Introducing Traffic Analysis

George Danezis and Richard Clayton

January 26, 2007

1 Introduction

In the Second World War, traffic analysis was used by the British at Bletchley Park to assess the size of Germany's air-force, and Japanese traffic analysis countermeasures contributed to the surprise of their 1941 attack on Pearl Harbour. Nowadays, Google uses the incidence of links to assess the relative importance of web pages, credit card companies examine transactions to spot fraudulent patterns of spending, and amateur plane-spotters revealed the CIA's 'extraordinary rendition' programme. Diffie and Landau, in their book on wiretapping, went so far as to say that "traffic analysis, not cryptanalysis, is the backbone of communications intelligence" [1]. However, until recently the topic has been neglected by Computer Science academics. A rich literature discusses how to secure the confidentiality, integrity and availability of communication content, but very little work has considered the information leaked from communications 'traffic data' and how these compromises might be minimised.

Traffic data records the time and duration of a communication, and traffic analysis examines this data to determine the detailed shape of the communication streams, the identities of the parties communicating, and what can be established about their locations. The data may even be sketchy or incomplete – simply knowing what 'typical' communication patterns look like can be used to infer information about a particular observed communication.

Civilian infrastructures, on which state and economic actors are increasingly reliant, are ever more vulnerable to traffic analysis: wireless and GSM telephony are replacing traditional systems, routing is transparent and protocols are overlaid over others – giving plenty of opportunity to observe, and take advantage of the traffic data. Concretely, an attacker can make use of this

information to gather strategic intelligence, or to penetrate particular security protocols and thus violate traditional security properties.

In this short introduction to the topic, we will highlight the key issues around traffic analysis. We start with its military roots and present the defences that the military have developed. We then consider how traffic analysis is being used in modern civilian contexts. We move on to specific 'Computer Science' issues, and provide an overview of the relevant research literature on attacks and defences in contemporary networks. Finally, we discuss some of the current, rather contentious, policy issues relating to the retention of traffic data.

2 Military Roots

Traffic analysis is a key component of signal intelligence and electronic warfare. In his book 'Intelligence Power in Peace and War' [2] Michael Herman, who has served as chair of the UK Joint Intelligence Committee, discusses how information about messages (which he calls "non-textual" to distinguish it from the message content) is capable of establishing "targets' locations, order-of-battle and movement". He goes on to make the comparison that even when messages are not being deciphered, traffic analysis "provides indications of his [the enemy's] intentions and states of mind, in rather the same way as a neurologist develops insights about a silent patient by studying EEG traces from the brain".

Traffic analysis was used by the military even before the invention of wireless communications, but it was the broadcast nature of radio, permitting anyone to listen in, that transformed its usefulness. The first naval action of the First World War, on 5 August 1914, was the cutting of Germany's trans-Atlantic cables by the British cable ship Telconia [3], so that wireless telegraphy would have to be used instead of hard-to-intercept cable communications. Traffic analysis became an extremely potent source of intelligence as wireless communication became more widespread, particularly in naval and air operations. Ships at sea had to balance the value of communicating against the threat of being detected via direction finding if they transmitted. When transmitting, strict standards, governing call-signs and communication procedures, had to be adhered to in order to minimize the information that traffic analysis could provide.

Another example of traffic analysis providing valuable intelligence (by Herman [2]) is the British

reconstruction in 1941 of the structure of the German Air Force radio network. This confirmed that a unit was composed of nine and not twelve planes, which led to a more accurate estimate of total strength. Identification of radio equipment was also used for accurate detection of redeployments: each transmitter can be 'fingerprinted' by characteristics such as unintentional frequency modulations, the shape of the transmitter turn-on signal transient, the precise centre of frequency modulation and so on. These fingerprints can be used to track the device even though the messages it is transmitting are in an unbreakable code. Similar techniques can be used today to identify GSM phones [4]. In World War Two, radio operators became skilled at recognizing the 'fist' of other operators, i.e. the characteristic way in which they typed their Morse code. Indeed, prior to Pearl Harbour, the Japanese transferred their aircraft carrier radio operators ashore and took replacement crew, in order to persuade any eavesdropping Americans that the Japanese fleet was still in port. Even in more modern times, as the 'Desert Storm' campaign began in 1991, the British 'Operation Rhino' replayed radio traffic from an exercise a few weeks earlier, and thereby misled the Iraqi forces as to where they were attacking [5].

Intelligence does not necessarily come from radio communications. The recording of aircraft identification numbers, by amateur plane-spotting enthusiasts the world over, permitted the reconstruction of recent CIA activities, and helped to prove the existence of their 'extraordinary rendition' programme, which transferred terrorist suspects to third countries, for imprisonment and interrogation [6].

It might be wondered why traffic analysis is so valuable to the military? The technique, although impressive in what it can determine, necessarily provides lower quality information when compared with cryptanalysis and recovery of message content. However, it is both easier and cheaper to extract and process traffic data than content. It is easier, because ciphers need considerable effort to break (when they break at all). It is cheaper, because traffic data can be automatically collected and processed to provide high level intelligence. Computers can collect traffic data and map out structures and locations, whilst a skilled human operator is needed to listen to every radio transmission (often in a foreign language) in order to extract intelligence. For these reasons, traffic analysis is often used to perform 'target selection' for further intelligence gathering (such as more intensive and expensive surveillance), jamming or destruction. Given the enormous amount of communication and information on public networks we can expect these 'economics of surveillance'

to be ever more relevant and applicable.

An insight into the power of traffic analysis in the military setting, and its relationship with code breaking techniques, can be obtained by working through the Zendian Problem [7]. This is a series of problems concerning a fictitious operation against the totalitarian island of Zendia, that were used on a course taught to US National Security Agency (NSA) cryptanalysts in the late 1950s, and that have now been declassified.

Signals Intelligence (or Sigint), the military term for techniques that include traffic analysis, is an arms race, and many 'low probability of intercept and position fix' communication methods have been devised by the military to minimize exposure to traffic analysis and jamming (a key reference here is Anderson [4]). Their principles of operation are simple: scanning many frequencies can only be done at some maximal rate and a great deal of power is necessary to jam a wide part of the frequency spectrum. Therefore, the first technique used to evade interception, and foil jamming was 'frequency hopping', now used in commercial GSM communications to improve reliability in the face of environmental noise. The basic technique is for Alice and Bob to share a key that determines, for each given time period, the frequency at which they will transmit. Eve, on the other hand, does not know the key and has to observe or jam the entirety of the frequency spectrum that may be used. In practice, hopping is cheap and easy to implement, and makes it difficult to jam the signal (given that the hop frequency is high enough), but it is poor at hiding the fact that communication is taking place. It is mainly used for tactical battlefield communications, where the adversary is unlikely to have very large jammers to hand.

A second technique is called 'Direct Sequence Spread Spectrum' (DSSS). This transforms a high-power low-bandwidth signal into a high-bandwidth low-power signal, using a key that is shared between Alice and Bob. It is easy for them to pick out the transmitted signal, using their key, but an adversary will have to try to extract the signal from the noise, a difficult task given its low power (that will ideally be under the noise floor). DSSS has also inspired commercial communication systems and is now used in ADSL and cable modems as Code Division Multiple Access (CDMA). Its most significant implementation problem is synchronization, and the availability of a reference signal (such as GPS) is of great help when implementing a practical system.

The final technique in the arsenal against interception is 'burst communication'. The key idea is to communicate in a very short burst, so as to minimize the probability the adversary is monitoring

the particular frequency being used at the relevant time. A cute variant of this is meteor scatter communications, using the ionization trail of small meteorites hitting the atmosphere to bounce transmissions between special forces troops in the field and a base station. Meteor scatter can also be used in civilian applications when low bandwidth, high latency, but very low cost and high availability communications are required.

3 Civilian Traffic Analysis

Contemporary sociology models groups of individuals, not as a mass or a fluid, but in terms of their positions within a 'social network'. The paradigm that underpins much of this research is that the position of an agent in the social network is in many ways more characteristic of them than any of their individual attributes. This position determines their status, but also their capacity to mobilize social resources and act (social capital). This position can also be determined via traffic analysis, yielding a map of the social network, and the position of each actor within it.

Social Network Analysis [8], and experimental studies, have recently gained popularity and led to interesting results that are of use not only to traffic analysis, but also to network engineering more generally. It was first noted by Milgram [9] that typical social networks present a 'small world' property, in that they have a low diameter (experimentally determined to be about six hops between any two members) and are efficiently navigable. In other words there are short paths (i.e. intermediaries) between you and anyone else in the world, and you can find them efficiently: think of using hints from location and profession. This work has been used to build efficient peer-to-peer networks, but remains underused in security and trust analysis. Another key finding is that 'weak links' – people you do not know all that well – are instrumental in helping you with activities that are not commonplace but still very important. A well studied example is finding a job, where people using 'far links' are on average more successful, than those who limit themselves to their local contacts [10].

The first mathematical studies [11] of social networks (or 'power law networks' as they are often described because of the degree distribution of their edges) tell us a lot about their resilience to failure. It turns out that they are extremely resistant to random node failures, meaning that they stay connected and maintain a low diameter even when many random nodes have been removed.

On the other hand, such networks are very sensitive to the targeted removal of the nodes with high degree. After a few nodes have been removed the network will become disconnected, and well before that the diameter increases substantially. An equally effective attack is for an adversary to remove nodes according to their 'between-ness', i.e. how many other nodes in the network they are connected to. Traffic analysis can be used to select the appropriate targets to maximize communication degradation and disruption.

Carley *et al.* [12] proposed using network tools to disrupt networks of terrorists, and addressed the issues raised when multiple agents were involved, so that removing a single 'leader' would be effective. Garfinkel [13] considers the 'Leaderless Resistance' model of self-organising independent cells without any central control. He notes that it is "a desperate strategy employed by movements that do not have broad popular support and that fear infiltrators" and makes a number of policy suggestions for combating it. More recent research by Nagaraja and Anderson [14] tries to find strategies for a peer-to-peer network of nodes to resist node deletion attacks. The intuition behind these defensive strategies is that nodes connect to other random nodes in order to get resilience, while connecting according to a power law strategy to get efficient routing. When under attack the network regenerates links to maximize fault tolerance, when things are calmer it reconfigures itself to be efficient.

Social network analysis is starting to be used for criminal intelligence [15, 16]. Investigators try to map out criminal organisations by the use of traffic analysis techniques on telephone or network traffic and location data. This can be used to select targets for more intensive surveillance, and also to select appropriate targets for arrest and prosecution. Often these arrests are aiming to maximally disrupt the organization targeted. It is not always appropriate to arrest the most central or the most well-connected member – this would merely serve as a promotion opportunity for smaller crooks to take up the position. It is found to be more effective to arrest the 'specialists', i.e. those people in the organization that have a unique position or skills, that others would find difficult to fill. Examples include those who can forge papers, or crooked customs officials.

Similar techniques were used by the US military to locate Saddam Hussein in 2003. Tribal and family linkages were used to identify particular individuals with close ties to him, and these were selected for closer surveillance [17]. The latest (December 2006) US Army Counterinsurgency Manual now specifically deals with social network analysis, and discusses the Saddam Hussein

operation as an example [18]. The ties between the 9/11 conspirators have also been mapped, and these connections clearly pick out Mohamed Atta as the central figure [19]. Additionally, Dombrowski *et al.* [20] show how it is possible to predict the shape of a social network only some of whose members and links are known.

Moving away from social links, in the 1970s the German police searched for Baader-Meinhof safe-houses by analysing gas and electricity records, looking for rented apartments with spikes in fuel usage where the bills were paid by transfers from banks in different parts of the country. Thirty years later, the UK police search for cannabis farms (where the plants are in kept warm in artificial sunlight) by looking for unusually heavy usage of electricity – or, if the meter has been overridden, a mismatch between the power consumed in a locality and that which is billed for: an infra-red scan from a helicopter will then locate the house which is warmer than its neighbours. In more academic work, Fawcett and Provost [21] show how data mining techniques can be used to detect cellular phone fraud, with their automated approach proving better than hand-crafted detection rules.

Traffic analysis inspired techniques can also be used to protect systems and build trust. Advogato [22] is a social network based system, that provides a community for free software developers. The fact that they introduce each other allows the system to establish whether an author is likely to be a spammer, and filter their messages out. Gibson *et al.* [23] observed that the apparently anarchic structure of web page links could be seen to comprise of many communities with central 'authoritative' pages linked by 'hub pages'. Google's PageRank [24] uses techniques that are very similar to web-page and social network profiling – in that it considers pages that are more central in the network (with more links pointing to them) as more authoritative. Techniques have also been devised [25] to automatically detect and extract web communities. These results can be used both to assist and to attack users.

In a different milieu, Renesys Corporation monitors the Internet's global routing table and analyses the BGP protocol traffic sent by service providers as they announce which blocks of IP addresses they will carry traffic for. Analysis of this data permits Renesys to generate 'market intelligence' indicating when major ISP customers are starting to move to new providers, when ISP market share is changing, or the impact of mergers or acquisitions on customer numbers [26].

4 Contemporary Computer and Communications Security

Traffic analysis techniques can naturally be applied to Internet communications. Secured systems can be successfully attacked, and sensitive information extracted. However, a key difference to keep in mind when studying civilian traffic analysis research is that the attackers are generally far from omnipotent. It is not military powers, with large budgets and the ability to intercept most communications that worry us, but commercial entities, local governments, law enforcement, criminal organizations and terrorist networks that have become the adversary. Therefore research has focused on attacks and solutions that can be deployed at low cost, and provide tangible tactical benefits (a pass phrase, a record of web accesses, ...). Beyond this, more strategic work is beginning to be done on the ways in which Internet traffic analysis can be of use to law enforcement, along with practical approaches for ensuring that routine surveillance can be evaded.

So what can we do if we are not allowed to look at the plaintext content?

4.1 The Traffic Analysis of SSH

The secure shell protocol (SSH) permits users to log in remote terminals in a secure fashion. It does this by performing authentication using a public keyring, with the private keys accessed locally via a passphrase. It subsequently encrypts all information transmitted or received, guaranteeing its confidentiality and integrity. One would think that any subsequent password entry (that might be required to log in to further remote services), over an SSH connection, should be safe. However, Song *et al.* [27] show that there is a lot of information still leaking. In interactive mode, SSH transmits every key stroke as a packet and hence the password length is trivially available.

However, because keyboard layouts are not random, and passwords are often based upon real words, the exact timing of the keystrokes is related to how quickly one particular character can be typed after another. Hence more advanced techniques, using hidden Markov models, can be used to extract further information from inter-packet timing and lower the effective entropy of the passwords, thereby making brute force guessing far easier.

It turns out that you do not need to measure the typing abilities of the person entering the password and another user can be used to build a profile, because the similarities between users are exploitable. This links in with subtly different results from Monrose and Rubin's [28] research

on identifying and authenticating users using keystroke dynamics. Although their focus was on biometrics and authentication their results have a clear relevance to the traffic analysis of SSH. They show that there can be enough variability in typing patterns between users to be able to identity them, particularly after a long sequence has been observed. As a result, not only the content of your communications may be leaked but also your identity – despite all of confidentiality that SSH apparently affords.

4.2 The Traffic Analysis of SSL

The Secure Socket Layer (SSL), and its close friend Transport Layer Security (TLS), were introduced primarily to provide private web access. HTTP protocol requests and replies are encrypted and authenticated between clients and servers, to prevent information from leaking. Yet there is plenty of research [29, 30, 31, 32, 33] to suggest that information is leaking out of this shell.

The key weaknesses come down to the shape of traffic that is inadequately padded and concealed. Browsers request resources, often HTML pages, that are also associated with additional resources (images, stylesheets, ...). These are downloaded through an encrypted link, yet their size is apparent to an observer, and can be used to infer which pages are accessed (for example, it would be possible to tell which specific company reports were being downloaded by an investment banker – with consequent possibilities for profitable stock trading). There are many variants of this attack: some attempt to build a profile of the web-site pages and guess from that which pages are being accessed while others use these techniques to overcome naive anonymizing SSL proxies. In the latter cases, the attacker has access to the cleartext input streams and he tries to match them with encrypted connections made to the proxy.

It should be noted that latent structure and contextual knowledge are of great use when extracting information from traffic analysis. Levene and Loizou [34] provided a theoretical basis for computing the entropy of web navigation and demonstrated that this 'surfing' should not be seen as just random. Danezis [32] assumed that users will usually follow links between different web resources. By learning just the approximate lengths of the resources that were accessed, he showed that a hidden Markov model can be used to trace the most likely browsing paths a user may have taken,. This approach provides much faster and more reliable results than considering users that browse at random, or web-sites that have no structure at all.

4.3 Web Privacy

Can a remote web server that you are accessing tell if you have also been browsing another site? If you were looking at a competitor's site then maybe giving you a better price might be in order!

Felten *et al.* [35] show that it is possible to use the caching features of modern web browsers to infer information about the web-sites that they have been previously browsing. The key intuition is that recently accessed resources are cached, and therefore will load much more quickly than if they had to be downloaded from the remote site. Therefore, by embedding some foreign resources into a served page, the attacker's web-server can perform some timing measurements, and infer particular previous browsing activity.

Note that this attack can be performed even if the communication medium is anonymous and unlinkable. Most anonymization techniques work at the network layer, making it difficult to observe network identities, but perform only minimal filtering in higher layers. The presence of caches leads to the Felten attack, but doing away with any caching would be a major problem for anonymous communication designers, since it is important to use any efficiency improvements possible to make the, already slow, browsing more usable.

4.4 Network Device Identification and Mapping

Can you tell if two different addresses on the Internet are in fact the same physical computer? Kohno *et al.* at CAIDA [36] have devised a technique that allows an attacker to determine if two apparently different machines are the same device. They note that the clock skew (the amount by which the clock drifts per unit of time) is characteristic of a particular machine, differing even amongst otherwise identical models from the same manufacturer. Therefore, if the clock drift of two remote machines seems to match for a long time, it is possible to conclude that there is just one machine present. The technique they use is resistant to latency, and can be applied remotely, even if the target machine synchronises its clock with NTP.

The technique can be used in forensics to link visiting machine identities together, and to determine if two web-sites are hosted on the same consolidated server. Equally, it can be used by hackers to detect if the multiple machines they are accessing are merely different versions of a virtualized honey-pot machine.

Murdoch [37] has extended this work by observing that the clock skew will change as the temperature changes. He has shown that by modulating the amount of traffic sent to a machine he can affect the amount of work it must do, and he can detect the resultant changes in system temperature by examining variations in the clock skew. Hence, if he accesses a 'hidden' machine via an anonymizing overlay network (such as Tor [38]) and varies how much traffic he sends to it, then it will heat up and cool down as the workload changes. If he can observe a corresponding pattern of clock skew change on a candidate machine to which direct access is possible, this is sufficient to link that machine to the hidden identity – and the anonymization scheme is overcome.

The opposite question of is often of interest – are machines physically different? Given two connections originating from the same network address, have they actually been initiated by one or multiple machines? It can be of particular relevance to count the number of machines behind NAT (Network Address Translation) gateways and firewalls. Bellovin [39] noted that the TCP/IP stack of many operating systems provides a host specific signature that can be detected, and used to estimate the number of hosts behind a gateway. To be exact, in many operating systems at that time, the IPID field, used as a unique number for each IP packet, was a simple counter that was incremented every time a packet is transmitted. By plotting the IPID packets over time, and fitting lines through the graph, one could estimate the number of unique Windows hosts. However, this technique is becoming less effective because many systems now scramble the IPID field to prevent 'idle scanning' (as discussed further below) and so more complex analysis would now be necessary.

In IPv6 (the latest Internet protocol version) device addresses consist of a 64-bit network prefix and a 64-bit network identifier. This identifier needs to be unique, and initial proposals were for it to be constructed from the 48-bit Ethernet MAC address for the interface. However, this provides a way for remote systems to link visits from the same mobile machine, despite them coming from different network locations. Narten and Draves (RFC3041) [40] developed a 'privacy extension' for allocating identifiers randomly, and Aura (RFC3972) [41] documented a method of creating IPv6 addresses that are bound to a public key, so that machines could formally demonstrate address ownership without disclosing their identity to remote systems. However, Escudero Pascual [42] criticises these schemes, particularly because it is possible for remote machines to determine that visitors are using privacy preserving addresses – which may of itself be sufficient to make their traffic stand out.

Finally, many network mapping techniques have been introduced in the applied security world, and included in tools such as `nmap` [43]. The key operations that such tools perform are scanning for network hosts, scanning for open network ports on hosts, and identifying the operating systems and services running on them – this info being used to assess whether they might be vulnerable to attack. The degree of sophistication of these tools has increased with the deployment of network intrusion detection (IDS) tools, such as the open source `snort` [44], that can detect the scanning activities. `nmap` now can be configured to detect hosts and open ports using a variety of techniques including straightforward `ping`, TCP connect, TCP SYN packet, but also indirect scans. For example, idle scanning involves forging a TCP open (SYN) packet claiming to be from a third-party machine and destined to the target. It is possible to determine whether the target was prepared to accept the connection (it will send SYN/ACK) or if the port is 'closed' (it will send RST or nothing). This is done by determining if the IPID value of the third-party machine has been altered by the sending of a RST in response to the unexpected (to it) SYN/ACK. The obvious advantage is that any IDS system at the target will believe that the third-party machine is the instigator of the scan. The full `nmap` documentation is well worth a read [45].

4.5 Detecting Stepping Stones

Much work has been done by the intrusion detection community to establish if a host is being used as an attack platform [46, 47]. The usual scenario involves a firewall that sees incoming and outgoing connections, and tries to establish if a pair of them may be carrying the same stream. This might mean that the internal machine is compromised and used to attack another host, i.e. it is a 'stepping stone' for the attacker to hide their identity.

The two main classes of techniques for detecting stepping stones are 'passive', where the firewall only observes the streams, and 'active', where the stream of data is modulated (often called 'watermarked'). Since an adversary is controlling the content of the stream, and maybe encrypting it, both types of detection rely on traffic data – usually the correlation between packet inter arrival times – to match incoming and outgoing streams. The family of traffic analysis techniques that arise are similar to those that are used to attack anonymous communication channels.

The key result in this area [48, 49] is that if the maximum latency of the communication is bounded there is no way of escaping detection in the long run. This result is of course tied to a

particular model (the adversary can match packet for packet, which is not obvious if the streams are encrypted under different keys or mixed with other streams), and 'covert' channels out of its scope may prove it wrong and escape detection. It is worth observing that an arbitrary set of active detectors is extremely difficult (maybe even impossible) to defeat.

5 Exploiting Location Data

Wireless communication equipment often leaks location data to third parties, or wireless operators. The extent to which this data can be used to degrade security properties is still to be seen, but some experiments have already been performed, and their results are a precursor of a much richer set of attacks to come.

Escudero Pascual [50] describes an experiment he set up at the 'Hacker's at Large' (HAL) summer camp. The camp had multiple wireless LAN access points, which recorded the wireless MAC address of the users whose traffic they handled. This provided a time-map of users' movements throughout the event, including clues about which talks they attended (the access points were related to the venues). Even more striking were the inferences that could be drawn about the relationship between users: random pairs of users could be expected to have a low probability of using the same access point at any time and access point usage between them should be uncorrelated over time. As a result, any above average correlation between two users, is indicative of a social relationship between the users, i.e. they are consistently moving together at the same time around the camp.

Intel Research at Cambridge designed a similar experiment. Members of staff were issued with Bluetooth devices that would record when another transmitting Bluetooth device was in range. The idea was to measure the ambient Bluetooth activity, not only to tune ad-hoc routing protocols for real world conditions, but also to establish how often a random pair of devices meet – thereby establishing how effective the ad-hoc communication infrastructure would be for two way communications. To the surprise of the researchers analyzing the data, the devices of two members of staff were found to be meeting each other rather often at night – which led them to draw conclusions about their, otherwise undisclosed, relationship.

This is completely in line with evidence gathered by the MIT 'Reality Mining' project [51].

The project distributed about a hundred mobile phones to students and staff of the Media Lab, under the condition that all their traffic data (GSM, Bluetooth and location data) could be used for analysis. The users were also asked to fill in forms about themselves and who they considered to be their friends or colleagues. The traffic data and questionnaires were then used to build classifiers: it turned out that calling or being with someone at 8pm on a Saturday night is a very good indicator of friendship.

They also uncovered location signatures that could differentiate a student from a member of staff. What is even more impressive is that they did not use the physical locations to draw inferences, but instead the frequency at which they were found to be at places designated as 'work' or 'home'. Students tended to have a more uncertain schedule, while members of staff were much more predictable in their habits. This of course led to research about the amount on entropy that location data provides, and as might be expected, for some individuals if one is given a set of locations and time, it is possible to predict with high probability their next move and new location.

So the evidence from these preliminary studies is highly suggestive that whatever the wireless medium used, mobile phone, wireless LAN or Bluetooth, sensitive information about your identity, your relations to others and your intentions can be inferred merely though traffic analysis.

6 Resisting Traffic Analysis on the Internet

A relatively old, but only recently mainstream, sub-area of computer security research is concerned with 'anonymous communications' and more generally communications that do not leak any residual information from their meta data. The field was started by Chaum [52], introducing the 'mix' as a basic building block for anonymity, and has continued since, adapting the techniques to provide private email communications and more recently web-browsing. A thorough overview of the field and key results is available in two recent PhD theses by Danezis and Serjantov [53, 54].

Fielded anonymous communication systems, that are the direct products of twenty years of research, include Mixmaster [55] and Mixminion [56] for email, and JAP [57] and Tor [38] for web-browsing. They all increase the latency of communication and its cost in terms of traffic volumes.

A range of traffic analysis attacks have been used to degrade the security of anonymous commu-

nications networks. Long term intersection attacks (also referred to as disclosure attacks) exploit long term observations of input and output messages to detect communicating parties. These attacks [58, 59, 60, 61] consider the anonymity network as a black box, and only observe parties sending and receiving messages. The key observation is that for anonymous communications to be usable, the latency of messages has to be bounded. As a result, the act of sending a message is correlated in time, albeit not exactly, with observing the corresponding massage being received. An adversary can therefore observe the anonymity system for a sufficiently long period to obviate the lack of exactness, and infer the communication relationships between different users, and in turn de-anonymize the messages. Since this family of attacks in not concerned with the internals of the anonymity network, it is considered to represent a fundamental limit on how well any such technology can protect users against traffic analysis.

Stream traffic analysis has been used to trace web requests and replies through low-latency networks. Such attacks make use of the timing of the packet streams transferred by each anonymizing relay to follow the connection between the communicating parties. Packet counting is the simplest variant – an adversary simply counts the number of packets in a certain time interval and tries to match it with the number of packets on another network link [54]. Low-latency anonymity systems are required to transport packets so quickly that this attack is often possible. A slightly more sophisticated method involves creating a template (a probabilistic model) of the stream to be traced, and matching it with other streams [53]. Unless a very strict traffic regime is imposed, with the side effect of slowing down data transfer or adding large amounts of dummy traffic, such attacks will always be successful in the long run. As a result, stream tracing attacks also represent a fundamental limit on the anonymity of low latency systems.

Finally, the attacker can infiltrate the network or try to influence the way in which honest nodes chose paths to anonymize their traffic. An important study of the effect of insiders on the security of anonymity systems is presented by Wright *et al.* [62], along with the predecessor attack on the crowds anonymity system. Crowds implements a simple pass-the-parcel algorithm to anonymize traffic: messages are passed from one node to the other, until one of them – with some preset probability – sends it out onto the network. Only link encryption is used, and the intention is that anonymity will be achieved because although nodes will know the content of messages, they will be unable to tell who the initial sender of the message was. The predecessor attack relies upon nodes

having persistent patterns of communications. This means that the actual initiator will appear as the predecessor of a particular message or request rather more often than other random nodes (that merely relay the communications).

Lately, attacks have focused on weaker adversaries, such as those considered by the Tor system, and it has been shown that some forms of traffic analysis can be performed without even having any access at all to the actual data streams to be traced. In particular, remote network monitoring techniques have been used to lower the anonymity of Tor [63]. Streams travelling over the same infrastructure influence each other's timing, and therefore can be used by an adversary to perform traffic analysis on remote hosts. Similarly, as already mentioned, covert channels based on the effects of temperature on clock drift can be used to de-anonymize servers [37]. The fact that even such minuscule phenomena can be used to perform traffic analysis against hardened systems illustrates how difficult the task of securing systems against traffic analysis is. It also illustrates that so little importance has been paid to securing public networks against traffic analysis that the information leaked can be detected and abused far, far away from its source.

Source and destination network addresses are not the only raw material for traffic analysis: the timing characteristics of encrypted traffic on a link, such as its frequency or particular bursts, may also reveal information to a third party (as seen with the examples of SSL and SSH). Military and diplomatic circles have long been avoiding this problem by using line encryptors that fill a leased line with ciphertext, no matter if any information is being transmitted. This prevents an enemy noticing that traffic has either increased (or indeed decreased) as the result of an event (as, apocryphally, it is said that volume of late-night Pentagon pizza orders change when hostilities are imminent [64, 65]).

Fixed rate encryption equipment is expensive to purchase (and operate) so there is a temptation to move to off the shelf routers, software encryption and the use of general purpose wide-area network links. Very little research has been done on protecting encrypted Internet Protocol links against traffic analysis, despite warnings about the threat posed against standard protocols like IPSec [66] and TLS. Venkatraman and Newman-Wolfe [67, 68] have looked at imposing traffic schedules to minimize information leaked as well as covert channels. Ways to analyse the cost and anonymity provided by such systems is presented in [69]. The earliest mention of this problem can be found in 1983 [70], with the conclusion that "beyond the host level, further limitation on

information release becomes increasingly expensive and are probably not necessary in a non-military environment".

A related problem, of concern in military circles, is that an enemy could observe a network and even though all the traffic was encrypted, determine the function of each node through traffic analysis. A weather station would generate reports on an hourly basis, but the more interesting target of the military headquarters could be distinguished by the multiple flows in and out of its node. The US DARPA Agency set this problem as one of their Challenges in 1998 [71] and it has been addressed, albeit only for fairly limited network topologies, in a number of papers from Guan *et al.* [72, 73, 74] that consider adding extra traffic (padding) and rerouting some of the traffic along alternative network paths.

7 Data Retention

For some time, Law Enforcement officers (the police, secret services etc) have been using telephone call traffic data to identify criminals. Initially, very simple enquiries were made: determining who made the last call that the murder victim received, tracking the source of a ransom demand, and so on. However, there has been a growing use of genuine traffic analysis techniques to develop 'friendship trees' and thereby identify the roles of individuals within a conspiracy [13]. However, the denationalisation of incumbent fixed line telephone companies has broken their close ties with the police, and the growth of mobile telephone usage has led to a fragmentation of the market and fierce price competition, so that collection and storage of traffic data is now seen as an expensive burden. At the same time, new flat-rate business models have seen the business justification for call traffic data disappear. This has led to considerable anxiety within Law Enforcement that a valuable source of information will cease to be available.

In parallel, criminals have started to use the Internet for their communications and Law Enforcement has found that within this open system, with an extremely disparate set of service providers, the 'traceability' of communications can be problematic, and traffic analysis almost impossible. In particular, there has been concern that voice traffic will migrate from the closed and ordered telephony world to 'Voice over IP' (VoIP) running on the open and anarchic Internet.

In response, particularly after the terrorist attacks in Madrid (2004) and London (2005) interest

grew in mandatory 'Data Retention', requiring communications service providers to retain their traffic data logs for a fixed period, often far longer than their business needs would require. The term Data Retention should be contrasted with a 'Data Preservation' regime, where data is preserved specially in response to a specific request from Law Enforcement.

The United States has long had a Data Preservation regime, but in 2006 Congress started being pressured to consider moving to a Data Retention regime, with online child exploitation being cited as unnecessarily hard to investigate [75]. At much the same time, the 1994 CALEA requirements on traditional telephony (call data provision, wiretapping capability) were extended to VoIP providers [76].

Meanwhile, in Europe, the EU adopted the Data Retention Directive (2006/24/EC) in March 2006 [77]. This provides for telephone companies to implement Data Retention by September 2007 and Internet companies by March 2009 at the latest. There is some doubt over the legal status of the Directive, which is being challenged (early 2007) by Ireland on the basis that it should have been implemented under 'Third Pillar' procedures for 'Police and Judicial Co-operation in Criminal Matters' rather than a 'First Pillar' Directive for 'Market Harmonisation'. In practice, even though it is a Directive there is little harmonisation, with EU member states free to decide on retention periods of anything between six months and two years, and with such technically incompetent definitions having been chosen that it they could refer to every point-to-point connection made over the Internet, or merely to records of emails passing through major servers. It looks like being several years before any clarity emerges, and it is very likely indeed that retention regimes will differ markedly in different countries.

Notwithstanding all this technical confusion, there has been very little informed debate on the types of information that will be capable of being extracted from the retained data. As should be apparent from even the limited survey we have presented in this chapter, there is significant scope for drilling down to reveal the most private of information about activities, habits, interests and even opinions. Storing this data, in an easily accessible manner, represents a systemic vulnerability that cannot be overstated enough.

In order to make balanced judgments between the needs of Law Enforcement and the entitlement of law-abiding citizens to privacy, policy makers must become far more aware of the wealth of information that could be extracted from such data about every aspect of the networked society.

Even the extraction of apparently anonymous profiles from traffic databases would greatly facilitate privacy violations and routine surveillance. We believe that resistance to traffic analysis must be perceived of as a public good – the more that any attacker knows about the habits of your neighbours the more they can tell about you!

8 And Finally...

We have seen how traffic analysis has been used by the military, and how broadly similar techniques are beginning to be seen in civilian life. Much activity still remains classified, but more is entering the public domain, not least because of a wish to reduce costs by having a broad range of 'Commercial Off The Shelf' (COTS) equipment available.

However, our understanding of the threat that traffic analysis attacks represent on public networks remains somewhat fragmented, although the active research in this field has led to considerable improvement. The results we have presented in this chapter, from what we know so far, should act as a warning against ignoring this threat: traffic analysis not only can be used to reveal what is going on, but can also be used to bypass apparently robust security mechanisms.

References

[1] Diffie, W. and Landau, S., *Privacy on the Line: The Politics of Wiretapping and Encryption*, MIT Press, 1998.

[2] Herman, M., *Intelligence Power in Peace and War*, Cambridge University Press, 1996.

[3] Kahn, D., *The Codebreakers*, Scribner, 1967.

[4] Anderson, R., *Security engineering*, Wiley, 2001.

[5] Fullerton, J., British ruse held Iraqi's attention while real invasion came elsewhere, *The Philadelphia Inquirer*, 3 March, 1991.

[6] Paglen, T. and Thompson, A.C., Planespotting: Nerds with binoculars bust the CIA's torture taxis, *The Village Voice*, 15 October, 2006.

[7] Callimahos, L.D., *Traffic Analysis and the Zendian Problem*, Aegean Park Press, 1989.

[8] Wasserman, S. et al., *Social Network Analysis : Methods and Applications (Structural Analysis in the Social Sciences)*, Cambridge University Press, 1994.

[9] Travers, J. and Milgram, S., An experimental study of the small world problem, *Sociometry*, 32, 1969.

[10] Lin, N. and Smith, J., *Social Capital: A Theory of Social Structure and Action*, volume 19 of *Structural Analysis in the Social Sciences*, Cambridge University Press, 2002.

[11] Reed, W.J., A brief introduction to scale-free networks, *Technical report*, Department of Mathematics and Statistics, University of Victoria, 2004.

[12] Carley, K.M., Lee, J.S., and Krackhardt, D., Destabilizing networks, *Connections*, 22, 79, 2002.

[13] Garfinkel, S.L., Leaderless resistance today, *First Monday*, 3, 2003.

[14] Nagaraja, S. and Anderson, R., The topology of covert conflict, *Technical Report UCAM-CL-TR-637*, University of Cambridge, Computer Laboratory, 2005.

[15] Sparrow, M.K., The application of network analysis to criminal intelligence: An assessment of the prospects, *Social Networks*, 13, 251, 1991.

[16] Klerks, P., The network paradigm applied to criminal organisations, *Connections*, 24, 53, 2001.

[17] Hougham, V., Sociological skills used in the capture of Saddam Hussein, *Footnotes, Newsletter of the American Sociological Association*, 33, 2005.

[18] US Army Headquarters Department, *Field Manual 3-24: Counterinsurgency*, US Army, 2006.

[19] Krebs, V.E., Uncloaking terrorist networks, *First Monday*, 7, 2002.

[20] Dombroski, M., Fischbeck, P., and Carley, K., Estimating the shape of covert networks, in *Proceedings of the 8th International Command and Control Research and Technology Symposium. Conference held at the National Defense War College, Washington DC. Evidence Based Research, Track 3, Electronic Publication, Vienna, VA.*, CCRP, 2003.

[21] Fawcett, T. and Provost, F., Adaptive fraud detection, *Journal Data Mining and Knowledge Discovery*, 1, 291, 1997.

[22] Levien, R., Attack resistant trust metrics, 2003, `http://www.levien.com/thesis/compact.pdf`.

[23] Gibson, D., Kleinberg, J., and Raghavan, P., Inferring web communities from link topology, in *Proceedings of the 9th ACM Conference on Hypertext and Hypermedia*, ACM, 1998.

[24] Page, L. et al., The pagerank citation ranking: Bringing order to the web, *Technical report*, Stanford Digital Library Technologies Project, 1998.

[25] Kleinberg, J.M., Hubs, authorities, and communities, *ACM Computing Surveys*, 31, 5, 1999.

[26] Renesys Corporation, Market intelligence provides objective analysis of the service provider market, `http://www.renesys.com/products_services/market_intel/`.

[27] Song, D.X., Wagner, D., and Tian, X., Timing analysis of keystrokes and timing attacks on SSH, in *Tenth USENIX Security Symposium*, USENIX, 2001.

[28] Monrose, F., Reiter, M.K., and Wetzel, S., Password hardening based on keystroke dynamics, in *ACM Conference on Computer and Communications Security*, 73, ACM, 1999.

[29] Cheng, H. and Avnur, R., Traffic analysis of SSL encrypted web browsing, 1998, `http://www.cs.berkeley.edu/~daw/teaching/cs261-f98/projects/final-reports/ronathan-heyning.ps`.

[30] Hintz, A., Fingerprinting websites using traffic analysis, in R. Dingledine and P.F. Syverson, eds., *Privacy Enhancing Technologies*, volume 2482 of *Lecture Notes in Computer Science*, 171, Springer, 2002.

[31] Sun, Q. et al., Statistical identification of encrypted web browsing traffic, in *IEEE Symposium on Security and Privacy*, 19, IEEE, 2002.

[32] Danezis, G., Traffic analysis of the HTTP protocol over TLS, 2003, `http://www.cl.cam.ac.uk/~gd216/TLSanon.pdf`.

[33] Bissias, G.D. et al., Privacy vulnerabilities in encrypted HTTP streams, in G. Danezis and D. Martin, eds., *Privacy Enhancing Technologies*, volume 3856 of *Lecture Notes in Computer Science*, 1, Springer, 2005.

[34] Levene, M. and Loizou, G., Computing the entropy of user navigation in the web, *International Journal of Information Technology and Decision Making*, 2, 459, 2003.

[35] Felten, E.W. and Schneider, M.A., Timing attacks on web privacy, in *ACM Conference on Computer and Communications Security*, 25, ACM, 2000.

[36] Kohno, T., Broido, A., and Claffy, k.c., Remote physical device fingerprinting, in *IEEE Symposium on Security and Privacy* [78], 211.

[37] Murdoch, S.J., Hot or not: revealing hidden services by their clock skew, in A. Juels, R.N. Wright, and S.D.C. di Vimercati, eds., *13th ACM Conference on Computer and Communications Security (CCS), Alexandria, VA, USA*, 27, ACM, 2006.

[38] Dingledine, R., Mathewson, N., and Syverson, P., Tor: The second-generation onion router, in *Proceedings of the 13th USENIX Security Symposium*, USENIX, 2004.

[39] Bellovin, S.M., A technique for counting NATted hosts, in *Internet Measurement Workshop*, 267, ACM, 2002.

[40] Narten, T. and Draves, R., *Privacy Extensions for Stateless Address Autoconfiguration in IPv6*, RFC3041, IETF, 2001.

[41] Aura, T., *Cryptographically Generated Addresses (CGA)*, RFC3972, IETF, 2005.

[42] Pascual, A.E., Privacy extensions for stateless address autoconfiguration in IPv6 – "requirements for unobservability", in *RVP02, Stockholm*, Stockholm, 2002.

[43] Fyodor, Nmap – free security scanner for network exploitation and security audit, `http://www.insecure.org/nmap/`.

[44] Snort team, Snort, `http://www.snort.org/`.

[45] Fyodor, Nmap manual, 2006, `http://www.insecure.org/nmap/man/`.

[46] Wang, X. and Reeves, D.S., Robust correlation of encrypted attack traffic through stepping stones by manipulation of interpacket delays, in S. Jajodia, V. Atluri, and T. Jaeger, eds., *ACM Conference on Computer and Communications Security*, 20, ACM, 2003.

[47] Blum, A., Song, D.X., and Venkataraman, S., Detection of interactive stepping stones: Algorithms and confidence bounds, in E. Jonsson, A. Valdes, and M. Almgren, eds., *RAID*, volume 3224 of *Lecture Notes in Computer Science*, 258, Springer, 2004.

[48] Wang, X., Reeves, D.S., and Wu, S.F., Inter-packet delay based correlation for tracing encrypted connections through stepping stones, in D. Gollmann, G. Karjoth, and M. Waidner, eds., *ESORICS*, volume 2502 of *Lecture Notes in Computer Science*, 244, Springer, 2002.

[49] Peng, P., Ning, P., and Reeves, D.S., On the secrecy of timing-based active watermarking trace-back techniques, in *S&P 2006* [79], 334.

[50] Pascual, A.E., *Anonymous Untraceable Communications: Location privacy in mobile internetworking*, Ph.D. thesis, Royal Institute of Technology – KTH / IMIT, 2001.

[51] MIT Media Lab Human Dynamics Group, Reality mining, `http://reality.media.mit.edu/`.

[52] Chaum, D., Untraceable electronic mail, return addresses, and digital pseudonyms, *Communications of the ACM*, 24, 84, 1981.

[53] Danezis, G., Designing and attacking anonymous communication systems, *Technical Report UCAM-CL-TR-594*, University of Cambridge, Computer Laboratory, 2004.

[54] Serjantov, A., On the anonymity of anonymity systems, *Technical Report UCAM-CL-TR-604*, University of Cambridge, Computer Laboratory, 2004.

[55] Moeller, U. et al., Mixmaster protocol version 2, *Technical report*, Network Working Group, 2004, Internet-Draft.

[56] Danezis, G., Dingledine, R., and Mathewson, N., Mixminion: Design of a type III anonymous remailer protocol, in *IEEE Symposium on Security and Privacy*, IEEE, Berkeley, CA, 2003.

[57] Berthold, O., Federrath, H., and Köpsell, S., Web MIXes: A system for anonymous and unobservable Internet access, in H. Federrath, ed., *Designing Privacy Enhancing Technologies*, volume 2009 of *LNCS*, 115, Springer-Verlag, 2000.

[58] Agrawal, D. and Kesdogan, D., Measuring anonymity: The disclosure attack, *IEEE Security & Privacy*, 1, 27, 2003.

[59] Kesdogan, D. and Pimenidis, L., The hitting set attack on anonymity protocols, in Fridrich [80], 326.

[60] Danezis, G. and Serjantov, A., Statistical disclosure or intersection attacks on anonymity systems, in Fridrich [80], 293.

[61] Kesdogan, D. et al., Fundamental limits on the anonymity provided by the mix technique, in *S&P 2006* [79], 86.

[62] Wright, M. et al., An analysis of the degradation of anonymous protocols, in *NDSS*, The Internet Society, 2002.

[63] Murdoch, S.J. and Danezis, G., Low-cost traffic analysis of Tor, in *S&P 2005* [78], 183.

[64] Gray, P., And bomb the anchovies, *Time*, 13 August, 1990.

[65] Warinner, A., Security clearances required for Domino's, 1996, `http://home.xnet.com/~warinner/pizza.html`.

[66] Bellovin, S.M., Probable plaintext cryptanalysis of the IP security protocols, in *NDSS*, IEEE Computer Society, 1997.

[67] Newman-Wolfe, R. and Venkatraman, B., High level prevention of traffic analysis, *Seventh Annual Computer Security Applications Conference*, 102, 1991.

[68] Venkatraman, B. and Newman-Wolfe, R., Transmission schedules to prevent traffic analysis, *Proceedings, Ninth Annual Computer Security Applications Conference*, 108, 1993.

[69] Newman, R.E. et al., Metrics for trafic analysis prevention, in R. Dingledine, ed., *Privacy Enhancing Technologies*, volume 2760 of *Lecture Notes in Computer Science*, 48, Springer, 2003.

[70] Voydock, V. and Kent, S., Security Mechanisms in High-Level Network Protocols, *ACM Computing Surveys (CSUR)*, 15, 135, 1983.

[71] Defense Advanced Research Projects Agency, Research challenges in high confidence networking, 1998.

[72] Guan, Y. et al., Preventing traffic analysis for real-time communication networks, in *Proceedings of The IEEE Military Communication Conference (MILCOM) '99, November 1999*, IEEE, 1999.

[73] Guan, Y. et al., Efficient traffic camouflaging in mission-critical QoS-guaranteed networks, in *Proceedings of IEEE Information Assurance and Security Workshop, West Point, June 2000*, 143, IEEE, 2000.

[74] Guan, Y. et al., Netcamo: Camouflaging network traffic for QoS-guaranteed mission critical applications, *IEEE Transactions on Systems, Man, and Cybernetics, Part A*, 31, 253, 2001.

[75] Petersen, R., Towards a U.S. data-retention standard for ISPs, *Educause Review*, 41, 78, 2006.

[76] Federal Communications Commission, Second report and order and memorandum opinion and order, 2006.

[77] European Union, Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, *Official Journal of the European Union*, L 105, 54, 2006.

[78] *2005 IEEE Symposium on Security and Privacy (S&P 2005), 8–11 May 2005, Oakland, CA, USA*, IEEE Computer Society, 2005.

[79] *2006 IEEE Symposium on Security and Privacy (S&P 2006), 21–24 May 2006, Berkeley, CA, USA*, IEEE Computer Society, 2006.

[80] Fridrich, J.J., ed., *Information Hiding, 6th International Workshop, IH 2004, Toronto, Canada, May 23–25, 2004, Revised Selected Papers*, volume 3200 of *Lecture Notes in Computer Science*, Springer, 2004.