Lumen: Fine-Grained Visibility and Control of Mobile Traffic in User-Space

PIs: Narseo Vallina-Rodriguez, Christian Kreibich, Mark Allman, Vern Paxson (ICSI)

https://www.haystack.mobi

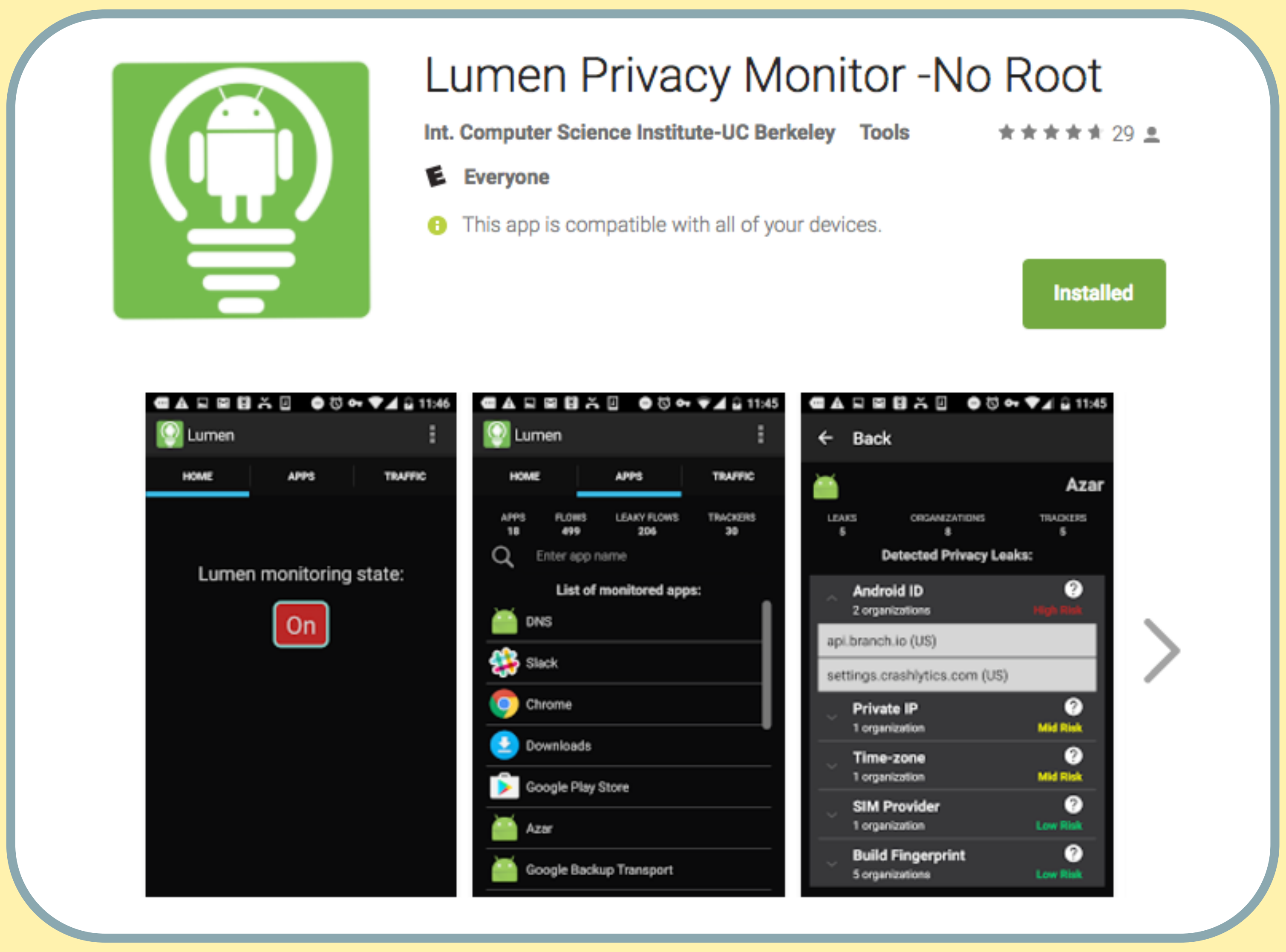
Introduction

Analyzing how mobile apps access user sensitive data, whether they manage it correctly and who they share it with in the wild is extremely challenging due to platform limitations.

Techniques such as dynamic and static analysis present shortcomings (accuracy and scale) that limit our understanding of the mobile ecosystem.

Project goals:

- Study empirically the mobile ecosystem at scale
- Promote mobile transparency
- Enable user-control over mobile traffic and apps
- Analyze app's traffic with real user-stimuli
- Identify privacy violations and malicious apps
- Evaluate app's network security



Lumen Privacy Monitor -No Root

Int. Computer Science Institute-UC Berkeley Tools ★★★★★ 29

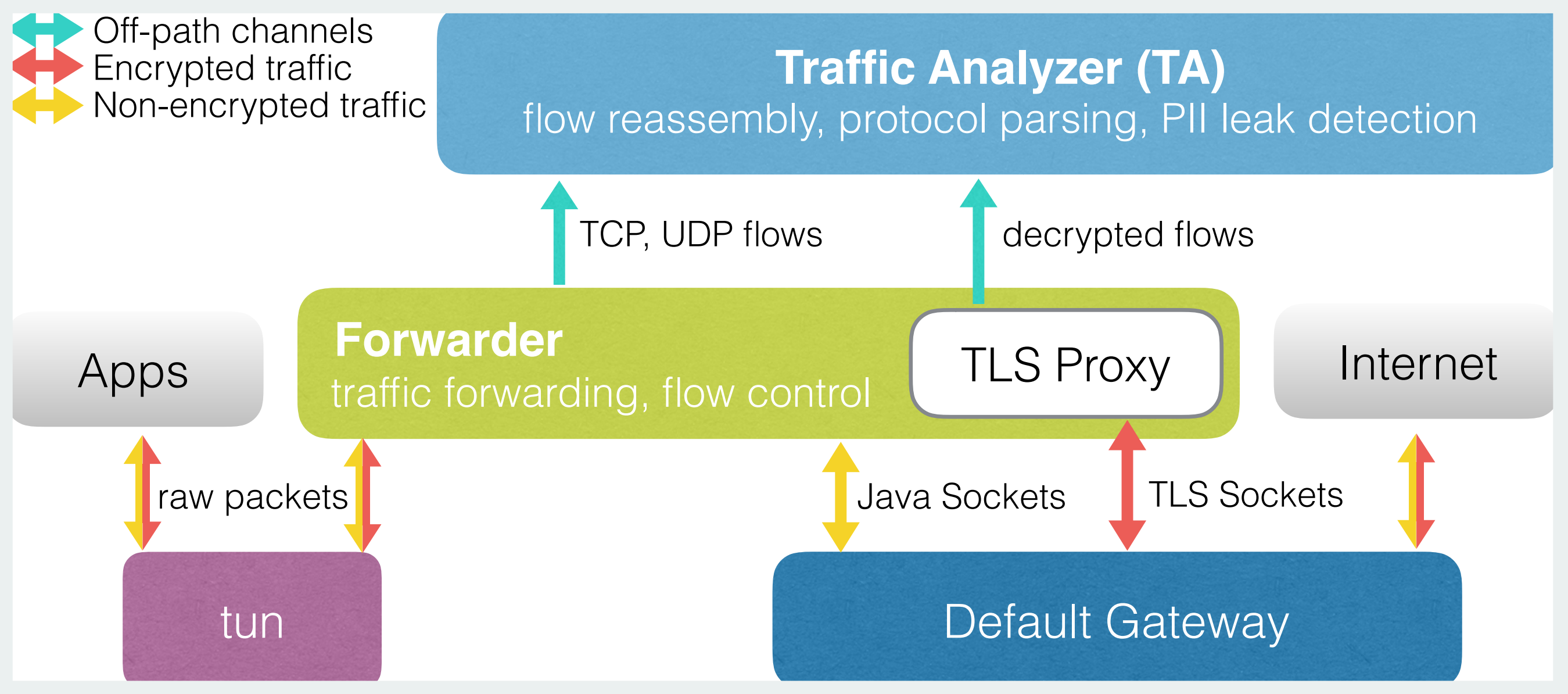
Everyone

This app is compatible with all of your devices.

Installed

The Lumen Privacy Monitor

- User-space traffic analyzer and controller
- Uses Android's VPN API to intercept traffic
- DPI and full flow-reassembly to detect PI leaks
- Maps proceses to TCP/UDP flows
- Supports TLS interception (opt-in)
- Provides accurate app traffic fingerprints



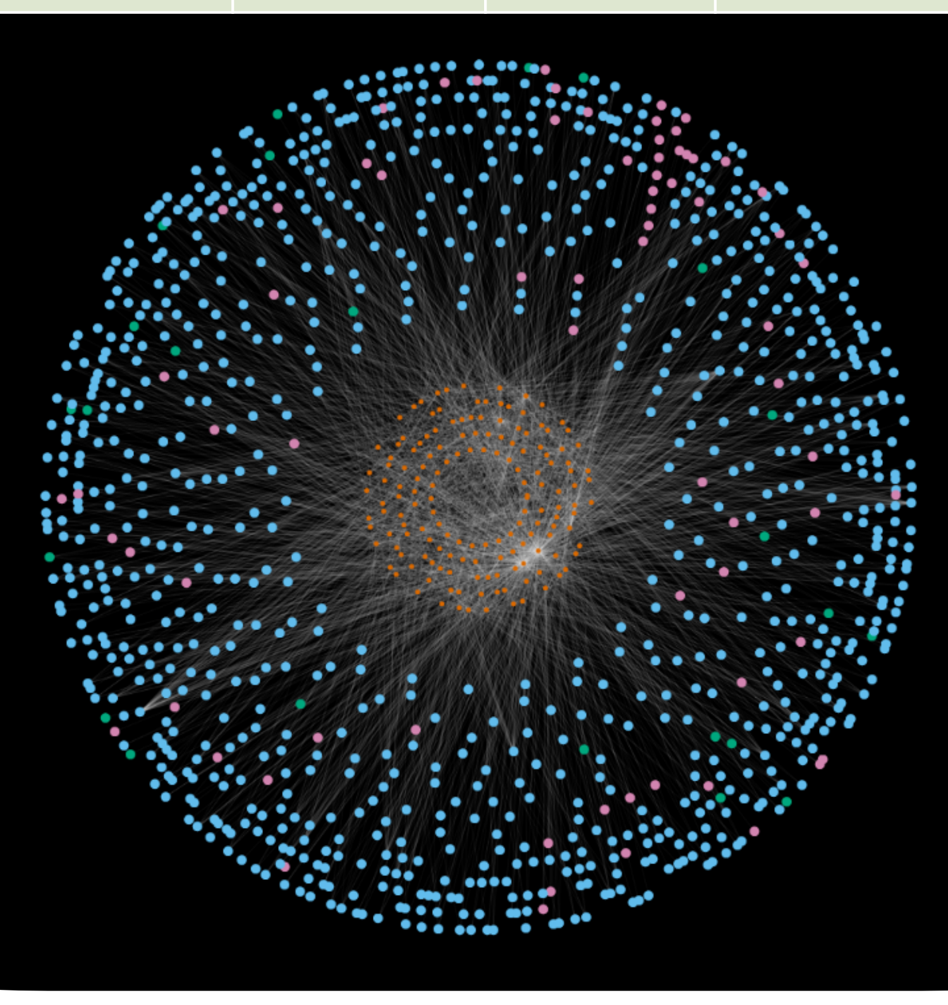
Analysis of the Privacy and Security Implications of Android VPN apps (IMC'16)

- Exhaustive analysis of 280+ VPN apps
- 38% VPN apps have malware presence
- 18% VPN apps tunnel traffic without encryption
- Instances of JS injection and TLS interception

Who's who in the mobile ecosystem?

- URL classifiers and blacklists fail to identify 3rd-party mobile advertising and tracking domains (ATS)
- Developed ATS classifier based on app-domain data flows
- 406 ATS domains found: 109 previously unidentified
- High penetration:
  - >70% Android apps connect to ATS domains
  - Games have the higher prevalence
- 68% of ATS domains offer cross-platform services

Users	Apps	Flows	Domains
953	2,468	1.9M	13,049



Current development efforts and research studies

- Improve app usability and enable user-control
- Develop REST API for data sharing
- Analyze TLS usage across mobile apps
- Measure impact of PPI services on mobile app ranks and data harvesting
- Illuminate pre-installed apps

https://www.haystack.mobi narseo@icsi.berkeley.edu

National Science Foundation
WHERE DISCOVERIES BEGIN

The 3rd NSF Secure and Trustworthy Cyberspace Principal Investigator Meeting
January 9-11, 2017
Arlington, Virginia

ICSI
INTERNATIONAL COMPUTER SCIENCE INSTITUTE