CrossbearSSH: Notary and Attack Reporting for SSH

Ralph Holz, Oliver Gasser

Network Architectures and Services
Technische Universität München

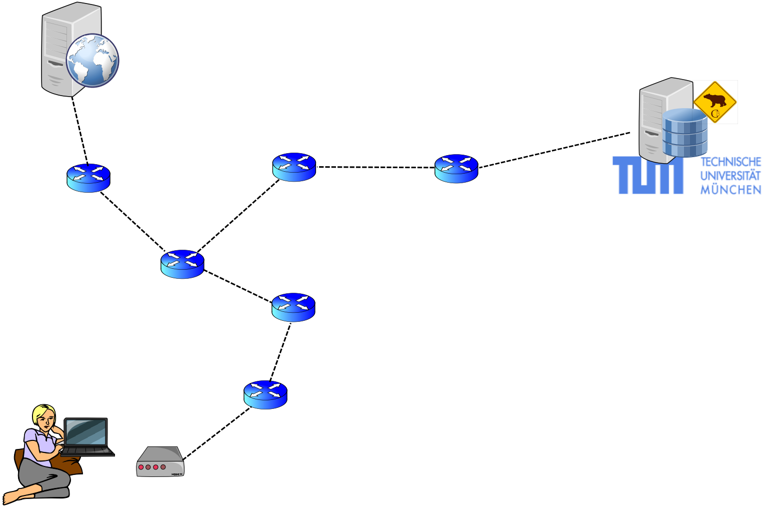
29C3

Crossbear

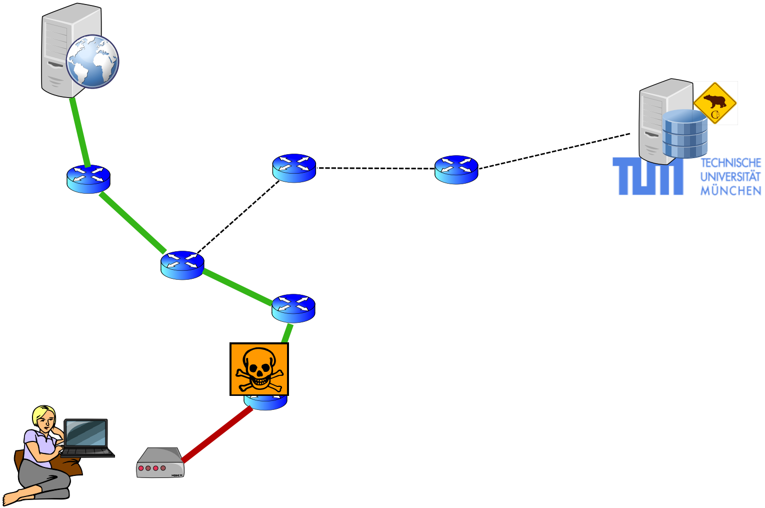
Last year at 28C3:

- We introduced Crossbear
- Detection and localisation of Men-in-the-middle on SSL
- Notary principle plus hunting from many vantage points on the Internet
- We had quite some fun with it: got a grant, OONI implementation etc.

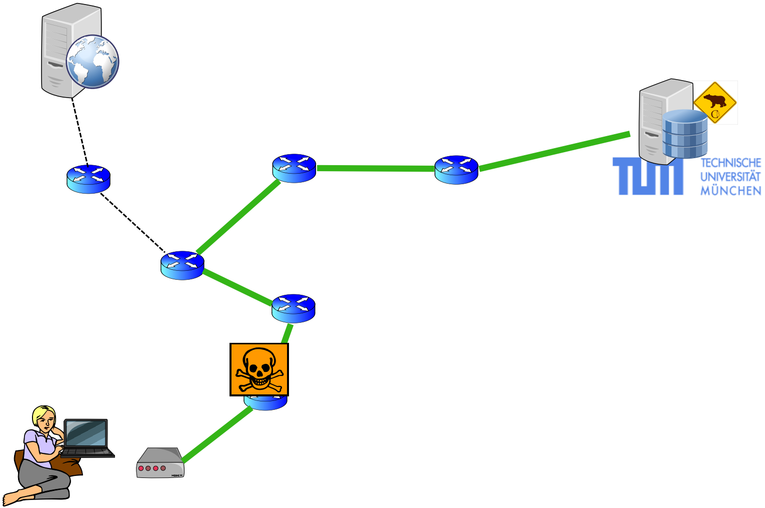
Alice accesses a host...



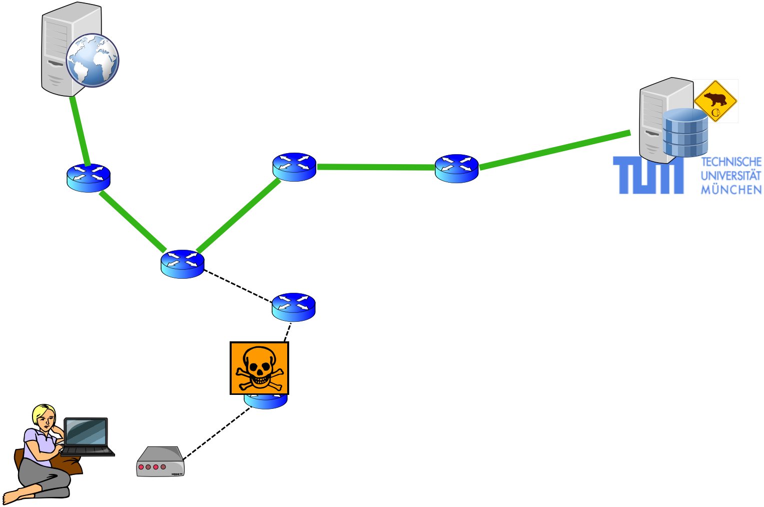
Man-in-the-middle



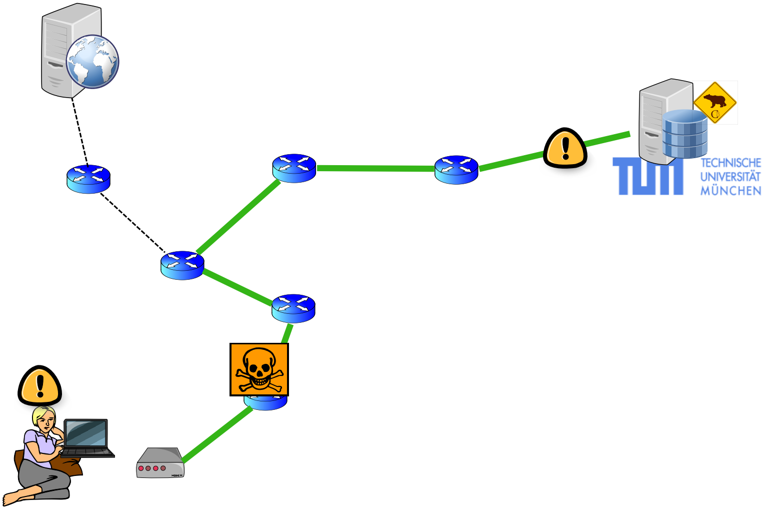
Alice queries Crossbear



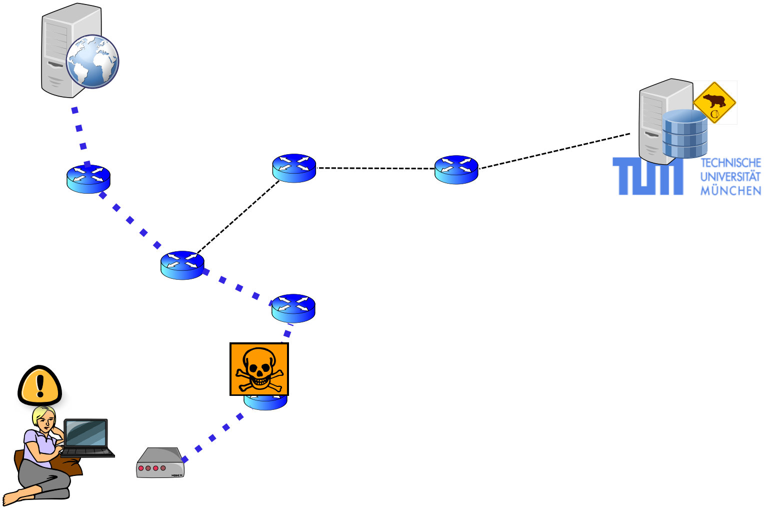
Crossbear checks the server



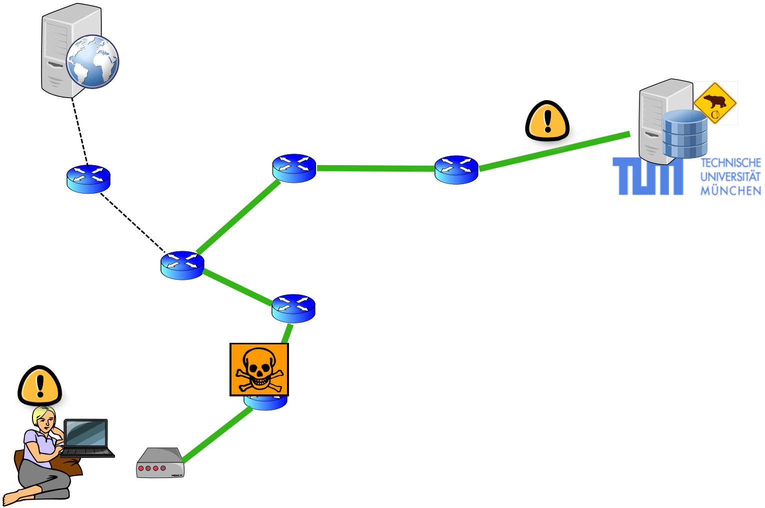
Crossbear reports result



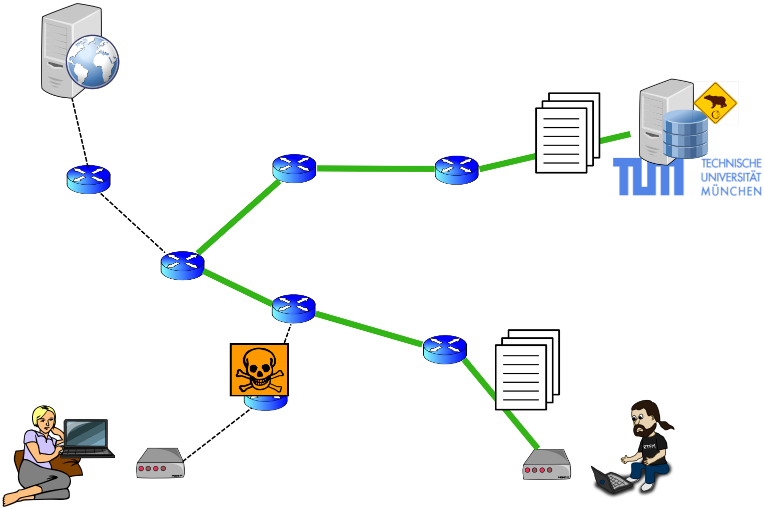
Alice traceroutes to server



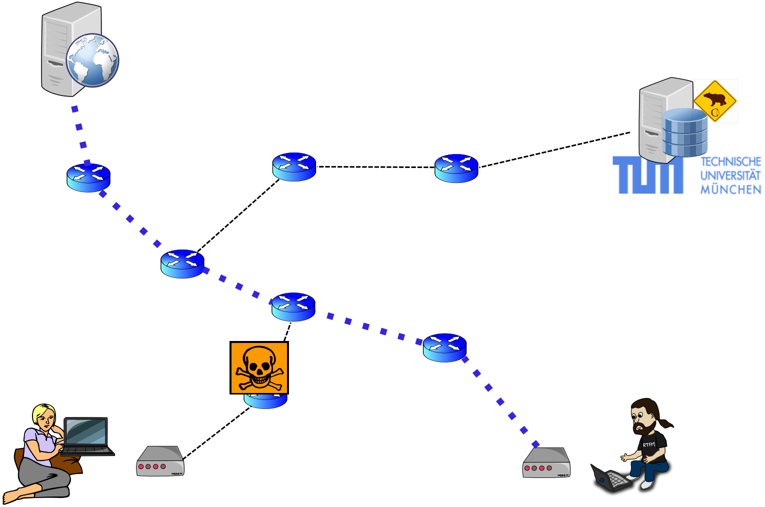
Alice reports to Crossbear



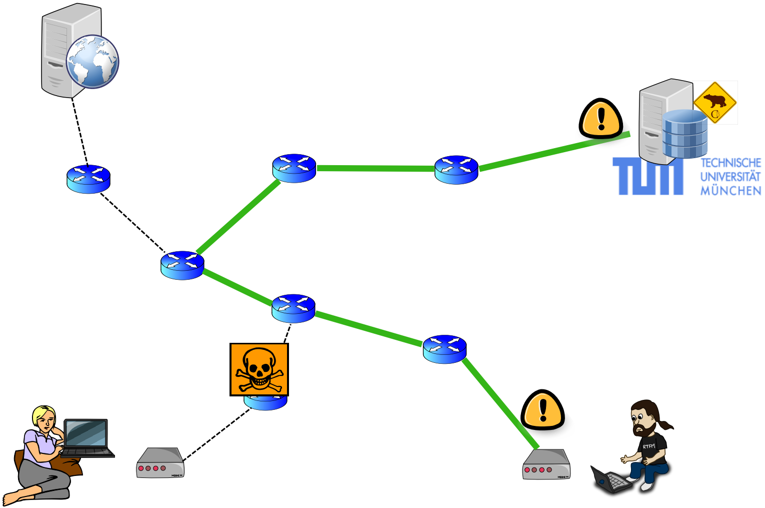
Distribute hunting tasks



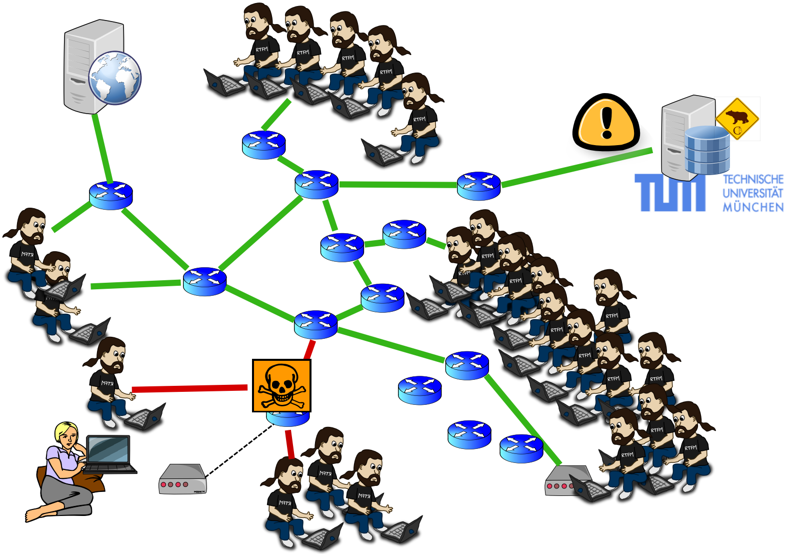
Bob goes hunting



Bob reports



There are many Bobs



Crossbear is coming to SSH

Like, *now*.

- Ever wanted to compare an SSH fingerprint but had no 2nd channel and no idea what the correct host-key should be?
- (There used to be Perspectives, but it was mostly for SSL, and not maintained.)

Use our shiny new notary

- `cbssh.net.in.tum.de`
- Based on our own IPv4-wide SSH scans, plus live checks

OpenSSH live checking/querying

Proof-of-concept implementation

- Try our patch for `openssh`:

  ```
  ssh -o VerifyHostKeyNotary=Yes user@example.com
  ```
- This will connect to the Crossbear server and ask it to do a live check for the host-key fingerprint.
- `openssh` will warn on mismatch
- Tracerouting for stand-alone hunters soon

Don’t want to use our notary?

- Set up your own! Everything is GPL.

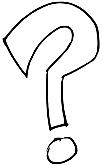
Querying our database

We scanned IPv4 3 times and stored SSH info.

- Query the results via DNS
- DNSSEC coming soon

```
dig -t TXT 5.135.53.222.cbssh.net.in.tum.de
...
;; ANSWER SECTION:
5.135.53.222.cbssh.net.in.tum.de.  86400 IN TXT ‘‘{ip:  5.135.53.222, [{fp:
45:a2:43:de:80:2f:af:4f:18:81:01:b5:b4:95:2b:82, first-seen: 2012-09-10 18:33:28,
last-seen: 2012-11-19 14:39:45, count: 2, type: ssh-rsa, ver: ssh2}, {fp:  a1:80:
03:06:f6:b8:5d:91:87:11:7b:ae:ba:b4:32:a4, first-seen:  2012-09-10
18:33:38, last-seen:  2012-11-19 14:39:57, count:  2, type:  ssh-dss, ver:
ssh2}]}’’
```

Questions?



Contact

- We are here at the P2PHackers Assembly.
- A longer talk on day 4 (see Fahrplan).
- Twitter: @crossbearteam
- `https://github.com/crossbear/Crossbear`
- `https://pki.net.in.tum.de`