

Flawed & Unnecessary: Governments Significantly Reduce Citizens Freedom to Prevent Acts of Terrorism

William M. Fitzgerald, *Telecommunications Software & Systems Group (TSSG), Waterford Institute Of Technology Ireland*

Abstract—In today’s society in particular after the events of September 11th World Trade Center attacks, citizens are been subjected to strict and sometimes unnecessary privacy infringements. Unfortunately due to a few bad apples in society all citizens must be monitored by government nanny state systems. This paper highlights the potential evasion of state-of-the-art identity management systems which are enforced on the law abiding citizen.

Index Terms—Privacy, European Citizen Security, Security. Sensor networks, Biometrics, Smart Cards

I. INTRODUCTION

DEFENDING the global society against terrorists, promoting economic growth, and protecting constitutional liberties are all prerequisites for a sound global security strategy. Everyday, new mechanisms are put in place to protect the many due to the malicious intention of the few.

More and more civil rights of the normal citizen are eroded away in order to reduce malicious societal behavior of a minority of citizens. But are these mechanisms working? Are these mechanisms beneficial to the normal citizen or are they beneficial to government and commercial fat cats?

Throughout this paper the author describes hypothetically how the criminal masterminds of our society can bypass the security mechanisms bestowed upon everyday citizens. Two hypothetical case studies are presented to show how citizens will always be vulnerable to the determined bad apples of society. Both criminal mastermind and terrorist are used interchangeably throughout this paper.

Note this paper purposely takes a one sided view that the privacy rights of the citizen are being eroded with no concrete justification. A future paper will discuss issues that try to justify citizen privacy erosion for the better good of man kind. It is important to get a balanced and accurate view of both sides of the coin.

Manuscript written 03 March, 2005. “*Flawed & Unnecessary: Governments Significantly Reduce Citizens Freedom To Prevent Acts Of Terrorism*”

William M. Fitzgerald is with the Telecommunications Software & Systems Group, at Waterford Institute of Technology, Ireland (phone: 00353 51 302937; fax: 00353 51 302901; e-mail: wfitzgerald@tssg.org).

II. IDENTIFYING THE TERRORIST, PROTECTING THE CITIZEN?

By developing the Holy Grail citizen identity, it is envisioned that because every citizen can be accounted for, crime will be minimised and in some cases prevented. This section describes some of the measures put in place to identify citizens and how these measures can be rendered useless.

A. ID cards

National ID cards have long been advocated as a means to enhance national security, unmask potential terrorists, and guard against illegal immigrants. They are currently in use in many countries around the world including most European countries, US, Hong Kong, Malaysia, Singapore and Thailand.

ID Card Vulnerabilities:

Identification cards will never work in the world of today for a number of reasons [2]:

- **Names Change:** Most women on entering marriage choose to take their partners surname. It's common for Arab men, for example, to change their names on the arrival of their first son. In Germany you can change your ID number by losing your ID card as the number attaches to documents rather than the individual.
- **Identity Theft:** The ideal ID system reports theft immediately and universally. However this is not always the case and was quite evident when one of the World Trade Organisation (WTO) hijackers used a passport previously stolen from a Saudi Arabian National in America five years earlier. Hence if a United States (US) airline cannot detect a theft reported in its own country, how probable is a streamlined international system going to be?
- **Staff Integrity:** Thousands of staff are employed in airports with minimal screening. A national ID card system would face similar problems.
- **Unknown Terrorists:** England's experience shows that for major operations the Irish Republican Army (IRA) use individuals unknown to police and other government agencies.

- **Forged ID Cards:** International terrorists can forge ID cards as well as passports, which is already a lucrative international trade.
- **Danger of Complacency:** ID cards can produce a false sense of security. Relying on them at the expense of other identity checks could mean crimes become easier to commit.

B. Biometrics

Biometrics refers to the field of technology devoted to identification of individuals using biological traits, such as those based on retinal or iris scanning, fingerprints, voice, face recognition or DNA.

A biometric portrays characteristic mathematical data that is exclusive to an individual. The claimed advantage of using biometrics is that it doesn't change and it goes everywhere with you. It is also supposed to be very difficult to forge or fake. Biometrics provides a very strong access control security solution covering authentication, confidentiality, integrity and non-repudiation.

I will discuss biometric vulnerabilities but even with its vulnerabilities, biometrics does provide a means to present security credentials that are unique.

Biometric Vulnerabilities:

Authentication based biometric systems have to be designed to cater for day-to-day alterations of biometric data, for example a scratch on an individual's fingerprint, facial changes with age, stubble, suntans etc. A margin of error is necessary so that variations of an individual's biometric does not cause an authorised user to be rejected because the offered biometric does not match the stored mathematical version [1].

From a criminal mastermind's point of view, there are four categories in which a biometric system can be compromised:

1. **System Circumvention:** Avoid using the system as intended using an administrator backdoor.
2. **Fraud Verification:** Attempts to circumvent the system during the verification process. A criminal mastermind or terrorist (both used interchangeably in this paper) could forcefully make an individual verify his/her identity. Or use the chopped limbs of that authenticatable user (e.g. use a finger or eyeball). In fact blood does not have to be drawn! A Swedish Engineering student succeed in copying fingerprints and put the fingerprints onto her own finger to trick commercial fingerprint readers [3].

Method:

- Locate and discover a fingerprint on a surface.
- Then sprinkle on the fingerprint coal dust to make it clearer.
- Next photograph it with a digital camera.
- Perform some image-processing to improve the fingerprint.

- Printed the corresponding film negative of it.
- The negative can be used to expose a normal photosensitive Printed Circuit Board (PCB) to transfer the fingerprint to the PCB
- Then place gelatin (similar texture to human skin) on the PCB fingerprint to transfer it to the gelatin.

3. **Fraud of Enrolment:** where by a system is needed to verify that a person is who they say they are.
4. **Network Eavesdropping:** this can often be overlooked. Biometric data need not be local to the device reading the data and can be stored remotely in a central or distributed location. Therefore the security of the biometric authentication relies on the strength of the network architecture too. Most attacks of this nature will be Man-In-the-Middle attacks utilising replay attack methods.

C. Smart Cards

A smart card can be viewed as a credit card sized plastic card embedded with an integrated circuit chip. It provides not only memory capacity, but computational capability as well.

The self-containment of smart card is supposed to make it resistant to attack, as it does not need to depend upon potentially vulnerable external resources. Because of this characteristic, smart cards are often used in different applications that require strong security protection and authentication.

The smart card can be used as an identification card that is used to prove the identity of the cardholder. It also can be a medical card that stores the medical history of a person. Furthermore, the smart card can be used as a credit/debit bankcard that allows off-line transactions.

All of these applications require sensitive data to be stored in the card, such as biometric information of the card owner, personal medical history, and cryptographic keys for authentication, etc.

Smart Card Vulnerabilities:

Smart cards can provide encryption and decryption of data for the card and some smart cards can even be used to generate cryptographic keys. The secret of the cryptographic algorithm, the keys stored, and the access control inside the smart card becomes the target of the criminally minded cracker.

Two common types of attacks on smart cards are [4]:

1. **Logical Attack:** the key material of a smart card is stored in the electrically erasable programmable read only memory (EEPROM), and due to the fact that EEPROM write operations can be affected by unusual voltages and temperatures, information can be trapped by raising or dropping the supplied

voltage to the micro controller.

2. **Physical Attacks:** At a Cavendish laboratory in Cambridge, a technique exists for reverse engineering the circuit chips. The layout and function of the chip can be identified using that technique. Then another technique developed by IBM can be used to observe the operation of the chip. As a result its secret can be fully revealed. Besides this, there are many different ways to perform physical attacks. For instance, erasing the security lock by focusing UV light on the EPROM, probing the operation of the circuit by using micro probing needles, or using laser cutter microscopes to explore the chip, and so on.

III. PRIVACY

Europe and the world will have to address its citizen's privacy issues and will need to weigh up the pros-and-cons for whatever privacy action it takes. Citizens are concerned about knowingly and unknowingly being monitored. Citizens are currently being monitored by the latest in technological advancements such as:

- Mobile Location Services.
- Internet Surfing (cookies, hackers, government national security etc).
- Identity Cards (described earlier).
- Citizens having to give biometric details at work or for government reasons.
- Subjected to video surveillance and so forth.

Given this knowledge the author suspects that citizens are opposed to these measures and predicts citizens taking a stance on this very issue in the near future. It is an infringement of civil rights to be constantly monitored and having to verify who we are for the sake of a few bad apples in society.

If biometrics is to become mandatory in Europe and the rest of the world, there needs to be strict international guidelines as to how biometric data will be recorded and stored. The guidelines would have to state when and where biometrics could be used and so forth. As a citizen, the author personally would be concerned about his biometric detail ending up in the wrong hands for illegal purposes.

IV. CASE STUDY 1: HYPOTHETICALLY STEALING HIGHLY CLASSIFIED DATA AND MATERIALS IN THE FACE OF CURRENT SECURITY MEASURE

This case study sets about describing a hypothetical robbery of state of the art security facility.

A. *Setting The Scene*

Imagine a top-secret research chemical plant called "ChemWarfare" is housing a deadly biological warfare chemical.

A terrorist (Mr. Threat) wants to get his hands on that

chemical in order to do the act of terrorism. Lets assume that Mr. Threat has an insider (Mr. Insider) helping him (but does not necessarily need one). In order for Mr. Threat to get the chemical he must assemble a team to carry out various tasks.

B. *Initial Steps*

Mr. Threat sets about short-listing potential candidates to do his bidding due to financial gain, politics, trust, personal values, religious values, anger at current employee management etc. Having found Mr. Insider(s), Mr. Threat requires information relating to:

- Security systems in operation (staff and technological).
- What is ChemWarfare's security plan?
- What is ChemWarfare's evacuation plan?
- Security equipment maps and whereabouts
- And so forth.

C. *Surveillance*

Mr. Threat would assemble a surveillance team to gather as much information as possible. Information from satellite photos [5, 6], employee and security guards rota's, habits etc.

D. *Physical Break-In*

In order to bypass the security guards uniforms and identification cards have be acquired and duplicated.

At the perimeter door a swipe card is required. Luckily Mr. Insider has stolen one and the card has not yet been reported stolen. *Note:* Mr. Threat's Physical Break-In team were aware of other measures to bypass the smart card reader if needed.

In the main foyer and throughout the corridors of ChemWarfare are biometric face recognition readers. The Physical Break-In team use digital photos of authenticated users hung in front of their faces to bypass the simple 2-D face recognition readers. *Note:* the Physical Break-In team could have undergone plastic surgery if the facial recognition systems were more sophisticated but Mr. Insider assures Mr. Threat that the system is based on 2-D imaging.

The Physical Break-In team have acquired fake fingerprints from coffee cups in the canteen prior to the actual break in. They have to produce their (false) fingerprints on entry into the secure corridor that leads to the research laboratory. *Note:* the Physical Break-In team could have kidnapped an employee with the required security clearance and chopped off his/her fingers!

To enter the restricted research laboratory the team must provide an eye for the installed iris reader. They gain entry with a state-of-the-art fake eye of a security-cleared employee who was drugged one night in a bar and remembers nothing of that night and how his biometric eye detail was copied.

After the Physical security team enters the laboratory, they head straight for the heavy-duty steel safety box housing the bio hazardous chemical. The have to enter a PIN to get access. Most manufactures have a master code for each of its products for use by security professionals. Armed with this and observing worn digits on the number panel they gain access.

Failing this they have been equipped with hydraulic guns to pries open the door. Voila, Mr. Threat has his weapon!!!

An emergency exit was also incorporated into the plan in case of mishaps. If an alarm was triggered in the event that the Physical Break-In has been noticed, they know that ChemWarfare uses Halon gas to quench fires and not water. So they set about triggering a fire alarm. In doing so they cause panic amongst the employees and cause random movements of people in a flurry to get out of the building. Thus making it harder for the security guards to track them down. Not only that, the Physical Break-In team know that because Halon is a dangerous gas most security systems release the locks on emergency door!! And again, voila Mr. Threat has his weapon!!!

Note: this case study was just a hypothetical story of what could happen and what is very plausible given the huge vulnerabilities in the current state-of-art security systems.

V. CASE STUDY 2: POTENTIALLY CRIPPLING FUTURE SENSOR BASED TECHNOLOGY SYSTEMS AIMED AT PROTECTING THE CITIZEN IN PUBLIC AND PRIVATE SPACES

The security of public areas like harbours, airports, stations, big buildings, hospitals and research centers etc is considered today's future challenge. Despite the advances in sensor-based systems and control rooms, in particular video surveillance, current systems do not provide the situation assessment required to master the complexity of the space and the behavior of citizens within those spaces in order to prevent risks and to increase security with more accurate situation awareness.

It is the aim of global research bodies such as the European Security Research Programme (ESRP) or the Preparatory Action for Security Research (PASR) to enhance security of sensor-based networks to provide reliable and confident security levels for its citizens.

For example, future research aims to develop an improved access control and video surveillance service in order to enhance the safety and security level in such areas that will be characterised by the following sub-area types:

1. **Full Public Areas:** accessed by every citizen. The system will have to monitor the activity of the citizens within these areas.
2. **Private Areas:** accessed with a badge or equivalent method. The system has to authenticate the users.
3. **Restricted Area:** accessed through biometrics authentication.

Case Study 1, showed how a plausible plan could be put together in order to render Steps 2 and 3 just described as useless. All that is needed are a couple of body limbs, digital photos, smart card fraud and a few other bits and bobs. It will be a long time before Steps 2 and 3 will be cheat proof, if ever!

Lets focus on Step 1, *Full Public Areas*, whereby future research aims at protecting citizens in open spaces such as parks and airports. Some researchers are researching and

developing social behavior models related to individual or groups of individuals, specified as ontology's for automatic reasoning about "normal" or "abnormal" behavior classification for people in large public areas. Recent research focuses on ontology based surveillance systems but unfortunately, in the author's opinion, this method has a number of vulnerabilities. Let's go through a couple of scenarios of how it should work.

A. Scenario 1

Imagine a public park full of children playing and parents chatting. It's a hot summers afternoon and all is well. Suddenly a man in a long grey coat is spotted on the futuristic state-of-art video surveillance system as being suspicious.

Why is he suspicious? He has been noticed by the ontology and automated reasoning based surveillance system as wearing a dark pair of glasses and a long coat on a hot summer's day. Furthermore the surveillance system shows him to be carrying a black sports bag that seems rather heavy as it lies across his shoulder. The suspicious man also seems to be looking over his shoulder repeatedly and is looking rather erratic. The man sits down on a park bench and drops his bag beside him. A young child kicks a ball towards him by accident and the suspicious man leaves his seat to avoid been hit by the ball. The man then walks towards the ball (leaving his bag behind) so he can kick it back to the child. Suddenly he is ambushed by security guards and wrestled to the ground. The park is evacuated and a bomb squad is already waiting to defuse the potential bomb.

The problem is that, the surveillance system saw the man as a threat but in fact the man has a rare skin condition that reacts to sunlight (hence the reason why he is covered up), his bag was full of college books and he was not leaving the scene of the crime but in fact retrieving the child's ball!

B. Scenario 2

Again, it's a nice summer's day at the park and all seems well. A suicidal young couple carrying a picnic basket full of bio chemicals enters the park. The young couple proceed to sit down in front of the duck pond. They intend to release the deadly chemical into the atmosphere killing all in the park and surrounding city. The couple intend to die in the process for their perceived cause (maybe they believe a space ship will come and save them!!). The surveillance system did not notice anything erratic about the so called normal couple and so citizens died that day.

How could this have happened? Well, the ontology and automated reasoning surveillance system did not see anything suspicious as there wasn't anything odd going on. The suicidal couple wore the correct clothing for the given day, they were carrying a picnic basket as one would expect (a romantic afternoon out), and they didn't act in an erratic manner.

So to conclude, these future surveillance systems will inevitably be flawed and may never provide the real security

citizens need to live happily in society. In some cases there will be too many false alarms as shown on scenario 1 and in other cases no warnings at all as shown in scenario 2.

VI. CONCLUSION

This paper presented at an abstract level some of the vulnerabilities in the current and future citizen security protecting systems. What seems to be a plausible solution for protecting the citizen from harm can in fact provide a false sense of security and seriously reduce a citizen's right to privacy within society. The criminal mastermind is always one step ahead and until we can think like one, we don't stand a chance at leveling the playing field.

The author is not trying to halt current and future security mechanisms to protect the innocent, as we do need them to deter smaller societal crimes and so forth, but is rather advising not to use such severity with ID based systems. The question is do we really need to limit a citizen's privacy in order to achieve overall citizen security? It doesn't seem to provide a full proof protection system!

To conclude, further research is required in designing efficient, safe and less intrusive security systems that take into account the citizens privacy concerns.

The main aim of the author is to point out, that we need to change our perception of how to protect the innocent and to try stimulate researchers to develop other potentially equal solutions in the same problem space.

REFERENCES

- [1] ETSI, "Response from CEN and ETSI to the Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of Regions: Network and Information Security: proposal for a European policy Approach", ESTI SR 002 298 version 1.1.1, 2003.
- [2] Anderson Ross, "Commonsense in the Crisis", Cambridge University
- [3] http://www.nyteknik.se/skrivUt.asp?art_id=37392
- [4] Anderson Ross & Kuhn Markus, "Tamper Resistance - A Cautionary Note", Cambridge University, 1996.
- [5] <http://www.digitalglobe.com/>
- [6] <http://www.spaceimaging.com/>
- [7]

Malware (Virology, RAT's, Worms, Phyogenetic's). Prior to his current employment he was employed as an applied security researcher with Ericsson's Systems Expertise Group, Dublin, Ireland. There he researched security of Ad-Hoc networks, reputation based metrics and novel game theoretic approaches to network node cooperation.

Some of William's publications: (1) *An Approach for Network Forwarding Systems Quality*, Information Technology and Telecommunications (IT& T), Athlone, Ireland, pp 103 -111, ISSN 1649 - 1246, 2001, (2) *Performance Analysis of Host Based Routing*, Masters of Science, N.U.I. Maynooth Library, 2002, (3) *Ericsson OSS Security Architecture: Current State and Challenges Ahead*, Ericsson R&D Ireland, 2003, (4) *Reputation and Cooperation in Ad Hoc Networks*, Ericsson R&D Ireland, Ericsson R&D Ireland, 2003, (5) *Constructing a Wireless Intrusion Detection System with Snort, MySQL, Apache, PHP, ACID & BASE on a Linux Platform*. Visit www.williamfitzgerald.org



William M. Fitzgerald (MSc, BSc) obtained a Master of Science Degree in Computer Science from National University of Ireland Maynooth (N.U.I.M) in Maynooth in 2002 and an Honors Bachelor of Science degree (majoring in Computer Science & Mathematics) also from N.U.I.M in 2000.

He is currently employed as an applied researcher for the Telecommunications Software & Systems Group (TSSG) at the Waterford Institute of Technology in Waterford, Ireland. William is focused on the security arena within European projects such as SecurIST, Daidalos and the PASR initiative. His current research interests are security (wired & wireless)