

VERIFY YOUR EMAIL SECURITY WITH TCPDUMP

SPY ON YOURSELF

Carla Schroder

I confess, I'm an outlaw at heart. I like using packet sniffers like **tcpdump** because it satisfies my base snooping impulses. Packet-sniffing is wiretapping after all, only it's applied to TCP/IP packets, not voice transmissions. Sure, they're my packets on my systems, but still the idea is appealing. Even more appealing is knowing I have the ability to monitor incoming and outgoing traffic, and knowing exactly what's going on.

For example, being an untrusting soul as all wise network administrators are, I can use tcpdump to verify that encryption is working. Here is what a plain unencrypted POP mail session looks like. This is an abbreviated example showing only the initial three-way TCP handshake. You can do this yourself by firing up tcpdump, then checking mail. Ctrl+C stops it:

```
# tcpdump port 110
15:04:49.050227 windbag.34348 > venus.domain.com.pop3: S
2974284112:2974284112(O) win 5840 (DF)
15:04:49.190076 venus.domain.com.pop3 > windbag.34348: S
2862911212:2862911212(O) ack 2974284113 win 5840 (DF)
15:04:49.190168 windbag.34348 > venus.domain.com.pop3: . ack 1 win 5840 (DF)
```

Handshake Dissection

There is a whole lot going on here, which I shall now deign to explain.

15:04:49.050227 is the timestamp, in *hh:mm:ss:fraction* format.

windbag.34348 > is the originating host and port.

venus.domain.com.pop3: is the destination host and port (see */etc/services*).

S is the first part of the three-way TCP handshake (SYN, SYN, ACK).

2974284112:2974284112 is the byte sequence/range. The initial sequence number (ISN) is generated randomly. Then sequence numbers for the rest of the bytes in the connection are incremented by 1 from the ISN. Since no data are exchanged at this stage, both numbers are the same.

win 5840 is the window size, or the number of bytes of buffer space the host has available for receiving data.

mss 1460 is the maximum segment size, or maximum IP datagram size that can be handled without using fragmentation. Both sides of the connection must agree on a value; if they are different, the lower value is used.

sackOK means "selective acknowledgments," or allow the receiver to acknowledge packets out of sequence. Originally, packets could only be acknowledged in sequence. So if the third packet out of a thousand packets received went missing, the host could only acknowledge

VERIFY YOUR EMAIL SECURITY WITH TCPDUMP

SPY ON YOURSELF

Carla Schroder

the receipt of the first two packets, and the sender would have to resend all packets from number three through one thousand. sackOK allows only the missing third packet to be re-sent.

timestamp 995173 0 measures the round-trip time. There are two fields: the Timestamp Value and the Timestamp Echo Reply. On the first exchange, the Echo Reply is set to 0. When the second host receives that packet, it transfers the timestamp from the old packet's Timestamp Value field to the new packet's Timestamp Echo Reply field. Then it generates a new value for the Timestamp Value field. So the Timestamp Value field contains the latest timestamp, while the Timestamp Echo Reply field contains the previous timestamp.

nop, or "no operation," is just padding. TCP options must be multiples of 4 bytes, so nop is used to pad undersized fields.

wscale 0> is a nifty hack to get around the original window size limitation of 65,535 bytes, because the window size field is only 16 bits long. wscale provides for a full gigabyte of buffer. Both sides of the connection must support this and agree; otherwise the window size does not change.

(DF) means "don't fragment."

Here is a sample of the rest of the dump, showing data transfer:

```
15:04:49.548954 windbag.34348 > venus.domain.com.pop3: P 46:52(6) ack 181 win 5840 (DF)
15:04:49.653945 venus.domain.com.pop3 > windbag.34348: P 181:238(57) ack 52 win 5840
(DF)
```

The **P** flag means "push", or data are being sent. And now you see an example of the byte sequence/range when data are sent: 181:238(57); or 57 packets in this particular exchange.

Verifying Encryption

Now let's get back to our original task of examining packets to verify that logging in to our mail server is properly encrypted. Here is the quick way:

```
# tcpdump port 995
tcpdump: listening on eth0
16:10:05.054198 windbag.34465 > venus.euao.com.pop3s: S
2698160498:2698160498(0) win 5840 (DF)
16:10:05.171235 venus.domain.com.pop3s > windbag.34465: S
2694170013:2694170013(0) ack 2698160499 win 5840 (DF)
16:10:05.171319 windbag.34465 > venus.domain.com.pop3s: . ack 1 win 5840 (DF)
```

This shows the protocol is pop3s, rather than pop3, which is what we want. We can dig even deeper and view the login itself:

VERIFY YOUR EMAIL SECURITY WITH TCPDUMP

SPY ON YOURSELF

Carla Schroder

```
# tcpdump -X port 995
```

The **X** option displays the packet in nice readable ASCII, as this snippet shows:

```
E...R(@.5..fE8..
.....
P...`.....J...
F..A....yY.I.D..
=2....'i..E.....J.
```

Readable enough to verify that anyone snooping on our connection cannot capture logins and passwords. This snippet plainly shows the login and password in a clear text login:

```
# tcpdump -X port 110
```

```
E8.....n....V%.
P...T...USER.car
la@domain.com..
```

```
32:46(14) ack 70 win 5840 (DF)
```

```
E..6..@.@..x....
E8.....n..."V&.
P...n...PASS.mgY6Rf9W..
```

Hubs Are Blabbermouths

If your LAN is connected with hubs, which is so twentieth century, you can sniff traffic for any host on the network from the comfort of your own chair. Anyone on the LAN can simply name the host they wish to surveil:

```
# tcpdump dst host workstation5
```

Or specify the host's IP address. `tcpdump` automatically puts your NIC into promiscuous mode, but you won't see this with `ifconfig`. You'll see it in `dmesg` or `/var/log/messages`. Just for kicks, open two terminal windows. In one, run `tail -f /var/log/messages`. In the other, run `tcpdump`, then stop it. The first one will show something like

```
Nov 22 20:43:30 windbag kernel: eth0: Promiscuous mode enabled.
Nov 22 20:43:30 windbag kernel: device eth0 entered promiscuous mode
Nov 22 20:44:07 windbag kernel: eth0: Promiscuous mode enabled.
Nov 22 20:44:07 windbag kernel: device eth0 left promiscuous mode
```

Foiled By Switches

If your LAN is blessed with switches instead of hubs, you cannot do this. You must first put the switch in SPAN (Switch Port Analyzer) mode. This is also called "port mirroring." Whatever you call it, it puts the switch in broadcast mode just like a hub, with one major difference: all the LAN traffic is directed to a sniffer port, so only you, the godlike admin, can

VERIFY YOUR EMAIL SECURITY WITH TCPDUMP

SPY ON YOURSELF

Carla Schroder

see the packets. Low-cost SOHO switches, such as those made by Linksys, D-Link, and Netgear, cannot do this; this is a feature of higher-priced products from Cisco and Extreme.

Come back next week to learn some nifty network diagnostic tricks with tcpdump, such as finding signs of evil activity, diagnosing network problems, and sending tcpdump's output to binary files suitable for parsing by utilities like Ethereal and Snort.

Resources

Unlike my columns, RFCs are less-than-riveting reading. But they contain complete information.

- rfc 793 describes the transmission control protocol (tcp) in exhaustive detail.
- rfc 1180 is an excellent tutorial.
- [tcpdump home page](#)