Critical Infrastructure Security
Critical Infrastructure Security
Assessment, Prevention, Detection, Response

Edited by
Francesco Flammini
To Liana
# Contents

Preface ................................................................. xv

Part I  Fundamentals of Security Risk and Vulnerability Assessment

1  Model-based risk analysis for critical infrastructures ............... 3

   1  Introduction .................................................. 3
   2  The critical infrastructure problem .......................... 5
   3  Tools .......................................................... 6
   4  Multi-criterion tools (CARVER and MSRAM) ............... 8
      4.1  CARVER .................................................. 8
      4.2  MSRAM .................................................. 9
   5  CI/KR as a Network .......................................... 10
      5.1  MBRA ..................................................... 11
      5.2  KDAS ..................................................... 13
   6  Resource allocation ......................................... 14
      6.1  Network science ......................................... 15
      6.2  An illustration ........................................... 16
   7  Conclusion .................................................... 18

2  Physical vulnerability assessment .................................. 21

   1  Introduction .................................................. 21
      1.1  Terminology ............................................. 21
      1.2  What a VA is not ........................................ 22
   2  Common techniques for finding vulnerabilities ................. 23
      2.1  Security Survey .......................................... 23
      2.2  Security Audit .......................................... 23
      2.3  Design Basis Threat (DBT) ............................ 24
      2.4  CARVER Method ........................................ 25
      2.5  Delphi Method ........................................... 25
      2.6  Fault Tree Analysis ..................................... 26
      2.7  Software tools .......................................... 26
      2.8  Adversarial Vulnerability Assessments .................. 26
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>VA best practices</td>
<td>28</td>
</tr>
<tr>
<td>3.1 VA personnel</td>
<td>28</td>
</tr>
<tr>
<td>3.2 Brainstorming</td>
<td>29</td>
</tr>
<tr>
<td>3.3 Common security mistakes</td>
<td>31</td>
</tr>
<tr>
<td>3.3 The VA report: Delivering the “bad news”</td>
<td>33</td>
</tr>
<tr>
<td>Vulnerability myths and mistakes</td>
<td>34</td>
</tr>
<tr>
<td>Part II Modeling and Simulation Tools for Critical Infrastructures</td>
<td></td>
</tr>
<tr>
<td>3 Modeling and simulation of critical infrastructures</td>
<td>39</td>
</tr>
<tr>
<td>1 Introduction</td>
<td>39</td>
</tr>
<tr>
<td>2 Interdependency modeling</td>
<td>40</td>
</tr>
<tr>
<td>3 Holistic approaches</td>
<td>42</td>
</tr>
<tr>
<td>4 Critical Infrastructures as Complex Systems</td>
<td>45</td>
</tr>
<tr>
<td>4.1 Topological analysis</td>
<td>45</td>
</tr>
<tr>
<td>4.2 Functional analysis</td>
<td>47</td>
</tr>
<tr>
<td>5 Simulative approaches</td>
<td>48</td>
</tr>
<tr>
<td>5.1 Agent-based approaches</td>
<td>50</td>
</tr>
<tr>
<td>5.2 Multilayer approaches</td>
<td>51</td>
</tr>
<tr>
<td>6 Conclusions</td>
<td>52</td>
</tr>
<tr>
<td>4 Graphical formalisms for modelling critical infrastructures</td>
<td>57</td>
</tr>
<tr>
<td>1 Introduction</td>
<td>57</td>
</tr>
<tr>
<td>2 Requirements for CI modelling and simulation</td>
<td>58</td>
</tr>
<tr>
<td>3 Graphical formalisms for CI modelling and simulation</td>
<td>60</td>
</tr>
<tr>
<td>3.1 Graph-based techniques</td>
<td>60</td>
</tr>
<tr>
<td>3.2 Petri Nets (PNs)</td>
<td>61</td>
</tr>
<tr>
<td>3.3 General simulation environments</td>
<td>62</td>
</tr>
<tr>
<td>3.4 Agent-based modelling and simulation</td>
<td>62</td>
</tr>
<tr>
<td>3.5 Discussion of requirements</td>
<td>63</td>
</tr>
<tr>
<td>4 Practical experiences in modelling CIs: meeting the requirements with SAN</td>
<td></td>
</tr>
<tr>
<td>4.1 CRUTIAL and HIDENETS: a brief introduction</td>
<td>66</td>
</tr>
<tr>
<td>4.2 On the usage of SAN to match requirement R4</td>
<td>66</td>
</tr>
<tr>
<td>4.3 On the usage of SAN to match requirement R6</td>
<td>69</td>
</tr>
<tr>
<td>5 Conclusions</td>
<td>70</td>
</tr>
<tr>
<td>5 Semantic interoperability among federated simulators of critical infrastructures – DIESIS project</td>
<td>75</td>
</tr>
<tr>
<td>1 Introduction</td>
<td>76</td>
</tr>
<tr>
<td>2 Related works and initiatives</td>
<td>78</td>
</tr>
</tbody>
</table>
### 3 DIESIS project

3.1 Managerial, legal and economic features

3.2 Technical features

4 Conclusion

### 6 Game theory in infrastructure security

1 Introduction

2 Game-theoretic models
   2.1 Simultaneous AD games
   2.2 Sequential DA games
   2.3 Sequential AD games
   2.4 Sequential DAD games
   2.5 Simultaneous DD games

3 Limitations of game-theoretic models

4 Conclusion

### Part III Cybersecurity in Information and SCADA Systems

7 Modelling, measuring and managing information technology risks

1 Introduction

2 What is risk with respect to information systems?
   2.1 Threats
   2.2 Vulnerabilities

3 Why is it important to manage risk?

4 Managing risk at the organizational level

5 How is risk assessed?
   5.1 Quantitative risk assessment
   5.2 Qualitative risk assessment

6 How is risk managed?
   6.1 Strategies for managing individual risks
   6.2 High-level risk management strategies
   6.3 Communicating risks and risk management strategies

7 What are some common risk assessment/management methodologies and tools?
   7.1 NIST methodology
   7.2 OCTAVE®
   7.3 FRAP
   7.4 GRC tools

8 Summary
# 8 Trustworthiness evaluation of critical information infrastructures

1 Introduction ............................................. 125
2 Dependability and security evaluation approaches .......... 126
   2.1 A taxonomy for evaluation approaches .................. 126
   2.2 Common evaluation approaches and applications ....... 128
3 On the evaluation of Financial Infrastructure
   Protection (FIP) ......................................... 131
   3.1 FCI: Trustworthiness evaluation trends .................. 131
   3.2 FIP trustworthiness requirements and key components ... 132
   3.3 FIP example: CoMiFin as a FCI wrapper ................. 133
   3.4 Metric-based FIP trustworthiness evaluation ............. 134
4 On the evaluation of CIIP .................................. 134
   4.1 Design requirements for CIIP ............................ 135
   4.2 Peer-to-Peer (P2P)-based CIIP ......................... 136
   4.3 Mitigation strategy for node crashes ..................... 137
   4.4 Mitigation strategy for illicit SCADA data modification ................................. 137
   4.5 Evaluation of P2P-based CIIP ........................... 137
5 Conclusion ................................................ 138

# 9 Network resilience ........................................ 141

1 Introduction ............................................. 141
2 A component-based framework for improving network resilience in CIs .............................. 144
3 Intrusion detection and reaction in satellite networks ........ 146
4 Detection and remediation of a distributed attack over an IP-based network ....................... 148
5 Diagnosis-driven reconfiguration of WSNs .................... 149
6 Conclusions .............................................. 152

# 10 Wireless sensor networks for critical infrastructure protection ........................................... 155

1 Introduction ............................................. 155
2 Security threat analysis .................................... 157
   2.1 Adversary models ..................................... 157
   2.2 Risk assessment ....................................... 158
3 Survey of the state of the art ............................... 159
   3.1 Sensor node protection .................................. 159
   3.2 Dependable sensor networking ......................... 161
   3.3 Dependable sensor network services .................... 164
4 Conclusions and identification of further research topics .................................................. 165
Part IV  Monitoring and Surveillance Technologies

11 Intelligent video surveillance ................................. 177
   1 Introduction ............................................... 177
   2 Architecture of an IVS system ............................. 179
   3 Examples of applications .................................. 181
      3.1 LAICA project ......................................... 181
      3.2 THIS project ......................................... 182
      3.3 Other examples ....................................... 186
   4 Conclusions ................................................. 187

12 Audio surveillance ............................................. 191
   1 Introduction ............................................... 191
   2 Sound recognition for audio surveillance ............... 193
   3 A representative picture of the related literature ...... 197
      3.1 Evaluation of audio surveillance frameworks ....... 199
   4 Privacy ..................................................... 201
   5 Conclusion ................................................ 202

13 Terahertz for weapon and explosive detection ............. 207
   1 Introduction ............................................... 207
   2 Terahertz technology ....................................... 208
      2.1 Overview .............................................. 208
      2.2 THz systems .......................................... 209
   3 Terahertz for weapons detection ............................ 211
   4 Terahertz for explosive detection .......................... 213
   5 Discussion ................................................. 216

14 Structural health monitoring ................................. 221
   1 Introduction ............................................... 221
   2 Structural evaluation ...................................... 222
   3 Sensor selection ........................................... 223
      3.1 Accelerometers ........................................ 224
      3.2 Strain sensors ........................................ 224
      3.3 Tilt sensors .......................................... 224
      3.4 Displacement sensors .................................. 224
      3.5 Corrosion sensors ..................................... 225
      3.6 Fiber Bragg Gratings (FBGs) .......................... 226
      3.7 Acoustic emission sensors ............................. 227
      3.8 Additional technologies ............................... 227
15 Networks of simple sensors for detecting emplacement of improvised explosive devices ........................................ 233

1. Introduction ........................................................................ 233
2. Clues to IED emplacement .................................................. 234
   2.1 Cameras versus nonimaging sensors ................................. 234
   2.2 Prior probabilities for emplacement ................................. 235
   2.3 Anomalous behavior .................................................... 238
   2.4 Goal changing and coordinated activity ......................... 239
3. Sensor management .......................................................... 241
4. Experiments ....................................................................... 242
5. Conclusions ....................................................................... 244

Part V Security Systems Integration and Alarm Management

16 Security systems design and integration ................................. 249

1. Introduction ........................................................................ 249
2. The intrusion detection system ............................................ 250
   2.1 Sensors ......................................................................... 251
   2.2 Internal sensors .......................................................... 253
   2.3 External sensors .......................................................... 254
3. The access control system .................................................... 255
4. The video surveillance system ............................................. 257
5. The communication network .............................................. 260
6. Integration of security systems: The supervision and control system .................................................. 263
7. Conclusions ....................................................................... 265

17 Multisource information fusion for critical infrastructure situation awareness ........................................ 267

1. Introduction ........................................................................ 267
2. Joint Directors of Laboratories (JDL) data fusion process model .................................................. 268
3. Comments on the state of the art ........................................ 270
4. Human-centric information fusion ..................................... 271
5. Implications for infrastructure situation awareness ............. 274
6. Summary ........................................................................... 274
18 Simulation-based learning in the physical security industry ........ 279
   1 Introduction ................................................................. 279
   2 Simulation overview .................................................... 279
   3 Security simulation ...................................................... 280
   4 Security simulation domains ........................................... 280
      4.1 Computation simulators ........................................... 280
      4.2 Interactive simulation ............................................ 282
   5 Simulation in a training environment ................................. 283
      5.1 Systematic approach to training for simulation ............. 284
   6 Interactive simulators and simulation learning theory ........... 287
      6.1 Learning retention .................................................... 288
   7 Security simulation and vulnerability assessment .................. 289
   8 Historical adoption curve of use of simulators ................. 289
   9 Conclusion ................................................................. 291

19 Frameworks and tools for emergency response and crisis management ............................ 293
   1 Introduction ................................................................. 293
   2 CATS ................................................................. 294
      2.1 CATS architecture ................................................... 294
      2.2 Model descriptions ................................................... 296
      2.3 Consequence assessment ........................................... 298
   3 Summary and conclusions ............................................ 301
Preface

The security of critical infrastructures is a paramount issue in modern society. In fact, infrastructures like those for transportation, energy, telecommunication, banking, etc. whose operability is essential for the well-being of a large number of individuals are nowadays exposed to severe threats, both natural (earthquakes, landslides, flooding, etc.) and intentional (thefts, vandalism, terrorism, etc.). In recent years, the scientific community has addressed the issue of Critical Infrastructure Security (CIS) through conferences, journals and other publications. However, in most cases, the published material fails to address the CIS issue as a multi-faceted and multi-disciplinary problem which needs to be analysed in an integrated manner both at the organizational and technological levels, and looking at digital (“cyber”) as well as physical security.

The purpose of this book is to provide a comprehensive picture of the state-of-the-art and trends in methods and tools for infrastructure protection, focusing on the following topics:

- **Assessment**, that is the understanding of risks and vulnerabilities as well as expected results of possible mitigations. This can be achieved by analysis, modelling and simulation.

- **Prevention**, that is the reduction of risk by predicting threat effects. This can be achieved by means of deterrence and other “passive” countermeasures (e.g. security by design).

- **Detection**, that is the capability of real-time recognition of abnormal conditions or behaviours. This can be achieved by means of “active” sensors and other technological tools.

- **Response**, that is the quick reaction to threats. This can be achieved by adopting early warning, situational awareness and decision support systems.
Most of the current best practices are based on intrusion detection/access control, people scanning and video surveillance designs which are often weak and poorly effective since they are not rigorous enough and frequently not systematically guided by risk analysis principles. This book provides the necessary balance between the analysis aspects, which involve people (personnel, operators, adversaries, etc.) taking into account organizational and interdependency effects, and the technological tools (smart-detectors, information networks, control software, etc.), which are required to implement modern integrated surveillance and security management systems. Therefore, the topics presented in the volume progress smoothly from security evaluation methods and tools to security enhancement approaches and technologies.

It is the Editor’s belief that the book provides the most up to date compendium of Critical Infrastructure Security and he is grateful to all authors for their excellent contributions.

The Editor, 2012