The Usability Challenge for DNS Privacy and End Users

Sara Dickinson (Sinodun)
Willem Toorop (NLnet Labs)
Allison Mankin (Salesforce)

NDSS: DNS Privacy Workshop San Diego (Feb 2017)

Background

- DPRIVE: Encrypted DNS standards/proposals now available for **stub to recursive**
    - DNS-over-TLS (RFC7858), Authentication profiles, padding, etc.
    - Several Stub implementations (e.g. Stubby)
    - Several experimental DNS-over-TLS servers
    - But deployment faces many challenges

This talk will focus on Usability challenges (USEC)

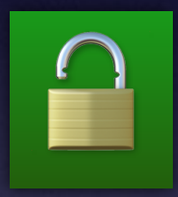
I'm not an expert!

Usable Security - Theory

- Usable systems (effective, efficient, accurate) - minimise unintentional errors
- Secure systems (motivation, attention, vigilance) - mitigate undesirable actions
- A conflict? For both - need to understand and be aware of
    - Mental models that complicate security or privacy
    - Creating an good user experience (effort vs benefit)
    - Lessons learned from designing, deploying, managing or evaluating security and privacy technologies

Usable Security - Practice

- Authentication - passwords, 2F auth,
- PKI - HTTP(S) green locks, cert warnings



  - GUI but much work done here to get it right
- Email Encryption - PGP
- Device pairing, etc.

And now DNS!

Where does DNS fit?

- Today - most ‘regular’ end users are unaware of DNS
  - ‘It should just work’ vs ‘It is a privacy issue’
- DNS is an ‘enabler’ service, not primary service (email, web).
- Basic Need: To improve awareness & education about DNS and the of lack of DNS Privacy (DNSSEC)

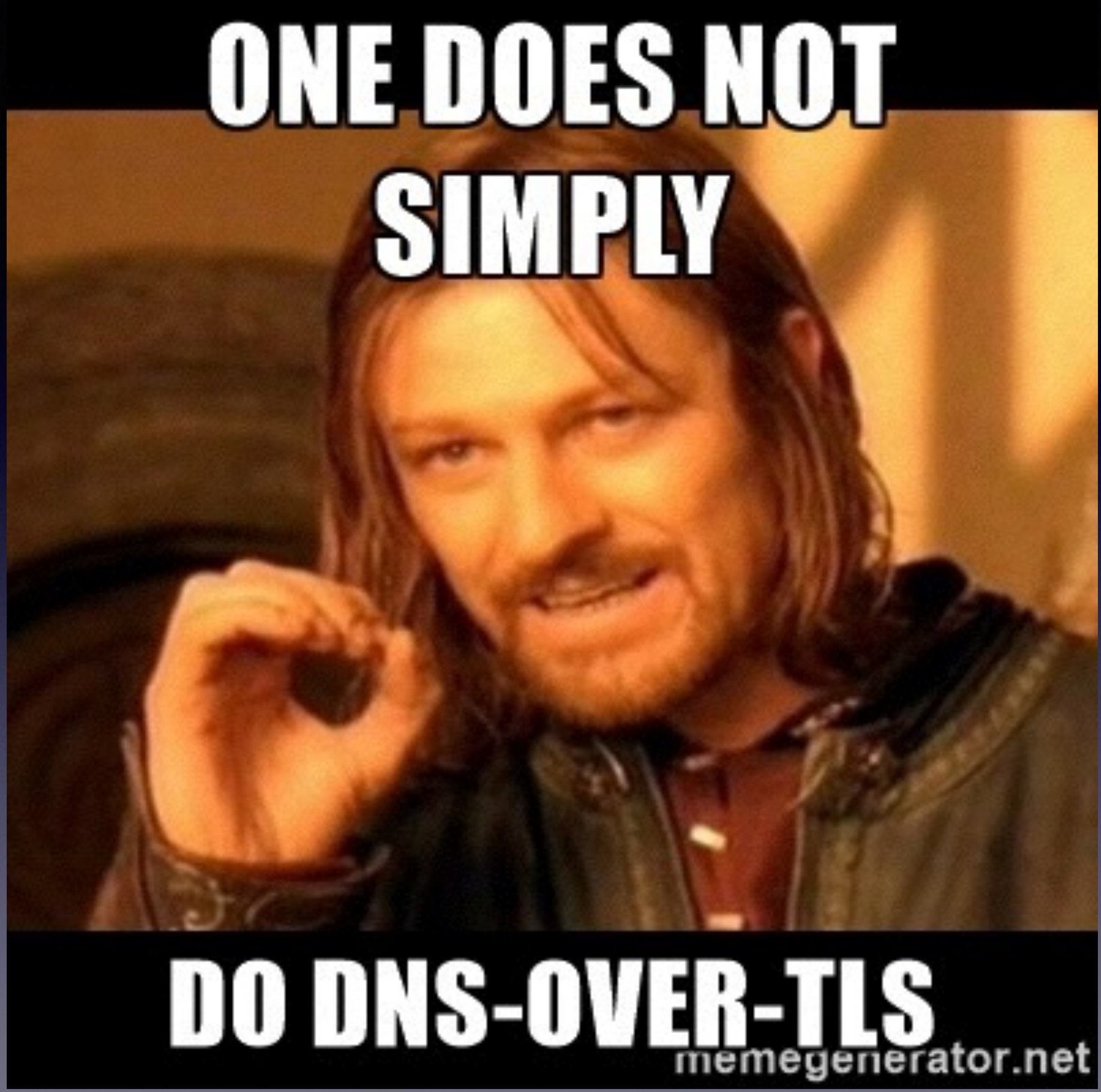
Deploying a Privacy Enabled Stub Resolver

- **Availability** - choice of software, easy to install packages, integration into OS (non-trivial)

- **Configuration** - user intervention? (choice of server, Strict or Opportunistic, authentication mechanism)

- **DNS-over-TLS Service** - performance, logging, errors (signalling - decoupled from a ‘goal’)

- **Usable security** - no model to force users to adopt it


ONE DOES NOT
SIMPLY
DO DNS-OVER-TLS
memegenerator.net

Prototype: Stubby

- A Privacy Enabling Stub resolver
- Uses DNS-over-TLS, based on getdns library
- Runs as daemon handling local requests
- Configure OS DNS resolution to point at 127.0.0.1
- Demos available: Sara, Allison, Willem

Stubby In Practice (today)

- **Availability**: 1.1.0 develop
  - How to build and use Stubby

"For technical users"

- **Configuration**: Reads config from /etc/stubby.conf
  - Strict and Opportunistic profiles + Authentication
- **DNS Service**: start from command line, crude logging to stdout, very coarse grained errors

Stubby in Practice

Config

Logging

"For technical users"

```
{ resolution_type: GETDNS_RESOLUTION_STUB
, dns_transport_list: [ GETDNS_TRANSPORT_TLS ]
, upstream_recursive_servers:
  [ { address_data: 145.100.185.16
    , tls_auth_name: "dnsovertls1.sinodun.com"
    , tls_pubkey_pinset:
      [ { digest: "sha256"
        , value: 0x659B41EB08DCC70EE9D624E6219C76EE31954DA1548B0C8519EAE5228CB24150
      } ]
   } ]
, tls_authentication: GETDNS_AUTHENTICATION_REQUIRED
, listen_addresses: [ 127.0.0.1, 0::1 ]
, idle_timeout: 10000
}
```

```
[01:14:33.667974] GETDNS_DAEMON:   145.100.185.15 : Conn init
[01:15:30.746646] GETDNS_DAEMON:   145.100.185.15 : Conn closed: Conn stats     - Resp=36,Timeouts=0,Auth=Success,Keepalive(ms)=10000
[01:15:30.746687] GETDNS_DAEMON:   145.100.185.15 :               Upstream stats - Resp=36,Timeouts=0,Best_auth=Success,Conns=1
[01:15:30.746698] GETDNS_DAEMON:   145.100.185.15 :               Upstream stats - Conn_fails=0,Conn_shutdowns=0,Backoffs=0
[01:15:36.567899] GETDNS_DAEMON:   145.100.185.15 : Conn init
[01:16:32.377446] GETDNS_DAEMON:   145.100.185.15 : Conn closed: Conn stats     - Resp=233,Timeouts=0,Auth=Success,Keepalive(ms)=10000
[01:16:32.377545] GETDNS_DAEMON:   145.100.185.15 :               Upstream stats - Resp=269,Timeouts=0,Best_auth=Success,Conns=2
[01:16:32.377578] GETDNS_DAEMON:   145.100.185.15 :               Upstream stats - Conn_fails=0,Conn_shutdowns=0,Backoffs=0
[01:16:41.664881] GETDNS_DAEMON:   145.100.185.15 : Conn init
[01:16:59.188199] GETDNS_DAEMON:   145.100.185.15 : Conn closed: Conn stats     - Resp=13,Timeouts=0,Auth=Success,Keepalive(ms)=10000
[01:16:59.188265] GETDNS_DAEMON:   145.100.185.15 :               Upstream stats - Resp=282,Timeouts=0,Best_auth=Success,Conns=3
[01:16:59.188284] GETDNS_DAEMON:   145.100.185.15 :               Upstream stats - Conn_fails=0,Conn_shutdowns=0,Backoffs=0
[01:17:07.794347] GETDNS_DAEMON:   145.100.185.15 : Conn init
[01:17:18.745280] GETDNS_DAEMON:   145.100.185.15 : Conn closed: Conn stats     - Resp=1,Timeouts=0,Auth=Success,Keepalive(ms)=10000
[01:17:18.745350] GETDNS_DAEMON:   145.100.185.15 :               Upstream stats - Resp=283,Timeouts=0,Best_auth=Success,Conns=4
[01:17:18.745372] GETDNS_DAEMON:   145.100.185.15 :               Upstream stats - Conn_fails=0,Conn_shutdowns=0,Backoffs=0
[01:17:45.707624] GETDNS_DAEMON:   145.100.185.15 : Conn init
[01:17:56.670120] GETDNS_DAEMON:   145.100.185.15 : Conn closed: Conn stats     - Resp=1,Timeouts=0,Auth=Success,Keepalive(ms)=10000
[01:17:56.670188] GETDNS_DAEMON:   145.100.185.15 :               Upstream stats - Resp=284,Timeouts=0,Best_auth=Success,Conns=5
[01:17:56.670211] GETDNS_DAEMON:   145.100.185.15 :               Upstream stats - Conn_fails=0,Conn_shutdowns=0,Backoffs=0
[01:18:05.323299] GETDNS_DAEMON:   145.100.185.15 : Conn init
[01:18:16.207892] GETDNS_DAEMON:   145.100.185.15 : Conn closed: Conn stats     - Resp=2,Timeouts=0,Auth=Success,Keepalive(ms)=10000
[01:18:16.207974] GETDNS_DAEMON:   145.100.185.15 :               Upstream stats - Resp=286,Timeouts=0,Best_auth=Success,Conns=6
[01:18:16.207997] GETDNS_DAEMON:   145.100.185.15 :               Upstream stats - Conn_fails=0,Conn_shutdowns=0,Backoffs=0
```

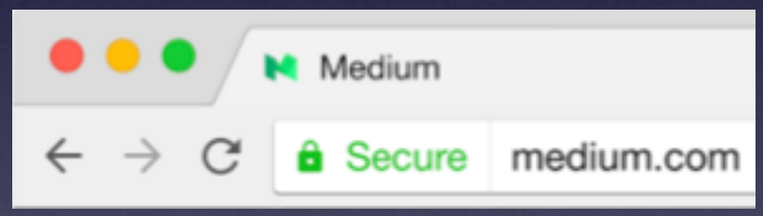
How to make Stubby Usable: Key questions

- Obviously need a set-up wizard, GUI, etc.
- Basic paradigm for signalling to users
  - green lock equivalent?

  - passive vs disruptive alerts
- Leverage *Opportunistic* mode to increase adoption without false sense of security

Lessons learned from…

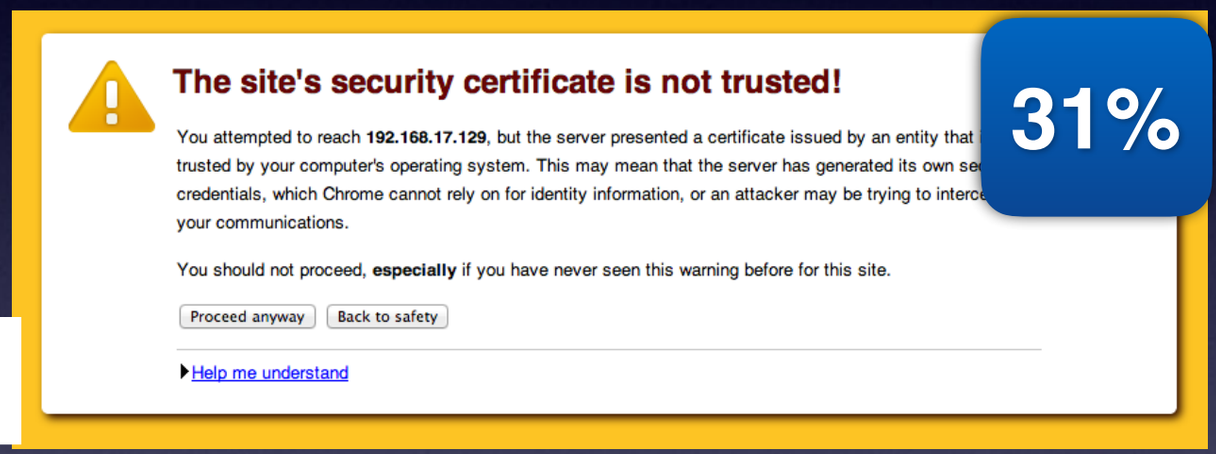
- HTTP(S):
  - Much research e.g. Adrienne Porter Felt
  - Consistency across implementations/platforms
- Security indicators



- Getting warnings right (subtle + non-obvious)
  - Adherence vs Comprehension
  - Get the language, logic and layout right

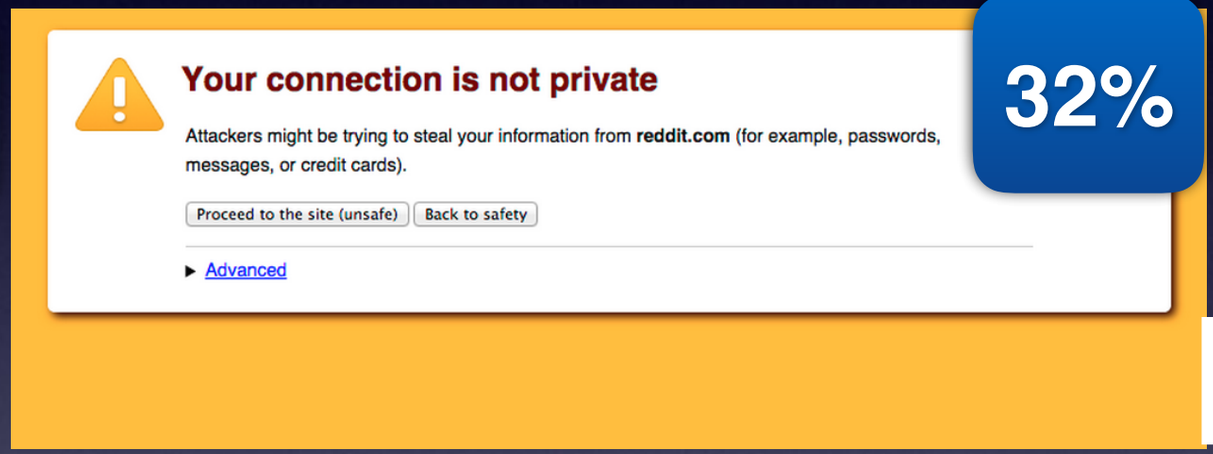
Lessons Learned
- Adherence to Certificate Warnings

Improving SSL Warnings: Comprehension and Adherence, Felt et al.



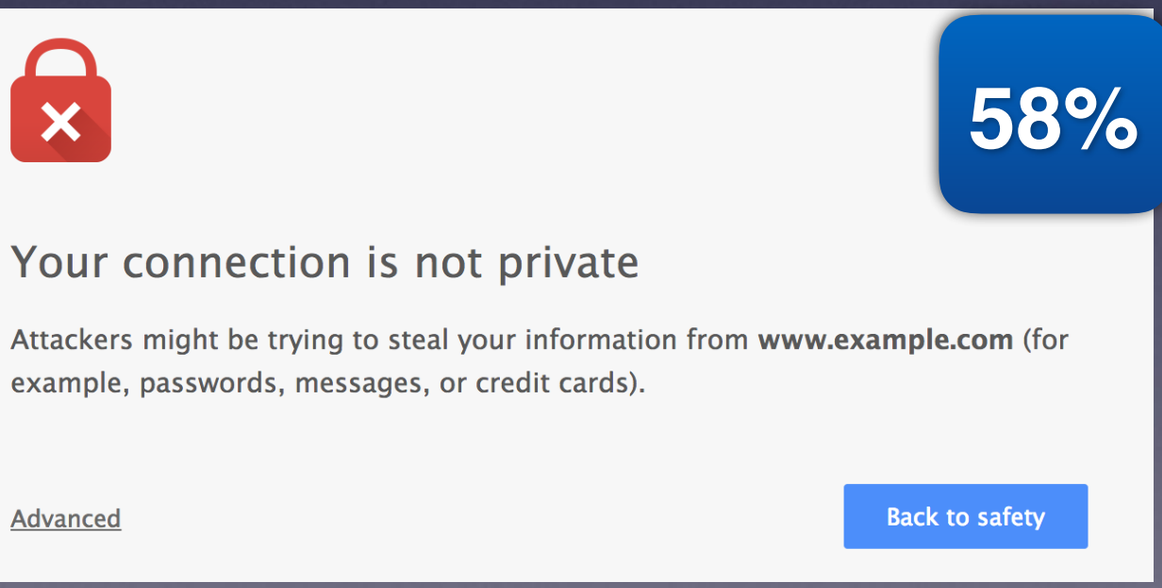
31%

1



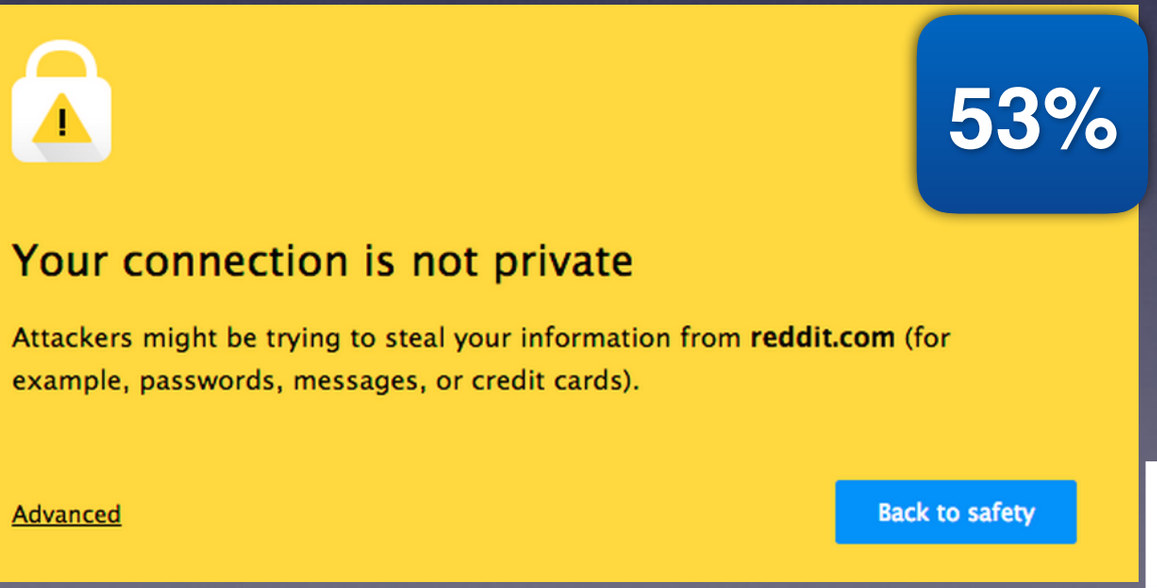
32%

2



58%

3



53%

4

Lessons learned from…

- PGP/HTTPS: Comprehension
    - Good GUIs aren’t enough - users still struggle with the basics if they don’t understand what they are doing
- DNSSEC:
    - DNS folks aren’t used to dealing with ‘users’ (or usability or GUIs)
    - DNS folks like things done the DNS way

Summary

- DNS Privacy is a new paradigm for end users
- End users are a new paradigm for DNS people!
- Ideas welcomed on making *Stubby* ‘Usable Security’
- DNS Privacy uptake critically dependant on this being successful