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?

Invalid Server Certificate

You attempted to reach www.google.com, but the server presented an invalid certificate.

Back

Help me understand

When you connect to a secure website, the server hosting that site presents your browser with something called a server certificate. This certificate contains identity information, such as the address of the website, which is verified by a third-party called a certificate authority (CA). Checking that the address in the certificate matches the address of the website, it is possible to verify that the website you intended, and not a third party (such as an attacker on your network).

In this case, the server certificate or an intermediate CA certificate presented to your browser is invalid. The certificate is either malformed, contains invalid fields, or is not supported.
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

Ralph Holz, Oliver Gasser: One year of Crossbear
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 (→ continuity)
- AS number of hosts in traceroute (→ frequent reports?)
- Geo data: location of hosts in traceroute (→ traversed countries)
- WHOIS info

**Firefox add-on**

- For *savvy users*
- Score-based, several factors
- UI → see code on github
Non-selective, close to victim client
Non-selective, state-level attacker
Analysis: non-selective attacker

Detection

- Attack is detected if $\geq 1$ reports

Lends itself well to localisation

- Get $\geq 1$ traceroute from victim, $\geq 1$ 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
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.
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:
```
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!
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!
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!
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!
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!
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!
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!
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!
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.