Some observations of TLS in the web
## Perspectives

<table>
<thead>
<tr>
<th>Easy</th>
<th>Hard</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Browser</strong></td>
<td></td>
</tr>
<tr>
<td>% of transactions</td>
<td>% of sites</td>
</tr>
<tr>
<td><strong>Servers / hosting providers</strong></td>
<td></td>
</tr>
<tr>
<td>% of clients, transactions</td>
<td>% of sites</td>
</tr>
<tr>
<td><strong>Scanning</strong></td>
<td></td>
</tr>
<tr>
<td>% of sites*</td>
<td>% of transactions</td>
</tr>
</tbody>
</table>
How much TLS is there?

36%
How much TLS is there?

Time series for HTTP_TRANSACTION_IS_SSL, bin(s) 1 (in %)

From Sep 30, 2013 To May 3, 2015

Percentage

Volume

Nov '13 Jan '14 Mar '14 May '14 Jul '14 Sep '14 Nov '14 Jan '15 Mar '15 May '15

55%
How much RC4?

0.75%
Where did the RC4 go?

Time series for SSL_SYMOMETRIC_CIPHER_FULL, bin(s) 7 (in %)

Percentage

From Sep 1, 2014 To Jul 12, 2015

30%
How about key exchange?

- RSA: 20%
- ECDH: 75%
TLS 1.2 on the march!

Time series for SSL_HANDSHAKE_VERSION, bin(s) 3 (in %)

From Feb 7, 2014 To Jul 12, 2015
Summary

Need to bend the curve on TLS adoption

Ciphers and versions moving in the right direction

[[ All data sets shown in this preso are public. Ask me about how to use them! ]]