The State of OnionCat

Dipl.-Ing. **Bernhard R. Fischer**

#itsecx2019

11.8.2019

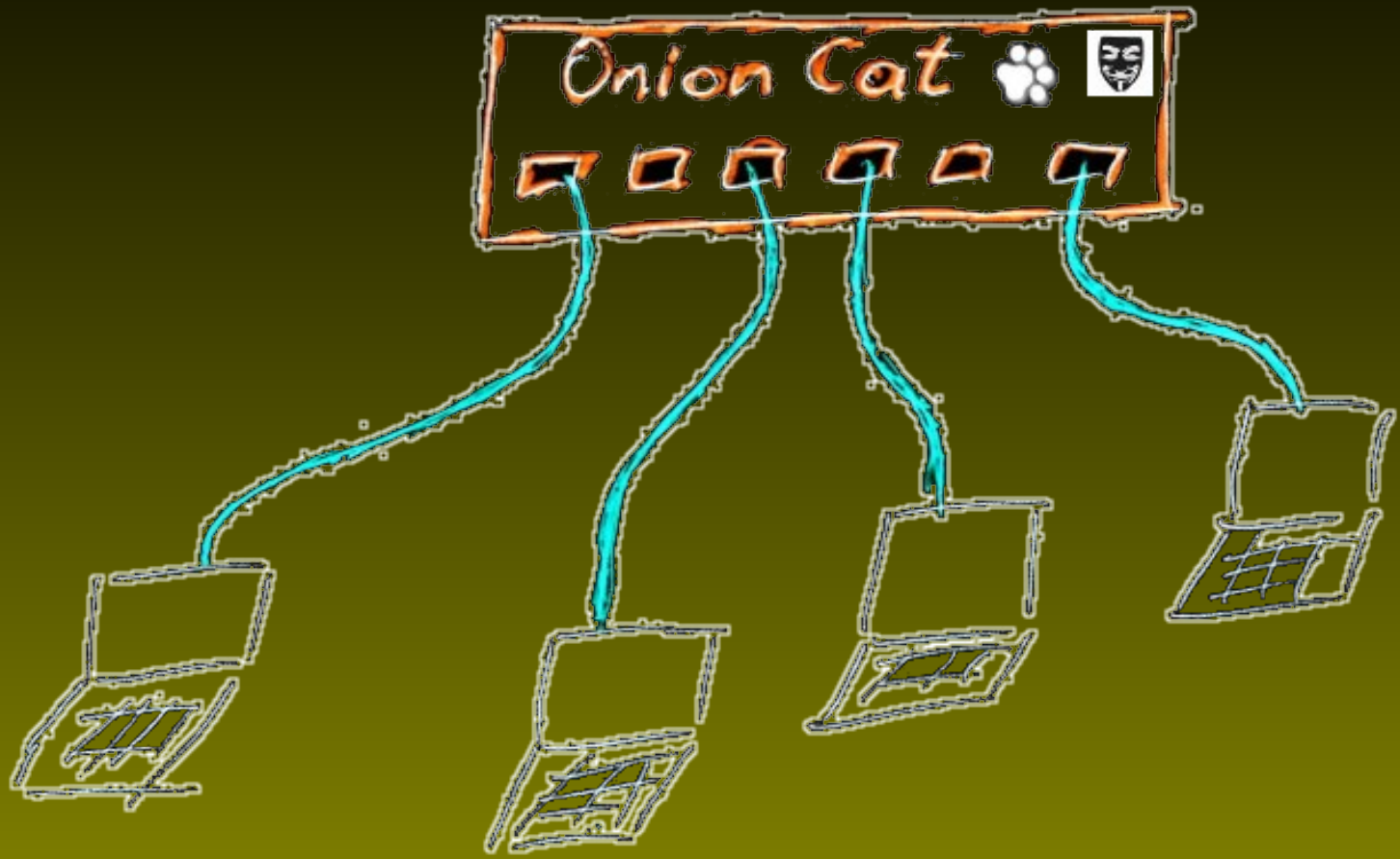
<bf@abenteuerland.at>
98678E06 063007E4 A1F0B9C5 9BD60166 8E24F29D

```
say(what_is(”OnionCat”));
```

say(what_is(”OnionCat”));

OnionCat is a peer-to-peer VPN providing anonymity by using Tor/I2P.

OnionCat acts like a switch



OnionCat.addressing()

OnionCat translates between

donofeeddeadbeef.onion

and

fd87:d87e:eb43:1b9a:e290:8319:30:9085

Method was adapted by ”Bitcoin Core” ;)

history <<OnionCat

2006/12: 1st ideas (@23C3)
2008/02: 1st commit (not sure...)
2008/06: 1st package online
2008/12: 1st talk @25C3/Berlin
2014/11: talk @itsecx, upcoming HSv3
…ongoing development…
2019/09: latest commit ;)

git log | head -10

- Rewrite of ifup code.
- **SOCKS5** support and **DIRECT_CONNECT**
- loopback_responders
- support for **HSv3**

```
% ping6 fd87:d87e:eb43::dead:beef
PING fd87:d87e:eb43::dead:beef(fd87:d87e:eb43::dead:beef) 56 data bytes
64 bytes from fd87:d87e:eb43::dead:beef: icmp_seq=1 ttl=64 time=0.343 ms
64 bytes from fd87:d87e:eb43::dead:beef: icmp_seq=2 ttl=64 time=0.468 ms
64 bytes from fd87:d87e:eb43::dead:beef: icmp_seq=3 ttl=64 time=0.642 ms
^C
% ping6 fd87:d87e:eb43::feed:beef
PING fd87:d87e:eb43::feed:beef(fd87:d87e:eb43::feed:beef) 56 data bytes
64 bytes from fd87:d87e:eb43::feed:beef: icmp_seq=1 ttl=64 time=2049 ms
64 bytes from fd87:d87e:eb43::feed:beef: icmp_seq=2 ttl=64 time=1628 ms
64 bytes from fd87:d87e:eb43::feed:beef: icmp_seq=3 ttl=64 time=741 ms
```

Hidden services V2

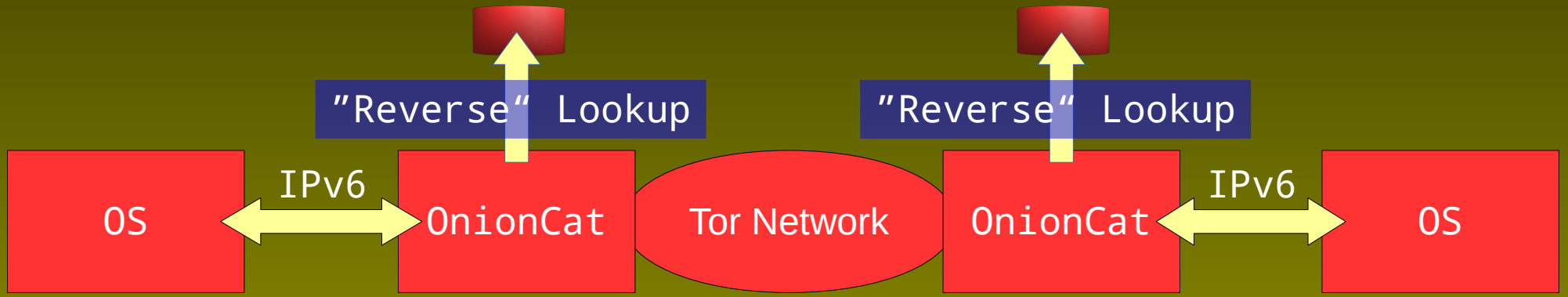
- crypto: SHA1 + RSA1024
- onion ids 80 bits

schqjb7xmas3siqd.onion

Hidden services V3

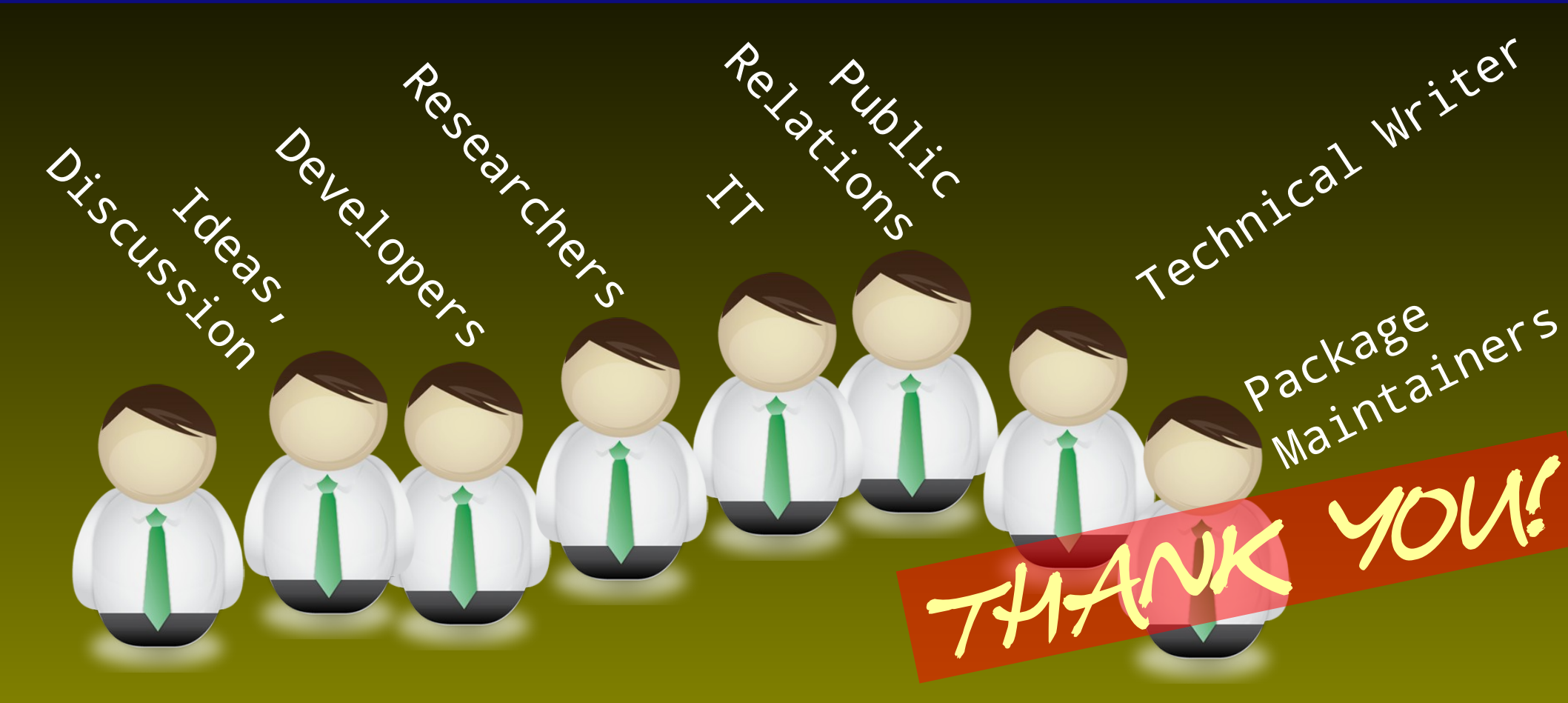
- implemented since Tor 0.3.2 (2017)
- new crypto: SHA3 + Curve25519
- onion ids 280 bits

qr4sshhsbcqfyircxqmi77j5pmgcki4keh5f6kybschqjb7xmas3siqd.onion



It's **not** just about writing code.

OnionCat->ProjectTeam();



OnionCat->ProjectTeam();

grep important <<topics

- Portable code
- Packages
- Documentation
- Revisioning, issues tracker
- Discussion board → be reachable!

Packaging.set_important(true);

If you want your software to be used,
you need **packages**!

tgz/txz, deb, rpm, BSD ports,…

```
use autotools or cmake;

BEGIN Packaging:

    do Portability()

    while !has_ported_to(”any”);
```

pthread_join(project, &NOW);

- Doing: package maintainance
  (who can do .msi?)
- Research: HSv3 lookup mechanism
- Development: Android, GUI,...
- Users, testers, writers, fans,...

return OnionCat->Internet;

https://www.onioncat.org/

https://github.com/rahra/onioncat

fd87:d87e:eb43:4506:3bbb:9faf:5877:4319
iuddxo47v5mhoqyz.onion

And feel free to donate! (₿ accepted ;)