Towards Solving the Identity Challenge Faced by Digital Forensics

A. Valjarevic and H. Venter

Department of Computer Science, University of Pretoria
e-mail: alexander@vlatacom.com

Abstract

The importance of digital forensics is on a steady rise. One of the biggest challenges posed to digital forensics is the identity challenge. The authors define the identity challenge as the difficulty to prove beyond reasonable doubt in a court of law that a specific person was using a specific identity of a digital subject at a certain time. In order to meet or at least decrease this challenge, organised action within the digital forensics field is needed. The authors propose a set of requirements to be introduced within digital forensics in order to help solve this issue. These requirements include the following: defining the principles of digital identity within digital forensics; introducing strong authentication methods for all information systems and electronic devices; introducing digital signatures for all transactions within information systems and electronic devices; constant interaction with other relevant fields and last but not least, putting an end to internet anonymity. The authors believe that, if implemented, the proposed requirements would not only bring about the higher admissibility of digital evidence related to digital identity in a court of law, but also increase the efficiency of digital forensic investigations.

Keywords

Identity, Digital Identity, Identity Challenge, Digital Forensics, Information Security

1. Introduction

Information technology is advancing at a high rate and modern society is becoming more dependant on it. Together with the increase of incidents requiring digital forensic investigations, this makes digital forensics rapidly gaining in importance. One of the aims of the digital forensic process is to produce (through a process of digital evidence analysis) a hypothesis on who did what, where and how, regarding the incident being investigated. The question of *who* is crucial, especially if the digital forensic process were to lead to the presentation of findings in a court of law. Digital forensic investigators have to link identity of a digital subject (hereafter referred to as a 'digital identity') to a human identity. This is a challenging task.

It is against this background that the authors have defined the following problem statement. The problem is that the identity challenge faced by digital forensic investigations is increasing. We define the concept "identity challenge" as the effort to prove beyond reasonable doubt in a court of law that a specific human has used a specific identity of a digital subject at a certain time. Lack of awareness of this challenge might become a great obstacle in the development of digital forensics as a

whole. There is a need to define requirements that have to be obliged by digital forensics scientists and practitioners in order to make progress towards solving this challenge.

The first section of this paper has introduced the paper and the problem statement. Section 2 gives background on digital forensics, attribution, digital identity and legal requirements. The following section proposes requirements for solving the identity challenge faced by digital forensics. Section 4 discusses the proposed requirements, their benefits and associated challenges. The last section concludes the paper and indicates possible future research work.

2. Background

An overview of digital forensics, attribution, digital identity and legal requirements regarding digital evidence is provided in the following subsections.

2.1. On Digital Forensics

In this section the authors wish to explain the basic principles and importance of digital forensics.

Digital Forensics is defined as the use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorised actions shown to be disruptive to planned operations (Palmer, 2001). The digital forensic process comprises several phases. The authors define these phases as: Incident detection, First response, Planning, Preparation, Incident scene documentation, Potential evidence identification, Potential evidence collection, Potential evidence transportation, Potenial evidence storage, Potential evidence analysis, Presentation and Conclusion. (Other authors define phases differently and there is currently no consensus for a single process model in the digital forensics community.) Analysis of the potential digital evidence is performed in order to make a hypothesis on how the incident occurred, what its exact characteristics are and who is to be held responsible. In this paper, we concentrate on proposeing requirements to digital forenics that could make it easier to identify the person to be held responsible for a particular incident.

The importance of the digital forensics can be seen through the fact that, by the time of writing, we have an entire forensic community. For example, there exists a digital forensics group on Linkedin, called the Digital Forensic Association, which has over 4000 members. The importance of digital forensics can be also seen in the light of the large number of national and international bodies that are working towards the development and standardisation of this discipline. (i.e. The European Network of Forensic Science Institutes, The International Organization on Computer Evidence, International Federation for Information Processing Work Group 11.9 on Digital

Forensics etc.) There are also numerous evidence units and laboratories that are well funded and that produce forensically sound digital evidence.

2.2. On attribution

This section gives an overview of attribution in the light of digital forensics.

Attribution is defined as determining the identity or location of an attacker or an attacker's intermediary (Wheeler and Larsen, 2003). In (Hunker et al., 2008) it is stated that sufficient attribution may be satisfied by knowing the IP address of the host that initiated the attack, identifying the originator's e-mail address, locating the physical location of the source of the attack or by identifying the actual individual who was at the attacking computer. In this paper, however, we are concentrating only on the issue of identifying the actual individual who was responsible for a certain action in digital realm. To achieve successful attribution, investigators today have to introduce methods and techniques outside of the digital forensics and cooperate with investigators performing the physical investigation. Techniques used include authorship attribution (i.e. through typing pattern biometrics, stylometry), introducing circumstantial evidence from physical forensics investigations (i.e. the suspect was in the room where computer, used for committing cyber-crime, is located, based on interviews with witnesses). Ideally, a digital forensics investigation would be able to produce direct and circumstantial evidence sufficient for the successful identification of the individual involved in the incident being investigated.

The next section explains the basics of digital identity.

2.3. On Digital Identity

Digital identity can be defined as the digital representation of a set of claims made by one digital subject about itself or another digital subject (Cameron, 2006). Note that this paper concentrates solely on digital identity associated to humans. Also note that a human can not have a digital identity, for the simple fact that a human cannot exist in the digital realm. However, a human can use a certain digital identity and be responsible for that use. In order to make the above clearer we provide some definitions of some terms used so far.

"A *digital subject* can be defined as a representation of a person, or a representation or existence of a thing in the digital realm, that is being described or dealt with." This definition was constructed by modifying the definition in (Cameron, 2006). Examples of digital subjects would be a user account belonging to a human, an avatar in a computer game, an IP address of a computer, digital resources (e.g. files) operating system, etc. Further, if we concentrate on the digital identity of humans, we can say: "A *digital subject* is a representation of a person in the digital realm."

"*The claim* is defined as an assertion of the truth of something, typically one that is disputed or in doubt (Cameron, 2006)." Examples of claims made about a digital

subject would be that the user account has a certain password, or that the IP address of a computer has a certain digital certificate associated to it, etc.

Thus, a typical example of a digital identity would be the claim that a certain user account on a certain operating system has a certain username and password. Further, let us try to define how human identity can be connected to digital identity.

The process of verifying the validity of a claimed identity (human identity) is known as authentication. Thus, the identity of a person can be confirmed only through appropriate authentication. Different forms of the authentication for human identity exist, including (Stewart et al., 2008): PIN numbers, passwords, favourite colour, etc. (*something you know* type of credentials); One-time pads, usb drives, smart-cards, digital certificates, state issued documents (*something you have* type of credentials); Biometrics– fingerprints, iris pattern, vane pattern, hand geometry, voice, face geometry, keystroke pattern (*something you are* type of credentials). In modern information systems it is considered good practice to introduce multi-level authentication (Stewart et al., 2008), where different types of authentication credentials are used in combination with one another, e.g. providing a password together with using a biometric trait such as a fingerprint.

In (Milgate, 2006) identity is defined as a relationship between one entity and a particular registration. The authors would rephrase this to the following: "The connection between the identity of a human and a digital identity is established through registration." An example would be a person registering an email account. We can only claim that a certain human used a certain digital identity when the identity authentication process was performed during registration and/or before each particular use of the digital identity. Figure 1 illustrates the concept of digital identity and the connection between human identity and digital identity. Namely, digital identity is formed with set of claims and digital subject and then is connected to human identity through process of registration, which should include identity authentication. Human identity exists solely in physical realm. Digital identity exists solely in digital realm.

The next section provides an overview of legal requirements regarding digital evidence and digital identity.

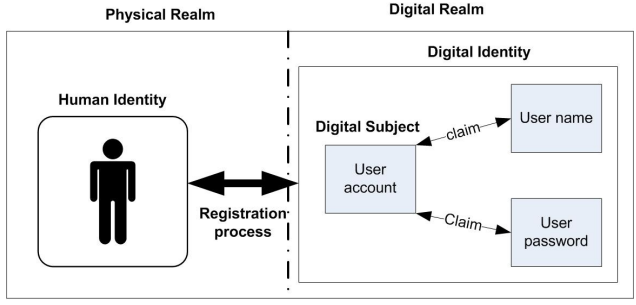

Figure 1: Concept of digital identity and connection with human identity

2.4. Legal requirements

In this section the authors give an overview of the legal requirements pertaining to digital forensics and especially the admissibility of digital evidence in a court of law. It should be noted that legal requirements may differ extensively in different jurisdictions across the world. The premise of this section is not to advocate specific legal systems, but rather to note the generic requirements in terms of legal issues that should be adopted by the legal system of a specific jurisdiction.

For example, in the United Stated of America cases that include the presentation of digital evidence are treated under rule 702 of the Federal Rules of Evidence. For application of this rule, the Daubert case (Daubert v. Merrell Dow Pharmaceuticals, 1993) is the most important. In the Daubert case, the court suggested the following factors to be considered: whether the theories and techniques employed by the scientific expert have been tested; whether they have been subjected to peer review and publication; whether the techniques employed by the expert have a known error rate; whether they are subject to standards governing their application; and whether the theories and techniques employed by the expert enjoy widespread acceptance. Other countries have similar requirements regarding the admissibility of digital evidence.

It is notable however that there are no established legal requirements for accepting the claim that certain digital identity has been used by certain person at certain time. Proving that certain digital identity has been used by certain person at certain time can be challenging. Following case clearly depicts that challenge (Leyden, 2003). Aaron Caffrey was arrested under the suspicion of launching a denial of service attack against the Port of Houston's systems. The defense claimed that Trojan was installed on the defendant's computer and that attack was performed by the Trojan. The digital forensics investigation showed no sign of a Trojan, and did find tools used for attack on the computer, but could not rule out that a Trojan may have been in volatile storage media. The jury unanimously decided that the defendant was not guilty.

The next section explains the proposed requirements to be imposed in order to solve the identity challenge faced by digital forensics.

3. Requirements for solving the identity challenge

The authors propose the following requirements to be imposed on digital forensics in order to decrease the impact of the identity challenge: Definition of the principles of digital identity within digital forensics science, Introduction of multi-level authentication for all digital devices and information system, Introduction of digital signing of all digital transactions where possible, Interaction with fields of digital identity, identity management and biometrics, Terminating anonymity on Internet.

The subsections that follow discuss each of the above requirements in more detail.

3.1. Requirement 1 (Principles requirement): Definition of principles of digital identity within digital forensics science

The authors believe that it is essential for digital identity and digital identity principles to be defined within the science of digital forensics. Not only must digital identity itself be defined, but the principles have to be defined of how a specific digital identity can be associated with a specific person. These principles could later be used in a court of law in order to achieve higher admisibility of digital evidence. These definitions must be comprehensive and have to take into account as many as possible different types of information systems and electronic devices.

The main challenge for implementation of this requirement would be to achieve consensus in the digital forensics community and to enforce the use of the principles in a court of law, through cooperation with legal authorities. However, the authors firmly believe that achieving this requirement is possible and highly needed.

3.2. Requirement 2 (Authentication requirement): Introduction of multi-level authentication for all digital devices and information systems

The authors believe that there should be a requirement that the verification of identity – when accessing or registering to use a digital device or an information system (at all levels, i.e. OS, application and firmware) – should be performed via multi-factor authentication, for example requiring biometrics, a digital certificate and a password. There should be an interface to an identity management system within every electronic device and information system. (Such identity management system can be embedded within the device, or it can work as a standalone and be independent from other devices or information systems.) The interface with the identity management system should ensure that proper management of identities is performed. One physical person should have one identity (not limited to one role) within the device or system.

The authors understand that the implementation of this requirement would be challenging in terms of needed expenditure, technology development, and technology accessibility to users. We, however, do believe that in years to come the expenditure needed would become lower and technology needed for implementation would become more accessible.

3.3. Requirement 3 (Digital signatures): Introduction of digital signing of all digital transactions where possible

The authors believe that all transactions performed within any digital device or information system should be digitally signed by the entity performing the transaction. Note that we use the term *entity*. An entity can be any digital subject. This would enable non-repudiation and accountability for all transactions and would therefore decrease the identity challenge faced by digital forensics. It would also permit more efficient digital investigations due to the fact that transactions would be more easily tracked.

Digital signatures are now accepted all over the world as valid for authorising transactions. Within the European Union, for example, the Electronic Signature Directive (Directive 1999/93/EC, 2000) defines an electronic signature and what the legal effects of electronic signatures are. Similar statements are made in the South African Electronic Communications and Transactions Act (Electronic Communications and Transactions Act, South Africa, 2002). It is clear from this that appropriate legislature exists and supports the introduction of digital signatures for electronic (digital) transactions.

The challenges anticipated are as same as for *Requirement 3*. The authors believe that the implementation of this requirement (*Requirement 4*) would become possible in terms of needed expenditure and technology in the foreseeable future.

3.4. Requirement 4 (Interaction requirement): Interaction with fields of digital identity, identity management and biometrics

It is vital that digital forensic scientists and practitioners should constantly cooperate and interact with scientists and practitioners from the fields of digital identity, identity management and biometrics. Such collaboration is not limited to these fields and includes other fields that might have an interest in digital identity or digital forensics. Digital forensics has to take into account all the latest discoveries and practical solutions in these fields so as to stay up to date and geared up to adjust and improve in line with changes in these fields. Interaction would be facilitated most successfully through the introduction of common international bodies consisting of scientists and practitioners from all relevant fields.

3.5. Requirement 5 (No anonymity on the Internet): Terminating anonymity on the Internet

First of all, the authors want to stress that they believe that terminating anonymity on the Internet does not and should not mean putting an end to privacy on the Internet. The authors believe that if appropriate mechanisms and policies are in place, privacy on the Internet does not require anonymity. Future technological solutions should enforce the verification of digital identity when accessing or using information systems, while protecting personal identifiable information of the users.

It is striking to note that, most often, no identity authentication is performed when a person registers to use a certain digital subject (i.e. email account) on the Internet. This enables anonymity and privacy on the Internet, but makes the work of digital forensic investigators much harder. For example, hacker groups such as Anonymous and LulzSec have their own websites and social network accounts (i.e. twitter.com/lulzsec, http://lulzsecurity.com). Even though the digital identities are known, these cannot easily be linked with the identities of the human beings.

The authors believe that in order for every individual to be accountable for his/her actions on the Internet, it essential that no anonymity exists. This would enable digital forensic practitioners to associate digital identities on the Internet with the

physical identities in a quick and easy manner. Many calls have been heard for abandoning this custom of anonymity, but serious concerns about privacy remain a major reason for the inaction in this regard. The authors believe that the global society must take responsibility for the Internet and initiate action while implementing all that should still ensure the preservation of Internet users' privacy. The authors understand very well that implementing a measure such as terminating anonymity on the Internet would require world-wide discussions that would have to involve stakeholders and participants from all the relevant fields, ranging from law to information technology and from national security agencies to civil society representatives. We do recognize that this action would be against current legal environments in some countries, i.e. in The United States of America, but we expect that these legal environments could be changed if broader consensus is reached on this matter. The authors also realise that implementing this requirement would come at a cost and entail significant investments in hardware and software infrastructure of the Internet. They nevertheless believe that this requirement is essential from a digital forensics point of view, and are confident that abandoning anonymity on the Internet would hold much benefit in the long term.

Finally, note the following. In Facebook's Statement of Rights and Responsibilities, it is said: "Facebook users provide their real names and information... You will not provide any false personal information on Facebook, or create an account for anyone other than yourself without permission..." In Google's Terms of service, it is said: "...you may be required to provide information about yourself (such as identification or contact details) as part of the registration process for the service, or as part of your continued use of the services. You agree that any registration information you give to Google will always be accurate, correct and up to date." The above-mentioned examples practically mean that there are numerous service providers on the internet who do require personally identifiable information when you register to use the services, and still the bulk of the people using these services have no objection on that. But, how can a service provider guarantee that the supplied information is accurate? Currently it is very hard, and that is why it is now possible and common practice that people register user accounts by supplying other people's or imaginary personally identifiable information. Therefore, mechanisms should be in place to ensure identity authentication when registering to use services on the Internet, which would ensure the users conform to terms of service that they have accepted.

Of all the requirements proposed, this one is the most challenging. The implementation of this requirement would entail significant expenditure into developing and implementing technological solutions needed to end anonymity on internet, while preserving privacy of the users. A significant challenge would also be the development or change of existing legislature to accomodate for this requirement, or to implement the requirement in such a way that would not contravene current legislature. The agreement of the global community would be needed, which might be extremely hard to achieve. Inspite of all the challenges, the authors believe that the time for implementation of this requirement would be possible in the foreseeable future, due to technological advancements and the increasing importance of digital forensics.

4. Discussion

In this paper, the authors give a comprehensive explanation of digital identity and how it can be connected to a human identity, and propose a set of requirements to decrease the identity challenge faced by digital forensics. The proposed requirements are high-level statements and should be further developed by the entire digital forensics community. Note that the implementation guidelines, methods and techniques are outside the scope of this document. If implemented, these requirements can bring about multiple benefits for digital forensics, such as the higher admissibility of digital evidence pertaining to digital identity in a court of law, and preventing the identity challenge from becoming even more problematic. In addition, the implementation of these requirements might make digital investigations into digital identity issues more efficient and effective, both in regards of identifying humans involved.

It should be stressed that in order to implement these requirements, the engagement of the digital forensics community at large will be needed. An implementation plan needs to be developed in accordance with legal requirements and current technology capabilities. The work must be performed in close cooperation with other relevant fields such as identity management, biometrics and public key infrastructure in order for the implementation plan to be in line with current trends and technologies in these fields. For example, it should be taken into account that what we consider a suitable means of verifying identity today might not be suitable tomorrow. For example, we can envisage that with the development of more powerful computers with high processing power, public key infrastructure with current key lengths may become obsolete. Further, consensus on the requirements is needed in the digital forensics community if implementation is to be effective. The authors believe that the proposed requirements should bring about significant changes. Support from national and international bodies that govern information technology development, Internet and information security would be needed, together with support from the governments themselves in order for all or some of the requirements to be accepted and implemented. The authors also realise that the proposed requirements imply that significant expenditure has to be incurred. Technological advancement and cost efficiency of the solutions for implementing these requirements would teherfore play a major role in acceptance of the requirements.

5. Conclusion

Let us revisit the problem statement. The problem is that the identity challenge faced by digital forensics is increasing. Thus, it is currently difficult for digital forensic scientists and investigators to prove beyond reasonable doubt in a court of law that a specific human being used a specific identity of a digital subject at a certain time. In an attempt to address this problem, the authors proposed a set of requirements to be imposed for the sake of digital forensics. These requirements constitute a first step towards solving the identity challenge. The authors strongly believe that, if implemented, these requirements will have multiple benefits, among others

enhancing the admissibility of digital evidence related to a digital identity in a court of law and improving efficiency of digital investigations.

We also realise that such requirements cannot suddenly all happen over night; it will take time. The person reading this might also perceive these requirements as a Utopia. Feel not alone, since the authors also realise that some of these requirements are far fetched. However, if one thinks with an open mind about the huge advantages some of these requirements are posing, then surely they cannot simply be ignored. It is not impossible to accomplish such requirements, albeit, it will be a mammoth task. The authors hope, however, that this paper will lay a corner stone towards the prospect of solving the identity challenge in the digital realm.

Future research work in this regard will include defining lower-level requirements and proposing an implementation plan. This will have to be done systematically with the aid of the entire digital forensic community and with support from the wider information security research community and other interested parties.

6. References

Cameron, K. (2006), "Laws of Identity", http://www.identityblog.com/?p=352, (Accessed 01.02.2012)

Daubert v. Merrell Dow Pharmaceuticals Inc. (1993), 509 U.S. 579

Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, O.J. L 13/12, 19 January 2000 (2000)

Electronic Communications and Transactions Act, Act No. 25 of 2002, Republic of South Africa (2002)

Hunker, J., Hutchinson, B., Margulies, J. (2008), "Role and Challenges for Sufficient Cyber-Attack Attribution", Institute for Information Infrastructure Protection

Leyden, J. (2003), "Caffrey acquittal a setback for cybercrime prosecution", The Register U.K. Press 3

Milgate, A. (2006), "The Identity Dictionary", http://identityaccessman.blogspot.com, (Accessed 01.02.2012)

Palmer, G. (2001), "A Road Map for Digital Forensic Research", *Technical Report DTR-T001-01*, Report from the First Digital Forensic Research Workshop (DFRWS)

Pollitt, M.M. (2001), "Report on digital evidence", 13th Interpol Forensic Science Symposium, Lyon, France

Stewart, J.M., Tittel, E., Chapple, M. (2008), "*Certified Information Systems Security Professional Study Guide*", Fourth Edition, Wiley Publishing, Inc., Indianapolis, Indiana, ISBN: 978-0-470-27688-4.

Wheeler, D.A. and Larsen, G.N. (2003), "Techniques for Cyber Attack Attribution", *IDA Paper*, Institute for Defense Analysis, P-3792.