#RSAC

RSAConference2018

San Francisco | April 16 – 20 | Moscone Center

SESSION ID: PDAC-R02

NETWORK MONITORING IS GOING AWAY… NOW WHAT? TLS, QUIC, AND BEYOND

MODERATOR: **Kathleen M. Moriarty**
Global Lead Security Architect, Dell EMC
@KathleeMoriarty

PANELISTS:

Daniel Kahn Gillmor
Senior Staff Technologist
ACLU

Darin Pettis
VP - Infrastructure Consultant
Large Financial, speaking for himself

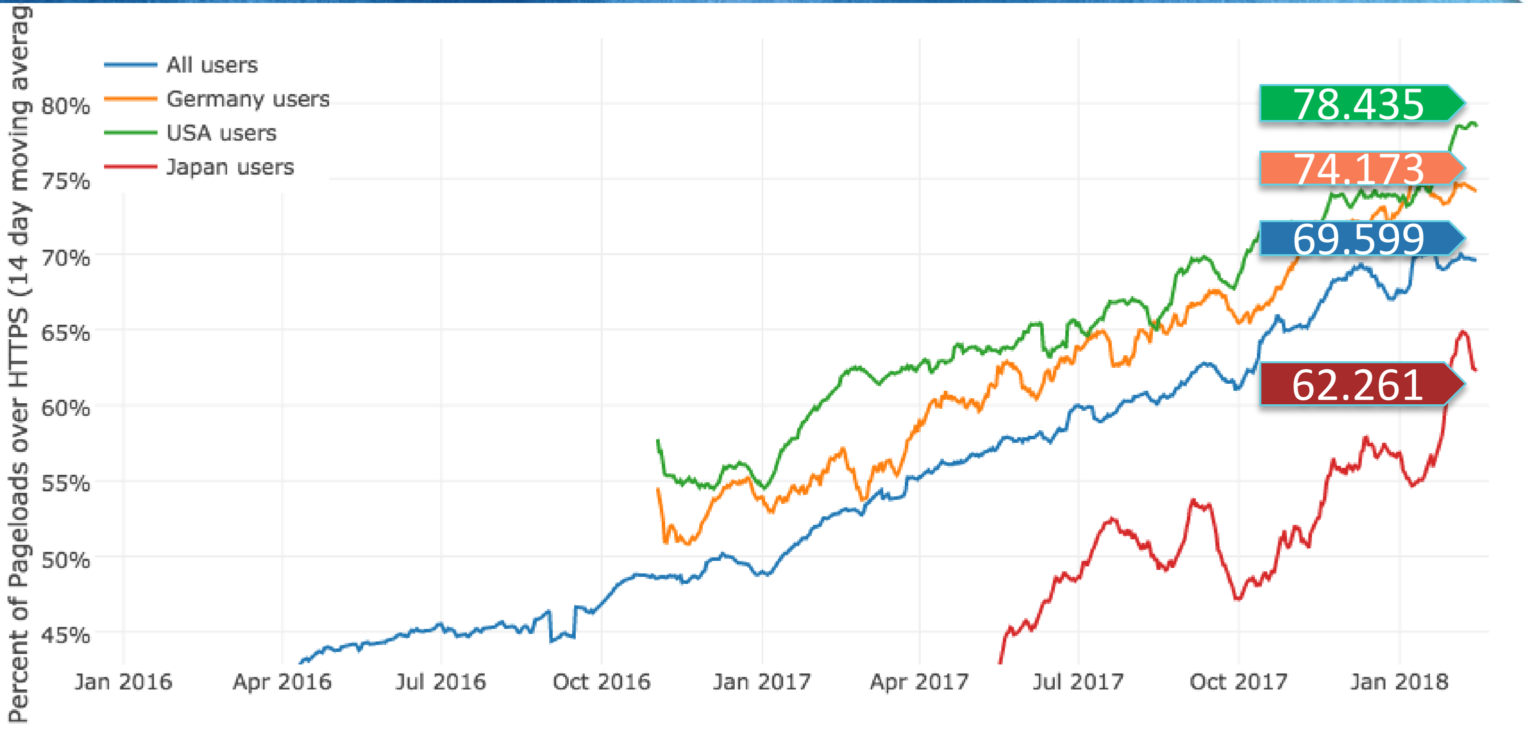
Tim Polk
Computer Scientist
NIST

Bottom line up front

Trends in encryption use encryption protocol standards and standard-based products are and will continue to increase the complexity of monitoring for management and security

Options exist to maintain visibility, but identifying and implementing the most appropriate choice for your network will require careful planning

Motivators for Increased Internet Encryption



Source: Firefox Telemetry

- Pervasive Monitoring Is an Attack - RFC7258
- Privacy for Internet Protocols – RFC6973
- Opportunistic Security: Some Protection Most of the Time – RFC7435
- Research into Human Rights Protocol Considerations – RFC8280
- Impact: The Effect of Pervasive Encryption on Operators

Enterprise encryption drivers

COMPLIANCE

INTELLECTUAL PROPERTY PROTECTION

CUSTOMER INFORMATION

PROTECTION FROM EXTERNAL THREATS

Source: Global Encryption Trends Study, Ponemon Institute 2017

Enterprise Monitoring

Regulatory Requirements for Transaction Monitoring

Threat Detection

Troubleshooting

Detailed in the following drafts:

Why Enterprises Need Out-of-Band TLS Decryption

TLS 1.3 Impact on Network-Based Security

Transport Layer Security(TLS) v1.3 changes

IMPROVED PROTECTION AGAINST INTERCEPTION

- Public-key exchange mechanisms provide forward secrecy
- More secure key exchange based on the Elliptic Curve Diffie-Hellman algorithm
- Static RSA and Diffie-Hellman cipher suites deprecated
- Supported symmetric algorithms are Authenticated Encryption with Associated Data (AEAD)

INTRODUCTION OF 0-RTT

- Enhances performance
- Replay attack possible, loss of forward secrecy
- See mitigating options or use 1-RTT, configurable on server

ALL HANDSHAKE MESSAGES AFTER THE SERVERHELLO

- Via EncryptedExtensions
- ALPN response now encrypted

New session encryption protocols

QUICK UDP INTERNET CONNECTIONS (QUIC)↗

- QUIC↗ protocol is UDP-based
- Provides stream-multiplexing
- encrypted transport protocol
- Uses TLSv1.3 used by default

TCPcrypt↗

- Opportunistic security applied to TCP
- Header in clear text
- Eases configuration automation
- Used with TCP Encryption Negotiation Option (TCP-ENO)

Increase security automation!

NEAR-TERM

Automatic Certificate Management Environment (ACME)

- Enables automated certificate management
- Support for multiple types of certificates

MID- TO LONG-TERM

Interface to Network Service Function (I2NSF)

- Developing standards to automate configuration management
- IPsec YANG modules and other protocols

GET INVOLVED NOW!

Security Automation and Continuous Monitoring (SACM)

- Improving security assessments for endpoint, follow on to NIST SCAP

Adapting to new protocols

#RSAC

NEAR-TERM

Evaluate application and device logs

- Work with vendors to ensure monitoring requirements are met at endpoints
- Evaluate tools to assist with endpoint monitoring at scale

MID-TERM

Consider TLSv1.3 for Internet-based sessions

- Improve Security for your customers
- Evaluate if 0-RTT is a good option for your servers or not
- Libraries and interoperability have been well tested

LONG-TERM

Consider what you define as the end point, shift monitoring to endpoints

Consider protocols better suited to data center monitoring

Continue to use TLSv1.2 in your data center

- Deprecation is likely a long ways off!
- Configure according to recommendations in RFC7525 ↘