Briefing paper

September 2010 > Issue: 1

CEPS ARC Centre of Excellence in Policing and Security

Review of Computer Chip Identification Systems

Alice Hutchings

The aim of this series is provide reliable up-to-date summaries of research by CEPS scholars. Written in an accessible style, the papers to provide material useful for practitioners and policymakers, as well as scholars and students. It also provides an opportunity to profile the work done within CEPS to a wider audience and encourage dialogue between the research and policy/practice communities. In our inaugural briefing paper, Alice Hutchings shares her expertise on smart card technologies, outlining the technological vulnerabilities of the smart card as both a tool and target of crime.

This topic is relevant to CEPS research relating to vulnerable infrastructure. The vulnerable infrastructure project examines the attributes of Australian and regional infrastructure that are most susceptible to exploitation and attack by transnational threats.

Simon Bronitt

Professor Simon Bronitt

Director

Overview

This paper reviews the key literature relating to embedded computer chip identification systems such as those used in smartcards and ePassports. It identifies social, policy and legal issues associated with their use, particularly as they relate to the Australian context. Computer chip identification systems, while offering many benefits, may contain valuable personal data and/or provide access to restricted areas. Therefore, the use of this technology has potential implications for the commission of offences such as identity theft, identify fraud and even terrorism.

Embedded computer chip identification systems are considered to be a countermeasure against identity theft as they include additional security measures compared to their predecessors (e.g. magnetic strip cards). However, due to the nature of the records that may be stored on the chip, including identification information and biometric data, they are valuable to offenders and breaches of their security may actually facilitate this type of offence. Choo, Smith and McCusker (2007, p. xiii) predict that “the future will also see new hardware devices and software programs that seek to compromise the quality of data-protection mechanisms used in smartcards”.

This paper provides an overview of computer chip identification systems, discusses potential vulnerabilities relating to the misuse of this technology, and the regimes for data protection and privacy, including the technical standards that apply in Australia and internationally.

Computer Chip Identification Systems

The first patent for a computer chip identification card was registered in France in 1974 by Roland Moreno (Rankl & Effing, 2004). The first applications of this technology were for bank and telephone cards in France and Germany in 1984. Computer chip identification systems and smartcards have since been used internationally for credit cards, stored-value cards, passports, national identification cards, driver licences and physical access tags (Kfir & Wool, 2005). “Smartcards” hold their data in an embedded chip that is accessed using a reader. Computer chip identification systems come in two distinct types: *contact*, which require physical contact with the reader; and *contactless*, which use radio frequency identification (RFID) induction technology to transmit the data between the chip and reader (Kfir & Wool, 2005).

Views expressed are personal to the author, and should not be attributed to CEPS or its industry partners.

The chips used are similar to those employed for mobile phone SIM cards, USB keys and RFID road toll tags (Australian Government Information Management Office, 2008b). Results from the Australian Institute of Criminology's Australian Business Assessment of Computer User Survey for the 2006/07 financial year indicated that less than one per cent of small, three per cent of medium and nine per cent of large businesses use smartcards (Richards, 2009). It is likely that these figures underestimate the use of smartcards by Australian businesses when taking into consideration their popularity for access control to restricted areas. While smartcard technology is not currently used in Australia for driver licences, it has been proposed that Queensland laminated driver licences be switched to smartcards in 2010 (Department of Transport and Main Roads, 2009). In 2007 a proposed National Health and Social Services access card based on smartcard technology was cancelled by the incoming federal Labor Government (Dearne, 2007), while passports with contactless smartcard chips have been progressively introduced in Australia since 2005 (Department of Foreign Affairs and Trade, 2008). Data stored on the ePassport chips include a digital photograph, which can be compared with the passport bearer using facial recognition technology. In addition, name, gender, date of birth, nationality, passport number and expiry date are stored (Department of Foreign Affairs and Trade, 2008). Smartcards are also used for public transport ticketing systems in some Australian jurisdictions, including Queensland, New South Wales and Victoria.

Computer chips may be partitioned so that data can be stored and accessed separately. This allows cards to be multi-functional. For example, a chip may incorporate an 'open' partition that contains the cardholders' details, while 'working' components include information relevant to the various functions of the card. 'Secret' partitions are accessible only with a PIN or biometric information such as a thumbprint (Hart, 2007).

Smartcard readers are available to be purchased commercially, however software may be required for the reader to interact with the smartcard. There are a variety of different types of readers available, including readers for contact and contactless smartcards, handheld and static readers, and readers that allow for a PIN or biometric information to be entered to verify the cardholder's identity and to access secret partitions (Australian Government Information Management Office, 2008b). It has been indicated that the software required to read the proposed Queensland smartcard driver licence will be commercially available (Austroads, 2008b). Cardholders would be required to enter a PIN to enable the information stored on the card to be read by standard readers, while authorised parties such as driver licensing authorities, police and driver licence enforcement personnel would be provided with specially configured smartcard readers (Austroads, 2008a). Austroads (2008a, p. 5) claim that "these readers will be subject to strict authentication and security controls to minimise the risk of unauthorised access to licensing information if they are lost or stolen".

Smartcards can be used to replace traditional magnetic strip cards, which are vulnerable to 'skimming' (Australian Government Information Management Office, 2008b). However, smartcards are generally more expensive than their counterparts. A cost analysis by the London School of Economics and Political Science (2005) into the proposed UK identity card estimated that smartcards would cost approximately 40 to 100 per cent more than a traditional card. Smartcards may also need to be replaced more frequently (London School of Economics and Political Science, 2005).

Identity Crime Risks

Passports and driver licences are not solely used for travel purposes. They often play an additional role to their primary function, namely as a form of validating identity when a person applies for government or business services, such as opening a bank account or applying for welfare. The more potential applications for computer chip identification systems, the bigger the implications are for misuse and the greater the target they become for identity thieves.

Identity theft commonly refers to stealing another's identity, while identity fraud is the use of another's real or a fictitious identity for an unlawful purpose (Australasian Centre for Policing Research, 2004). Cuganesan and Lacey (2003) estimated that identity fraud cost AUD$1.1 billion in the 2001/02 financial year. This included the cost to public and private sector organisations, including expenditure relating to prevention, deterrence, detection, investigation, recovery, restoration, financial loss, intangible loss and opportunity costs (Cuganesan & Lacey, 2003).

A study by Copes and Vieraitis (2007) identified that common ways to acquire information used for the commission of identity theft was to buy it from business and government employees, to steal mail from mailboxes and rubbish bins, to appropriate the identity of someone known to the offender, or obtain it during the course of employment. Personal information obtained in such a way was commonly used to apply for further identification documentation, such as driver licences. Once offenders had acquired information about the identity of the victim they then used it to commit other types of identity fraud, such as applying for credit cards and loans (Copes & Vieraitis, 2007). In addition, an underground market exists that trades in identify information (Baker et al., 2009).

Security Features

Smartcards are considered to be more secure than laminate or magnetic strip cards due to the use of chips and the potential for biometric data to be stored, such as digital photographs or thumbprints. In relation to driver licences, this means that the ability to tamper with and swap photographs is or should be severely limited (Department of Transport and Main Roads, 2010). In addition, the use of digital photographs allows for matching using facial recognition software, thereby increasing the likelihood that the instances where one person has applied for licences in multiple names, or where different people have used the one identity, will be detected (Department of Transport and Main Roads, 2010). Inaccuracies, however, may result in false positives, where the program may falsely detect duplicates, or false negatives, where the program fails to detect where the same person has applied for more than one licence (Hart, 2007).

Because embedded chips contain processing ability as well as storage ability more advanced protection may be implemented than is possible with magnetic strip systems. Additional security features that potentially can be included in computer chip identification systems applications include:

- A PIN and/or biometric template (such as a fingerprint) to both verify the cardholder and to restrict access to the data;
- Card and terminal verification to ensure each is genuine;
- Encryption;
- Design features such as codes or serial numbers that are hard-wired into the hardware or firmware to prevent duplication; and
- Tamper resistance (Australian Government Information Management Office, 2008b).

To prevent contactless computer chip identification systems being read without the cardholder's authorisation they can be stored in a metallic cover, known as a Faraday cage, to limit radio frequency penetration when the card is not in use (Choo et al., 2007).

Security Implications

Data is stored on the computer chip, the face of the card and supporting databases, creating three potential targets for identity thieves. The use of computer chips has a number of potential security implications, including unauthorised access to the data held on the chip, unauthorised modification of the data, and the cloning of chips to create counterfeit smartcards. The data held on computer chip identification systems are accessed using readers, either by direct contact or from a short distance. Contact computer chip identification systems are generally considered to be more secure than their contactless counterparts (Gupta, 2008). Contactless smartcards means that the collection of identification for the commission of offences could take place without the offender physically being in possession of the card. Although chips may be built with a read range of only a short distance, say, ten centimetres, they may still be capable of being read at greater distances with readers with a high signal transmission or a more powerful antenna (Langheinrich, 2007). Even with the generally accepted read range of about four inches for smartcard chips (Kfir & Wool, 2005), there is still the possibility that cards in pockets and handbags, or being sent by mail, could be scanned without the cardholder's knowledge (Juels, 2005). The range for eavesdropping between tags and legitimate readers can also reportedly span up to hundreds of metres (Langheinrich, 2007).

Encryption of the data makes it harder for eavesdroppers to read the signal between chip and reader (Rotter, 2008). The Queensland Department of Transport and Main Roads, while not providing information about the types of security that will be used for the proposed smartcard licence have advised that:

> Sensitive and personal data is currently transmitted and stored in a secure manner either through restricted access or encryption and this will continue (Department of Transport and Main Roads, 2010).

However, researchers have reported that smartcards and encrypted RFID chips have already been compromised:

> Several researchers have demonstrated that the security of [RFID] systems can often be easily broken, resulting in more or less severe forms of identity theft (Langheinrich, 2007, p. 443).

Despite the Australian Government Information Management Office (2008b, p. 7) claiming that "it is not possible to copy or counterfeit a smartcard", devices compromised by researchers include:

- A road toll payment device and a RFID car key being cloned (Juels, 2005);
- Data from an e-passport being read (Lettice, 2006);
- A chip in an e-passport being cloned (Evers & McCullagh, 2006);
- The encryption on the Mifare Classic Smartcard, used for public transport systems in a number of countries, being cracked (Nohl, 2010);
- Data from first-generation RFID-enabled credit cards being read, including name, credit card number and expiry date (Heydt-Benjamin, Bailey, Fu, Juels, & O'Hare, 2007);
- Computer chip card readers being tampered with to expose credit card and PIN details (Drimer, Murdoch, & Anderson, 2008); and
- Genuine computer chip credit cards being authenticated without the correct PIN being entered using a "man-in-the-middle" attack (Murdoch, Drimer, Anderson, & Bond, 2010).

The use of biometric data, namely digital fingerprints, to verify the identity of smartcard holders has also reportedly been compromised using a relay attack (Baker, 2002; Smith, 2006). It is important to note that some of the systems compromised above had lower levels of security than others.

However, there is no reason to think that people with the technical skills, although less noble motives, have not also attempted, and been successful, with such endeavours (Juels, 2005). Choo et al. stated, in relation to the proposed National Health and Social Services access card, that:

> Despite the security architecture – supported by rigorous access controls, logging and auditing – that will be deployed, organised criminal groups will seek ways of compromising the system's computer infrastructure or obtaining personal and confidential information (Choo et al., 2007, p. 42).

Additional security concerns relate to the integrity of the system, rather than the theft of data, namely the potential for denial of service attacks and viruses in the future (Ortiz, 2006). Further, the wealth of data held in supporting databases may be vulnerable to employee misuse.

Smith (1999, p. 3) states that "a more simple problem with smartcards, of course, is that access to the card is usually only protected by a PIN". These problems include the possibility of:

- The cardholder being tricked into revealing it through the use of social engineering;
- The PIN being guessed or cracked using computer technology;
- The legitimate cardholder being observed entering the PIN, known as "shoulder surfing";
- Rubbish being searched for relevant information, known as "dumpster diving";
- The cardholder storing the PIN on or with the card; and
- Cardholders being threatened with violence in order to obtain the PIN (Smith, 1999, 2006).

Supporting databases that contain information data are also an attractive target for identity thieves. Baker et al. (2009) found that 90 breaches in 2008 resulted in 285 records being compromised. The majority of data breaches (74 per cent) were the result of attacks from outside the organisation, and 64 per cent involved hacking (Baker et al., 2009).

Technical Standards

The use of computer chip identification systems by Australian state and territory governments is potentially problematic in relation to national consistency. Therefore, the Australian Government Information Management Office has developed a National Smartcard Framework for all levels of government that includes a minimum, but not mandatory, set of requirements for interoperability at both the infrastructure and application levels. The framework is based on relevant industry standards and includes principles relating to interoperability, privacy and data protection, risk management, security and trust, and choice and flexibility (Australian Government Information Management Office, 2008a).

Other standards and protocols may relate to specific applications of computer chip identification systems. For example, driver licences permit holders to drive, and therefore there will be a requirement that police and road safety authorities in all Australian jurisdictions can verify the details of licences issued in other states. As a result Austroads has been working with licensing authorities to develop the Smartcard Licence Interoperability Protocol (SLIP), relating to the use of smartcard driver licences in Australia (Austroads, 2008b). Passports, used internationally, are required to conform to International Civil Aviation Organization standards (Choo et al., 2007).

The Australian Government Information Management Office (2008a) has identified a number of Australian and international standards that apply to the use of smartcards. These standards relate to technical and privacy risks, project development, requirements for smartcards and infrastructure, physical characteristics of cards and provide common definitions for cardholder data items. As noted by the Australian Government Information Management Office (2008a), relevant standards and frameworks need to be constantly updated to keep up with technological changes.

Privacy Issues

The handling of personal information, such as records stored on computer chip identification systems and their supporting databases, by the federal government and the private sector is regulated by the *Privacy Act 1988* (Cth), while state governments have separate legislative or administrative privacy regimes (Australian Law Reform Commission, 2008). The Australian Law Reform Commission (2008) has recommended that Australian jurisdictions should adopt a nationally consistent privacy regime to ensure that personal information attracts similar protections across government agencies and the private sector and to assist individuals in knowing what their rights are and how to enforce them.

Smartcards enable large amounts of information to be collected about cardholders, particularly when used for multiple commercial and government applications. For example:

> Smart cards will be able to generate records of the date, time and location of all movements on public and private transport systems, along with details of all goods purchased, telephone use, car parking, attendance at the cinema, and any other activities paid for by smart cards. These records will also be processed and stored in central databases, where they will be used to create detailed customer profiles (Privacy Committee of New South Wales, 1995, p. ii).

The ability for the one card to be used for a number of different government and business services also creates ambiguities in relation to who controls the data, as well as who is accountable for its use, disclosure, accuracy and security (Australian Law Reform Commission, 2008). The Council of Europe (2004) has adopted guiding principles primarily aimed at the card issuer relating to the collection, processing, use, protection and deletion of personal data on smartcards and their supporting databases and the information provided to the cardholder about the management of their data, how to access and modify their personal data, and what to do in cases of fraud or unauthorised disclosure.

The privacy principles set out by the Australian National Smartcard Framework include:

- All relevant privacy regimes should be complied with;
- A communications plan should be developed to ensure that potential cardholders understand the ways in which their information will be protected;
- There should be a comprehensive privacy policy;
- A privacy impact assessment should be undertaken at relevant points in the design of the smartcard deployment, including initial and final design stages, and whenever the functionality of the system is to be altered, particularly when adding new applications or for secondary use of the data;
- Data should be protected by reasonable security safeguards;
- All contracted service providers are obligated to protect the data in accordance with the agency's requirements; and
- Data should not be stored in human readable forms, and access should require authorisation and include audit trails (Australian Government Information Management Office, 2008a).

There are three main privacy issues relevant to the use of computer chip identification systems that will be addressed here, namely function creep, location privacy and data mining. Privacy issues are particularly important when considering the use of computer chip identification systems by government agencies to access services or to fulfil, for example, licensing requirements. This is because individuals may not have any genuine choice as to whether their data is stored and accessed in this way due to the lack of alternatives (Hart, 2007). It is noted that the more data that is held on smartcards, the greater the potential implications are if their security is breached, not only for the potential loss caused by misuse, but also in relation to damage to the issuer's reputation.

"Function creep" refers to the use of information for a purpose other than its original intent. An example of function creep is the recent announcement that in Queensland Translink's go card will be combined with Seniors cards (Nolan, 2009). The Queensland Department of Transport and Main Roads (2010) have not ruled out the possibility of function creep for the new smartcard driver licence, stating that "while it is possible for the Smartcards to contain additional information and have extra functions, Queensland Government has no current plans for the expansion of the Smartcard driver licence (or associated Smartcards) beyond what is currently proposed". The Department has not indicated whether future plans and usages for the proposed smartcard licence would be subject to scrutiny or oversight. It is noted that there is the ability for multi-function cards to have additional security measures built in to ensure that data in one part of the card remains separate from other sectors (Hart, 2007).

Recently in Australia and overseas licensed premises have resorted to scanning the drivers licenses of its patrons as a condition of admission, purportedly for security purposes (Palmer, Warren, & Miller, 2009). This raises security concerns about the storage and potential misuse of this information (Palmer et al., 2009). In Australia businesses are not required to comply with the *Privacy Act 1988* (Cth) if their annual turnover is $3 million or less.

"Location privacy" (Langheinrich, 2007, p. 441) refers to the potential ability for information to be stored about cardholders' movements by the keeping of records as to whose smartcards were read at a particular time and place. The threat to location privacy is increased with contactless computer chip identification systems, especially since cardholders may not be aware that their card has been read (Australian Law Reform Commission, 2008).

Data matching and data mining refer to the processing and analysis of information across databases (Australian Law Reform Commission, 2008). For example, if the smartcard is used for multiple purposes in the future, or if data are retained relating to when and where smartcards are read, these data could potentially be linked to identify what resources or services the holder has accessed. Biometric information such as digital photographs or fingerprints can potentially be matched using recognition software to link images of individuals with identities (Hart, 2007). Privacy concerns that arise in relation to data matching and data mining include the amount of previously unknown personal information about individuals and the lack of knowledge or consent provided by the data subject (Australian Law Reform Commission, 2008).

Conclusion

Computer chip identification systems have been implemented worldwide to make identification and card systems more robust and less vulnerable to fraud and misuse. However, recent examples demonstrate that such systems are not invulnerable to attack, with chips, readers and supporting databases being compromised. The numerous privacy issues arising from the use of this technology is particularly pertinent in the Australian context, where there is currently no nationally consistent privacy regime.

References

Australasian Centre for Policing Research (2004). Standardisation of Definitions of Identity Crime Terms. Marden: Australasian Centre for Policing Research.

Australian Government Information Management Office (2008a). National Smartcard Framework. Barton: Department of Finance and Deregulation.

Australian Government Information Management Office (2008b). National Smartcard Framework: Smartcard Handbook. Barton: Department of Finance and Deregulation.

Australian Law Reform Commission (2008). For Your Information Report 108: Australian Privacy Law and Practice (Vol. 1). Barton: Commonwealth of Australia.

Austroads (2008a). Smartcard Licence Interoperability Protocol (SLIP): SLIP and Privacy. Adelaide: Austroads.

Austroads (2008b). Smartcard Licence Interoperability Protocol (SLIP): SLIP Compliant Driver Licence - Business Impacts. Adelaide: Austroads.

Baker, L. (2002). Rule of thumb: Don't rely on new security systems. ANU Reporter, 33(9), 1.

Baker, W. H., Hutton, A., Hylender, C. D., Novak, C., Porter, C., Sartin, B., et al. (2009). 2009 Data Breach Investigations Report. Retrieved May 11, 2010, from http://www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf

Choo, K.-K. R., Smith, R. G., & McCusker, R. (2007). Future Directions in Technology-Enabled Crime: 2007-09. Canberra: Australian Institute of Criminology.

Copes, H., & Vieraitis, L. (2007). Identity Theft: Assessing Offenders' Strategies and Perceptions of Risk. Birmingham: University of Alabama.

Council of Europe (2004). Guiding Principles for the Protection of Personal Data With Regard to Smart Cards. Strasbourg: Council of Europe.

Cuganesan, S., & Lacey, D. (2003). Identity Fraud in Australia: An Evaluation of its Nature, Cost and Extent. Sydney: Standards Australia International Ltd.

Dearne, K. (2007). Canberra to cancel access card. Retrieved March 4, 2010, from https://www.passports.gov.au/Web/ServiceCharter.aspx

Department of Foreign Affairs and Trade (2008). The ePassport. Barton: Department of Foreign Affairs and Trade.

Department of Transport and Main Roads (2009). Queensland Smartcards. Retrieved February 11, 2010, from http://www.transport.qld.gov.au/Home/Licensing/Queensland_smartcards/

Department of Transport and Main Roads (2010). Frequently Asked Questions. Retrieved February 11, 2010, from http://www.transport.qld.gov.au/Home/Licensing/Queensland_smartcards/Frequently_asked_questions#question_03

Drimer, S., Murdoch, S. J., & Anderson, R. (2008). Technical Report Number 711 Thinking Inside the Box: System-Level Failures of Tamper Proofing. Cambridge: University of Cambridge.

Evers, J., & McCullagh, D. (2006). Researchers: E-passports pose security risk. Retrieved March 9, 2010, from http://www.theregister.co.uk/2006/01/30/dutch_biometric_passport_crack/

Gupta, A. (2008). Design and Implementation of Public Key Infrastructure on Smart Card Operating System. Indian Institute of Technology, Kanpur.

Hart, C. (2007). Micro-chipping away at privacy: Privacy implications created by the new Queensland driver licence proposal. QUT Law and Justice Journal, 7(2), 305-324.

Heydt-Benjamin, T.S., Bailey, D. V., Fu, K., Juels, A., & O'Hare, T. (2007). Vulnerabilities in first-generation RFID-enabled credit cards. Lecture Notes in Computer Science, 4886, 2-14.

Juels, A. (2005). Attack on a cryptographic RFID Device. Retrieved February 17, 2010, from http://www.rfidjournal.com/article/articlereview/1415/1/39.

Kfir, Z., & Wool, A. (2005). Picking virtual pockets using relay attacks on contact-less Smartcard systems. Paper presented at the First International Conference on Security and Privacy for Emerging Areas in Communications Networks, Washington DC.

Langheinrich, M. (2007). RFID and privacy. In M. Petkovic & W. Jonker (Eds.), Security, Privacy, and Trust in Modern Data Management (pp. 433–450). Heidelberg: Springer.

Lettice, J. (2006). Face and Fingerprints Swiped in Dutch Biometric Passport Crack. Retrieved February 17, 2010, from http://www.theregister.co.uk/2006/01/30/dutch_biometric_passport_crack/

London School of Economics and Political Science (2005). The Identity Project: An assessment of the UK Identity Cards Bill and its implications. London: The Department of Information Systems.

Murdoch, S. J., Drimer, S., Anderson, R., & Bond, M. (2010). Chip and PIN is broken: To appear at the 2010 IEEE Symposium on Security and Privacy (draft). Retrieved May 13, 2010, from http://www-test.cl.cam.ac.uk/~sjm217/papers/oakland10chipbroken.pdf

Nohl, K. (2010). Mifare Security. Retrieved February 17, 2010, from http://www.cs.virginia.edu/~kn5f/

Nolan, R. (2009). Paperless public transport a smarter way to go. Retrieved February 18, 2010, from http://statements.cabinet.qld.gov.au/MMS/StatementDisplaySingle.aspx?id=66877

Ortiz, S. (2006). How secure is RFID? IEEE Computer, 39(7), 17-19.

Palmer, D., Warren, I., & Miller, P. (2009). ID scanners in night-time economy: Social sorting or social order? Paper presented at the Australian and New Zealand Society of Criminology Conference.

Privacy Committee of New South Wales (1995). Smart Cards: Big Brother’s Little Helpers. Sydney: Privacy Committee of New South Wales.

Rankl, W., & Effing, W. (2004). Smart Card Handbook. Chichester: John Wiley & Sons, Ltd.

Richards, K. (2009). The Australian Assessment of Computer User Security: A National Survey. Canberra: Australian Institute of Criminology.

Rotter, P. (2008). A framework for assessing RFID system security and privacy risks. IEEE Pervasive Computing, 7(2), 70-77.

Smith, R. G. (1999). Identity-related economic crime: Risks and countermeasures. Trends & Issues in Crime and Criminal Justice, 129, 1-6.

Smith, R. G. (2006). Identification systems: A risk assessment framework. Trends & Issues in Crime and Criminal Justice, 324, 1-6.

About the Author

Alice Hutchings graduated from Griffith University in 2007 with a Bachelor of Arts in Criminology and Criminal Justice with First Class Honours. Alice commenced her PhD, titled Theory and Crime: Does it Compute? In early 2008.   This research consists of testing existing sociological theories of crime to determine whether they explain computer crimes that compromise data and financial security. Alice aims to establish a new theoretical modal that incorporates the initiation, maintenance and desistance from these types of crime.

All papers in this series are subject to expert peer review.

General Editor of this series: Professor Simon Bronitt, Director, ARC Centre of Excellence in Policing and Security.

For a complete list and the full text of the papers in this series, please visit www.ceps.edu.au.

ARC Centre of Excellence in Policing and Security

M10_3.01
Mt Gravatt Campus
170 Kessels Road
NATHAN QLD 4122
Ph: 07 3735 6903
Fax: 07 3735 1033