 2004

Deise, M. V., Nowikow, C., King, P., & Wright, A. (2000). *Executive's Guide to e-Business: From Tactics to Strategy*. New York: John Wiley & Sons, Inc.

Dornan, R. (2001). *The essential guide to wireless communication applications*. Upper Saddle River, NJ: Prentice Hall PTR.

Fink, D. (2000). Developing trust for Electronic Commerce. In L. Janczewski (Ed.), *Internet and Intranet: Security and Management: Risks and Solutions* (pp. 44-86): Idea Group Publishing.

Fitzgerald, T. (2003). The HIPAA Final Rule: What's Changed? *Information Systems Security*(May/June), 50-59.

Freeman, E. H. (2003). Privacy Notices under the Gramm-Leach-Bliley Act. *Legally Speaking* (May/June), 5-9.

Ghosh, A. K. (2001). *Security and Privacy for E-Business*. New York: Wiley.

Green, P. (2000, 4 June). Eastern Europe's Foray into M-Commerce. *The New York Times,* p. 3.8.

Hayes, S. (2001, 27 February 2001). Indian Giant Wants Service Staff. *The Australian,* p. 38.

Hulme, G. (2000). Services Seeks to Bring e-Business to Small Businesses. *Informationweek.com, August 2000,* 21.

Loney, M. (2000). M-Commerce safety fears. *IT Week, 3,* 6.

McConnel, B. (2000). Kennard pushes cable DTV. *Broadcasting & Cable* (February), 37.

McCullagh, A., Little, P., & Caelli, W. (1998). Electronic Signatures: Understand the past to develop the future. *University of NSW Law Journal, 21*(2), 1-13.

Morger, O., Nitsche, U., & Teufel, S. (1997). *Security Concerns for Mobile Information Systems in Health Care.* Paper presented at the 8th Int'l workshop on database and Expert Systems Applications.

Schiller, J. (2000). *Mobile Communications*. New York: Addison-Wesley.

Shroeder, S. (1999). Wired for business. *Risk Management*(March), 12-22.

Smith, D., & Andrews, W. (2001). *Exploring Instant Messaging*: Gartner Research and Advisory Services.

Warrington, T. B., Abgrab, N. J., & Caldwell, H. M. (2000). Building Trust to Develop Competitive Advantages in e-Business Relationships. *CR, 10*(2), 160-168.

Zhang, Y., & Lee, W. (2000). *Intrusion detection in wireless ad-hoc networks.* Paper presented at the ACM/IEEE MobiCom.