DHS Science and Technology Directorate

MOBILE DNS SECURITY THREATS

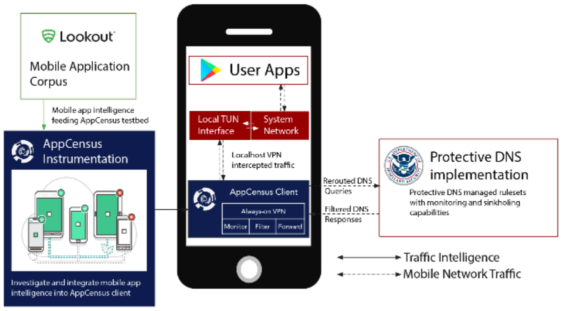
The ubiquity and convenience of smartphones mean employees have these devices with them constantly as they move between networks beyond enterprise control. Also, when roaming outside the enterprise network, Domain Name System (DNS) traffic and configurations are difficult to control—oftentimes traffic is intercepted by DNS proxies and other middleboxes deployed by the mobile network—making it difficult for enterprises to prevent access to malicious sites or protect against domain hijacking. This lack of control over DNS traffic opens new vectors for attack on the mobile devices including DNS cache poisoning and DNS manipulation attacks.

Further, by observing DNS queries originating on mobile devices enterprise network operators can gain deeper insight and control over mobile traffic and the Internet services users visit. Thus, an approach is required to enforce routing of a device's DNS requests to protect clients from such DNS-related security and privacy threats.

AppCensus seeks to provide a solution for DHS for secure mobile DNS traffic control. Leveraging and extending existing AppCensus technology, AppCensus will create a solution in user-space on mobile devices that allows DNS queries to be managed. The solution will intercept a device's DNS queries and route them to CISA managed trusted DNS recursive resolver. This resolver would check requests against threat intelligence feeds and allow/block and block malicious traffic accordingly.

MANAGING MOBILE DNS TRAFFIC

The AppCensus Secure and Resilient Mobile Network Infrastructure (SRMNI) project will research the three potential protective DNS solutions and determine their fit for use the mobile proof-of-concept. Leveraging the Lookout and AppCensus infrastructure, the company will evaluate potential solutions through a variety of traffic scenarios. Key metrics include proper handling of known malicious domains, device authentication and monitoring, logging and interception of DNS traffic in both plaintext (i.e., unencrypted payload using either Transmission Control Protocol or User Dataram Protocol via port 53), and encrypted form (i.e., DNS over Hypertext Transfer Protocol Secure, DNS over Transport Layer Security).


Lookout
Mobile Application Corpus
Mobile app intelligence feeding AppCensus testbed
AppCensus Instrumentation
Investigate and integrate mobile app intelligence into AppCensus client
User Apps
Local TUN Interface
System Network
Localhost VPN intercepted traffic
AppCensus Client
Always-on VPN
Monitor
Filter
Forward
Rerouted DNS Queries
Filtered DNS Responses
Protective DNS implementation
Protective DNS managed rulesets with monitoring and sinkholing capabilities
Traffic Intelligence
Mobile Network Traffic

Overview of System Architecture.

The project focus is to develop a protective DNS proof-of-concept implementation through on-device traffic interception and control with a mobile client. This mobile client will securely communicate with a designated DNS resolver to filter DNS queries for known malicious content.

Also, the research team will explore solutions for controlling encrypted DNS communications and research solutions for authenticating and securing device DNS settings for iOS and Android devices, to include capturing the origin agency.

EXTENDING NETWORK SECURITY

The platform will provide capabilities to analyze each mobile app's runtime behaviors and assess its security and privacy risks at scale in a privacy-preserving manner. Leveraging this platform, CISA can seek to extend the capabilities into user-space, thereby providing real-time analysis in the field.

UPCOMING MILESTONES

- Demonstration - July 2021
- Use-Cases and Results of Pilot—August 2022

SRMNI R&D PERFORMER

AppCensus Inc., El Cerrito, California.