Effect of Ubiquitous Encryption
draft-mm-wg-effect-encrypt-02

Abstract

Increased use of encryption will impact operations for security and network management causing a shift in how these functions are performed. In some cases, new methods to both monitor and protect data will evolve. In more drastic circumstances, the ability to monitor may be eliminated. This draft includes a collection of current security and network management functions that may be impacted by the shift to increased use of encryption. This draft does not attempt to solve these problems, but rather document the current state to assist in the development of alternate options to achieve the intended purpose of the documented practices.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on January 7, 2016.

Copyright Notice

Copyright (c) 2015 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of
publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction .............................................. 3
2. Network Service Provider Monitoring .......................... 5
   2.1. Middlebox Monitoring .................................. 5
       2.1.1. Traffic Analysis Fingerprinting .................. 5
       2.1.2. Traffic Surveys .................................. 6
       2.1.3. Deep Packet Inspection (DPI) ..................... 6
       2.1.4. Connection to Proxy for Compression ............. 7
       2.1.5. Mobility Middlebox Content Filtering ............ 7
   2.2. Network Monitoring for Performance Management and Troubleshooting ...................................... 8
   2.3. Inter Data Center Encryption ............................ 9
  2.3.1. new section ........................................ 9
3. Encryption in Hosting SP Environments .......................... 9
   3.1. Management Access Security .............................. 9
       3.1.1. Customer Access Monitoring ....................... 10
       3.1.2. Application SP Content Monitoring ............... 11
   3.2. Hosted Applications .................................... 11
       3.2.1. Monitoring needs for Managed Applications .......... 12
       3.2.2. Mail Service Providers ............................ 12
       3.2.3. Code Repositories ................................ 13
       3.2.4. Document Management .............................. 13
   3.3. Data Storage ........................................... 13
       3.3.1. Host-level Encryption .............................. 14
       3.3.2. Disk Encryption, Data at Rest ................... 15
       3.3.3. Cross Data Center Replication Services .......... 15
   3.4. new section ............................................ 16
4. Encryption for Enterprise Users ............................... 16
   4.1. Monitoring Needs of the Enterprise ..................... 16
   4.2. Techniques for Monitoring Internet Session Traffic .................................................. 17
5. Encryption for Home Users .................................... 19
   6.1. Mail Abuse and SPAM .................................. 19
   6.2. Denial of Service ................................... 19
   6.3. Phishing ............................................. 20
   6.4. Botnets ............................................. 21
   6.5. eCrime .............................................. 21
   6.6. Malware .............................................. 21
   6.7. Blocklists ........................................... 21
   6.8. [Any other subsections to be contributed?] ........... 22
1. Introduction

In response to pervasive monitoring revelations and the IETF consensus that Pervasive Monitoring is an Attack [RFC7258], efforts are underway to increase encryption of Internet traffic. Session encryption helps to prevent both passive and active attacks on transport protocols, with pervasive monitoring being primarily a passive attack. The Internet Architecture Board (IAB) released a statement advocating for increased use of encryption in November 2014. Views on acceptable encryption have also shifted and are documented in "Opportunistic Security" (OS) [RFC7435], where cleartext sessions should be upgraded to unauthenticated session encryption, rather than no encryption. OS encourages upgrading from cleartext, but cannot require or guarantee such upgrades. Once OS is used, it allows for an upgrade to authenticated encryption. These efforts are necessary to improve end user’s expectation of privacy, making pervasive monitoring cost prohibitive. Active attacks are still possible on sessions where unauthenticated sessions are in use.

The push for ubiquitous encryption via OS is specific to improving privacy for everyday users of the Internet. Many attackers and those that pose a greater threat are already using strong encryption and tools like TOR [TOR] to prevent active attacks on their data streams.

Although there is a push for OS, there is also work being done to improve implementation development and configuration flaws of TLS and DTLS sessions to prevent active attacks used to monitor or intercept session data. The (UTA) working group is in process of publishing documentation to improve the security of TLS and DTLS sessions. They have documented the known attack vectors in [I-D.ietf-uta-tls-attacks] and have documented Best Practices for TLS and DTLS in [I-D.ietf-uta-tls-bcp].

Current estimates of session encryption approximate that about 30% of web sites have session encryption enabled, according to the Electronic Frontier Foundation [EFF]. The Mozilla Foundation maintains statistics on SSL/TLS usage and as of March 2015, 64% of HTTP transactions are encrypted. Enterprise networks such as EMC...
observe that about 78% of outbound employee traffic was encrypted in June 2014. Although the actual number of sites may only be around 30%, they include some of the most visited sites on the Internet for corporate users.

In addition to encrypted web site access (TLS over HTTP), other application level transport encryption efforts are underway. This includes a push to encrypt session transport for mail (SMTP - gateway to gateway) and other protocols such as instant messaging (TLS over XMPP). Although this does provide protection from passive wiretapping [RFC4949] attacks, the servers could be a point of vulnerability if user-to-user encryption is not provided for these messaging protocols. User-to-user content encryption schemes, such as S/MIME and PGP for email and Off-the-Record (OTR) for Extensible Messaging and Presence Protocol (XMPP) are used by those interested to protect their data as it crosses intermediary servers, preventing the vulnerability described by providing an end-to-end solution. User-to-user schemes are under review and additional options will emerge to ease the configuration requirements, making this type of option more accessible to non-technical users interested in protecting their privacy.

Increased use of encryption (either opportunistic or authenticated) will impact operations for security and network management causing a shift in how these functions are performed. In some cases new methods to monitor and protect data will evolve, for other cases the need may be eliminated. This draft includes a collection of current security and network management functions that may be impacted by this shift to increased use of encryption. This draft does not attempt to solve these problems, but rather document the current state to assist in the development of alternate options to achieve the intended purpose of the documented practices.

In this document we consider several different forms of service providers, so we distinguish between them with adjectives. For example, network service providers (or network operators) provide IP-packet transport primarily, though they may bundle other services with packet transport. Alternatively, application service providers primarily offer systems that participate as an end-point in communications with the application user, and hosting service providers lease computing, storage, and communications systems in datacenters. In practice, many companies perform two or more service provider roles, but may be historically associated with one.

[Contributions are welcome to expand the list of documented practices]
2. Network Service Provider Monitoring

Network Service Providers (SP) are responding to encryption on the Internet, some helping to increase the use of encryption and others preventing its use. Network SPs for this definition include the backbone Internet Service providers as well as those providing infrastructure at scale for core Internet use (hosted infrastructure and services such as email).

Following the Snowden revelations, application service providers responded by encrypting traffic between their data centers to prevent passive monitoring from taking place unbeknownst to the providers (Yahoo, Google, etc.). Large mail service providers also began to encrypt session transport to hosted mail services. This had an immediate impact to help protect the privacy of users data, but created a problem for network operators. They could no longer gain access to session streams resulting in actions by several to regain their operational practices that require cleartext data sessions.

The EFF reported several network service providers taking steps to prevent the use of TLS over SMTP by breaking StartTLS, preventing the negotiation process resulting in fallback to the use of clear text. The use of encryption prevents middle boxes from performing functions that range from load balancing to monitoring for attacks or enabling "lawful intercept", such that described in [ETS1101331] and [CALEA] in the US. Some of these practices may be on the decline now that they are exposed through the media, but they are representative of the struggles administrators will have with changes in their ability to monitor and manage traffic.

2.1. Middlebox Monitoring

Network service providers use various monitoring techniques for security and operational purposes. The following subsections detail the purpose of each type of monitoring and what protocol fields are used to accomplish the task.

2.1.1. Traffic Analysis Fingerprinting

Fingerprinting is used in traffic analysis and monitoring to identify traffic streams that match certain patterns. This technique may be used with clear text or encrypted sessions. Some Distributed Denial of Service (DDoS) prevention techniques at the Network SP level rely on the ability to fingerprint traffic in order to mitigate the effect of this type of attack. Thus, fingerprinting may be an aspect of an attack or part of attack countermeasures.
The first/obvious trigger for DDoS mitigation is uncharacteristic traffic volume and/or congestion at various points associated with the attackee’s communications. One approach to mitigate such an attack involves distinguishing attacker traffic from legitimate user traffic through analysis. The ability to examine layers and payloads above transport provides a new range of filtering opportunities at each layer in the clear. Fewer layers are in the clear means reduced filtering opportunities to mitigate attacks.

Traffic analysis fingerprinting could also be used on web traffic to perform passive monitoring and invade privacy.

For example, browser fingerprints are comprised of many characteristics, including User Agent, HTTP Accept headers, browser plug-in details, screen size and color details, system fonts and time zone. [PANO] will audit these details for users. A monitoring system could easily identify a specific browser, and by correlating other information, identify a specific user.

2.1.2. Traffic Surveys

Internet traffic surveys are useful in many well-intentioned pursuits, such as CAIDA data [CAIDA] and SP network design and optimization. Tracking the trends in Internet traffic growth, from earlier peer-to-peer communication to the extensive adoption of unicast video streaming applications, has required a view of traffic composition and reports with acceptable accuracy. As application designers and network operators both continue to seek optimizations, the role of traffic surveys from passive monitoring grows in importance.

Passive monitoring makes inferences about observed traffic using the maximal information available, and is subject to inaccuracies stemming from incomplete sampling (of packets in a stream) or loss due to monitoring system overload. When encryption conceals more layers in each packet, reliance on pattern inferences and other heuristics grows, and accuracy suffers. For example, the traffic patterns between server and browser are dependent on browser supplier and version, even when the sessions use the same server application (e.g., web e-mail access). It remains to be seen whether more complex inferences can be mastered to produce the same monitoring accuracy.

2.1.3. Deep Packet Inspection (DPI)

The features and efficiency of some Internet services can be augmented through analysis of user flows and the applications they provide. For example, network caching of popular content at a
location close to the requesting user can improve delivery efficiency, and authorized parties use DPI in combination with content distribution networks to determine if they can intervene effectively. Encryption of packet contents at a given protocol layer usually makes inspection of that layer and higher layers impossible, as well as DPI processing at the formerly clear text layers.

Data transfer capacity resources in cellular radio networks tend to be more constrained than in fixed networks. This is a result of variance in radio signal strength as a user moves around a cell, the rapid ingress and egress of connections as users handoff between adjacent cells, and temporary congestion at a cell. Mobile networks alleviate this by queuing traffic according to its required bandwidth and acceptable latency: for example, a user is unlikely to notice a 20ms delay when receiving a simple Web page or email, or an instant message response, but will certainly notice a re-buffering pause in a video playback or a VoIP call de-jitter buffer. Ideally, the scheduler manages the queue so that each user has an acceptable experience as conditions vary, but the traffic type must be known. Application and transport layer encryption make the traffic type detection less accurate, and affect queue management.

2.1.4. Connection to Proxy for Compression

In contrast to DPI, various applications exist to provide data compression in order to conserve the life of the user’s mobile data plan and optimize delivery over the mobile link. The compression proxy access can be built into a specific user level application, such as a browser, or it can be available to all applications using a system level application. The primary method is for the mobile application to connect to a centralized server as a proxy, with the data channel between the client application and the server using compression to minimize bandwidth utilization. The effectiveness of such systems depends on the server having access to unencrypted data flows. As the percentage of connections using encryption increases, these data compression services will be rendered less effective, or worse, they will adopt undesirable security practices in order to gain access to the unencrypted data flows.

2.1.5. Mobility Middlebox Content Filtering

Service Providers may, from time to time, be requested by law agencies to block access to particular sites such as online betting and gambling, sites promoting anorexia, or access to dating sites. Content Filtering can also happen at the endpoints or at the edge of enterprise networks. This section is intended to merely document this current practice by operators and the effects of encryption on the practice.
Content filtering in the mobile network usually occurs in the core network. A proxy is installed which analyses the transport metadata of the content users are viewing and either filters content based on a blacklist of sites or based on the user’s pre-defined profile (e.g. for age sensitive content). Although filtering can be done by many methods one common method occurs when a DNS lookup reveals a URL which appears on a government or recognized block-list. The subsequent requests to that domain will be re-routed to a proxy which checks whether the full url matches a blocked url on the list, and will return a 404 if a match is found. All other requests should complete.

Even with encrypted connections, transport and lower layer metadata is able to be viewed. As such, systems content filtering should be able to continue in most applications. Cases when they may not work include when TLS proxies are being used which obscure metadata with the proxy metadata, and future versions of HTTP and TCP that may encrypt metadata, preventing content filtering software from working (this is currently not the case and has not been standardized).

Some sites involve a mixture of universal and age-sensitive content and filtering software. In these cases, more granular (application layer) metadata may be used to analyze and block traffic, which will not work on encrypted content.

2.2. Network Monitoring for Performance Management and Troubleshooting

Similar to DPI, the performance of some services can be more efficiently managed and repaired when information on user transactions is available to the service provider. It may be possible to continue such monitoring activities without clear text access to the application layers of interest, but inaccuracy will increase and efficiency of repair activities will decrease. Also, there may be more cases of user communication failures when the additional encryption processes are introduced, leading to more customer service contacts and (at the same time) less information available to network operations repair teams.

[Types of network and performance monitoring used by IP-level service providers should be discussed here. How does encryption impact their current techniques? What do they use in data streams to maintain expected service levels?]

With the growing use of WebSockets [RFC6455], many forms of communications (from isochronous/real-time to bulk/elastic file transfer) will take place over HTTP port 80, so only the messages and higher-layer data will make application differentiation possible. If the monitoring systems sees only “HTTP port 443”, it cannot...
distinguish application streams that would benefit from priority queueing from others that would not. In short, systems that invoked policies for the user’s benefit are rendered less-effective (or ineffective) by encryption of information they once viewed easily.

2.3. Inter Data Center Encryption

The use of encryption at an IP-level between data centers of large application service providers has increased as a result of revelations that governments were passively monitoring these connections. [How has security and operations monitoring of these session been impacted or has that been fully addressed and how? Storage section contains one example that fits this scenario.]

2.3.1. new section

[Needs for monitoring from an operational perspective could be in subsections to this bullet, contributions welcome to understand and document the struggle to determine alternate approaches in subsequent efforts. This should include specific monitoring goals as well as what is currently used to achieve those goals - how and why.]

3. Encryption in Hosting SP Environments

Hosted environments have had varied requirements in the past for encryption, with many businesses choosing to use these services primarily for data and applications that are not business or privacy sensitive. A shift prior to the revelations on surveillance/passive monitoring began where businesses were asking for hosted environments to provide higher levels of security so that additional applications and service could be hosted externally. Businesses understanding the threats of monitoring in hosted environments only increased that pressure to provide more secure access and session encryption to protect the management of hosted environments as well as for the data and applications.

3.1. Management Access Security

Hosted environments may have multiple levels of management access, where some may be strictly for the Hosting SP (infrastructure that may be shared among customers) and some may be accessed by a specific customer for application management. In some cases, there are multiple levels of hosting service providers, further complicating the security of management infrastructure and the associated requirements.

Hosting service provider management access is typically segregated from other traffic with a control channel and may or may not be
encrypted depending upon the isolation characteristics of the management session. Customer access may be through a dedicated connection, but this is becoming less common with newer hosted service models leveraging the Internet.

3.1.1. Customer Access Monitoring

Hosted applications that allow some level of customer management access may also require monitoring by the hosting service provider. The monitoring needs could include access control restrictions such as authentication, authorization, and accounting for filtering and firewall rules to ensure they are continuously met. Customer access may occur on multiple levels, including user-level and administrative access. The hosting service provider may need to monitor access either through session monitoring or log evaluation to ensure security service level agreements (SLA) for access management are met. The use of session encryption to access hosted environments will limit the ability to use session data to ensure access restrictions are maintained. Monitoring and filtering may occur at an:

- 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.

Session encryption at the application level, TLS for example, currently allows access to the 5-tuple. IP-level encryption, such as IPsec in tunnel mode prevents access to the 5-tuple and may limit the ability to restrict traffic via filtering techniques. This shift may not impact all hosting service provider solutions as alternate controls may be used to authenticate sessions or access may require that mobile clients access such services by first connecting to the organization before accessing the hosted application. Shifts in access may be required to maintain equivalent access control management. Logs may also be used for monitoring access control restrictions are met, but would be limited to the data that could be observed due to encryption at the point of log generation. Log analysis is out of scope for this document.

Intrusion detection, performance, availability, [What else should be covered in this section?]
3.1.2. Application SP Content Monitoring

Application Service Providers may offer content-level monitoring options to detect intellectual property leakage, or other attacks. The use of session encryption will prevent Data Leakage Protection (DLP) used on the session streams from accessing content to search on keywords or phases to detect such leakage. DLP is often used to prevent the leakage of Personally Identifiable Information (PII) as well as financial account information, Personal Health Information (PHI), and Payment Card Information (PCI). If session encryption is terminated at a gateway prior to accessing these services, DLP on session data can still be performed. The decision of where to terminate encryption to hosted environments will be a risk decision made between the application service provider and customer organization according to their priorities. DLP can be performed at the server for the hosted application and on an end users system in an organization as alternate or additional monitoring points of content, however is not frequently done in a service provider environment.

[What other monitoring is specific to SP Applications? This likely includes monitoring equipment, change control processing, configuration monitoring, security control compliance, performance, availability, OAM, etc. A number of the possibilities within these brackets may occur within the SP environment and may or may not be impacted by the push for encryption. With increasingly security applications moving to hosted environments, tenant isolation may require use of encryption inside of the data center. Should we discuss that here so the impact is understood and what monitoring performed today is documented?]

Secure overlay networks may be used in multi-tenancy scenarios to provide isolation assurance and thwart some active attacks. Section 7 of [RFC7348] describes some of the security issues possible when deploying VXLAN on Layer 2 networks. Rogue endpoints can join the multicast groups that carry broadcast traffic, for example. Tunneled traffic on VXLAN can be secured by using IPsec, but this adds the requirement for authentication infrastructure and may reduce packet transfer performance. Deployment of data path acceleration technologies can help to mitigate the performance issues, but they also bring more complex networking and management.

3.2. Hosted Applications

Organizations are increasingly using hosted applications rather than in house solutions that require maintenance of equipment and software. Examples include Enterprise Resource Planning (ERP) solutions, payroll service, time and attendance, travel and expense
reporting among others. Organizations may require some level of management access to these hosted applications and will typically require session encryption or a dedicated channel for this activity.

In other cases, hosted applications may be fully managed by a hosting service provider with service level agreement expectations for availability and performance as well as for security functions including malware detection.

3.2.1. Monitoring needs for Managed Applications

Performance, availability, and other SLA requirements, etc. [What monitoring is done by these SPs, why, and what do they monitor? Can this section cover the operational aspect for each of the offerings listed below, or do they need to be broken out by service?]

Performance, availability, and other aspects of a SLA are often collected through passive monitoring. For example:

- Availability: ability to establish connections with hosts to access applications, and discern the difference between network or host-related causes of unavailability.

- Performance: ability to complete transactions within a target response time, and discern the difference between network or host-related causes of excess response time.

Here, as with all passive monitoring, the accuracy of inferences are dependent on the cleartext information available, and encryption would tend to reduce the information and therefore, the accuracy.

3.2.2. Mail Service Providers

Mail (application) service providers vary in what services they offer. Options may include a fully hosted solution where mail is stored external to an organization’s environment on mail service provider equipment or the service offering may be limited to monitor incoming mail to remove SPAM [Section 6.1], malware [Section 6.6], and phishing attacks [Section 6.3] before mail is directed to the organization’s equipment. In both of these cases, content of the messages and headers is monitored to detect SPAM, malware, phishing, and other messages that may be considered an attack.

In addition to the monitoring needs for specific attack types discussed in Section 6, mail service providers [Need descriptions for other types of monitoring performed. What is used now in their monitoring? How will use of TLS between servers impact their ability to monitor for security or operations? Users have no idea if the TLS
covers their entire session stream or if it’s left in clear text over some of the hops in this hop-by-hop protection – does this matter and how does it impact monitoring or do monitoring needs lead to this problem (broken STARTTLS negotiations)?

Many efforts are emerging to improve user-to-user encryption to protect end user’s privacy. Some of these efforts involve encryption of email header information such as the message subject. Mail system operators could still find enough helpful information in the rest of the header fields if the subject was no longer accessible, however it could reduce effectiveness of administrators. In some cases, administrators may search on mail systems for known subject fields of abuse messages from inboxes or mail queues to remove phishing or other messages that contain malware or links to malware. Their ability to perform prevention may be more limited with full deployment of end-to-end mail encryption with header fields inaccessible. The header fields [RFC2822] used most often in their operational work include:

- Subject: – may be considered privacy sensitive
- To:/From: – may be considered privacy sensitive
- Received: from
- Date:
- Sent:

### 3.2.3. Code Repositories

Intrusion detection, performance, availability, malware detection, etc. [What monitoring is done by these SPs, why, and what do they monitor?]

### 3.2.4. Document Management

Intrusion detection, performance, availability, malware detection, etc. [What monitoring is done by these SPs, why, and what do they monitor?]

### 3.3. Data Storage

Numerous service offerings exist that provide hosted storage solutions. This section describes the various offerings and details the monitoring for each type of service and how encryption may impact the operational and security monitoring performed.
Trends in data storage encryption for hosted environments include a range of options. The following list is intentionally high-level to describe the types of encryption used in coordination with data storage that may be hosted remotely, meaning the storage is physically located in an external data center requiring transport over the Internet. Options for monitoring will vary with both approaches from what may be done today.

3.3.1. Host-level Encryption

For higher security and/or privacy of data and applications, options that provide end-to-end encryption of the data from the users desktop or server to the storage platform may be preferred. With this description, host level encryption includes any solution that encrypts data at the object level, not transport. Encryption of data may be performed with libraries on the system or at the application level, which includes file encryption services via a file manager. Host-level encryption is useful when data storage is hosted or when in scenarios when storage location is determined based on capacity or based on a set of parameters to automate decisions. This could mean that large data sets accessed infrequently could be sent to an off-site storage platform at an external hosting service, data accessed frequently may be stored locally, or decision could be based on the transaction type. Host-level encryption is grouped separately for the purpose of this document as the monitoring needs as this data is bursted to off-site storage platforms, where traffic crosses the Internet are similar. If session encryption is used, the protocol is likely to be TLS.

3.3.1.1. Monitoring for Hosted Storage

The general monitoring needs of hosted storage solutions that use host-level (object) encryption is described in this subsection. Solutions might include backup services and external storage services, such as those that burst data that exceeds internal limits on occasion to external storage platforms operated by a third party.

Monitoring of data flows to hosted storage solutions is performed for security and operational purposes. The security monitoring may be to detect anomalies in the data flows that could include changes to destination, the amount of data transferred, or alterations in the size and frequency of flows. Operational considerations include capacity and availability monitoring.

[What is monitored in the flows? What data is monitored when the sessions are encrypted vs. when session encryption is not in use? Note that object encryption may not be used in all cases.]
3.3.1.1.1. Backup Storage

[This is a placeholder in case there are distinct monitoring needs for any of the options that fall into this category. Backup Storage is listed as an example, but will be removed if there are no monitoring needs that needs to be discussed at a more granular level than the general description.]

3.3.2. Disk Encryption, Data at Rest

There are multiple ways to achieve full disk encryption for stored data. Encryption may be performed on data to be stored while in transit close to the storage media with solutions like Controller Based Encryption (CBE) or in the drive system with Self-Encrypting Drives (SED). Session encryption is typically coupled with encryption of these data at rest (DAR) solutions to also protect data in transit. Transport encryption is likely via TLS.

3.3.2.1. Monitoring Session Flows for DAR Solutions

The general monitoring needs for transport of data to storage platforms, where object level encryption is performed close to or on the storage platform are similar to those described in the section on Monitoring for Hosted Storage. The primary difference for these solutions is the possible exposure of sensitive information, which could include privacy related data, financial information, or intellectual property if session encryption via TLS is not deployed. Session encryption is typically used with these solutions, but that decision would be based on a risk assessment. There are use cases where DAR or disk-level encryption is required. Examples include preventing exposure of data if physical disks are stolen or lost as data is decrypted upon access when that access is from the expected and configured application or service.

[What is monitored in the flows? What data is monitored when the sessions are encrypted vs. when session encryption is not in use? There is obvious exposure of data when session encryption is not in use and session monitoring is not necessarily limited to the 5-tuple. Contributions welcome from those that have knowledge of what is actually used in monitoring of these sessions.]

3.3.3. Cross Data Center Replication Services

Storage services also include data replication which may occur between data centers and may leverage Internet connections to tunnel traffic. The traffic may use iSCSI [RFC7143] or FC/IP [RFC7146] encapsulated in IPsec. Either transport or tunnel mode may be used for IPsec depending upon the termination points of the IPsec session,
if it is from the storage platform itself or from a gateway device at the edge of the data center respectively.

3.3.3.1 Monitoring Of IPSec for Data Replication Services

The general monitoring needs for data replication are described in this subsection.

Monitoring of data flows between data centers may be performed for security and operational purposes and would typically concentrate more on the operational needs since these flows are essentially virtual private networks (VPN) between data centers. Operational considerations include capacity and availability monitoring [Contributions to expand this description and the more detailed data used for analysis below is welcome.]. The security monitoring may be to detect anomalies in the data flows, similar to what was described in the "Monitoring for Hosted Storage Section".

[What is monitored in the flows? What data is monitored when the sessions are encrypted vs. when session encryption is not in use? Note that object encryption may not be used in all cases.]

4. Encryption for Enterprise Users

This section is limited to the use of encryption by enterprise users to the Internet and not that of internal enterprise networks. To date, there is not yet demand to encrypt internal networks, with the exception of sensitive data and applications and those that require encryption through regulatory requirements.

4.1. Monitoring Needs of the Enterprise

Enterprise users are subject to the policies of their organization. As such, proxies may be in use to:

1. intercept outbound session traffic to monitor for intellectual property leakage (by users or more likely these days through malware and trojans),

2. detect viruses/malware entering the network via email or web traffic,

3. detect malware/Trojans in action, possibly connecting to remote hosts,
4. detect attacks (Cross site scripting and other common web related attacks),

5. track misuse and abuse by employees,

6. restrict the types of protocols permitted to/from the corporate environment,

7. assess traffic volume on a per-application basis, for billing, capacity planning, optimization of geographical location for servers or proxies, and other needs,

8. assess performance in terms of application response time and user perceived response time, and

9. re-direct to requests to caches of popular or bandwidth-intensive Internet content.

For each type of monitoring, different techniques and parts of the data stream may be necessary. As we transition to an increased use of encryption that is increasingly harder to break, alternate methods of monitoring for operational purposes will be necessary to prevent the need to break encryption and thus privacy of users (which may not apply in a corporate setting by policy).

4.2. Techniques for Monitoring Internet Session Traffic

Corporate networks commonly monitor outbound session traffic to detect or prevent attacks as well as to guarantee service level expectations. In some cases, alternate options are available when encryption is in use, but techniques like that of data leakage prevention tools at a proxy would not be possible if encrypted traffic can not be intercepted, thus requiring alternate options to emerge.

Data leakage detection prevention (DLP) tools intercept traffic at the Internet gateway or proxy services with the ability to man-in-the-middle (MiTM) encrypted session traffic (HTTP/TLS). These tools may use key words important to the enterprise including business sensitive information such as trade secrets, financial data, personally identifiable information (PII), or personal health information (PHI). Various techniques are used to intercept HTTP/TLS sessions for DLP and other purposes, and are described in "Summarizing Known Attacks on TLS and DTLS" [I-D.ietf-uta-tls-attacks]. Note: many corporate policies allow access to personal financial and other sites for users without interception.
Monitoring traffic patterns for anomalous behavior such as increased flows of traffic that could be bursty at odd times or flows to unusual destinations (small or large amounts of traffic). This traffic may or may not be encrypted and various methods of encryption or just obfuscation may be used.

Restrictions on traffic to approved sites: Web proxies are sometimes used to filter traffic, allowing only access to well-known sites known to be legitimate and free of malware on last check by a proxy service company. This type of restriction is usually not noticeable in a corporate setting, but may be to those in research who could access colleagues individual sites or new web sites that have not yet been screened. In situations where new sites are required for access, they can typically be added after notification by the user or proxy log alerts and review. Home mail account access may be blocked in corporate settings to prevent another vector for malware to enter as well as for intellectual property to leak out of the network. This method remains functional with increased use of encryption and may be more effective at preventing malware from entering the network. Web proxy solutions monitor and potentially restrict access based on the destination URL or the DNS name. A complete URL may be used in cases where access restrictions vary for content on a particular site or for the sites hosted on a particular server.

Desktop DLP tools are used in some corporate environments as well. Since these tools reside on the desktop, they can intercept traffic before it is encrypted and may provide a continued method of monitoring intellectual property leakage from the desktop to the Internet or attached devices.

DLP tools can also be deployed by Network Service providers, as they have the unique and efficient vantage point of monitoring all traffic paired with destinations off the enterprise network. This makes an effective solution for enterprises that allow "bring-you-own" devices and devices that do not fit the desktop category, but are used on corporate networks nonetheless.

Enterprises may wish to reduce the traffic on their Internet access facilities by monitoring requests for within-policy content and caching it. In this case, repeated requests for Internet content spawned by URLs in e-mail trade newsletters or other sources can be served within the enterprise network. Gradual deployment of end to end encryption would tend to reduce the cacheable content over time, owing to concealment of critical headers and payloads. Many forms of enterprise performance management and optimization based on monitoring (DPI) would suffer the same fate.
5. Encryption for Home Users

[Text]

6. Security Monitoring for Specific Attack Types

Effective incident response today requires collaboration at Internet scale. This section will only focus on efforts of collaboration at Internet scale that are dedicated to specific attack types. They may require new monitoring and detection techniques in an increasingly encrypted Internet. As mentioned previously, some service providers have been interfering with STARTTLS to prevent session encryption to be able to perform functions they are used to (injecting ads, monitoring, etc.). By detailing the current monitoring methods used for attack detection and response, this information can be used to devise new monitoring methods that will be effective in the changed Internet via collaboration and innovation.

6.1. Mail Abuse and SPAM

The largest operational effort to prevent mail abuse is through the Messaging, Malware, Mobile Anti-Abuse Working Group (M3AAWG). Mail abuse is combated directly with mail administrators who can shut down or stop continued mail abuse originating from large scale providers that participate in using the Abuse Reporting Format (ARF) agents standardized in the IETF [RFC5965], [RFC6430], [RFC6590], [RFC6591], [RFC6650], [RFC6651], and [RFC6652]. The ARF agent directly reports abuse messages to the appropriate service provider who can take action to stop or mitigate the abuse. Since this technique uses the actual message, the use of TLS over SMTP between mail gateways will not effect its usefulness. As mentioned previously, TLS over SMTP only protects data while in transit and the messages may be exposed on mail servers or mail gateways if a user-to-user encryption method is not used. Current user-to-user message encryption methods on email (S/MIME and PGP) do not encrypt the email header information used by ARF and the service provider operators in their abuse mitigation efforts.

6.2. Denial of Service

Response to Denial of Service (DoS) attacks are typically coordinated by the SP community with a few key vendors who have tools to assist in the mitigation efforts. Traffic patterns are determined from each DoS attack to stop or rate limit the traffic flows with patterns unique to that DoS attack.
Data types used in monitoring traffic for DDoS are described in Open Threat Signaling using RPC API over HTTPS and IPFIX (DDoSMitigation: [I-D.teague-open-threat-signaling]).

Data types used in DDoS attacks have been detailed in the IODEF Guidance draft [I-D.ietf-mile-iodef-guidance], Appendix A.2, with the help of several members of the service provider community. The examples provided are intended to help identify the useful data in detecting and mitigating these attacks independent of the transport and protocol descriptions in the drafts. [We don’t care about a format battle for the purpose of this draft, just what is useful for monitoring.]

[several experts in this area participate in the IETF. It would be good to get an up-to-date picture of this and what information is typically helpful in those flows.]

[If sessions are encrypted, how does that affect the ability of SPs and vendors to mitigate or stop the DoS? ACM: a short description of the effect appears in section 2]

6.3. Phishing

Investigations and response to phishing attacks follow well-known patterns, requiring access to specific fields in email headers as well as content from the body of the message. When reporting phishing attacks, the recipient has access to each field as well as the body to make content reporting possible, even when end-to-end encryption is used. The email header information is useful to identify the mail servers and accounts used to generate or relay the attack messages in order to take the appropriate actions. The content of the message often contains an embedded attack that may be in an infected file or may be a link that results in the download of malware to the users system.

Administrators often find it helpful to use header information to track down similar message in their mail queue or users inboxes to prevent further infection. Combinations of To:, From:, Subject:, Received: from header information might be used for this purpose. Administrators may also search for document attachments of the same name, size, or containing a file with a matching hash to a known phishing attack. Administrators might also add URLs contained in messages to block lists locally or this may also be done by browser vendors through larger scales efforts like that of the Anti-Phishing Working Group (APWG).

A full list of the fields used in phishing attack incident response can be found in RFC5901. Future plans to increase privacy
protections may limit some of these capabilities if some email header fields are encrypted, such as To:, From:, and Subject: header fields. This does not mean that those fields should not be encrypted, only that we should be aware of how they are currently used. Alternate options to detect and prevent phishing attacks may be needed. More recent examples of data exchanged in spear phishing attacks has been detailed in the IODEF Guidance draft [I-D.ietf-mile-iodef-guidance], Appendix A.3.

6.4. Botnets

Botnet detection and mitigation is complex and may involve hundreds or thousands of hosts with numerous Command and Control (C&C) servers. The techniques and data used to monitor and detect each may vary. Connections to C&C servers are typically encrypted, therefore a move to an increasingly encrypted Internet may not affect the detection and sharing methods used.

[Contributions welcome to detail data used in Botnet detection and how that may change in an increasingly encrypted Internet.]

6.5. eCrime

[Contributions welcome to better understand data used in tracking eCrime and how that may change in an increasingly encrypted Internet.]

6.6. Malware

Malware monitoring and detection techniques vary. As mentioned in the enterprise section, malware monitoring may occur at gateways to the organization analyzing email and web traffic. These services can also be provided by service providers, changing the scale and location of this type of monitoring. Additionally, incident responders may identify attributes unique to types of malware to help track down instances by their communication patterns on the Internet or by alterations to hosts and servers.

[Contributions welcome to expand this (or any other) section.] Data types used in malware investigations have been summarized in an example of the IODEF Guidance draft [I-D.ietf-mile-iodef-guidance], Appendix A.1.

6.7. Blocklists
6.8. [Any other subsections to be contributed?]

Although incident response work will continue, new methods to prevent system compromise through security automation and continuous monitoring [SACM] may provide alternate approaches where system security is maintained as a preventative measure.

7. Response to Increased Encryption and Looking Forward

As the use of encryption continues to increase, efforts to prevent it will continue to emerge. In the best case scenario, engineers and other innovators would work to solve the problems at hand in new ways rather than prevent the use of encryption. It will take time to devise alternate approaches to achieve similar goals.

There has already been documented cases of service providers preventing STARTTLS [NoEncrypt] to prevent session encryption negotiation on some session to inject a super cookie. There are other service providers who have been injecting Java Script into sessions [Net-Neutral], which has obvious security implications as well as threatens Net-Neutrality. The use of session encryption will help to prevent possible discrimination to maintain net neutrality, but a backlash should be expected.

National surveillance programs have a clear need for monitoring terrorism [CharlieHebdo] as do Internet security practitioners for cyber criminal activities. The UK prime minister, David Cameron, emphasized the need for monitoring [UKMonitor] at the expense of user privacy and protection of data and assets. This approach ignores the real need to protect users identity, financial transactions and intellectual property, which requires security and encryption to prevent cyber crime. A clear understanding of technology, encryption, and monitoring needs will aid in the development of solutions to appropriately balance the need of privacy and avoid the fears of terrorism. As this understanding increases, hopefully the discussions will improve and this draft is meant to help further the discussion.

Terrorists and cyber criminals have been using encryption for many years. The current push to increase encryption is aimed at increasing users privacy. There is already protection in place for purchases, financial transactions, systems management infrastructure, and intellectual property although this too can be improved. The Opportunistic Security (OS) [RFC7435] efforts aim to increase the costs of monitoring through the use of encryption that can be subject to active attacks, but make passive monitoring broadly cost prohibitive. This is meant to restrict monitoring to sessions where there is reason to have suspicion.
As the use of encryption increases, does passive monitoring become limited to metadata analysis? What metadata should be left in protocols as they evolve to also protect users privacy? Can we make changes to protocols and message exchanges to alter the current monitoring needs at least for operations and security practitioners?

Options are on the technology horizon that will help to end the struggle between the need to monitor by operators, security teams, and nations and those seeking to protect users privacy. The solutions are very interesting, but are several years out and include homomorphic encrypt, functional encryption, and filterable decryption [homomorphic]. This technology will allow for searching and pattern matching on encrypted data, but is still several years out.

8. Operational Monitoring

9. Security Considerations

There are no additional security considerations as this is a summary and does not include a new protocol or functionality.

10. IANA Considerations

This memo makes no requests of IANA.

11. Acknowledgements

Thanks to our early reviewers, Ashutosh Dutta and Brandon Williams, for their editorial and content suggestions.

12. References

12.1. Normative References


12.2. Informative References

[CAIDA] "CAIDA [http://www.caida.org/data/overview/]."

Europe Considers Surveillance Expansion After Deadly Attacks [CharlieHebdo]
https://firstlook.org/theintercept/2015/01/20/europe-considers-surveillance-expansion/.

Electronic Frontier Foundation [EFF]
https://www.eff.org/.

Telecommunications security; Lawful Interception (LI); Requirements of Law Enforcement Agencies, August 2001 [ETSI101331]
ETSI TS 101 331 V1.1.1 (2001-08).

Securing the Cloud [homomorphic]

IODEF Usage Guidance [I-D.ietf-mile-iodef-guidance]
Kampanakis, P., draft-ietf-mile-iodef-guidance-03 (work in progress), May 2014.

Summarizing Known Attacks on TLS and DTLS [I-D.ietf-uta-tls-attacks]

Recommendations for Secure Use of TLS and DTLS [I-D.ietf-uta-tls-bcp]

Open Threat Signaling using RPC API over HTTPS and IPFIX [I-D.teague-open-threat-signaling]

Messaging, Malware, Mobile Anti-Abuse Working Group [M3AAWG]
https://www.maawg.org/.

Comcast Wifi serving self-promotional ads via JavaScript injection [Net-Neutral]

ISPs Removing their Customers EMail Encryption [NoEncrypt]
"Panopticlick [https://panopticlick.eff.org/]".


Li, K. and B. Leiba, "Email Feedback Report Type Value: not-spam", RFC 6430, November 2011.


Falk, J. and M. Kucherawy, "Redaction of Potentially Sensitive Data from Mail Abuse Reports", RFC 6590, April 2012.


Falk, J. and M. Kucherawy, "Creation and Use of Email Feedback Reports: An Applicability Statement for the Abuse Reporting Format (ARF)", RFC 6650, June 2012.

Kucherawy, M., "Extensions to DomainKeys Identified Mail (DKIM) for Failure Reporting", RFC 6651, June 2012.


[TOR] "TOR ...".

[UKMonitor] "Cameron wants to ban encryption
http://www.theguardian.com/commentisfree/2015/jan/13/cameron-ban-encryption-digital-britain-online-shopping-banking-messaging-terror".

Authors’ Addresses

Kathleen Moriarty
EMC Corporation
176 South St
Hopkinton, MA
USA

Phone: +1
Email: Kathleen.Moriarty@emc.com

Al Morton
AT&T Labs
200 Laurel Avenue South
Middletown,, NJ  07748
USA

Phone: +1 732 420 1571
Fax:  +1 732 368 1192
Email: acmorton@att.com
URI:  http://home.comcast.net/~acmacm/