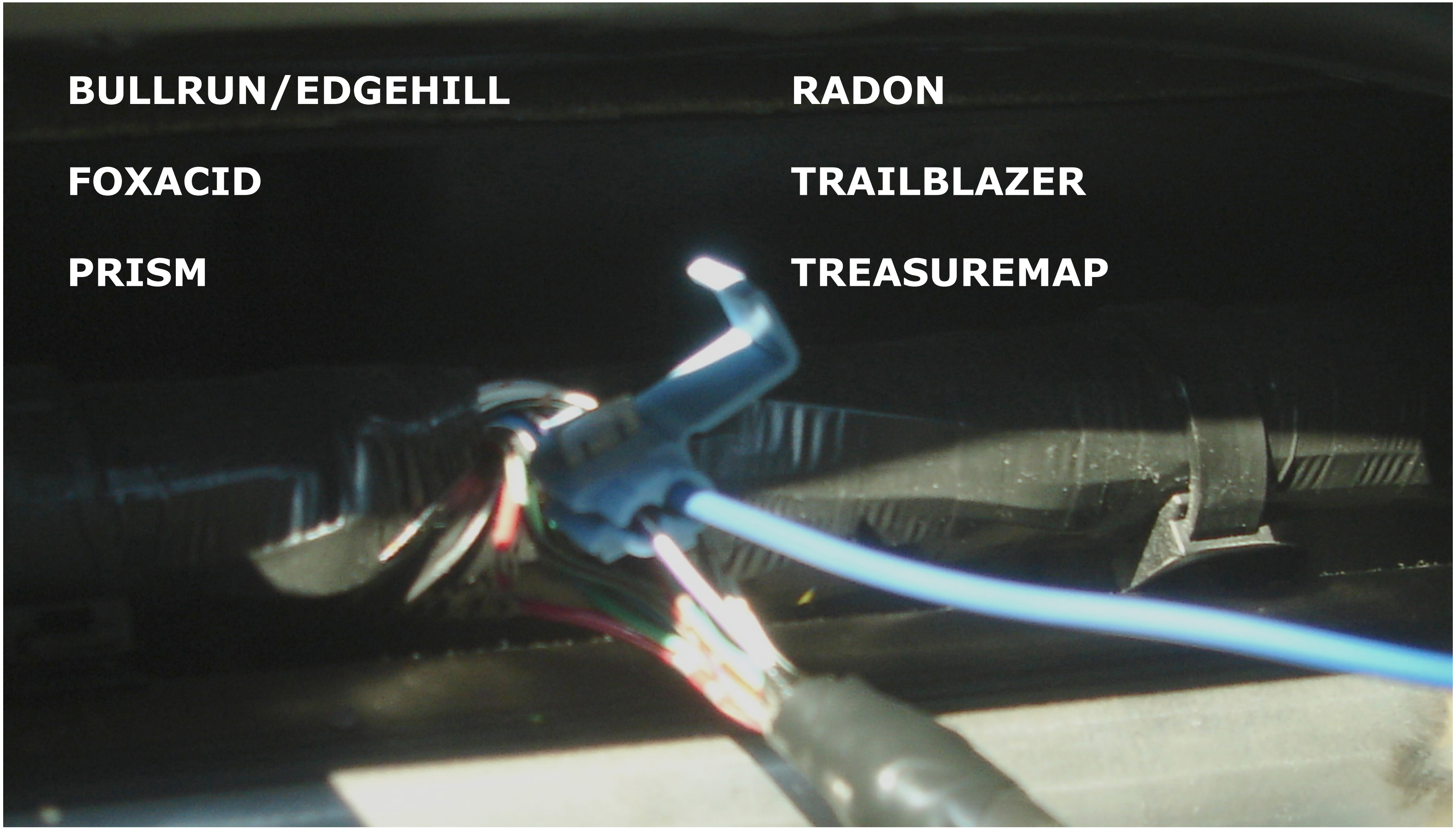
Security, Privacy, and the Effects of Ubiquitous Encryption

Kathleen Moriarty

Security Area Director (1 of 2)

(Speaking for myself, not the IETF)

Motivation for Increased Privacy Protections



BULLRUN/EDGEHILL

FOXACID

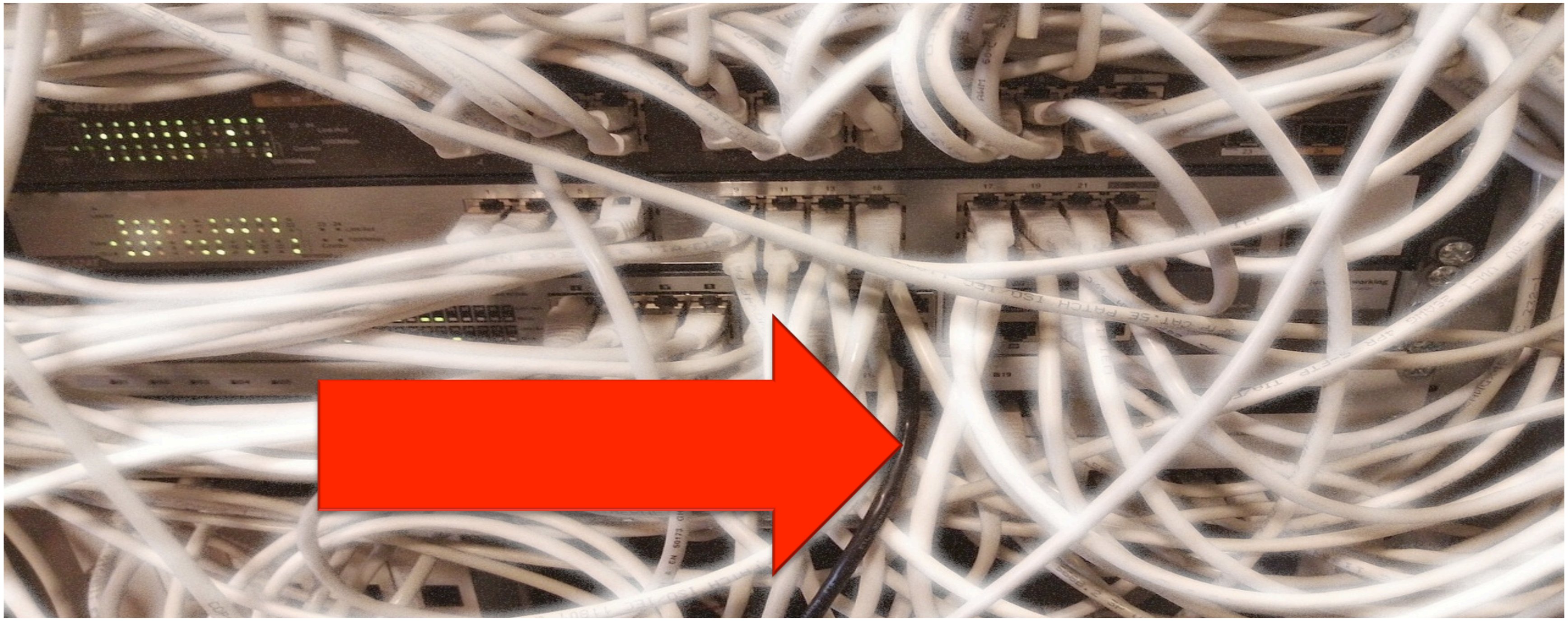
PRISM

RADON

TRAILBLAZER

TREASUREMAP

Pervasive Monitoring Changed the Game



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

How are Operators and Security Professionals Impacted?

The Effects of Ubiquitous Encryption

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

Effects of Ubiquitous 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

What’s the Problem?

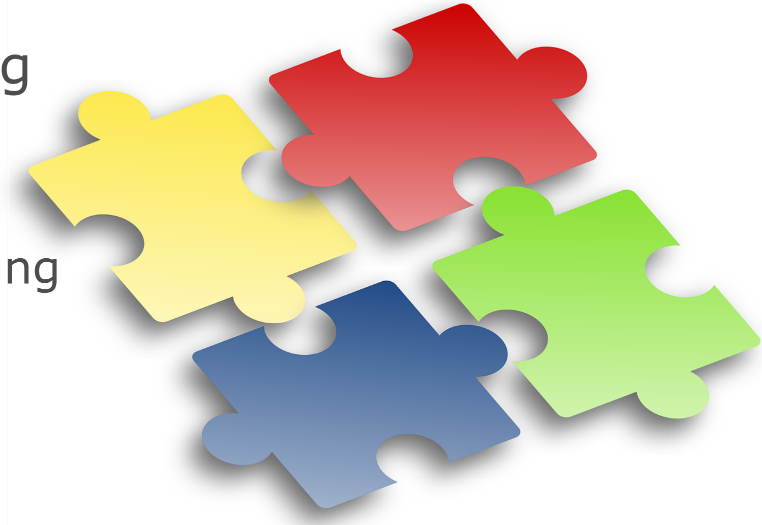
Encryption blocked to prevent impact on current operations

Ad Injection

- 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

Middlebox Monitoring

Traffic Interception and Pattern Matching



- Traffic Analysis Fingerprinting
  - Encrypted and clear text pattern matching
    - Attack detection and monitoring
    - Invade Privacy, web traffic
- Traffic Surveys
  - Observations over time
  - Inferences about observed traffic using maximal information available
  - Accuracy of patterns decline with encryption
- Deep Packet Inspection
  - Analysis of user flows and apps (for resource optimization)
  - Used with content distribution networks to improve efficiency
    - Note: CDNs moving to end-to-end control of data now
- Data Compression Gateway
  - Minimize traffic required using resource-constrained services, e.g., Data Caps

Performance Management and Troubleshooting

Current methods for existing functions impacted by encryption

- Availability and Performance monitoring impacted by move to encryption
  - Inability to discern difference between network and host-related causes of unavailability
- Inaccuracy will increase and efficiency of repair activities will decrease
- Use of websockets will make application differentiation more difficult

Encryption in Hosted SP Environments

Drivers different for Increased Security Protections

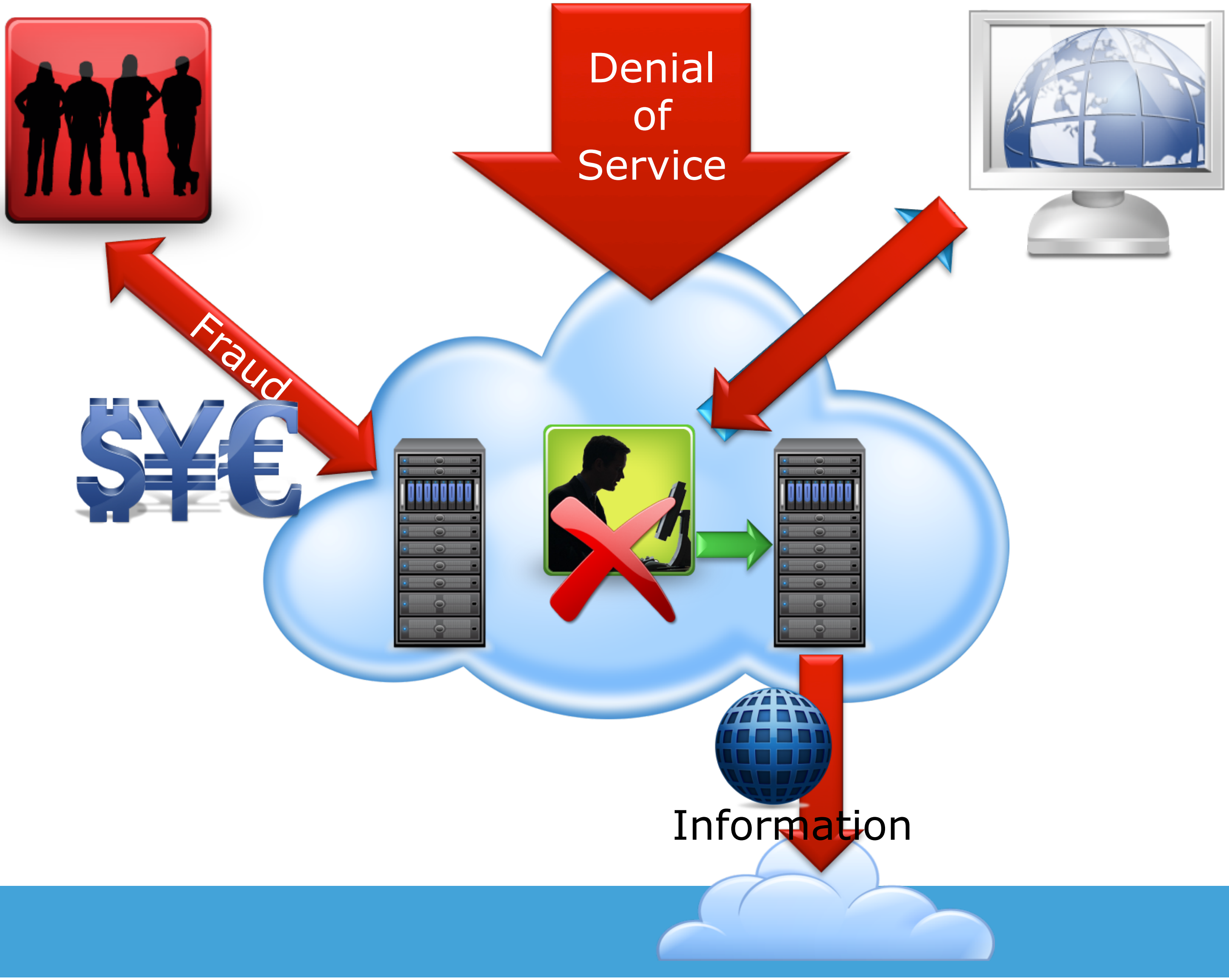
- Management Access
  - SP access to manage infrastructure: encrypted or isolated
  - Customer management access encrypted
- Hosted Applications
  - Increasingly sensitive applications
  - Data leakage protection (DLP) now limited
- Access Control Management and monitoring shifting
  - Logs may be used as an alternative monitoring data source
  - Monitoring and filtering may be restricted to:
    - 2-tuple IP-level with source and destination IP addresses alone, or
    - 5-tuple IP and protocol-level with source IP address, destination IP address, protocol number, source port number, and destination port number.

Data Storage

Capabilities changed, but solution providers have adapted

- Host-level encryption
  - End-to-end, encrypted at application or prior to transition to hosted environment
  - Backup, external storage
- Disk encryption, Data at Rest
  - Requires transport encryption to protect data on the wire
  - May only be used to protect from physical theft of disk
  - Controller based encryption or Self Encrypting Drives
- Data replication between data centers
  - IPsec may limit ability to monitor

Incident Monitoring



Summary

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 Ubiquitous Encryption”

Discussion

- What are the biggest challenges as a result of increased encryption?
- Are there additional impacts to operators and security professionals that need to be considered?
    - Not yet documented
- What alternative options exist to enable administrators/operators to achieve their operational objectives?
    - Solutions

Thank you!