A client-side analysis of TLS usage in mobile apps

Abbas Razaghpanah ‡, Narseo Vallina-Rodriguez †, Phillipa Gill ‡
†ICSI, ‡ Stony Brook University

How securely do mobile apps use TLS?

We need to study the state of TLS to

- Assess security of TLS usage by apps and servers
- Study TLS failures and app resilience to TLS attacks

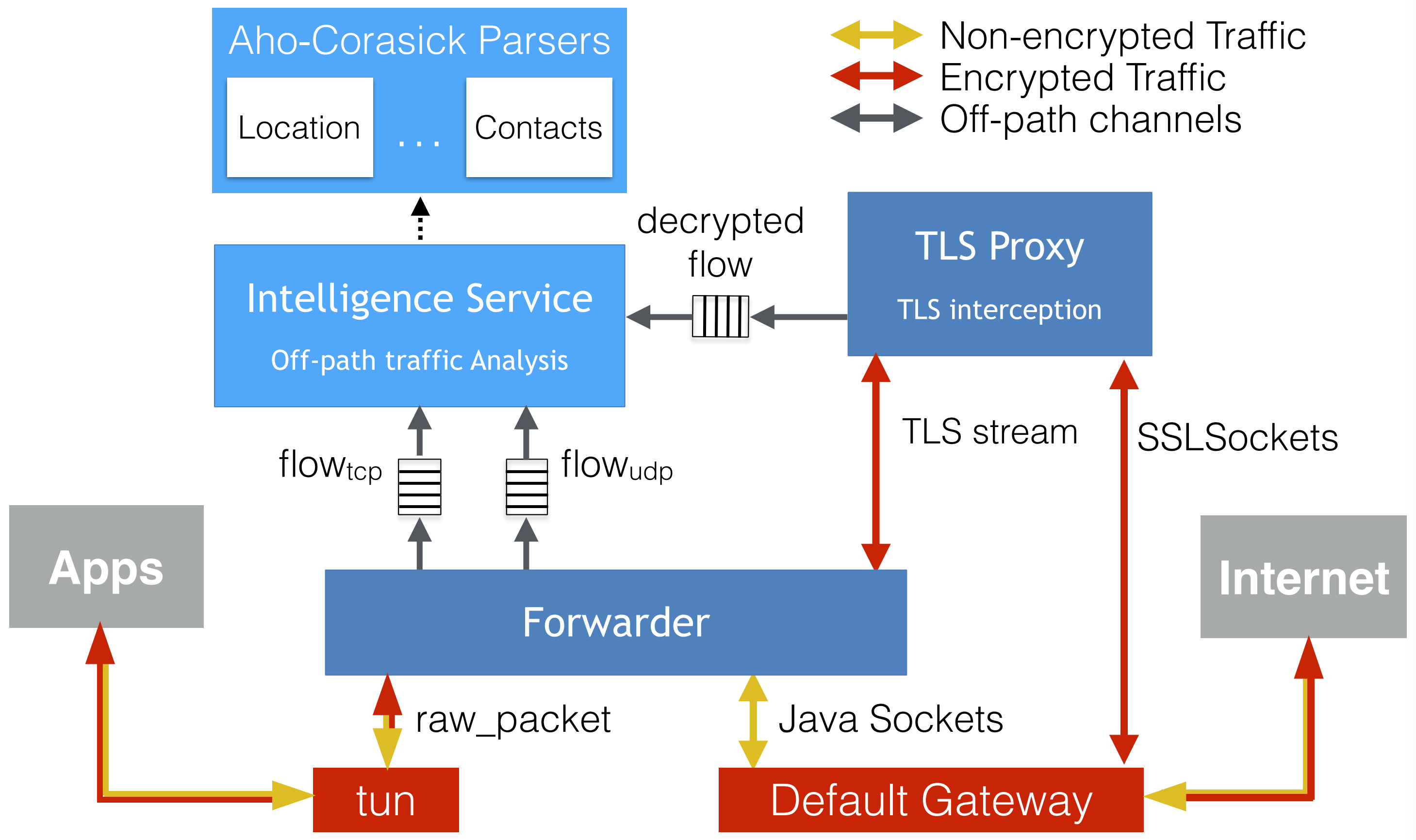
State of the art

- There hasn't been a study of mobile app TLS usage at scale

Haystack

A **handset-**, **traffic-**, and **user-centric** platform that provides high-fidelity insight about security, privacy, and performance aspects of mobile apps **in the wild**

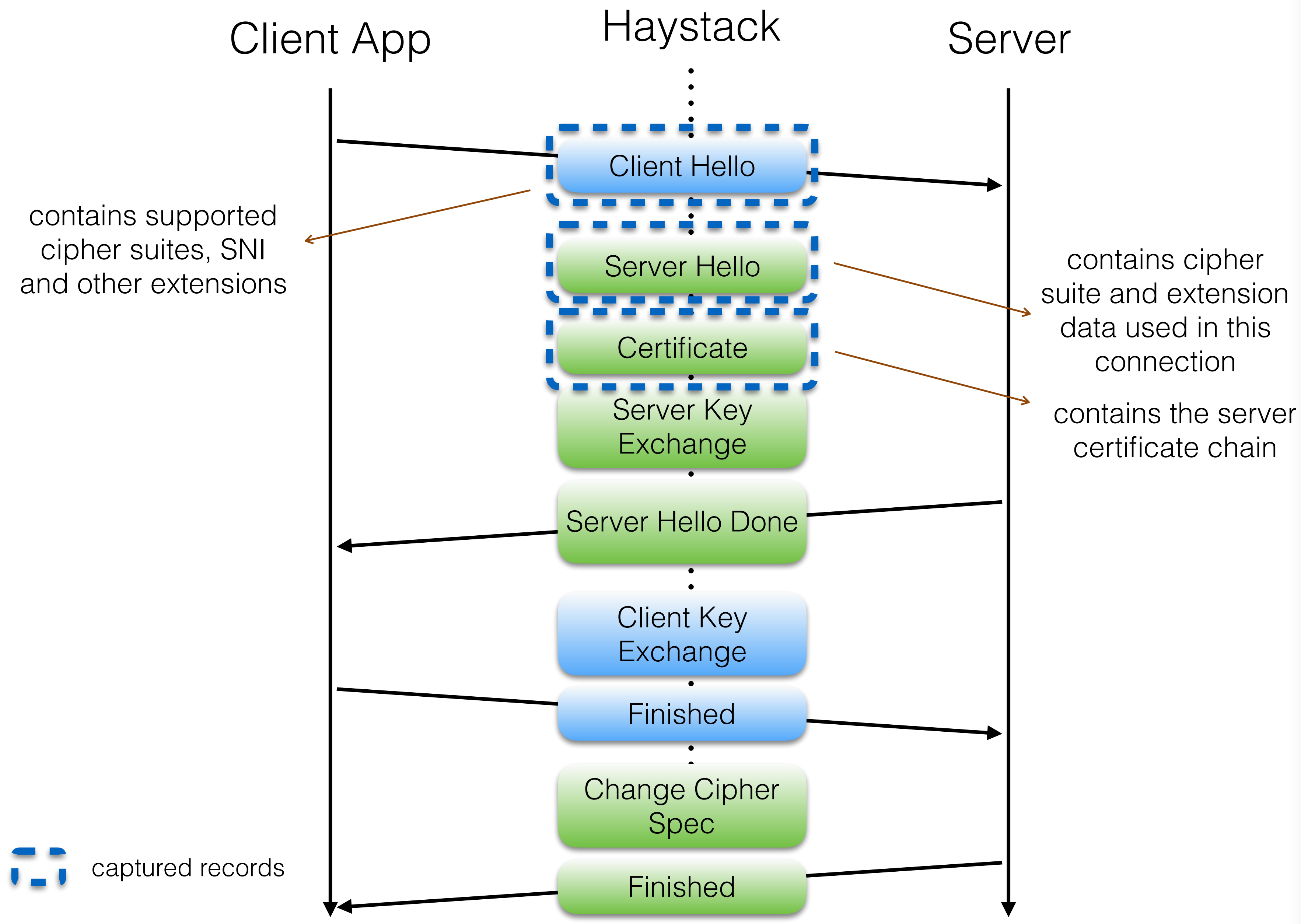
- Haystack captures and **analyzes all app's traffic in userspace**
- Runs **locally** on the phone
- **No root** access required
- User-friendly
- Available on **Google Play**
- Performs **TLS interception** (optional)



Measuring TLS traffic

We capture and analyze TLS records. Haystack also maps traffic to domain names and applications.
Handshake packets are analyzed to extract relevant information

- Sever Name Indication (SNI) and other TLS extensions
- Cipher suites supported by the client
- Final cipher suite used for the connection
- Server certificate and the certificate chain
- Alert records and other types of connection failures



Studying TLS connection failures

Haystack measures TLS failures and collects TLS alert records. This helps us understand **how apps use TLS**

- How do they react to poorly configured TLS servers?
- How do they handle servers with invalid, or self-signed certs?
- How do they handle servers using vulnerable ciphers/protocols?
- Can they detect/are they resilient to TLS proxies?

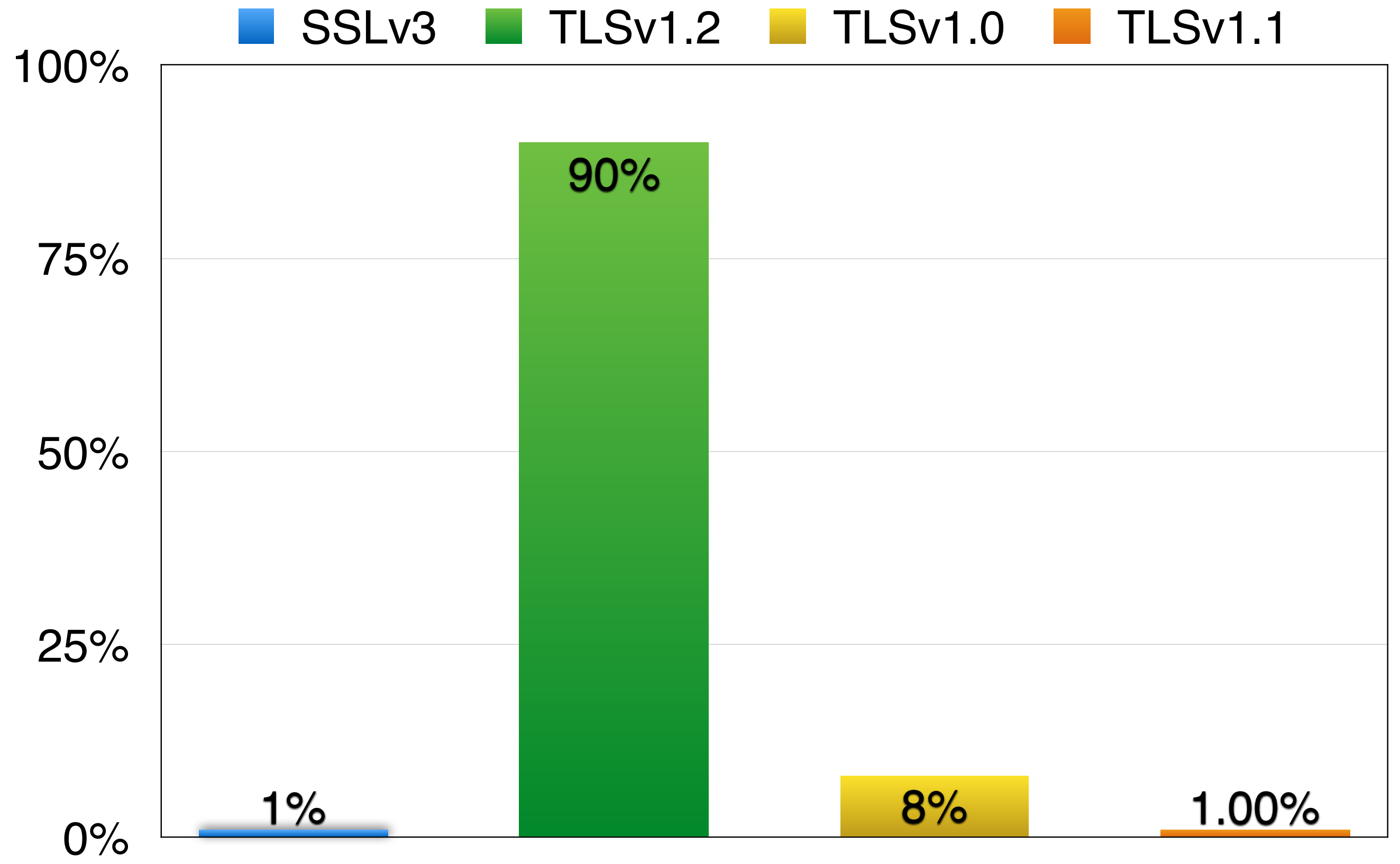
We can also assess **how servers use TLS** by analyzing server alert records:

- Do servers detect TLS proxies?
- Which TLS extensions do they support?

Preliminary Results

Protocol breakdown of 2.7 million TLS flows sampled from 1700 apps and over 500 installs shows that the phones that use lower versions of SSL are likely to be running older versions of Android.

- TLSv1.2 is supported in Android 4.1 onwards
- Previous versions have ~4% market share



Data shows a large number of clients support:

- **RC4** cipher suite (**76%** of clients)
- **MD5** hashing algorithm (**8%** of clients)

Future Work

- Longitudinal study of protocol usage by apps
- Detect network- and state-wide TLS proxies
- Study invalid certificates and TLS failures to detect potential TLS attacks in the network

Visit our website:

https://www.haystack.mobi

Download Haystack from **Google Play**