Spis treści

Słowo wstępne **9**

1. PLC PRIME w systemach zdalnego odczytu **11**

1.1. Wprowadzenie 12
1.2. Charakterystyka PLC PRIME 12
1.3. Warstwa fizyczna PLC PRIME 14
1.4. Warstwa MAC PLC PRIME 14
1.5. Adresowanie urządzeń 15
1.6. Zabezpieczenia 16
1.7. Warstwa konwergencji 17
1.8. Aktualizacja oprogramowania sprzętowego 18
1.9. Podsumowanie 19

2. Zastosowanie standardu Wi-Fi w systemach AMR **21**

2.1. Wprowadzenie 22
2.2. Moduł komunikacyjny Wi-Fi 25
2.3. Konfiguracja transmisji 30
2.4. Podsumowanie 31

3. Technologia GSM w metodach zdalnego odczytu liczników energii elektrycznej **33**

3.1. Metody zdalnego odczytu 34
3.1.1. Sieci PLC/PLD 34
3.1.2. Dedykowane łącza teletechniczne i telefoniczne 35
3.1.3. Modemy radiowe, a w szczególności ZigBee 35
3.1.4. Technologia GSM 36
3.2. System zdalnego odczytu wykorzystujący technologię GSM 37
3.3. Podsumowanie 43

4. Ochrona danych pomiarowych oraz przeciwdziałanie atakom na liczniki energii **45**

4.1. Wprowadzenie 46
4.2. Uwarunkowania prawne ochrony danych pomiarowych w Polsce 47
4.3. Bezpieczeństwo danych w systemach pomiarowych energii elektrycznej 48
4.3.1. Bezpieczeństwo danych w licznikach elektromechanicznych 48
4.3.2. Bezpieczeństwo danych w licznikach mikroprocesorowych 49
4.3.3. Bezpieczeństwo danych w inteligentnych systemach pomiarowych 51

4.4. Wybrane zagrożenia dla danych pomiarowych w inteligentnych systemach pomiarowych energii elektrycznej 52
4.4.1. Zagrożenia w procesie identyfikacji 52
4.4.2. Zagrożenia w procesie uwierzytelniania 53
4.4.3. Zagrożenia w procesie autoryzacji 54
4.5. Współczesne zagrożenia dla sieci energetycznych 55
4.5.1. Wojna energetyczna, wojna informacyjna 55
4.5.2. Wojna informacyjna w energetyce 56
4.5.3. Jakich cyberataków na infrastrukturę pomiarową należy się spodziewać? 57
4.6. Wnioski 58

5. Rozproszony system do kryptoanalizy szyfrów opartych na krzywych eliptycznych 61

5.1. Wstęp 62
5.2. Kryptografia oparta na krzywych eliptycznych 62
5.2.1. Krzywe eliptyczne 62
5.2.2. Elementy kryptosystemu 63
5.2.3. Algorytm *rho* Pollarda 63
5.3. Środowisko OpenCL 65
5.4. System do kryptoanalizy ECC 65
5.4.1. Serwer 65
5.4.2. Klient 66
5.4.3. Komunikacja klient-serwer 67
5.5. Implementacja systemu 67
5.5.1. Płaszczyzna sterowania 67
5.5.2. Płaszczyzna obliczeniowa 68
5.6. Testy systemu 70
5.6.1. Weryfikacja funkcjonalna 70
5.6.2. Testy wydajności 71
5.7. Podsumowanie 71

6. Ochrona własności intelektualnej projektów w układach FPGA poprzez szyfrowanie danych konfiguracyjnych 73

6.1. Wprowadzenie 74
6.2. Układy FPGA 74
6.3. Układy sterowania 75
6.4. Projektowanie w technologii układów FPGA 77
6.5. Szyfrowanie danych konfigurujących układ FPGA 79
6.5.1. Tworzenie zaszyfrowanych danych konfiguracyjnych 80
6.5.2. Instalacja klucza szyfrującego 80

6.5.3. Wgrywanie zaszyfrowanych danych konfiguracyjnych 80
6.5.4. Zasilanie wydzielonej pamięci 81
6.6. Przykład projektu z szyfrowaniem danych 81
6.6.1. Opis procesu obróbczego 81
6.6.2. Działanie sterownika – ujęcie formalne 82
6.6.3. Praca z dedykowanym oprogramowaniem CAD 83
6.7. Podsumowanie 84

7. Bezpieczeństwo w systemach Smart Grid na przykładzie projektu e-balance 87

7.1. Wprowadzenie 88
7.2. Projekt *e-balance* *89*
7.3. Aspekty prawne i socjalne 90
7.4. Architektura systemu *e-balance* *92*
7.5. Ochrona prywatności i bezpieczeństwa danych 96
7.5.1. Zabezpieczenie urządzeń i komunikacji 96
7.5.2. Zabezpieczenie danych prywatnych 97
7.6. Podsumowanie 98

8. Projekt SMARTIE: bezpieczeństwo, prywatność i poufność w zarządzaniu danymi w inteligentych miastach 99

8.1. Wprowadzenie 100
8.2. Projekt SMARTIE 100
8.3. Bezprzewodowe sieci sensorów 102
8.4. Proponowane rozwiązanie 103
8.4.1. *tinyDSM* *103*
8.4.2. *shortECC* *104*
8.4.3. Symbioza *tinyDSM* i *shortECC* *106*
8.4.4. Ewaluacja proponowanego rozwiązania 108
8.5. Podsumowanie 109

9. Systemy monitorowania energii w zarządzaniu przedsiębiorstwem 111

9.1. Zarządzanie energią w przedsiębiorstwach 112
9.1.1. Systemy zarządzania energią (SZE) wg PN-EN ISO 50001 113
9.1.2. Audyt przedwdrożeniowy 115
9.1.3. Rola systemów monitorowania strumieni energii w systemach SZE 115
9.1.4. Systemy monitorowania energii w usługach w formule ESCO 116
9.2. Zarządzanie przedsiębiorstwem 117
9.2.1. Zarządzanie produkcją poprzez energochłonność 118
9.2.2. Organizacja ucząca się 119

9.3. Przykłady wykorzystania systemów monitorowania energii 120
9.3.1. Przypadek 1 120
9.3.2. Przypadek 2 120
9.3.3. Przypadek 3 121
9.4. Podsumowanie 121

10. System monitoringu i zarządzania zużyciem energii elektrycznej 123

10.1. Wprowadzenie 124
10.2. Monitoring jako inwestycja 124
10.3. Struktura, elementy systemu 125
10.4. Realizacja systemu monitoringu 127
10.5. Podsumowanie 130

11. Aplikacje internetowe w obliczu ataków sieciowych na przykładzie CodeIgniter Framework 133

11.1. Wprowadzenie 134
11.2. Podstawowe definicje 134
11.2.1. Atak *brute-force* i słownikowy 134
11.2.2. *Web Parameter Tampering* 134
11.2.3. *SQL Injection* 135
11.2.4. *Cross Site Scripting* (XSS) 135
11.2.5. *Cross Site Request Forgery* (CSRF lub XSRF) 136
11.3. Platforma programistyczna CodeIgniter 136
11.4. Ataki internetowe a CodeIgniter 137
11.4.1. *SQL Injection* 137
11.4.2. *Cross Site Scripting* (XSS) 138
11.4.3. *Cross Site Request Forgery* (CSRF lub XSRF) 139
11.5. Podsumowanie 140

12. Modelowanie wymagań bezpieczeństwa w procesach biznesowych w chmurze 141

12.1. Wstęp 142
12.2. Chmura obliczeniowa 142
12.3. Bezpieczeństwo 143
12.3.1. *Compliance* 143
12.3.2. *Enterprise security* 143
12.4. System wspomagający bezpieczeństwo danych 144
12.4.1. Projekt PREsTiGE 144
12.4.2. Zarys architektury systemu wspomagającego bezpieczeństwo danych 144

12.5. Modelowanie wymagań bezpieczeństwa 146
12.5.1. Wymagania bezpieczeństwa 147
12.5.2. Języki modelowania wymagań bezpieczeństwa w BPMN 148
12.6. Podsumowanie 149

13. A new pseudo-random number generator based on the irrationality of some numbers 151

13.1. Pseudo-random sequences and their generators 152
13.2. Pseudo-random generators based on the expansion of a real number in positional number systems 153
13.2.1. Rational approximations of an irrational number 154
13.2.2. Rational approximations of $\sqrt{N}$ 156
13.2.3. The $\sqrt{N}$-algorithm 157

14. On elliptic curve point compression 161

14.1. Introduction 162
14.2. Point compression on elliptic curves 162
14.2.1. The Montgomery ladder 163
14.2.2. Point compression using elliptic curves over rings 166
14.3. Backgrounds on pairings 167
14.3.1. Useful facts for efficient implementation 170
14.4. Computing pairings on elliptic curves using *x*-coordinates only 172

15. Malware – a survey on threats and mitigation techniques 177

15.1. Introduction 178
15.2. Malware definitions 178
15.3. Motivation 179
15.4. Malware classification 181
15.5. The lifecycle 183
15.6. Malware detection 184
15.7. Detection evasion techniques 187
15.8. Summary 188

16. Aspekty prawne wykorzystania nowych technologii w celu bezprawnego skopiowania danych z kart płatniczych 193

16.1. Wstęp 194
16.2. Pojęcie karty płatniczej, karty debetowej oraz karty kredytowej 195
16.3. Pojęcie *skimmingu* 196
16.4. Kwalifikacja karty płatniczej jako przedmiotu czynności wykonawczej

przestępstwa 197
16.4.1. Karta płatnicza jako inny środek płatniczy 197
16.4.2. Karta płatnicza jako dokument....198
16.5. Budowa aparatury badawczej 199
16.5.1. Budowa modułu NFC 200
16.5.2. Procedura instalacyjna karty 201
16.5.3. Sposób zbierania pomiarów 202
16.5.4. Wyniki 202
16.5.5. Wykorzystanie zdobytych danych....203
16.6. Przebieg *skimmingu* *204*
16.6.1. Uwagi ogólne 204
16.6.2. Pobieranie danych z kart wyposażonych w moduły NFC 205
16.7. Pobieranie danych ze *skimmera* 206
16.8. Zapobieganie zjawisku *skimmingu* 206
16.9. Odpowiedzialność wystawcy karty płatniczej 206
16.10. Uwagi końcowe....208

17. Aktualne i przyszłe rozwiązania prawne w zakresie rozwiązań technicznych stosowanych przy przetwarzaniu danych pomiarowych 211

17.1. Wstęp....212
17.2. Aktualne rozwiązania prawne w zakresie danych pomiarowych....212
17.2.1. Obowiązek wdrożenia inteligentnych sieci....212
17.2.2. Wspólnotowe postulaty w zakresie ochrony prywatności w inteligentnych sieciach 213
17.2.3. Regulacje prawne w zakresie ochrony danych pomiarowych w Polsce 216
17.3. Projektowane regulacje w zakresie ochrony danych pomiarowych 220
17.3.1. Nowe ramy ochrony danych osobowych w Unii Europejskiej i regulacje w zakresie cyberbezpieczeństwa....220
17.3.2. Plany wdrożenia inteligentnych sieci w Polsce....221
17.4. Podsumowanie 223