**Association for Information Systems**
**AIS Electronic Library (AISeL)**

CONF-IRM 2010 Proceedings

International Conference on Information Resources Management (CONF-IRM)

5-2010

# 39P. Nature and Extent of Identity Crime through Wireless Technology Abuse and its Impact on Individual and Organisational Levels

Salman Ahmad
*The University of New South Wales*, salpals_bs@yahoo.com

Donald Winchester
*The University of New South Wales*, d.winchester@unsw.edu.au

Lesley Land
*The University of New South Wales*, l.land@unsw.edu.au

Rodger Jamieson
*The University of New South Wales*, r.jamieson@unsw.edu.au

# 39P. Nature and Extent of Identity Crime through Wireless Technology Abuse and its Impact on Individual and Organisational Levels

Salman Ahmad
The University of New South Wales
salpals_bs@yahoo.com

Donald Winchester
The University of New South Wales
d.winchester@unsw.edu.au

Lesley Land
The University of New South Wales
l.land@unsw.edu.au

Rodger Jamieson
The University of New South Wales
r.jamieson@unsw.edu.au

## *Abstract*
Perpetrator(s) are stealing personal data abusing wireless networks to commit identity fraud and related crimes that is affecting us on individual, organisational and national levels. These threats affect national security also (Smith et al. 2010). There have been instances of identity and data theft crimes involving millions of debit and credit card numbers, which indicate the seriousness of this issue and reinforce the concerns of security professionals. These cases were taken from newspapers and recent research papers related to this field and analysed in this study. The objective of this research paper is to investigate the security weaknesses in the wireless protocols and examine how perpetrators are exploiting the wireless networks. The security limitations found in the commonly used types of wireless networks are also presented. The sharing of information on social networking services such as Facebook and Twitter also pose privacy and security threats. The current study presents guidelines and discusses approaches employed to safeguard and protect wireless networks in organisations. It is a study to create public awareness about the threats and related privacy issues in the use of wireless and hand held communication devices.

## *Keywords*
Wireless Technology, Wireless Security, Identity Crime, Identity Fraud, Identity Theft, Privacy, Regulations, Standards.

## 1. Introduction
This paper investigates the increasing abuse of wireless networks. Criminals are exploiting traditional vulnerabilities because individual users are paying little attention to them. Perpetrators are targeting all sectors (e.g., public, private, financial, retail) in order to gain access to private information and use it for their own benefit. Besides economic threats, our national security is also at stake (Smith et al. 2010). Wireless communication devices are also

vulnerable to attacks and most of the users are unaware of how to improve their wireless security.

An example of a well publicised security breach in the retail sector occurred when hackers broke into the wireless networks of the Marshals store in United States (US) (Tarasewicha et al. 2008). They stole customers' credit and debit cards information. The growing power of handheld devices, faster Internet connections, and the increasing deployment of wireless networks are bringing a new range of services to users but also raising many more security and privacy threats to them.

This paper investigates the persistent problems in wireless networks abuse. We ask the following research questions: What are the major weaknesses and security limitations of wireless networks? What are the threats and privacy issues involved in the use of wireless communication devices? How can the stolen personal data be abused? How can employers and organisations be adversely affected due to insecure wireless networks and devices? The study includes the analysis of high profile wireless abuse cases and describes how wireless networks are being exploited. The cases were identified by searching through proprietary databases, library databases, government agencies statistics reports, and online journals and newspaper articles using keywords such as identity thefts/crimes/deception (and synonyms), with a focus particularly on breaches that have occurred in wireless networks.

The rest of the paper is structured as follows. Section 2 discusses the current status on wireless abuse and related abuses resulting in identity crime events, as reported from various sources of the literature. Section 3 concludes and outlines future research.

# 2. Wireless Abuse - Current Status

Identity crimes and abuses are on the rise. Therefore, unsurprisingly, there is an increasing need of developing strong security protocols for wireless networks. An increase of 22% of these abuses was recorded in 2008, when about 9.9 million Americans were victims of identity theft (Finklea 2009). There is also a need to create awareness about the secure use of mobile and wireless devices among people. Many standards are put forward to address the weaknesses in security and they are continuously revised by the authorities. These standards are reported in section 2.5.

## 2.1 Common Terms and Definitions Related to Wireless Abuse

The main types of wireless connectivity based on the distances over which they operate, are summarised in Table 1 (Urbas and Krone 2006). Wireless Wide Area Network (WWAN) covers the largest distance and Wireless Personal Area Network (WPAN) covers the least.

Medium Access Control (MAC) spoofing occurs when a perpetrator is able to listen in on network traffic and identify the MAC address of a computer/device. Most wireless systems allow some kind of MAC filtering to only allow authorised access. However, a number of programs exist that have network 'sniffing' capabilities. Perpetrators can combine these programs with other software that allow a computer to pretend it has any MAC address that they desire, and they can easily get around that hurdle to access resources on the network.

In 2008 the US Department of Justice filed charges against eleven individuals who abused the wireless network of major retailers in US resulting in theft and sale of approximately forty million credit and debit card numbers (IBLS 2008). The hackers used a tactic called 'war-driving' that involves driving around with a laptop computer and trying to access weak wireless networks in the range of the car.

| Abbreviation | Name | Example | Distance |
|---|---|---|---|
| WWAN | Wireless Wide Area Network | GSM (Global System for Mobile communication) mobile phones, 3G (Third Generation) mobile phones | 10 km |
| WMAN | Wireless metropolitan area network (IEEE 802.16) | Suburb of city connected to the internet at broadband speeds | 1 km |
| WLAN | Wireless local area network (IEEE 802.11) | Local area network on the floor of a building connecting all workstations and servers | 100 m |
| WPAN | Wireless personal area network (Bluetooth, Infrared) | Connecting and controlling various products and devices | 1 m |

**Table 1**: Four main types of wireless connectivity, based on the distances over which they operate (Source: Urbas and Krone 2006, p. 2).

## 2.2 Attacks on Wireless Networks

Ad hoc networks are formed dynamically, where all the devices connect via wireless links. The topology of networks keeps on changing when these mobile devices move in and out of other devices' transmission range. This makes the ad hoc networks vulnerable to attacks (Vainio 2000). The attacks on wireless networks include monitoring transmission for:

- Message content (known as eavesdropping), and
- Patterns of communication (known as traffic analysis).

Another type of wireless network called Wireless Sensor Network (WSN) is formed by a large number of sensor nodes, each equipped with sensor(s) to detect physical phenomena such as heat, light, motion, or sound. WSN devices have severe resource constraints which lead to many open issues. Key distribution is such an issue which refers to the distribution of multiple unique keys among the sensor nodes. Key management (Lee et al. 2007) is a broader terms for key distribution. Since WSN nodes are frequently deployed in unsupervised and remote locations, physical tampering is a real threat, and the WSN must be able to withstand the compromise of any node.

The risks involved in wireless networks include:

- Intrusion – unauthorised access to network
- Leeching- unauthorised use of bandwidth by intruders, and
- Exploitation - misuse of network to launch Denial of Service (DOS) attacks against third parties (Urbas and Krone 2006).

Often devices in wireless networks have limited battery power. So with battery exhaustion attacks (Vainio 2000), a malicious user can consume energy from the battery of a device, causing the power to go out prematurely. A perpetrator may also exploit a wireless network

by probing the network to discover whether they are accessible. This is also called sniffing (Urbas and Krone 2006). The perpetrator can then access the information on network and exploit it.

The threat of viruses and worms are spreading to cell phones and other wireless devices as well. The first mobile-specific malware, a worm called 'Cabir' (Tarasewicha et al. 2008) was created in 2004 and was transmitted through open Bluetooth connections. Hackers can remotely access a Bluetooth-enabled phone and use it to make calls, send texts and browse the web without the phone-owner's knowledge. This is referred to as 'Bluebugging' (see http://www.stuff.co.nz/technology/gadgets/2739051/Guide-to-Bluetooth).

## 2.3 Impact of Identity Crimes

Identity crime is an umbrella term for identity fraud, identity theft and identity deception acts. Identity theft and identity deception acts occur prior to the perpetrator committing identity fraud. Identity Deception is when identity details are obtained by deceit through changes to an actual entity's (individual or organisation) identifying information data or the invention of fictitious details. Identity theft is when someone steals entity's identifying information details.

"*Identity Fraud* is crystallised when identity details of an entity obtained via theft or deceptive means are used to avoid an obligation or liability or misrepresent with intent. *Identity Related Crimes* include using identity details of an individual or entity obtained via theft or deceptive means for money laundering, terrorism, trafficking – people, weapons, drugs or illicit material. Note an act or event is only a 'crime' if legislation is enacted" (Jamieson et al. 2008, p. 448). Identity crime sub-classes are often interconnected with various other criminal activities and the effects extend outside of pure financial burdens. Figure 1 illustrates these concepts. This section discusses these effects on us at different levels.

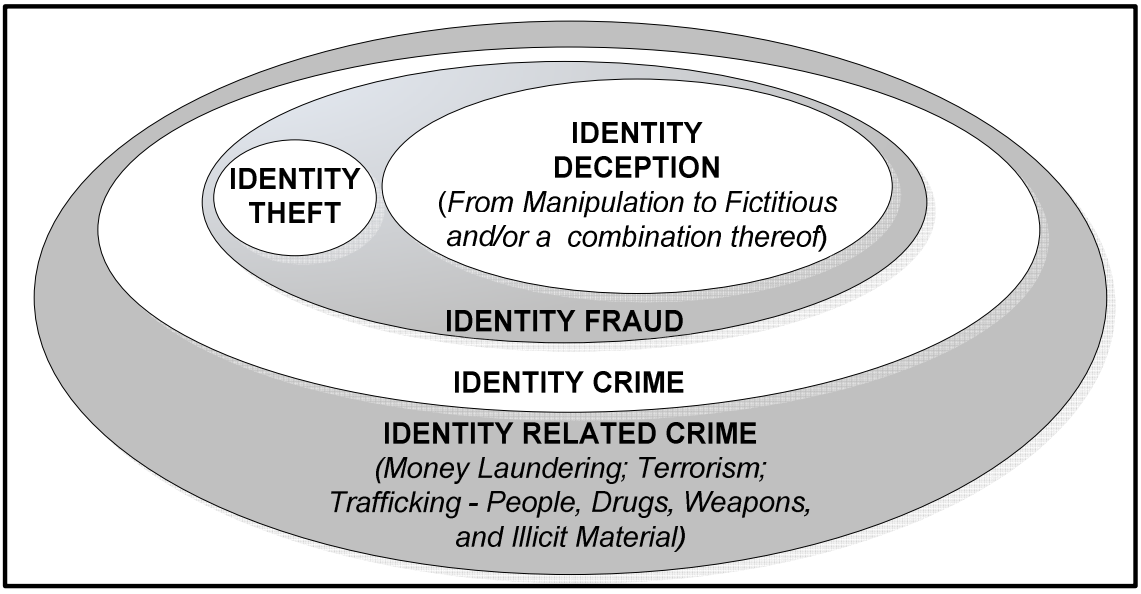


**Figure 1**. Conceptual model of identity definitions (Jamieson et al. 2008, p. 447)

### *2.3.1 Impact on Individuals*

Mobile phones are the next easy targets for professional hackers. People conduct private conversations in public places without regard for privacy, raising criminal opportunities to exploit their security. Although Bluetooth in phones can operate only within 10 metres, hackers can easily extend this hacking distance with the use of an inexpensive antenna. This threat is present in any WPAN. In an experiment (Loo 2009), researchers were able to capture address books from Bluetooth enabled devices at a taxi stand, from the 11th floor of a building. Thus a small distance wireless network should not be considered safe.

Leaking address book information may have serious consequences. The perpetrators may sell the information to users' competitors which may be very valuable for them. Perpetrators may eavesdrop on user conversations turning the mobile device into a perfect bugging device. Users tend to store their sensitive information such as bank account details, passwords, Personal Identification Number (PIN) on their phones. Employees may download important files on to their mobile devices, from their employer's computer systems. Such information if compromised can have serious impact on individuals as well as on their employers e.g., loss of trust and reputation. Figure 2 illustrates the most common misuses of victims' identities. The most common misuse (except for category 'Other') in 2008 has been credit card fraud followed by government documents or benefits fraud.

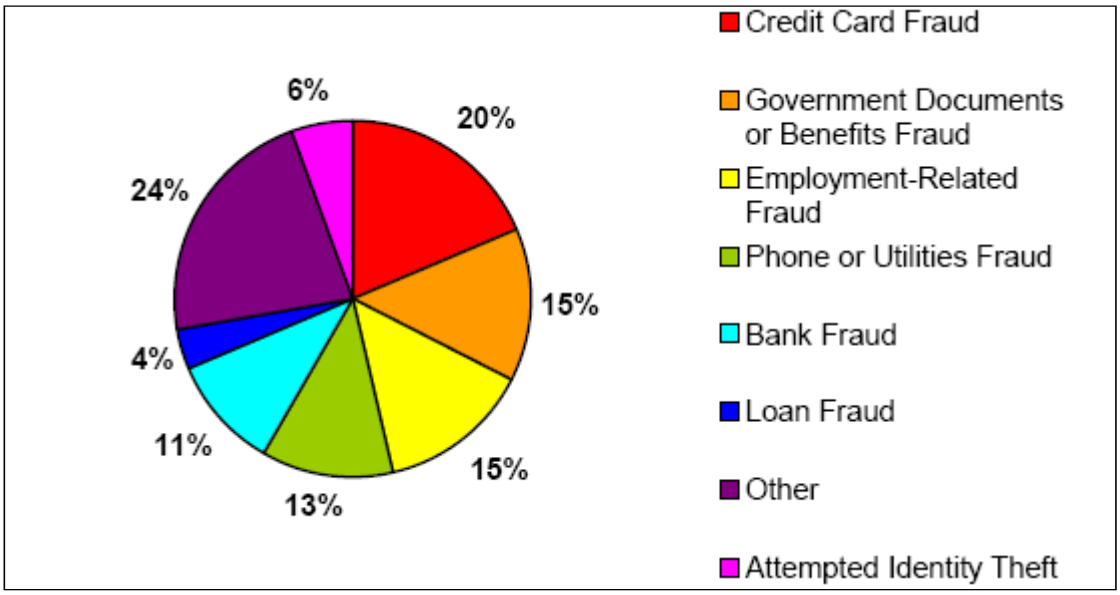


**Figure 2**: How Victims' Information is Misused (Federal Trade Commission 2009, p.11).

The identities or other personal data can be stolen by a large number of methods including taking advantage of a vulnerable wireless network. The incidence of a security breach at TJX/Marshals (Tarasewicha et al. 2008) in US mentioned previously is an example. The thieves stole customers' data streaming through the air between cash registers and handheld price checking devices, using a telescope-like antenna. Once the thieves have access to the personal information, they can use it to fake documents such as birth certificates, driver licences, open bank accounts, etc. This directly affects the victim if the victim attempts to legitimately apply for benefits and then is denied. The thieves can even illegally use the information for 'employment fraud' (Finklea 2009) adversely affecting the victim's credit

and ability to obtain future employment, amongst other things. Criminals are now targeting online banking customers using localised text message scams that leave virtually no trail. A Sydney based cyber-gang ripped off an individual (Fowler 2009). They trapped him with a 'phishing' scam i.e., a fake email request from his bank, asking for his personal details. They misused his credit card, stole money from his bank account and tricked a phone company into redirecting his phone calls and Short Message Services (SMS) to a different phone and thus misused the internet banking services on his behalf. Though the bank compensated for the stolen money later, the experience for the victim was devastating where his identity was totally taken over by a criminal. There are even online forums available that allow perpetrators to network and trade in criminal activities with other perpetrators. It is like criminal eBay where everything is for sale including stolen personal information, credit card numbers and software tools to attack networks and compromise them. Once the money is stolen online, the thieves convert their electronic theft into hard cash with the help of 'mules'. First a professional looking website is created with vacancies for so-called financial officers with attractive remuneration offers. The potential job applicant - that is a potential mule - will have a lot of money transferred to their account which they are asked to deposit into the fraudster's account, using some sort of wire transfer agency. Eventually the authorities will track and come after the mule while the fraudster can get away clean as they are very hard to discover in cyber space or other jurisdictions

### *2.3.2 Impact on Organisations*

Any security breach announcements from an organisation have adverse effect on the financial market (GAO 2007). The bond ratings and stock price of the organisation often decline. Customers lose confidence and this gives competitors an advantage. Any public announcement of security breach alerts other hackers about the vulnerability of the organisation, who may try out even more attacks on the organisation. These are a few of the reasons that organisations are reluctant to even report such incidences to law enforcement agencies.

Loss of a single mobile or wireless device from an organisation can result in extraordinarily large amounts of data being compromised. For example, a laptop theft resulted in the loss of veterans' personal data maintained by the US Department of Veteran Affairs which heightened the risks of identity theft for more than 26 million US veterans (Tarasewicha et al. 2008). Thus securing corporate networks and corporate wireless assets is essential. A denial of service attack can typically cost a company US$100,000 an hour (Wallace 2009). Thus the financial impact on an organisation can also be massive.

An interesting Television program named "Fear in the Fast Lane" (Fowler 2009) by Australian Broadcasting Corporation (ABC) network covered some interesting facts about wireless networks. The reporter went 'war-driving' in a suburb of Sydney, and just within 20 minutes, discovered more than a hundred vulnerable wireless networks. The perpetrators were also able to browse through the documents and data on a weak wireless network of the broadcasting company's employee, while war-driving near his house. This is an example of how an organisation's data can be at stake due to insecure wireless network at an employee's home.

### *2.3.3 Impact on Countries/Nations*

This subsection discusses how our national security is at stake due to identity thefts through wireless technology. The creation of fraudulent documents (Finklea 2009) may, among other things, provide fake identities for unauthorised immigrants or fake passports for people trying

to illegally enter the country. Radio frequency identification (RFID) chips are used in the credit cards, passports and in cars. Technology is available that can scan these chips from up to a metre away (Schliebs 2009). There is a need of research on how to encrypt the chips so that scanning them by perpetrators is impossible. Identity theft is implicated in international terrorism. The Indonesian police believe that the 2002 terrorist bombings in Bali were partially financed through online credit card fraud (GAO 2007). Identity theft and resulting frauds can thus have an impact on national and international security as well. Terrorists may send false bomb threats to airlines using the compromised wireless phone of an individual, in order to mislead governments and to waste their resources in the wrong direction.

## 2.4 Privacy Issues

Privacy laws differ in different regions of the world. While Europe's laws are generally applicable to all sectors, in US, privacy regulation tends to be sector specific. Under the European legal regime, automatic data collection by monitoring systems (RFID- Radio Frequency Identifier, cameras, Wi-Fi (Wireless Fidelity) location, GPS-Global Positioning System) including location data requires notification and consent from the owner as well as access rights by the owner (Subirana and Bain 2006).

In mobile/cellular networks, a mobile user must expose their personally identifiable information and credentials to each foreign network that they roam on to. This is necessary for billing purpose. However a security architecture that gives the users the flexibility to remain anonymous may be a significant step in securing mobile users privacy (Ring et al. 2007). Privacy levels from organisational and personal perspectives may differ, which can potentially lead to conflicts when a device supports both personal and business use. The role of intelligent agents and sensors will play an even more dominant role in future services.

Highly Dynamic Systems (HDS) discussed in (Subirana and Bain 2006) are evolving in the retail industry that involves automated intelligent agents. A grocery-based scenario is an instance where the individual's privacy rights may be violated. Merchants can use features such as RFID-based customer recognition, monitoring of the customer's position and shopping cart contents. A competitor store may pickup the consumer's personal RFID tag from nearby and may contact them via SMS or telephone, claiming that they have better deals to offer. Undesired products and services can be 'pushed' to consumers regardless of any consent or rejection to receive such advertisements. Most of the data processed within the retail scenario presented is personal data as defined by law. The misuse of personal data is a potential reason of mistrust on wireless technology.

People often have problems with creating, and then remembering, strong passwords, and the increasing tendency to disclose personal information on services like Twitter and Facebook. They must be careful about what they make public while using such social networking applications. The privately-held Twitter is reported to have six million unique visitors each month (Keizer 2009). A breach occurred when a hacker broke into an administrative assistant's e-mail account by taking advantage of a weak password, then used that to collect information that let him access the employee's Google Apps account. He then forwarded hundreds of pages of internal Twitter documents to other web sites on the Internet. The hacker likely dug up possible responses to several personal questions to authenticate the user, by rooting through the Web for details about the employee, then used those to reset the password to one only he knew. Weak passwords is beyond the scope of this paper but the purpose of mentioning this incidence here is to indicate that any security breach in networks

of such social networking sites can have serious implications in terms of the privacy of the users.

## 2.5 Laws, Regulations, and Standards

Authorities can enforce regulations like requiring security measures and warnings for wireless network devices as they have done in California (US). The Westchester County, New York, security law requires that commercial businesses secure their wireless networks or face fines. The law also requires businesses providing wireless internet access, to put up signs advising users of the security risks (GAO 2007). In New Zealand, there is a jail sentence of two to seven years, for unauthorised access of computer for identity crime (Rilkoff 2009). Similarly there is a maximum penalty of imprisonment for two years according to clause 308H of "Crimes Act 1900 No 40" (http://www.legislation.nsw.gov.au) in Australia for unauthorised access to data in a computer. The US Department of State is trialling RFID chip encoded passports (McGinity 2004) on airports to combat identity crimes related to fake identity and passports. Thus the authorities are trying to make regulations for the use of wireless networks. Bluetooth and Institute of Electrical and Electronics Engineers (IEEE) 802.11 (Wi-Fi- Wireless Fidelity) are the two communication protocol standards for wireless devices within short range (1-100m) and are discussed next.

### *2.5.1 Bluetooth*

There are weaknesses in the Bluetooth standard. In order to communicate, the two Bluetooth devices must exchange their secret PIN and pair up (Loo 2009). The first step of this pair-up process takes place in plain text which is a weakness. When a connection is made with a Bluetooth device, it is easy to track and monitor the owner. Record can be maintained for all Bluetooth transactions and hence owner privacy is violated (Vainio 2000). Switching the device to 'hidden' mode can provide protection. However most of the manufacturers keep the default settings to be 'discoverable'. Moreover it may not be easier for most of the users to discover how to change this setting to hidden mode. In an experiment with a hidden computer in a public place, a Bluetooth sniffing program was able to detect more than 1,400 vulnerable mobile devices (Loo 2009).

### *2.5.2 IEEE 802.X*

The IEEE 802.11 standard has been referred to as Wi-Fi (Wireless Fidelity) and there have been many amendments to the 802.11 family. The Wi-Fi security protocol is called Wireless Equivalent Privacy (WEP), which is a weak and deprecated algorithm. But it is still widely used. In mid-2004 the 802.11i working group finalised an amendment providing a comprehensive authentication framework based on 802.1X and Extensible Authentication Protocol (EAP) methods, also known as Wi-Fi Protected Access 2 (WPA2). WPA2 provides Wi-Fi users with a high level of assurance that their data will remain protected and that only authorised users can access their wireless networks. WPA2 uses the Advanced Encryption Standard (AES) for data encryption and is eligible for Federal Information Processing Standards (FIPS) 140-2 compliance (Group 2009). A risk in Wi-Fi networks is MAC address spoofing. The attacker steals the MAC address of the device and uses it in his own device for unauthorised access. The threat of address spoofing is equally applicable to Bluetooth ad-hoc networks as well (Hall 2006)**.**

## 2.6 Approaches to Secure Wireless Networks

Wireless access and communication in an organisation is a potential security risk factor that is taken into account, while auditing information security systems. The information security

professional must fully understand the wireless protocols and must make informed decision for their particular case. Wireless security is a layer 2 (data link) problem and not layer 3 (network) problem (Kindervag 2007). Specialised audit tools can be used to test information security controls (GAO 2009). For example:

- Password crackers can identify the use of vendor-default or easily guessed passwords.
- Network 'sniffers' (software that can intercept and log traffic passing over a network) can identify the transmission of passwords or sensitive information in clear text.
- War driving software used to detect unauthorised wireless access points.

An organisation must carefully decide how many authentication steps are required to access a device and its data. The relationship between number of factors in authentication and usability must be investigated. There is a need of mechanism that provides security with increased usability. Employees can be educated how to select and use their phones properly. This may also force the manufacturers to improve their products' interfaces. An organisation must take an integrated approach to secure its infrastructure and security should be the focus of all business groups within the organisation. As discussed in Kindervag (2007), the wireless network must be regularly monitored and segmented from internal network. Network intrusion prevention tools are useful to protect the data stream. The Payment Card Industry (PCI) Data Security Standard (DSS) Wireless guidelines supplement is a very good source for the retail sector on how to secure their network (Group 2009). The PCI Security Standards Council was formed by the major payment card brands such as American Express and Visa Inc. Although the document is specifically for organisations that deal with cardholder data with or without wireless LAN (WLAN) technology, but it can be equally good for all organisations with wireless networks.

An organisational policy for securing mobile devices should restrict unnecessary downloads and all mobile devices must be equipped with up-to-date security software. Advanced security solutions such as data storage encryption, tools that can track lost mobile devices must be employed. Organisations may invest in mobile devices with biometric capabilities to restrict unauthorised access if stolen, and multiple forms of user authentication are recommended. Wireless access via a Virtual Private Network (VPN) can also be highly effective as suggested in (Tarasewicha et al. 2008).

For better protection, individuals should only activate their Bluetooth when required, otherwise should keep their devices in the "hidden mode". Users must not accept any unsolicited request to pair up and should regularly monitor their devices to discover any suspicious connections. Moreover individuals must also monitor the power consumption rate of the phone. While using a wireless device in a public place, privacy covers that make the screen difficult to view by another observer can be used. These approaches can be effective in making wireless technology abuse more difficult for the perpetrators.

# 3. Conclusion

In the wireless world, one must always be vigilant and proactive. We can only make the wireless networks more difficult for the perpetrators to exploit but still not completely secure. The problem is that often the data in wireless network is either not encrypted or weakly encrypted, allowing the perpetrators to steal it. In other cases, users are just careless or naïve enough not to enable the security features of their equipment.

Most Information Technology equipment manufacturers ship their products with the security settings turned off by default. Manufacturers must stop doing it and must make their device interface user-friendly so that users may find it convenient to set the security settings to an appropriate level. The WEP encryption standard used by many access points is weak, though the recent WPA standard is tougher. Further research should be directed to investigate design mechanisms and improve mobile device interfaces in order to minimise customers' privacy concerns and to make the Wi-Fi security protocols impossible to crack. Although there are a variety of laws that make it illegal to access a computer network without permission, very few of these laws have been tested in the courts. There should be strict laws that make it difficult for the perpetrators to trade their stolen data online.

Further research is required to investigate the factors that motivate individuals to secure their wireless communications and understand how employees can be motivated to protect employer's data while using their wireless (mobile) devices. Academia and practitioners can assist by undertaking collaborative research to strengthen security protocols for wireless networks. There is a need for future research on measures that can be applied to secure wireless networks in specific sectors which carry a high level of economic and financial risks such as in government and banking transactions. Technology alone cannot prevent identity crimes. An effective approach in this regard would necessarily be multi-pronged involving standardisation, education and awareness, policy and legislation development, governmental and organisational collaboration and technical/technological mechanisms (to name a few). Research in this area can be very challenging but rewarding.

## *References*


Fantacci, R., Maccari, L., Pecorella, T. (2007) "Analysis of Secure Handover for IEEE 802.1X-Based Wireless Ad Hoc Networks", *IEEE Wireless Communications*, (14)5, pp. 21-29 (available at: http://awin.cs.ccu.edu.tw/magazine/IEEE_Wireless/2007/October/04396939.pdf)

Federal Trade Commission (FTC). (2009) "Identity Theft Clearinghouse data, Consumer Sentinel Network Data Book for January – December 2008", February 26. (available at: http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2008.pdf.)

Finklea, K. M. (2009) "Identity Theft: Trends and Issues", CRS Report for Congress Congressional Research Service, May, (available at: http://www.fas.org/sgp/crs/misc/R40599.pdf)

Fowler, A. (2009) "Fear in the Fast Lane", *Australian Broadcasting Corporation*, August 17. (Program Transcript available at: http://www.abc.net.au/4corners/content/2009/s2658405.htm)

GAO (2007) "Cybercrime - Public and private Entities Face Challenges in Addressing Cyber Threats", US Government Accountability Office, Report to Congressional Requesters. June. (available at: http://www.gao.gov/new.items/d07705.pdf)

Group, W. S. I. (2009). Information Supplement: PCI DSS Wireless Guideline. (available at: https://www.pcisecuritystandards.org/pdfs/PCI_DSS_Wireless_Guidelines.pdf)

Hall, J. (2006). "Detection of rogue devices in Wireless Networks", Ottawa-Carleton Institute for Computer Science School of Computer Science, Carleton University, August. (available at: http://people.scs.carleton.ca/~barbeau/Theses/jen_hall.pdf)

IBLS, Editorial Board. (2008) "INTERNET LAW – Identity Theft from Wireless Networks", *Internet Business Law Services (IBLS)*, November 26. (available at: http://www.ibls.com/internet_law_news_portal_view.aspx?s=latestnews&id=2177)

Jamieson, R., Land, L., Sarre, R., Steel, A., Stephens, G., Winchester, D. (2008) "Defining Identity Crimes", *19th Australasian Conference on Information Systems. Christchurch*, December 3-5, pp. 442-451

Keizer, G. (2009) "Hacker break-in of Twitter e-mail yields secret docs", *Computerworld*, July 16. (available at: http://www.networkworld.com/news/2009/071609-hacker-break-in-of-twitter-e-mail.html).

Kindervag, J. (2007) "(Mis) Understanding Wireless LAN Security", *Business Communications Review*, (37)10, pp. 50-54.

Lee, J.C., Leung, V.C.M., Wong, K.H., Cao, J., Chan, H.C.B. (2007) "Key Management Issues In Wireless Sensor Networks: Current Proposals And Future Developments", *IEEE Wireless Communications*, (14)5, pp. 76-84.

Loo, A. (2009) "Security Threats of Smart Phones and Bluetooth", *Communications of the ACM*, (52)3, pp. 150-152

McGinity, M. (2004) "Weaving a Wireless Safety Net", *Communications of the ACM*, (47)9, pp. 15-18.

Rilkoff, M. (2009) "Networks open to hack attacks", Taranaki Daily News, September 22. (available at:http://www.stuff.co.nz/technology/2888134/Networks-open-to-hack-attacks)

Ring, J., Foo, E., and Looi, M. (2007) "A Secure Billing Architecture for 4G Wireless Networks", *Proceedings AusCERT Asia Pacific Information Technology Security Conference (AusCERT2007)*. Australia. pp. 14-30.

Smith, S., Winchester, D., Bunker, D., Jamieson, R., (2010 forthcoming). "Circuits of Power: A Study of Mandated Compliance to an Information Systems Security De Jure Standard in a Government Organization". *MIS Quarterly*.

Subirana, B., Bain, M. (2006) "Legal Programming", *Communications of the ACM*, (49)9, pp. 57-62.

Schliebs, M. (2009) "Credit cards targeted in high-tech street scams", *News.com.au*, August 14. (available at: http://www.news.com.au/story/0,27574,25924418-421,00.html)

Tarasewicha, P., Gong, J., Fiona Fui-Hoon Nahc and DeWester, D. (2008) "Mobile interaction design: Integrating individual and organisational perspectives", *Information Knowledge Systems Management*, (7)1, pp. 121-144.

Urbas, G., Krone, T. (2006) "Mobile and Wireless Technologies: security and risk factors", *Trends and Issues in Crime and Criminal Justice*, no. 329, pp. 1-6. (available at: http://search.informit.com.au.viviena.library.unsw.edu.au/fullText;res=AGISPT;dn=200 70575)

Vainio, J. T. (2000) "Bluetooth Security", Internetworking Seminar: Department of Computer Science and Engineering Helsinki University of Technology. (available at: http://www.mowile.com/bluesec.pdf)

Wallace, S. (2009) "Enterprise Security - So important yet so often ignored", *Business Week*. (available at: http://businessweek.ro/adsections/2005/pdf/0523_security.pdf)