Informing Protocol Design Through Crowdsourcing: the Case of Pervasive Encryption

Anna Maria Mandalari  amandala@it.uc3m.es
Marcelo Bagnulo  marcelo@it.uc3m.es
Andra Lutu  andra@simula.no
Is the Internet Ossified?

Today, many aspects appear to be “set in stone”

Criticism: Middleboxes behavior

How will Internet react to a new protocol?

The case of pervasive encryption

Understand the feasibility of pervasive encryption in the Internet.

Understand the interaction of middleboxes with the TLS across the different TCP ports that currently use plain text protocols.
How to measure a thousand end-users?

• Be Google (or any other large Internet players)

or

• Get your code to run on a thousand users’ machines through another delivery channel
Crowdsourcing platform

microWorkers
work & earn or offer a micro job

Existing user Login New user? Register for free

Employers, ask people to...
— Blog about your product
— Post reviews to Websites & Blogs

Workers, sign up and...
— Browse micro jobs
— Select jobs you like

Perform large-scale Internet measurement campaigns
Experimental setup: Measurement Agent Common Procedure

- In the background, HTTP and HTTPS connections are performed from the measurement devices to our servers in all the 68 ports.
Aggregated results

\[
\text{ERROR} = (\text{success [HTTP]} - \text{success [TLS]})
\]

25\% of the users are not able to perform a TLS connection over port 80 in mobile network.
70% of the users that use a proxy are not able to perform a TLS connection over port 80 in mobile network.

\[ \text{ERROR} = (\text{success [HTTP]} - \text{success [TLS]}) \]
Conclusion

• Overcome several of the limitations of the crowdsourcing platforms;

• It is probably feasible to roll out TLS protection for most ports except for port 80, assuming a low failure rate (6%);

• Our results can serve as a lower bound for the failure rate for using protocols other than expected in different ports.