



SECURED BY DESIGN

Always A Target,

Never The Victim

Kevin M. Moore

Secured By Design

A collection and sharing of experiences and “Best Practices”
for building & Securing Information Technology Systems

First Edition



© Engineering Sciences & Technology, 2020

SECURED BY DESIGN

Dedications Page

In my career as a technology professional, I've had the opportunity to meet and work with people from the United States and from all around the world. I've made many friends in my travels, all with vastly different skill sets and approaches to solving problems.

I'd like to dedicate this writing to all those professionals who have inspired me to look at things through their perspectives and have learned so much from them along the way. What I have learned the most from these innovators is there are no limitations to solving many of the same challenges. Learning how my colleagues have used the same technologies to solve the same problems across the different organizations has kept my mind wide open towards the possibilities.

I would like to name many of my friends and their companies but cannot as I'm required to maintain their confidentiality. To all my professional contacts I say THANK YOU for what I learned from you because you've made me a better professional !!!!!

And to those Vendors who allowed me to use their software for the development of contact for this book, I say THANK YOU. It is my sincere hope that companies try and implement your companies software and engage your implementation teams. You folks made it possible to complete this publication.

Hands down, the most fulfilling part of my career working with people from all over the world was getting to know where they came from, their customs and traditions, and for that I am a better person. I've made many friends over my years in consulting and support and your friendship will be cherished, always !!!

About the Author

My career began in the Aerospace industry with the title of Software Engineer. Key tasks undertaken were systems administration, documentation preparation, device driver development, systems programming, embedded systems development, and application software development in multiple languages such as COBOL, Fortran (Formula Translation), Basic Assembler Language (BAL), Macro-11, Macro-32, VAX Macro, PL/1, BASIC, Pascal, ADA, C & C++.

Systems being used for the various projects were the Systems Engineering Labs (SEL) 3277, Digital PDP-11 Series (23, 34, 70, 84) Q-Bus and Unibus, Digital Equipment Corporation VAX 11/x series, Intel 8086/8274/8088, IDM database machine, IBM 360, and the IBM 4341. If you're lucky, you may be able to find these systems in a museum someplace as they were the foundation for modern computing. What I did not know at the time, and did not appreciate, was the exposure I had been given to what made computers function and at all their respective levels.

Around 1991 or so, my employer purchased a chemical analysis system that was hosted on an Intel 486 based system. The operating system was SCO Unix, and relational database was the Oracle database version 6.0.83. I had not had access to a UNIX operating system or the Oracle database on anything before this. The task of educating myself involved purchasing Linux Operating system Administration and Oracle DBA books. There was no web applications tier per se as the application was written in PRO*C and connected directly to the database. Since becoming fluent with the Oracle RDBMS, I've added MS SQL Server, PostgreSQL, MySQL, and IBM's DB2 to the list of RDBMS engines supportable.

Having been a system programmer on platforms that were losing adoption in the market, regardless of their technical prowess, it did not take much time to realize I had struck technology gold and that the decision to remain relevant was in my hands. This

was an easy decision, not one that involved a great bit of thought that database technology was the path forward. As it turned out, this decision was one of the best conscious decisions I've ever made.

System security was not much of a consideration at that time because network computing was not what it is today. I've since migrated to current technologies across the entire stack.

Hands down, the biggest change since I started has been the move from proprietary hardware and vendor specific UNIX operating system to "commodity" hardware with Linux as the operating system and Intel Xeon or AMD CPU's. Barring something substantial, this combination will be the platform of choice for the foreseeable future.

Next time you're on a commercial aircraft, keep an eye on the in-flight entertainment system. It is run using Linux. So for an "old hat" like me, things are much simpler as in less choices for building and deploying systems today.

Table of Contents

Preface / Why this book is being written.....	12
What we plan to accomplish and in what order.....	19
Security Begins at the data layer	21
1. Environment Configuration	22
Database Servers	24
SAN/Storage.....	25
Operating Systems	28
Network Infrastructure	33
Installed Software	36
Summary	58
2. Oracle Database Server Preparation.....	59
3. Oracle Database Vault	140
Configuring Oracle Database Vault.....	153
Summary	192
4. Oracle Audit Vault & Database Firewall.....	193
Configuring Oracle Audit Vault	198
Installing OAV Agents and HOSTMON	207
Configuring Oracle Database Firewall.....	221
5. Monitoring Servers with Oracle Audit Vault.....	227
Operating System Monitoring.....	227
Monitoring Oracle.....	234
Monitoring MySQL.....	249
Monitoring IBM DB2	254

Monitoring SQL Server.....	257
Monitoring PostgreSQL.....	264
Summary	265
6. IBM Guardium.....	268
Summary	275
7. SQL Firewalls	276
Summary	277
8. Identity & Access Management.....	278
Summary	297
9. Application Security	299
Userid & Passwords	299
IP Whitelisting.....	303
Application Whitelisting.....	305
Blacklisting	307
Biometric Security.....	309
Active Directory/LDAP	311
Summary	314
10. Blockchain Technology.....	317
Summary	332
11. Forensic Collection & Data Use.....	333
Collected Data Storage & Reporting	334
Big Data	341
Data Collection Format(s)	344
Splunk.....	346
Advanced Threat Detection	346

Insider Threat.....	347
Incident Investigation, Forensics, and Response.....	348
SOC Automation.....	350
Compliance	355
Fraud Detection	357
Security Monitoring	358
Splunk Add-on Applications.....	359
Elasticsearch.....	416
Monitoring Logins and Failed Login Attempts	430
Monitoring Password File	431
Examining System Logfiles	433
CPU & Memory Analysis	439
Monitoring Network Traffic	446
Collecting Shell Histories.....	453
Gathering Filesystem Information	459
Amazon S3 Monitoring Tools.....	480
Summary	490
12. Email Servers.....	491
Email Phishing Attacks	496
MALWARE Scanning.....	510
Summary	520
13. Penetration Testing.....	521
Information Gathering	522
Vulnerability Analysis.....	539
Wireless Attacks.....	546

Web Applications	562
Exploitation Tools.....	571
Stress Testing	574
Forensics Tools.....	577
Sniffing & Spoofing.....	586
Password Attacks	593
Maintaining Access	604
Reverse Engineering.....	609
Hardware Hacking.....	614
Reporting Tools	616
Summary	619
14. Web Proxy Servers	624
Summary	631
15. VPN Appliance.....	632
Summary	642
16. Best Practices	643
Summary	649
17. Advanced Security Technology Adopters	651
Summary	654
18. Managing the System Retrofit	655
Application Software.....	657
Application Servers	693
Multi-Factor Authentication	695
HTTP Web Servers.....	700
Microsoft IIS	702

Apache	704
Nginx	706
Google	719
HTTP Server Attacks	719
Encryption Appliances.....	722
Oracle Database Encryption.....	725
Blockchain	728
IBM DB2 Database and file Encryption	729
IBM Multi-Cloud Data Encryption	735
HP-UX Data Security Offerings	738
Splunk Encryption	741
Elastic Encryption	744
MySQL Encryption.....	749
SQL Server Encryption.....	755
Sybase Encryption	771
SAP HANA Encryption	788
AWS Encryption	806
MariaDB Encryption	838
Teradata (FDE) Encryption	857
Apache Spark Encryption	864
Informix Encryption	871
Filesystem Encryption	883
Hardware Encryption Modules	927
Network Traffic Encryption	929
Summary	932

19. Performance Testing (Encrypted vs. Non-Encrypted).....	934
Performance Testing Expectations	952
Summary	955
20. Relational Databases.....	957
IBM DB2	959
Microsoft SQL Server	960
MySQL.....	961
Oracle.....	963
PostgreSQL.....	964
Database Migration	967
Reporting.....	969
High Availability	972
Database Replication	977
Summary	991
21. Migration Strategies.....	993
NoSQL Databases	1018
Containers.....	1035
Kubernetes (Google platform).....	1036
Docker	1044
Vendor Support.....	1051
Server Replication	1054
Summary	1057
Network Infrastructure	1058
Wireless Networks	1063
Wired Networks.....	1067

Operating Systems	1069
Hardware / Server	1072
Password Complexity	1078
Platform Change	1084
IPMI Vulnerability	1087
Virtualization	1091
Oracle Virtualization	1091
IBM Virtualization	1093
Hewlett Packard (HP) Virtualization	1094
Microsoft Server Virtualization	1096
Intel Virtualization Technology (Intel VT)	1099
AMD-V (Advanced Micro Devices Virtualization)	1101
X86 Virtualization Products	1103
Migration to the CLOUD	1105
Summary	1118
22. Vulnerability Assessment	1120
Summary	1122
23. Machine Learning	1123
Summary	1130
24. Orderly Shutdown	1131
Index	1135