Online ID theft techniques, investigation and response

Olga Angelopoulou,* Paula Thomas, Konstantinos Xynos and Theodore Tryfonas

Information Security Research Group,
Faculty of Advanced Technology,
University of Glamorgan,
Pontypridd CF37 1DL, UK
E-mail: oangelop@glam.ac.uk
E-mail: pthomas@glam.ac.uk
E-mail: kxynos@glam.ac.uk
E-mail: ttryfona@glam.ac.uk
*Corresponding author

Abstract: ID theft, especially in its online form, is currently one of the most prevalent types of computer crime. The limited end-user awareness as well as the retention and business processing of large amounts of personal data in a manner that does not meet security and regulatory requirements provide plenty of opportunities to fraudsters. A number of organisations have produced guidelines of good practice targeted to individuals and organisations, however the matter is still on the rise. In this paper, we review computer-based techniques employed by fraudsters in order to steal IDs and refer to published guidelines and the documented good practice against those. We discuss the issues related to the investigation of such incidents and provide the grounds for the development of a framework to assist in their forensic examination.

Keywords: e-Crime; ID theft; incident investigation; digital evidence; computer forensics.


Biographical notes: Olga Angelopoulou is a Research Student at the Faculty of Advanced Technology (Information Security Research Group) in the University Glamorgan, where she is working on her PhD in Computer Forensics. She holds a BSc in Computer Science and an MSc in Information Security and Computer Crime. Her research subject is Analysis of Digital Evidence in Identity Theft Investigations, while the research areas she is interested in include computer forensics, digital evidence and identity theft.

Paula Thomas is a Senior Lecturer in the School of Computing at the University of Glamorgan. She is an Active Member of the Information Security Research Group (ISRG) and has a number of publications on network and wireless security. Her research interests also include the security of mobile devices and developing secure applications for PDA’s and mobile phones.

Konstantinos Xynos has an Honours in Software Engineering, BSc (Hons) and a Masters in Computer Systems Security, MSc from the University of Glamorgan. He is part of the Information Security Research Group (ISRG) at the University of Glamorgan.
the University of Glamorgan and is currently working towards a PhD in Data Mining of Intrusion Detection Systems. His research areas of interest include: programming, network security, computer forensics, security aspects of a system, networks and databases.

Theodore Tryfonas is a Lecturer at the Faculty of Advanced Technology of the University of Glamorgan with a specialisation in Computer Forensics and Systems Audit. He has many years of experience in the fields of information security and software systems development and he is a Certified Information Systems Auditor. Besides his academic work, he also functions as an Expert Witness in cases of computer-related crime. His current research interests include amongst others security issues of emerging technologies (RFID, VoIP, biometrics, etc.). He has a PhD in Information Systems Security, an MSc in Information Systems and a BSc in Computer Science.

1 Introduction

According to a study of the Identity Theft Resource Center (2003), ID theft is distinguished in three forms: financial, criminal and identity cloning. This study takes as examples real victims and drawing upon these cases those three forms are defined. Ultimate purposes for ID theft could be either financial and other resource and privilege gains or protection of one’s real identity and masquerading behind another, mostly legitimate entity. ID thefts can also take advantage of an organisation’s good name in order to attract individuals and hence then there is a case of a double ID theft, the corporation’s and the consumer’s (Dwan, 2004).

Identity theft can occur in many forms, for example, by lost or stolen wallets, discarded documents containing personal details, phishing e-mails, etc. According to The Identity Theft Resource Centre (2003), students, old people and the military appear to be more vulnerable to ID theft than any other group of people. By the time the end user has found out that they have been a victim of identity theft, is already too late and their personal details have been used for fraudulent purposes (Dwan, 2004). It also seems that most perpetrators of this kind of crime are not alone, but rather organised and well equipped. Indeed, ID Theft is nowadays directly linked to drug trafficking, money laundering and terrorism (Collins, 2003).

Based on the US Federal Trade Commission’s report for National and State Trends in Fraud and Identity Theft 2004 of the 635,173 complaints received, 246,570 were ID theft reports. The most common form of reported identity theft was Credit Card fraud, followed by phone or utilities fraud, bank fraud and employment fraud. It is very important to note that only 30% of victims notified a police department. It can therefore be assumed that the majority of people are not aware that they could have contacted law enforcement agencies and prefer not to make their ID theft incident known.

In 1999 20,000 cases of ID Theft were reported in the UK, in 2001 there were 53,000 and in 2003 the number had almost doubled. It can take a victim up to 300 hr of work when dealing with the consequences of their ID theft with banks and credit card companies (Porter, 2004). This emerging and developing trend in crime triggers complex investigations that require extensive use of information technology, both as a medium for analysis and as evidence at the same time. Fraudsters are obtaining more sophisticated technological ways and manage to conceal their crimes.
For example, in ID theft cases for financial purposes, the investigator can first focus on credit history, transactions made on the victim’s name, applications for bank accounts, loans and credit cards. This evidence trail is to be recovered in the form of data, logs, etc. formats through various systems within one or even multiple financial organisations. As a result, the investigation is complicated and time-consuming. With identity-related ID theft cases, the investigator will need to consider not only the financial evidence but the personal information gained, subsequent actions triggered by a hijacked identity, etc.

In this paper, we discuss how ID theft can occur in the interconnected world and what evidence may be left behind for the computer forensic investigator. We intend to provide an initial insight into this computer-fuelled crime in order to facilitate the analyst in identifying and analysing the related digital evidence.

2 ID theft techniques and digital evidence

2.1 Techniques and tools of identity thieves

Information can be obtained from stolen wallets or handbags which usually contain identification papers, driving licences, credit and bank cards, etc. Alternatively, someone’s personal mail might be stolen to gain bank and credit card statements, preapproved credit offers and tax information. The techniques used to collect this information include searching through household litter bags, burglary, social engineering or even identification of a deceased person.

The identity theft criminals may contact a person who has lost his credit card claiming that they found it, ask for personal details and then use it in a fraudulent manner (Dwan, 2004). They may apply for a new credit card using someone else’s personal details, buy items they never pay for and the offence will be against the legitimate owner. They might even bankrupt on someone’s account or give stolen personal details in case of an arrest (Federal Trade Commission, 2003).

High-tech techniques for ID theft require the use of a computer, and usually the internet, in order to gain the required information. The techniques that are used require at least intermediate information technology knowledge and skills and the most common techniques are detailed below.

3 Phishing

Phishing is used to gain personal information by sending e-mail messages that appear to come from trusted organisations. A phishing attack takes the form of a mass distribution of ‘spoofed’ e-mail messages in which the reply addresses, links and branding appear to come from banks, insurance agencies, retailers or credit card companies. The messages look authentic by using corporate logos and formats similar to those that are used by the official companies. The threat is perceptively dangerous when personal information is requested for auditing or verification purposes, for example, personal account numbers, passwords and other private information. In April 2004, an unemployed 21-year-old British man was arrested by the UK National Hi-tech Crime Unit, allegedly for a phishing attack against The Cooperative bank and targeting the Smile Internet Bank. However this man was just an amateur and according to the police he is not related with the organised crime (news paper ‘Police Catch UK Phisher’, 2004).
4 Web-spoofing

Web spoofing is the method by which the users believe that they have been directed to the official website of a company. Instead, they have actually been directed to a ‘spoofed’ website where any personal information that is entered, will be stored and used for malicious purposes. The web pages will have been designed by skilled web designers and are often an exact copy of the original company’s website. The important difference is that there are minor changes that allow for user information to be stored on the fraudster’s servers.

5 Malicious software: spyware, viruses and Trojans

Spyware is designed for exploiting infected computers usually for marketing purposes. The activity of the web browser is monitored, resulting to routing of HTTP requests to the web sites that are advertised through the spyware. Also, pop-up advertisements can be delivered or theft of personal information can be achieved, including users’ financial information. Recently, spyware was used by an identity theft ring to retrieve and store remotely, user information. This was identified by research conducted by an antispyware firm, Sunbelt (Vijayan, 2005).

Some Trojan Horses are security-breakers that have the ability to steal passwords and personal details and forward them through a number of ways to the fraudsters. Smart Trojan software can keep a log from keystrokes (key-loggers) or takes a screenshot when a customer is visiting a financial website and the information is then forwarded to the fraudster (news item ‘Exit old fashion phishing […]’, 2005).

6 Biometrics circumvention

Biometrics was supposed to be a countermeasure for Identity Theft. Even though it is a relatively new method for identity verification and the aim is to replace the vulnerable passwords, there are already numerous ways of the fraudsters to dump a biometric system. It can be easy to deceive biometric technology by tampering machines that read biometric data or altering the records that are contained within them. Finger prints that are left behind on scanners can be reused by breathing on the glass, cooling down the sensors to give false information, using graphite powder to dust the fingerprint and then copy it to a ‘jelly finger’ etc. Facial recognition can also be duped in some cases by playing someone’s video at the reader and gaining access to a system (Hamadi, 2004).

7 Other techniques

Other techniques, not discussed in further detail here as we focus on online ID theft, may include card cloning (Gerard et al., 2004a,b), attacks on off-line kept data (e.g. back-up copies and disaster recovery facilities) or data media in general (McKinley, 2004) and use of CCTV footage, etc.
7.1 Forensic investigation of online ID theft

Identity theft in its online form is considered as a relatively new method of fraud and there is not enough guidance for forensic investigators. The investigator will have to unfold the digital trail of evidence and try to present potential explanations of how such a crime occurred. This digital trail involves examining how a crime was committed using computers and the internet. The investigation should identify how the leak of personal information occurred that made it possible to conduct a misuse of resources such as a credit card number. It should also include details of the misuse such as dates, goods purchased and amounts spent. If it is possible the perpetrator should also be identified. The latter is perhaps one of the most challenging tasks as, unlike DNA evidence, computer records can identify user accounts that are logically, not physically, linked to individuals (Tryfonas et al., 2006).

Forensic extraction and analysis of data from a computer hard disk will detail much of this information. However, the conversion of data to evidence is a lengthy and costly process that, at the end of the process, has also to be made understandable to a jury. Therefore, there would be value in creating an analytical framework to facilitate the investigation of internet Identity Theft cases and the handling of the related digital evidence. The construction of a formalised and structured approach that would assist the computer forensic investigative practice in terms of identification of evidence, presentation in a court of Law, etc. presents an opportunity for further research.

Towards such a direction, in Table 1 the types of threats have been combined against on-line identities and the means to achieve illegitimate gains based on the research of the literature up to now. There is an initial attempt to identify and record any digital evidence that may be found per category. Other factors of concern for an investigation are also recorded, such as required skills and capability profile of the perpetrator etc. Forensics professionals could then refer to this when they have to examine a case concerning online ID Theft. The main idea is that the professional will be able to identify and understand the nature of the crime scene in future through such a systematic analytical framework.

7.2 ID theft response: detection and prevention

According to the Federal Trade Commission (FTC, 2005) the majority of people discovered they were victims by monitoring their accounts. However, it is only 50% of the victims who finally found out how thieves retrieved their personal data (DeMarrais, 2003). The majority of ID theft incidents in the UK can be traced back to a suspicious phone call (Edwards, 2005). This fact alone raises concerns about communication of individuals’ personal information and the precautions that are required when such an exchange is needed. Further to precautions on releasing personal information to not trusted sources, both individuals and organisation have to be suspicious of the ways personal data can be stolen and used for malicious reasons. According to the FTC, individuals should order a copy of their credit report from credit card bureaus in order to check whether the information held there is accurate. Personal information at home should be held in a secure place and individuals should be informed about who has access to their personal information in the workplace.
<table>
<thead>
<tr>
<th>ID theft category</th>
<th>Attacker’s profile</th>
<th>Evidence</th>
<th>Popularity</th>
</tr>
</thead>
</table>
| Phishing: may be also called carding or e-mail spoofing.  
It has the form of an official e-mail claiming to come from an online bank or retailer, because in fact is a scam that steals personal information.  
To gain/get:  
- Bank accounts  
- Cheque books  
- Credit cards  
- Loans  
- Financial account hijacking | High  
- Official e-mail or website claim  
- Unsecured wireless mediums  
- Unregistered domains  
- Graphics  
- Pop-up windows  
- URL cloning  
- Trojans  
- Key-loggers | No use of port 80, mainly use of port 4903  
E-mails – image map or with encoded URL in JavaScript  
Respond to 'SHS' web server  
Run on 'zombie' machines  
Trojan code hits exploitable machines | Growing very fast, about 56% per month (Lininger et al., 2005) |
| Web-spoofing: the method that the users believe they are on a website that actually they are not.  
Store personal information  
Use passwords and personal details for malicious reasons | High  
- redirection to the fraudster’s website  
- Web servers  
- Web page design software  
- Domain name registration  
- URL rewriting | Professionally designed web pages  
Copied web pages linked to the original  
Information is redirected and stored to the fraudster’s server  
Respond to 'SHS' web server | Growing as most users can get convinced |
<table>
<thead>
<tr>
<th>ID theft category</th>
<th>Attacker’s profile</th>
<th>Evidence</th>
<th>Popularity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spyware, viruses and Trojans: malicious software that</td>
<td><em>Motivation</em> - Infect a computer to gain access to</td>
<td><em>Malicious code</em></td>
<td>Growing at an alarming rate and considered as an explosion in privacy issues</td>
</tr>
<tr>
<td>can gain access on a system and infect it</td>
<td>personal information</td>
<td><em>Pop-up windows</em></td>
<td></td>
</tr>
<tr>
<td></td>
<td><em>Skills</em> - High and very technical</td>
<td><em>Infected websites</em></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The fraudster needs to have high standard programming</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>skills</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><em>Methods/tools</em> - Programming software</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Key loggers: tracking personal data a user may enter</td>
<td><em>Motivation</em> - Track data entered on a computer</td>
<td><em>HTTP requests routing</em></td>
<td></td>
</tr>
<tr>
<td></td>
<td><em>Skills</em> - Medium to Technical Knowledge of the</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>acquisition process and how they are used is required</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><em>Methods/tools</em> - Physical presence of the fraudster</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>required in order to install the hardware key logger</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><em>Technology</em> - Hardware key loggers are invisible</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><em>Characteristics</em> - Key logger software code can be</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>downloaded free</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><em>Popularity</em> - Keyboard events are captured and record</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>data entered</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><em>Goals</em> - Growing at an alarming rate</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 1
A categorisation of hi-tech ID theft techniques, the associated attacker's profiles and the potential digital evidence left on the crime scene (continued)
Table 1
A categorisation of hi-tech ID theft techniques, the associated attacker's profiles and the potential digital evidence left on the crime scene (continued)

<table>
<thead>
<tr>
<th>ID theft category</th>
<th>Attacker's profile</th>
<th>Evidence</th>
<th>Characteristics</th>
<th>Popularity</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Biometrics circumvention:</strong></td>
<td>To gain/get:</td>
<td></td>
<td></td>
<td>Static, however the ID Theft interest on this subject is expected to grow</td>
</tr>
<tr>
<td></td>
<td>Innovative, high</td>
<td>Loggers store information to send to the authentication machine</td>
<td>Physical access to such devices</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Knowledge of the acquisition process and how they are used is required</td>
<td>Replayed information can give access to an unauthorised person</td>
<td>Physical access is transformed to digitised</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Photograph</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Silicone</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Graphite powder</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Video screening equipment</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Low to Technical</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Depends on whether the fraudster retrieves published information or needs hacking skills to access a database</td>
<td>Internet</td>
<td>Knowledge on how to process data</td>
<td>Growing as more and more personal information is published on internet</td>
</tr>
<tr>
<td></td>
<td>Retrieve personal and private information</td>
<td>Databases</td>
<td>Access to public shared information</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Retrieve financial information</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Data retrieval:</strong></td>
<td></td>
<td></td>
<td></td>
<td>Growing as more and more personal information is published on internet</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ID theft category</td>
<td>Attacker's profile</td>
<td>Evidence</td>
<td>Popularity</td>
<td></td>
</tr>
<tr>
<td>--------------------------------------------------------</td>
<td>---------------------------------------------------------</td>
<td>-----------------------------------------------</td>
<td>------------------------------</td>
<td></td>
</tr>
<tr>
<td><strong>Storage devices and media:</strong> hard disks, USB sticks, floppy disks and CD’s, as well as stolen computers are a source for stealing personal data</td>
<td>Retrieve personal and private information</td>
<td>Low to High Technical</td>
<td>Only basic knowledge of how to extract data</td>
<td>Computers stolen, discarded or sold information</td>
</tr>
<tr>
<td><strong>PDA’s, mobile phones and Bluetooth:</strong> to wide use of PDAs, Mobile Phones and Bluetooth is a matter of deception for retrieving personal data</td>
<td>Acquire address book</td>
<td>Technical, none when the device is stolen</td>
<td>Knowledge on how to extract data</td>
<td>E-mail messages, Logs/internet activity</td>
</tr>
<tr>
<td><strong>Card cloning:</strong> an important part of Identity Thieves’ work, Card Cloning needs a person with basic technical skills in order to manipulate a card replication machine and reproduce credit cards</td>
<td>Retrieve personal details stored (even photos)</td>
<td>Simple extraction and copying of the files</td>
<td>Bluetooth technology is still insecure</td>
<td>Stolen PDAs and mobile phones</td>
</tr>
<tr>
<td></td>
<td>Gain complete access on the device</td>
<td>Forensic extraction software</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>To replicate bank account cards, credit cards</td>
<td>Low to basic technical</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The fraudster should know how to process the card replicate machine</td>
<td>Skimming devices</td>
<td>Card reader</td>
<td>Tampered ATM machines</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Card replication machines</td>
<td>Compromised ATM</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Appropriate computer software</td>
<td></td>
<td>Fradsters own card replication equipment</td>
</tr>
</tbody>
</table>
### Table 1
A categorisation of hi-tech ID theft techniques, the associated attackers' profiles and the potential digital evidence left on the crime scene (continued)

<table>
<thead>
<tr>
<th>ID theft category</th>
<th>Attacker’s profile</th>
<th>Evidence</th>
<th>Popularity</th>
</tr>
</thead>
</table>
| **Social engineering:** the method used for retrieving personal information from someone by claiming to be another person | **Motivation** To gain/get:  
- Bank accounts details  
- Passwords  
- Personal information  
**Skills** Conspicuous  
The fraudster only needs to convince the victim  
**Methods/tools**  
- Official e-mail claim  
- Official phone call claim | **Technology**  
- E-mail  
- Graphics  
**Characteristics**  
- Influence the victim’s psychology  
- Cooperation with the victim  
- Legitimate-look e-mail messages | Growing |
| **CCTV/wireless cameras:** CCTV can be monitoring the behaviour of a person, even following his steps. Often the motive is a PIN Number collection and for this reason widely used on ATM machines from fraudsters | **Motivation** How a person behaves  
- States how the thief should then behave  
**Skills** Medium to low  
The fraudster should know how to process  
**Methods/tools**  
- Camera operation  
- Knowledge of filming and processing video | **Technology**  
- Camera hardware  
- Video processing software  
**Characteristics**  
- Video tapes  
- Expensive camera equipment  
- Unofficially installed cameras | Growing as the use of cameras extends |
From an organisational point of view, the security community has now accepted that in organisations a major security threat against information comes from inside. Research has proved that 70% of the total identity thefts start from employees who steal personal data from the company they work for (Hinde, 2004). The majority of companies cannot cope with well organised attacks coming from internal sources, or even instances of an employee giving out information unintentionally (Porter, 2004). Hence, in the light of the rising figures of online ID theft, the protection of personal information of clients and other affiliates held by organisations is much more than a compliance issue. Indeed, the same FTC survey shows that $48 billion loss was of businesses and financial institutions comparing to $5 billion loss of the consumers (DeMarrais, 2003). Therefore, organisations need to become more active on how they detect and prevent ID theft. Regulatory compliance with the Data Protection Act is then a very important issue in a company’s security architecture agenda and its information security and privacy policy.

The detection controls comprise authorisation, internal auditing and whistleblower hotlines that alert the employees of the company about a committed or potential fraud underway. From a technological perspective automated detection systems that process large volumes of transaction data and look to highlight any suspicious actions based on specific patterns should be used (Porter, 2004). In addition to monitoring business information for external instances of ID theft, there is also the need to protect corporate information with references to identification and related information from the threat from within. In order to prevent such internal instances of identity theft, personal information held inside the company should be treated with the appropriate confidentiality. Information assets that contain such personal and sensitive information should be protected in terms of allowed access (Solomon et al., 2003) and destruction/disposal of those electronic or paper-based records (Gerard et al., 2004a,b).

The most common measure for protecting unauthorised access to a computer network is to use passwords. However, problems arise when users choose easily guessed words for a password. In addition, they should change their secret password regularly in order to avoid any problems (Gerard et al., 2004a,b). File encryption is commonly used as most database software packages provide built-in encryption and decryption of data. In addition, hardware or software firewalls have a wide use and are necessary in any company to limit the risk of intrusion to its network. Access logs should be kept for those files that contain personal and private data. Internal auditors of the company should have the authorisation to analyse and evaluate these audit records (Gerard et al., 2004a,b).

8 Conclusions and further research

Hardly is ID theft or a simple masquerade a new crime; however it is now fuelled by information technology resulting in high numbers of such crimes committed annually, corporate liabilities and financial loss – and of course personal inconvenience. As ID fraudsters have discovered new tools, so must forensic investigators and Law practitioners in order to be able to cope with this trend and tackle it effectively. A responsive plan should include components of prevention and detection, reaction and investigation of incidents.

However, whilst prevention and reaction can be largely covered within the organisation’s security architecture plans, given an emphasis in meaningful compliance with regulations such as the Data Protection Act, detection and investigation require new
tools and methods. Through such a perspective, we try to initiate a framework for the investigation of this crime, by recording artefacts of evidential value and creating suspect profiles against potential instances of hi-tech ID theft. Such a systematic approach to explaining ID theft will hopefully facilitate the understanding of the crime scene by the forensic investigator.

Table 1 is an initial attempt to address this issue and it demonstrates how a categorisation of ID theft incidents against the method used, the required skills behind the attack, the technologies exploited and the potential digital evidence left behind can provide an investigative insight. Potential future work would include a detailed categorisation of the majority of known ID theft attacks (or a meaningful, representative grouping of those), a detailed recording of potential evidence in the corresponding crime scenes, guidance on how to locate and extract these artefacts in an evidentially sound manner, etc. A review of secondary empirical data from published cases and public court proceedings may also complement or cross-validate this approach.

References


