Protecting Tor from Sybils

July 2, 2015

Philipp Winter, Roya Ensafi,
Karsten Loesing, Nick Feamster

Motivation

- Every other week, Sybil cluster comes online
  - Misconfiguration, botnets, attackers, researchers
  - Some attackers make effort to stay undetected

- Sybils have increased exposure to relayed traffic

- Sybils can manipulate onion service DHT
  - Take onion service offline
  - Gather statistics for onion service

Typical questions

- “Here’s a bad relay. Are there others just like it?”
- “Do these bad relays all belong together?”
- “Which related relay groups are currently online?”
- Passive and active analysis methods
  - Active: nmap, p0f3, ssh-keyscan, … (not very polite)

```
@type server-descriptor 1.0
router Karlstad1 193.11.166.194 9001 0 0
platform Tor 0.2.5.12 on Linux
protocols Link 1 2 Circuit 1
published 2015-06-29 06:58:30
fingerprint CCEF 02AA 454C 0AB0 FE1A C683 04F6 D8C4 220C 1912
uptime 6781675
bandwidth 5242880 5242880 2214019
extra-info-digest 5CDE5D433BABE03AA8E36FC7EA84F3CA97F92478
onion-key
-----BEGIN RSA PUBLIC KEY-----
MIGJAoGBALvtj4jzSZM0lUCa36sHxAplLY4Sd9EpOaLlt560m++olFiM7sPFM3i5
7fuZwQkXgbvDUEpFIk9araj5/LYax+BHssXWuJgPdVYl3DzFDw0oQh3dcXo2nROX
o5Rme1oztaaz1pIbQeJI1tEN3E+B6gr1+DaAq++zeqgOlP+dc48fAgMBAAE=
-----END RSA PUBLIC KEY-----
signing-key
-----BEGIN RSA PUBLIC KEY-----
MIGJAoGBAKzSFKy+UGxsZqfzcHcuFzFQtFho77Q5HukiyQJMpJIOq+MRPLbhgzpI
U0GnLjYrDBHsbvznt+VOmV1s35W9AvyNBh4kQxyifacBB6bUBFqvPxRR3WsFIvwg
fhCp2aa5qTdbH281UbrIXTD4eOtdvYvTGSSbJDTYZSMWmgDl6TDNAgMBAAE=
-----END RSA PUBLIC KEY-----
family $9B94CD0B7B8057EAF21BA7F023B7A1C8CA9CE645
hidden-service-dir
contact 4096R/D7FDC0D0 Philipp Winter <philwint@kau.se>
ntor-onion-key XdfQ8OmEyqj7ef9OcF9F7TuVaku/EGn/MbZfiJaPT3A=
reject *:*
router-signature
-----BEGIN SIGNATURE-----
iEn9DtKJ9qGHIFVSAtb8aeInpzFEY75nV8OgnYnrViSOcA8Z3CsYNZ3HwIbYp50k
hxHGkHN+TumEsUFRjk+UGr5Uro07EUvtAbMie+kkX2LdVCqeGules7Jq/jNilbVc
9pqHXUSKh6dIFZVqPxPOup0rw3nVkOUJ18GIkJmqh1U=
-----END SIGNATURE-----
```

```
@type server-descriptor 1.0
router Karlstad1 193.11.166.194 9001 0 0
platform Tor 0.2.5.12 on Linux
protocols Link 1 2 Circuit 1
published 2015-06-29 06:58:30
fingerprint CCEF 02AA 454C 0AB0 FE1A C683 04F6 D8C4 220C 1912
uptime 6781675
bandwidth 5242880 5242880 2214019
extra-info-digest 5CDE5D433BABE03AA8E36FC7EA84F3CA97F92478
onion-key
-----BEGIN RSA PUBLIC KEY-----
MIGJAoGBALvtj4jzSZM0lUCa36sHxAplLY4Sd9EpOaLlt560m++olFiM7sPFM3i5
7fuZwQkXgbvDUEpFIk9araj5/LYax+BHssXWuJgPdVYl3DzFDw0oQh3dcXo2nROX
o5Rme1oztaaz1pIbQeJI1tEN3E+B6gr1+DaAq++zeqgOlP+dc48fAgMBAAE=
-----END RSA PUBLIC KEY-----
signing-key
-----BEGIN RSA PUBLIC KEY-----
MIGJAoGBAKzSFKy+UGxsZqfzcHcuFzFQtFho77Q5HukiyQJMpJIOq+MRPLbhgzpI
U0GnLjYrDBHsbvznt+VOmV1s35W9AvyNBh4kQxyifacBB6bUBFqvPxRR3WsFIvwg
fhCp2aa5qTdbH281UbrIXTD4eOtdvYvTGSSbJDTYZSMWmgDl6TDNAgMBAAE=
-----END RSA PUBLIC KEY-----
family $9B94CD0B7B8057EAF21BA7F023B7A1C8CA9CE645
hidden-service-dir
contact 4096R/D7FDC0D0 Philipp Winter <philwint@kau.se>
ntor-onion-key XdfQ8OmEyqj7ef9OcF9F7TuVaku/EGn/MbZfiJaPT3A=
reject *:*
router-signature
-----BEGIN SIGNATURE-----
iEn9DtKJ9qGHIFVSAtb8aeInpzFEY75nV8OgnYnrViSOcA8Z3CsYNZ3HwIbYp50k
hxHGkHN+TumEsUFRjk+UGr5Uro07EUvtAbMie+kkX2LdVCqeGules7Jq/jNilbVc
9pqHXUSKh6dIFZVqPxPOup0rw3nVkOUJ18GIkJmqh1U=
-----END SIGNATURE-----
```

```
@type server-descriptor 1.0
router Karlstad1 193.11.166.194 9001 0 0
platform Tor 0.2.5.12 on Linux
protocols Link 1 2 Circuit 1
published 2015-06-29 06:58:30
fingerprint CCEF 02AA 454C 0AB0 FE1A C683 04F6 D8C4 220C 1912
uptime 6781675
bandwidth 5242880 5242880 2214019
extra-info-digest 5CDE5D433BABE03AA8E36FC7EA84F3CA97F92478
onion-key
-----BEGIN RSA PUBLIC KEY-----
MIGJAoGBALvtj4jzSZM0lUCa36sHxAplLY4Sd9EpOaLlt560m++olFiM7sPFM3i5
7fuZwQkXgbvDUEpFIk9araj5/LYax+BHssXWuJgPdVYl3DzFDw0oQh3dcXo2nROX
o5Rme1oztaaz1pIbQeJI1tEN3E+B6gr1+DaAq++zeqgOlP+dc48fAgMBAAE=
-----END RSA PUBLIC KEY-----
signing-key
-----BEGIN RSA PUBLIC KEY-----
MIGJAoGBAKzSFKy+UGxsZqfzcHcuFzFQtFho77Q5HukiyQJMpJIOq+MRPLbhgzpI
U0GnLjYrDBHsbvznt+VOmV1s35W9AvyNBh4kQxyifacBB6bUBFqvPxRR3WsFIvwg
fhCp2aa5qTdbH281UbrIXTD4eOtdvYvTGSSbJDTYZSMWmgDl6TDNAgMBAAE=
-----END RSA PUBLIC KEY-----
family $9B94CD0B7B8057EAF21BA7F023B7A1C8CA9CE645
hidden-service-dir
contact 4096R/D7FDC0D0 Philipp Winter <philwint@kau.se>
ntor-onion-key XdfQ8OmEyqj7ef9OcF9F7TuVaku/EGn/MbZfiJaPT3A=
reject *:*
router-signature
-----BEGIN SIGNATURE-----
iEn9DtKJ9qGHIFVSAtb8aeInpzFEY75nV8OgnYnrViSOcA8Z3CsYNZ3HwIbYp50k
hxHGkHN+TumEsUFRjk+UGr5Uro07EUvtAbMie+kkX2LdVCqeGules7Jq/jNilbVc
9pqHXUSKh6dIFZVqPxPOup0rw3nVkOUJ18GIkJmqh1U=
-----END SIGNATURE-----
```

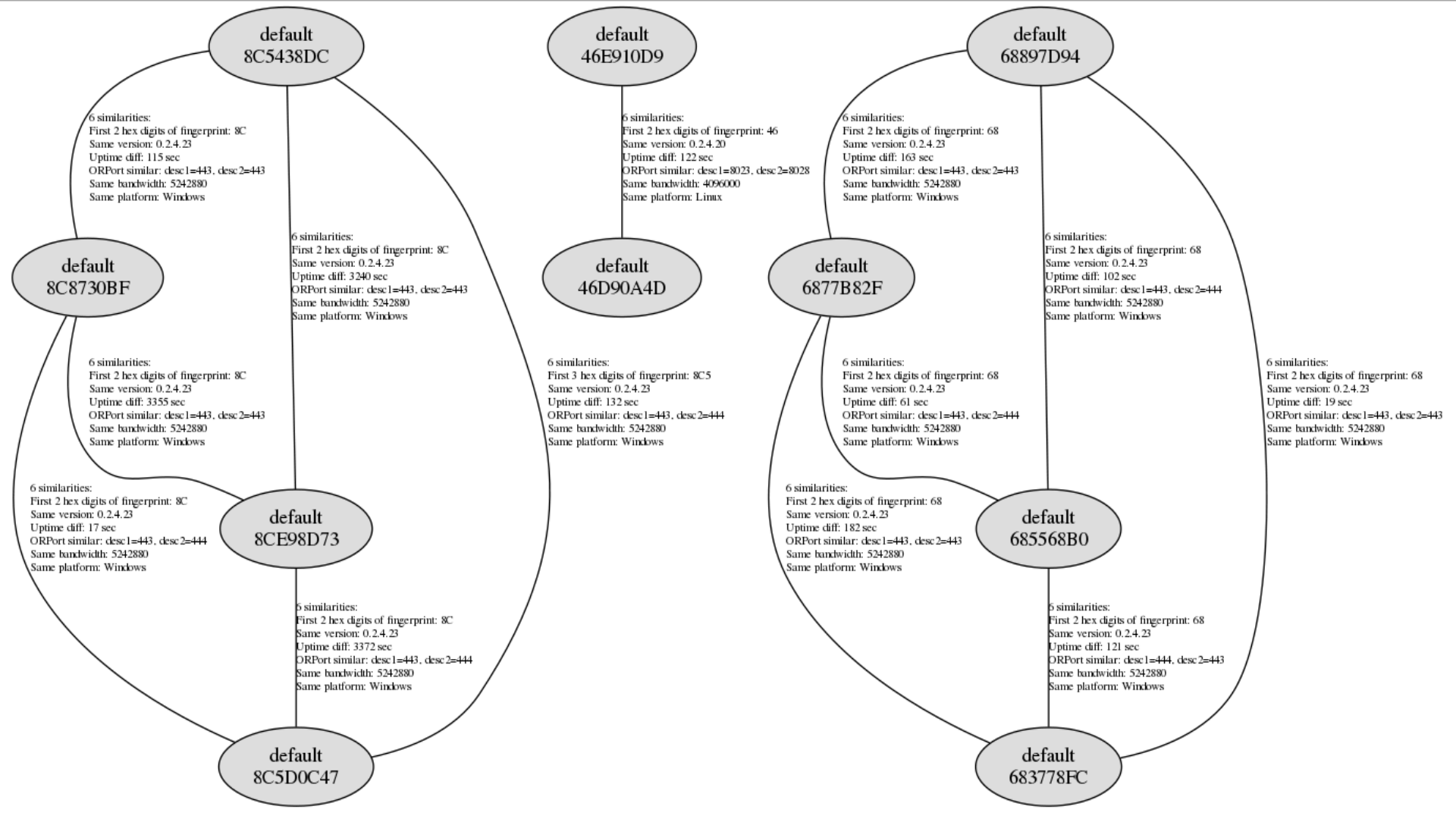
```
@type server-descriptor 1.0
router Karlstad1 193.11.166.194 9001 0 0
platform Tor 0.2.5.12 on Linux
protocols Link 1 2 Circuit 1
published 2015-06-29 06:58:30
fingerprint CCEF 02AA 454C 0AB0 FE1A C683 04F6 D8C4 220C 1912
uptime 6781675
bandwidth 5242880 5242880 2214019
extra-info-digest 5CDE5D433BABE03AA8E36FC7EA84F3CA97F92478
onion-key
-----BEGIN RSA PUBLIC KEY-----
MIGJAoGBALvtj4jzSZM0lUCa36sHxAplLY4Sd9EpOaLlt560m++olFiM7sPFM3i5
7fuZwQkXgbvDUEpFIk9araj5/LYax+BHssXWuJgPdVYl3DzFDw0oQh3dcXo2nROX
o5Rme1oztaaz1pIbQeJI1tEN3E+B6gr1+DaAq++zeqgOlP+dc48fAgMBAAE=
-----END RSA PUBLIC KEY-----
signing-key
-----BEGIN RSA PUBLIC KEY-----
MIGJAoGBAKzSFKy+UGxsZqfzcHcuFzFQtFho77Q5HukiyQJMpJIOq+MRPLbhgzpI
U0GnLjYrDBHsbvznt+VOmV1s35W9AvyNBh4kQxyifacBB6bUBFqvPxRR3WsFIvwg
fhCp2aa5qTdbH281UbrIXTD4eOtdvYvTGSSbJDTYZSMWmgDl6TDNAgMBAAE=
-----END RSA PUBLIC KEY-----
family $9B94CD0B7B8057EAF21BA7F023B7A1C8CA9CE645
hidden-service-dir
contact 4096R/D7FDC0D0 Philipp Winter <philwint@kau.se>
ntor-onion-key XdfQ8OmEyqj7ef9OcF9F7TuVaku/EGn/MbZfiJaPT3A=
reject *:*
router-signature
-----BEGIN SIGNATURE-----
iEn9DtKJ9qGHIFVSAtb8aeInpzFEY75nV8OgnYnrViSOcA8Z3CsYNZ3HwIbYp50k
hxHGkHN+TumEsUFRjk+UGr5Uro07EUvtAbMie+kkX2LdVCqeGules7Jq/jNilbVc
9pqHXUSKh6dIFZVqPxPOup0rw3nVkOUJ18GIkJmqh1U=
-----END SIGNATURE-----
```

```
@type server-descriptor 1.0
router Karlstad1 193.11.166.194 9001 0 0
platform Tor 0.2.5.12 on Linux
protocols Link 1 2 Circuit 1
published 2015-06-29 06:58:30
fingerprint CCEF 02AA 454C 0AB0 FE1A C683 04F6 D8C4 220C 1912
uptime 6781675
bandwidth 5242880 5242880 2214019
extra-info-digest 5CDE5D433BABE03AA8E36FC7EA84F3CA97F92478
onion-key
-----BEGIN RSA PUBLIC KEY-----
MIGJAoGBALvtj4jzSZM0lUCa36sHxAplLY4Sd9EpOaLlt560m++olFiM7sPFM3i5
7fuZwQkXgbvDUEpFIk9araj5/LYax+BHssXWuJgPdVYl3DzFDw0oQh3dcXo2nROX
o5Rme1oztaaz1pIbQeJI1tEN3E+B6gr1+DaAq++zeqgOlP+dc48fAgMBAAE=
-----END RSA PUBLIC KEY-----
signing-key
-----BEGIN RSA PUBLIC KEY-----
MIGJAoGBAKzSFKy+UGxsZqfzcHcuFzFQtFho77Q5HukiyQJMpJIOq+MRPLbhgzpI
U0GnLjYrDBHsbvznt+VOmV1s35W9AvyNBh4kQxyifacBB6bUBFqvPxRR3WsFIvwg
fhCp2aa5qTdbH281UbrIXTD4eOtdvYvTGSSbJDTYZSMWmgDl6TDNAgMBAAE=
-----END RSA PUBLIC KEY-----
family $9B94CD0B7B8057EAF21BA7F023B7A1C8CA9CE645
hidden-service-dir
contact 4096R/D7FDC0D0 Philipp Winter <philwint@kau.se>
ntor-onion-key XdfQ8OmEyqj7ef9OcF9F7TuVaku/EGn/MbZfiJaPT3A=
reject *:*
router-signature
-----BEGIN SIGNATURE-----
iEn9DtKJ9qGHIFVSAtb8aeInpzFEY75nV8OgnYnrViSOcA8Z3CsYNZ3HwIbYp50k
hxHGkHN+TumEsUFRjk+UGr5Uro07EUvtAbMie+kkX2LdVCqeGules7Jq/jNilbVc
9pqHXUSKh6dIFZVqPxPOup0rw3nVkOUJ18GIkJmqh1U=
-----END SIGNATURE-----
```

```
@type server-descriptor 1.0
router Karlstad1 193.11.166.194 9001 0 0
platform Tor 0.2.5.12 on Linux
protocols Link 1 2 Circuit 1
published 2015-06-29 06:58:30
fingerprint CCEF 02AA 454C 0AB0 FE1A C683 04F6 D8C4 220C 1912
uptime 6781675
bandwidth 5242880 5242880 2214019
extra-info-digest 5CDE5D433BABE03AA8E36FC7EA84F3CA97F92478
onion-key
-----BEGIN RSA PUBLIC KEY-----
MIGJAoGBALvtj4jzSZM0lUCa36sHxAplLY4Sd9EpOaLlt560m++olFiM7sPFM3i5
7fuZwQkXgbvDUEpFIk9araj5/LYax+BHssXWuJgPdVYl3DzFDw0oQh3dcXo2nROX
o5Rme1oztaaz1pIbQeJI1tEN3E+B6gr1+DaAq++zeqgOlP+dc48fAgMBAAE=
-----END RSA PUBLIC KEY-----
signing-key
-----BEGIN RSA PUBLIC KEY-----
MIGJAoGBAKzSFKy+UGxsZqfzcHcuFzFQtFho77Q5HukiyQJMpJIOq+MRPLbhgzpI
U0GnLjYrDBHsbvznt+VOmV1s35W9AvyNBh4kQxyifacBB6bUBFqvPxRR3WsFIvwg
fhCp2aa5qTdbH281UbrIXTD4eOtdvYvTGSSbJDTYZSMWmgDl6TDNAgMBAAE=
-----END RSA PUBLIC KEY-----
family $9B94CD0B7B8057EAF21BA7F023B7A1C8CA9CE645
hidden-service-dir
contact 4096R/D7FDC0D0 Philipp Winter <philwint@kau.se>
ntor-onion-key XdfQ8OmEyqj7ef9OcF9F7TuVaku/EGn/MbZfiJaPT3A=
reject *:*
router-signature
-----BEGIN SIGNATURE-----
iEn9DtKJ9qGHIFVSAtb8aeInpzFEY75nV8OgnYnrViSOcA8Z3CsYNZ3HwIbYp50k
hxHGkHN+TumEsUFRjk+UGr5Uro07EUvtAbMie+kkX2LdVCqeGules7Jq/jNilbVc
9pqHXUSKh6dIFZVqPxPOup0rw3nVkOUJ18GIkJmqh1U=
-----END SIGNATURE-----
```

```
@type server-descriptor 1.0
router Karlstad1 193.11.166.194 9001 0 0
platform Tor 0.2.5.12 on Linux
protocols Link 1 2 Circuit 1
published 2015-06-29 06:58:30
fingerprint CCEF 02AA 454C 0AB0 FE1A C683 04F6 D8C4 220C 1912
uptime 6781675
bandwidth 5242880 5242880 2214019
extra-info-digest 5CDE5D433BABE03AA8E36FC7EA84F3CA97F92478
onion-key
-----BEGIN RSA PUBLIC KEY-----
MIGJAoGBALvtj4jzSZM0lUCa36sHxAplLY4Sd9EpOaLlt560m++olFiM7sPFM3i5
7fuZwQkXgbvDUEpFIk9araj5/LYax+BHssXWuJgPdVYl3DzFDw0oQh3dcXo2nROX
o5Rme1oztaaz1pIbQeJI1tEN3E+B6gr1+DaAq++zeqgOlP+dc48fAgMBAAE=
-----END RSA PUBLIC KEY-----
signing-key
-----BEGIN RSA PUBLIC KEY-----
MIGJAoGBAKzSFKy+UGxsZqfzcHcuFzFQtFho77Q5HukiyQJMpJIOq+MRPLbhgzpI
U0GnLjYrDBHsbvznt+VOmV1s35W9AvyNBh4kQxyifacBB6bUBFqvPxRR3WsFIvwg
fhCp2aa5qTdbH281UbrIXTD4eOtdvYvTGSSbJDTYZSMWmgDl6TDNAgMBAAE=
-----END RSA PUBLIC KEY-----
family $9B94CD0B7B8057EAF21BA7F023B7A1C8CA9CE645
hidden-service-dir
contact 4096R/D7FDC0D0 Philipp Winter <philwint@kau.se>
ntor-onion-key XdfQ8OmEyqj7ef9OcF9F7TuVaku/EGn/MbZfiJaPT3A=
reject *:*
router-signature
-----BEGIN SIGNATURE-----
iEn9DtKJ9qGHIFVSAtb8aeInpzFEY75nV8OgnYnrViSOcA8Z3CsYNZ3HwIbYp50k
hxHGkHN+TumEsUFRjk+UGr5Uro07EUvtAbMie+kkX2LdVCqeGules7Jq/jNilbVc
9pqHXUSKh6dIFZVqPxPOup0rw3nVkOUJ18GIkJmqh1U=
-----END SIGNATURE-----
```

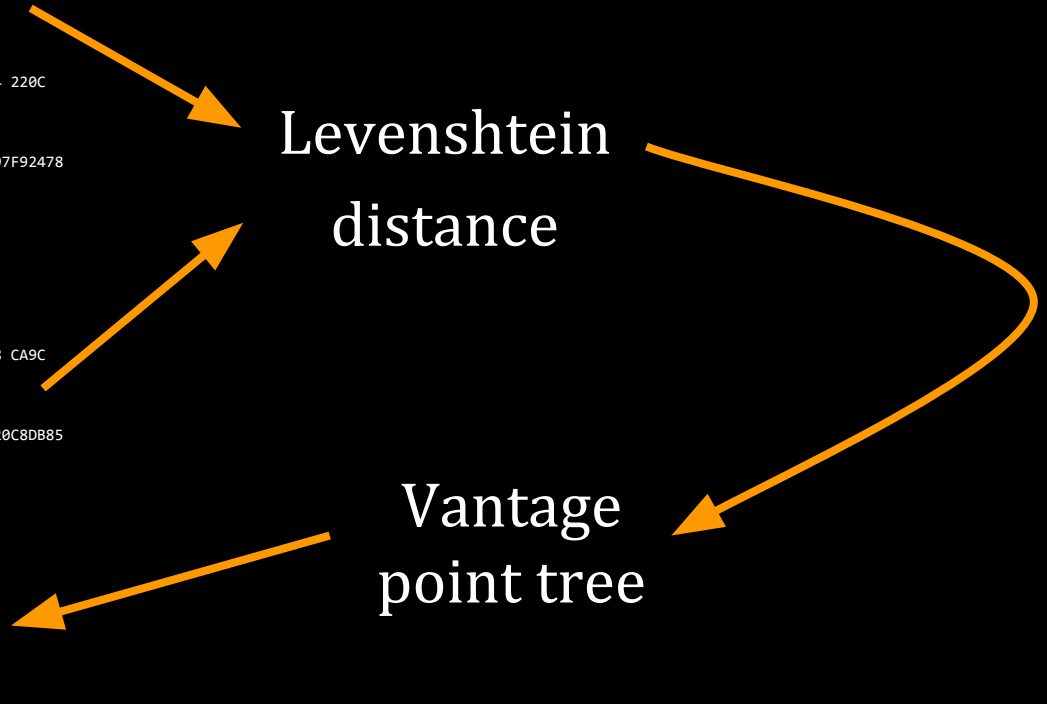
```
@type server-descriptor 1.0
router Karlstad1 193.11.166.194 9001 0 0
platform Tor 0.2.5.12 on Linux
protocols Link 1 2 Circuit 1
published 2015-06-29 06:58:30
fingerprint CCEF 02AA 454C 0AB0 FE1A C683 04F6 D8C4 220C 1912
uptime 6781675
bandwidth 5242880 5242880 2214019
extra-info-digest 5CDE5D433BABE03AA8E36FC7EA84F3CA97F92478
onion-key
-----BEGIN RSA PUBLIC KEY-----
MIGJAoGBALvtj4jzSZM0lUCa36sHxAplLY4Sd9EpOaLlt560m++olFiM7sPFM3i5
7fuZwQkXgbvDUEpFIk9araj5/LYax+BHssXWuJgPdVYl3DzFDw0oQh3dcXo2nROX
o5Rme1oztaaz1pIbQeJI1tEN3E+B6gr1+DaAq++zeqgOlP+dc48fAgMBAAE=
-----END RSA PUBLIC KEY-----
signing-key
-----BEGIN RSA PUBLIC KEY-----
MIGJAoGBAKzSFKy+UGxsZqfzcHcuFzFQtFho77Q5HukiyQJMpJIOq+MRPLbhgzpI
U0GnLjYrDBHsbvznt+VOmV1s35W9AvyNBh4kQxyifacBB6bUBFqvPxRR3WsFIvwg
fhCp2aa5qTdbH281UbrIXTD4eOtdvYvTGSSbJDTYZSMWmgDl6TDNAgMBAAE=
-----END RSA PUBLIC KEY-----
family $9B94CD0B7B8057EAF21BA7F023B7A1C8CA9CE645
hidden-service-dir
contact 4096R/D7FDC0D0 Philipp Winter <philwint@kau.se>
ntor-onion-key XdfQ8OmEyqj7ef9OcF9F7TuVaku/EGn/MbZfiJaPT3A=
reject *:*
router-signature
-----BEGIN SIGNATURE-----
iEn9DtKJ9qGHIFVSAtb8aeInpzFEY75nV8OgnYnrViSOcA8Z3CsYNZ3HwIbYp50k
hxHGkHN+TumEsUFRjk+UGr5Uro07EUvtAbMie+kkX2LdVCqeGules7Jq/jNilbVc
9pqHXUSKh6dIFZVqPxPOup0rw3nVkOUJ18GIkJmqh1U=
-----END SIGNATURE-----
```


default
8C5438DC
6 similarities:
First 2 hex digits of fingerprint: 8C
Same version: 0.2.4.23
Uptime diff: 115 sec
ORPort similar: desc1=443, desc2=443
Same bandwidth: 5242880
Same platform: Windows
default
8C8730BF
6 similarities:
First 2 hex digits of fingerprint: 8C
Same version: 0.2.4.23
Uptime diff: 3240 sec
ORPort similar: desc1=443, desc2=443
Same bandwidth: 5242880
Same platform: Windows
6 similarities:
First 2 hex digits of fingerprint: 8C
Same version: 0.2.4.23
Uptime diff: 3355 sec
ORPort similar: desc1=443, desc2=443
Same bandwidth: 5242880
Same platform: Windows
6 similarities:
First 2 hex digits of fingerprint: 8C
Same version: 0.2.4.23
Uptime diff: 17 sec
ORPort similar: desc1=443, desc2=444
Same bandwidth: 5242880
Same platform: Windows
default
8CE98D73
6 similarities:
First 2 hex digits of fingerprint: 8C
Same version: 0.2.4.23
Uptime diff: 3372 sec
ORPort similar: desc1=443, desc2=444
Same bandwidth: 5242880
Same platform: Windows
default
8C5D0C47
default
46E910D9
6 similarities:
First 2 hex digits of fingerprint: 46
Same version: 0.2.4.20
Uptime diff: 122 sec
ORPort similar: desc1=8023, desc2=8028
Same bandwidth: 4096000
Same platform: Linux
default
46D90A4D
6 similarities:
First 3 hex digits of fingerprint: 8C5
Same version: 0.2.4.23
Uptime diff: 132 sec
ORPort similar: desc1=443, desc2=444
Same bandwidth: 5242880
Same platform: Windows
default
68897D94
6 similarities:
First 2 hex digits of fingerprint: 68
Same version: 0.2.4.23
Uptime diff: 163 sec
ORPort similar: desc1=443, desc2=443
Same bandwidth: 5242880
Same platform: Windows
default
6877B82F
6 similarities:
First 2 hex digits of fingerprint: 68
Same version: 0.2.4.23
Uptime diff: 102 sec
ORPort similar: desc1=443, desc2=444
Same bandwidth: 5242880
Same platform: Windows
6 similarities:
First 2 hex digits of fingerprint: 68
Same version: 0.2.4.23
Uptime diff: 61 sec
ORPort similar: desc1=443, desc2=444
Same bandwidth: 5242880
Same platform: Windows
6 similarities:
First 2 hex digits of fingerprint: 68
Same version: 0.2.4.23
Uptime diff: 19 sec
ORPort similar: desc1=443, desc2=443
Same bandwidth: 5242880
Same platform: Windows
6 similarities:
First 2 hex digits of fingerprint: 68
Same version: 0.2.4.23
Uptime diff: 182 sec
ORPort similar: desc1=443, desc2=443
Same bandwidth: 5242880
Same platform: Windows
default
685568B0
6 similarities:
First 2 hex digits of fingerprint: 68
Same version: 0.2.4.23
Uptime diff: 121 sec
ORPort similar: desc1=444, desc2=443
Same bandwidth: 5242880
Same platform: Windows
default
683778FC

Nearest-neighbour search

```
@type server-descriptor 1.0
router Karlstad1 193.11.166.194 9001 0 0
platform Tor 0.2.5.12 on Linux
protocols Link 1 2 Circuit 1
published 2015-06-29 06:58:30
fingerprint CCEF 02AA 454C 0AB0 FE1A C683 04F6 D8C4 220C
1912
uptime 6781675
bandwidth 5242880 5242880 2214019
extra-info-digest 5CDE5D433BABE03AA8E36FC7EA84F3CA97F92478
onion-key
```

```
@type server-descriptor 1.0
router Karlstad0 193.11.166.194 9000 0 80
platform Tor 0.2.5.12 on Linux
protocols Link 1 2 Circuit 1
published 2015-06-29 13:03:35
fingerprint 9B94 CD0B 7B80 57EA F21B A7F0 23B7 A1C8 CA9C
E645
uptime 6803575
bandwidth 5242880 5242880 4100229
extra-info-digest C94BD16AFD3DFB98DB226EF5669855E220C8DB85
onion-key
```



```
$ sybilhunter -data 2015-06-28-00-00-00-consensus -neighbours 3 -referencerelay 9B94CD0B7B8057EAF21BA7F023B7A1C8CA9CE645



CCEF02AA:           Karlstad1 9001    02015-06-27 18:57:33 +0000 UTC0001100110100           0.2.5.12        27301-6553
9B94CD0B:           Karlstad0 9000   802015-06-27 07:01:26 +0000 UTC0001110110110           0.2.5.12        52801-6553
Dist(9B94CD0B, CCEF02AA) = 14



2FA8AD68:           garryhost 9001 90302015-06-27 13:51:28 +0000 UTC0001110110110           0.2.5.12        41801-6553
9B94CD0B:           Karlstad0 9000   802015-06-27 07:01:26 +0000 UTC0001110110110           0.2.5.12        52801-6553
Dist(9B94CD0B, 2FA8AD68) = 17



9FA42860:            brwyatt1 9001 90302015-06-27 07:05:02 +0000 UTC0001110110110           0.2.5.12        64001-6553
9B94CD0B:           Karlstad0 9000   802015-06-27 07:01:26 +0000 UTC0001110110110           0.2.5.12        52801-6553
Dist(9B94CD0B, 9FA42860) = 18
```

- Ideally, a relay's fingerprint never changes
- Regular changes could be attempt to manipulate DHT
- Monitor consensus and look for frequent changes

```
5.39.122.66 (20 unique fingerprints)
      FCB43143DBE4B80AF1D089DA0FE356D7184C5C7D (seen 1
times)
      B78DA4EB6003675506184F4279A2D213D109CE6C (seen 1
times)
      ADA11D7A6F7A996EEA95DED8B21BD14C8486B9A4 (seen 1
times)
      99A628177CA621F0A11535C77D5C66D19FF212AF (seen 1
times)
      D1375F8B0E53EA5543D89FEBB516122C07659B58 (seen 1
times)
      4898F12858724681404E523CB52452E01B9581A6 (seen 1
times)
      0B8E187E01BB7CD6218B8612125BE7A940E2532B (seen 1
times)
      9D4D7ABF2207E7E45961E0D93C9FEC17F455251E (seen 1
times)
      6642B3258BA0F45C4715D2DF28CB27769ACBEE0A (seen 1
times)
      C3A2A2B17F0770F65723B79821FDEC410B4B6B0C (seen 1
times)
      0EC4B788917E90DB14CB126FAC751EE0B7C42DC7 (seen 1
times)
      DF3F8C5A654E784D88B3E497371C66BD78B0511E (seen 1
times)
      665068101A5B64A87FABE025F57F4B91F115CF19 (seen 1
```

Defending against Sybils

- Existing work about social graphs and proof-of-work
- Current blocking process tedious and error-prone
- Increase cost of obtaining privileged status
  - Guard, exit, HSDir

Open questions and problems

- Better algorithms for similarity metric?
- Make better use of derived data, e.g., Onionoo
- Machine learning difficult because of adversarial setting

phw@nymity.ch

Experimental open science page:
https://nymity.ch/sybilhunting/