Building the Infrastructure for Cloud Security

A Solutions view

Raghu Yeluri
Enrique Castro-Leon

Apress
open

Building the Infrastructure for Cloud Security

Raghu Yeluri and Enrique Castro-Leon

ISBN-13 (pbk): 978-1-4302-6145-2

ISBN-13 (electronic): 978-1-4302-6146-9

President and Publisher: Paul Manning
Lead Editors: Steve Weiss (Apress); Patrick Hauke (Intel)
Coordinating Editor: Melissa Maldonado
Cover Designer: Anna Ishchenko

Distributed to the book trade worldwide by Springer Science+Business Media New York, 233 Spring Street, 6th Floor, New York, NY 10013. Phone 1-800-SPRINGER, fax (201) 348-4505, e-mail orders-ny@springer-sbm.com, or visit www.springeronline.com.

For information on translations, please e-mail rights@apress.com, or visit www.apress.com.

About ApressOpen

What Is ApressOpen?

- ApressOpen is an open access book program that publishes high-quality technical and business information.
- ApressOpen eBooks are available for global, free, noncommercial use.
- ApressOpen eBooks are available in PDF, ePub, and Mobi formats.
- The user friendly ApressOpen free eBook license is presented on the copyright page of this book.

To Sunita, Sonia, and Rajeev. Without your motivation, patience, and sacrifice, I couldn't have succeeded. Many thanks for maintaining and managing normalcy while I spent hours writing this book.

—Raghu Yeluri

To Kitty, for her infinite patience and both explicit and tacit support during the long hours it took to put together this book project.

—Enrique Castro-Leon

Contents at a Glance

About the Authors xv

About the Technical Reviewers xvii

Acknowledgments xix

Foreword xxi

Introduction xxiii

■ Chapter 1: Cloud Computing Basics 1

■ Chapter 2: The Trusted Cloud: Addressing Security and Compliance 19

■ Chapter 3: Platform Boot Integrity: Foundation for Trusted Compute Pools 37

■ Chapter 4: Attestation: Proving Trustability 65

■ Chapter 5: Boundary Control in the Cloud: Geo-Tagging and Asset Tagging 93

■ Chapter 6: Network Security in the Cloud 123

■ Chapter 7: Identity Management and Control for Clouds 141

■ Chapter 8: Trusted Virtual Machines: Ensuring the Integrity of Virtual Machines in the Cloud 161

■ Chapter 9: A Reference Design for Secure Cloud Bursting 179

Index 211

Contents

About the Authors xv

About the Technical Reviewers xvii

Acknowledgments xix

Foreword xxi

Introduction xxiii

Chapter 1: Cloud Computing Basics 1

Defining the Cloud 1

The Cloud's Essential Characteristics 2

The Cloud Service Models 3

The Cloud Deployment Models 4

The Cloud Value Proposition 5

Historical Context 6

Traditional Three-Tier Architecture 6

Software Evolution: From Stovepipes to Service Networks 7

The Cloud as the New Way of Doing IT 10

Security as a Service 12

New Enterprise Security Boundaries 12

A Roadmap for Security in the Cloud 16

Summary 17

Chapter 2: The Trusted Cloud: Addressing Security and Compliance 19

Security Considerations for the Cloud 19

Cloud Security, Trust, and Assurance 21

Trends Affecting Data Center Security 23

Security and Compliance Challenges 24

Trusted Clouds 26

Trusted Computing Infrastructure 27

Trusted Cloud Usage Models 28

The Boot Integrity Usage Model 30

The Trusted Virtual Machine Launch Usage Model 31

The Data Protection Usage Model 32

The Run-time Integrity and Attestation Usage Model 33

Trusted Cloud Value Proposition for Cloud Tenants 34

The Advantages of Cloud Services on a Trusted Computing Chain 35

Summary 36

Chapter 3: Platform Boot Integrity: Foundation for Trusted Compute Pools 37

The Building blocks for Trusted Clouds 37

Platform Boot Integrity 38

Roots of Trust–RTM, RTR, and RTS in the Intel TXT Platform 39

Measured Boot Process 40

Attestation 42

Trusted Compute Pools 43

TCP Principles of Operation 44

Pool Creation 46

Workload Placement 46

Workload Migration 46
Compliance Reporting for a Workload/Cloud Service 47
Solution Reference Architecture for the TCP 47
Hardware Layer 48
Operating System / Hypervisor Layer 49
Virtualization/Cloud Management and Verification/Attestation Layer 50
Security Management Layer 51
Reference Implementation: The Taiwan Stock Exchange Case Study 54
Solution Architecture for TWSE 55
Trusted Compute Pool Use Case Instantiation 56
Remote Attestation with HyTrust 57
Use Case Example: Creating Trusted Compute Pools and Workload Migration 59
Integrated and Extended Security and Platform Trust with McAfee ePO 60
Summary 64
Chapter 4: Attestation: Proving Trustability 65
Attestation 65
Integrity Measurement Architecture 67
Policy Reduced Integrity Measurement Architecture 67
Semantic Remote Attestation 68
The Attestation Process 68
Remote Attestation Protocol 68
Flow for Integrity Measurement 71
A First Commercial Attestation Implementation: The Intel Trust Attestation Platform 72
Mt. Wilson Platform 74
Mt. Wilson Architecture 76
The Mt. Wilson Attestation Process 78

Security of Mt. Wilson 81
Mt. Wilson Trust, Whitelisting, and Management APIs 83
Mt. Wilson APIs 84
The API Request Specification 85
API Response 86
Mt. Wilson API Usage 87
Deploying Mt. Wilson 87
Mt. Wilson Programming Examples 88
Summary 91

Chapter 5: Boundary Control in the Cloud: Geo-Tagging and Asset Tagging 93

Geolocation 94
Geo-fencing 94
Asset Tagging 96
Trusted Compute Pools Usage with Geo-Tagging 97
Stage 1: Platform Attestation and Safe Hypervisor Launch 99
Stage 2: Trust-Based Secure Migration 100
Stage 3: Trust- and Geolocation-Based Secure Migration 100
Adding Geo-Tagging to the Trusted Compute Pools Solution 100
Hardware Layer (Servers) 101
Hypervisor and Operating System Layer 102
Virtualization, Cloud Management, and the Verification and Attestation Layer 102
Security Management Layer 103
Provisioning and Lifecycle Management for Geo-Tags 103
Geo-Tag Workflow and Lifecycle 104
Tag Creation 104
Tag Whitelisting 105
Tag Provisioning 105

Validation and Invalidation of Asset Tags and Geo-Tags 107
Attestation of Geo-Tags 108
Architecture for Geo-Tag Provisioning 108
Tag Provisioning Service 109
Tag Provisioning Agent 110
Tag Management Service and Management Tool 110
Attestation Service 112
Geo-Tag Provisioning Process 113
Push Model 114
Pull Model 114
Reference Implementation 116
Step 1 117
Step 2 118
Step 3 119
Step 4 120
Summary 121
Chapter 6: Network Security in the Cloud 123
The Cloud Network 123
Network Security Components 124
Load Balancers 125
Intrusion Detection Devices 126
Application Delivery Controllers 126
End-to-End Security in a Cloud 126
Network security: End-to-End security: Firewalls 127
Network security: End-to-End security: VLANs 127
End-to-End Security for Site-to-Site VPNs 128
Network security:End-to-End security: Hypervisors and Virtual Machines 129

Software-Defined Security in the Cloud 131
OpenStack 135
OpenStack Network Security 136
Network Security Capabilities and Examples 137
Summary 139

Chapter 7: Identity Management and Control for Clouds 141

Identity Challenges 142
Identity Usages 143
Identity Modification 144
Identity Revocation 145
Identity Management System Requirements 145
Basic User Control Properties 146
Key Requirements for an Identity Management Solution 148
Accountability 148
Notification 148
Anonymity 148
Data Minimization 149
Attribute Security 149
Attribute Privacy 149
Identity Representations and Case Studies 150
PKI Certificates 150
Security and Privacy Discussion 151
Identity Federation 152
Single Sign-On 153
Intel Identity Technologies 153
Hardware Support 153
Summary 158

Chapter 8: Trusted Virtual Machines: Ensuring the Integrity of Virtual Machines in the Cloud 161

Requirements for Trusted Virtual Machines 162

Virtual Machine Images 164

The Open Virtualization Format (OVF) 166

A Conceptual Architecture for Trusted Virtual Machines 167

Mystery Hill (MH) Client 167

Mystery Hill Key Management and Policy Server (KMS) 168

Mystery Hill Plug-in 169

Trust Attestation Server 170

Workflows for Trusted Virtual Machines 171

Deploying Trusted Virtual Machines with OpenStack 173

Summary 177

Chapter 9: A Reference Design for Secure Cloud Bursting 179

Cloud Bursting Usage Models 180

An Explanation of Cloud Bursting 180

Data Center Deployment Models 183

Trusted Hybrid Clouds 184

Cloud Bursting Reference Architecture 186

Secure Environment Built Around Best Practices 187

Cloud Management 188

Cloud Identity and Access Management 188

Separation of Cloud Resources, Traffic, and Data 188

Vulnerability and Patch Management 188

Compliance 189

Network Topology and Considerations 191

Security Design Considerations 194
Hypervisor Hardening 194
Firewalls and Network separation 195
Management Network Firewalling 197
Virtual Networking 197
Anti-Virus Software 198
Cloud Management Security 198
Practical Considerations for Virtual Machine Migration 207
Summary 209

Index 211

About the Authors

Raghu Yeluri is a Principal Engineer and lead Security Solutions Architect in the Data Center & Cloud Products Group at Intel Corporation, with focus on virtualization and cloud security usages, solution architectures, and technology initiatives. In this role, he drives security solution pathfinding and development to deliver hardware-assisted security solutions that enable deep visibility, orchestration, and control in multi-tenant clouds. Prior to this role, he has worked in various engineering and architecture positions in systems development and deployment, focusing on service-oriented architectures and large data analytics, in information technology and manufacturing technology groups during the last 15+ years at Intel. Raghu has multiple patents filed in security, attestation, and control in virtualization and cloud computing, and he is a co-author of a book, *Creating the Infrastructure for Cloud Computing: An Essential Handbook for IT Professionals*. He holds an MS degree in Computer Science, and a B.S in Electrical Engineering, and was involved in multiple artificial intelligence/knowledge-engineering startup ventures prior to joining Intel.

Enrique Castro-Leon is an Enterprise Architect and Technology Strategist with the Intel Architecture Group at Intel Corporation, working in enterprise IT solution integration, cloud computing, and service engineering. As a technology strategist, Enrique has been investigating the disruptive effects of emerging technologies in the marketplace. He is the lead author of a book on the convergence of virtualization, service-oriented methodologies, and distributed computing, titled *The Business Value of Virtual Service Grids: Strategic Insights for Enterprise Decision Makers*. He is also the lead author of a second book, *Creating the Infrastructure for Cloud Computing: An Essential Handbook for IT Professionals*. Enrique holds a Ph.D. in Electrical Engineering and M.S. degrees in Electrical Engineering and Computer Science from Purdue University, and a BSEE degree from

the University of Costa Rica. Enrique is also a co-founder and President of Neighborhood Learning Center (NLC), a tax-exempt organization providing computer education and tutoring services to K-12 in Oregon. Since its inception in 2000, the NLC has served over 300 children at risk of falling behind in the school system, and currently serves over 60 families. It has received recent grant awards from the Meyer Memorial Trust, the Templeton Foundation, and the Rose E. Tucker Charitable Trust.

About the Technical Reviewers

Martin Guttmann is a Principal Engineer at Intel Corporation. He has 30+ years of extensive experience ranging from computer systems and software to operating systems, including the data center operation, security solutions, and enterprise architecture. As member of the office of the CTO at Intel, he was responsible for defining end-to-end manageability and security architecture for enterprise IT and data center infrastructure, systems, products, and solutions.

Uttam Shetty is Director of Cloud Security Solutions at Intel Corporation, leading the engineering groups delivering security solutions that provide platform-derived trust assurance of the cloud Infrastructure. He has extensive experience (25+ years) in leading global development centers in delivering technologies and solutions that enable key transformation with Intel for e-business, manufacturing systems, and infrastructure technology.

Mitch Koyama is a subject-matter expert on Intel's enterprise products, solutions, and technologies. Emergence of cloud computing keeps Mitch busy with Intel's security technologies, where he has been working with various technology suppliers and vendors to provide solutions addressing the barriers for cloud adoption. Mitch has been in this field for more than 10 years, working in multiple locations.

Ren Wu is a technology-integration engineer for security technologies in Intel Corporation's data center group. Ren has rich and varied experience both at Intel and at AT&T Bell Labs and Lucent Technologies as a systems and solution architect and has contributed to their optical network architectures, standards, and the long-haul DWDM systems.

Acknowledgments

This book is an embodiment of work by many different Intel Corporation communities of engineers, architects, technical and product marketing engineers, software architects, and researchers at Intel labs, as well as many external software and solution partners. The work could not have been created without the multi-year effort and development of Security Technologies by Intel's Data Center Group and Software and Services Group. Their technical whitepapers, industry engagements, and eco-system development work provided the impetus for the development of the solution architectures, solution components, and reference implementations discussed in this book. It is not feasible to name all the people involved, but here is a very likely nonexhaustive list of folks we would like to acknowledge: Monty Wiseman, Joe Cihula, Steve Orrin, James Blakley, James Greene, Iddo Kadim, Lynn Comp, Tracie Zenti, Hemma Prafullchandra, Vince Lubsey, Murugiah Souppaya, Michael Bartock and Nikhil Sharma. Special acknowledgement to the Intel Cloud Security team, including Ravi Varanasi, Uttam Shetty, Sudhir S. Bangalore, Jonathan Buhacoff, Kamal Natesan and Jerry Wheeler. This team has been at the forefront of the solution definition and development that are covered in this book.

The authors gratefully acknowledge the time, guidance, and expertise of the technical reviewers, Martin Guttmann, Uttam Shetty, Ren Wu, and Mitch Koyama.

Authors would like to offer special thanks to acknowledge a small set of contributors who provided particular content to these chapters:

- Chapter 1 – ***Blake Dournaee***.
- Chapter 4, 5 - ***Jonathan Buhacoff and Sudhir Bangalore***.
- Chapter 6 – ***William Bathurst, M2Mi, Inc***.
- Chapter 7 – ***Abhilasha Bhargav and Ned Smith***.
- Chapter 9 – ***Gregsie Leighton and Pete Nicoletti, VirtuStream, Inc***.

Foreword

I've worn a lot of hats in my career, from investment banker to venture capitalist to business entrepreneur. And I've been fortunate to have been at the forefront of a number of technology waves, from mainframe to client/server computing, the Internet boom, and now the continuing rise of mobile and cloud computing. Each new wave brings technology disruption driven by an industry in transformation, and each enables new levels of efficiency and operational productivity. However, in line with that, each new wave also brings new security risks and operational concerns.

Virtualization and cloud technologies are no different. They're bringing about the most significant data center transformation in the last 20 years, and are enabling enormous benefits in terms of cost savings, flexibility, and business agility. But at the same time, there's been a correspondingly significant shift in the security risk posture. The new platform that cloud environments create brings together all an organization's critical systems, applications, and data, which, in essence, leads to a concentration of risk. That on its own should get executives to stop, sit up, and take notice. Without the proper controls in place (as you can very well imagine) a data center–and thus business–disaster can ensue. Critical systems and data might be accessed, copied, and deleted in one fell swoop or at touch of a button. Servers that IT used to think of as physical boxes that can be racked and stacked are now simply sets of files. The data center is becoming a software abstraction that can entirely be managed remotely.

Further, in this new environment, godlike privileges are enabled over the entire set of virtualized resources. A single systems administrator—or someone hijacking someone's privileges to escalate an attack—can copy a virtual machine or delete an entire virtual data center in a matter of minutes. Misconfigurations can now cause serious downtime owing to the greater number of systems. And, audit failures are more likely to happen given that now the new platform is subject to audit.

And we aren't done yet. Technology is moving toward software-defined networks and storage to enable the "software-defined data center." This concentrates risk further and creates additional security and compliance challenges.

Such radical changes demand a new approach to security and chain of trust—one that addresses these risks *specifically*. It's more critical than ever, given these factors: (1) concentration of risk, as noted; (2) attackers becoming much more sophisticated; and (3) higher stakes, such as insider risk and data leaks, and advanced external threats and privilege hijacking and to escalate attacks. A few good examples include Edward Snowden's leak of classified NSA documents; the theft of hundreds of millions of Target customers' personal information; and the Adobe breach that compromised tens of millions of user accounts and payments information, not to mention top-secret source code.

The new chain of trust must start from the hardware as well as the virtual infrastructure, to ensure you can trust the operating systems and applications that are running on virtual machines. It needs to work across private, hybrid, and public clouds so that the policies required for workloads can be dictated and enforced automatically. And it must be tied to data security to ensure VMs are encrypted unless they're running in authorized environments.

Looking ahead, cloud security from hardware-to-data will be critical to enabling faster adoption of cloud services.

This book is a great read for those looking to build secure foundations for cloud environments. As seasoned experts in virtualization, enterprise architectures, and security technologies, Raghu and Enrique provide a pivotal discussion of cloud security issues, the challenges companies face as they move into the cloud, and the infrastructure solution components required to address the new security requirements and controls.

—Eric Chiu, President & Co-Founder, Hytrust, Inc.

Introduction

Security is an ever-present consideration for applications and data in the cloud. It is a concern for executives trying to come up with criteria for migrating an application, for marketing organizations in trying to position the company in a good light as enlightened technology adopters, for application architects attempting to build a safe foundation and operations staff making sure bad guys don't have a field day. It does not matter whether an application is a candidate for migration to the cloud or it already runs using cloud-based components. It does not even matter that an application has managed to run for years in the cloud without a major breach: an unblemished record does not entitle an organization to claim to be home free in matters of security; its executives are acutely aware that resting on their laurels regardless of an unblemished record is an invitation to disaster; and certainly past performance is no predictor for future gains.

Irrespective of whom you ask, security is arguably the biggest inhibitor for the broader adoption of cloud computing. Many organizations will need to apply best practices security standards that set a much higher bar than that for on-premise systems, in order to dislodge that incumbent on-premise alternative. The migration or adoption of cloud services then can provide an advantage, in that firms can design, from the ground up, their new cloud-based infrastructures with security "baked-in;" this is in contrast to the piecemeal and "after the fact" or "bolted-on" nature of security seen in most data centers today. But even a baked-in approach has its nuances, as we shall see in Chapter 1. Cloud service providers are hard at work building a secure infrastructure as the foundation for enabling multi-tenancy and providing the instrumentation, visibility, and control that organizations demand. They are beginning to treat security as an integration concern to be addressed as a service like performance, power consumption, and uptime. This provides a flexibility and granularity wherein solution architects design in as much security as their particular situation demands: security for a financial services industry (FSI) or an enterprise resource planning (ERP) application will be different from security for a bunch of product brochures, yet they both may use storage services from the same provider, which demands a high level of integrity, confidentiality, and protection.

Some practices—for instance, using resources in internal private clouds as opposed to public, third-party hosted clouds—while conferring some tactical advantages do not address fundamental security issues, such as perimeter walls made of virtual Swiss cheese where data can pass through anytime. We would like to propose a different approach: to anchor a security infrastructure in the silicon that runs the volume servers in almost every data center. However, end users running mobile applications don't see the servers. What we'll do is define a logical chain of trust rooted in hardware, in a manner not unlike a geometry system built out of a small set of axioms. We use the hardware to ensure the integrity of the firmware: BIOS code running in the chipset and firmware

taking care of the server's housekeeping functions. This provides a solid platform on which to run software: the hypervisor environment and operating systems. Each software component is "measured" initially and verified against a "known good" with the root of trust anchored in the hardware trust chain, thereby providing a trusted platform to launch applications.

We assume that readers are already familiar with cloud technology and are interested in a deeper exploration of security aspects. We'll cover some cloud technology principles, primarily with the purpose of establishing a vocabulary from which to build a discussion of security topics (offered here with no tutorial intent). Our goal is to discuss the principles of cloud security, the challenges companies face as they move into the cloud, and the infrastructure requirements to address security requirements. The content is intended for a technical audience and provides architectural, design, and code samples as needed to show how to provision and deploy trusted clouds. While documentation for low-level technology components such as trusted platform modules and the basics of secure boot is not difficult to find from vendor specifications, the contextual perspective—a usage-centric approach describing how the different components are integrated into trusted virtualized platforms—has been missing from the literature. This book is a first attempt at filling this gap through actual proof of concept implementations and a few initial commercial implementations. The implementation of secure platforms is an emerging and fast evolving issue. This is not a definitive treatment by a long measure, and trying to compile one at this early juncture would be unrealistic. Timeliness is a more pressing consideration, and the authors hope that this material will stimulate the curiosity of the reader and encourage the community to replicate the results, leading to new deployments and, in the process, advancing the state of the art.

There are three key trends impacting security in the enterprise and cloud data centers:

- *The evolution of IT architectures*. This is pertinent especially with the adoption of virtualization and now cloud computing. Multi-tenancy and consolidation are driving significant operational efficiencies, enabling multiple lines of business and tenants to share the infrastructure. This consolidation and co-tenancy provide a new dimension and attack vector. How do you ensure the same level of security and control in an infrastructure that is not owned and operated by you? Outsourcing, cross-business, and cross-supply chain collaboration are breaking through the perimeter of traditional security models. These new models are blurring the distinction between data "inside" an organization and that which exists "outside" of those boundaries. The data itself is the new perimeter.

- *The sophistication of attacks*. No longer are attacks targeted at software and no longer are the hackers intent on gaining bragging rights. Attacks are sophisticated and targeted toward gaining control of assets, and with staying hidden. These attacks have progressively moved closer to the lower layers of the platform: firmware, BIOS, and the hypervisor hosting the virtual machine operating environment. Traditionally, controls in these lower layers are few, allowing malware to hide. With multi-tenancy and consolidation through virtualization, taking control of a platform could provide significant leverage and a large attack surface. How does an organization get out of this quandary and institute controls to verify the integrity of the infrastructure on which their mission-critical applications can run? How do they prove to their auditors that the security controls and procedures in effect are still enforced even when their information systems are hosted at a cloud provider?
- *The growing legal and regulatory burden*. Compliance requirements have increased significatly for IT practitioners and line-of-business owners. The cost of securing data and the risks of unsecured personally identifiable data, intellectual property, or financial data, as well as the implications of noncompliance to regulations, are very high. Additionally, the number of regulations and mandates involved are putting additional burdens on IT organizations.

Clearly, cloud security is a broad area with cross-cutting concerns that involve technology, products, and solutions that span mobility, networks security, web security, messaging security, protection of data or content and storage, identity management, hypervisor and platform security, firewalls, and audit and compliance, among other concerns. Looking at security from a tools and products perspective is an interesting approach. However, an IT practitioner in an enterprise or a cloud service provider iscompelled to look at usages and needs at the infrastructure level, and to provide a set of cohesive solutions that address business security concerns and requirements. Equally intriguing is to look at the usages that a private cloud or a public cloud have so as to address the following needs:

- For service providers to deliver enterprise-grade solutions. What does this compliant cloud look like? What are its attributes and behaviors?
- For developers, service integrators, and operators to deliver protected applications and workloads from and in the cloud. Irrespective of the type of cloud service, how does a service developer protect the static and the dynamic workload contents and data?
- For service components and users alike to granularly manage, authenticate, and assign trust for both devices and users.

Intel has been hard at work with its partners and as fellow travelers in providing comprehensive solution architectures and a cohesive set of products to not only address these questions but also deploy e solutions in private clouds, public clouds at scale. This book brings together the contributions of various Intel technologists, architects, engineers, and marketing and solution development managers, as well as a few key architects from our partners.

The book has roughly four parts:

- Chapters 1 and 2 cover the context of cloud computing and the idea of security, introducing the concept of trusted clouds. They discuss the key usage models to enable and instantiate the trusted infrastructure, which is a foundational for those trusted clouds. Additionally, these chapters cover the use-models with solution architectures and component exposition.
- Chapters 3, 4, and 5 cover use-cases, solution architectures, and technology components for enabling the trusted infrastructure, with emphasis on trusted compute, the role of attestation, and attestation solutions, as well as geo-fencing and boundary control in the cloud.
- Chapters 6 and 7 provide an interesting view of identity management and control in the cloud, as well as network security in the cloud.
- Chapter 8 extends the notion of trust to the virtual machines and workloads, with reference architecture and components built on top of the trusted compute pools discussed in earlier chapters. Then, Chapter 9 provides a comprehensive exposition of secure cloud bursting reference architecture and a real-world implementation that brings together all the concepts and usages discussed in the preceeding chapters.

These chapters take us on a rewarding journey. Starting with a set of basic technology ingredients rooted in hardware, namely the ability to carry out the secure launch of programs; not just software programs, but also implemented in firmware in server platforms: the BIOS and the system firmware. We have also added other platform sensors and devices to the mix, such as TPMs, location sensors. Eventually it will be possible integrate information from other security related telemetry in the platform: encryption accelerators, secure random generators for keys, secure containers, compression accelerators, and other related entities.

With a hardened platform defined it now becomes possible to extend the scope of the initial set of security features to cloud environments. We extend the initial capability for boot integrity and protection to the next goal of data protection during its complete life cycle: data at rest, in motion and during execution. Our initial focus is on the server platform side. In practical terms we use an approach similar to building a mathematical system, starting with a small set of assertions or axioms and slowly extending the scope of the assertions until the scope becomes useful for cloud deployments. On the compute side we extend the notion of protected boot to hypervisors and operating

systems running on bare metal followed by the virtual machines running on top of the hypervisors. Given the intense need in the industry secure platforms, we hope this need will motivate application vendors and system integrators to extend this chain of trust all the way to application points of consumption.

The next abstraction beyond trust established by secure boot is to measure the level of trust for applications running in the platform. This leads to a discussion on attestation and frameworks and processes to accomplish attestation. Beyond that there are a number of practical functions needed in working deployments, including geo-location monitoring and control (geo-fencing), extending trust to workloads, the protected launch of workloads and ensuring run time integrity of workloads and data.

The cloud presents a much more dynamic environment than previous operating environments, including consolidated virtualized environments. For instance, virtual machines may get migrated for performance or business reasons, and within the framework of secure launch, it is imperative to provide security for these virtual machines and their data while they move and where they land. This leads to the notion of trusted compute pools.

Security aspects for networks comes next. One aspect left to be developed is the role of hardened network appliances taking advantage of secure launch to complement present safe practices. Identity management is an ever present challenge due to the distributed nature of the cloud, more so than its prior incarnation in grid computing because distribution, multi-tenancy and dynamic behaviors are carried out well beyond the practices of grid computing.

Along with the conceptual discussions we sprinkle in a number of case studies in the form of proofs of concept and even a few deployments by forward thinking service providers. For the architects integrating a broad range of technology components beyond those associated with the secure launch foundation these projects provides invaluable proofs of existence, an opportunity to identify technology and interface gaps and to provide very precise feedback to standards organizations. This will help accelerate the technology learning curve for the industry as a whole, enabling a rapid reduction in the cost and time to deploy specific implementations.

The compute side is only one aspect of cloud. We'll need to figure out how to extend this protection to the network and storage capabilities in the cloud. The experience of building a trust chain starting from a secure boot foundation helps: network and storage appliances also run on the same components used to build servers. We believe that if we follow the same rigorous approach used to build a compute trust chain, it should be possible to harden network and storage devices to the same degree we attained with the compute subsystem. From this perspective the long journey is beginning to look more than like a trailblazing path.

Some readers will shrewdly note that the IT infrastructure in data centers encompasses more than servers; it also includes networks and storage equipment. The security constructs discussed in this book relate mostly to application stacks running on server equipment, and they are still evolving. It must be noted that network and storage equipment also runs on computing equipment, and therefore one strategy for securing network and storage equipment will be precisely to build analogous trust chains applicable to the equipment. These topics are beyond the scope of this book but are certainly relevant to industry practitioners and therefore are excellent subjects for subject-matter experts to document in future papers and books.

The authors acknowledge the enormous amount of work still to be done, but by the same token, these are enormously exciting areas to explore, with the potential of delivering equally enormous value to a beleaguered security industry—an industry that has been rocked by a seemingly endless stream of ever-more sophisticated and brazen exploits. We invite industry participants in any role, whether executive, architecture, engineering, system integration, or development, to join us in broadening this path. Actually, the path to innovation will never end—this is the essence of security. However, along the way, industry participants will build a much more robust foundation to the cloud, bringing some well-deserved assurances to customers.