1-1-2010

Digital forensics and the issues of identity

Andrew Jones
Edith Cowan University

Thomas Martin
Khalifa University of Science Technology and Research, United Arab Emirates

10.1016/j.istr.2010.10.008
This is an Author's Accepted Manuscript of: Jones, A. , & Martin, T. (2010). Digital forensics and the issues of identity. Information Security Technical Report, 15(2), 67-71. Available here

AUTHOR QUERY FORM

ELSEVIER	**Journal:** ISTR **Article Number:** 2172	**Please e-mail or fax your responses and any corrections to:** **E-mail: corrections.eseo@elsevier.tnq.co.in** **Fax: +31 2048 52789**

Dear Author,

Please check your proof carefully and mark all corrections at the appropriate place in the proof (e.g., by using on-screen annotation in the PDF file) or compile them in a separate list.

For correction or revision of any artwork, please consult http://www.elsevier.com/artworkinstructions.

Any queries or remarks that have arisen during the processing of your manuscript are listed below and highlighted by flags in the proof.

Location in article	Query / Remark: click on the Q link to go Please insert your reply or correction at the corresponding line in the proof
Q1	As per the journal style, abstract is mandatory. Please provide abstract for this article.
Q2	Please check the country name in affiliation “b”.

Thank you for your assistance.

INFORMATION SECURITY TECHNICAL REPORT XXX (2010) 1–4

available at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodinf.htm

Information Security Technical Report

Digital forensics and the issues of identity

Andy Jones [a,b,*], T. Martin [a]

[a] Khalifa University of Science Technology and Research, United Arab Emirates

[b] Edith Cowan University, Australia

1. Introduction

There are an increasing number of issues that relate to the identity of all users of Information and Communications Technologies (ICT). These are challenging not only individuals and organisations but also the law enforcement community. At perhaps the most fundamental level is the question of what we commonly consider to be the identity of an individual. Prior to the introduction of widely used ICT, in the developed world the identity of an individual was established and normally based upon documentary evidence. This was typically in the form of a birth certificate, a passport, an Identity card or some other, normally attested document such as a social security card or a driving license. Based on these documents, people had just one identity. The use of these documents was not foolproof and all could be forged, copied or stolen, although the effort required to acquire the original document and to produce a copy that would pass even the most cursory of inspections, somewhat limited this threat. As the use of ICT has increased, people in developing countries have gained access to global communications and the services that can be accessed through them. Many of these countries do not have accreditable document sources on which an identity can be founded. The birth certificate, which in the West is accepted as the foundation document for a persons' identity, in other countries either does not exist or is not held in a centralized system.

The concept of a person having one, unique identity has also changed. In the digital environment there are now a number of arguments for a single person having multiple identities. Examples of this might be one identity that is used for social networking while another that is used for on-line banking or shopping. This is a totally different approach to that which is normally applied in the physical world and as a result can be difficult to reconcile.

2. The changing environment

The introduction of a wide range of technologies has changed the whole environment we operate in. We find ourselves having a greater dependence on ICT systems. This is not to say that the environment has changed because of the technologies, but rather the new technologies have led to the introduction of products and services that have allowed society to change to meet a range of aspirations and pressures. In the last thirty years or so we have seen the introduction of public access to the internet and have now reached a point where mobile communications for both voice and data is almost ubiquitous. We can now easily check our location and share this information through the use of Global Positioning System (GPS) technology. This has become embedded in most mobile devices such as laptop computers, handheld devices such as Personal Digital Assistants (PDAs), mobile phones and even cameras.

In the computer environment, we have seen a progression from centralized management of computer systems, where organisations owned the infrastructure and could more easily control access to their systems, to the Internet and the use of the public infrastructure, where access to a system can potentially be gained at low or no cost from anywhere in the globe. At the same time the range of methods of access to an ICT system have grown from having to connect directly to a system by cable, to dial up access over the fixed telephony system to the current situation where it is possible to connect from a mobile handheld device (mobile phone, PDA, Netbook, laptop) via wireless access points or the mobile telephony system. It is currently possible in most parts of the world to obtain an anonymous email account through Hotmail or Google or a host of other sources and to gain anonymous access to the internet from either WiFi hotspots or from an untraceable pay-as-you-go mobile phone. This is before other

* Corresponding author. Khalifa University of Science Technology and Research, United Arab Emirates. Tel.: +971 509910578.
E-mail address: andrew.jones@kustar.ac.ae (A. Jones).

1363-4127/$ – see front matter © 2010 Published by Elsevier Ltd.
doi:10.1016/j.istr.2010.10.008

illicit methods of connection such as the hijacking of poorly protected home hubs is considered.

All of the advances in the technologies have not only made it increasingly easy to gain access to information, but have also made the issue of identifying the user more difficult as the credentials that they have to use to 'prove' their identity have had to become more international, more electronically based, and as a result, more difficult to validate.

Into this scenario we are seeing the introduction of services such as the ePassport and eVoting. A number of countries have introduced the ePassport, which aims to create harder to forge documents by digitally protecting and storing the information in embedded chips. When this was introduced in the UK, it was quickly demonstrated that the system was flawed and that the RFID tag could be cloned (Boggan, 2008; Zetter, 2006) within a very short period.

3. Identity in a global environment

One issue that has proven to be an increasing challenge to determining identity occurs when it becomes necessary to transliterate names from one language to another, for example from Russian or Chinese or Arabic to English. An open and wide interpretation is exhibited not only in the way in which the name is constructed, but also the way in which the name is translated. An example of this might be the translation of the name Mohammed Bin Hussein Bin Faisal Al Qhatani from Arabic to English. The name might be constructed from the Given Name, the Patronym (fathers name) and the Family Name or Tribal Name, but the patronym or the Tribal name may be omitted for convenience. In addition, the word "Bin" which means "Son of" and "Al" which means "the" can be also omitted. In some countries like Moritania, the word "Bin" is replaced by the word "Weld". So the aforementioned name can take different forms of transliteration as Mohammed Bin Hussein Faisal, Mohammed FaisalAlQahtani, Mohammed Hussein Qahtani, Mohmmed Hussein Faisal, etc. More seriously, each element of the name can be transliterated in a number of ways. For example, Mohammed can be represented as Mohammed, Mohammad, Mohamed, Muhammad, Muhammed, Muhamed, Mehmed, Muhamed, Muhammet, Muhamet, Mehmet or even Mohd.

This provides a huge potential for accidental or intentional confusion over the identity of an individual.

4. Social networking

One of the ways in which we communicate and share information has also changed significantly with the near ubiquitous availability and use of the World Wide Web has been the advent of social networking sites. There are currently in excess of 650 such sites, with nearly seventy of them claiming in excess of one million users. Facebook alone claimed over 500 million subscribers (Facebook Blog, 2010) in July 2010. Together with the popularity of social network sites have come warnings and reports of their use by criminals to gain information that is subsequently used to 'steal' the users identity (BBC News, 2007; Perez, 2009).

There is the obvious problem of account hijacking, which can and has been used to extort money from friends who do not know to double check a plea for help via different channels (Sullivan, 2009). But more sinister is the use of public knowledge in one social network to gain trust in another (Elgan, 2008). If you can become a "friend" of someone in one social network, it is possible to learn enough about them to impersonate them in another.

In the past, people mostly shared personal information with trusted friends when they met in person, during telephone conversations or via a letter. This limited the number of people who gained first hand access to the information and, with the exception of the letter, meant that there was no long term record of the information that was exchanged. With Social Networking, the number of people that an individual shares information with has increased dramatically (according to Facebook (Facebook Statistics), users have an average of 130 'friends') who have visibility of any information that a user posts. So we now have a vastly expanded circle of people who have instant access to personal information, combined with the fact that there is now a permanent record of all of the information that is posted. Consequently, we see a corresponding increase in the level of risk that the information may be misused in some way.

You would hope that the creators of these social networks would strive to make them safe. Any harm that comes to their users through Identity Theft is bad for business. Unfortunately, commercial pressures, whether in the form of advertising or as a result of the desire to capture the live-search/trending topics market is pushing us towards more open networks. The defaults are clearly in place to expose as much personal information as possible. Consider the case of Rebecca Javeleau (Jamieson, 2010) who wanted to invite fifteen of her friends to her birthday party. Over 20,000 Facebook users RSVP'd. Similar episodes in the past have lead to serious property damage (Daily Telegraph, 2010). Though the risk of such highly-publicized events is great, the ones that get so much attention are not the greatest threat, as they are likely to at least provide warning for any adults involved. How many children's birthday parties have been organized on Facebook where instead of thousands, only a handful of strangers learned the details?

For the most part, users of the world wide web and in particular of social network sites have continued the way they approach information sharing in the physical world into the electronic environment, but without realizing that the use of the new environment has changed the level of risk.

In the electronic world, the risk has increased in a number of ways. Firstly, the majority of people appear to be much less cautious about who they accept into their circle of friends. Recent experiments have shown that nearly 40 percent of people asked to be a 'friend' of a character that had been created, but that did not actually exist, accepted the character as a friend within a very short period of time. This gave the character access to the personal details that they had posted and also to the details of their other friends. For a criminal intent on blackmail, identity theft or cyber-stalking, this level of access to an individual's information provides a rich environment in which to operate. There now exists a market for the buying and selling of social network accounts, offering

Please cite this article in press as: Jones A, Martin T, Digital forensics and the issues of identity, Information Security Technical Report (2010), doi:10.1016/j.istr.2010.10.008

financial rewards for access to a large number of people's information (Milner, 2010). The level of incidents of identity theft has continued to rise with reports of almost ten million US citizens affected during the year 2008 according to a report by The Javelin Strategy & Research Center (Identity Theft Statistics, 2009), a rise of 20% on the previous year.

5. Technology

As the technologies have developed and become increasingly widely used, there has been a massive increase in the range of devices that might be used. We have moved from mainframe computers with 'dumb' terminals, to servers and networked PCs, laptops, PDAs, mobile phones, Netbooks, smart phones to the iPad and similar devices. We have also seen the introduction of a range of other digital devices including cameras, MP3 players and GPS devices, all of which have the capacity to store digital information. At the same time the storage capacity of the devices has continued to grow rapidly, which has meant that the volume of information that is stored on the devices is greater and as a result, takes longer to analyse. For the digital investigator, this has meant that they potentially have to have an in-depth understanding of an ever widening set of devices, their operating systems and the applications that they support. For any one investigator the diversity of devices has now passed the point where they can realistically be expected to have an in-depth knowledge of more than one or two of the device groups and has meant that they have had to specialize in specific areas. This in turn has put increasing pressure on an already limited resource and may mean that for an investigation into one incident in which a range of devices are involved, several investigators may be required.

6. Proving an identity

Both the theft of an identity or the use of a false identity in any digital environment is relatively easy. From this it follows that establishing the identity of a suspect to a point where it is beyond reasonable doubt is also increasingly difficult. In digital forensics, it has been relatively achievable to determine the computer or device that has been used in the commission of a crime. What has always been more difficult is proving who was using the device at the time and whether they were in control of the device and responsible for actions taken on it. The latter is increasingly a problem as malware has made modern computers unreliable. The problem now is how far does an investigator have to go to 'prove' that the suspect was using the device at the time in question and whether they were responsible for the actions taken by the device.

This was highlighted in the UK with the Caffrey case (BBC News, 2003) in 2003 when the 'Trojan Defence' was first successfully used. In this case, the suspect claimed that a trojan (malicious code installed on a system by disguising itself as something benign) had acted on his computer without his knowledge and then deleted itself from the system, leaving no trace. He was subsequently acquitted of the charge.

Proving the identity of the person who had operated a computer would be a relatively simple matter for the digital forensic investigator if, amongst other things, there was no malicious software and people protected their access credentials for a device and did not share them, either intentionally or inadvertently. It would also help if they selected strong passwords or used dual factor authentication and logged off the device when they had finished using the system. Unfortunately, the real situation is very different. People do not take this level of care in protecting the access to their systems and, as a result, the accountability for actions taken using the device is more difficult to determine. This means that proving a specific individual was using a device at a specific time and that they knew what actions were being performed on that device can be difficult or impossible. It is rarely possible to achieve this using just the records and logs that are maintained by the devices and systems being used and it is often a combination of records that will provide the required level of confidence. This may be a combination of the login details on the device, coupled with access control logs for the area in which the device was located (if the suspect was the only person in the room at the time that the device was used, the main problem remaining is to prove that there was no malicious software running on the system).

There are three sources of information from which an identity can be verified. Traditionally these have been using something that you know (a password) or something that you own (a token) or something that you are (a biometric such as a fingerprint or a retinal scan). The use of two factor authentication (two methods of identification) has been used increasingly to improve the level of confidence that the identity of a person is correct. Two factor authentication usually takes an identifying feature from two separate areas, such as a password and a token. This can significantly increase the confidence that the user is the person that they claim to be, but unfortunately even this is not foolproof.

The use of biometrics as a means of identification has existed for some time now and there has been a gradual improvement in the range of measures that can be used and the effectiveness of the systems used to capture the measurements. The range of measures that can be taken includes fingerprints, retinal scanning, voice recognition, wrist vein patterns, facial features and gait characteristics as well as keyboard input measurements, to name just the most common. One problem is that most biometric measurements are not universally applicable, for example elderly populations and manual labourers are often unable to enroll in a fingerprint biometric system.

The use of something that you own (normally a 'dongle' or a token which generates a one-time use numeric string) is an alternative, but also has potential problems. If you have a token for each separate account, you need to carry and protect them, which can be inconvenient and confusing. If you lose a token, it can be used by someone else who may try to guess the password. The loss of a token may also be extremely inconvenient and result in a denial of access to systems at a time when you need it most. The replacement of a lost token may also take some time.

While the use of passwords has long been regarded as a weak form of identification, there does not yet seem to be sufficient confidence for organisations and users to adopt just

Please cite this article in press as: Jones A, Martin T, Digital forensics and the issues of identity, Information Security Technical Report (2010), doi:10.1016/j.istr.2010.10.008

one of the other means of identification. However, the use of the flawed password system in conjunction with either a biometric measurement or a token significantly improves the likelihood that the user is who they claim to be.

7. How far do you have to go to prove the identity of a person?

Forensic science has developed significantly during the past century and we now have at our disposal the means to identify people through their fingerprints, their DNA and a range of other less common measures. In the area of ICT, digital forensics has also developed rapidly. Towards the end of the last century we saw the rise of computer forensics which started to examine the evidence that was available on computer hard disks and on logs maintained by the networks. This has developed with the changes in technology to the digital forensics of today that examines not only the hard disks of computers but also the storage media of Netbooks, PDAs, mobile phones including smart phones, games consoles, GPS systems, MP3 players, cameras and a range of other technologies.

As the range of devices has increased, the storage media has become capable of containing ever larger volumes of data and the software has become ever more sophisticated, so the job of identifying the user of the device has become more complex.

Identifying the device that was used when an incident occurred and tying it to the person who was using it at the time in question are two of the major challenges. This has always been a problem in digital forensics and it is often the case that the information available on the device itself is not sufficient to prove who the user was. In many cases, it is actually necessary to catch the person in the act or to find corroborating evidence from other sources. The increasing popularity of cloud computing may cause additional problems for the forensic investigator, as information that was previously stored on the device that was used by a suspect may now be stored elsewhere and may not be easily accessible.

The investigator must, in most scenarios, provide enough evidence to prove beyond reasonable doubt that the suspect was the person who was in control of the device when the actions took place. If a biometric authentication measure was used to access the device, it is unlikely that the fact that the user was operating the device would be challenged. The same does not apply to passwords and tokens as they could have been obtained and used by someone else. The investigator also has to be able to show that the device was not under the control of malicious software and that the user had knowledge of the actions that were taking place on the device. This may be achievable from the records that are created and retained by the device, such as typed search terms, network connections, SMSs or calls made. It can also be strongly inferred by the profiling of a users activity on the device over a period of time.

8. Conclusions

Establishing the identity of a user of a device and proving beyond a reasonable doubt that they were in control of a device at a specific time has always been difficult. The increased globalization of communications and easier and cheaper access has resulted in massively increased volumes of traffic and a much wider range of available services. This has lead to many more people using the Internet and sharing, either intentionally or inadvertently, information about themselves that can be used by others to steal their identity. At the same time, the technologies have developed to support the increasing demand for access to information at any time or place. The result is that while determining the identity of a user on a network or a device is less easy, the range of devices that must be examined and the storage capacity of these devices has continued to increase. In short, proving the identity of a user of a device without external corroboration is becoming increasingly difficult.

REFERENCES

BBC News. Questions cloud cyber crime cases, http://news.bbc.co.uk/2/hi/technology/3202116.stm; 17 October 2003.

BBC News. Web networkers 'at risk of fraud', http://news.bbc.co.uk/2/hi/uk_news/6910826.stm; 22 July 2007.

Boggan S. 'Fakeproof' e-passport is cloned in minutes. The Sunday Times, http://www.timesonline.co.uk/tol/news/uk/crime/article4467106.ece; 06 August 2008.

Daily Telegraph. Family home trashed after Facebook party goes wrong, http://www.telegraph.co.uk/technology/facebook/7291613/Family-home-trashed-after-Facebook-party-goes-wrong.html; 22 February 2010.

Elgan M. Why you can't trust 'friends' on Facebook, IT World, http://www.itworld.com/security/58447/why-you-cant-trust-friends-facebook; 26 November 2008.

Facebook Blog, http://blog.facebook.com/blog.php?post=409753352130 [accessed 19.09.10].

Facebook statistics, http://www.facebook.com/press/info.php?statistics.

Identity theft statistics, www.spendonlife.com; 2009, http://www.spendonlife.com/guide/2009-identity-theft-statistics; 2009 [accessed 20.09.10].

Jamieson A. Girl, 14, fears 21,000 party guests after Facebook invite blunder. Daily Telegraph, http://www.telegraph.co.uk/technology/facebook/8012043/Girl-14-fears-21000-party-guests-after-Facebook-invite-blunder.html; 20 September 2010.

Milner C. Undetectable, identity-stealing bots for sale, cheap. Epoch Times, http://www.theepochtimes.com/n2/content/view/36458/; 2 June 2010.

Perez S. Fake social network profiles: a new form of identity theft in 2009, Read Write Web, http://www.readwriteweb.com/archives/fake_social_network_profiles_a.php; 3 February 2009.

Sullivan B. Facebook ID theft targets 'friends'. The Red tape Chronicles, http://redtape.msnbc.com/2009/01/post-1.html; 30 January 2009.

Zetter K. Hackers clone e-passports. Wired Magazine, http://www.wired.com/science/discoveries/news/2006/08/71521; 03 August 2006.

Please cite this article in press as: Jones A, Martin T, Digital forensics and the issues of identity, Information Security Technical Report (2010), doi:10.1016/j.istr.2010.10.008