International Journal of Computing Science and Information Technology, 2013, Vol.1 (02) 44 - 48
ISSN: 2278-9669, April 2013 (http://ijcsit.org)

National ID Cards

Yazeed ALKHURAYYIF
Computer Science & Info System. Dept., Shaqra University, Al Quwayiyah, Saudi Arabia.
yalkhurayyif@su.edu.sa

Abstract

The September 11 terrorist attacks changed the world, governments and many people became more and more concerned about their security. A number of countries have considered or are considering again their approach to a form of ID card. Despite the support for ID cards, there are growing fears about the possible loss of privacy, freedom, and that the new technology could increase police power more than it should be. The main idea of this paper is to look at the main advantages and disadvantages of National ID cards, security properties of resident ID cards, possible threat and security features. Moreover, a number of alternative proposes to the National ID cards is mentioned.

Keywords: National ID card, Smart ID card, identity card, Resident ID cards, Security

1. Introduction

The National ID card is one of official cards which can prove who you are, and can also show unique human identities. Many countries, such as Saudi Arabia and Germany, force their citizens to carry their identity card with them all the time, in while; a number of counties, for example Austria and Finland use the resident identity card as one options that can be used as proof of identity. On the other hand, numerous of countries do not have a National identity card, for instance the United Kingdom and the United states. The September 11 terrorist attacks changed the world, governments and many people became more and more concerned about their security. A number of countries have considered or are considering again their approach to a form of ID card. Since the 9-11 attacks the majority of national polls showed that approximately two-thirds of the American public were in favour of a U.S National identity card (Harrow, 2001). However, despite the support for ID cards, there are growing fears about the possible loss of privacy, freedom, and that the new technology could increase police power more than it should be. Civil liberty groups have warned that resident identity cards could appreciable simplify information sharing among government agencies and consequently increase police power significantly (Scheeres, 2001). The ID card issue is one that is discussed and debated regularly in the media. Governments reassure its citizens by introducing "smart" ID cards or upgrading existing identification cards with biometric smart ID cards which have many security features, but many people still question whether it is really an effective approach to tackle terrorism and improve national security.

This paper will be divided into four main sections. The first section will show the benefits and drawbacks of National identity card; subsequently, the security properties will be discussed; chapter three will analysis the possible threat and their results after that, mentioning the possible alternative of National ID cards and the enhancements of the existing identity cards and the last section will summarise what has been discussed.

2. Advantages and disadvantages

2.1. Advantages

New technologies introduce both positive and negative features and the National identity card is one of the contentious issues areas where opinion is divided. Hence it is not surprising that some countries have mandatory identity cards, some have voluntary identity cards whereas the rest do not have resident identity cards at all. The following are some of advantages of the National ID card:

- **Deal with illegal working and immigration:** identity cards can help tackle both these issues if ID cards are made compulsory for all citizens.
- **Combating crime and potential attacks by terrorists:** identification cards can eradicate the possibility of having more than one identity. Identity theft is restricted and associated activities such money-laundering is eradicated.
- **Enhancing access to public services:** resident identity cards are easy and convenient to use especially for people who do not have either a passport or a driving licence. (The House of Commons, 2004)
- **Gathering the information in one card:** identity

cards may contain an extensive amount of personal information including some of the following: bearer's name, photo(s), an identification number, ID's serial number, age, gender, address, telephone number, religion, profession, issuing agency, place of birth, signature, date of issue, blood group, parents name, citizenship and physical embedded characteristics. The "smart" ID cards, with embedded chips can also record fingerprints, medical data, iris measurements and driving records all of which can be linked to a central database (Krajewska, 2010). The information contained on the identity card can be useful so that in the event of a medical emergency, medical records can be scanned and searched on a national database and the appropriate action taken (Froomkin, 2004).

- **Prevent forged identity:** at elections a number of voters attempt to vote more than one, however, with ID cards this can be stopped (Gemalto, 2006).
- **More convenience:** Gulf Cooperation Council (GCC) citizens, for instance can travel in GCC counties with their identity cards and consequently, they do not have to carry their passports. In addition, resident identity cards give people a choice of which document to use in daily life. Another convenience feature of ID cards is that a person who does not have a driving licence or a passport can use it as proof of age when purchasing cigarettes for example.

2.2. Disadvantages

On the other hand, many people argue the disadvantages of identity cards:

- **Expensive to administer:** implementing an ID card system can be very expensive. According to James Hall, who heads the Identity and Passport Service, £257 million has been spent on developing the identity card scheme in United Kingdom prior it was abandoned.
- **Encroachment of privacy:** there are inherent dangers of storing the personal data of citizens in one single place and, as the UK government has observed, it is "poor security and poor privacy practice," comment by Jerry Fishenden, Microsoft Corp.'s national technology officer for the UK in an article for The *Scotsman* in 2005. By putting so much personal data in one place hackers are given a clear target to focus on. Furthermore, Simon Davies, who is director of the watchdog organization Privacy International, in London, and a visiting fellow at the LSE, mentions that if a government decides that the database saves information every time a citizen's identity is verified, then, a detailed trial of a person's activities could be accessed by anyone who has authority to access the system (Guizzo, 2006).
- **Increased threat for fraudsters to acquire people's identities:** all resident ID cards have a unique number. It would be an extremely trusted identifier and would be used widely by many organizations, hence, it would eventually be easier for fraudsters to obtain the information without permission (Guizzo, 2006).
- **Restricting the freedom and increasing monitoring:** in Germany for instance, people would be required to inform the authorities if they change their address or other circumstances.
- **Potential abuses of identification cards:** many people are worried about increasing the power of the police which might lead to abuse. A report from Elrick (2001) reveals that 90 Michigan police officers have abused their authorised use of the police database to stalk women, settle scores and threaten motorists (Elrick, 2001).

3. Security properties

"Smart" identity cards have great security features as listed below:

1. **Access control mechanisms (ACM):** an ID card contains the data of a cardholder; this data is shown as plain text. When the bearer of the National ID card and/or the service provider proves either the private key or the knowledge of a pin, then the data can be accessed by the card reader or the service provider. This method can protect the confidentiality of the holder against an attacker who attempts to eavesdrop for the purpose of accessing the data.
2. **Domain-specific unique identify (UID):** this feature averts combing databases by employing verity identifiers in different application domains. By employing this approach the person's data cannot be misrepresented.
3. **Selective Disclosure:** in order to respect the privacy and authorization principles, only specific information should be disclosed when a cardholder's information is accessed. For example if a banker would like to check the customer's address, the card reader should retrieves just the address of the customer.
4. **Verify-only mode:** employing verify-only mode method makes the data in an identity card more secure. The identification cards should have a query engine that runs in opposition to the ID cards' data or authorize the card to return just selected fields and match it within a certain data range. Take the case of bank checking the age of customer. Questioning the customer is whether above 10 years old or not, the identity cards just respond with a yes or no answer rather than revealing the user's date of birth.
5. **Biometric templates:** this approach is an effective

technique to reduce the amount of risk that comes from theft or loss of identification cards. In this method a biometric template is stored on the card which can access the biometric data stored on a central database. This means that no actual information is stored on the card and therefore it gives a high level of protection to the CIA triad (Confidentiality, Integrity, Availability). (Naumann and Hogben, 2009)

6. **Availability:** The biometric smart ID cards have more availability than their precursors. When an identification card is connected to the main computer database, the card can be accessed and retrieved easily (Lyon and David, 2004).

4. Threat analysis

As with many new technologies, ID cards have a number of weaknesses which need to be considered. However, identity cards have more concerned and intention because if the National ID card obtained an attack that will affect all citizens and locate the issuing government in embarrassing situation. The following are some of the National identity card's vulnerability:

- **Human error:** a number of experts say human error is the biggest threat to e-ID card schemes vulnerability. The potential threat can appear at any moment where the scheme of identification card is interacted. It is a big challenge to ensure that all personal's information is entered correctly, furthermore; there has to be a tool in the system that allows the modification of database entries when a user of the identity card changes their address or other information. Installing incorrect cardholder's data at any stage of the enrolment process is likely to create many problems of the bearer of the ID card. According to press story in the Guardian newspaper, a foreign woman could not travel for more than a month because she received incorrect information on her identity card which enforced her to send her ID card and passport to the responsible institution (UK Borders Agency) to solve the problem (Poty, 2009). Human error may inadvertently restrict the freedom of an individual, cause distress and might breach information security. It can also cause delay in issuing ID cards and waste government money (Siddhartha Arora, 2008).
- **Forged identity and counterfeit cards:** the traditional ID card, which is still being used in a number of counties, is easier clone than the "smart" National identity card. A threat may come from the lack of security features or conventional materials on the ID cards which do not match the requirement of accredited security printers. The fake identity card can be misused by teenagers to purchase alcohol, cigarettes or any unauthorized products, or even by terrorist to enter a country illegally.
- **Falsification of content:** an attacker exploits the vulnerability of the electronic ID card's system to change the citizens' data. The consequences are various and depend upon an attacker's motives, for example it could be used to take revenge on a particular person.
- **Man in the middle attacks:** As a result of lack of National ID card system security, an attacker might intercept communication between the identity card and server. The attacker stands between the two victims (see **Figure1** below) and then they able to access the sensitive data of a card holder.

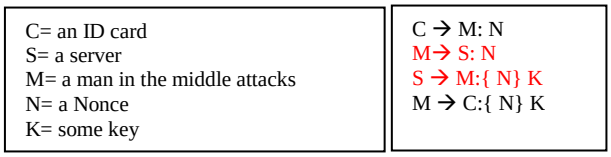

Figure 1. Example of Man in the middle attacks

- **Skimming attacks:** the threat comes from creating a clandestine connection to the ID card in order to obtain data. An attacker can use a hidden, small machine like a reading device which is able to skim the information from "smart" identity cards and misuse the information. (Naumann and Hogben)
- **Centralization of database storing:** in spite of giving hackers an obvious target to concentrate on by storing citizens' data in one place, hackers are intelligent enough to discover the weak aspects of their victim(s) before they attack. Hackers can observe the data for illicit purposes or to corrupt the identity card system.
- **Abuse by authorised personal:** people are already concerned about misuse of their information by criminals. However, a greater, threat is if such misused comes from authorised people such as the police or employers who deal with the citizens' database. They might use this information to stalk, threaten people, take revenge or settle scores.
- **Decrypting the data:** there is a small possibility of decrypting the biometric card's data when a secret key is known. For instance, hackers can interfere with the data stored on chips and also monitor data flows using probing pins. This enables them to steal private keys and to access private data (Naumann and Hogben).
- **Theft or loss the ID cards:** if the identity card has been stolen or lost it put a lot of pressure on both the government and bearer especially in the case of tradi-

tional ID cards which have more information on them than "smart" ID Cards. For example, the traditional Saudis identity cards used to contain sensitive information such as the card holders' full name, an identification number, address and the telephone number, but such information is now hidden in the new biometric ID cards.

5. Potential alternatives and enhancements

Due to the traditional ID card's vulnerability, it should no longer be used in any country in the world. In addition, any government that uses the biometric resident identity card or is planning to use one, should take into account the physical security requirements as a matter of priority.

National identity card should have visible and invisible digital watermarking with embedded text information. For example the card holder's picture(s) or the government's logo, Laser engraving should be utilised to protect optical personalization and also use of kinematic structure is advised which changes the images while adjusting the viewer's angle. Contrast reversal when the card is tilted, OVI (Optically Variable Inks); which is an effective technique against colour-copied counterfeits, MLI (Multiple Laser Image): which is for anti-counterfeiting measurements, Microlettering; which is a security feature that make plain text only viewable by magnifying glass. Furthermore, ID cards should be laminated multilayer cards and made of Polyester material in order to give the ID card a life cycle of around 10 years. Moreover, employing the more obvious security properties mentioned earlier in this report {ACM, UID, selective disclosure, verify-only mode, Biometric templates} should be established as a matter of course.

An alternative to identity cards proposed by the UK Biometrics Ltd was that a citizen's data should be saved on small smart card chips on the individual's credit card. This would eradicate the need for a centralised database of resident ID cards. This alternative has solved the fraud problem associated with the sharing of personal data between parties. Furthermore, the encrypted data which is stored in a chip cannot be reproduced (Marshall, 2007). However, this suggestion did not obtain much support and the UK Biometrics Ltd did not present the finer details of the proposal. Other alternatives; which already exist and are used in a number of counties, are drivers' licenses and passports. Both drivers' licenses and passport can show unique human identities and prove who you are, and act as functional equivalents of national ID card in the United Kingdom. Passports can perform most of identity card duties. For instance, it can be used to prove a person's identity which is one of the priority purposes of introducing the National ID cards. In addition, the passport has better security and economic features. Passports do not store citizen's information on them or on a government's database eliminates the fear of encroachment of privacy, freedom or abuse of the individual's information. Moreover, it will have financial benefits by saving on the introduction and use of National ID cards.

6. Conclusion

This piece of research has investigated the main benefits and drawbacks of the National identity cards, the most obvious security properties of resident ID cards, and then analysed the possible threats that may arise from the introduction of identity cards. It has also highlighted some security features that should be implemented in any National identification card scheme and some alternative proposes to the ID cards.

It is questionable whether the introduction of a National ID card scheme is an effective way to tackle terrorism and improve national security. There are also serious considerations with regard to data security and civil liberties which need to be taken into account. However, a number of countries have been using identity cards for many years and also ID cards are continually being developed to make them more secure.

Taking all things into account and from what it have been examined, the passport is a suitable document to prove identity and is also sufficient for maintaining National and international security.

REFERENCES

[1] Elrick, M. (2001) Cops Tap Database to Harass, Intimidate. sweetliberty organization Retrieved January 13, 2011, from World Wide Web http://www.sweetliberty.org/issues/privacy/lein1.htm

[2] Froomkin, MA. (2004) The Uneasy Case for National ID Cards. USA

[3] Gemalto (2006) Identity solutions for the public sector. Retrieved January 13, 2011, from World Wide Web www.gemalto.com/brochures/download/**identity**.pdf

[4] Guizzo, E.; , "Britain's identity crisis [biometric ID cards]," Spectrum, IEEE , vol.43, no.1, pp. 42- 43, Jan. 2006. doi: 10.1109/MSPEC.2006.1572352 URL:http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1572352&isnumber=33265

[5] Guizzo, E. (2006) Loser britain's identity crisis. IEEE organization. Retrieved January 13, 2011, from World Wide Web http://spectrum.ieee.org/computing/software/loser-britains-identity-crisis

[6] Lyon and David. "Identity cards: social sorting by database," Oxford Internet Institute, Internet Issue Brief No. 3, November 2004 as cited in Krajewska, M. (2010) The Politics and History of National Identification Docu-

ments: The United Kingdom and the United States in Comparative Perspective. British politics group. Retrieved January 13, 2011, from World Wide Web www.british**politics**group.org/**documents**/BPG2010-Krajewska_000.pdf

[7] Marshall, R. (2007) Alternatives to ID cards put forward. Computing. Retrieved January 13, 2011, from World WideWeb http://www.computing.co.uk/ctg/news /1859967/alternatives-id-cards-forward

[8] Naumann, I. and Hogben,G. (2009) Privacy Features of European eID Card Specifications. The European Network and information Security Agency (ENISA). Retrieved January 13, 2011, from World Wide Web http://www.enisa.europa.eu/act/it/eid/eid-cards-en

[9] O' Harrow, R. Jr. and Krim, J., (2001) "National ID Card Gaining Support," Washington Post, December 17, 2001, p A01.

[10] Porter, H (2009) The horror of the ID card system. Guardian Newspaper. Retrieved January 13, 2011, from World Wide Web http://www.guardian.co.uk/commentisfree/2009/feb/04/idcards-biometrics

[11] Scheeres, J. (2001) ID cards Are de Rigueur Worldwide, Wired News. Retrieved September, 25, 2001, from World Wide Web http://www.wired.com. Ac cited in Starr Roxanne Hiltz, Hyo-Joo Han, and Vladimir Briller. 2003. Public Attitudes towards a National Identity "Smart Card: " Privacy and Security Concerns. In Proceedings of the 36th Annual Hawaii International Conference on System Sciences (HICSS'03) - Track 5 - Volume 5 (HICSS '03), Vol. 5. IEEE Computer Society, Washington, DC, USA, 139.1-.

[12] Siddhartha Arora. 2008. National e-ID card schemes: A European overview. Inf. Secur. Tech. Rep. 13, 2 (May 2008), 46-53. DOI=10.1016/j.istr.2008.08.002 http://dx.doi.org/10.1016/j.istr.2008.08.002

[13] The House of Commons. (2004) Identity card. London: The Stationery Office Limited