

Defeating traffic analysis.

At first sight analysis of traffic data seems to be a very powerful technique for detecting crime.

If logs of both the sender and recipient can be kept, then it is possible to trace the progress of a communication, to trace the contacts of a suspect, and to compare patterns of communications and external events and thereby either predict future events or get information about who is likely to be responsible for past events.

If only one of the sender or recipient can be logged then it is possible to trace the likely location of an individual and the volume of traffic he sends or receives.

However, if the subject wants to prevent this from happening and is prepared to take measures to do so, it is usually possible to defeat traffic analysis. Espionage agents, serious criminals, terrorists and the like who are aware of the threat posed to them by traffic analysis can avoid giving out any useful traffic information at all. The same is true of lesser criminals as well, although they will not bother to use the more extreme methods.

In many cases the ordinary man in the street, who may wish to keep something private for entirely legal and proper reasons, will either not know that he needs to, or will not know how to avoid traffic analysis.

The simplest method of defeating traffic analysis is not to generate loggable traffic data. Other methods, such as hiding secret traffic in overt traffic, are possible. This document discusses some of the measures presently used, and some possible future trends, sorted by the method of transmission.

1) Postal items:

Traffic analysis of postal items is largely limited by practical considerations. Individual items can be traced, as can mail to one address, but long-term mass traffic data retention is impractical except in the case of registered or recorded delivery items.

As the act of putting mail into a postbox is anonymous, tracing the sender is difficult, and can be made nearly impossible by a determined participant. As there is in general no way to track both senders and recipients, tasks like finding the contacts of a determined participant are not practical.

On occasion PO boxes, false/unused addresses and remailers are used, but this is rare and is not usually done to prevent traffic analysis, except in the case of credit card fraud when goods are sent by post.

2a) Telephone, land lines:

With the advent of CLI it has become obvious that almost all UK calls can be traced almost instantaneously, even when CLI is blocked by the caller. The "two minutes to trace" beloved of fiction authors has become a thing of the past, at least in the public's perception (though it can still happen in practice).

While it is in general inconvenient for the public at large to take measures to defeat traffic analysis of fixed telephones, the use of public and prepay mobile telephones is widespread even among lesser criminals. This will be discussed

further in the drug-dealer example below. Large criminal organisations will use cutouts (people willing to relay a message) as well. If one end of the communications data chain is unavailable then many of the techniques of traffic analysis are not possible.

2b) Telephones, mobile:

Big-time criminals use mobiles a lot, the biggest and most security conscious will even use a mobile telephone once only. While insecure use of mobiles does happen, it is generally limited to the lower levels of crime:

2c) An Example. Mobile telephones and the drug dealer:

This protocol, or a variant on it, is fairly widely used by drug dealers.

Clients send text messages to the street-level dealer who uses a prepay mobile telephone, preferably from public telephones or prepay mobile telephones. In the US the use of pagers instead is common, and more secure as the approximate location of the recipient is not knowable.

The dealer contacts his supplier through a method that does not use the mobile telephone number used by his clients. If the dealer is caught the clients who have failed to use untraceable means to contact the dealer can be identified as likely suspects from records of the calls to the dealer's mobile telephone.

However the supplier, who has more to lose and tends to be more security-conscious, will not be identified by analysis of this traffic data. Suppliers will insist that the dealer uses eg public telephones to contact him, and in some cases will instruct the dealer in the security procedures he requires.

The dealer will change his mobile telephone every few months, partly as a general security measure and partly to prune his client list - few drug dealers will continue to supply any customer who eg gives out his number without asking his permission, or is otherwise seen as a threat. Even if unrestricted access to long-term traffic data is available to investigators the "leakiness" of the client-level security will do little more than identify the new number used by the dealer.

Cannier clients will appreciate that using anonymous methods to contact the dealer will protect them if the dealer is caught, and if a conviction for possession would mean more than a small fine (eg loss of job) they will be prepared to trudge to the nearest 'phone box on a cold wet night. The dealer will trudge there, because he won't be able to buy if he gets a reputation for insecurity.

2d) There is another noteworthy property of mobile telephones, the ability to trace the movement of an individual on a continuous basis, whether or not he is making a call - mobiles send out a signal every minute or so, in order to maintain registration. The simplest counters are to switch the mobile off, or use a pager instead. More complex techniques include leaving the mobile behind or putting it in eg a car, which can provide a weak alibi. However for tracing the movements of the average man in the street this is a very powerful technique. At present location accuracy is limited to the cell, but this may change.

3) Electronic Communications:

The standard technique for email anonymity is the remailer, perhaps "onion-skinning" a message through a network of remailers so the compromise of one remailer will not affect overall anonymity. Anonymised "Hushmail" is popular. Messages can be sent to webmail addresses and collected in internet cafe's. For web browsing a web forwarder such as "Safeweb" can be used, although as that one is partly funded by the CIA I wouldn't recommend it.

More advanced techniques include hiding traffic in other traffic, as in the growing use of VPN's (virtual private networks), and posting images with steganographically hidden messages on popular 'net sites. For the more serious criminal the use of mobile phones to connect to the internet using false Credit Card details to pay the ISP's bill is growing (and prepay mobile internet services are available too).

This is an area that changes rapidly, and research or development is going on into the use of "feeds" and applying PIR (private information retrieval) technology, both of which will give "beyond suspicion" anonymity.

4) Likely effect of the introduction of mass traffic data retention:

While the introduction of long-term data retention might seem to offer an opportunity to "catch the criminals with their pants down" until they learn to defend against traffic analysis, initial Police unfamiliarity with the necessary techniques and the present widespread implementation of anti-traffic analysis measures by even lesser criminals will blunt the expected impact. Some of the unwary will be caught, and the dumb/careless/lazy will continue to be caught as now, but overall the effect will not be huge, especially on the serious criminal.

Retention for periods of over 12 months will be less effective as an anti-crime measure. Criminals already change mobiles fairly frequently.

The failed cruise missile attack on Bin Laden, based on Satellite phone traffic data, several events in the middle East, and the conviction in the Omagh Bombing case based on mobile location data have alerted the terrorist to the dangers of traffic analysis, and he will have taken measures to defeat it. The crime lord has been aware of the danger for some time. Even minor criminals already take precautions.

Traffic data retention will mostly be effective against the unwary, and the innocent. Almost everyone has something they'd like to hide. Against the determined, aware and intelligent criminal it is likely to be almost completely ineffective.

--

Peter Fairbrother

peter@m-o-o-t.org

10 Sheepcote Barton

Trowbridge

Wiltshire

BA14 7SY

UK

+44/0 1225 764449 landline

+44/0 771 408 1141 mobile

Numbers of requests for Communications Data, and a Suggestion

The total number of requests is not available (letter from Bob Ainsworth, 24 July 2002), but estimates range between "hundreds of thousands" (Simon Watkin, Home Office) to around 500,000 per year (*1).

Taking the 500,000 figure, these can be divided roughly as follows:

Subscriber details (name and address):
484,000

Billing details (who called whom):
14,500

Other requests (usually of a more intrusive nature):
1,500.

Might I suggest that the last two categories, or at least the last one, should and could be dealt with by prior judicial authorisation, instead of through Chapter 2 of RIPA.

This would require primary legislation, but I suspect some primary legislation will probably be needed in the overall context of this discussion. It might allay the fears of those who do not trust investigating authorities to approve their own requests.

An adequate system of penalties for abuse might also help achieve this confidence.

--

Peter Fairbrother

peter@m-o-o-t.org

10 Sheepcote Barton
Trowbridge
Wiltshire
BA14 7SY
UK

+44/0 1225 764449 landline
+44/0 771 408 1141 mobile

note (*1)This is based on Lord Bassam of Brighton, Hansard Col 124, 19 June 2000

"I can advise the Committee that during the first three months of this year, 96.8 per cent of all the communications data requested by HM Customs & Excise has been for subscriber details, which is the most basic level of check. Some 2.9 per cent of the remainder has been for itemised billing inquiries; the remaining 0.3 per cent has been for other services, none of which is more intrusive than those carried out by a surveillance team. That equates to a total of 18,940 requests, which is clearly far more than could easily be accommodated by judicial authorisation. It is important to record that point."

And the figure of 127,000 requests made by the Metropolitan Police in 2001 given by Mr John Denham, Hansard Column 1497W 24 July 2002.