redhat.

https: Certificate Not Trusted

Stanislav Židek
szidek@redhat.com

Quality Engineering - BaseOS Security

Motivation

- Level? - beginner
- Why? - problems with https
- What? - understand what is happening
- How? - get your hands dirty in CLI!

Theory

- public key cryptography
  - "hey, everybody, this is my public key!"
  - vs. "let's meet in the docks to exchange private keys"
- certificate
  - "whose public key is that?"
  - attested by certification authority (CA)
- public key infrastructure
  - "should I trust this key?"

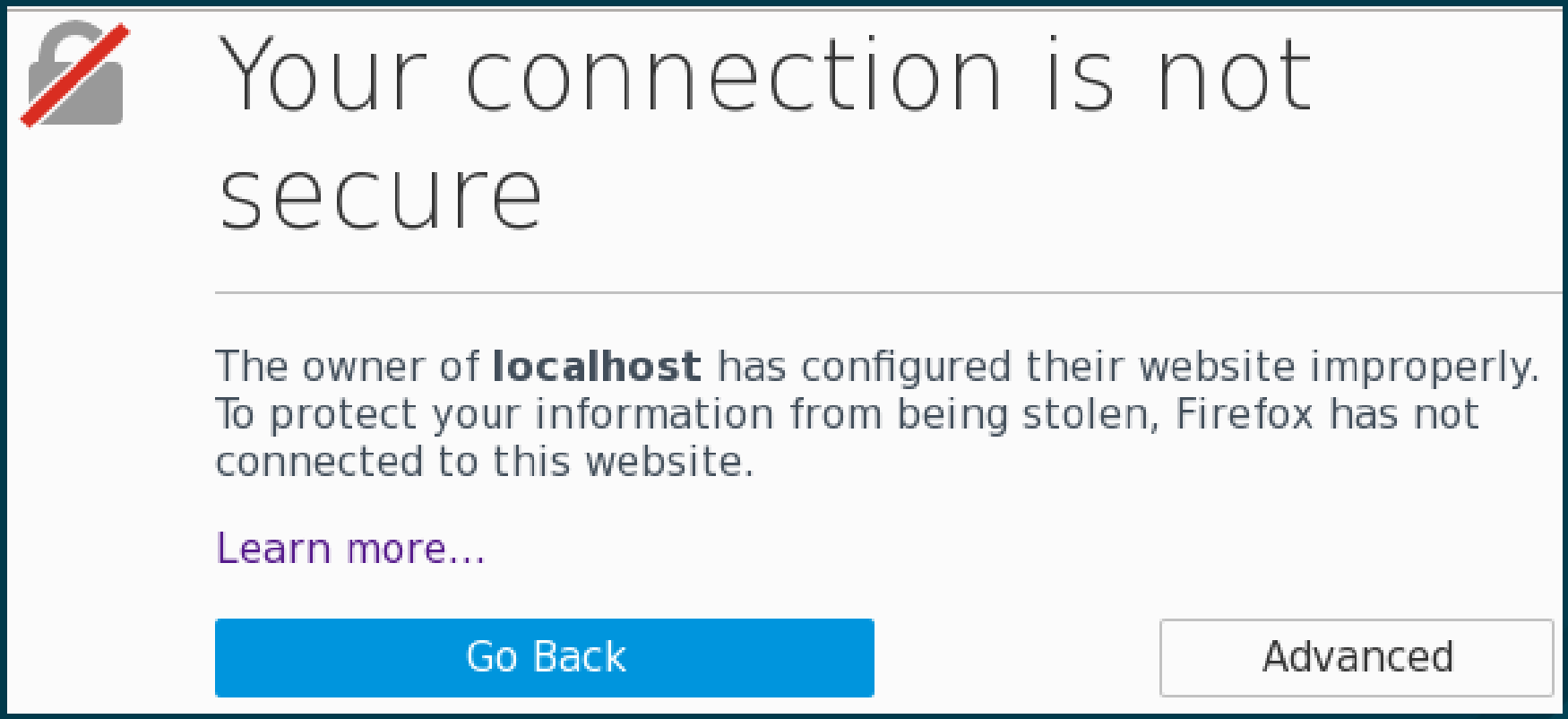
Theory - continued

- root CA
  - intermediate CA (0-N)
    - server certificate

Practice

- trusted certificate authorities preinstalled
  - system or browser
- situation is complicated
- let's get our hands dirty

Situation - Bad Domain



Situation - Bad Domain

Get Certificate

```
openssl s_client
    -connect <host>:<port>
    -showcerts
    -servername <name>
```

Get Certificate

```
CONNECTED(00000003)
...
Certificate chain
 0 s:/CN=badname
   i:/CN=DevConf2017CA
-----BEGIN CERTIFICATE-----
MIIDMzCCAhugAwIBAgIBBjANBgkq
b25mMjAxN0NBMCIYDzIwMTcwMTI4
KcW/3vlbfdH/DrYGzR0SqWEiDa/l
Cmj3+oSBUulpdHF3K2CVvPEadihm
hrH47JuVyQ==
-----END CERTIFICATE-----
...
```

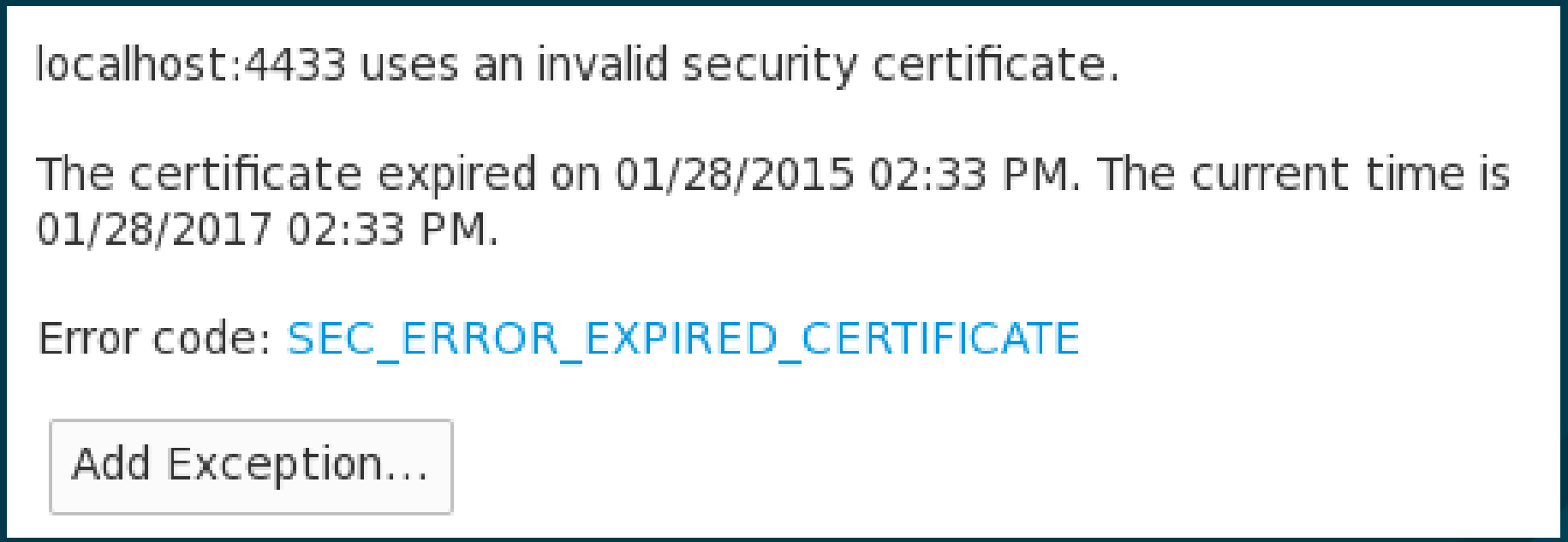
View Certificate

```
openssl x509
    -noout -text
    -in <filename> (or stdin)
```

View Certificate

```
Certificate:
  Data:
...
    Issuer: CN=DevConf2017CA
    Validity
      Not Before: Jan 28 12:29:18 2017 GMT
      Not After : Jan 28 12:29:18 2018 GMT
    Subject: CN=badname
...
```

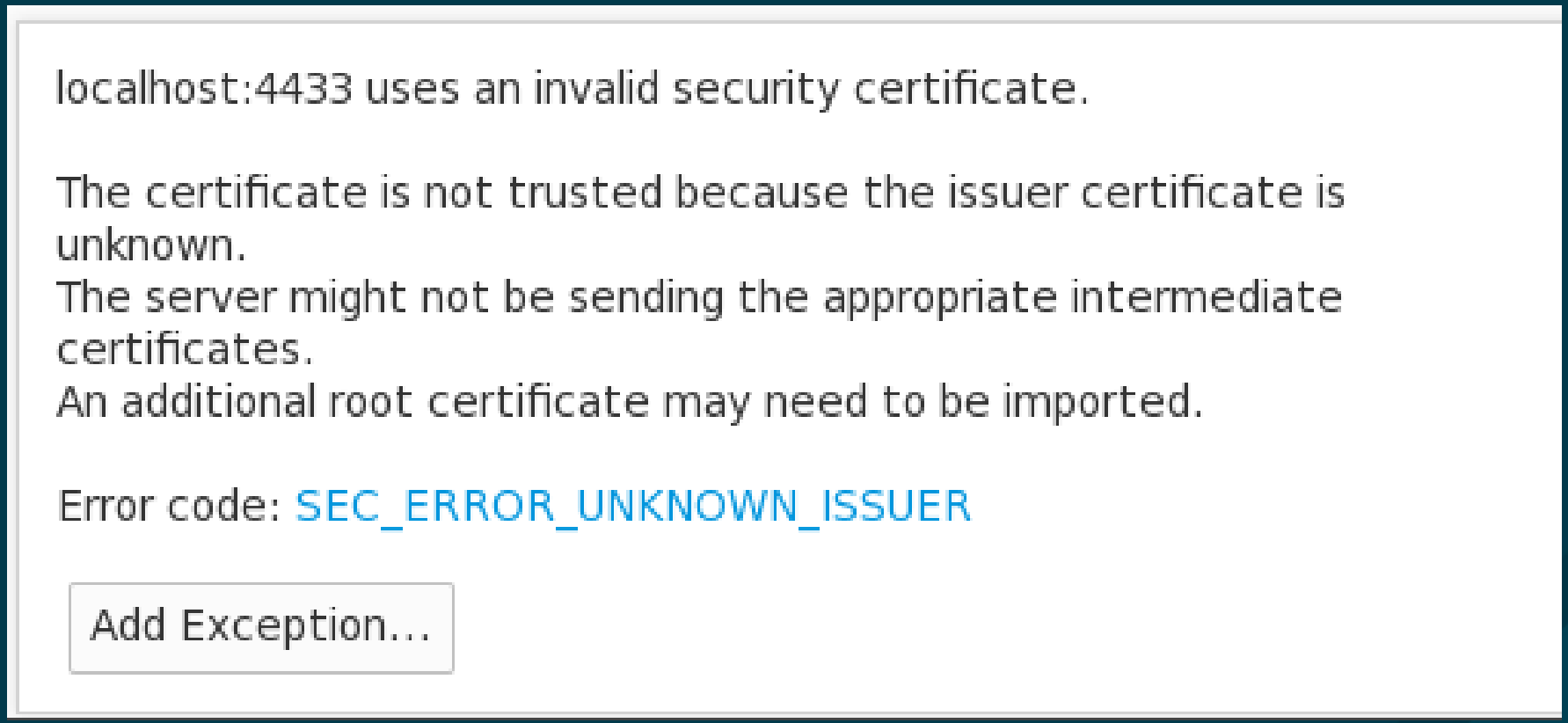
Situation - Expired



Get and View Certificate

```
Certificate:
  Data:
...
    Issuer: CN=DevConf2017CA
      Validity
        Not Before: Jan 28 13:33:26 2014 GMT
        Not After : Jan 28 13:33:26 2015 GMT
```

Situation - Unknown Issuer



Get Certificate

```
Certificate chain
 0 s:/CN=localhost
   i:/CN=localhost
-----BEGIN CERTIFICATE-----
MIIDJDCCAgygAwIBAgIBATANBgkqhki
bGhvc3QwIhgPMjAxNzAxMjAwOTI5MDd
3lAGP4leYcH3HEecJVNGTDMcVrtSOCp
4NMQM+eb1Cl6Vskeq2zf+eJug==
-----END CERTIFICATE-----
...
    Verify return code: 21 (unable to
verify the first certificate)
```

Get Certificate - alternative

```
Certificate chain
 0 s:/CN=localhost
   i:/CN=UnknownCA
-----BEGIN CERTIFICATE-----
-----END CERTIFICATE-----
 1 s:/CN=UnknownCA
   i:/CN=UnknownCA
-----BEGIN CERTIFICATE-----
-----END CERTIFICATE-----
    Verify return code: 19 (self
signed certificate in certificate
chain)
```

Verify Certificate

```
openssl verify
     -CAfile <rootca>
     <cert>

cert.pem: OK
```

Verify Certificate - alternative

```
cert.pem: CN = localhost
error 20 at 0 depth
lookup:
unable to get local
issuer certificate
```

Get Certificate - alternative

```
Certificate chain
 0 s:/CN=localhost
   i:/CN=IntermediateCA
-----BEGIN CERTIFICATE-----
-----END CERTIFICATE-----
 1 s:/CN=TrustedCA
   i:/CN=TrustedCA
-----BEGIN CERTIFICATE-----
-----END CERTIFICATE-----
```

Verify Certificate Chain

```
openssl verify
     -CAfile <rootca>
     -untrusted <inter>
     <cert>

cert.pem: OK
```

Conclusion

- we covered some typical problems
- reality is much more complicated
  - very complex system (X.509)
  - many other possible problems
    - extensions
    - certificate revocation
    - ...
- come talk to me if you are interested
  - possible project on certificate verification

redhat.

THANK YOU

plus.google.com/+RedHat

facebook.com/redhatinc

linkedin.com/company/red-hat

twitter.com/RedHatNews

youtube.com/user/RedHatVideos