Information Security Management Handbook

Sixth Edition

Edited by

Richard O'Hanley · James S. Tiller

Volume 7

CRC Press
Taylor & Francis Group
AN AUERBACH BOOK

Information Security Management Handbook

Sixth Edition

Volume 7

OTHER INFORMATION SECURITY BOOKS FROM AUERBACH

Asset Protection through Security Awareness
Tyler Justin Speed
ISBN 978-1-4398-0982-2

Automatic Defense Against Zero-day Polymorphic Worms in Communication Networks
Mohssen Mohammed and Al-Sakib Khan Pathan
ISBN 978-1-4665-5727-7

The Complete Book of Data Anonymization: From Planning to Implementation
Balaji Raghunathan
ISBN 978-1-4398-7730-2

The Complete Guide to Physical Security
Paul R. Baker and Daniel J. Benny
ISBN 978-1-4200-9963-8

Conflict and Cooperation in Cyberspace: The Challenge to National Security
Panayotis A. Yannakogeorgos and Adam B. Lowther (Editors)
ISBN 978-1-4665-9201-8

Cybersecurity: Public Sector Threats and Responses
Kim J. Andreasson
ISBN 978-1-4398-4663-6

The Definitive Guide to Complying with the HIPAA/HITECH Privacy and Security Rules
John J. Trinckes, Jr.
ISBN 978-1-4665-0767-8

Digital Forensics Explained
Greg Gogolin
ISBN 978-1-4398-7495-0

Digital Forensics for Handheld Devices
Eamon P. Doherty
ISBN 978-1-4398-9877-2

Effective Surveillance for Homeland Security: Balancing Technology and Social Issues
Francesco Flammini, Roberto Setola, and Giorgio Franceschetti (Editors)
ISBN 978-1-4398-8324-2

Electronically Stored Information: The Complete Guide to Management, Understanding, Acquisition, Storage, Search, and Retrieval
David R. Matthews
ISBN 978-1-4398-7726-5

Enterprise Architecture and Information Assurance: Developing a Secure Foundation
James A. Scholz
ISBN 978-1-4398-4159-4

Guide to the De-Identification of Personal Health Information
Khaled El Emam
ISBN 978-1-4665-7906-4

Information Security Governance Simplified: From the Boardroom to the Keyboard
Todd Fitzgerald
ISBN 978-1-4398-1163-4

Information Security Policy Development for Compliance: ISO/IEC 27001, NIST SP 800-53, HIPAA Standard, PCI DSS V2.0, and AUP V5.0
Barry L. Williams
ISBN 978-1-4665-8058-9

Information Technology Control and Audit, Fourth Edition
Sandra Senft, Frederick Gallegos, and Aleksandra Davis
ISBN 978-1-4398-9320-3

Iris Biometric Model for Secured Network Access
Franjieh El Khoury
ISBN 978-1-4665-0213-0

Managing the Insider Threat: No Dark Corners
Nick Catrantzos
ISBN 978-1-4398-7292-5

Network Attacks and Defenses: A Hands-on Approach
Zouheir Trabelsi, Kadhim Hayawi, Arwa Al Braiki, and Sujith Samuel Mathew
ISBN 978-1-4665-1794-3

Noiseless Steganography: The Key to Covert Communications
Abdelrahman Desoky
ISBN 978-1-4398-4621-6

PRAGMATIC Security Metrics: Applying Metametrics to Information Security
W. Krag Brotby and Gary Hinson
ISBN 978-1-4398-8152-1

Securing Cloud and Mobility: A Practitioner's Guide
Ian Lim, E. Coleen Coolidge, and Paul Hourani
ISBN 978-1-4398-5055-8

Security and Privacy in Smart Grids
Yang Xiao (Editor)
ISBN 978-1-4398-7783-8

Security for Wireless Sensor Networks using Identity-Based Cryptography
Harsh Kupwade Patil and Stephen A. Szygenda
ISBN 978-1-4398-6901-7

The 7 Qualities of Highly Secure Software
Mano Paul
ISBN 978-1-4398-1446-8

AUERBACH PUBLICATIONS
www.auerbach-publications.com • To Order Call: 1-800-272-7737 • E-mail: orders@crcpress.com

Information Security Management Handbook

Sixth Edition

Volume 7

Edited by

Richard O'Hanley · James S. Tiller

CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business
AN AUERBACH BOOK

CRC Press
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

Version Date: 20130723

International Standard Book Number-13: 978-1-4665-6752-8 (eBook - PDF)

Contents

Introduction ix
Contributors xiii

DOMAIN 2: TELECOMMUNICATIONS AND NETWORK SECURITY
Communications and Network Security

1 **Securing the Grid** 3
TERRY KOMPERDA

Network Attacks and Countermeasures

2 **Attacks in Mobile Environments** 23
NOUREDDINE BOUDRIGA

DOMAIN 3: INFORMATION SECURITY AND RISK MANAGEMENT
Security Management Concepts and Principles

3 **Security in the Cloud** 35
SANDY BACIK

4 **Getting the Best Out of Information Security Projects** 45
TODD FITZGERALD

5 **Mobility and Its Impact on Enterprise Security** 57
PRASHANTH VENKATESH AND BALAJI RAGHUNATHAN

6 **An Introduction to Digital Rights Management** 67
ASHUTOSH SAXENA AND RAVI SANKAR VEERUBHOTLA

7 **Information Security on the Cheap** 81
BEAU WOODS

8 **Organizational Behavior (Including Institutions) Can Cultivate Your Information Security Program** 101
ROBERT K. PITTMAN, JR.

9 Metrics for Monitoring....121
SANDY BACIK

Policies, Standards, Procedures, and Guidelines

10 Security Implications of Bring Your Own Device, IT Consumerization, and Managing User Choices....133
SANDY BACIK

11 Information Assurance: Open Research Questions and Future Directions....143
SETH J. KINNETT

Security Awareness Training

12 Protecting Us from Us: Human Firewall Vulnerability Assessments....151
KEN M. SHAURETTE AND TOM SCHLEPPENBACH

DOMAIN 4: APPLICATION DEVELOPMENT SECURITY
Application Issues

13 Service-Oriented Architecture....161
WALTER B. WILLIAMS

Systems Development Controls

14 Managing the Security Testing Process....179
ANTHONY MEHOLIC

15 Security and Resilience in the Software Development Life Cycle....197
MARK S. MERKOW AND LAKSHMIKANTH RAGHAVAN

DOMAIN 5: CRYPTOGRAPHY
Cryptographic Concepts, Methodologies, and Practices

16 Cloud Cryptography....209
JEFF STAPLETON

DOMAIN 6: SECURITY ARCHITECTURE AND DESIGN
Principles of Security Models, Architectures, and Evaluation Criteria

17 Identity and Access Management Architecture....221
JEFF CRUME

18 FedRAMP: Entry or Exit Ramp for Cloud Security?....239
DEBRA S. HERRMANN

DOMAIN 7: OPERATIONS SECURITY

Concepts

19 **Data Storage and Network Security** **251**
GREG SCHULZ

DOMAIN 9: LEGAL, REGULATIONS, COMPLIANCE, AND INVESTIGATIONS

Information Law

20 **National Patient Identifier and Patient Privacy in the Digital Era** **259**
TIM GODLOVE AND ADRIAN BALL

21 **Addressing Social Media Security and Privacy Challenges** **267**
REBECCA HEROLD

Investigations

22 **What Is Digital Forensics and What Should You Know about It?** **279**
GREG GOGOLIN

23 **eDiscovery** **287**
DAVID G. HILL

24 **Overview of the Steps of the Electronic Discovery Reference Model** **293**
DAVID G. HILL

25 **Cell Phone Protocols and Operating Systems** **303**
EAMON P. DOHERTY

Major Categories of Computer Crime

26 **Hacktivism: The Whats, Whys, and Wherefores** **321**
CHRIS HARE

Compliance

27 **PCI Compliance** **345**
TYLER JUSTIN SPEED

28 **HIPAA/HITECH Compliance Overview** **357**
JOHN J. TRINCKES, JR.

***Information Security Management Handbook*: Comprehensive Table of Contents** **387**

Introduction

This is the first annual edition of the *Information Security Management Handbook* since 1994 without the guidance and the insight of Hal Tipton. Hal passed away in March 2012. He will be missed by a lot of people for a lot of reasons.

It seems that every year is an interesting one for information security, and 2012 was no different. It is interesting, too, how perceptive Kaspersky Labs, for example, was with its forecast. It also foreshadows the end of online trust and privacy. If you cannot trust digital certificates, what is left to trust?

Kaspersky Cyberthreat Forecasts

2012	*2013*
Cyber weapons	Government surveillance
Mass targeted attacks	Continued targeted attacks
Mobile threats	Mac OS X malware and mobile malware
Attacks on online banking	Cloud attacks
PPI attacks	PPI threats
Hacktivism	More hacktivism
	Problems with trust and digital authorities
	Ramsomware and extortion malware
	Espionage and other government cyberattacks

Cyberwarfare has jumped to the front pages of every newspaper, both print and virtual. Stuxnet spawned Flame, Duqu, and Gauss. While we were all focused on attacks and espionage by China, France, and Israel, Iran mounted a DDoS (Distributed Denial of Service) attack against US banks in retaliation for sanctions that appear to be working. At the same time, Iran's central bank was attacked. Added to the online attacks is the growing threat of supply chain security, and products shipped with back doors or embedded systems that let them phone home. Witness the difficulty Chinese telecom equipment suppliers like Huawei are having with gaining toeholds in the United States by purchasing the US suppliers.

While Russians and Eastern Europeans are not singled out for cyberwarfare, crime syndicates based there continue to threaten commerce and privacy.

Theft of passwords from LinkedIn and Dropbox, and what seems like daily reports of attacks on or by Facebook show the lure of social media to hackers, and the dangers to the rest of us. And while Facebook and others do not install rootkits like Sony did, its data collection efforts, combined with the apparent insecurity of the site emphasizes the growing dangers of Big Data and the Cloud.

We saw a huge increase in hacktivism as Anonymous and LulzSec launched various attacks on both government and private sites around the world.

It was only a matter of time until Mac OS X became a profitable target. Once critical mass was reached, hackers could not resist investing the time to own it.

As with Mac OS X, mobile devices are becoming even more alluring targets. We have seen the same types of attacks and malware used against PCs adapted to mobile, plus new threats like SMS (short message service) spoofing. Not surprisingly, Android, Google's open platform, has suffered the most. Plus, the growing number of apps for all platforms introduces a level of threat that is hard to estimate, but definitely growing.

M2M and the Internet of Things are creating more opportunities for hackers. From NFC (near-field communication) payments to utility sensors sending unencrypted data, this is a potentially lucrative area for fraud and identity theft. Sensor networks are now in the DIY (do-it-yourself) arena, which creates yet a new class of threats.

BYOD (Bring Your Own Device), IT consumerization, whatever you call it, is making life so much more fun for black hats. It has given new meaning to "insider threats." With portable digital devices being introduced into the enterprise, both with and without permission, we are seeing a manifold increase in threats. Clearly, policies alone are not sufficient to deal with this, and it is unclear how draconian management wants to be with forcing compliance. The products exist, but does the will to use them?

Looking at 2013, the promise of more surveillance, both from governments and online data collectors, means less privacy, even for the most careful users. Short of totally disconnecting from the grid, if such a thing is possible now, it is apparent we do not and would not have privacy.

This edition of the *Information Security Management Handbook* addresses many of these trends and threats, plus new areas such as security SDLC (software development life cycle), as well as forensics, cloud security, and security management. Chris Hare takes an in-depth look at hacktivism, identifying the motivations and the players, and providing advice on how to protect against it. Becky Herold analyzes the security and privacy challenges of social media. Sandy Bacik looks at the security implication of BYOD, and the challenges of managing user expectations. The Smart Grid offers its own security and privacy challenges as Terry Komperda explains. Noureddine Boudriga explains attacks in mobile environments.

There is new guidance on PCI and HIPAA/HITECH compliance. In addition to forensics and e-discovery, a chapter looks at cell phone protocols and operating systems from the perspective of a forensic investigator.

I have heard it said, "You can't fix stupid." So many of these attacks are successful because of clueless or irresponsible users. In what I hope is not a vain effort, Ken Shaurette and Tom Schleppenbach look at human firewall testing, social engineering, and security awareness. We also look at security and resilience in the software development life cycle, managing the security testing process, and SOA (service-oriented architecture) security.

Here is a shout out to my friend Jim Tiller, head of Security Consulting, Americas for HP Enterprise Security Services, for his help in preparing this edition. Jim's done a lot for the Handbook over the years, and I am hoping he will continue.

All-in-all, this is a good volume of the *Information Security Management Handbook*. We are working on the next edition now. If you would like to contribute, please contact me at 917-351-7146 or rich.ohanley@taylorandfrancis.com.

Richard O'Hanley

Contributors

Sandy Bacik
Lord Corporation
Cary, North Carolina

Adrian Ball
TurningPoint Global Solutions
Rockville, Maryland

Noureddine Boudriga
Réseau National Universitaire
Tunis, Tunisia

Jeff Crume
IBM
Research Triangle Park, North Carolina

Eamon P. Doherty
Fairleigh Dickinson University
Teaneck, New Jersey

Todd Fitzgerald
ManpowerGroup
Milwaukee, Wisconsin

Tim Godlove
Department of Veterans Affairs
Washington, DC

Greg Gogolin
Ferris State University
Grand Rapids, Michigan

Chris Hare
Verizon
Dallas, Texas

Rebecca Herold
Rebecca Herold & Associates, LLC
Des Moines, Iowa

Debra S. Herrmann
Jacobs Engineering
Washington, DC

David G. Hill
Mesabi Group LLC
Westwood, Massachusetts

Seth J. Kinnett
Chicago, Illinois

Terry Komperda
Illinois Institute of Technology
Chicago, Illinois

Anthony Meholic
The Bancorp Bank
Wilmington, Delaware

Mark S. Merkow
PayPal
San Jose, California

Robert K. Pittman, Jr.
County of Los Angeles
Los Angeles, California

Lakshmikanth Raghavan
PayPal
San Jose, California

Balaji Raghunathan
Infosys Limited
Bangalore, India

Ashutosh Saxena
Infosys Limited
Hyderabad, India

Tom Schleppenbach
Inacom Information Systems, Inc.
Madison, Wisconsin

Greg Schulz
StorageIO
Stillwater, Minnesota

Ken M. Shaurette
FIPCO
Madison, Wisconsin

Tyler Justin Speed
Electronics International
Eugene, Oregon

Jeff Stapleton
Bank of America
Dallas, Texas

John J. Trinckes, Jr.
PathForwardIT
Cincinnati, Ohio

Ravi Sankar Veerubhotla
Infosys Limited
Hyderabad, India

Prashanth Venkatesh
Infosys Limited
Bangalore, India

Walter B. Williams
Lattice Engines
Boston, Massachusetts

Beau Woods
Stratigos Security
Atlanta, Georgia

DOMAIN 2

TELECOMMUNICATIONS AND NETWORK SECURITY

Communications and Network Security

Chapter 1

Securing the Grid

Terry Komperda

Contents

Introduction 4
The Power (Electrical) Grid 4
    Core Functions of a Power Grid 4
    Power Grid Components 5
    Power Distribution Topologies 5
    Communication Networks, Control, and Communications Protocol in the Grid 5
    Problems in Current Power Grids 6
Stuxnet 6
The Case for a Smart Grid 6
The Smart Grid 7
    Smart Grid Technologies, Systems, and Components 7
Grid Vulnerabilities 8
Threats in the Grid 9
    Threats by Confidentiality, Integrity, and Availability 9
    Privacy Threats 10
Potential Attacks on the Grid 10
    Attacking Consumers 10
    Attacking Utility Companies 11
Federal Efforts to Protect the Grid in North America 13
Standards Bodies and Standards for Protecting the Grid 14
Security for the Grid 16
    General Security Practices 16
    Technical Security Practices 17
    Privacy Practices 18
Conclusion 19
References 19
Further Reading 19

Introduction

Before we can dive into how utility networks will evolve and how those future networks will be exposed to issues that will affect their security and continued functioning, we need to look at some history on the current networks, why they need to change after functioning properly for so long, and the benefits to be realized related to their technological advancement.

The Power (Electrical) Grid

The power grids of the twentieth century were designed to be a one-way broadcast of power from a few central generators to a large number of electrical users. At the time of the design, the main goal was to keep the lights on without any regard for energy efficiency, environmental considerations, or consumer choices. Typically, it has been a geographically organized number of integrated utilities with control based on a fixed hierarchical infrastructure. The following section is a simple illustration of a power grid that shows the main functions that a power grid performs (Figure 1.1).

Core Functions of a Power Grid

The following factors are the core functions of a power grid:

a. *Power generation*—Power is generated at a power station and can emanate from coal and nuclear plants, dams, windmills, and so on.

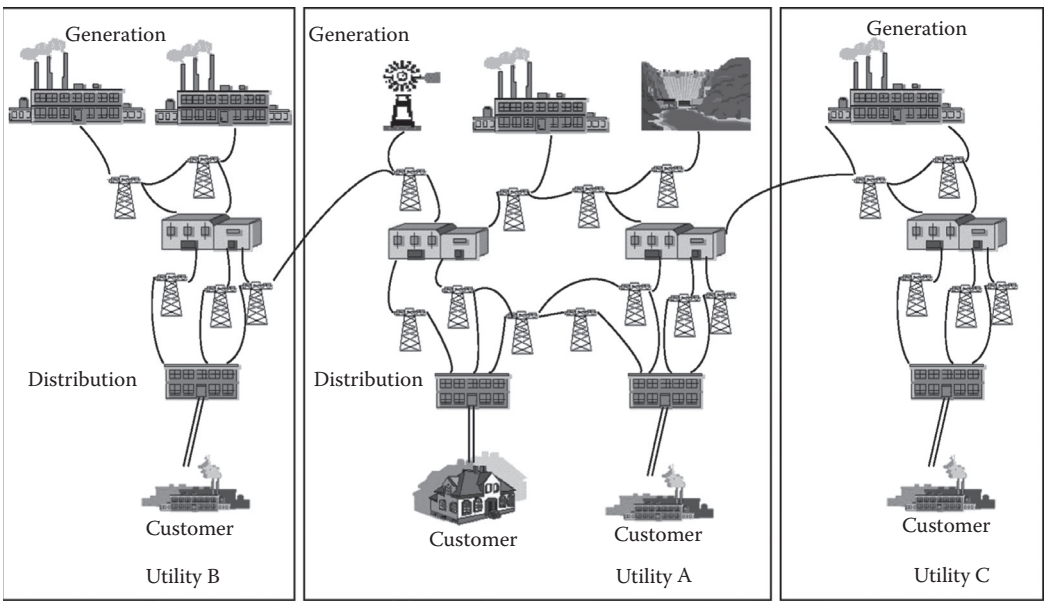

Figure 1.1 Power grid. (From Bakken, D. et al. 2003. Grid stat. Washington State University, School of Electrical Engineering and Computer Science, November 2003. Slide #4.)

b. *Transmission*—Electricity is transferred from power stations to power distribution systems at a substation. The substation is a point of monitoring and control in the grid, and high-voltage electricity is handled here.
c. *Distribution*—Medium-voltage electricity resides here, and this is where power is delivered to the end customers.

Historically, larger power companies have been granted a monopoly status and typically control all the three functions for a geographic area.

Power Grid Components

These are the major components in a power grid:

a. *Generator*—Its major function is to generate power.
b. *Substation*—This is a point of control and monitoring in the grid, and can service many generators, boost voltage, and serve as a distribution point to the customers.
c. *Control area*—This is a set or a group of substations in a geographic area covering a county to a few states. A control area performs all the three core functions and corresponds to one or a few utility companies.
d. *Grid*—A set of control areas that are synchronously controlled.

Power Distribution Topologies

Power is typically distributed in one of the three ways in a power grid:

a. *Radial grid topology*—Electricity is distributed from a substation in a pattern resembling a tree with branches and leaves. The branches and leaves receive power from a single source.
b. *Mesh grid topology*—Power is provided from other sources (other branches and leaves), and this allows a mesh grid to be more reliable than a radial grid.
c. *Looped topology*—This is a combination of mesh and radial topologies and is used primarily in Europe. This topology resists disruption in the grid, no matter where the problem occurs.

Communication Networks, Control, and Communications Protocol in the Grid

a. *Communication networks*—Frame relay, asynchronous transfer mode (ATM), public switched telephone network (PSTN), and the Internet are all used for communications in the current grid.
b. *Control*—Supervisory control and data acquisition (SCADA) is a serial system implementation used to remotely control and monitor the transmission and the distribution of power in electrical grids.
c. *Communications protocol*—The most popular utility automation protocol used in North America is distributed network protocol (DNP). It is applied through distribution and transmission networks and provides connections from master stations to substations, between devices in substations, and out-to-pole top devices.

Problems in Current Power Grids

Although current grids have worked well for many years and have had upgrades such as automatic meter reading (AMR) to remotely read meters, the communications network is hardwired, dedicated, and slow, and this has led to networks that are dangerously antiquated. In fact, the dog food industry spends more on research and development than the electrical sector does, and aging technologies have led to more blackouts, vulnerabilities, and colossal inefficiencies (Kingsbury, 2010). Additionally, the following factors are some of the other issues that are presenting themselves with:

- Distributed control systems (DCS) and SCADA that are now connected to the Internet, and when they were originally designed, the controls were not designed with public access in mind. These systems typically lack rudimentary security, and technical information and security flaws for penetrating into these systems are widely discussed in public forums and are therefore well known to attackers. In fact, many years ago, a 12-year-old broke into the computer system that runs Arizona's Roosevelt Dam. He had full control of the SCADA system that controlled the dam's floodgates (Bakken, 2003).
- The Energy Department came up with multiple scenarios for attacking the grid through SCADA systems and all of them worked.
- Continued automation is being added to substations to reduce human errors and mistakes, but the computer-controlled systems and software increase the potential for security vulnerabilities.

A recent special case confirms that current power grids are not immune to attacks and vulnerabilities.

Stuxnet

Stuxnet is the first known malware attack to target power plants. It is a worm that was introduced via a universal serial bus (USB) device in an Iranian nuclear plant. It infected a SCADA system that was considered as buffered from the attack as most of these systems are not connected to the Internet in nuclear power plants. It installs a rootkit on the control system and injects a malicious code into programmable logic controllers, reprograms them, and hides the changes. It was digitally signed with two stolen authentication certificates from two certificate authorities and this helped it to remain undetected for quite some time. Once inside, it uses default passwords (Siemens, the manufacturer of most SCADA systems, recommends against changing default passwords) to command the software and exploits four different Windows zero-day vulnerabilities to infect all sorts of computers. Siemens reported that it has discovered an additional 14 clients (power plants) that have been infected, a number of which are in Germany (Evron, 2010). This attack pretty much quietened those that argued for maintaining the current grid with proprietary protocols and systems because it was thought that the current systems were more secure (especially if they were not widely connected to the Internet).

The Case for a Smart Grid

The following factors are some of the reasons that it makes sense to evolve current electrical grids into smart grids:

- The rates can be variable based on true usage. The consumers would only pay for the power used and if more power is used (especially during peak periods), utilities could charge a premium. The customers will have to change their behavior, but they will be rewarded for saving energy.
- The consumers who have a power surplus (that they would not be using) could push the power back into the grid and sell it back to the utilities for other customers who could use it.
- The grid system could be more stable by automatically avoiding or mitigating power outages and power-quality issues and by repairing itself (self-healing) during a service disruption. This will lead to fewer brownouts and blackouts.
- Waste reduction: Cutting tiny inefficiencies can have dramatic effects on the overall grid and can lead to maintaining affordability for all.
- The grid will accommodate both renewable and traditional energy resources leading to better power quality and improved reliability.
- The grid will be able to account for new, larger potential loads in the network such as that from increasingly popular electrical vehicles.
- The reductions in the carbon footprint will help with the overall energy conservation and will promote better environmental responsibility.

The Smart Grid

Implementing a smart grid transforms the power grid from a one-way, closed, proprietary system to a modern, two-way, standards-based, intelligent system that allows operators to monitor and interact with numerous components in real time. It allows operators to detect issues and manage grid operations for faster problem resolutions and lower operating costs. A smart grid will not replace the legacy systems, but will have to incorporate them and evolve to a smarter grid over many years (and at a significant cost). Internet Protocol (IP)-based systems will tie SCADA and DCS into the evolving grid for efficient management and communication across the main stations and remote locations. IP-based systems will pose a security challenge (just like they do when deployed elsewhere) but trying to secure legacy devices (that used isolation as a security technique) will make the security job even more challenging.

Smart Grid Technologies, Systems, and Components

The following factors are some of the technologies, systems, and components that will be used in smart grids:

1. *Integrated communications*—Today, a good amount of data are still collected via the modem instead of direct communication. The implementation of direct communications can improve substation automation, distribution automation, demand response, and SCADA management. This will allow for real-time control as well as information and data exchange for optimizing system reliability, utilization of assets, and security.
2. *Improved interfaces and decision support*—The collection of extremely complex data will become difficult for humans to comprehend in a timely manner. The human machine interface (HMI) must simplify the data to enable operators and managers to make decisions quickly.

3. *Distributed grid management (DGM)*—This aims at maximizing the performance of feeders, transformers, and other components of network-distribution systems and integrates with transmission systems and customer operations. The benefits derived are better reliability, reductions in peak loads, and improvements in the capability to manage distributed renewable energy sources.
4. *Wide area situational awareness (WASA)*—This involves monitoring and display of power-system components and performance across interconnections and over large geographic areas. The goal is to optimize management and the performance of network components so that issues and disruptions can be anticipated, prevented, or responded before they occur.
5. *Sensing and measurement technologies*—These technologies evaluate congestion and grid stability as well as monitoring network and customer side equipment in terms of health and power consumption. The following factors are some of the components used:
   a. *Smart meters*—These are used to monitor usage statistics and report them to utility companies, businesses, consumers, and third-party service providers. They replace the old analog meters and record real-time usage. They can also show how much power is being used at different times of the day along with the related power costs. Two-way communication on these meters also allows for power-outage notification as well as remotely disabling the service (if necessary).
   b. *Advanced metering infrastructure (AMI)*—This remotely measures, collects, and analyzes usage statistics from smart meters. AMI is similar to advanced meter reading (AMR) but is an upgrade (two-way vs. one-way meter reading).
   c. *Phasor management units (PMU's)*—These are high-speed sensors distributed throughout the network to monitor power quality and respond automatically to power issues.
   d. *Wide area measurement system (WAMS)*—This is a network of PMU's that provides real-time monitoring on a regional and national basis.
   e. *Advanced components*—These include excess electricity storage, fault tolerance, smart devices, and diagnostic equipment. Smart (intelligent) devices are useful for providing consumption feedback to customers in the home.
6. *Home area network/business area network (HAN/BAN)*—These networks look to address demand/response and consumer energy efficiency. These networks include mechanisms and incentives for businesses, utilities, industrial customers, and residential consumers to cut energy use during peak demand or when power reliability is questionable.

Now, we know something about power grids, the evolving grid, and future smart grids, and we can look at vulnerabilities, threats, and attacks on these utility grids.

Grid Vulnerabilities

The following factors are some of the noteworthy security vulnerabilities:

- Many current security vulnerabilities are basic and include a failure to install security patches and poor password management. The fixes in these areas are inexpensive.
- Unsecure software-coding practices used in control networks and excessive allowance of portal access into networks are some of the prevailing security gaps. Poor code quality leads to bugs and vulnerabilities that can make the grid fragile and unstable as well as vulnerable to attacks.
- Ineffective passwords and lack of proper encryption for communications and databases are the common problems as well.

- Smart grid components and technologies such as smart meters and AMI/AMR networks use wireless Wi-Fi and/or BlueTooth technologies to transport the usage data from consumers back to utility companies. There are pervasive security issues with Wi-Fi networks, and many organizations have banned their use or have implemented policies that have restricted their access to corporate networks. Bluetooth is an unsecure technology, and there are known scanning tools that allow for Bluetooth device discovery, operating mode, and strength of the device. Bluetooth 3.0 uses Wi-Fi radios, and Wi-Fi can be susceptible to wireless packet sniffers.
- The utilities that do not use wireless networks can still be vulnerable if employee laptops, handhelds, and smart devices are used. A tool called Karmetasploit can turn a wireless laptop into an access point that can associate wireless clients with it. Once associated, that client can be taken to a malicious service.

Threats in the Grid

a. *Hacking*—Hackers may want to get into systems for an intellectual challenge or out of curiosity. Their actions could have negative impacts on consumers and utility companies.
b. *Theft*—The consumers can monitor their electricity usage but if that information ends up in the wrong hands, the usage can point to patterns in the home during certain times of the day. Determining when a homeowner is out of the house can lead to burglaries.
c. *Extortion*—The grid can be exploited for money and power. Extortive malware can be used to hold a system or data hostage, to extort a ransom from an owner/user. A specific service can lock a user out of the system or can prevent access to critical data (or a combination of these). Consumer access to power can be prevented and a monetary demand could be used by an attacker to restore power.
d. *Power disruption due to vengeance and vindictiveness*—A remote disconnect feature can be used by a problem neighbor, or the neighbor can also perform a physical attack on a smart meter on the side of the home.
e. *Terrorism*—This could affect a large number of people and could cause massive attention for a cause. It can occur by both digital means and physically by bombings.
f. *Warfare*—The attacks can be used during war time by an enemy to cripple a country's infrastructure.
g. *Poor patch management*—Patches would not always install correctly, and these may be found during an audit, security assessment, or by a hacker. If these occur, a customer may receive billing errors or electricity can be shut off.
h. *Intentional threats*—The angry employees could attack the consumers.
i. *Activists*—They can use the grid as an additional avenue to attack certain manufacturers (e.g., fur manufacturers).

Threats by Confidentiality, Integrity, and Availability

Flick and Morehouse (2011) discuss threats related to confidentiality, integrity, and availability.

Confidentiality—This involves protecting the information from unauthorized disclosure. In the grid, this has the greatest effect on consumers. Utility companies store names, addresses, social security numbers, and usage data. The hackers can compromise the

database through a structured query language (SQL) injection on a website used by consumers to manage their accounts, monitor usage, and make payments. The hackers could obtain credit card numbers or bank accounts from customers who use online or automatic bill payment.

Integrity—This focuses on protecting the information from unauthorized modification. If the information is modified, it has the greatest effect on utility companies in terms of fraud or service theft. Once it is determined how to hack smart meters, the information can be placed on the Internet, and customers as well as hackers can defraud the utility companies by stealing services (underreporting to lower bills) or by fooling the utility company into thinking that they are selling more electricity (over reporting to get more credits) back into the grid.

Availability—This is attained when the service is protected from unauthorized interruption. This impacts the service provider as well as customers. The threats can be from script kiddies or people the victim knows and the threat could affect power to the home. A smart meter can be attacked through the wireless configuration on the router allowing access to the wireless network to change the default password and to shutdown power. When the victim goes back in with her password to reenable power, the password is no longer known.

Privacy Threats

1. *Identity theft*—Grid identities (IDs) and other information can be placed on the Internet and can be sold. The thieves can use personally identifiable information (PII) obtained to impersonate customers for fraudulent utility use, and this could affect customer credit reports.
2. *Personal surveillance*—Sensitive personal behavioral patterns can be revealed to expose customer schedules or personal details about their lives (interactions with others, medical issues, etc.). It can be determined whether a person lives alone, whether they leave the house vacant all day, whether they are senior citizens, have small children at home, and so on.
3. *Energy use surveillance*—This focuses on meter data used to show the specific appliance used in the home. It can report the number of gadgets in the home, whether there is an alarm system (and how often it is turned on), and so on.
4. *Physical dangers*—Real-time data can be used to cause harm. Domestic violence offenders/stalkers/abusers can use the information to relocate the former victims who have an urgent and continued need for privacy.
5. *Misusing data*—Utilities could misuse the data by providing them to third-party marketing firms or a previous homeowner's smart meter may have the data that were not wiped clean when they moved, and now, there are data known about the previous users.

Potential Attacks on the Grid

Attacking Consumers

1. *Attacking smart meters*—Smart meters are a basic, low-cost technology that hackers can purchase to take apart and learn about the communications network. The customers have physical and perhaps logical access to them as well. Additionally, these could be some common attacks (Flick and Morehouse, 2011):
   - Since smart meters are accessible through wireless networks or HANs, a tool such as network mapper (NMAP) (network scanner) can be used for transmission control protocol

(TCP) pings for port scans to identify active hosts with the common services that are running.
   - NMAP can be used for probing on TCP or User Datagram Protocol (UDP) ports to determine a response on an associated port with a service running that may have a weakness that allows access.
   - If a smart meter contains a web component that allows the users to view/change the usage information, vulnerability identification and verification can be performed against the web application.
   - There can be an attempt to identify the valid credentials for a service or a web application by using a dictionary attack or through brute force.
   - Wireshark can be used to determine the typical traffic patterns, and NMAP can be used to increase the traffic and overload the meter or infrastructure to achieve a denial of service.
   - The code can be used to create a buffer overflow, or an SQL injection can be used to access a command shell through an input validation weakness in a web application.
   - Kismet (wireless sniffing tool) can be used to compromise the confidentiality, integrity, and availability (CIA) of the data going across the network. If Bluetooth is used, Kismet just added a Bluetooth component to its wireless sniffing tool. IF radio-frequency identification (RFID) is used, there are plenty of RFID sniffing kits that can be easily created.
   - A physical attack of the smart meter on the side of the building can occur. If a camera is monitoring it, the attacker can mask her identity.
2. *Attacking smart devices*—Smart devices can be purchased off of the net or can be picked up at the local retail store and studied. These devices can send the data over the wireless network or readings over power line communications (PLC) to a gateway that runs a web server. The web server can interface with something such as Google Power Meter to monitor and present the usage information.
   - Wireshark can be used to get device IP addresses and NMAP can be used to try to get responses. NMAP can also be used to identify any services that are running on TCP or UDP ports.
   - The weaknesses in web applications can be identified, and web browsers can be used with the device uniform resource locator (URL) to guess the password. Wireshark can be used to look for unencrypted passwords or encrypted passwords that are weak or contain flaws.
   - Vulnerability scanners can be used to detect whether the devices are susceptible to the denial of service attacks. A well-constructed disk-operating system (DOS) attack can cause a blackout.

Attacking Utility Companies

Companies will most likely be attacked through the use of multiple attack vectors (a combination of application, network, social engineering attacks, etc.) (Flick and Morehouse, 2011):

1. *Network attacks*—Attacks can come from systems, networks, and subnetworks. The following factors can be used to determine network-security access:
   a. *Reconnaissance*—Passive testing can be used to determine utility company infrastructure. The perimeter of the IP address ranges assigned to the utility company could be

determined. IP addresses/host names can be determined for web servers, Domain Name System (DNS) servers, e-mail servers, routers, gateways, and virtual private network (VPN) concentrators.

b. *Discovery*—Ping sweeps and port scans can be used to identify rogue systems (perhaps test systems placed in the network and never removed). Network routes can be determined, and it could be determined whether networks are properly segmented with strict access control lists (ACLs). Smart devices on the customer side could be examined to determine whether they can connect directly to the generation domain of the utility company. If they do connect all the way in, that could be the path of least resistance for a hacker. Business partner networks could be examined to determine whether they have unrestricted access into the utility networks. If they do, a hacker's path of least resistance into the utility network may be through the partner network.

c. *Vulnerability identification*—Vulnerability scanners can be used to identify services running on open ports and then interrogating the service. The scanners can inspect a service banner that can tell the name and version of the service. On the basis of version information, the scanner will determine what security patch-based vulnerabilities a service may be susceptible to. Exploiting the vulnerabilities can cause DOS, disclosure of pertinent information, or allow for remote code execution.

2. *System attacks*—If firewalls and IPS/intrusion detection system (IDS) are in place, it will make it harder for attackers to remotely attack the company; so, hackers may resort to e-mail attachments and website attacks. SCADA devices support web servers, telnet, and file transfer protocol (FTP), so that attackers may try to get in through these areas. Legacy systems will have support issues as they age and security patches may no longer be created for new vulnerabilities that are discovered. Since dial-up modems are still used (typically as the backup for outages), remote access to critical systems may be fairly easy especially if default passwords are never changed.
3. *Application attacks*—Web servers, web applications, and services will be used and may provide an avenue for the attack. Web applications can allow for a single point of failure. Web services secure login that do not accept the hypertext transfer protocol text (HTTPS) protocol (this exists today) that is vulnerable. The injection of the malicious code (scripts, commands, or queries) against web applications can allow for administrator level access to allow an attacker to perform any type of query against any table in the database.
4. *Wireless attacks*—Discovery, device profiling, and exploits can be used on wireless networks (RF, Wi-Fi, BlueTooth, and cellular), wireless clients, and access points to identify unauthorized (rogue) clients, networks, and so on. The attacks in the network can cause DOS, revealing critical information, and bypassing perimeter controls to gain access to internal networks.
5. *Social engineering attacks*—The focus here should be on security awareness and training of company employees. The attackers can try to fool employees into revealing user names and passwords or can provide the attacker with additional access by
   - Impersonating an employee and calling the information technology (IT) help desk to change the password.
   - Impersonating a vendor to obtain proprietary information or for the purpose of sabotaging the equipment.
   - Dropping USB sticks with the malicious code in strategic locations to provide a way into the network.
   - Sending phishing e-mails to solicit confidential information.

6. *Physical attacks*—This could involve gaining access to buildings without a badge, copying or taking pictures of information that is out in the open, eavesdropping, stealing unlocked mobile devices, or using an available/unlocked personal computer (pc).

The attackers do not stick to only one type of attack, and they will use a combination of the above factors to attack the utility companies.

Federal Efforts to Protect the Grid in North America

Now, the vulnerabilities, threats, and potential attacks have been identified, and we can look at the efforts to protect the grid in North America. The following factors are the Federal efforts in place to achieve the proper protections:

1. *Federal agencies*—The following agencies are concerned with protecting the grid:
   a. *Department of Homeland Security (DHS)*—The DHS is tasked with creating a national infrastructure protection plan (NIPP) for the critical infrastructure and key resources. The plan must ensure that the infrastructure and resources are safe, secure, and resilient, through prevention, neutralization, and mitigation of deliberate efforts by terrorists to exploit or destroy the grid. The objective of the effort is to strengthen national preparedness, provide timely response to attacks, and allow for rapid recovery in the event of attack, natural disasters, or emergencies.
   b. *Department of Energy (DOE)*—This organization was established by the Federal Government in the late 1970s to organize fragmented regulatory processes and to create a national energy plan. The DOE is also responsible for monitoring and reporting on the security of smart grids. The objectives of the reporting are to determine how to make the grid less vulnerable to disruption, how to restore the integrity of the grid after disruption, how nationwide emergency communications can be facilitated after a local, regional, or nationwide emergency takes place, and what grid risks must be taken into account and how the risks should be mitigated. The DOE also established the Federal Energy Regulatory Commission (FERC) as an independent regulatory body within the DOE.
   c. *FERC*—FERC regulates the interstate transmission of natural gas, oil, and electricity, and has the authority to mandate reliability standards and impose penalties for noncompliance. FERC also issues orders for emergency measures to protect the reliability of the bulk power system and critical infrastructure when the President identifies a security threat to the grid.
2. *Federal legislation*—The following factors are some of the federal legislations designed to protect the grid:
   a. *H.R. Bill 5026*—This is the Grid Reliability and Infrastructure Defense Act or Grid Act. This establishes federal authority to address emergencies (with or without notice) if the President identifies an imminent threat to the bulk power system. It also establishes measures to protect the grid against the key vulnerabilities so that we are prepared if an emergency occurs and gives FERC the authority to protect portions of the grid that serve the top 100 facilities against a cyber threat or electromagnetic weapon attacks. Additionally, it allows FERC to bypass the standards setting process and issue orders to utilities to address security vulnerabilities not addressed by the standards. Finally, it

allows for requiring entities that own or operate large transformers to ensure adequate availability of replacements to promptly restore the operation, should a transformer be destroyed or becomes inoperable.

b. *H.R. Bill 2195*—This bill directs the Secretary of Homeland Security working with other security and intelligence agencies to conduct research and determine if networks critical to the operation of critical electricity infrastructure have been compromised. It also amends the Federal Power Act to direct the Secretary to make ongoing assessments to provide periodic reports on cyber vulnerabilities or threats to critical infrastructure, including AMI, and looks to enhance domestic preparedness in case of a cyber attack.

Standards Bodies and Standards for Protecting the Grid

The following factors are a couple of the important standard bodies for developing standards to help protect the grid in North America:

1. *National Institute of Standards and Technology (NIST)*—This is a federal technology agency that works with the industry to develop and apply technology and standards. NIST is responsible for coordinating the development of a smart grid interoperability framework and a plan to create standards to address the remaining gaps and the integration of new technologies, testing, and certification to ensure smart grid equipment and systems that conform to security and interoperability standards. It further engages utilities, vendors, consumers, and so on to achieve standards on architecture, priorities for interoperability and cyber security standards, and any plans to meet the remaining standard needs. NIST Publication SP800-82 is one of the important publication as it addresses how to secure industrial control systems that include SCADA, DCS and PLCs, and identification of the common threats and vulnerabilities of these systems as well as any countermeasures to mitigate the risks associated with the threats and vulnerabilities.
2. *North American Reliability Corporation (NERC)*—FERC established this organization to create reliability standards and enforce them through severe financial penalties for noncompliance. NERC developed Critical Infrastructure Protection Standards (CIP) that are mandatory for utility companies to comply with. The standards cover two security categories (electronic security and physical/personnel security) and are as follows*:

   CIP-002—This covers the critical cyber asset identification and documentation concerned with assets that enable the reliable operation of the grid. The assets must be identified through a risk-based assessment approach and documentation of the assessment is necessary along with the methodologies used, evaluation criteria, and procedures/processes. Risk-based assessments must be conducted annually.

   CIP-003—This states that minimum security management controls must be implemented to protect critical cyber assets. The core requirement here is the cyber security policy, and this policy must be available to all personnel responsible for, or having access to, critical cyber assets. The exceptions to the security policy are also covered here, and the exceptions must be documented and authorized by a senior manager.

* Reliability standards for the bulk electric systems of North America. North American Electric Reliability Corporation. Critical Information Protection Standards.

CIP-004—This is concerned with the personnel and training. A security awareness program must be developed and documented for those with access to critical cyber assets and quarterly updates must occur. A cyber security training program is also required for those accessing critical cyber assets. The training must address policies, procedures, and access control related to the assets and must be performed at least annually. Also required is a documented personnel risk assessment program that verifies social security numbers and looks at a 7-year criminal background check that is reassessed every 7 years or for a cause. Finally, a list of personnel authorized to access the critical assets must be maintained and reviewed quarterly or must be updated within 7 days due to any change in personnel access rights. Physical access must be revoked within 24 h for any terminated employee.

CIP-005—This covers protecting all access points on the electric security perimeter that houses the critical cyber assets. The perimeter and associated access points must be identified and documented, and technical procedures must follow a default deny policy (only ports and services required for operating and monitoring of assets within the perimeter are enabled). Access to the perimeter must be monitored and logged and a vulnerability assessment of the perimeter must be performed annually. The results of the vulnerability assessment must be documented and an action plan to remediate the identified vulnerabilities must be established.

CIP-006—This is concerned with developing and implementing a physical security program to protect critical cyber assets. The controls to manage access to the physical security perimeter on a 24/7 basis must be implemented. In this standard are specifics related to card keys, special locks, security personnel, and authentication devices. Physical access must be monitored and logged by human observation, alarm systems, video systems, or manual logging. Physical access logs must be kept for 90 days and testing of physical security must take place every 3 years. The records of the testing must be kept.

CIP-007—Processes, methods, and procedures for securing critical cyber assets residing within the perimeter must be defined, and testing procedures must be in place to protect against adverse effects from significant changes in cyber assets. The significant changes are patches, service packs, updates, and upgrades, and procedures must be in place to test the security of the changes. A patch management program must be defined and documented, and controls must be in place for antivirus software and antimalware tools. The use of shared accounts must be identified, and these accounts must be secured in case of personnel changes. Data-storage media must be destroyed or erased prior to disposal and records of disposed or redeployed cyber assets must be maintained.

CIP-008—This looks at incident reporting and response planning. Cyber security incidents related to critical cyber assets must be identified, classified, responded, and reported. The incident response plan must include classification procedures to determine which cyber incidents are reportable, actions required to respond to the incidents, a process for escalating and reporting incidents, a process to ensure plans that are updated within 90 days of any changes, a process to ensure plans that are reviewed and exercised at least annually, and all documentation of incidents must be made available for at least 3 calendar years.

CIP-009—This looks at disaster recovery. The recovery plans for critical cyber assets must be established and must ensure that the plans follow established business continuity, disaster-recovery techniques, and practices. The plans must include definitions for roles and responsibilities associated with recovery, and recovery plans must be tested annually.

> Backup storage, restoration processes, and procedures must be documented and backup media deemed essential for recovery must be tested annually.

Although these standards are a good practice and are necessary, many legacy systems and devices are not able to meet these requirements. NERC is formalizing the procedures to allow entities to submit technical feasibility exceptions (TFEs) for cyber assets that cannot comply with the CIP standards. Also, NERC has determined that today, many utilities are underreporting critical assets to avoid compliance requirements.

Security for the Grid

There are a number of areas that must be looked at when considering security for the grid and the goal of cyber security is on prevention.

General Security Practices

- Bottom-up risk assessment should focus on authentication and authorization as it relates to substations, intelligent electronic devices (IEDs), key management for smart meters, and intrusion detection for power equipment. Top-down risk assessment should look at logical interfaces for priority areas such as electricity transportation and storage, WASA, demand response, AMI, and DGM architecture. The identified risks can be avoided, transferred, mitigated, or accepted. The risks should first be avoided or mitigated, and avoidance involves implementing information security controls.
- The grid will be composed of multiple networks that belong to different organizations and individuals and there must be a strict set of interoperability standards to facilitate communications between the networks. Firewalls should be placed between networks, and trust relationships and segmentation must be established between components and networks so that a threat or vulnerability in one network does not have a chance of spreading across the entire grid.
- Intentional attacks on consumers by utility company employees could be minimized by implementing least privilege (access is both required and authorized) and separation of duties (only the level of access required to perform a specific job). An employee who is responsible for billing, for example, should also not be able to shut off power to the home.
- The IT principles and security objective priorities of confidentiality, integrity, and availability are important, but they have different priorities in power networks as availability of the network is most important followed by integrity and confidentiality. Mesh architectures capable of self-organizing and healing can be used to ensure integrity and availability under adverse conditions. Although confidentiality is least important today, it is becoming increasingly important as more data will be collected on consumers and privacy of customer information will be stressed. The effective privacy practices will be covered later.
- Well known, open-security standards used elsewhere should be leveraged. The security mechanisms operating at multiple layers of the protocol stack should be employed to deliver a layered defense (defense in depth), and the security framework should be flexible, adaptable, and expandable to address an evolving threat landscape.
- Securing the grid requires cooperation between utility companies, the federal government, suppliers, consumers, NERC, the DHS, and the DOE to name a few.

- Data security should focus on critical asset identification and documentation, data classification, encryption of data at rest and in transit, database access monitoring, alerting and reporting, and change control and configuration management. Data security programs should be all about policy, process, and people.
- Business continuity management needs to be stressed so that incidents that threaten the continuity of operations are able to be addressed. The critical infrastructure needs to be identified (along with the associated risks) and security controls need to be implemented to minimize impacts from disasters, security breaches, and DOS. Without business continuity management, it will be difficult to survive a coordinated and targeted cyber attack.

Technical Security Practices

The following factors are the technical security practices that can be implemented to protect the grid*:

1. *Threat modeling*—The developers of software or any other solution should identify the potential attack vectors on their deployable solution. They need to develop abuse cases and ponder how their software can be used for a malicious intent. Once the potential attacks are identified, controls can be implemented for mitigation and attacks can be looked at in terms of confidentiality, integrity, and availability.
2. *Segmentation*—The goal here is to minimize the impact of a successful attack through the use of stateful firewalls, for example, not through ACLs on switches or routers. Smart meter traffic, for instance, should be contained to one geographic location so that if there is an issue, it does not spread throughout various networks.
3. *Default deny firewall rules*—These rules should apply to all inbound and outbound connections, and outbound connections should only occur from systems that have direct access to the Internet. All the other systems should be forced through a proxy for protections such as content filtering and detection of malware.
4. *Code and command signing*—Crypto hashes to validate software authorization and code integrity need to be implemented. Otherwise, attackers can run the arbitrary code on smart meters and can issue commands on the infrastructure that will be trusted. Most smart meters deployed today do not use authentication before running updates or disconnecting the service from a customer.
5. *Honeypots*—These appear to be the production systems that can be used to identify and contain attackers. They can provide alerts when successfully attacked or compromised. This can be used to understand threats and types of probes by attackers.
6. *Encryption*—This needs to be used in the transport layers where customer data are transported and also needs to be used in databases and any removable media. For example, advanced encryption standard (AES) can be used in databases and removable media and laptops should also use encryption in case they are stolen and end up in the wrong hands.
7. *Vulnerability management*—The purpose here is to determine where configuration policies, procedures, and processes are effective and where they are not. Vulnerability scanning can be used to identify weaknesses and provides information to be used for dealing with threats. Knowing where the vulnerabilities exist will allow the utility to use a risk-based approach to deal with and manage the vulnerabilities.

* *Securing the Smart Grid*—Tony Flick, Justin Morehouse. Syngress/Elsevier, Inc., 2011, pp. 153–159.

8. *Penetration testing*—This is used to validate the risks associated with the identified vulnerabilities and should be reviewed quarterly.
9. *Source code review*—This is the review of the software source code for vulnerabilities before the software is released. This is to be done on all software developed internally or by vendors. This is used during the software development phase (using the SDLC) to fix the vulnerable code before the software goes into production.
10. *Configuration hardening*—This is the hardening of the system before it goes into production. A hardened system image should be used to build the system as opposed to trying to harden an image supplied by a vendor. Penetration testing and vulnerability scanning then needs to be performed regularly on the hardened system images.
11. *Strong authentication*—To authorize access to a resource, two of the three authentication categories need to be used:
    - Something you know (such as a password)
    - Something you possess (such as a smart card)
    - Something you are (such as a fingerprint)

    This prevents unauthorized access when one of the two authentication categories are compromised.
12. *Logging and monitoring*—This allows for information necessary to identify attacks as well as being able to reproduce an event in case of an incident. For example, an unsuccessful log in attempts on a website can illustrate trying to break into a customer account. Logging and monitoring should be used in application, operating system (OS), and network levels and should be used on intrusion detection and prevention systems.

Privacy Practices

The following factors are some of the things that can be done to ensure customer privacy:

- Limit the collection of personal customer data. It should be collected by lawful means and with the consent of the customer.
- The data collected should be for a specific purpose and should be complete, accurate, and updated. The data collected for one purpose should not be used for another purpose.
- Those that handle the data need to comply with privacy guidelines.
- Privacy impact assessments (PIAs) need to be conducted on use of personal information or new forms of PII. PIAs should be conducted annually and a copy of the results should be provided to the State's Public Utility Commission Office for review.
- A clearly specified notice should be sent to the consumers before collection, use, retention and sharing of usage data, and personal information. This should also be employed when new data are to be collected for a specific purpose, as well as if the collected data are to be used for new purposes.
- The data should only be divulged to parties authorized to receive them.
- The customers should be allowed to see their personal data and should be able to request correction of any inaccuracies.
- The data should only be linked with a location or a customer's account when used for billing, certain operation needs, or for restoring the service.
- The data need to be protected from loss, theft, unauthorized access, disclosure, use, copying, or modification.
- Privacy policy statements should be made available to the consumers.

Conclusion

The customer, utility company, and environmental benefits of evolving to a smart grid further outweigh the security challenges that these networks present. The requirements and adherence for compliance do not always equate to security, and 100% secure networks are not an achievable goal. But, following sound security practices and managing the risk to an acceptable level are prudent and the industry's goal is not on compliance but on preserving national security given the vulnerabilities, threats, and potential attacks that will become apparent.

References

Bakken, D., Hauser, C., Bose, A., Gjermundrød, H., Dionysiou, I., Johnson, R., Jiang, P., Sheshadri, S., and Swenson, K. 2003. Grid stat. Washington State University, School of Electrical Engineering and Computer Science, November 2003.

Evron, G. 2010. Stuxnet: An amateur's weapon. *Dark Reading.com*, October 15.

Flick, T., Morehouse, J. 2011. *Securing the Smart Grid*. Syngress/Elsevier, Inc.

Kingsbury, A. 2010. A "smart" electrical grid could secure the energy supply. *U.S. News and World Report*, April 7.

Further Reading

Abel, A. 2004. Government activities to protect the electric grid. *Congressional Research Service Report for Congress*, October 20.

Bain, B. 2010. House moves to protect grid from cyber threats. *Federal Computer Week*, June 10.

Bindra, A. 2010. Securing smart grid from cyber attacks. Smart-grid.tmcnet.com, August 4.

Bockman, A. 2010. An irksome tale: The battle to secure the smart grid. *Huffington Post*, 1–2, September 19.

Chari, N. 2010. Securing the smart grid. Tropos Networks, September 26.

Cisco Systems. 2009. Securing the smart grid. White Paper.

Coleman, K. 2010. Protecting the smart grid from cyber attack. Defensetech.org, June 17

Condon, S. 2009. Senators aim to protect electric grid from hackers. *Cnet News*, 1–2, April 30.

Coney, L. 2010. Privacy perspective on protecting the grid and consumer data topic: Smart grid cyber security and privacy. *Smart Grid Policy Summit*, 1–17, April 8.

Dark Reading. 2010. Landis+Gyr and Safenet team for smart grid security. *Dark Reading.com*, October 20.

Echols, M. and Sorebo, G. 2010. Protecting your smart grid. *Transmission and Distribution World*, 1–2, July 1.

Edison Electric Institute. 2010. *EEI Principles for Cyber Security and Critical Infrastructure Protection*. September 9. www.eei.org.

Evron, G. 2010. Stuxnet: An amateur's weapon. *Dark Reading.com*, October 15.

Federal Energy Regulatory Commission. 2010. Smart grid standards adoption: Staff update and recommendation. Item No. A-3, July 15.

Fehrenbacher, K. 2009. Securing the smart power grid from hackers. *Bloomberg Businessweek*, 1, March 23.

Gunther, E. 2008. DNP secure authentication—Essential to smart grid progress. *Smartgridnews.com*, November 18.

Higgins, K.J. 2010. Stuxnet heralds new generation of targeted attacks. *Dark Reading.com*, September 23.

International EMP Council. H.R. 2195: Critical electric infrastructure protection. www.empcouncil.org.

IO Active. 2009. IO Active verifies critical flaws in next generation energy infrastructure. Press release, March 23. www.ioactive.com.

Luallen, M. 2009. Securing a smarter grid: Risk management in power utility networks. A SANS White Paper, 1–17, October.

Mantooth, H.A. 2010. How can we protect the smart grid? *Connected Planet*, 1, May 4.

Mark, R. 2008. Electrical grid exposed to cyber-threats. *E-week*, 1–4, September 12.

Mills, E. 2010. Securing the smart grid. *Cnet News*, 1–5, April 9.
National Institute of Standards and Technology. 2001. Security requirements for cryptographic modules. FIPS Pub 140-2, May 25.
National Institute of Standards and Technology. 2010. Smart grid cyber security strategy and requirements. Draft NISTIR 7628. Smart Grid Interoperability Panel, Cyber Security Working Group. February.
North American Electric Reliability Corporation. n.d. Reliability standards for the bulk electric systems of North America. Critical Information Protection Standards.
Oracle, 2010. Protecting the electric grid in a dangerous world. Oracle White Paper, 1–17, April.
Phys.org. 2010. Dartmouth researchers help secure the power grid. January 26. www.physorg.com.
Science Daily, 2006. Securing America's power grid. *Science Daily*, June 26.
Swanson, S.A. 2010. Securing the smart grid. *Scientific American*, 1–2, May 13.
TD World, 2010. DOE announces latest efforts to address cybersecurity. *Transmission and Distribution World*, 1–2, September 24.
U.S. Federal Energy Regulatory Commission. 2009. Smart Grid Policy—128 FERC 61,060. 18 CFR, Chapter 1, July 16.
U.S. House of Representatives. 2009. H.R. 2195, 111th Congress, 1st session, April 20.
U.S. House of Representatives. 2010. Grid Reliability and Infrastructure Defense Act—H.R. 5026. 111th Congress, 2nd Session, April 14, 2010; *Congressional Record*, 1–12, June 9.
Wikipedia. Smart grid. http://en.wikipedia.org/wiki/smart_grid.
Wikipedia. Stuxnet. http://en.wikipedia.org/wiki/stuxnet.
Wikipedia. Unified smart grid. http://en.wikipedia.org/wiki/unified_smart_grid.

Network Attacks and Countermeasures

Chapter 2

Attacks in Mobile Environments*

Noureddine Boudriga

Contents

Basic Attacks 24
Class of Illicit Use Attacks..... 24
Wireless Spoofing 24
Man-in-the-Middle Attacks 25
Denial of Service Attacks 25
Distributed DoS Attacks in Mobile Communications..... 26
Targeted Environments 27
Defending against DDoS Attacks..... 28
Mobile Malware 29
Basics on Malware 29
Examples of Mobile Malware.....31

The threats to mobility space are increasing significantly and having far greater impacts on users and organizations alike. In many ways, we face problems in mobility space security similar to what was experienced at the initial stages of the Internet. There are vast and evolving levels of communication options, growth in the number and diversity of applications, and rapidly evolving platforms where security vulnerabilities explode disproportionately year after year.

One of the reliable methods for securing systems is understanding the threats, vulnerabilities, and the systems that you are seeking to secure. Knowing more about the types of attacks and threats and employing better tactics will help in troubleshooting the security challenges with mobility.

Basic Attacks

Basic attacks can be classified into four major classes, namely illicit use, wireless spoofing, man-in-the-middle attacks, and denial of service attacks. A description of the features of the basic attacks is given as follows.

Class of Illicit Use Attacks

Illicit use is a passive attack that does not cause damage to the physical network. It involves an attacker that is close to an access point (AP) (or base station [BS]) and obtains information extracted from the traffic the attacker has exposed. Illicit use includes the following attacks:

- *Wireless network sniffing:* When wireless packets traverse the air, attackers equipped with appropriate devices and software can capture them. The sniffing attack methods include the following:
  - *Passive scanning:* This attack aims at listening to each wireless communication channel and copying the traffic flowing through it, for future analysis. It can be done without sending information and can use some tools such as the radio frequency (RF) monitors, which allow copying frames on a channel.
  - *Identity detection:* This attack consists of retrieving the identity of important entities occurring in a wireless network (such as the identity of the AP, in a wireless LAN [WLAN]) by scanning specific frames such as the frames of the following types: beacon, probe requests, probe responses, association requests, and reassociation requests.
  - *MAC address collection:* To construct spoofed frames, the attacker has to use legitimate MAC addresses. These addresses can be utilized for accessing active AP by filtering out the frames with nonregistered MAC addresses.
- *Probing and network discovery:* This attack aims at identifying various wireless targets. It uses two forms of probing: active and passive. Active probing involves the attacker actively sending probe requests with no identification using the Service Set Identifier (SSID) configured to solicit a probe response with SSID information (and other information) from any active AP. When an attacker uses passive probing, he listens on all channels for all wireless packets.
- *Inspection:* The attacker can inspect network information using tools such as Kismet and Airodump. He could identify MAC addresses, IP address ranges, and gateways.

Wireless Spoofing

The spoofing intent is to modify identification parameters in data packets for different purposes. Typical spoofing attacks include the following:

- *MAC address spoofing:* MAC spoofing aims at changing the attacker's MAC address to a legitimate MAC address. This attack is easy to launch because some client-side software allows the user to manipulate his MAC addresses.
- *IP spoofing:* IP spoofing attempts to change the source or destination IP addresses by talking directly with the network device.
- *Frame spoofing:* The attacker injects frames with spoofed content. When the network lacks authentication, spoofed frames cannot be detected.

Man-in-the-Middle Attacks

This attack attempts to insert the attacker in the middle (MITM attack) of a communication for purposes of intercepting a client's data and modifying them before discarding them or sending them out to the real destination. To perform this attack, two steps have to be accomplished. First, the legitimate AP serving the client must be manipulated to create a "difficult to connect" scenario. Second, the attacker must set up an alternate rogue AP with the same credentials as the original for purposes of allowing the client to connect to it. Two main forms of the MITM exist: the eavesdropping and manipulation MITM attacks. Eavesdropping can be done by receiving radio waves on the wireless network, which may require sensitive antenna. Manipulation requires not only having the ability to receive the victim's data but then be able to retransmit the data after changing it.

Denial of Service Attacks

Denial of service (DoS) attacks aim at denying or degrading the quality of a legitimate user's access to a service or network resource. It also can bring down the server offering such services itself. DoS attacks can be classified into two categories:

1. *The disabling services attacks:* A DoS attacker makes use of implementation weaknesses to disable service provision. Weaknesses that are used with these attacks include buffer overflow.
2. *Resource undermining:* Undermining can be achieved by causing expensive computations, storage of state information, resource reservations, or high traffic load.

The techniques used in DoS attacks can be applied to protocol-processing functions at different layers of the communication architecture. DoS attacks can threaten the services offered to mobile users (e.g., servers offering specific information, or servers of specific companies) and the communication infrastructure itself. Especially, specific access resources such as bandwidth can represent a serious problem (since it most likely will remain a scarce resource in access networks). DoS attacks can target different network layers as explained in the following:

- *At the application layer:* DoS occurs when a large amount of legitimate requests are sent. It aims to prevent other users from accessing the service by forcing the server to respond to a large number of request transactions.
- *At the transport layer:* DoS is performed when many connection requests are sent. It targets the operating system of the victim's computer. The typical attack in this case is a SYN flooding.
- *At the network layer:* If the network allows associating clients, an attacker can flood the network with traffic to deny access to other devices. Typically, this attack is performed by allowing one among the following three tasks:
  - The malicious node participates in a route but simply drops several data packets. This causes the deterioration of the connection.
  - The malicious node transmits falsified route updates or replays false updates. These might cause route failures, thereby deteriorating performance.
  - The malicious node reduces the time-to-live field in the IP header so that packets never reach destinations since they are dropped by other nodes before destination.

- *At the data link layer:* DoS targeting the link layer can be performed as follows:
  - Since we assume that there is a single channel that is reused, keeping the channel busy in the node leads to a DoS attack at that node.
  - By inducing a particular node to continually relay spurious data so that the battery life of that node may be drained. An end-to-end authentication may prevent these attacks from being launched.
- *At the physical layer:* This kind of DoS can be executed by emitting a very strong RF interference on the operating channel. This will cause interference to all wireless networks that are operating at or near that channel.

Distributed DoS Attacks in Mobile Communications

To make DoS threats worse, attackers have developed effective tools to coordinate distributed denial of service (DDoS) attacks that can be launched and coordinated from a large number of sites, systems, and devices. A DDoS attack is distinguished from a common DoS attack by its ability to launch its actions in a distributed manner over the wireless communicating system and to aggregate these forces to create dangerous traffic. According to different reports including the annual CSI computer crime and security report, the DDoS attacks have induced large financial costs to companies in recent years. In addition, they cause damage to consumer confidence in e-commerce of impacted organizations.

There are various types of DDoS attacks. They all share the same typical structure that is depicted in Figure 2.1. The attacker, in a DDoS, first gains control of several master computers connected to the wireless network by hacking into them, for example. Then the master computers gain control of more computers (zombies) by different means. Finally, a message is sent by the attacker to synchronize all zombies to send the required traffic to the victim.

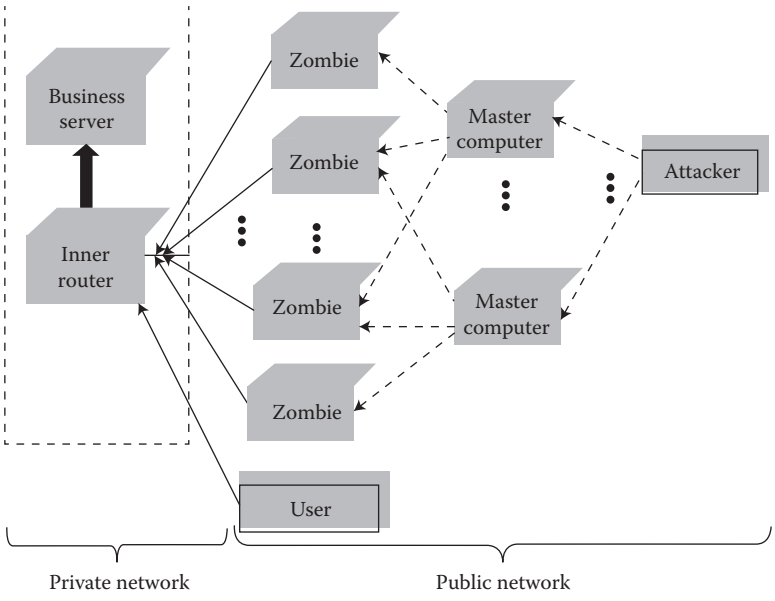

Figure 2.1 Typical DDoS structure.

In Figure 2.1, we first describe two examples of mobile systems that are targeted by DDoS attacks. Then we present some of the countermeasures that should be provided to protect against DDoS.

Targeted Environments

Two wireless communication systems are of interest to DDoS attackers, the wireless extended Internet-based networks (WEIN), where wireless technology is used only for the last mile, and the ad hoc networks (AHN), which represent, in the opinion of a large number of experts, the best architectures against DDoS attacks, since they have no central nodes and may implement severe admission policies making it very difficult for malicious users to enter into the communication infrastructure.

An example of WEIN is a network that is able to connect mobile devices to fixed networks via RF channels using the traditional Client/Server architecture and the existing transport layer protocols; for example, TCP. All the DDoS attacks achievable in the wired Internet are still feasible in the WEIN.

DDoS targeting WEIN and mobile ad hoc networks include, but are not limited to, the following attacks:

- *Attacking the wireless Internet content servers:* Since mobile devices have little computation and communication capabilities, a DDoS attack, even launched by a small number of powerful fixed terminals, can effortlessly disable a large range of mobile devices. Wireless Internet content servers, such as the WAP server, the wireless game servers, and the mail server, are often optimized for small throughput and timely response. They are particularly vulnerable to DDoS attacks compared with traditional wired servers. Furthermore, new forms of DDoS attacks may emerge taking advantage of the attractive features presented by the WEIN and ad hoc networks.
- *DDoS attacks on radio spectrum:* Often, the limited availability of radio spectrum is the bottleneck in a mobile network. Even if license-free RF bands are used and pico-cell-based (or reduced area) technologies are employed to expand transmission rates, the radio spectrum is still a scarce resource as the number of users and the demand for bandwidth is increasing tremendously. A DDoS attack can deliberately coordinate mobile devices to send out synchronized traffic to easily consume all spectrum resources or (at least) significantly reduce the capacity of any communication channel offered by the networks.
- *Attacks aiming at avoiding tracing back DDoS:* Some of the WEINs, such as the mobile IP protocol-based networks, present weaknesses that a DDoS attacker can use to launch attacks. For example, the Mobile IP protocol requires two IP addresses: the home address and the care-of address. The home address is permanently assigned to a mobile device, while the care-of address is temporarily assigned by the visiting foreign network. This allows a mobile device to send IP packets using its fixed home address, even when it is roaming, while applying the Non-Disclosure Method (NDM), which gives mobile users control over the revelation of their location information. Consequently, victim sites will find it hard to trace sources of DDoS attacks.
- *DDoS attacking devices using aggregated traffic:* Although the bandwidths used for the transmission in WEIN and ad hoc networks are much lower than those in wired networks, potential DDoS attacks are feasible mainly because of the fact that a large set of mobile devices can be involved. In particular, any wireless data packet traffic is a potential path for DDoS attacks.