draft-krose-multicast-security

Making multicast safe for the web

Kyle Rose <krose@krose.org>
Max Franke <mfranke@inet.tu-berlin.de>
Jake Holland <jakeholland.net@gmail.com>

Web Security Model

Confidentiality: A passive observer must not be able to identify or access content through simple observation of the bits being delivered, up to the limits of metadata privacy (such as traffic analysis, peer identity, application/transport/security-layer protocol design constraints, etc.).

Authenticity: A receiver must be able to cryptographically verify that the delivered content originated from the desired source.

Integrity: A receiver must be able to distinguish between original content as sent from the desired source and content modified in some way (including through deletion) by an attacker.

Non-linkability: A passive observer must not be able to link a single user across multiple devices or a single client roaming across multiple networks.

Web Security Model: Unicast

Confidentiality: TLS, up to traffic analysis

Authenticity: TLS, aided by CAB infrastructure

Integrity: TLS, aided by CAB infrastructure

Non-linkability: Partly mitigated by a variety of measures

Web Security Model: Multicast?

Confidentiality: Distinct model: multicast is for shared content

Authenticity: Conceptual equivalence feasible

Integrity: Conceptual equivalence feasible

Non-linkability: Distinct model: multicast is for shared content

Confidentiality

Unicast

- Unique transport keys per endpoint pair
- Still vulnerable to traffic analysis and cleartext metadata

Access control and (some) privacy

Multicast

- Protected from unauthorized users
- Encryption keys shared by all authorized users
- Still vulnerable to traffic analysis and cleartext metadata

Access control only

So what about privacy?

Privacy with multicast

K-anonymity

- Hop-by-hop with no end-to-end addressing
  ⇒ Need tap point close to a user to know who is subscribed to what
- No standard mechanism to discover content given (S,G)
  ⇒ Private, access-controlled content protected from identification beyond traffic analysis
    - DORMS can be access-controlled to minimize metadata offered to unprivileged devices/users
- Unicast control plane protected by unicast confidentiality
  ⇒ Linking unicast control plane to multicast delivery limited to traffic analysis

Personal data?

- Providers should not put private data on a billboard
- Providers should not post private data on a public website
- Providers should not multicast private data to a group

Mishandling happens at layer 8 before at layer 2

⇒ Not an issue specific to multicast

Other issues discussed

- Forward secrecy
- Request/response binding
- Linkability
- Browser-specific threats
- Referer checks

Motivation

- Importantly: some multicast or multicast-like solution is inevitable (q.v., MAUD, MoQ relays) simply because *unicast doesn't scale* to universal live content delivery

Do we want something end-to-end, or something under the control of networks and CDNs that creates more privacy and security attack surface?

Questions?
Adoption?