Internet Filtering

Nalini Elkins, Barry Shein, Vittorio Bertola
What is the problem?

• Filtering of objectionable content

• One of the biggest problems the world faces

• Dark side of the Internet

• Human Rights Considerations of Internet Filtering
  https://datatracker.ietf.org/doc/draft-elkins-hrpc-ifilter/
8 Risk Zones

1. Risk Zone 1: Truth, Disinformation, Propaganda
2. Risk Zone 2: Addiction & the Dopamine Economy
3. Risk Zone 3: Economic & Asset Inequalities
4. Risk Zone 4: Machine Ethics & Algorithmic Biases
5. Risk Zone 5: Surveillance State
6. Risk Zone 6: Data Control & Monetization
7. Risk Zone 7: Implicit Trust & User Understanding
8. Risk Zone 8: Hateful & Criminal Actors
How ISIS became the world’s deadliest startup

• ISIS uses technology better than most tech start-ups. Ghost Security Group, a counterterrorism organization, has noted in the past that ISIS utilizes almost every social app imaginable to communicate and share its propaganda, including mainstays like Twitter and Facebook; encrypted chat apps such as Telegram, Surespot, and Threema; and messaging platforms including Kik and WhatsApp. The terror group shares videos of beheadings on YouTube and even more gruesome clips on LiveLeak.

• They use the remarkably secure Apple iMessage to communicate. They preach to their disciples across the world using Internet radio stations. When a terror attack takes place, they use Twitter to claim responsibility and their followers subsequently cheer with favorites and retweets. Perhaps most frighteningly, the group’s dominance as a modern-day terror network is visible through how quickly their social-media dominance is accelerating.

Network Service Header Encoding (RFC 8300)

- Version (0x0)
- TTL counts down from 63
- Length (in long words) of whole NSH
- Meta Data type (see later slide)
- Next Protocol (Protocol type of next header)
  - IPv4/IPv6/MPLS/Ethernet etc.

<table>
<thead>
<tr>
<th>Ver</th>
<th>TTL</th>
<th>Length</th>
<th>MD Type</th>
<th>Next Protocol</th>
</tr>
</thead>
</table>

- Service Path Identifier (SPI)
- SI indicates which SF to process next

- SPI indicates the specific SFP in use
- One or more Extension Headers
  - Used principally (only?) to carry Meta Data
    - See later slide

Transport Encapsulation

NSH

Payload Packet

Base Header

Service Path Header

Extension Header

Service Path Identifier (SPI)

Extension Header

Extension Header

Extension Header

Transport Encapsulation

NSH

Payload Packet
Meta Data

• What is Meta Data?
  • Information about the packet that is carried along with the packet
    • May be derived from the packet (e.g., hash or DPI)
    • May be generated by an SF (e.g., caller ID or content type)
  • Used by SFs to help execute their functions on the packet
    • Generally, Meta Data could be regenerated by an SF, but would be wasteful of processing and configuration

• Where do you draw the line?
  • A Classifier works on a packet to select the SFP
  • That work is carried in the NSH as the SPI
    • The SPI is not considered to be Meta Data
Contact Us

- Nalini Elkins
  - nalini.elkins@e-dco.com

- Barry Shein
  - bzs@theworld.com

- Vittorio Bertola
  - vittorio.bertola@open-xchange.com