# Forensics

**David Malone**

**<dwmalone@{maths.tcd,cnri.dit}.ie>**

**10 June 2003**

## What is Forensics?

- Strictly: linked to courts of law.
- Computer forensics rarely directly useful.
- Finding out what happened after rum and uncanny goings on.

## Why is it useful?

- To convict people?
- Is reinstalling a good idea if broken in to?
- To convince people you're innocent.

## Security is a probabilistic game

Each month (roughly):

- $\mathbb{P}$[I can Crack a DES password] $\approx 1/20000$
- $\mathbb{P}$[30 year old man dies] $\approx 1/10000$
- $\mathbb{P}$[OpenBSD remote root exploit] $\approx 1/100$
- $\mathbb{P}$[psychosis diagnosed in 1000 people] $\approx 1/90$

## Plan

- First look at techniques: non-computer, logs, filesystem, disks, processes, network.
- Then give some examples.

## Non-computer sources

- Users.
- Security people, cleaners, . . . .
- Swipe card logs.
- Security cameras.

## Log files

- System logs: messages, mail logs, login times, HTTP/Proxy logs, process accounting.
- Check .history files. Note unusual commands or flags.
- Small anomalies can be important (change in file size, missing entries).
- Remember to check for changes in RPM like databases.

## Filesystem

- Build database of all files using find -ls.
- If you might be root kitted, examine from clean host.
- Remember 3 timestamps in the filesystem: ctime, mtime, atime. Can be faked.
- Mtime on a directory means file was added or removed.
- Check md5/rpm/Solaris checksums and interesting file content.

## Disks

- dd off all the partitions to another machine.
- Then use strings to find removed source code/logs/...
- Don't forget swap partition.
- Examining directory blocks can give deleted filenames.

```
% ls -l
total 0
-rw-r--r--  1 dwmalone  wheel  0 Jun  8 16:01 hello
% rm hello
% ls
% strings .
hello
```

## Processes

If still alive:

- Open files persist.
- Look in /proc to get open files, suspicious executables, compare with ps, . . .
- Examine running processes with gcore or debugger.
- Panic machine and get vmcore (save swap first!)

## Network

- Usual tools: dig, whois, traceroute, nmap, google, usenet, own logs . . .
- Check other network logs: cisco accounting, MRTG, other local hosts (ident), . . .
- Pool information with other local admins/CERTs.
- Keep explicit network logs.

## Pulling it all together

- Organise what you've gathered — probably by time. Use a format you can sort and grep easily.
- Keep an open mind.
- As you discover more, go back to primary sources.

## Local happenings

- Sending mail with finger.
- Harassed by quirky code.
- Account sharing.

According to the log from my firewall, I have been probed/attacked by one of the machines attached to your domain. As these probes/attack occur in concert with other machines from other institutions, it appears that a daemon has been installed on the machine in question and is being used to probe external machines for vulnerabilities. Could you please investigate the machine in question and remove the daemon that is probing my machine.

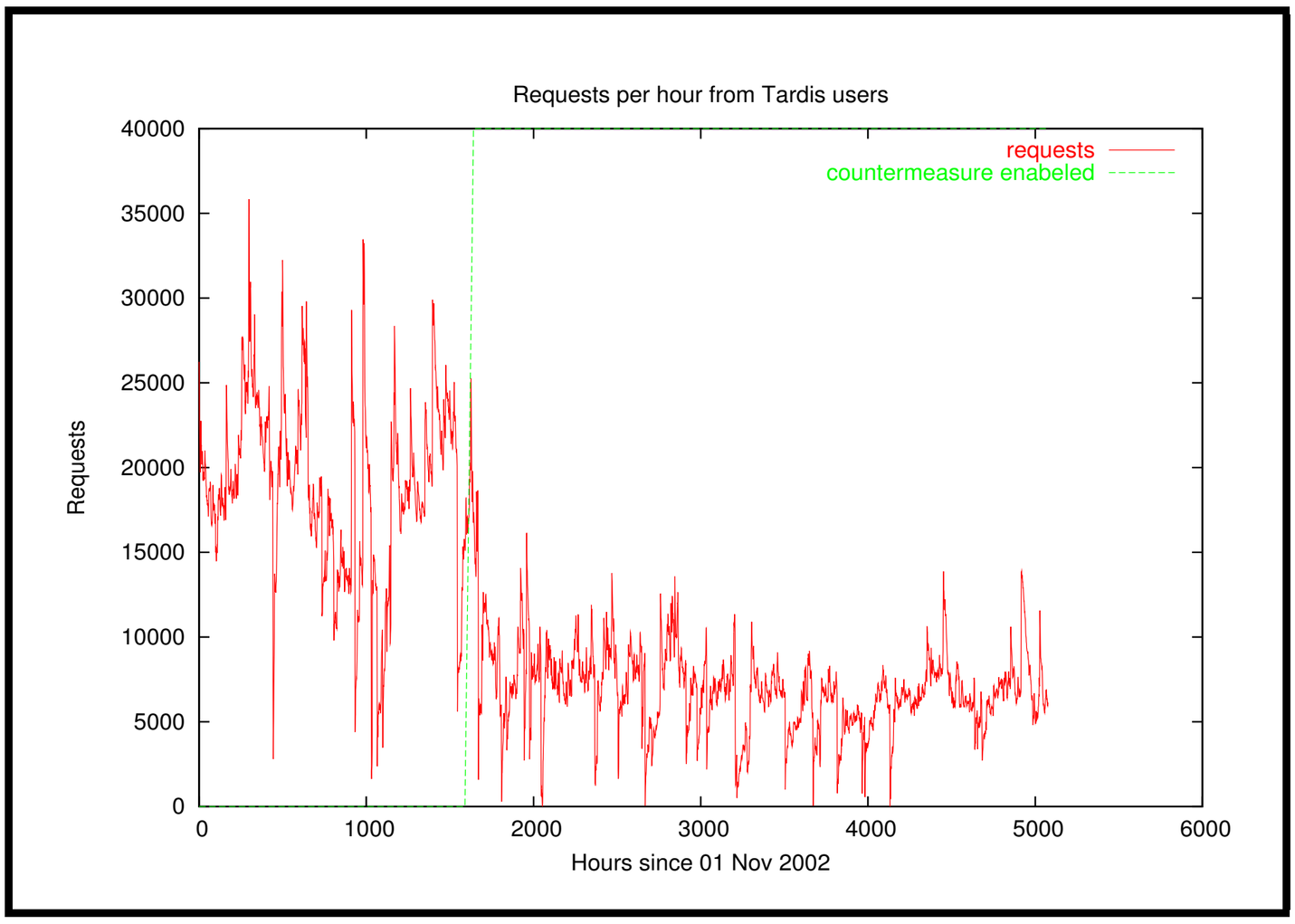
Shown below is some pertinent information from my log concerning when the probes/attacks occurred. As you will notice, the frequency is increasing.

| timestamp (GMT) | issueName | intruderIp | intruderName |
|---|---|---|---|
| 2000-09-13 02:41:21 | UDP port probe | 134.226.81.11 | salmon.maths.tcd.ie |
| 2000-09-19 07:11:03 | UDP port probe | 134.226.81.11 | salmon.maths.tcd.ie |
| 2000-09-22 14:00:50 | UDP port probe | 134.226.81.11 | salmon.maths.tcd.ie |

## Flipside

- Users complain of failing cgi scripts.
- Frequent periodic requests for home page from hundreds of hosts.

```
16:45:21.930978 adsl-63-205-116-37.dsl.lsan03.pacbell.net.1085 > salmon.maths.tcd.ie.http: P 1:37(36) ack 1 win 8760 (DF)
0x0000   4500 004c 2e6d 4000 6a06 565f 3fcd 7425        E..L.m@.j.V_?.t%
0x0010   86e2 510b 043d 0050 09be a141 2d51 ebbe        ..Q..=.P...A-Q..
0x0020   5018 2238 8e53 0000 4745 5420 2f20 4854        P."8.S..GET./.HT
0x0030   5450 2f31 2e30 0d0a 5072 6167 6d61 3a20        TP/1.0..Pragma:.
0x0040   6e6f 2d63 6163 6865 0d0a 0d0a                  no-cache....
```


Requests per hour from Tardis users
requests
countermeasure enabeled
Requests
Hours since 01 Nov 2002
0
5000
10000
15000
20000
25000
30000
35000
40000
0
1000
2000
3000
4000
5000
6000

## www.tcd.ie

- All logs removed.
- Recovered most logs and process accounting.
- Good example of sorting events.

## Blame Canada?

- Odd account use reported by users.
- Curious sshd log lines.
- Checking security tape/swipe card logs.

- Problems on Netsoc host.
- Persisting after back doored ssh replaced.
- Monitoring finds second back door.
- Eventually spotted by security people.