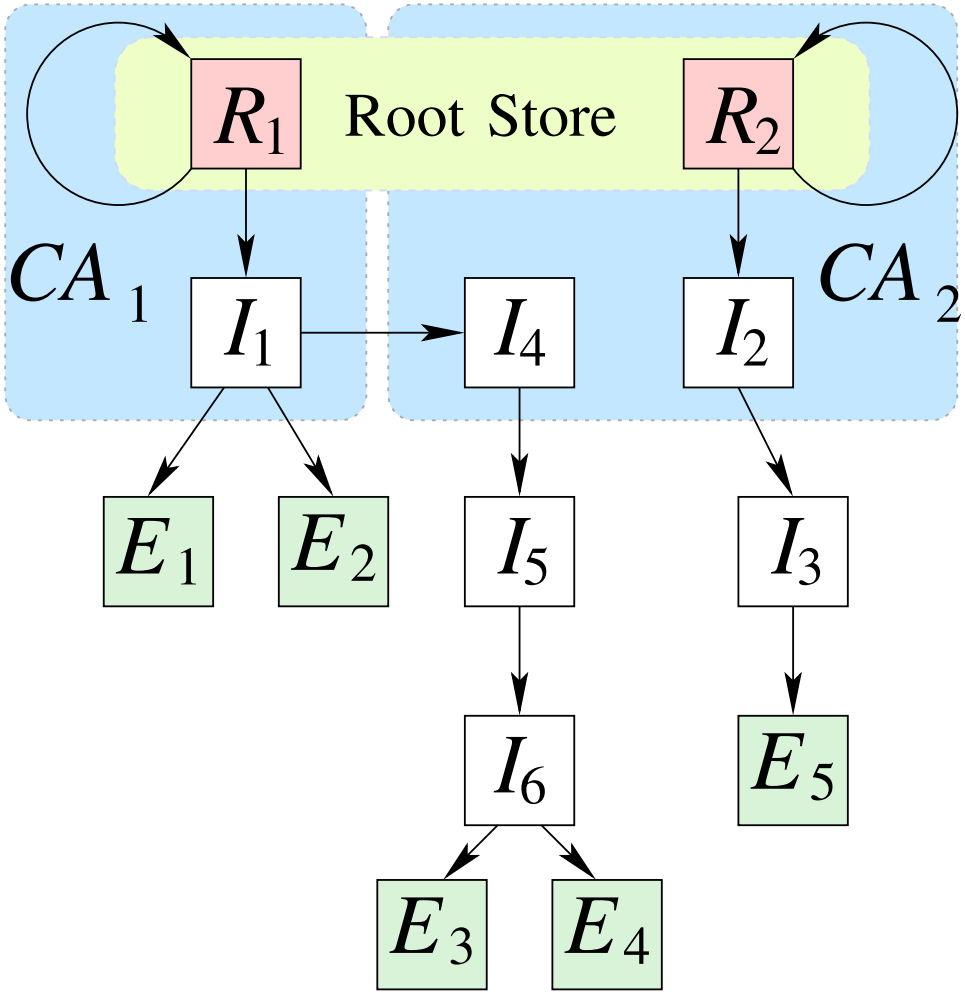
One year of Crossbear (now with SSH, too!)

Ralph Holz, Oliver Gasser

Network Architectures and Services
Technische Universität München

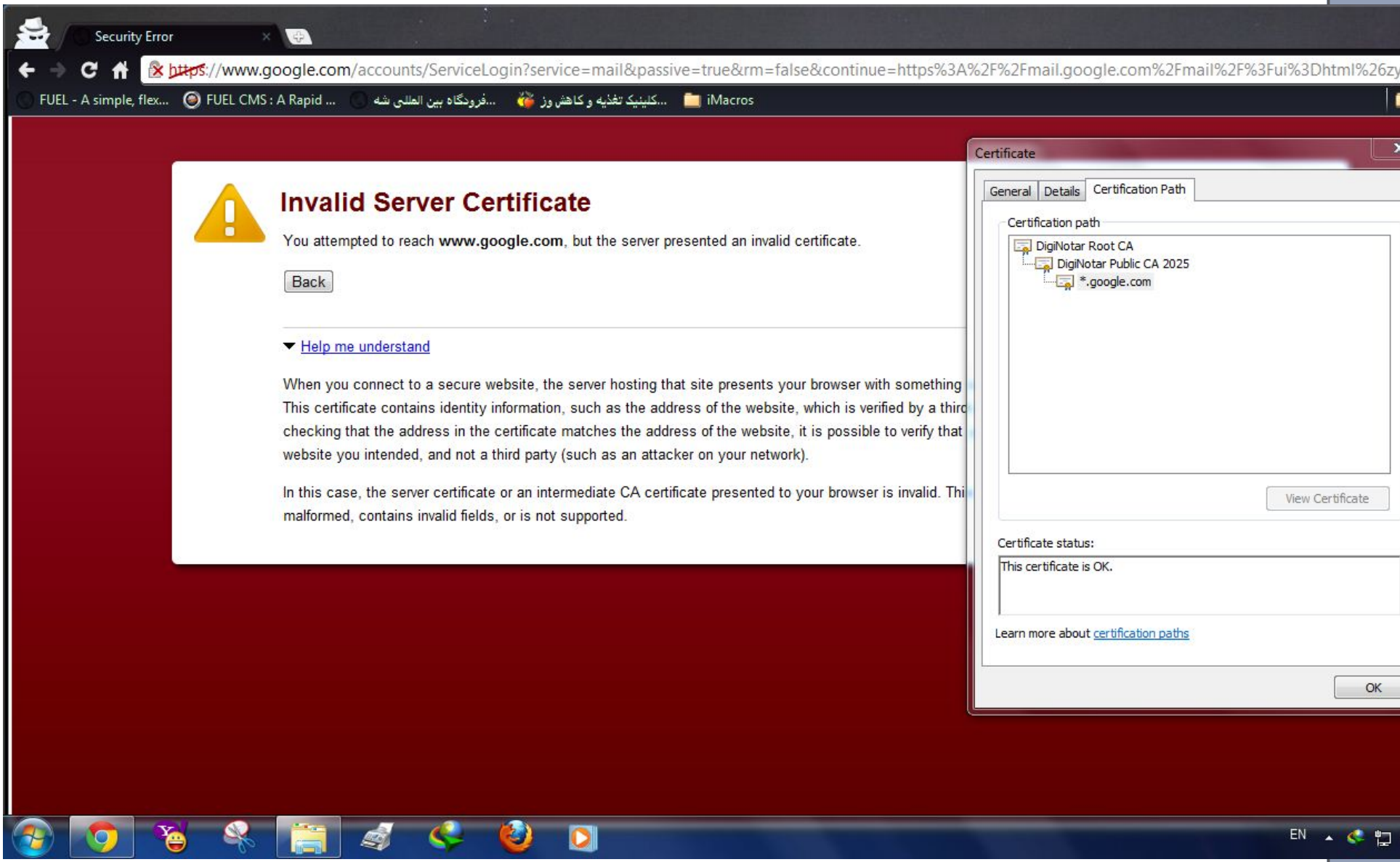
29C3

X.509 PKI: hierarchy



All CAs equal. Break one CA, break everything.

Case study: DigiNotar vs. Iran?



Crossbear: hunting the MitM

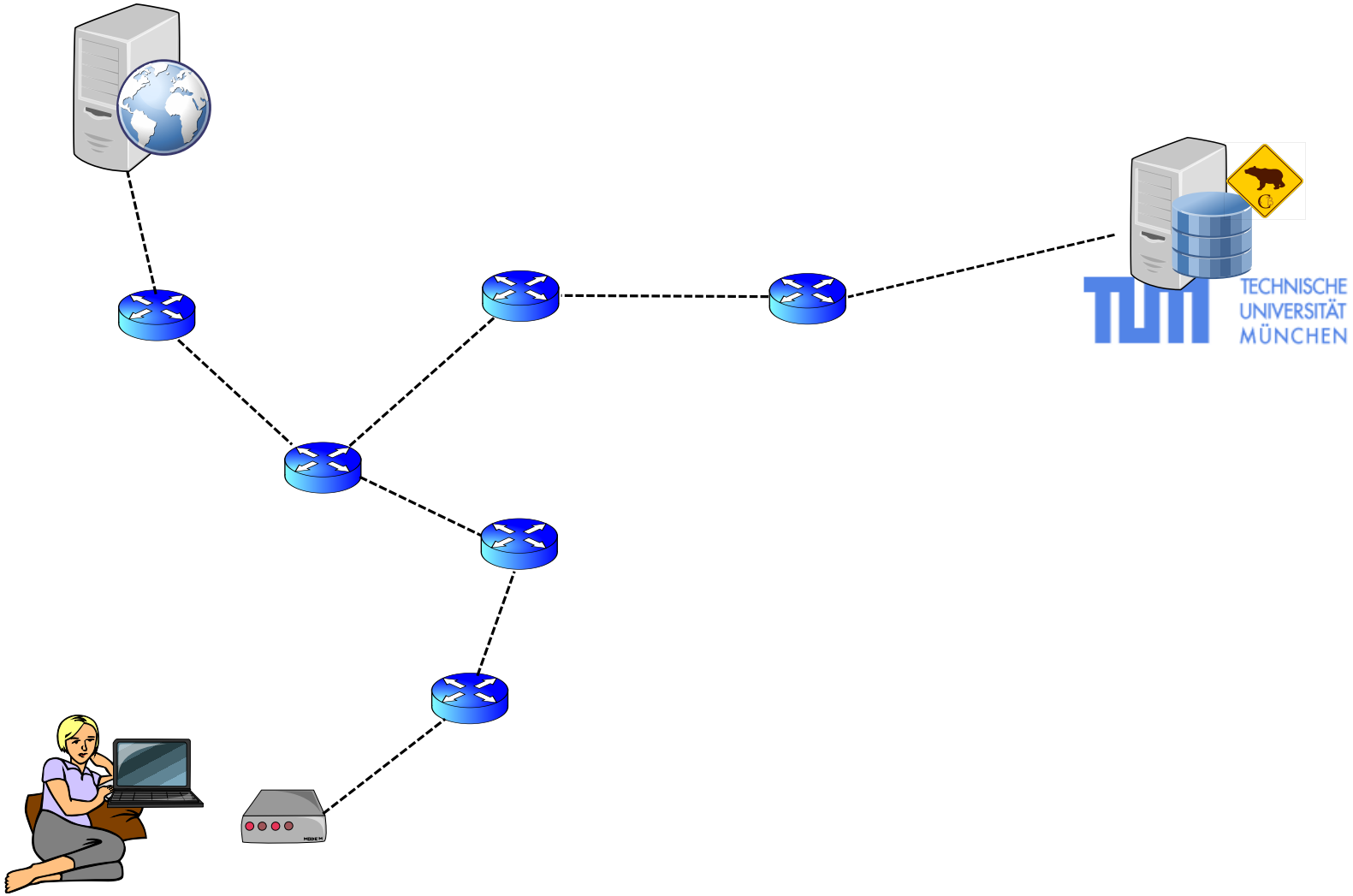
This is *not* a proposal to strengthen X.509.

Crossbear: a tool to gather *hard data*.

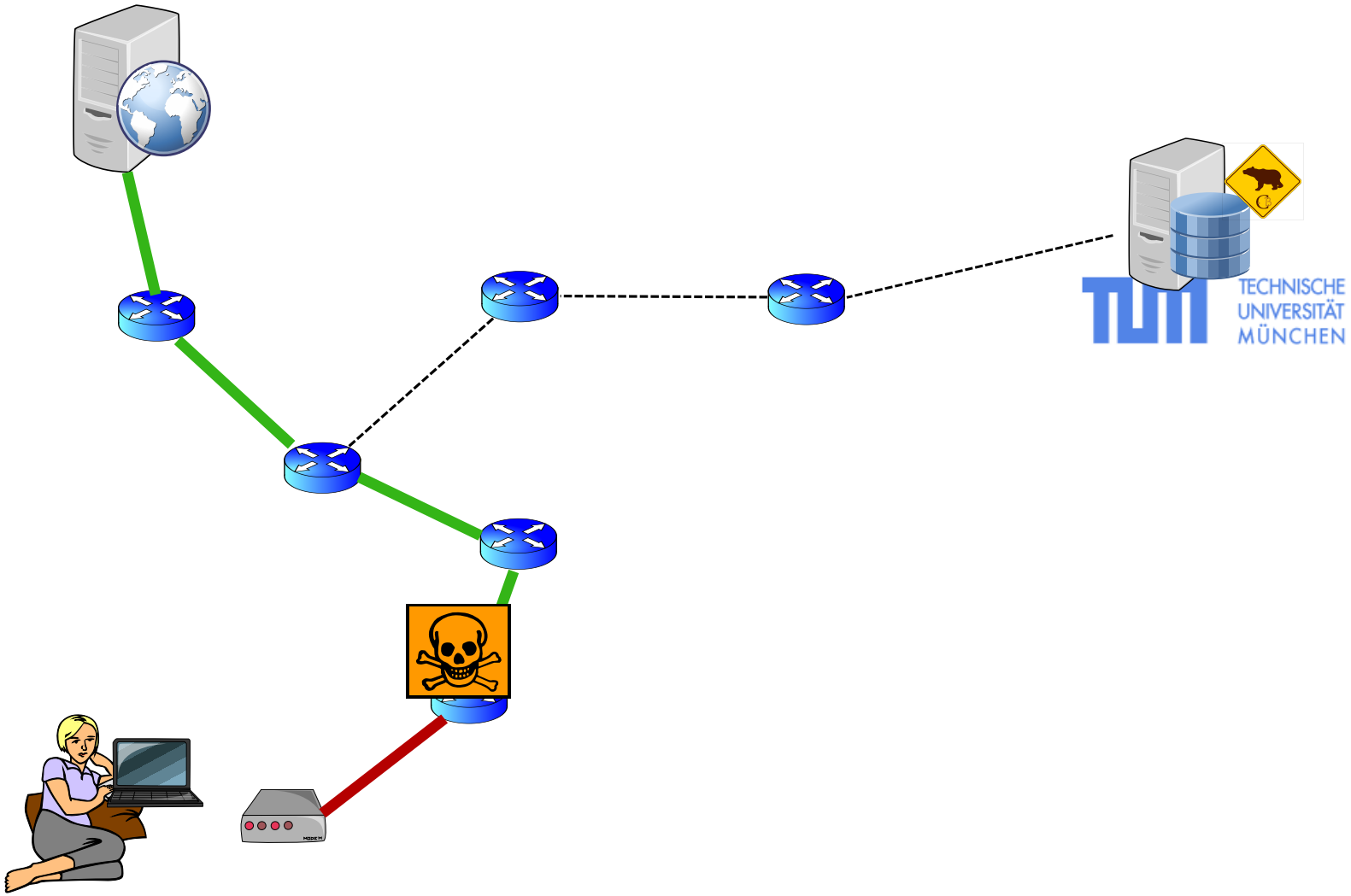
- Raise reliable data about MitM *in the wild*
- *How often* do MitM occur?
- *Where* are the attackers located?
- *Who* are the attackers?
- Are we jumping at shadows?

Method: combine notary principle, tracing and centralised reporting and analysis.

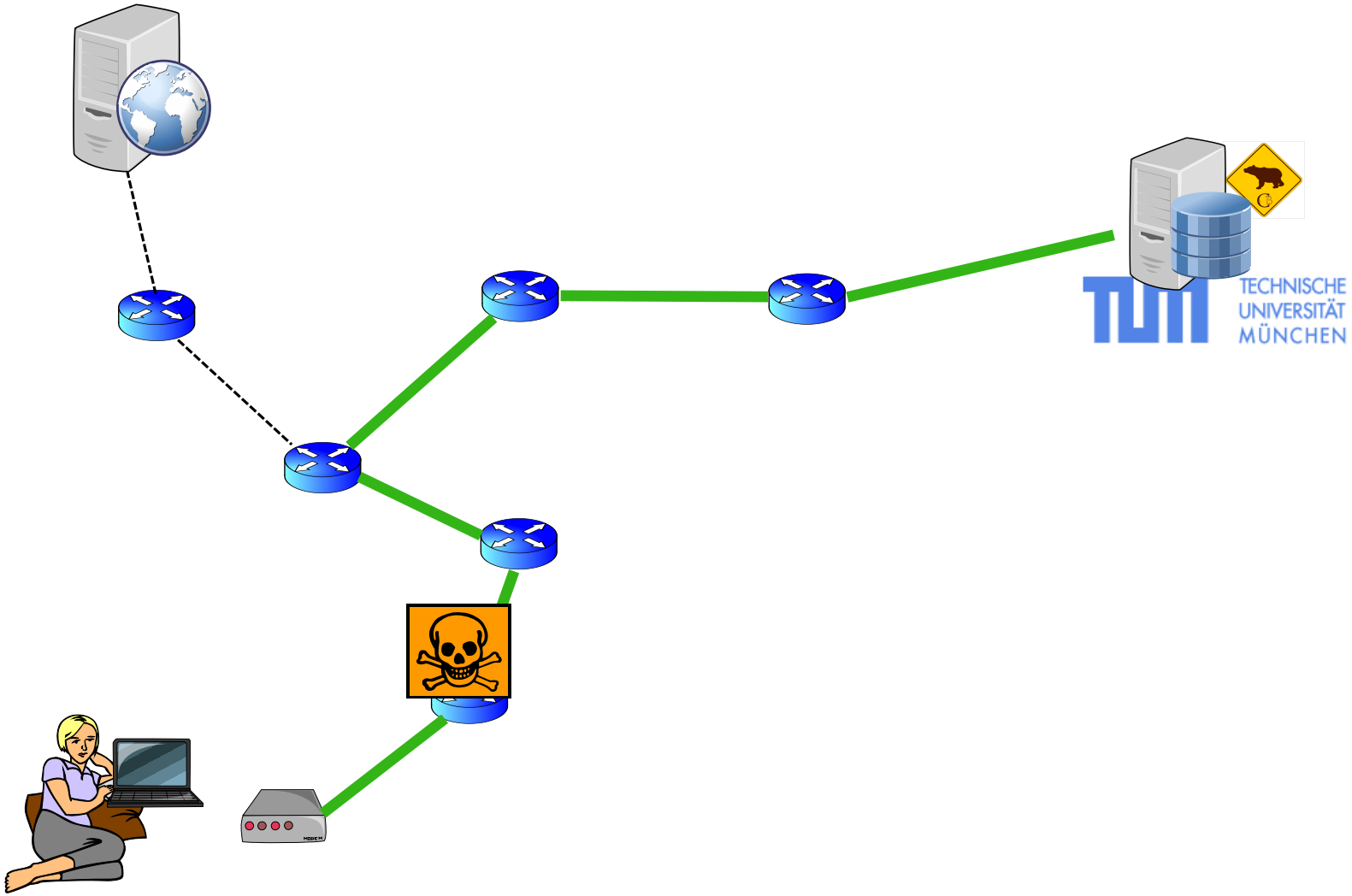
Alice is surfing...



Man-in-the-middle

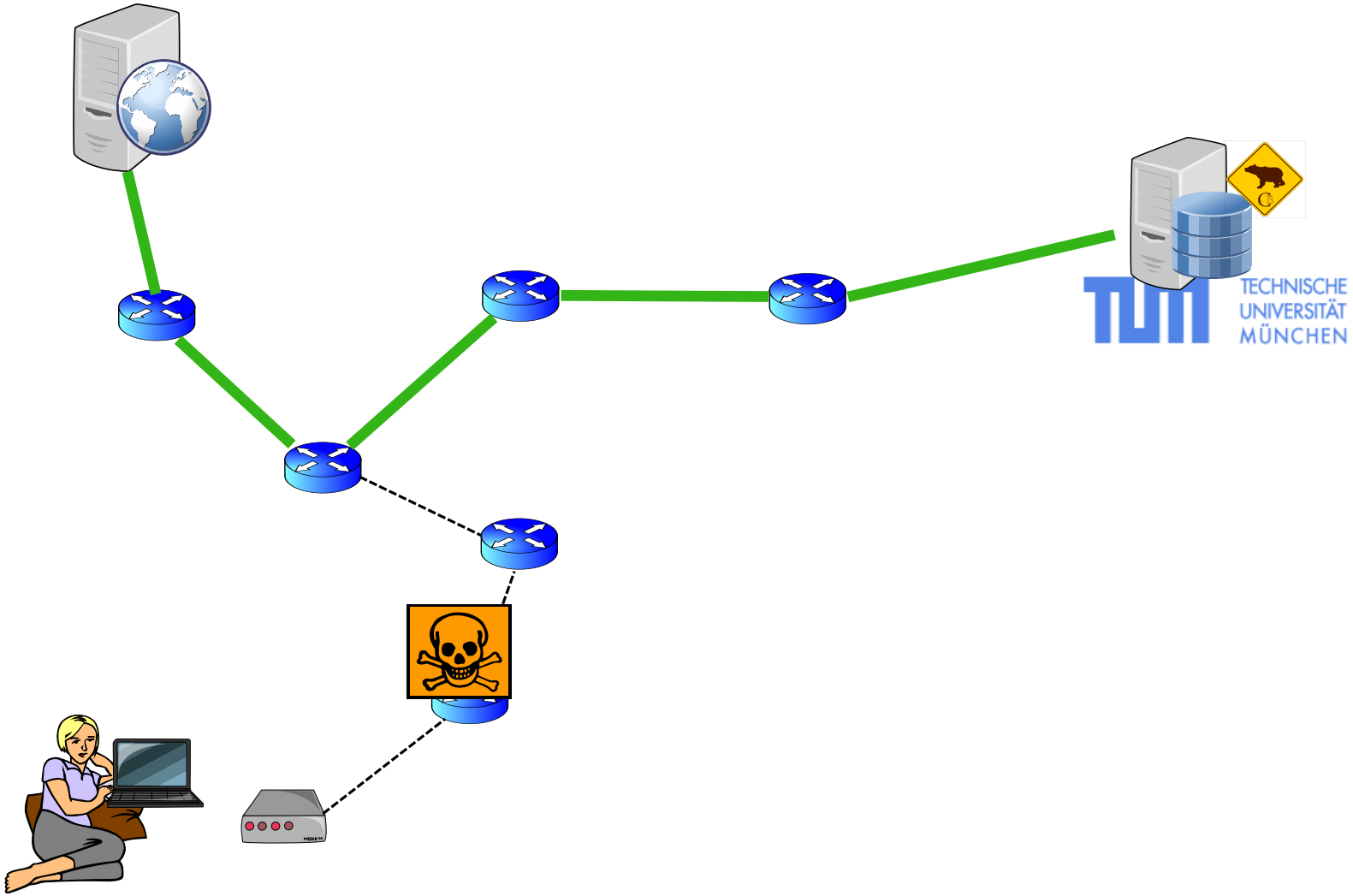


Alice queries Crossbear

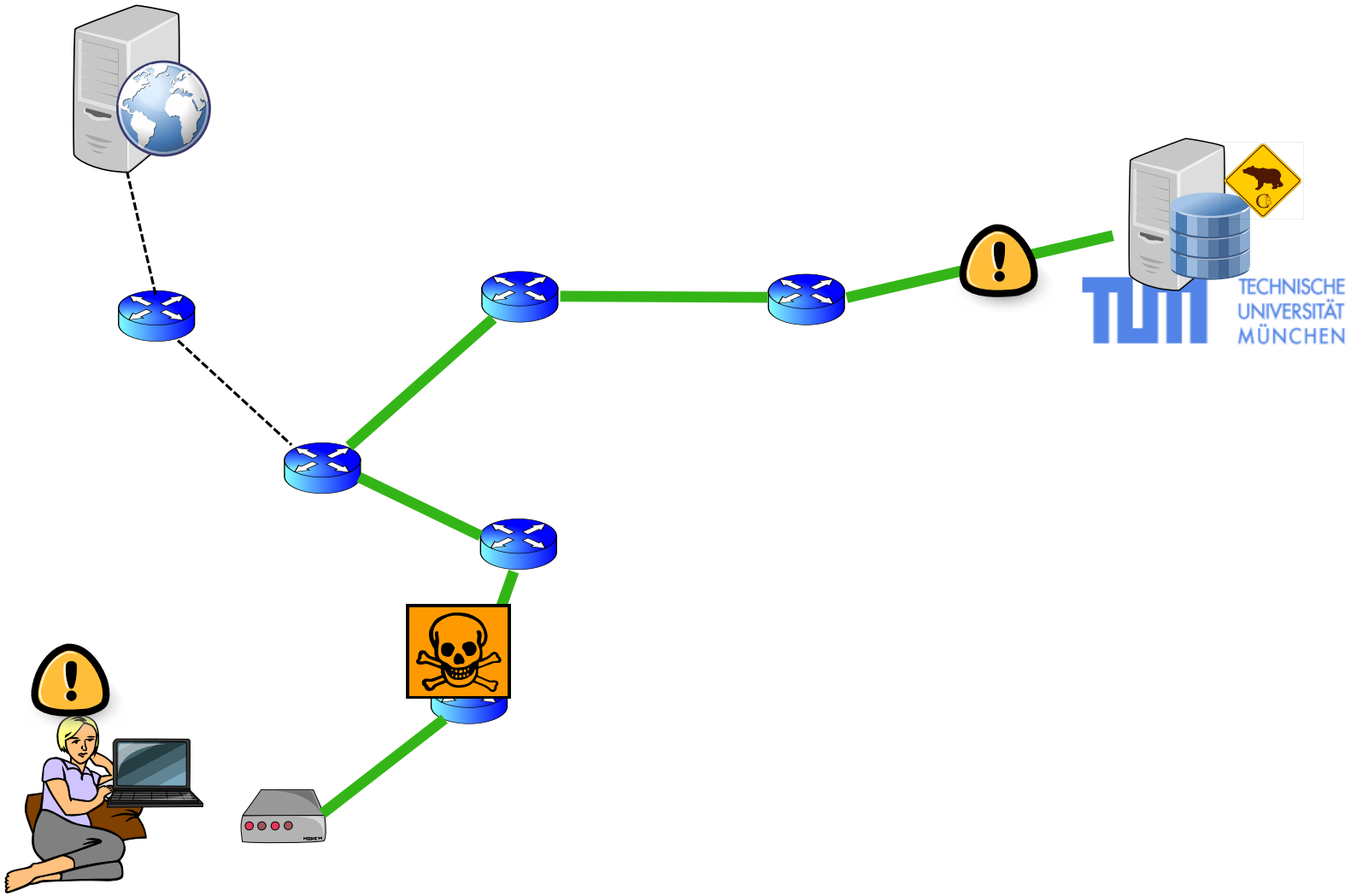


NB: SSL-secured connection, server cert hard-coded

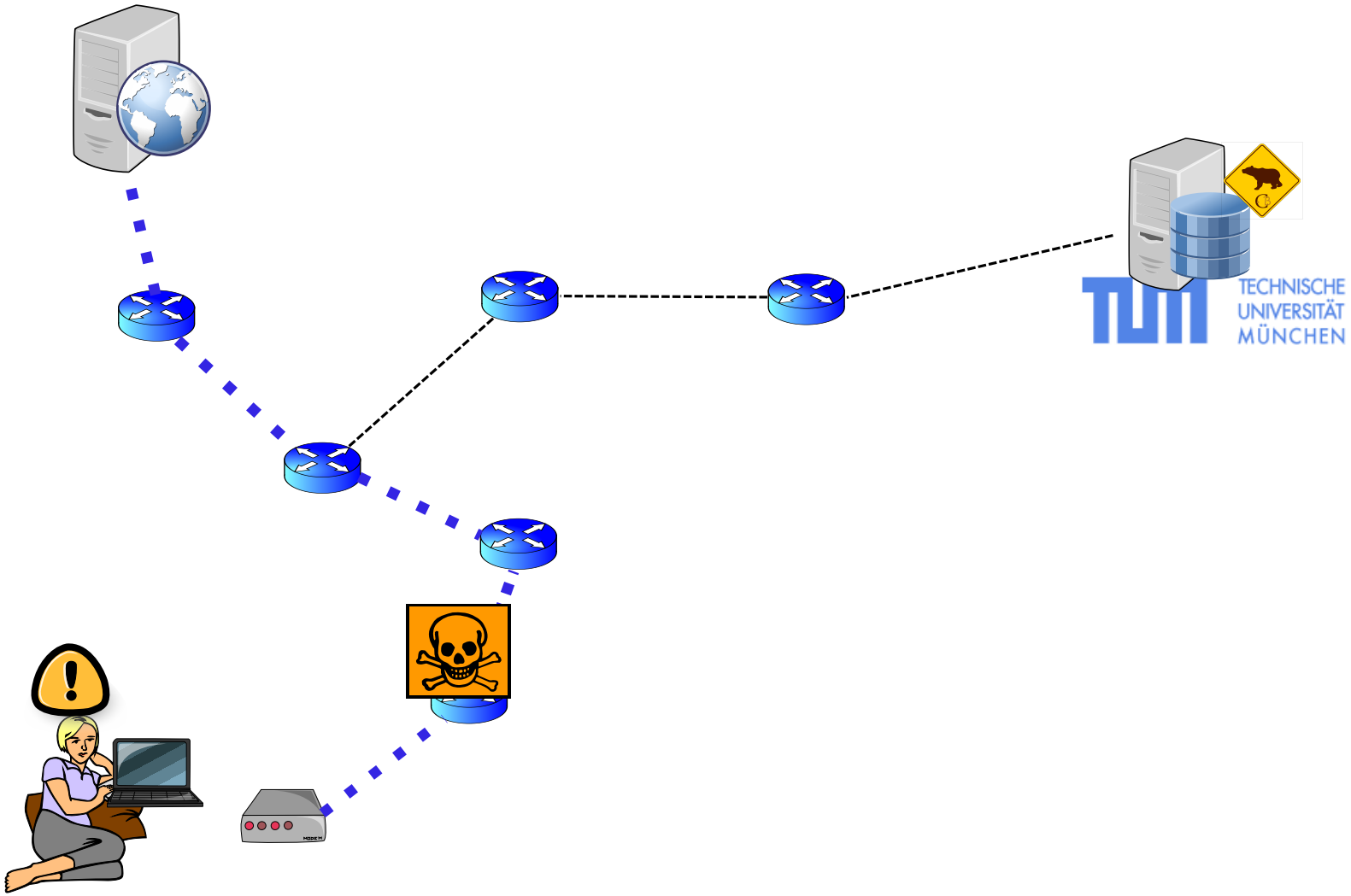
Crossbear checks the server



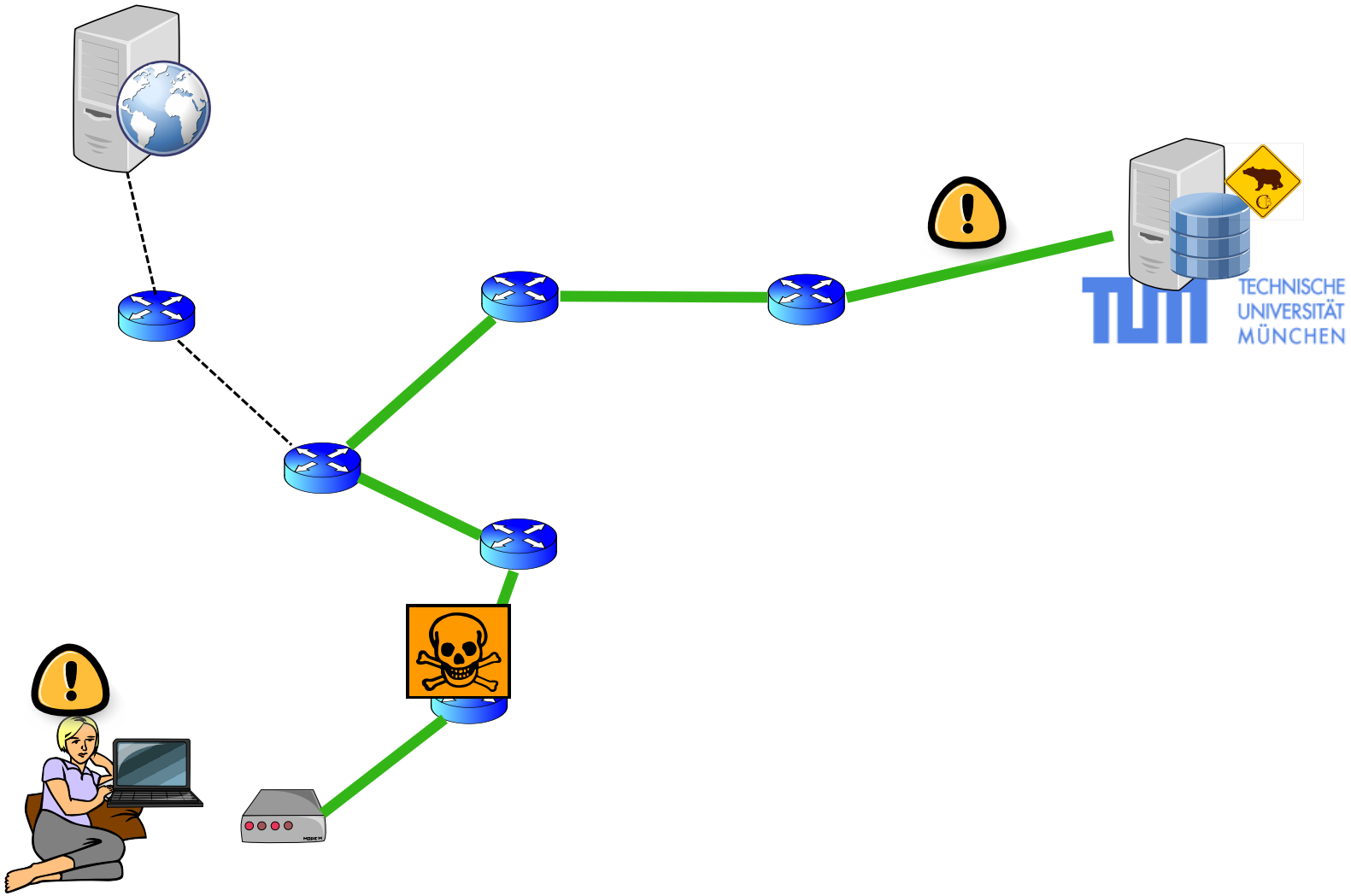
Crossbear reports result



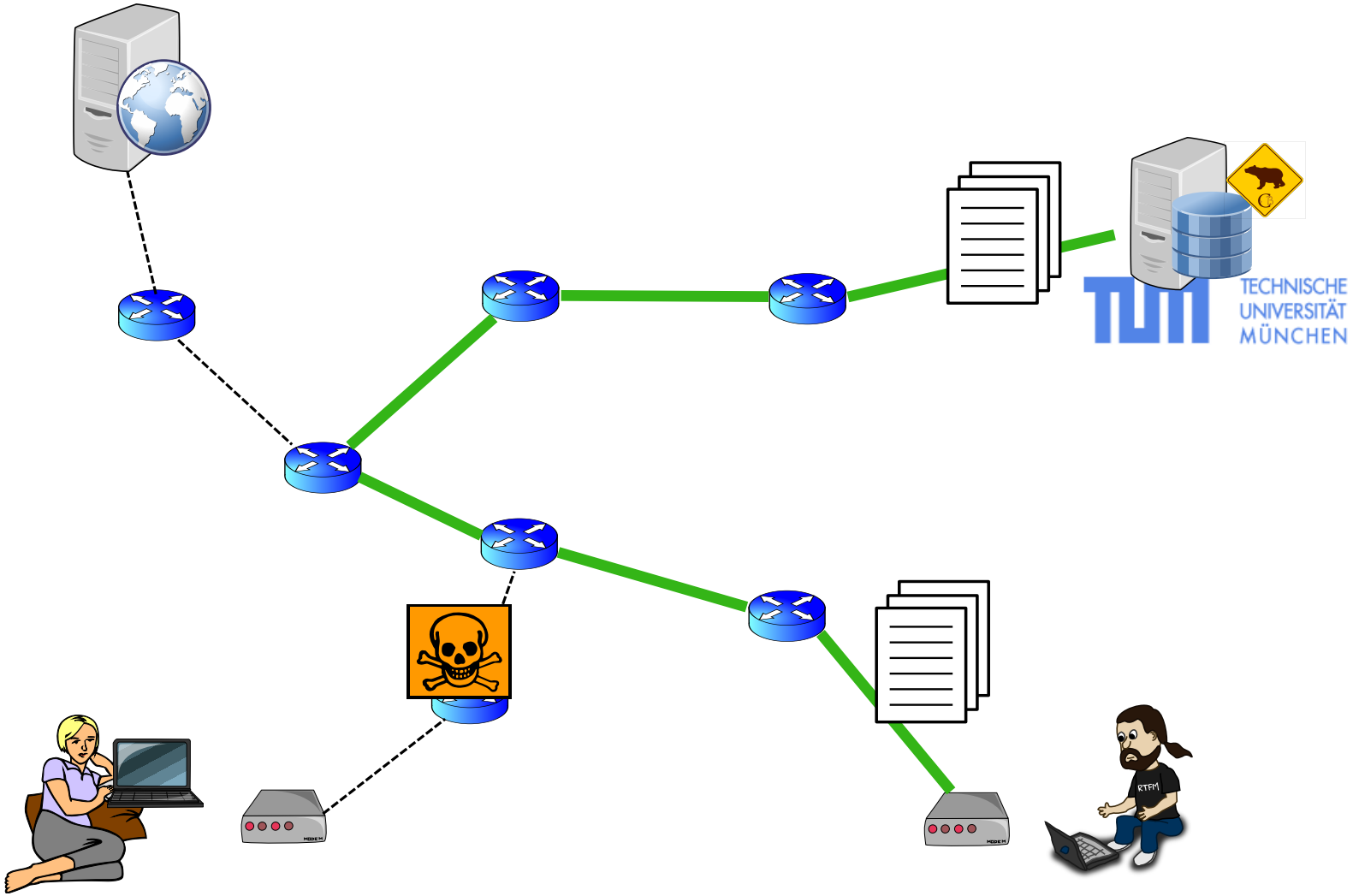
Alice traceroutes to server



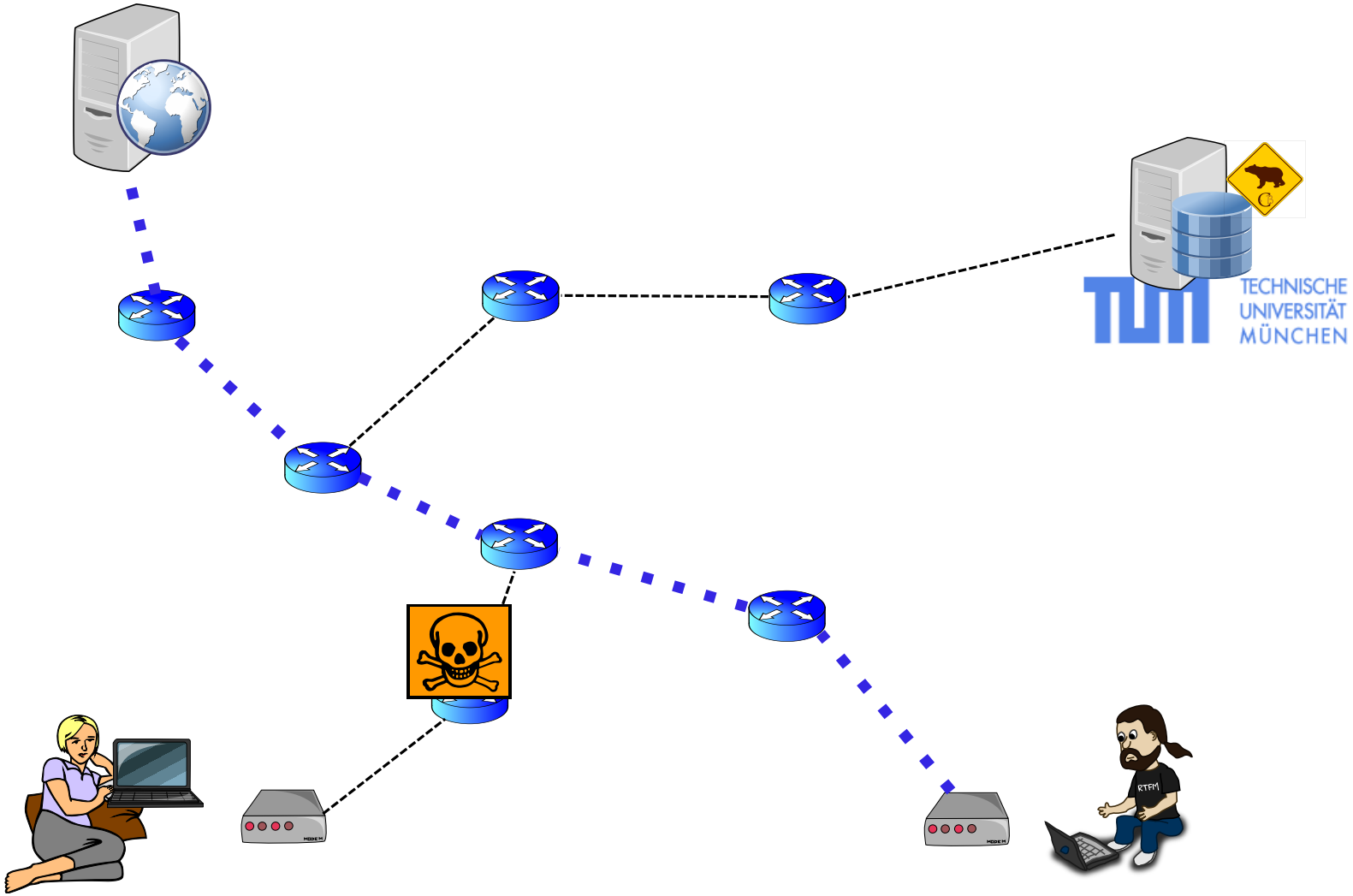
Alice reports to Crossbear



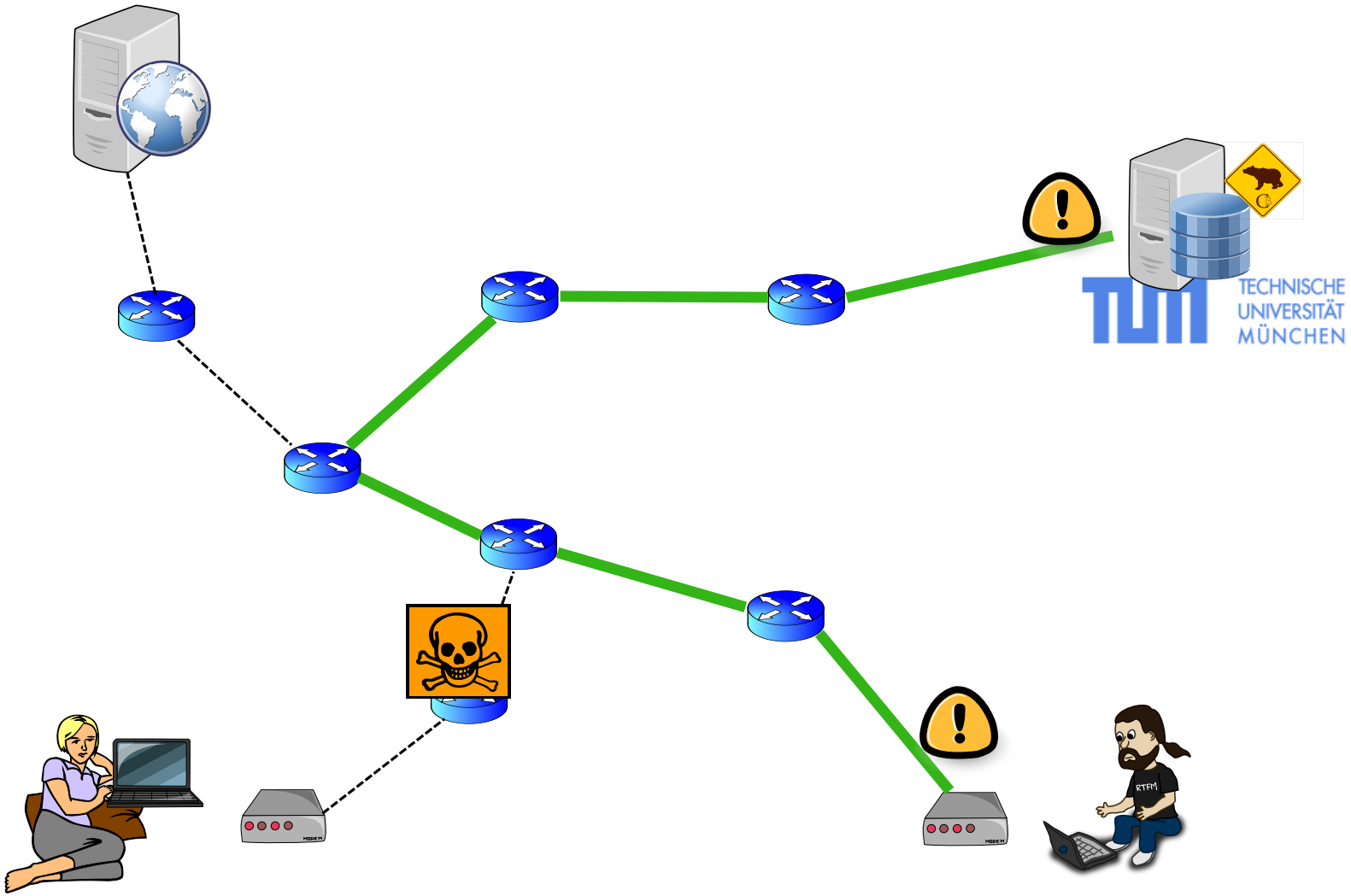
Distribute hunting tasks



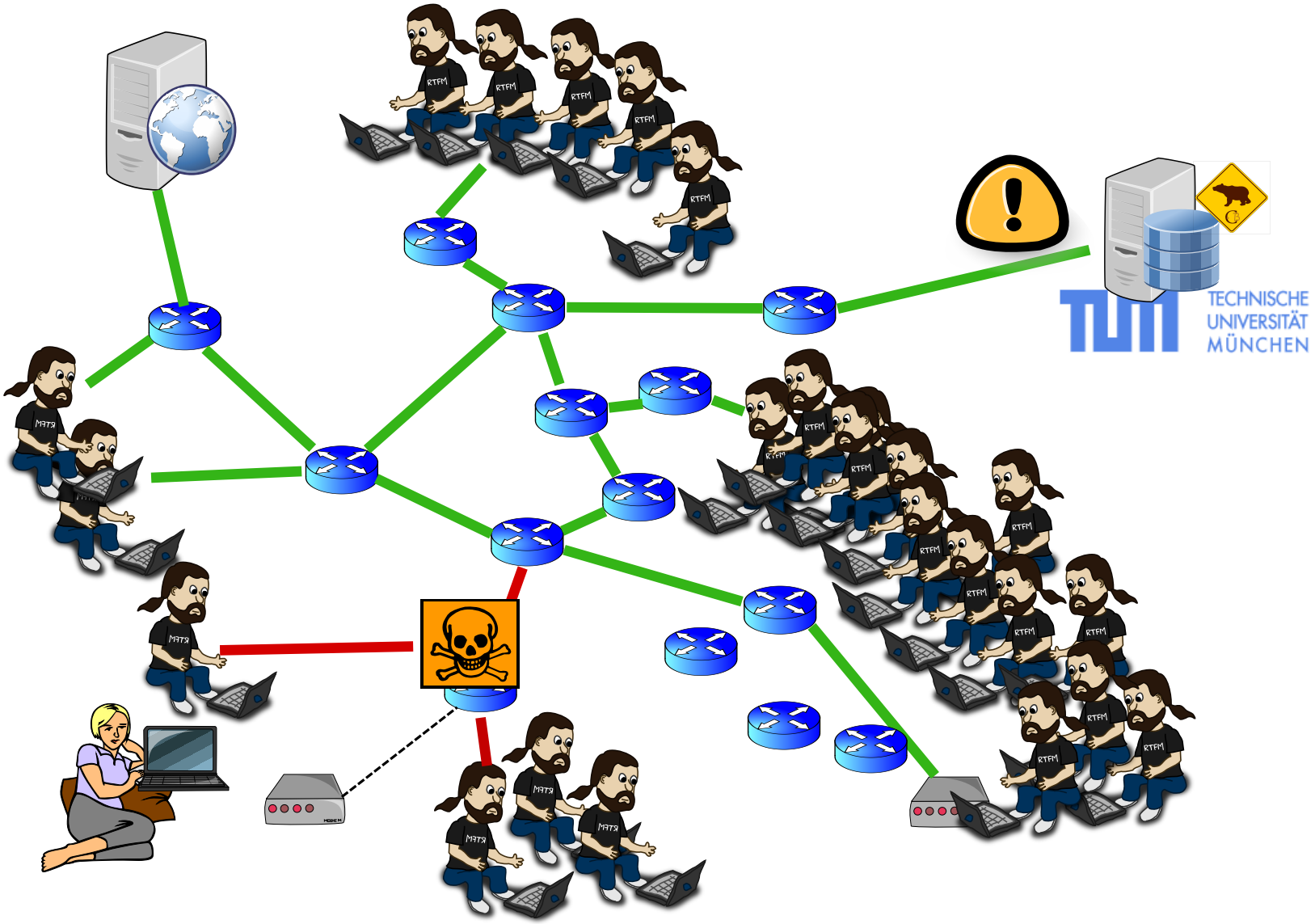
Bob goes hunting



Bob reports



There are many Bobs



Additional data raised

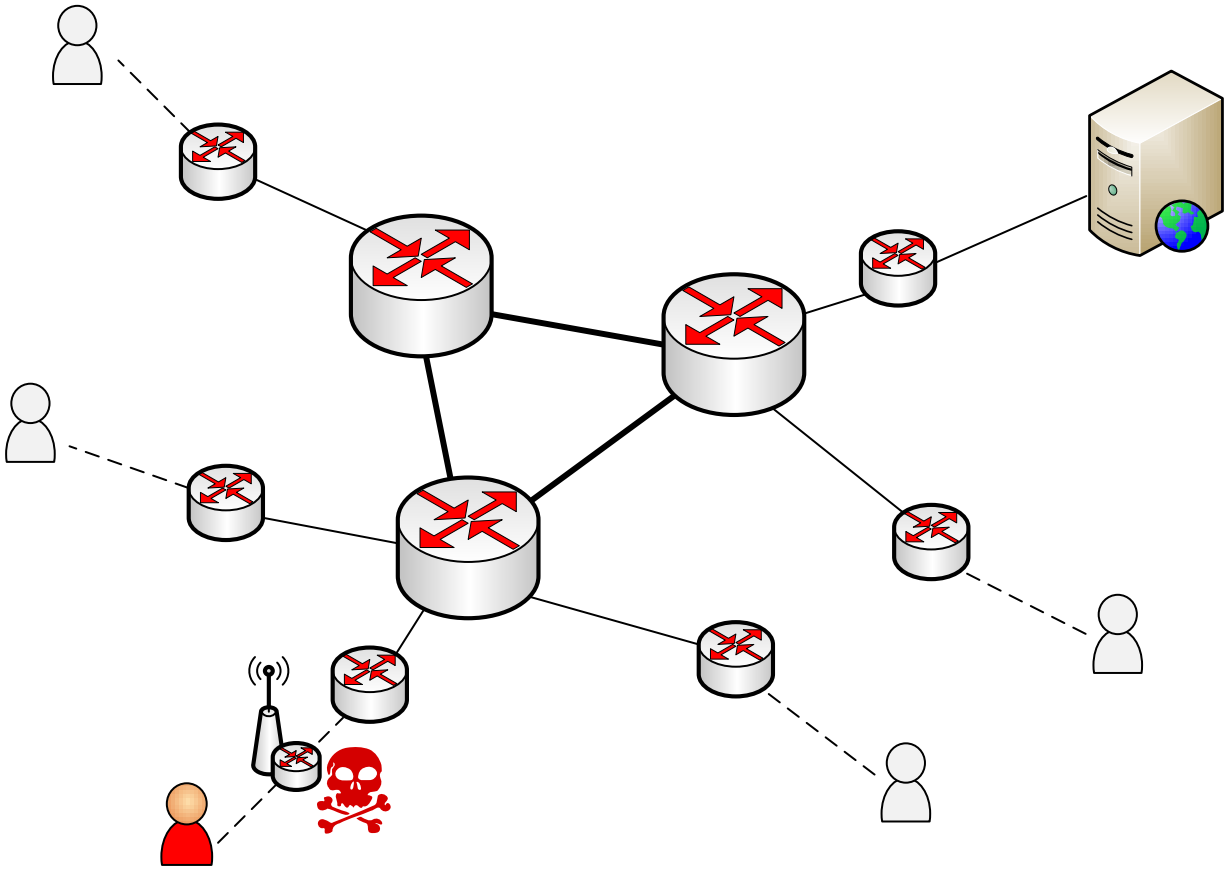
Actually, we also determine on server-side:

- CAs used in certificate chain ($\rightarrow$ continuity)
- AS number of hosts in traceroute
  ($\rightarrow$ frequent reports?)
- Geo data: location of hosts in traceroute
  ($\rightarrow$ traversed countries)
- WHOIS info

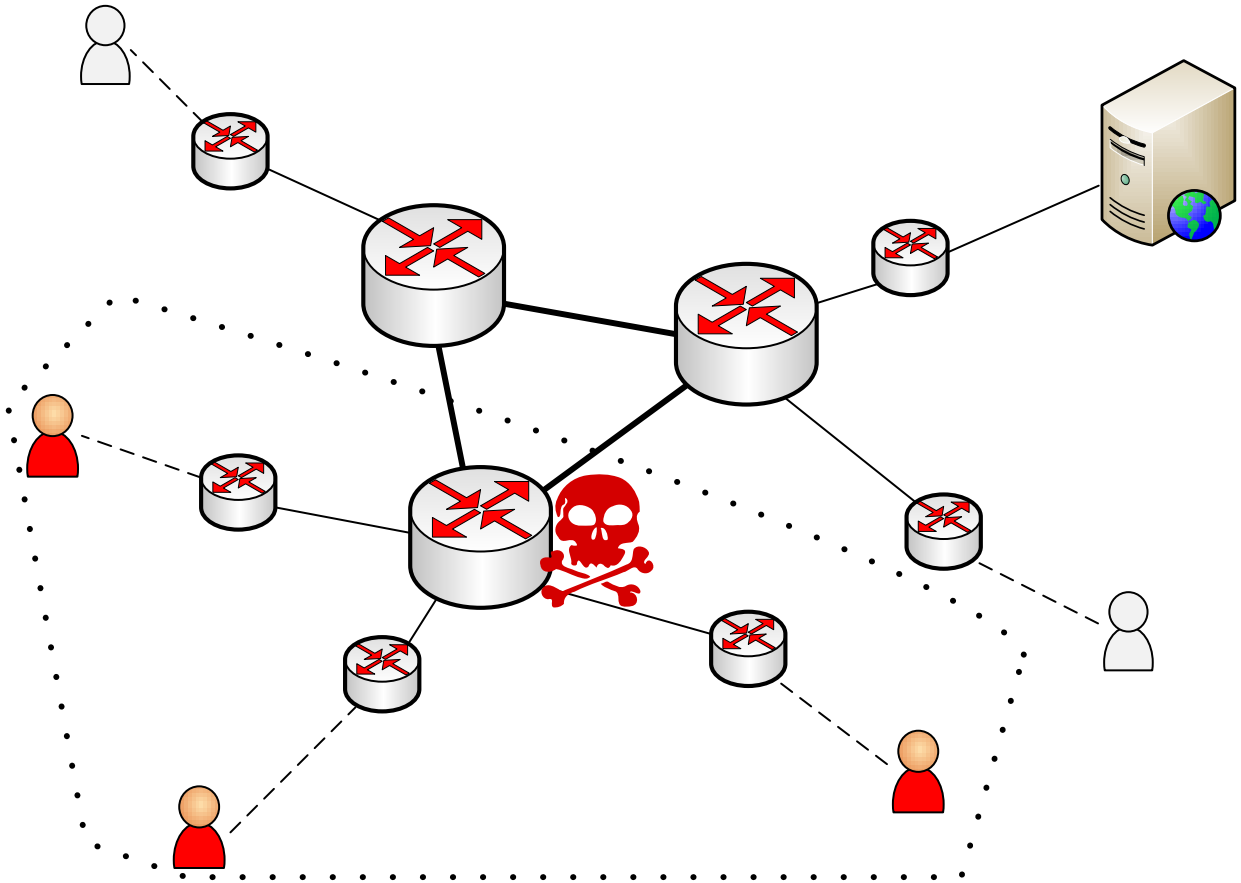
Firefox add-on

- For *savvy users*
- Score-based, several factors
- UI $\rightarrow$ see code on github

Non-selective, close to victim client



Non-selective, state-level attacker



Analysis: non-selective attacker

Detection

- Attack is detected if ≥ 1 reports

Lends itself well to localisation

- Get ≥ 1 traceroute from victim, ≥ 1 from unpoisoned hunter
- The more, the better. The closer to intersection point, the better.
- An estimate can be given:
  < 100 hunters for 95% accuracy on AS-level
- Adaptive attackers are a problem (can't discuss here)
- Full details in our research paper

Different problem: SSH

```
ralph@fiorentino:~$ ssh root@in.tum.de
The authenticity of host 'in.tum.de (131.159.0.35)' can't be established.
RSA key fingerprint is e4:c4:24:27:19:dc:e0:e2:96:1a:be:23:d5:e6:9d:18.
Are you sure you want to continue connecting (yes/no)?
```

Ever had this problem?

- Want to compare an SSH fingerprint without 2nd channel?
- No idea what the correct host-key should be?

Crossbear is coming to SSH

Use our shiny new notary

- `cbssh.net.in.tum.de`
- Allows live checks, and static lookups

Build a database of keys

- We scanned about 75% of IPv4 and collected host-keys
- Collected about 7.5 million keys
- That was a lot of fun...

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

To go live for general public in February

- Code still needs to undergo review
- Tracerouting for stand-alone hunters soon
- Don't want to use our notary? It's GPL. Set up your own.

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}]}’’
```

Scanning the IPv4 space on port 22

How to scan SSH – and live to tell the tale

- Get your own Autonomous System. Because your ISP will hate you.
- Be nice to your admin. He will hate you, too.
- Don’t do stateful tracking on your firewall.
- Be prepared to see your routers die at 75%
- Be prepared to get many complaints by mail.
- Write to CERTs! To Blacklists!
- You can scan in 5 days with just one strong server
- You will make new friends!

Scanning the IPv4 space on port 22

How to scan SSH – and live to tell the tale

- Get your own Autonomous System. Because your ISP will hate you.
- Be nice to your admin. He will hate you, too.
- Don’t do stateful tracking on your firewall.
- Be prepared to see your routers die at 75%
- Be prepared to get many complaints by mail.
- Write to CERTs! To Blacklists!
- You can scan in 5 days with just one strong server
- You will make new friends!

Scanning the IPv4 space on port 22

How to scan SSH – and live to tell the tale

- Get your own Autonomous System. Because your ISP will hate you.
- Be nice to your admin. He will hate you, too.
- Don’t do stateful tracking on your firewall.
- Be prepared to see your routers die at 75%
- Be prepared to get many complaints by mail.
- Write to CERTs! To Blacklists!
- You can scan in 5 days with just one strong server
- You will make new friends!

Scanning the IPv4 space on port 22

How to scan SSH – and live to tell the tale

- Get your own Autonomous System. Because your ISP will hate you.
- Be nice to your admin. He will hate you, too.
- Don’t do stateful tracking on your firewall.
- Be prepared to see your routers die at 75%
- Be prepared to get many complaints by mail.
- Write to CERTs! To Blacklists!
- You can scan in 5 days with just one strong server
- You will make new friends!

Scanning the IPv4 space on port 22

How to scan SSH – and live to tell the tale

- Get your own Autonomous System. Because your ISP will hate you.
- Be nice to your admin. He will hate you, too.
- Don’t do stateful tracking on your firewall.
- Be prepared to see your routers die at 75%
- Be prepared to get many complaints by mail.
- Write to CERTs! To Blacklists!
- You can scan in 5 days with just one strong server
- You will make new friends!

Scanning the IPv4 space on port 22

How to scan SSH – and live to tell the tale

- Get your own Autonomous System. Because your ISP will hate you.
- Be nice to your admin. He will hate you, too.
- Don’t do stateful tracking on your firewall.
- Be prepared to see your routers die at 75%
- Be prepared to get many complaints by mail.
- Write to CERTs! To Blacklists!
- You can scan in 5 days with just one strong server
- You will make new friends!

Scanning the IPv4 space on port 22

How to scan SSH – and live to tell the tale

- Get your own Autonomous System. Because your ISP will hate you.
- Be nice to your admin. He will hate you, too.
- Don’t do stateful tracking on your firewall.
- Be prepared to see your routers die at 75%
- Be prepared to get many complaints by mail.
- Write to CERTs! To Blacklists!
- You can scan in 5 days with just one strong server
- You will make new friends!

Scanning the IPv4 space on port 22

How to scan SSH – and live to tell the tale

- Get your own Autonomous System. Because your ISP will hate you.
- Be nice to your admin. He will hate you, too.
- Don’t do stateful tracking on your firewall.
- Be prepared to see your routers die at 75%
- Be prepared to get many complaints by mail.
- Write to CERTs! To Blacklists!
- You can scan in 5 days with just one strong server
- You will make new friends!

Scanning the IPv4 space on port 22

How to scan SSH – and live to tell the tale

- Get your own Autonomous System. Because your ISP will hate you.
- Be nice to your admin. He will hate you, too.
- Don’t do stateful tracking on your firewall.
- Be prepared to see your routers die at 75%
- Be prepared to get many complaints by mail.
- Write to CERTs! To Blacklists!
- You can scan in 5 days with just one strong server
- You will make new friends!

Scanning the IPv4 space on port 22

How to scan SSH – and live to tell the tale

- Get your own Autonomous System. Because your ISP will hate you.
- Be nice to your admin. He will hate you, too.
- Don’t do stateful tracking on your firewall.
- Be prepared to see your routers die at 75%
- Be prepared to get many complaints by mail.
- Write to CERTs! To Blacklists!
- You can scan in 5 days with just one strong server
- You will make new friends!

Scanning the IPv4 space on port 22

How to scan SSH – and live to tell the tale

- Get your own Autonomous System. Because your ISP will hate you.
- Be nice to your admin. He will hate you, too.
- Don’t do stateful tracking on your firewall.
- Be prepared to see your routers die at 75%
- Be prepared to get many complaints by mail.
- Write to CERTs! To Blacklists!
- You can scan in 5 days with just one strong server
- You will make new friends!

Some complaints

'No problem. Vielen Dank for the reply.'

- Many reports from academic institutes. In general, no need to blacklist.
- $<$ 10 wanted to be blacklisted – 50% of them private persons.

Some complaints

'No problem. Vielen Dank for the reply.'

- Many reports from academic institutes. In general, no need to blacklist.
- $<$ 10 wanted to be blacklisted – 50% of them private persons.

Some complaints

'No problem. Vielen Dank for the reply.'

- Many reports from academic institutes. In general, no need to blacklist.
- < 10 wanted to be blacklisted – 50% of them private persons.

Our position

A first step towards gathering better data

- We *do not* advertise Crossbear as a silver bullet
- Best results can be expected against the non-selective attacker
- These are also the attackers we are most interested in

Crossbear is deployed and ready

- 150 hunters on PlanetLab
- 4,000 certificate reports – no MitM

What's next?

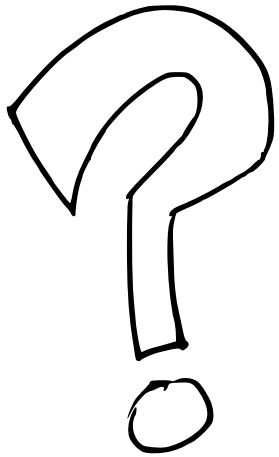
Integration with OONI

- Open Observatory of Network Interference
- Hopefully, many clients soon
- Plus people who are in the right locations...
- That is where all our efforts will go into in the next 6 months

Analysis tools

- Automate analysis of reports
- Filter out and group by suspicious cases

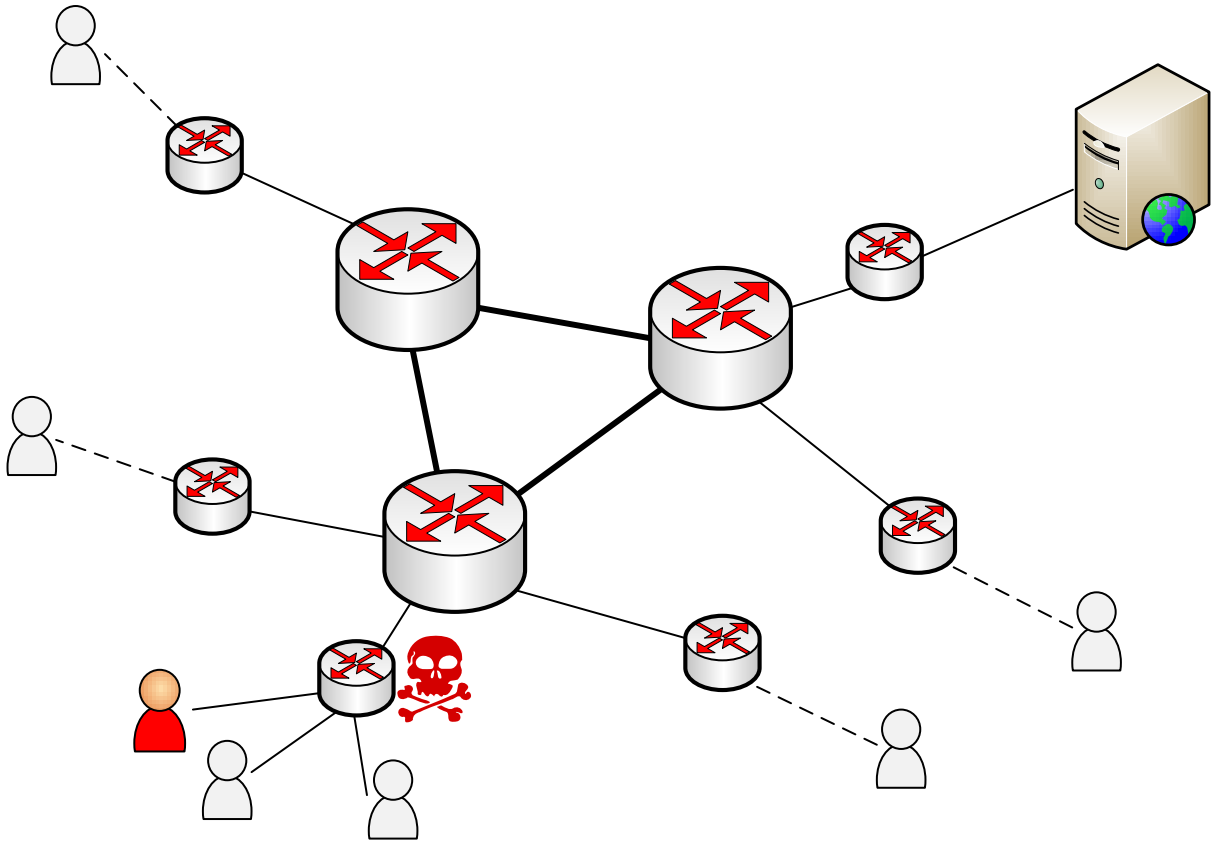
Thank you!



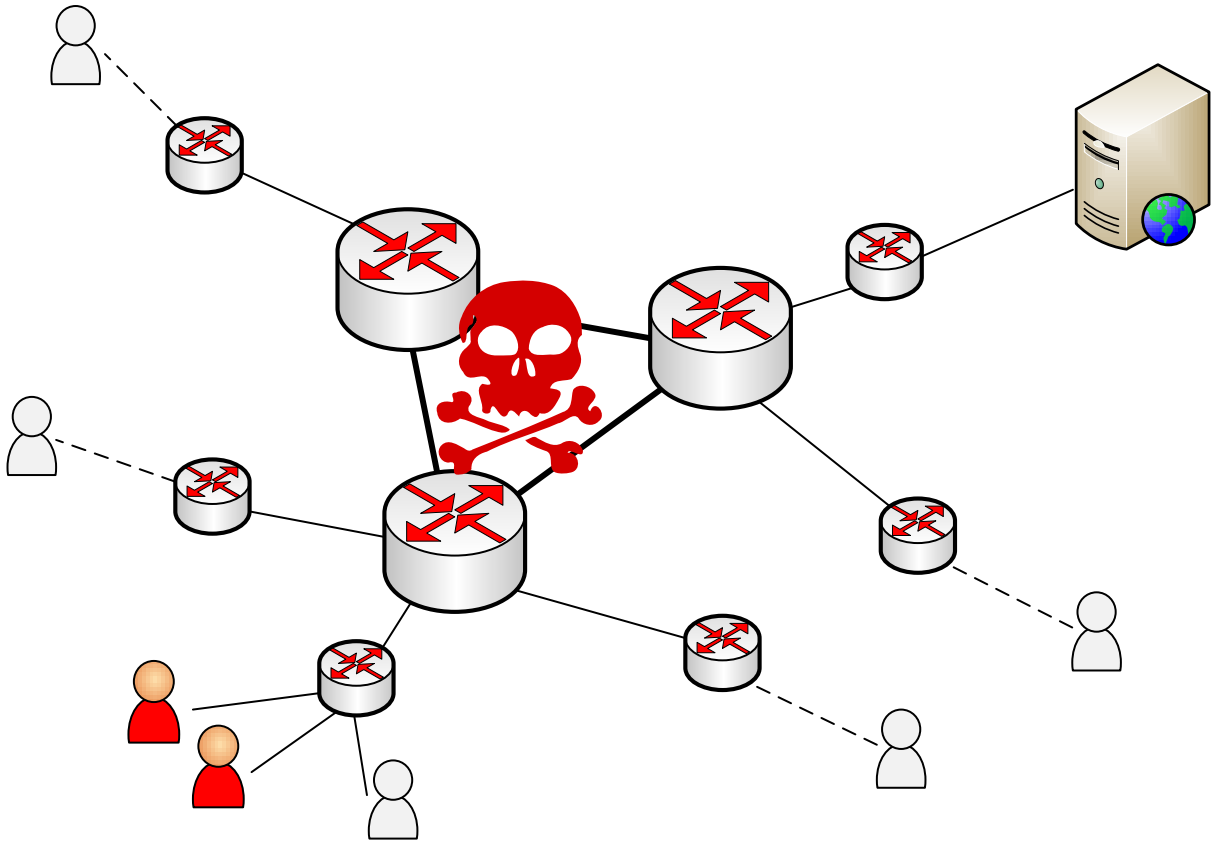
Contact

- Twitter: @crossbearteam
- WWW: `https://pki.net.in.tum.de`
- `https://github.com/crossbear/Crossbear`

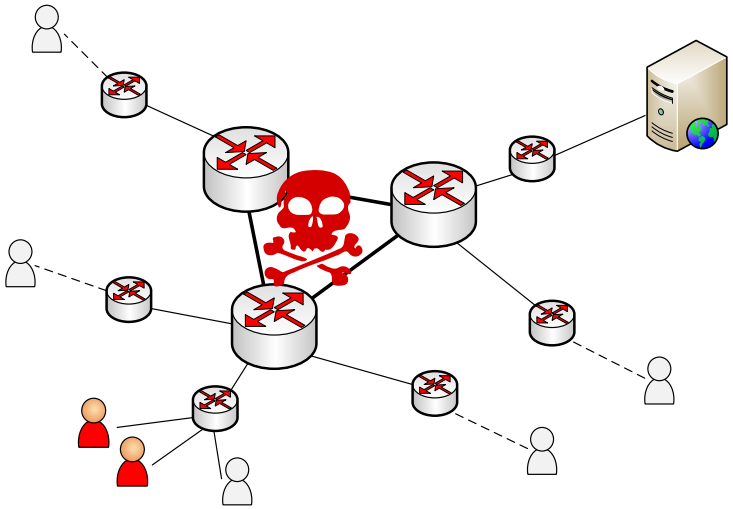
Selective attacker: close to victim



Selective attacker: in core



Selective attackers are a headache



Can be indistinguishable from non-selective attacks

- *Every* attack report to be checked for plausibility
- But attacker should leave some hints – cannot arbitrarily spoof IP addresses

Patterns to look for

Attack seems to be restricted to few stub AS

- Use BGP data to check traceroutes for plausibility
- Do MitM certificates share properties?
- Which AS in which countries involved?

MitM reports from just a few companies?

- Check traceroutes for traversed countries and AS
- Might be industrial espionage

All of this is intensive manual work. But only localisation is affected, and it is better than no data all.