

Browser SSL-Fingerprinting

- Use of HTTPS emerging
- SSL relies on set of different ciphersuites

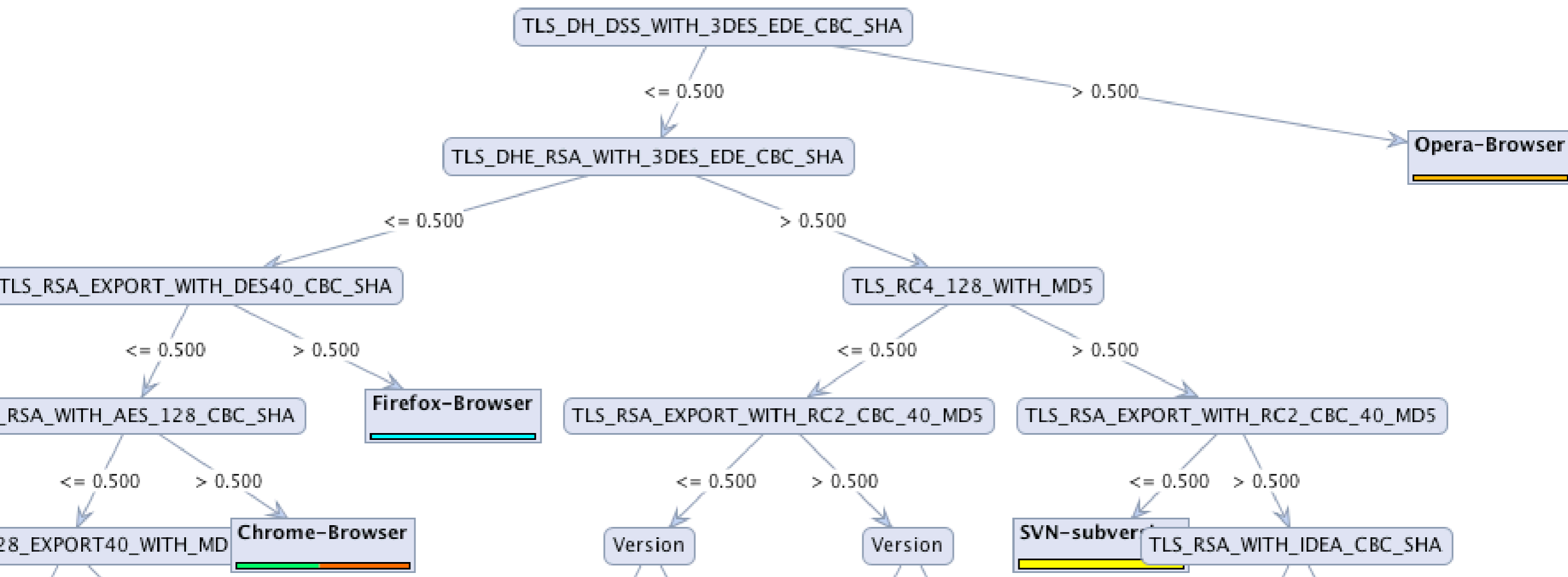
```
SSL_CK_RC4_128_WITH_MD5  
SSL_CK_RC4_128_EXPORT40_WITH_MD5  
SSL_CK_RC2_128_CBC_WITH_MD5  
SSL_CK_RC2_128_CBC_EXPORT40_WITH_MD5  
SSL_CK_IDEA_128_CBC_WITH_MD5  
SSL_CK_DES_64_CBC_WITH_MD5  
...
```

- Apache module to log ciphersuites used by web clients



Browser SSL-Fingerprinting

- Browser classification by Decision Tree



Browser SSL-Fingerprinting

- Classification to Browser „Types“, i.e. all Mozilla, msnbot/googlebot

accuracy: 86.63% +/- 0.82% (mikro: 86.63%)

	true Mozilla	true bot-Bo	true Apple-	true Firefox-	true Feedfel	true MSIE-B	true
pred. Mozill	1457	0	380	0	0	3	0
pred. bot-B	0	2704	0	0	171	315	0
pred. Apple	0	0	0	0	0	0	0
pred. Firefo	11	0	0	1381	0	37	0
pred. Feedf	0	0	0	0	0	0	0
pred. MSIE-	0	0	0	0	0	150	0
pred. slurn-	0	2	0	0	0	0	45

10-fold XVal on 7885 samples, ~54 binary attributes