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

Preface *vii*

Acknowledgments *xi*

1. Interconnected Trends 1
2. Board-level Program Evaluation and Guidance 19
3. Architect a Secure Network with Less 53
4. Encryption 73
5. Transport Evolution: The Encrypted Stack 101
6. Authentication and Authorization 131
7. The End Point 145
8. Incident Prevention, Detection, and Response 173
9. Looking Forward 195

References *199*

Index *215*

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.