User Attitudes Toward the Inspection of Encrypted Traffic

Scott Ruoti, Mark O'Neill, Daniel Zappala, Kent Seamons
Brigham Young University

Introduction

- TLS Proxies
- SSL Inspection
- Used by organizations to protect their networks
- Used by governments to spy on citizens

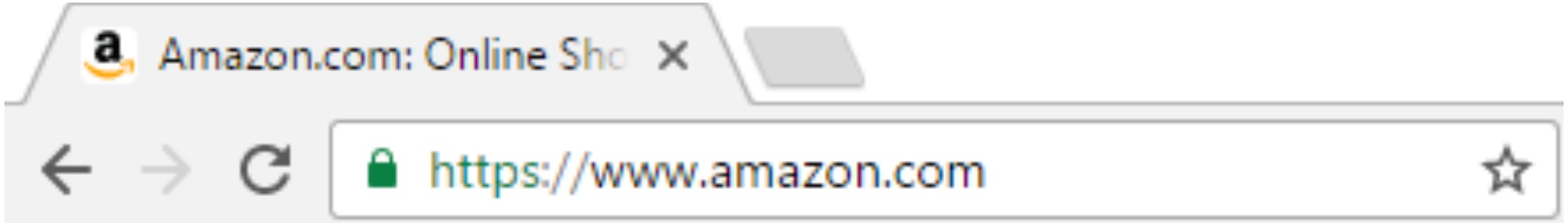
Attitudes on Inspection of Encrypted Traffic

- Security experts are actively trying to stop TLS proxies
  - Certificate transparency
  - DANE
- Business and governments want them
- What do end-users think?
  - Might decide which side wins this argument
  - Should guide research
  - Unexplored

TLS Proxies

Basic Questions

- Is the website who it says it is?
- Is the connection to the website secure?

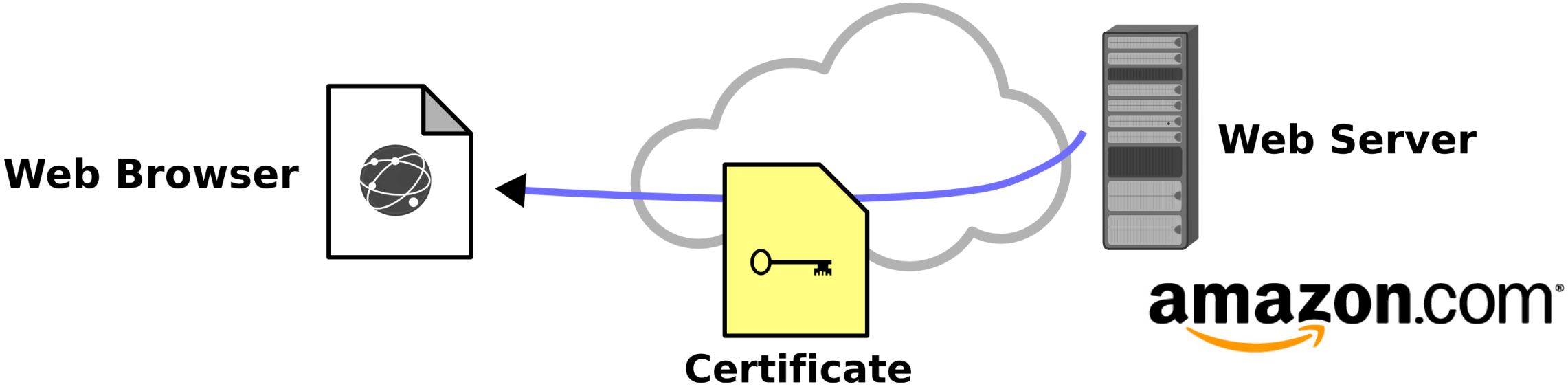


- The **lock icon** is supposed to indicate a secure connection

TLS Authentication

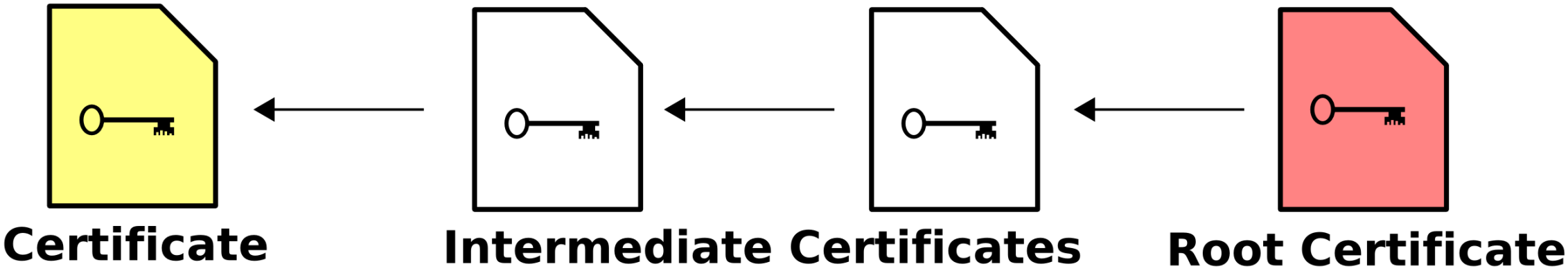
› Websites identify themselves using a X.509 certificate

› Browser validates this certificate to authenticate website



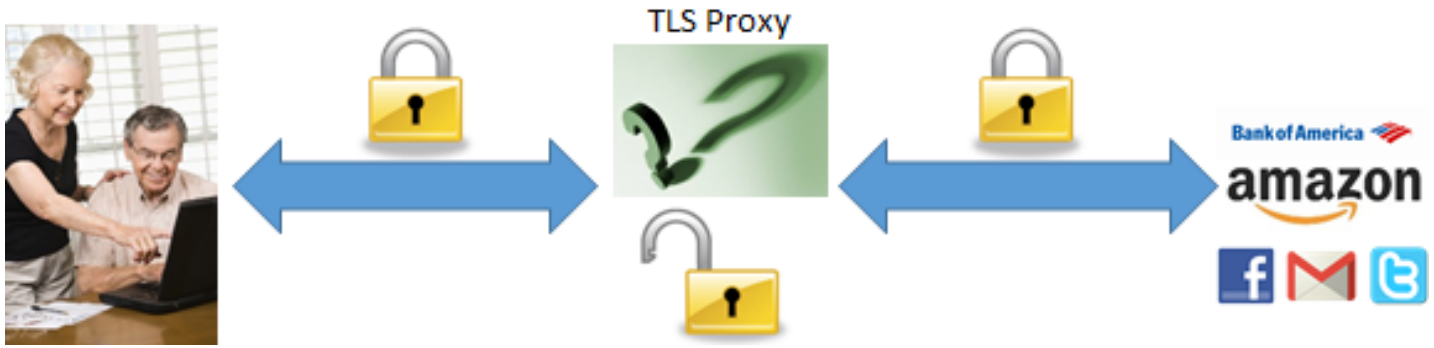
Certificate Verification

- X.509 certificates are signed by other X.509 certificates
- Browser checks that this chain ends at a trusted root certificate



TLS Proxy

- Man-in-the-middle TLS communication
- Generate substitute certificates
  - Signed properly by the CA system
  - Signed by a locally installed trusted root
- No visual indication that the connection isn't secure



Uses

MALICIOUS

- Stealing passwords
- Identity theft
- Tracking government dissidents
- Spying (for example the NSA)
- Censorship

PROTECTIVE

- Blocking malware and viruses
- Protecting company secrets
- Blocking harmful websites
- Catching malicious individuals

Teaching Users About TLS Proxies

Dilemma

- Goal: gather ordinary people's opinions
- If we only survey those with pre-existing knowledge…
  - Mostly security experts
  - Not our target demographic
- If we teach individuals about TLS proxies
  - Can survey are target demographic
  - Might influence participant responses
- Teaching about TLS proxies is not ideal, but is necessary

Creating the Description

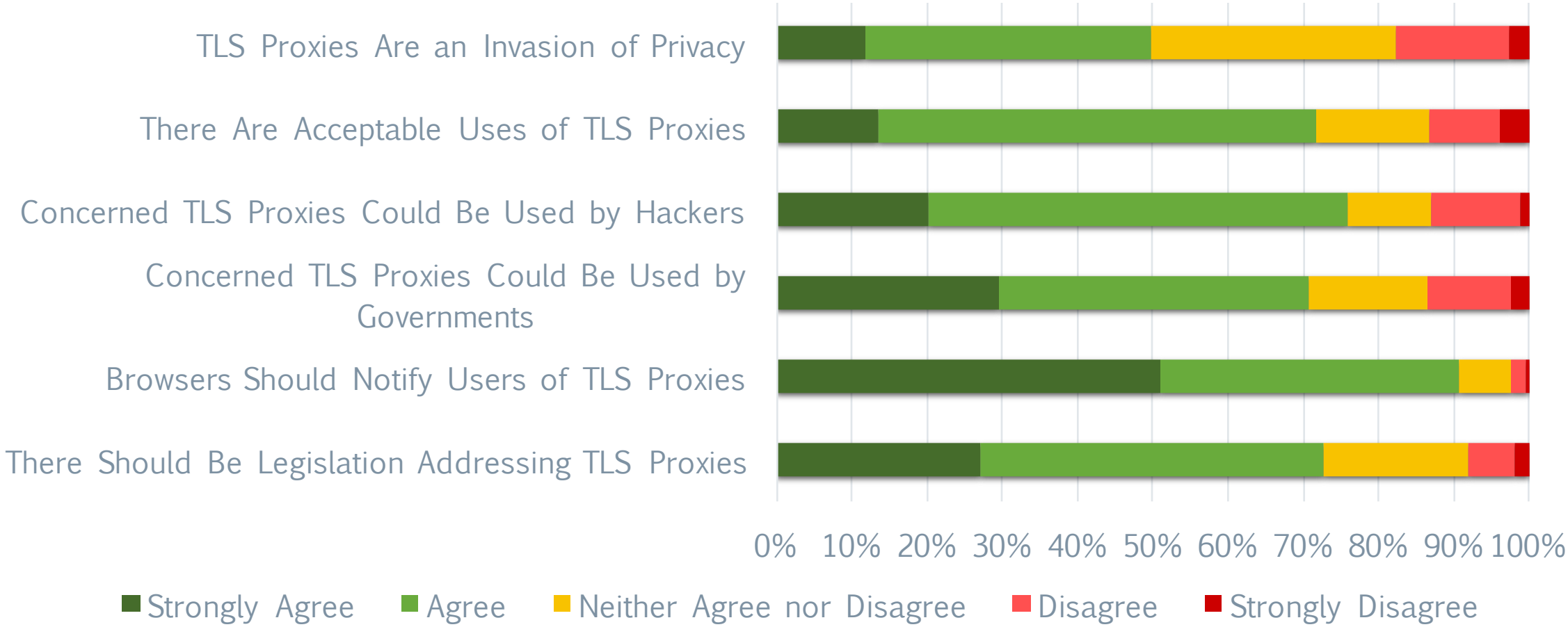
- Strived for neutrality
- Surveyed existing descriptions
  - Security experts
  - Businesses
- Established consensus
- Pilot studies
  - Convenience sample (6 participants)
  - MTurk (80 participants)

First Survey

Methodology

- Amazon Mechanical Turk (MTurk)
  - 1,049 responses
  - Skewed male (61%) and 25 – 34 years old (41%)
  - Participants mostly from the USA (87%) and India (12%)
- Instructed users regarding TLS proxies
- Asked participants about their opinions
  - Likert scale questions
  - Free response questions

Attitudes Regarding TLS Proxies



Acceptable Uses

- Protect organizations (51%)
  - It is the company's hardware
  - Companies need to inspect internal traffic to prevent attacks
- Protect individuals (35%)
  - E.g., anti-virus
- Censor content (7%)
  - Some indicated it was never acceptable to censor content (3%)

Concerns

- Hackers (76%)
- Government spying (71%)
- Privacy (55%)
  - Identity theft (10%)
- Performed without notification or consent (13%)

Reactions

PERCEPTION

- Negative (61%)
- Positive (5%)
- Depends (34%)

BEHAVIOR

- Suspicious (26%)
- Discontinue use (17%)
- Change behavior (6%)

Personas

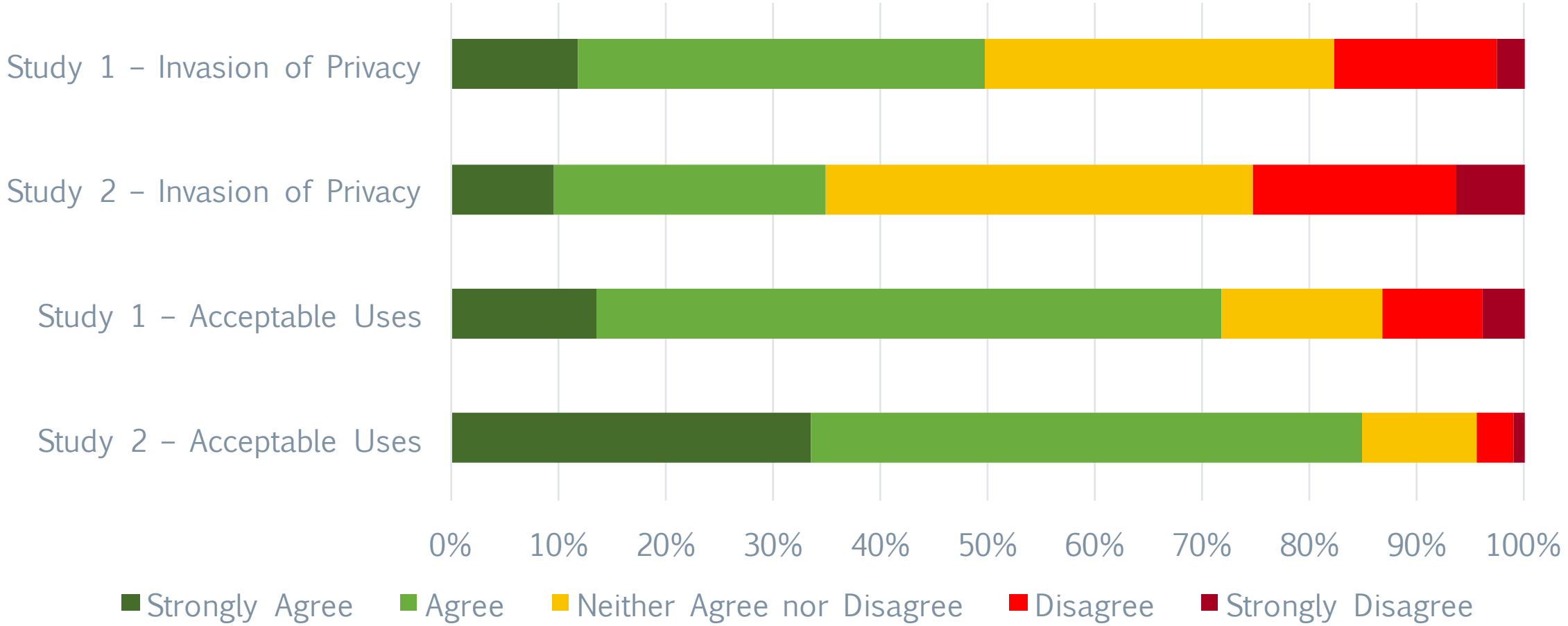
- Pragmatic majority (76%)
- Privacy fundamentalist (17%)
- Unconcerned (1%)
- **Jaded** (5%)
  - Cares about security
  - Feels there is no hope

Second Survey

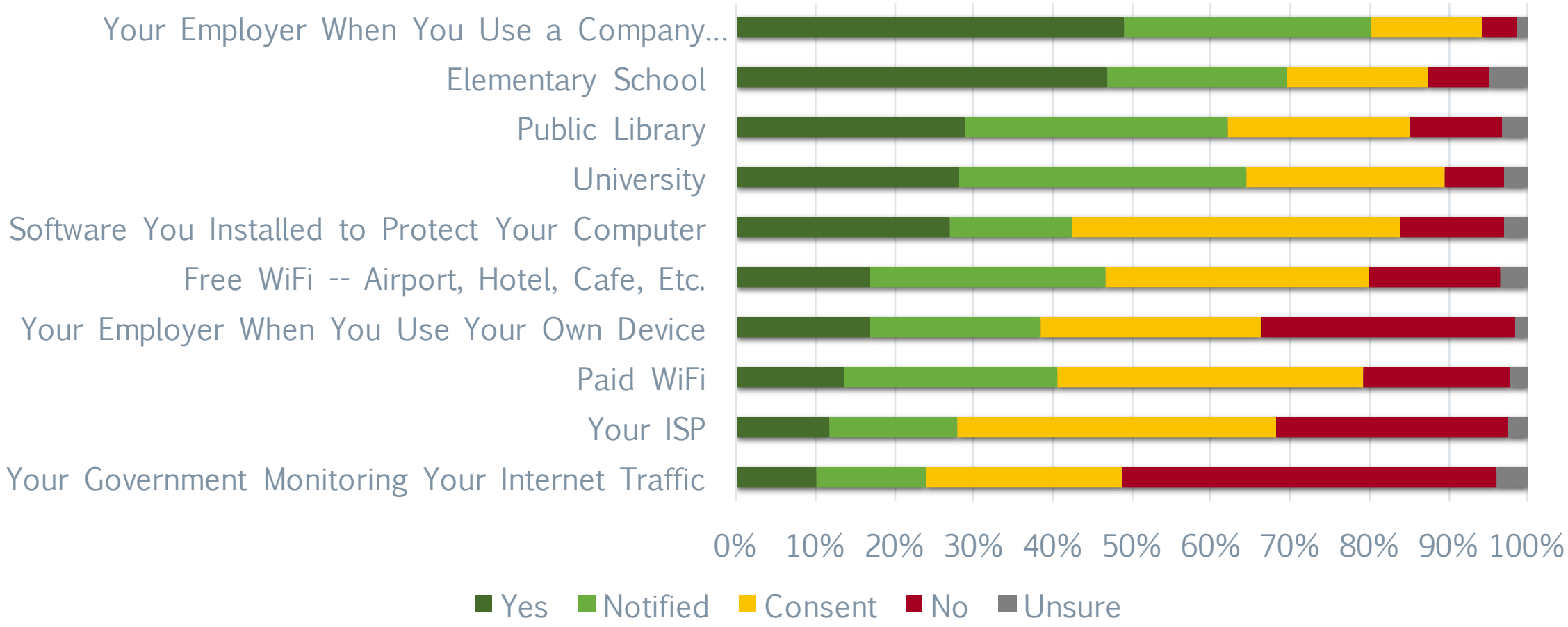
Methodology

- Amazon Mechanical Turk (MTurk)
  - 927 responses
  - Participants mostly from the USA (94%) and India (5%)
- Instructed users regarding TLS proxies
- Asked participants about specific use cases for TLS proxies

Attitudes Regarding TLS Proxies



Acceptable Uses



Participant Responses

Informed Participants

- High level of engagement
- Good understanding of problem
- Recognize tradeoffs

"This is one of those doubled-edged swords – it can be used for your good and security and it can be used to harm and spy on you.
Because of the distinct possibility of lost privacy, this type of proxy should [not be] used, except by your agreement, not by anyone else."

Notification and Risk

› Nearly all participants want notification

"Well for some things it would be understandable, I'd just like to be informed so I know the risk I'm taking."

› Most participants want consent to be required

"If I encrypt something no one has the right to unencrypt it unless I give them the right to - simple as that."

Conclusion

Conclusion

- Gathered user attitudes towards TLS proxies
- Participants had nuanced views of trade-offs
  - TLS proxies are an invasion of privacy
  - See acceptable uses
- Users want notification and consent
- We need to engage end-users more often