Transforming Information Security

Optimizing Five Concurrent Trends to Reduce Resource Drain

Kathleen M. Moriarty

TRANSFORMING INFORMATION SECURITY

This page intentionally left blank

TRANSFORMING INFORMATION SECURITY

Optimizing Five Concurrent Data Trends to Reduce Resource Drain

KATHLEEN M. MORIARTY
Dell Technologies, USA

United Kingdom – North America – Japan – India
Malaysia – China

Emerald Publishing Limited
Howard House, Wagon Lane, Bingley BD16 1WA, UK

First edition 2020

British Library Cataloguing in Publication Data
A catalogue record for this book is available from the British Library

ISBN: 978-1-83909-931-1 (Print)
ISBN: 978-1-83909-928-1 (Online)
ISBN: 978-1-83909-930-4 (Epub)

ISOQAR certified Management System, awarded to Emerald for adherence to Environmental standard ISO 14001:2004.

Certificate Number 1985
ISO 14001

INVESTOR IN PEOPLE

CONTENTS

This page intentionally left blank

PREFACE

Looking 5 to 10 years forward, to an ecosystem with end-to-end encryption, network architectures and hence security as we know it in enterprises will be transformed. The protocols for end-to-end encryption have been developed, but the management of security and networks have not caught up.

This is an opportunity to think strategically on the design of network architectures, the placement and use of management tools, and to plan for resources, especially the hard-to-find security practitioner.

Let's face it, information security is much more difficult than it needs to be, and this transformational period for protocols should be seen as an opportunity to fix these issues. The focus on this forward-looking strategic view is primarily considering the tremendous deficit in information security professionals will never be filled through training. The current set of security solution architectures involving middleboxes are geared toward the top 1% of organizations that can afford to hire multiple information security professionals. The other aspect of this strategic vision includes the goal of a truly improved and intrinsically more secure network environment. Envision a fully encrypted and authenticated network with functions better performed at scale where collective knowledge is strategically and carefully applied. As it has come to be an acceptable outcome in the Internet of Things (IoT) space,

envision elemental services from end point vendors to prevent, detect, and thwart threat actors leveraging collective knowledge on patterns and behaviors through the use of artificial intelligence and machine learning applied back to your systems to better scale incident detection and response.

This means no middleboxes that each require a full-time employee to manage. A reliance on information collected at the edge, or end point systems, as well as streams provided to these systems to prevent or block known threats would be managed by a smaller group of expert analysts with large swaths of data to make assessments. Vendors could provide services to prevent and resolve security issues on their applications and platforms in aggregate utilizing a small number of analysts specific to their technologies and threat landscapes. This already happens in hosted environments, but perhaps not in the ways this long-term vision moves us toward to further reduce human resource impacts. Gradually, this would all give way to intrinsically secure applications and the ability for users to better manage their personal data. Let's start with a few relevant examples that scale security and incident management well, and then the book will expand from there more broadly setting new architectural patterns that scale.

The APWG [APWG] hosts central repositories around use case-specific threats. This example is on the antiphishing repository. Anyone can contribute to this antiphishing repository containing attack-related information including web service links (URLs) with known malware, compromised email servers, etc. The information is used, verified, and updated by participating organizations, like RSA who engages law enforcement to take appropriate legal action and have malicious sites removed from the Internet. Where this gets interesting in terms of scale is the use of the information sources by programs like Google Safe Browsing [Google, 2019]. This particular program assesses threats and integrates

deny lists into the browser that are updated on a periodic basis throughout the day. Additionally, this is used as a plugin for every other major browser, greatly reducing the number of analysts needed to have a large impact on threats for just about every browser user on the planet, as an individual or within a corporate network benefiting.

Turning to the payment processing industry, threat detection occurs at the issuing bank, which is part of the payment processing flow that begins with the point of sale at millions of retail locations as well as online commerce sites. In this case, transactions are stopped at the point of sale or prior to the transaction being completed. In terms of scale and location of intelligence, this makes sense except for smaller issuing banks that may not have the fraud detection capabilities of larger organizations. The issuing bank has full records of card users' trends and patterns and can detect unusual behavior. The point of sale is able to verify whether or not your credit card is valid and has adequate funds to proceed with a transaction.

If you peel back this example a bit, there are providers of data that aid in fraud detection to further narrow the number of experts needed to detect threats. Fraud information services provide lists of compromised accounts and credit cards to the appropriate issuing bank, culled from the dark web. This compliments the work performed by issuing banks to detect fraud. Financial institutions also collaborate on threat detection, but not necessarily fraud detection techniques. There is room for improvement in each of these examples; however, they demonstrate collaboration between enterprises and vendors to protect enterprise users and individuals with fewer overall human resources. For some types of threats, solutions still do not scale and near-term work could help to reduce the number of analysts needed with architectural model changes with an eye toward efficiency given today's resource constraints. Longer term, methods will emerge to prevent the

attacks and thus reducing the need for defenses like these. Threat detection is just one area this book examines as it unfolds to map out security architectures to improve security and reduce human resource requirements for organizations of all sizes. It is imperative that we think toward new architectural patterns including ways to prevent such attacks now as protocol design changes and technology advancements enable this transformation.

ACKNOWLEDGMENTS

The research for this book began during Kathleen's two terms as an Internet Engineering Task Force (IETF) Security Area Director, March 2014–2018, reading all Internet drafts prior to publication. The text was independently produced while working in the Dell EMC and DELL Technologies Office of the CTO with permission. Proof of Concept and development to test hypothesis were performed by several of the DellEMC Office of the CTO Dojo teams and one by the USC supported by the DoD through the Hacking for Defense Program.

A tremendous thank you to Chris Inacio; his careful proofread of the contents looking to catch technical errors or areas that could benefit from further explanation. Special thanks to technical reviewers Spencer Dawkins and Rick Martinez who also aided in improving the book. Thank you to Nicole Reineke for your proofread and suggestions. Thank you to John Roese, Ken Durazzo, Frederic Lemieux, and Rowland Shaw for supporting my work and development of this book on security transformation. Gratitude also for those who helped validate the theories and projected evolution path including Rob Adams, Dennis Moreau, and Liam Quinn.

A tremendous thank you to the fabulous Dojo teams and business unit architects at Dell Technologies. I am forever grateful for the opportunity to work with each team member in collaborating and testing out some theories in proof of

concept development work. Dojo team members who implemented and developed additional ideas around proposals include Omar AbdulAal, Himanshu Arora, Shary Beshara, Gus Cantieni, Xuebin He, Akshaya Khare, James King, Omar Mahmoud, Lauren Marino, Amy Mullins, Megan Murawski, Thinh Nguyen, Xavier Nieves, Ahmed Osama, Alex Robbins, Seth Rothschild, Ben Santaus, Amy Seibel, Mohamed Shaaban, and Yuzhi Xiao. Thank you to security colleagues for your collaboration on several projects themed around scaling security management and helping to push the envelope with the goal of improving overall security for customers. Colleagues include Sachit Bakshi, Rudy Bauer, Travis Gilbert, Nicholas Grobelny, Samant Kakarla, Rick Martinez, Amy Nelson, Michael Raineri, and Charles Robison. Thank you to numerous colleagues in the IETF for your work and meaningful conversations to advance security.

Thank you to my dear son, who is an all-around wonderful child. I am grateful for all the mornings you slept late, giving me time to work on this book.

1

INTERCONNECTED TRENDS

There are at least five trends, when interconnected, that have the potential to result in a dramatic shift in how information security is managed today, for the better. Within each trend, there are some inevitable outcomes as well as interdependencies with other trends that are not often considered together to better map out a forward path. The trends include:

- increased deployment of encryption,
- strong session encryption, preventing interception,
- transport protocol stack evolution,
- data-centric security models, and
- users control of data.

While much work is happening within each trend, these trends are not typically all considered together. To realize positive change and reduce the overall threat space, it is imperative that we do just that. This chapter will explore each of the trends and how they interconnect to set the stage for

the proposed changes and deeper technical considerations discussed in the book as the trends are embraced. The increased deployment of strong encryption supports data-centric architectures and is contributing to the transport protocol stack evolution. User control of data is a desired outcome for those looking to protect user's privacy; however, work to support this trend is at an early stage. The general theme of the inability to manage information security as it is architected today, due to insufficient resources, will be explained detailing how embracing these trends and new architectural patterns improve efficiency and reduce resource requirements.

1.1 INCREASED DEPLOYMENT OF ENCRYPTION

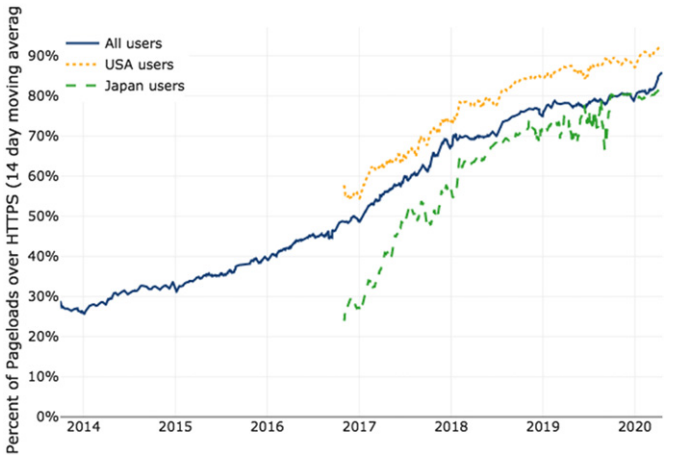
While the Snowden revelations (Gidda, 2013) starting in June 2013 led to an immediate increase in deployed session encryption, trends in standards development also shifted. The fundamental shift in standards was driven by the acceptance of less-than-perfect security in favor of deployability, leading to a sharper increase in deployed encryption starting around 2017. Examples of this include Opportunistic Security (Dukhovni, 2014) and the Internet Engineering Task Force (IETF) Automated Certificate Management Environment (ACME) (Internet Engineering Task Force, 2020h). Opportunistic security enables an upgrade path from clear text sessions to sessions encrypted without authentication, to authenticated session encryption. It is important to note that opportunistic security is breakable, but allows for easy automated configuration without knowledge of the other endpoint. Prior to this shift, such efforts would not have gone anywhere since the unauthenticated session could be

intercepted, leaving you with no security. From a purist point of view, that was not acceptable in the past, but now there's a justification. Opportunistic security raises the cost for pervasive monitoring, resulting in an in-feasibility to monitor all sessions passively. If nation states or malicious actors want to monitor traffic in this model, specific sessions would be targeted for decryption and observation.

While we haven't seen much deployment outside of opportunistic security use with IPsec (Internet Engineering Task Force, 2020d), automated certificate management is enjoying huge success via the Let's Encrypt project. Sessions not previously encrypted have used ACME via Let's Encrypt to automate the management of certificates, improving privacy protections for end users. While Let's Encrypt offers certificates for free, the ACME protocol can be used by other certificate providers who are interested in automating maintenance of certificates, including any type of certificate. An out-of-band process may be required for identity proofing of individuals and organizations for Extended Validation (EV) certificates or other certificate types. If you are not already using ACME, it should be considered a way to ease certificate management and say goodbye to the days where an expiring certificate causes extensive server outages without anyone realizing the root cause. Now, with automation needless downtime due to certificate management problems can be avoided.

The initial increase of deployed encryption on the web rose to around 30% in 2014, the year following Snowden revelations. ACME's automation and free certificates from the Let's Encrypt project helped that number climb to 85% in 2020 (Let's Encrypt, 2020) (Fig. 1.1).

This trend of pervasive encryption will continue now that session encryption is easier to deploy and there's ample motivation.



Source: https://letsencrypt.org/stats/

Fig. 1.1. Percentage of Page Loads Over HTTPS by Region.

1.2 STRONG ENCRYPTION

End user privacy, human rights protections, and prevention of protocol ossification are the primary drivers for the trend strengthening transport protocol encryption. Encryption is being designed to prevent interception and limit the exposure of previously exposed meta-data. When considering end user privacy, it's not only session content that can reveal sensitive information, but also meta-data. Meta-data and session signaling information may enable tracking of user sessions across the network with any identifier or combined set of unique data that can identify the communicating parties. The meta-data of the communication session may provide insight as to the two parties communicating (hostname and Internet protocol information), length of the session, amount of data exchanged, possibility of identifying encapsulated protocols, and types of data exchanged.

Privacy considerations for the end user have been a major driver for the increased deployment of strong encryption and

a reduction in availability of session meta-data. Transport architects and engineers are grappling with the go forward options to manage networks in an encrypted world. There has been some work to catalog the usage of data and meta-data and the goals of the monitoring performed prior to this shift in encryption (Moriarty & Morton, 2018). This impact is felt more by the enterprise than service providers as shown with a slower move toward adoption of strong encryption.

Transport layer protocols using provably secure strong encryption began to emerge in 2018. Deployment may have more limited success in environments where data is expected for monitoring (e.g., within the enterprise) near-term, the research from the cited survey indicates that deployment of these protocols should not suffer on Internet bound connections. The reason for this is that service provider monitoring is typically limited to the available protocol header information at the transport protocol, network, and link layer. These header fields will continue to be available with the current set of emerging transport encryption protocols including Transport Layer Security (TLS) version 1.3 (Rescorla, 2018), QUIC (Internet Engineering Task Force, 2020e), and TCPcrypt (Internet Engineering Task Force, 2020g).

A goal for an end-to-end encryption protocol is that the session initiates at the client application (web browser, streaming video application, etc.) and terminates at the server destination, thereby protecting the session across the entire transit of the network. In reality, the session likely terminates at a load balancer instead of a web server and may include some inspection at this point of termination. The load balancer termination point may be considered the server end point in today's web server architecture schemes. If there are additional servers, including application servers, content servers, databases, etc. used to deliver the return session content to the end user or client, there may be additional

encrypted streams established from the terminating load balancer to these other systems and applications. The subsequent sessions may or may not use the same encryption protocol as the initiating transport encryption protocol of the client. A simplified illustration is provided in Fig. 1.2.

Internet bound sessions have different security and privacy considerations from those within a data center, hence the possible variance on protocol selection for sessions within a data center from Internet bound sessions. For instance, human rights considerations in protocols (ten Oever & Cath, 2017) include many existing security and privacy controls, but add anonymity and pseudonymity as important to the design for end user protection. Users shouldn't have to fear for their safety when performing research on health-related or other similar queries that may be restricted or prohibited in some regions. When speaking on a panel in Geneva, organized by the Internet Society in 2015, another panelist told his story where he wanted to do research on the pros and cons of circumcision in his country in Africa, but was fearful for his life due to regional beliefs on this practice. This is just one of hundreds of examples where human rights considerations are sometimes factored into protocol design. The drivers are important as is the trend of increasing design and deployment of strong transport encryption. The threat landscape has evolved beyond basic confidentiality for information security

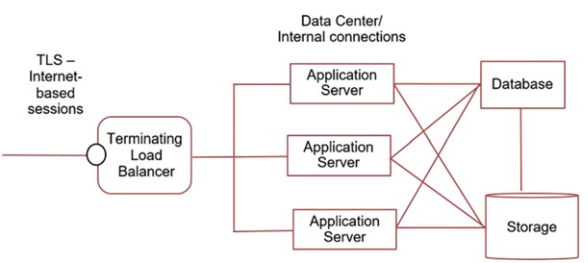


Fig. 1.2. Edge Termination to Data Center.

to include protection from session interception (passive or active hijacking), user privacy, and human rights considerations partly due to pervasive monitoring of governments.

1.3 TRANSPORT PROTOCOL STACK EVOLUTION

> *It seems to me that we're morphing into a really interesting protocol stack, where UDP is the transport protocol but QUIC is the REAL transport protocol, and IPv6 is the networking protocol, but GENEVE is the REAL networking protocol.*
>
> Spencer Dawkins, IETF Transport Area Director 2018.

The transport stack is evolving, partially a result of the need to develop and innovate Internet transport in response to the proliferation of middle-boxes that intercept and sometimes modify existing well-deployed protocols. End-to-end transport encryption helps toward this goal. Application developers are highly motivated in this push for strong encryption to allow for innovation in protocols supporting their applications. This is one reason why the protocol stack evolution starts from the application layer encryption protocols in addition to that being the point in the stack to protect end user data in transit. To be explicit, TLSv1.3 and QUIC are a couple of protocols driving the work of transport and routing engineers at lower layers for this now necessary protocol stack evolution.

The use of UDP and strong transport encryption is an attempt to address the ossification of existing network protocols and allow for innovative end-to-end protocol development.

> *TCP based applications are often intercepted and sometimes modified by middle-boxes. UDP has not been intercepted in general, having been deployed for connectionless query/response applications like DNS in the past,*
>
> Spencer Dawkins.

Performance benefits have been noted with applications using UDP and QUIC as a result. Through research, instances where UDP has been rate limited has been discovered as high usage may be interpreted by a middle-box as a DoS attack. Simply phrased, if traffic is not intercepted, the end points are free to evolve the protocol without fear that any update could cause the protocol to be blocked in its path. If the use of UDP is fully encrypted, including signaling information, packets cannot be modified in transit.

This all sounds very positive in that protocols may continue to evolve and protocol designers can be innovative in their solutions while protecting the privacy of end users. While those are both laudable goals, this leaves open questions for transport protocol engineers who focus on congestion control, performance, availability, and other traffic and operations management tasks that rely upon header information that has been available in transport protocols to date. Herein lies the tussle that has become a bit of an arms race between application developers who can evolve their protocols more easily if transport remains intact and the management of networks that has relied on visibility into packet streams to perform network and security management. For service providers, the visibility has been limited to publicly available transport, network, and link layer packet header data (Moriarty & Morton, 2018).