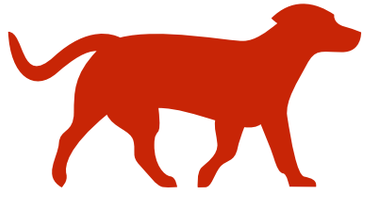


Red Rover

A collaborative approach to content filtering

Tommy Pauly & Richard Barnes

IAB M-TEN Workshop

Is there a conflict between filtering and privacy?

Let's look at what various entities want to do.

	Network Operator	Client Device & Applications
Goals	**Block malware** **Prevent objectionable content** **Enforce regulations** **Enforce Terms & Conditions**	**Protect user security** **Protect user privacy** **Access user-chosen content**

	Network Operator	Client Device & Applications
Goals	Block malware Prevent objectionable content Enforce regulations Enforce Terms & Conditions	Protect user security Protect user privacy Access user-chosen content
Mechanisms	DNS filtering & redirection TLS SNI filtering IP firewalling	Encrypted DNS TLS TLS ECH VPNs and Proxies

	Network Operator	Client Device & Applications
Goals	Block malware Prevent objectionable content Enforce regulations Enforce Terms & Conditions	Protect user security Protect user privacy Access user-chosen content
Mechanisms	DNS filtering & redirection IP firewalling TLS SNI filtering	Encrypted DNS TLS TLS ECH VPNs and Proxies

The intents do not inherently conflict (in most cases), just the protocol mechanisms.

Most clients don't want to expose users to harmful content, or to violate terms and conditions.

Most networks don't want to interfere with user privacy and security.

Existing models

Safe Browsing

Today, many browsers use "safe browsing", such as Google's service

- Browsers download a list of partial hashes for URLs that are "bad" content in different categories

- If the browser is about to load a page that matches, it looks up the complete hashes, and blocks if there is a match

A Collaborative Approach

Proposal

1. Discovery mechanism: network tells the client about a "block-list service"; client is able to check in to that service
2. Filtering mechanism: the "block-list service" operates like Safe Browsing, allowing clients to learn about the block list and reasons without revealing all client behavior

Solution space

Discovery

CAPPORT API

PvD Options

DHCP/RA Options

Block-list service

Standardized Safe Browsing

"Full" hash lists

Private Information Retrieval

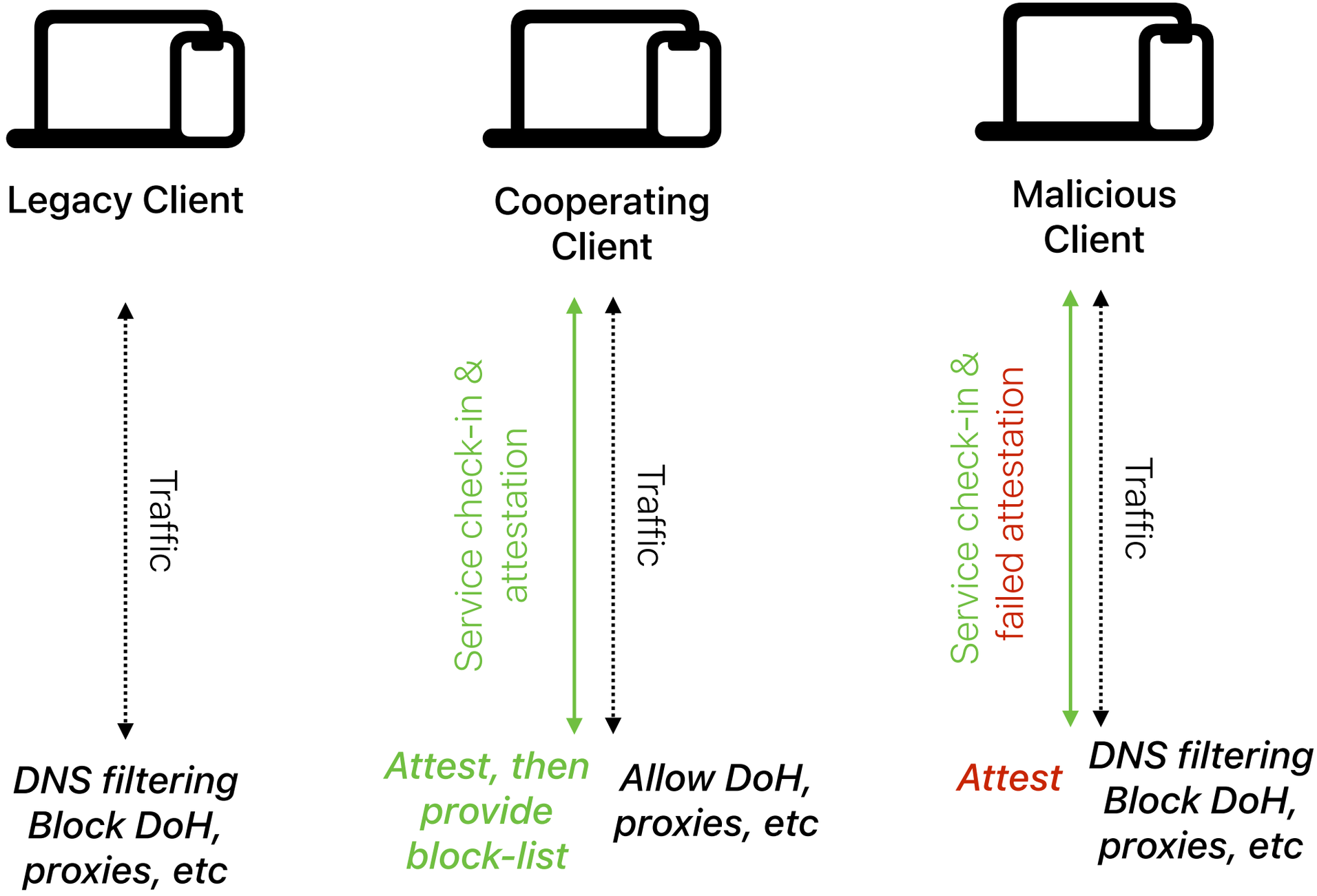
Circumvention and compatibility

On-device filtering using a hash list can provide stronger assurances than DNS or SNI blocking

Malicious or compromised endpoints could cheat

Legacy endpoints would not know about the block-list service

Selective enablement



Applicability

This won't work for all kinds of networks

- If you rely on TLS-intercepting firewalls, etc, this won't work for you

Aimed at the common use cases of public networks that need best-effort guarantees

Summary

Filtering content and user privacy do not need to conflict

Collaborative solutions can work when the goals of networks, endpoints, and users align

Standardized protocols could enable these collaborative models