The Effect of Pervasive Encryption on Operators

Kathleen M. Moriarty
(Speaking for myself, not Dell EMC or the IETF)
Al Morton
kathleen.moriarty.ietf@gmail.com

Effects of Pervasive Encryption

Editors: Kathleen Moriarty & Al Morton

- Increased encryption impacts security & network operations
  - Shift how these functions are performed
  - New methods to monitor and protect data will evolve
  - In more drastic circumstances, ability to monitor may be eliminated

- Collection of current security and network management functions impacted by encryption
  - Draft does not attempt to solve these problems
  - It merely documents the current state to assist in the development of alternate options to achieve the intended purpose of the documented practices

- https://datatracker.ietf.org/doc/draft-mm-wg-effect-encrypt/

Internet Privacy & Confidentiality

Current IETF and IAB Guidance

- IETF Privacy Considerations for Internet protocols
  - https://datatracker.ietf.org/doc/rfc6973/
  - Data protection
    - Object level encryption
    - Determining when data is not necessary
    - Obscuring data or generalizing when possible
    - Protections on sensitive data and indexes to that data
  - Push for encrypted traffic
- IAB Statement on Internet Confidentiality
  - https://www.iab.org/2014/11/14/iab-statement-on-internet-confidentiality/

What changed/is changing?

Pervasive Monitoring is an Attack - RFC7258

- Opportunistic security (OS)
    - TLS - minimal uses of OS with TLS
    - IPsec - NULL authentication
        - Implemented in a few Linux Operating Systems
        - System-to-system encryption using IPsec tunnel mode
- Stronger transport encryption
    - TLS 1.3 provides perfect forward secrecy
    - IPsec already provided end-to-end securely
- Multiple protocols in consideration for PATIENT side meeting/effort
- RFC7258 calls for balance between security & network monitoring

What’s the Problem?

Encryption blocked to prevent impact on current operations

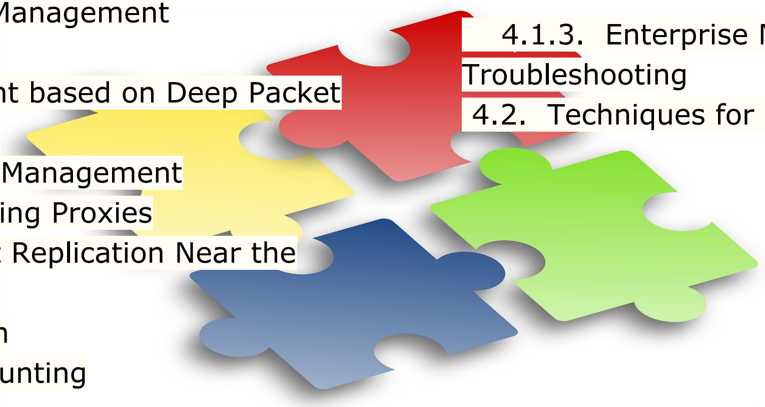
Ad Injection

0101001010100010011110010101

- Clear text has been used to inject ads, as well as monitor traffic for network and security purposes
- Operational capabilities are diminishing, some operators responded by stopping encryption negotiation
- Typically required exposure (media & regulators) to correct

Network Service Provider Monitoring

- 2.1. Passive Monitoring
  - 2.1.1. Traffic Surveys
  - 2.1.2. Troubleshooting
  - 2.1.3. Traffic Analysis Fingerprinting
- 2.2. Traffic Optimization and Management
  - 2.2.1. Load Balancers
  - 2.2.2. Differential Treatment based on Deep Packet Inspection (DPI)
  - 2.2.3. Network Congestion Management
  - 2.2.4. Performance-enhancing Proxies
  - 2.2.5. Caching and Content Replication Near the Network Edge
  - 2.2.6. Content Compression
- 2.3. Network Access and Accounting
  - 2.3.1. Content Filtering
  - 2.3.2. Network Access and Data Usage
  - 2.3.3. Application Layer Gateways
  - 2.3.4. HTTP Header Insertion



Encryption for Enterprises

- 4.1. Monitoring Practices of the Enterprise
  - 4.1.1. Security Monitoring in the Enterprise
  - 4.1.2. Application Performance Monitoring in the Enterprise
  - 4.1.3. Enterprise Network Diagnostics and Troubleshooting
- 4.2. Techniques for Monitoring Internet Session Traffic

Security Monitoring for specific Attack Types

5.1. Mail Abuse and SPAM

5.2. Denial of Service

5.3. Phishing

5.4. Botnets

5.5. Malware

5.6. Spoofed Source IP Address Protection

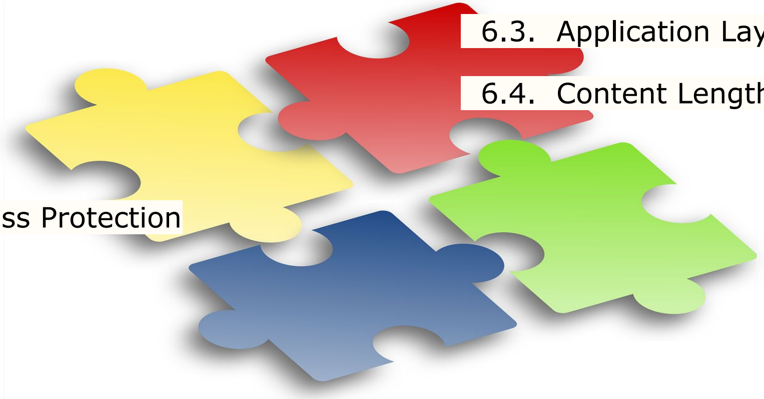
Application Flow Information Visible to a Network

6.1. IP Flow Information Export

6.2. TLS Server Name Indication

6.3. Application Layer Protocol Negotiation (ALPN)

6.4. Content Length, BitRate and Pacing



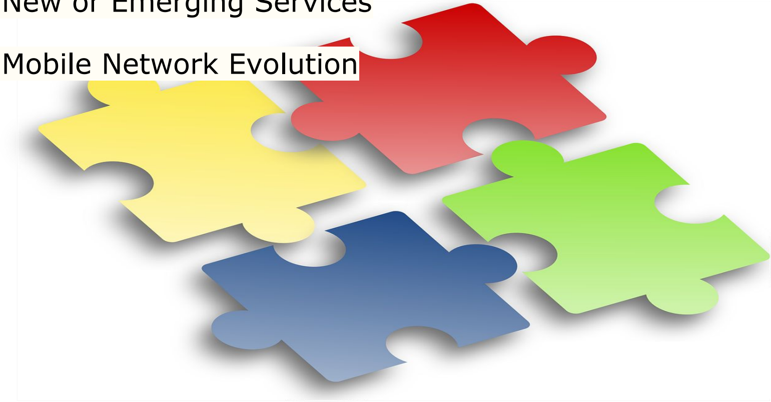
Impact on Mobility Network Optimizations and New Services

7.1. Effect of Encrypted ACKs

7.2. Effect of Encrypted Transport Headers

7.3. Effect of Encryption on New or Emerging Services

7.4. Effect of Encryption on Mobile Network Evolution



Service Provider Impact Varies

Impact summary

- Application service providers responded to revelations by increasing their use of encryption
- Data Storage increased use of encryption, management not impacted
- Backbone service provider monitoring impacted
- Some middlebox functions impacted
  - Content caching/Deep Packet Inspection
  - Content filtering - in network core for mobile users
  - Load balancers that use content for traffic redirection
  - Data Compression for mobile users
  - Data Leakage Prevention
- DDoS and incident management impact varies
- Enterprise operators impacted - but not necessarily for their cloud hosted solutions

Use of Encryption Encouraged to Protect Users Privacy

- Encryption increasing
  - in response to known threats and
  - move of sensitive application & data to hosted environments
- Protecting Users privacy at protocol level necessary
- Current techniques used by operators may no longer be possible in an encrypted Internet
- Devise new methods to accomplish goals
  - First document those goals and understanding objectives
  - Contribute to draft: "Effects of Pervasive Encryption"

Backup Slides

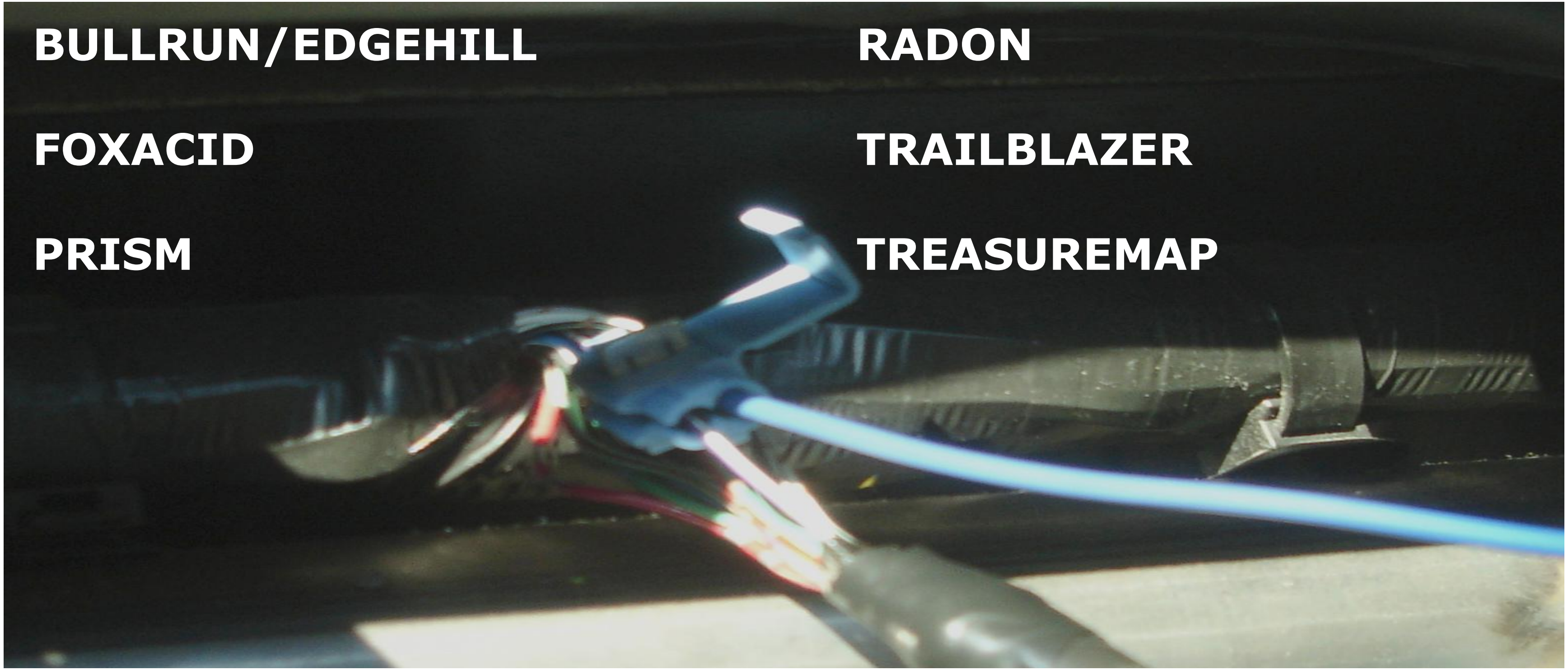
IETF Work Related to Pervasive Monitoring (PM)

- **“Pervasive Monitoring Is an Attack”**
  - RFC7258/BCP188 published after major IETF LC debate – sets the basis for further actions
  - https://www.rfc-editor.org/rfc/rfc7258.txt
  - BCP says to consider PM in IETF work
  - Existing-RFC privacy/PM review team formed
- **Opportunistic security (OS)**
  - Provides a way to get much easier deployment for some intermediate level of security
  - Fallback to unauthenticated encrypted sessions instead of plaintext
  - Updates to supported algorithms
  - Lower the barriers for key and certificate management
  - https://datatracker.ietf.org/doc/rfc7435/

IETF Work related to PM and Opportunistic Security

- Using TLS in Applications (UTA WG)
  - Update existing RFCs on how to use TLS in applications and mandate implementation of non-PFS ciphersuites
  - BCPs for TLS and DTLS attacks and configurations RFC7525
- TLS 1.3 (TLS WG)
  - TLS 1.3 being developed aiming for better handshake performance and encryption properties
  - Learning from our history of previous TLS problems
- HTTP/2.0 (HTTPBIS WG)
  - Major deployment model: HTTP over TLS, but not required yet
- TCP Increased Security (TCPInc)
  - Provide TLS functionality within TCP
  - Support Opportunistic security with a way to hook in authentication
- DNS Privacy (DPRIVE)
  - Reducing exposure of sensitive names found in DNS
  - https://datatracker.ietf.org/doc/draft-bortzmeyer-dnsop-dns-privacy/
- IPsec
  - NULL authentication support for Opportunistic Security approach

Motivation for Increased Privacy Protections



BULLRUN/EDGEHILL

FOXACID

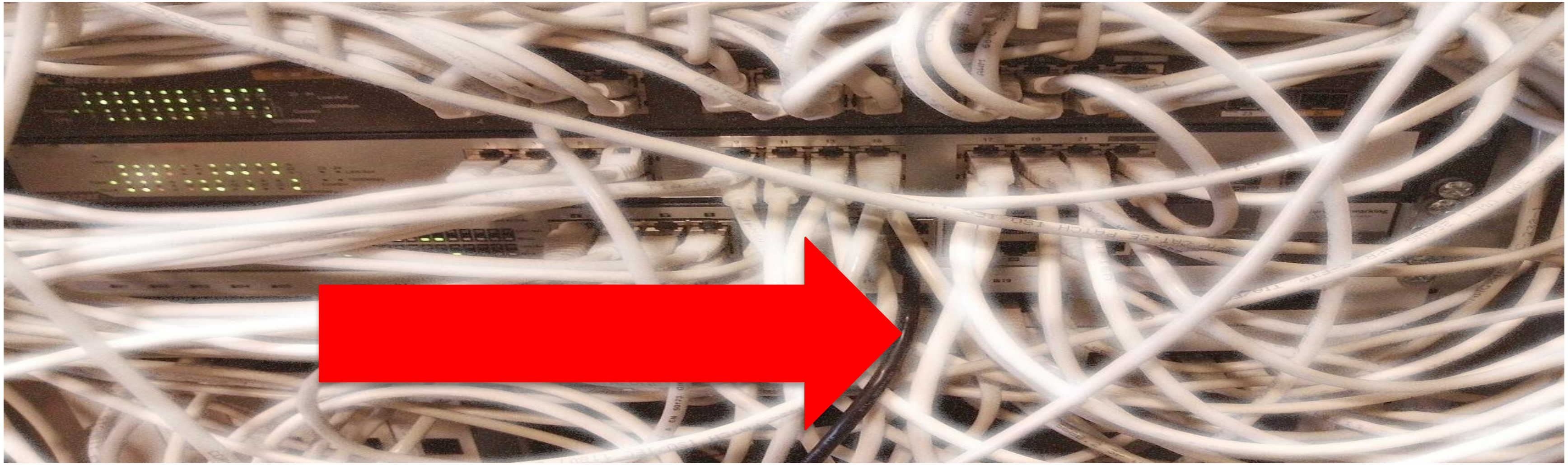
PRISM

RADON

TRAILBLAZER

TREASUREMAP

Pervasive Monitoring Changed the Game



- **Enable Opportunistic Security, making monitoring too costly to do broadly**
- **Force targeted attack on suspect traffic**