Encrypted SNI:
Threat Model Analysis

Don Davis & Rich Salz

TLS Working Group, IETF 90

July 20-25, 2014

Note Well

- Examples here are for evocative/illustrative purposes only.
- These are deliberate stereotypes.
- They do not represent the opinion of Akamai Technologies.

Overview

- Vulnerabilities for Encrypted SNI
  - Traffic Analysis
  - Cleartext DNS
  - Forced wiretaps at the server
- These hint at a messy threat model
  - Only some threat cases can be covered.
- Conclusion: This doesn’t cover main use-cases
  - NSA surveillance of US citizens
  - Tyrants’ surveillance of freedom-fighters
  - Are the other cases worth the costs?
  - Will we turn passive surveillance into active threats?

Vulnerabilities

- Vuln 1: Traffic Analysis
  - Not very hard
  - 1st world eavesdroppers do TA really well
- Vuln 2: Cleartext DNS
  - Eavesdropper must be near end-user.
  - But DNSCrypt exists
  - An Encrypted-DNS WG may be starting up.
  - But using Encrypt-DNS can be incriminating.
  - Likely run by ISP, often collaborator with gov’t
- Vuln 3: Gov’t pressures hosting service
  - Eavesdropper must be near server.
- Complicated threat model

Threat Model 1/6: Overview

- Who are the participants?
- Whom/what do we want to protect?
- Where is the eavesdropper?
- How technically savvy is the eavesdropper?
- How cruel / unfair is the eavesdropper?

Threat Model 2/6: Participants

- End-user: **client**, or **user**
  - Joe Sixpack, freedom fighters, Anonymous
- Hosting service: **freedom.com**
  - Mom-&-Pop Internet Café
  - Akamai.com
  - DNS Server
- Website: **unsafe.org**
- Attacker: **listen.gov**
  - NSA, Venezuela, Syria, N. Korea

Threat 3/6: Whom / What to Protect?

- Normal citizens’ privacy rights
  - N. America, EU, Japan
- Dissidents’ lives / freedom
  - Syria, N. Korea
  - Sensitive sites may be foreign
- Human rights
  - AIDS information where homosexuality illegal
- Whistleblowers
  - Anonymous / Assange, Snowden

Threat 4/6: Where is the Listener?

- Near the user
  - Main use-case for Encrypt-SNI
  - But eavesdropper can see DNS requests
  - So, the user needs Encrypt-DNS
- Near the server
  - NSA: buys off freedom.com
  - Syria: pressures / threatens freedom.com
  - No need for Encrypt-DNS
- Far from user & server
  - NSA: relies on great traffic analysis

Threat 5/6: Tech-Savvy Listeners

Who can do good traffic analysis?

- Very capable
  - First world countries: US, EU, Japan
  - Militarized states: PRC, N.Korea
- Some capability
  - Developing world: Brazil, Turkey, India
  - Surveillance states: Syria, Bahrain, Iran
- Not capable: other 3rd world

Threats 6/6: Cruel / Unfair Listeners

- Liberal democracies want accurate captures
  - False positives are bad
- Dictatorships want exhaustive captures
  - False negatives are bad
- Murderous regimes don’t care about FPs.
  - Even unfair prosecutions serve the state

Where Encrypt-SNI won’t help

- Encrypted SNI Fails:
  - if listener is near user (DNS): all gov’ts
  - if listener does traffic analysis well: many gov’ts
- Encrypted SNI is Useless:
  - if listener is near server (pressure): all gov’ts
  - if listener doesn’t care about fairness: N.Korea, etc

Where Encrypt-SNI will help

- If the Eavesdropper is:
  - Far from the user & server,
  - & bad at traffic analysis, (third world gov'ts)
  - & not cruel / unfair (liberal democracy)
- There aren't many of these:
  - Third-world liberal democracies that want to monitor expatriates' viewing of overseas websites.
  - But Encrypt-SNI *would* protect these expatriates!

Encrypt-DNS + Encrypt-SNI is better

- Helps even if eavesdropper is close to user.
- Helps citizens of 3rd-world liberal democracies.
- BUT:
- First-world gov’ts still can use traffic analysis
- Cruel gov’ts still don’t care about FPs.

- So, Encrypt-DNS+SNI helps only with middle-tier eavesdroppers:
  - Able to eavesdrop
  - Weak traffic Analysis
  - Not too cruel

Conclusion

- Basic problem: We're only trying to hide user's ass'n w/ unsafe.org, but gov'ts have ways to win:
  - Client-side listeners: DNS capture wins
  - Server-side listeners: Pressure on server wins
  - Tech-savvy listeners: Traffic Analysis wins
    - All first-world gov'ts
    - Militarized gov'ts
    - Surveillance states
- Most gov'ts can & will do one of these.