Is it safe?

H. B. Wolfe
University of Otago, New Zealand

Abstract

In the 1976 movie *Marathon Man* the term "Is it Safe" is used to great effect. This presentation is about some of the many security measures that we implement and expect to protect us. Many are hyped as protecting us completely from a given threat. The simple facts do not support these assertions. This paper will ask the question "Is it Safe" and address and describe the many failures and/or limitations of various accepted security measures. For example, RFID has become the darling of many who would use this technology to "secure" whatever is to be protected. Several countries have implemented RFID within their passport systems. All have shown to be easily cloned from a distance. Those that have used encryption to protect information contained on the RFID have also been shown to have used weak encryption. Some of these have been broken within a few seconds to a few minutes.

Every day organizations decide to make use of some of the many security measures currently in the market place assuming that they will be safe as a result. It is not apparent that they are aware of the failings and limitations of many of these measures and techniques. This paper will discuss and describe several of these limited techniques, showing how each has been compromised. Thinking that you are safe when you are in fact not presents an important risk.

Keywords: data encryption, mobile phones, RFID, biometrics, compromise.

1 Introduction

There are many information assurance (computer security) measures that can be put in place to mitigate risk. Just about every vendor claims that their product or technique will provide safety. In some cases this is true, however, in many instances it is not. This paper is about some of these failed techniques. It is the author's intention to show the reader that it is prudent to be sceptical of vendors' claims and to clarify the fact that simply installing a security measure does not

WIT Transactions on the Built Environment, Vol 108, © 2009 WIT Press
www.witpress.com, ISSN 1743-3509 (on-line)
doi:10.2495/SAFE090361

ensure its proper use therefore does not necessarily ensure risk mitigation. There are many examples of good measures being circumvented by various actions and means. This paper will discuss several of these to illustrate these assertions.

2 Data encryption – cryptography

Cryptography is the art and science of codes and ciphers. This technique is used to protect data/information both in transit (communications) and at rest (residing on some medium). All encryption is not of equivalent strength; however, to the uninitiated it all looks the same. Cryptographic techniques are used to translate data/information from one state to the other: *plain text* – that which is readable and not protected and *cipher text* – that which is protected and not understandable without being decrypted.

The way in which data is translated from one state to the other is managed is by using an encryption/decryption algorithm. In today's world of computing, these algorithms make use of the level of difficulty it takes to solve one complex mathematical problem or another. Because of the speed of computing power this function can operate quickly enough to be almost transparent to the user. Encryption translates plain text into cipher text. Decryption translates cipher text into plain text.

One attribute (but not the **ONLY** attribute) of an algorithm's strength is described by the number of bits required for the key. For example a 128-bit key translates into sixteen characters. In order to derive a key of this length by brute force (testing every key in the entire key space) it would take 2^{128} tests. This is equivalent to the number 340 with 36 zeros after it (a number larger than that representing all of the atoms in the universe). To put that into easily understandable terms: If you had a computer CPU that could test 1,000 trillion keys per second [1] and you could array 1,000 trillion of these CPUs into a massively parallel machine, it would take that machine less than 10 minutes of computing time to derive the key. Assuming that the algorithm is not weak (another attribute – which must be proven [2]). However, there is currently only one machine currently capable of 1,000 teraflops (trillion floating point operations). If we put that machine to work on solving a 128-bit key by brute force, it would take 10,790,283,070,806 years of computing time. The American AES (**A**dvanced **E**ncryption **S**tandard) can encrypt/decrypt using a 128-bit, 192-bit, or 256-bit key length. Assuming no proven weaknesses exist, the latter two would make brute force attacks computationally infeasible.

Many applications have, as one of their features, data security which performs the task of encryption/decryption. For example Lotus Notes has this feature. Internet Explorer and Netscape also have this feature. Lotus Notes uses 64-bit encryption for its security feature. Internet Explorer and Netscape use 128-bit encryption for their security feature. In all three examples, a file secured by this feature contains a *work factor reduction* [3] field. This field contains in the case of Lotus – 24-bits of the actual key used to encrypt. In the case of the other two, the work factor reduction field contains 88-bits of the key used to encrypt. In all three examples the security provided is rendered to be only at the level of 40-bit

encryption (about 1.1 trillion keys in the key space). This is trivially decrypted with a standard laptop computer within minutes.

The interesting thing about this fact is that none of these vendors tell the public who buy the product about the deliberate weakening of the security promised by their products.

Another example involves a forensics tool (Password Recovery Tool Kit by Access Data). This tool routinely recovers the keys for files that have relied on the built in security features of Word, Excel, PKZIP (and more than forty others) to protect their data. Many free incarnations of the modules available in this suite of software are also available for download on the Internet.

The lesson to be learned from these examples is that you must be careful when using encryption. Privacy is a human right guaranteed in *Article 12* of the *Universal Declaration of Human Rights* [4]. Cryptography can provide each of us with the tools to enforce our privacy. You must take the time to find out what the actual level of security is for any product considered. That cannot be done by relying on the vendor and their marketing minions. Their primary objective is selling product where your primary objective is to protect your data and your privacy. These objectives are not necessarily compatible. The question you have to ask "Is It Safe?".

3 Mobile phones

Mobile phones have become ubiquitous over the last few years. Unfortunately, the security and privacy offered by them has not kept up with the many uses that these devices have been put to. In the 1990s it was proven that the cryptographic methods used by various service providers did not in fact offer strong protection to the privacy of subscribers. Encryption algorithms used by GSM for example were proven to be deliberately weakened. This paper will not delve into the reasons for deliberately weakening cell phone security. The point to be made here is that any conversation on a mobile phone can be intercepted and encryption provided by the service provider can be overcome in such a way that any conversation can be listened to and recorded. "Is It Safe?" The answer is no.

There are many different kinds of risks associated with mobile phone use. The first is the failure to protect conversations from determined interceptors. Since the communication is nothing more than a radio technology, every conversation can be intercepted. There is nothing to stop that. What remains is the privacy of the content. If strong encryption were used and forced on every communication this weakness could be avoided. However, encryption is left in the hands of the service provider. They choose the algorithm and they decide as a matter of course when encryption can be used and when it cannot. For example, communications between a mobile phone and one of the seven naughty countries automatically turns off the encryption feature. It has been shown that this fact can be exploited in a way (the man in the middle attack [5]) to turn off the encryption feature between users not in the naughty countries as well.

Wire taps are usually done at the base station. There is nothing to stop that except law. We all know that laws are broken and in the US this sort of tap is

even done by Government agencies as a matter of course – without any warrants. In today's world anyone can be a terrorist for any reason and that could be you. I personally do not have a mobile phone. So, once again you have to ask "Is It Safe?".

The next failure in the mobile phone arena is a design failure and deals with its use. These devices are not just used for phone type communications. They are used to communicate with the Internet. They are used to store very sensitive information like passwords, encryption keys, bank account details and account numbers, credit card details and account numbers and PIN numbers, network logon details – account and password. Most of the newer phones come with an enabling feature – Bluetooth. This allows the user to communicate wirelessly with their personal computer. On the surface this sounds like a convenient way to back up your contact lists and other information held on the mobile phone.

The risk lies in the situation where Bluetooth is left active after the download and backup procedures. At this point anyone with the appropriate gear (BlueSniper Rifle for example) could detect this condition, connect to the mobile phone, and download the entire contents of the mobile phone for their own use – and from a distance (up to a mile and perhaps beyond). In many jurisdictions it is not legal to do this; however, it is certainly possible to do it. So for the uninitiated user it is time to understand that this feature MUST be turned off when not in use.

Mobile phones can easily be tracked by service providers. As a service provider, it makes sense to do this. Network analysis requires this kind of information in order to recognize any specific cell overload. This may be an indicator that it is time to provide additional network capability – normal network analysis and a necessary operational process. However, the fact that your mobile phone is being continuously tracked may be of importance to some people. It definitely violates their privacy. The only way to avoid this privacy breach is to turn your mobile phone off and in some cases remove the battery as well. On a few phones, turning it off only puts into "sleep" mode and that can be reactivated externally.

At this point the reader is probably thinking "if you don't have anything to hide, then you won't have anything to worry about". This is a spurious argument. Why would anyone want their movements to be tracked and recorded? This is simply not about having anything to hide. This is purely about your human right to privacy, nothing more.

One last thought on mobile phones: it is possible on some mobile phones to call the phone without causing it to ring. This presents a very different risk. If you were in a high level negotiation over something valuable or important, if a mobile phone were able to be silently activated, then the opposition could make some excuse to leave the room (leaving a mobile phone there) and activate their phone from outside. If you and your colleagues took the opportunity to discuss the progress of negotiations, the opposition could listen in on those conversations. You can see how this "feature" could be used in this and in many other ways to put someone at a disadvantage. The notion that it might be illegal will not stop someone who is determined. You have to protect private

conversations where mobile phones might be present. Safe means without them present.

4 RFID

Radio Frequency Identification (RFID) is a technology that has been around for a long time. The Thing is a good example of how the technology works. A signal is sent and a reflected signal is returned. The Thing returned a modulated signal representing sound. A modern RFID device's signal returns information overlaid by the electronic device – a chip. Some of these devices merely return a unique chip identification number. Others have the ability to return more complex data.

Wal-Mart, the largest single retail purchaser of goods in the world has dictated to its top one hundred suppliers that their products will contain RFID as a part of the product labelling and identification. That probably means that this type of identification will become ubiquitous in the near future. This technology is also used in ID cards, proximity cards, passports, medicine and many other places. It is sound technology.

However, like all things, it can be used for good and for bad purposes. There is no legislation that requires retailers to remove, deactivate or destroy the RFID tag. This means that anyone with an RFID scanner can easily read any RFID tag from distance. If that identifies a product then the person using the scanner will know what product has been identified. If a passport is scanned from a distance, the fact will be unknown to the passport holder; however, the person scanning can store, for later analysis and use, all information that is returned from the scan. This makes it possible to clone passports and assume identities. It has been argued that passports have used data encryption to "protect" individuals. It has been demonstrated that those passports where data encryption has been used can be trivially decrypted [6].

RFID has been used in various transit schemes. For example: the Dutch OV Chipkaart, London's Oyster Card, Boston's Charlie Card, etc. These and others have all been cloned. In other words you can ride those transit systems for free if you know how and that information is freely available over the Internet.

RFID vendors would have us believe that these devices can only be read from a few centimetres. Remote reading has been demonstrated in 2005 by Kevin Mahaffey. He was able to scan an RFID from fifty (50) feet. In 2006 Harko Robroch demonstrated reading a passport form five (5) metres.

So, what's the risk? The risk is that everyone's privacy can be intruded upon with this technology. If tags are not destroyed or removed at purchase time then anyone with a scanner can find out what we have on our person from a distance. That might be very attractive for a mugger to know. It might also be very attractive from a marketing perspective. For example if you were walking through a mall shopping and you were scanned by a retailer and they found that you were wearing an old pair of shoes, they could then use this marketing intelligence to market to you directly, particularly if you carried an RFID identity card or RFID driver's license.

RFID technology is small enough to be included on individual currency notes and there is continuing consideration in various countries of the potential use of this technology. The information returned from a scan could be the denomination, the serial number and probably other bits of data as well. Of course if I were a mugger with a scanner I would be instantly, after scanning you, able to tell how much cash you were carrying and in what denominations. That would save a lot of time choosing which person to mug.

RFID tags can be destroyed by various means. However, legislation needs to be crafted that will require all vendors of product to remove RFID tags or destroy them in place. You might notice that I have not said deactivate. Just remember that if you can deactivate something then you may also be able to reactivate that same thing. If your country has inflicted RFID on you in the form a RFID passport, you might consider the purchase of a special insulated wallet. These make use of the principal of the Faraday cage. They allow no signal to get out and they prevent all signals from getting in – thus protecting your RFID passport form being scanned. Is It Safe? You decide.

5 Biometrics

In order to gain access to a structure (a building, secured spaces within a building), to a network (local or Internet), to a specific computer, or to be granted authorization to use sensitive data while connected to a computer and/or a network we must first authenticate who we are. There are three elements that can be used: *what we know* (a password, a PIN), *what we have* (a token), and *what we are* (biometrics). Biometrics in the context of this paper refers to electronic devices that can scan or evaluate some physical attribute of an individual. The attributes normally used are thought to be unique for each person.

Some of the attributes that are most commonly used for this purpose are: fingerprints, iris prints, hand configuration, and facial recognition. There are others, however, with the possible exception of retinal recognition, they are not as reliable as the attributes mentioned. Retinal recognition is intrusive and used in military and intelligence institutions because of the fact that they are accurate and difficult to trick and because they have a captive audience. The general public are thought not to be willing to be subjected to that kind of intrusive technique.

One of the most commonly used of these techniques is facial recognition. Every time we go through immigration at an airport, our face is being scanned and evaluated to see if there is a match to a known terrorist. This method of biometric identification has improved over the years but still raises false positives (when the individual is "recognized" as being someone who they are not). Still, it is being used effectively all over the world.

Fingerprints have been used in criminology since Sir Francis Galton wrote his book [7] in 1889. According to his calculations there was 1 chance in 64 billion that two people would have the same fingerprint. The basic idea is sound. In technology terms, however, in practice it is less sound. Tsutomu Matsumoto's

work [8] has demonstrated that most fingerprint readers can be defeated a large percent of the time.

Iris recognition has been similarly proven. Even identical twins do not have identical irises. The basis for using this biometric is also sound. Matsumoto once again through experimentation proved the current crop of iris readers to be fallible and defeated three of them.

There is certainly room for improvement in the biometric arena. The fact that the early versions of these biometric devices failed to perform as expected – to authenticate an individual beyond doubt does not mean that future incarnations of these tools will also fail to provide adequate reliability in authentication. However, you still need to ask "Is It Safe?"

6 JavaScript and its use

For techies, JavaScript is the best thing since sliced bread. They use the scripting language for many applications. However, Internet browsers that automatically execute these scripts provide an avenue for hijacking the user's session. That means that malicious code can be introduced into the computer and executed. It is of course possible to turn JavaScript off. This is recommended by CERT (Computer Emergency Response Team) in several of its alerts [9].

Recently it has been shown that Adobe's Acrobat Reader and Editor both are susceptible to a JavaScript attack [10]. This also can be turned off. We really shouldn't have to turn features off. If the application was properly written these threats wouldn't be possible. There are a number of these threats that we can control. We can turn off JavaScript, Java, ActiveX, Visual Basic, and Cookies. None of them are necessary for web pages to work effectively and efficiently.

When you connect to a web site that requires JavaScript or cookies you have to ask yourself: "Is It Safe?"

7 Audit

Photo ID badges are used as a matter of course in many institutions. On the surface these provide a security measure of varied effectiveness. If staff are trained to look and consider every ID card that they encounter, the measure can be very effective. However, when staff are not trained properly the cards provide no security at all.

A few years ago I performed an audit of a large utility business. They too had ID cards that everyone was required to wear. Upon signing the contract to do the audit, I was photographed and issued an official ID card. As a matter of course, part of an audit is observation. It provides unexpected opportunities to identify security risks. In this particular instance, I noticed that no one ever seemed to look at ID cards.

At home I created a new "official" ID card in the official format and replaced my photo with an image of Mickey Mouse. On the next visit I displayed that ID card instead of the one issued. The experiment produced interesting results. No

one noticed. Not a single employee of the utility ever stopped me or commented or in any other way acknowledged the Mickey Mouse badge substitution.

This was an interesting example of an otherwise good security measure that did not work. It was easily remedied by training.

8 Conclusions

This paper has discussed a few specific examples of various failed security measures. It has been written to inform and illuminate rather than criticise any single individual or organization. This has been done in the hope that the reader will be better informed as to information assurance matters.

We should all be sceptical. Do not rely on vendors for final advice. Remember their primary objective is to sell product. That comes before your security in their business plan. Consult the experts when you need specific advice about a particular security measure or product. They are not perfect; however, you will get the best advice available from them.

References

[1] *Roadrunner* (Los Alamos National Laboratory) is currently, the world's fastest computer operating at 1,000 teraflops (trillion floating-point operations per second). However, a key test is a Boolean operation consisting of many individual instructions. Moreover, the Teraflop machines reach the speeds published by massively arraying thousands of CPUs – in *Roadrunner's* case more than 6,000. We are many years away from creating a single teraflop CPU that can operate at 1,000 teraflops per second. See: www.lanl.gov/discover/roadrunner_fastest_computer

[2] Swenson, Christopher, *Modern Cryptanalysis: Techniques for Advanced Code Braking*, John Wiley & Sons, 2008, ISBN: 978-0470135938.

[3] Cryptographic algorithms can be attacked via various cryptanalytic techniques. Examples of cryptanalysis types: Differential, Linear, Integral, Statistical, Birthday, Man-in-the-Middle, Plain Text, and others. Solution is possible when an algorithm has been proven to be weak using one of these and/or other cryptanalytic techniques. When an algorithm cannot be successfully attacked by these methods it is thought to be strong. It can then only be successfully attacked by brute force – cycling through the entire key space until the correct key is found. See:

[4] European Parliament's Scientific and Technical Options Assessment, Luxembourg, April 1999, PE168.184/Part 4/4.

[5] Proclaimed and adopted by the General Assembly of the United Nations – 10 December 1948 – see – http://www.un.org/Overview/rights.html

[6] Work by Professor David Wagner at the University of California at Berkley – September 2000 – See: www.snapshield.com/www_problems/United_States/ Cell_phone.htm

[7] Copacobana is a special purpose which computer arrays a number of field programmable gate arrays (FPGA) to provide computing power.

Copacobana can decrypt the German passport in 22 seconds and the Dutch passport in 10.3 seconds. See www.copacabana.org

[8] Galton, Sir Francis, *Fingerprints*, MacMillan, New York, 1892, ISBN: 1-57588-742-8.

[9] Tsutomu Matsumoto, *Gummy Fingers*. See: www.ifca.net/Fingerprint-System-Security-Issues.pdf

[10] CERT – *Cyber Security Tips ST04-0012* and *ST05-001* – Both of these deal with JavaScript, Java, and ActiveX explaining what the risks are and how to mitigate them. See www.us-cert.gov/cas/tips/STo4-212.html and www.us-cert.gov/STo5-001.html

[11] CERT – *National Cyber Alert System – TA09-051A*. This alert describes the JavaScript vulnerability and offers a solution. See: www.us-cert.gov/cas/techalerts/TA09-051A.html