foundation for both subjects. The historical disconnect between risk and marketing is certainly a factor here. At the end of the day, the goal should be to have a single source of data and understand what happens to that data as it moves through the bank, whether it is a financial reporting process, risk reporting or a customer relationship management process.

Implementing the single customer view is one of the biggest contributions that CRM can make to the Basel II effort. This includes:

- Providing a single current and historical view of each individual customer's profile and complete product portfolio
- Creating the same view for every household or demographic segment
- Detecting, storing and tracking customer events, i.e. key changes in a customer's behaviour or position within a product lifecycle. This provides a far more useful input into analytical engines than purely "static" data
- Providing reporting and analytical tools to support common needs ranging from regular reporting and ad-hoc exploration of customer data to detailed modelling of customer behaviour
- Linking analytics back to the operational environment in the form of customer treatment strategies (which translate into risk treatment strategies for Basel II)

The calm before the storm?

Although Detica's research study highlighted a number of areas for potential concern, many of them technology-related, the overall results were generally positive. This probably reflects the timing of the study, taking place as it did in the relatively quiet period between the conclusion of QIS3 (December 2002) and the publication of CP3 (May 2003). Most financial institutions, certainly the leading ones, have set up a Basel II programme, appointed a qualified leader and given full backing from senior management.

However, it is still relatively early days for Basel II programmes and in-depth IT development has yet to start for many banks. It will be interesting to witness the response from banks' IT departments once the final specifications are presented to them later this year. As one respondent from a Tier 1 bank remarked: "Achieving one hundred per cent linkage of data? Is that Nirvana?"

Author contact details

david.porter@detica.com

The Basel II survey was conducted by Metrica Research on behalf of Detica to ascertain the current situation at 55 UK banks. Interviews were conducted in early 2003. For a copy of the research report, Basel II: please contact Lucy Bartley by email: lucy.bartley@detica.com

Arson, Archaeology, and Computer Crime Investigation

Eoghan Casey

Crimes of this kind [arson] are usually carried out to leave few, if any, direct clues, and proof of criminality is far from easy to establish by circumstantial evidence[1].

At a time when there is competition to create new terms for different aspects of computer crime investigation, it may come as a surprise to find an article referencing the distant past. However, when even basic grammar is disregarded (using the noun *computer* as an adjective and the adjective *forensic* as a noun) there is a clear need to revisit our secondary school textbooks. Wit aside, it is useful to examine well-established disciplines, such as arson investigation and archaeology, to gain insight into the problems we face today in computer crime investigations. Although computer crime is a new development, there are many similarities between a computer that contains evidence and an arson crime scene or archaeological dig. Most essentially, in all cases, people are responsible for the actions that left clues behind. Additionally, as noted in the opening quotation, we are dealing with evidence that has deteriorated significantly.

An arson investigator’s task is to recover fragmentary evidence and use it to determine what occurred. Archaeologists perform similar types of analysis, studying excavated artefacts to ascertain when and where they initially existed and synthesizing the results to gain insight into the original context.

Like a detective, the archaeologist searches for clues in order to discover and reconstruct something that happened. Like the detective, the archaeologist finds no clues too small or insignificant. And like the detective, the archaeologist must usually work with fragmentary and often confusing information. Finally, the detective and the archaeologist have as their goal the comple-

Feature	Arson	Computer Crime
Dimensional expansion	Evidence may be found far from the blast or may have been projected vertically onto roofs, into trees, etc.	Evidence may be located in distant hosts. Network monitoring systems may have relevant log files
Layering	Burnt, collapsed structures create layers of evidence	Deleted data on a computer disk is layered under active data
Tools	Accelerants, explosive materials, bomb fragments, and other items found at the crime scene may have class characteristics that help connect the crime to the perpetrator	Toolkits and other items found at a computer scene may have class characteristics that help connect the . crime to the perpetrator
Secondary scenes	An arsonist's home or bomb maker's workshop generally have evidence that can be linked with the scene	Computers used by the offender to compile programs or launch an attack usually have evidence that can be linked to the scene
MO, signature, skill	The composition of an incendiary device can be unique to the offender, such as detonator or explosive mixture used, revealing the offender's skill level	Tools used by computer criminals can have unique characteristics introduced by the offender, revealing the offender's skill level

Table 1: Comparison of features in arson and computer crime

tion of a report, based on a study of their clues, that not only tells what happened but proves it.[2]

This article explores how some methodologies and techniques used in arson investigation and archaeology can be applied in computer crime investigations.

Arson and computer crime investigations

When computer criminals make no effort to conceal their activities, investigators can obtain information about the offender's behaviours from log files and other available digital evidence. However, if significant evidence has been destroyed, it is more difficult to determine what the offender intended and investigators must rely more heavily on crime scene characteristics and to understand the incident. Arson investigators are familiar with this type of situation – similarities between arson and computer intrusions are shown in table 1.

Despite a paucity of evidence and a chaotic crime scene, arson investigators have learned to methodically examine a scene for the kinds of clues that have been most useful for solving crimes in the past. Arson investigators look for several key crime scene characteristics that are applicable to computer intrusions: point of origin, method of initiation, requisite skill level, nature and intent (Table 2).

Let us first consider the nature and intent of the crime. Computer criminals and arsonists alike may destroy evidence to cover their tracks, to retaliate against some perceived wrong, and/or to demonstrate their power. To determine whether destruction was intended to inflict damage or simply as a precautionary act, it is helpful to consider whether the targeting was broad or narrow. Narrow targeting refers to any destruction that is designed to inflict specific, focused, and calculated amounts of damage on a specific target such as targeting "/home/janedoe" in Table 2. Broad targeting refers to destruction that is designed to inflict damage in a wide reaching fashion. Rather than targeting a single individual by deleting their files, an intruder might delete information that is important to the entire organization, targeting the entire organization or what it represents as in the following case example.

Case example

Tim Lloyd, the primary system administrator for Omega Engineering Corporation, was originally fired for stealing expensive equipment. In retaliation, Lloyd executed time-delayed commands on Omega's primary server that deleted all of the company's important data and programs on a specific date. Specifically the method of initiation was a modified version of the **DELTREE** command (**"FIX /Y F:\*.*"**) to delete everything on the drive combined with the **"PURGE F:\ /ALL"** command to obliterate the deleted data. A high degree of skill was required to implement this narrowly targeted attack and the intent was to destroy all of Omega's important data and programs. Lloyd also erased all related backup tapes. Experts spent years recovering pieces of information from the servers, desktops, and even computers of ex-employees. Although the damage was

Crime	Point of Origin	Method of Initiation	Requisition	Nature and Intent
Arson	Warehouse window	Matches and crude fuse (cotton rag soaked in gasoline)	Low (simple Moltov cocktail - readily available materials	Broad targeting (destroy warehouse)
Arson	Engine (front of car)	Electric arc (triggered by car ignition)	High (car bomb made with military grade explosives)	Narrow targeting (kill car driver)
Intrusion	SSH server (port 22)	Buffer overflow (CRC-32 compensation attack detector vulnerability)	Low (exploit freely available on Internet)	Narrow targeting (break into server)
Intrusion	/dev/.pts (cwd of process)	Rootkit (t0rnkit) script	Medium (rootkit available on Internet)	Concealment (precautionary act)
Intrusion	/home/janedoc (cwd of process)	“sudo rm -rf ../johndoe/*”	Low (simple Unix command)	Narrow targeting (delete user files)

Table 2: Comparison of crime scene characteristics in arson and computer intrusions where "cwd" refers to the current working directory of a process (where it was started)

extensive, this attack is considered narrowly targeted because it was designed to inflict a specific damage on a specific target.[3]

In this case, the nature of the crime was malicious and Lloyd’s intent was to punish his former employer for perceived wrongs. This case example also demonstrated that, in addition to knowing the perpetrator’s intent, determining who had access to the point of origin or method of initiation can lead to prime suspects. For instance, in Table 2 only a few people had access to the point of origin “/home/janedoe” and the method of initiation “sudo”, reducing the suspect pool to Jane Doe and others with administrative privileges on the system. In the previous case example, digital evidence recovered from the damaged system immediately implicated Lloyd because he was the only individual with the requisite access to the point of origin and ability to create the destructive program.

Determining skill level can also lead to suspects. The skill level and experience of a computer criminal is usually evident in the methods and programs used to break into and damage a system. For instance, an offender who uses readily available software and chooses weak targets for little gain is generally less skilled and experienced than an offender who writes customized programs to target strong installations. A skilled computer criminal might create a time bomb specifically designed to destroy important data at a particular time or when a certain triggering event occurs as in the previous case example. Having said this, a skilled offender can successfully achieve specific goals using programs that exist on the system. Therefore, what is known about point of origin, method of initiation, and nature and intent of the destructive act should all be taken into account when assessing the offender’s skill level.

Notably, precautionary acts – destroying data to conceal, damage, or destroy any items of evidentiary value – are not always very thorough. Items that an intruder intended to destroy can be examined by digital evidence examiners to exploit them for their full evidentiary potential, no matter how little debris is left behind. For example, if a small portion of a deleted file remains on a disk, this remaining digital evidence should be carefully reconstructed and examined to determine why the offender tried to destroy it.

Archaeology and computer crime investigation

Ultimately, computer crime investigators are responsible for determining what happened, who caused the events when, where, how, and why. To achieve these goal, they primarily rely on available evidence and witness interviews. Similarly archaeologists use artefacts at a site along with supporting reports such as inscriptions, ancient texts (and interviews with descendents when available) to develop a picture of what occurred, when, where, and how. Archaeologists are also interested in understanding the people represented in the artefacts, although not to the same degree as investigators who view offenders as the end point in their work.

Over the years, archaeologists have developed methodologies for combining fragmentary evidence to create temporal, relational, functional reconstructions that provide a more complete picture of the context. A simple example of a temporal reconstruction is a timeline. To more accurately determine when events occurred, archaeologists developed techniques such as carbon dating and dendrochronology. Although these do not have an obvious translation in the digital realm, other techniques such as stratigraphy can apply.

Stratigraphy is the scientific study of layers (a.k.a. strata) with the aim of determining the origin, composition, distribution, and time frame of each stratum. Applying this concept to data stored on a disk can be fruitful in computer crime investigations. For instance, when the creation time of a document is at issue, an examination of how data is positioned and overlaid on the disk may give a sense of when the document was created. If part of one document is found to be overwritten by another document, there is a good chance that the overwritten document was created first. This concept was applied in an extortion case to demonstrate that the suspect had created a document before leaving.

Case example

During the investigation of an alleged blackmail attempt, a number of fragments of deleted material were recovered from a computer belonging to Mr S. These fragments when subjected to an analysis procedure provided a recognized sequence of revisions and changes to the blackmail letter over a period of time. Mr S had been on holiday for two weeks and although admitting that he had written a similar letter, he suggested that the letter had been modified on his computer by someone else during his absence. It was not possible to ascribe a reliable date or time to all of the fragments and in any case computer dates and times indicate only the setting of the internal clock and may have no relevance to real world dates and times.

It happened however, that one of the fragments was in what is known as the “slack space” of another file (the owning file). The significance of this is that it is technically possible to show that the contents of slack space must have existed on the machine before the creation of the owning file. In this case the owning file was a letter to Mr S's bank manager and the date marking on the file was two days before Mr S went on his holiday. The bank manager was able to confirm receipt of the letter a day after the indicated date. Thus it could be shown that that fragment of the blackmail letter together with all previous fragments existed on the computer at least two days before the holiday. It will be seen that the content of the letter was immaterial except insofar as it enabled the bank manager to identify it unequivocally.[4]

Archaeology has many other techniques for studying relationships between artefacts that can be translated into the digital realm. For instance, when attempting to determine where a piece of digital evidence came from, a digital evidence examiner is essentially being asked to compare items to determine if they are the same as each other or if they came from the same source. The aim in this process is to compare the items, characteristic by characteristic, until the examiner is satisfied that they are sufficiently alike to conclude that they are related to one another. Ultimately, this comes down to probabilities. What is the probability of two similar items occurring independently? Archaeologists have been dealing with this and other questions for centuries that have parallels in computer crime investigation.

Summary

In this article, several methodologies and techniques from arson investigation and archaeology were applied to computer crime investigations. This is merely a sampling to demonstrate the potential of taking advantage of past work in these fields to address challenges that we face today. Analysis techniques from these fields can help us exploit evidence in computer crime investigations to determine the nature and intent of the act, the skill level of the offender, and other important characteristics that can narrow the suspect pool. Reconstruction methodologies used in these fields are already applied in computer crime investigation (e.g., timeline and link analysis) but only in a rudimentary manner. More advanced temporal and relational analysis methods have been developed in archaeology and can be used in computer crime investigation. Additionally, it can be illustrative to find out how a well-established field like arson investigation deals with routine issues such as procedures, investigator fatigue, and case management. Finally, these other disciplines can give us ideas for areas of new research in digital realm.

References

[1] Gross, H. (1924), Criminal Investigation, Sweet & Maxwell, pages 10-12

[2] Meighan, C. W. (1966), “Archaeology: An Introduction”, Chandler Publishing Co., page 18

[3] Gaudin, S. (2000), "Case Study of Insider Sabotage: The Tim Lloyd/Omega Case", Number 3, 2000, Computer Security Journal, Volume XVI

[4] Bates, J. (1997), International Journal of Forensic Computing, (http://www.forensiccomputing.com/archives/judicial.html)

About the author

Eoghan is currently a System Security Administrator for Yale University, where he investigates computer intrusions, cyberstalking reports, and other computer-related crimes, and assists in the research and implementation of university wide security solutions. He is author of Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet as well as editor of the Handbook of Computer Crime Investigation. Eoghan is a full partner and instructor with Knowledge Solutions LLC.