Bytestream in the bloodstream

(nie)bezpieczeństwo urządzeń i systemów medycznych

Maciej Chmielarz

maciej@chmielarz.it

O mnie

@MaciejChmielarz

maciej@chmielarz.it

O mnie

maciej@chmielarz.it

Pompy insulinowe

- 2011, Jay Radcliffe (pracownik IBM i cukrzyk) prezentuje na konferencji Black Hat zdalne przejęcie kontroli nad pompą
- Analizował własną pompę i czujniki ciągłego monitoringu glukozy (CGM) firmy Medtronic
- Źródłem informacji była instrukcja obsługi (częstotliwość, modulacja, długość pakietu), dokumenty dla FCC, patenty producenta
- Użył Arduino, układu Texas Instruments CC1101 i oscyloskopu

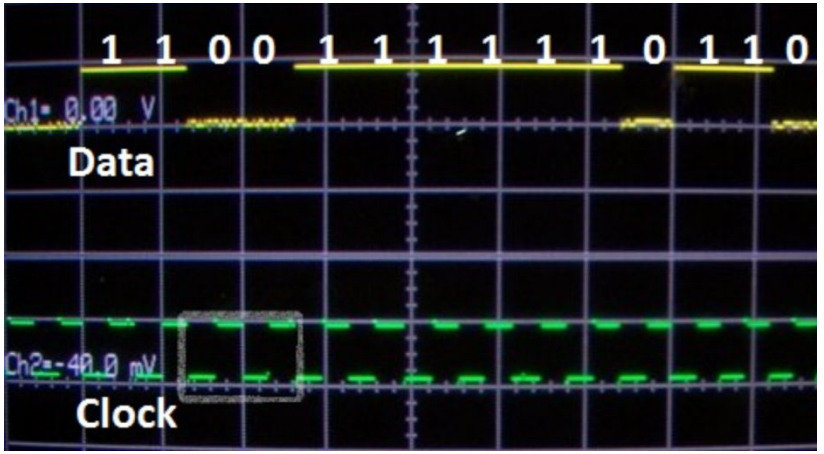
Pompa Medtronic

Źródło: Jay Radcliffe [1], fot. Medtronic

maciej@chmielarz.it

Pompy insulinowe

- Aplikacja Java do konfiguracji pompy nie była zabezpieczona przed inżynierią wsteczną (brak zaciemnienia kodu), ujawniła metodę kodowania, format wiadomości, kody poleceń
- Programator do pompy, używany < $100 na eBay, nowy można kupić bez recepty w sklepie medycznym



Źródło: Jay Radcliffe [1]

Pompy insulinowe

Możliwe ataki na czujniki CGM:

- Zagłuszanie rzeczywistych odczytów
- Przesłanie fałszywych odczytów:
  - Replay attack
  - Spoofing

Możliwe ataki na pompy insulinowe:

- Zmiana ustawienia dawki insuliny dla wymiennika węglowodanowego

Źródło: Jay Radcliffe [1], fot. Medtronic

maciej@chmielarz.it

Pompy insulinowe

- Październik 2016, Rapid7 ujawnia raport nt. systemu One Touch Ping
- Zidentyfikowane podatności:
  - Komunikacja otwartym tekstem
  - Parowanie ustanawia stały „klucz” CRC32 do wzajemnej identyfikacji
  - Brak potwierdzania odebrania wiadomości
  - Brak zabezpieczeń przed replay attack
- Październik 2017, Johnson & Johnson ogłasza wycofanie z biznesu pomp insulinowych

Zestaw Animas One Touch Ping

Źródło: Rapid7 R7-2016-07 [2], fot. Animas

maciej@chmielarz.it

Pompy infuzyjne

- Jesień 2013, Billy Rios uczestniczy w badaniach w Mayo Clinic
- Prywatnie kupuje pompę Hosipra, zdalnie przejmuje kontrolę
- Wiosna 2014, pisze raport do DHS, przekazany dalej do FDA
- Lato 2015, leży w szpitalu podłączony do pompy infuzyjnej ;)
- Przesyła ponaglenie, wideo i exploit
- Lato 2015, FDA wydaje rekomendację wycofania modelu

Hospira Symbiq

Źródło: Bloomberg Businessweek [3], fot. Hospira

maciej@chmielarz.it

Pompy infuzyjne

- Rekomendacja: jak najszybsze przejście na alternatywne systemy
- W międzyczasie…
  - Odłączyć od sieci (konieczne manualne aktualizowanie danych w pompach)
  - Upewnić się, że nieużywane porty są zamknięte, w tym 20/FTP i 23/TELNET
  - Monitorować i logować cały ruch sieciowy na portach 20/FTP, 23/TELNET i 8443
  - Skontaktować się ze wsparciem technicznym Hospira w celu zmiany domyślnego hasła dostępu do portu 8443 lub zamknąć go

Źródło: FDA [4]

Pompy infuzyjne

- Hospira MedNet – centralne zarządzanie pompami i dawkowaniem
- Informacje od pomp w systemie – żądania HTTP zabezpieczone CRC
- Niewidoczne konto backdoor *hospira_admin* z hasłem 12345678
- Konta sa do serwera SQL z hardkodowanymi hasłami typu H0sp1ra!!!
- Na urządzeniach uruchomione serwery przyjmujące żądania HTTP (np. w celu zmiany dawkowania) zabezpieczone CRC
- Kod do generowania sum kontrolnych na Githubie ;)

Źródło: Billy Rios [5], fot. Hospira

Pompy infuzyjne

Komentarz Pfizer (właściciel Hospira) dla mediów:

- Podstawową obroną przeciwko ingerowaniu w urządzenia medyczne są szpitalne systemy informatyczne i bezpieczne firewalle
- Zabezpieczenia w pompach infuzyjnych to dodatkowa warstwa bezpieczeństwa

Źródło: komentarz Pfizer

maciej@chmielarz.it

Pompy infuzyjne

- Wrzesień 2017, rekomendacja ICS-CERT dot. podatności wykrytych przez Scotta Gayou w pompach Smiths Medical Medfusion 4000
- Podatności możliwe do wykorzystania zdalnie, wśród nich:
  - Kopiowanie bufora bez sprawdzenia wielkości (buffer overflow) 3P
  - Czytanie pamięci spoza zakresu (crash modułu komunikacji) 3P
  - Użycie hardkodowanych danych dostępowych (Wi-Fi, FTP, Telnet)
  - Nieprawidłowa walidacja certyfikatu (MitM)
  - Brak uwierzytelniania serwera FTP
  - Hasła w pliku konfiguracyjnym
- Aktualizacja ma być w styczniu 2018

Smiths Medical Medfusion

Źródło: DHS ICS-CERT [6], fot. Smiths Medical

maciej@chmielarz.it

Rozruszniki serca

- 2008, analiza bezprzewodowego interfejsu krótkiego zasięgu wszczepialnego kardiowertera serca Medtronic Maximo
- Komunikacja tekstem jawnym, możliwość podsłuchania prywatnych danych pacjenta i danych telemetrycznych
- Podtrzymanie transmisji danych telemetrycznych przez replay attack
- 24 powtórzone wiadomości wyłączyły wszystkie „terapie”
- Co najmniej 3 z 30 powtórzonych wiadomości włączyły test migotania komór impulsem ok. 137 V
- Programator ma zabezpieczenie ;)

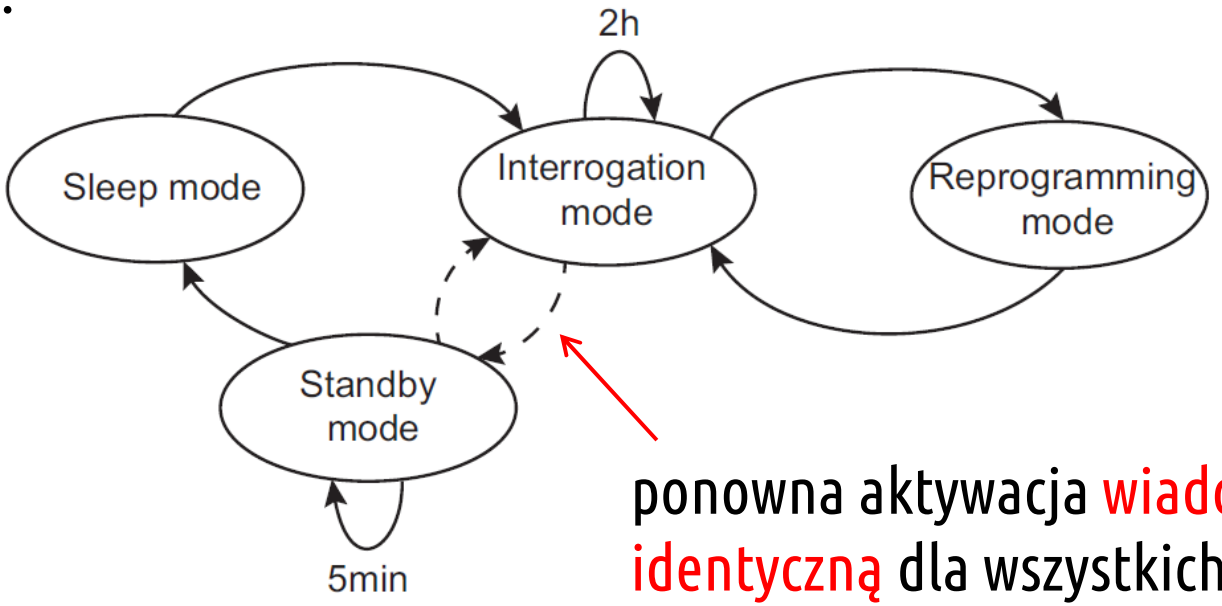
Medtronic Maximo

Źródło: University of Massachusetts Amherst [7], fot. Medtronic

maciej@chmielarz.it

Rozruszniki serca

- 2016, analiza interfejsów urządzeń nieujawnionej marki
- Zestaw trzech urządzeń: kardiowerter, programator, stacja bazowa
- Komunikacja krótkiego i długiego zasięgu (centymetry i metry)
- 4 tryby:

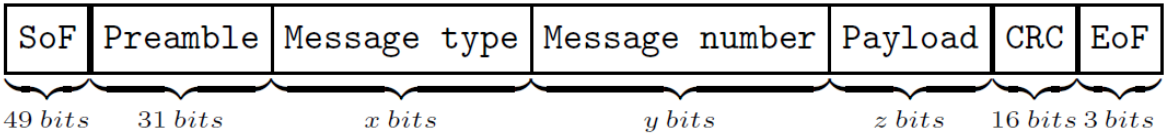


ponowna aktywacja wiadomością identyczną dla wszystkich urządzeń

Źródło: Katholieke Universiteit Leuven [8]

Rozruszniki serca

- Format wiadomości programatora:



- Nie są przesyłane tekstem jawnym – komunikacja zabezpieczona (!)

```
(d) "AAAA"          00101011 11101000 01101001 01111101
(e) LFSR seq  ⊕     01001010 10001001 00001000 00011100
                    --------------------------------------
(f) ASCII           01100001 01100001 01100001 01100001
                        A        A        A        A
```

- Algorytm „szyfrowania” to LFSR XOR, klucz ten sam dla każdego urz.
- Numery wiadomości resetowane dla każdej sesji
- Integralność zabezpieczona standardowym CRC-16-CCITT

Źródło: Katholieke Universiteit Leuven [8]

Rozruszniki serca

Zagrożenia:

- Prywatność (słabe „szyfrowanie”):
  - Dane pacjenta (dane osobowe, historia leczenia)
  - Numer seryjny urządzenia (śledzenie pacjentów)
  - Dane telemetryczne (bieżąca informacja o stanie zdrowia)
- Podtrzymanie aktywności:
  - Rozładowanie baterii (Denial of Service)
  - Po wyjściu od lekarza lub po przerwaniu komunikacji ze stacją bazową
- Fałszywe wiadomości (brak uwierzytelniania):
  - Replay attack
  - Spoofing

Źródło: Katholieke Universiteit Leuven [8]

Rozruszniki serca

- Kwiecień 2016, Abbott Labs ogłasza przejęcie St. Jude Medical za 25 mld $
- Sierpień 2016, firma inwestycyjna Muddy Waters ujawnia podatności wykryte przez startup MedSec
- Styczeń 2017, Abbott Labs dokonuje przejęcia St. Jude Medical
- Sierpień 2017, FDA zaleca aktualizację rozruszników przy najbliższej kontrolnej wizycie lekarskiej

NYSE:STJ

⬇10%

Merlin@home

Źródło: inf. medialne, FDA [9], fot. St. Jude Medical

maciej@chmielarz.it

Rozruszniki serca

- Badaczka bezpieczeństwa Marie Moe ma rozrusznik od 2012 roku
- Lekarze zaskoczeni pytaniami o potencjalne podatności
- Nikt nie poinformował pacjentki o interfejsach bezprzewodowych
- Przez błąd w oprogramowaniu puls zmniejszał się nagle ze 160 do 80
- Brak dostępu do kodu, własność intelektualna producenta
- Projekt hakowania rozruszników – kupione na eBay i podarowane

Źródło: Wired [10]

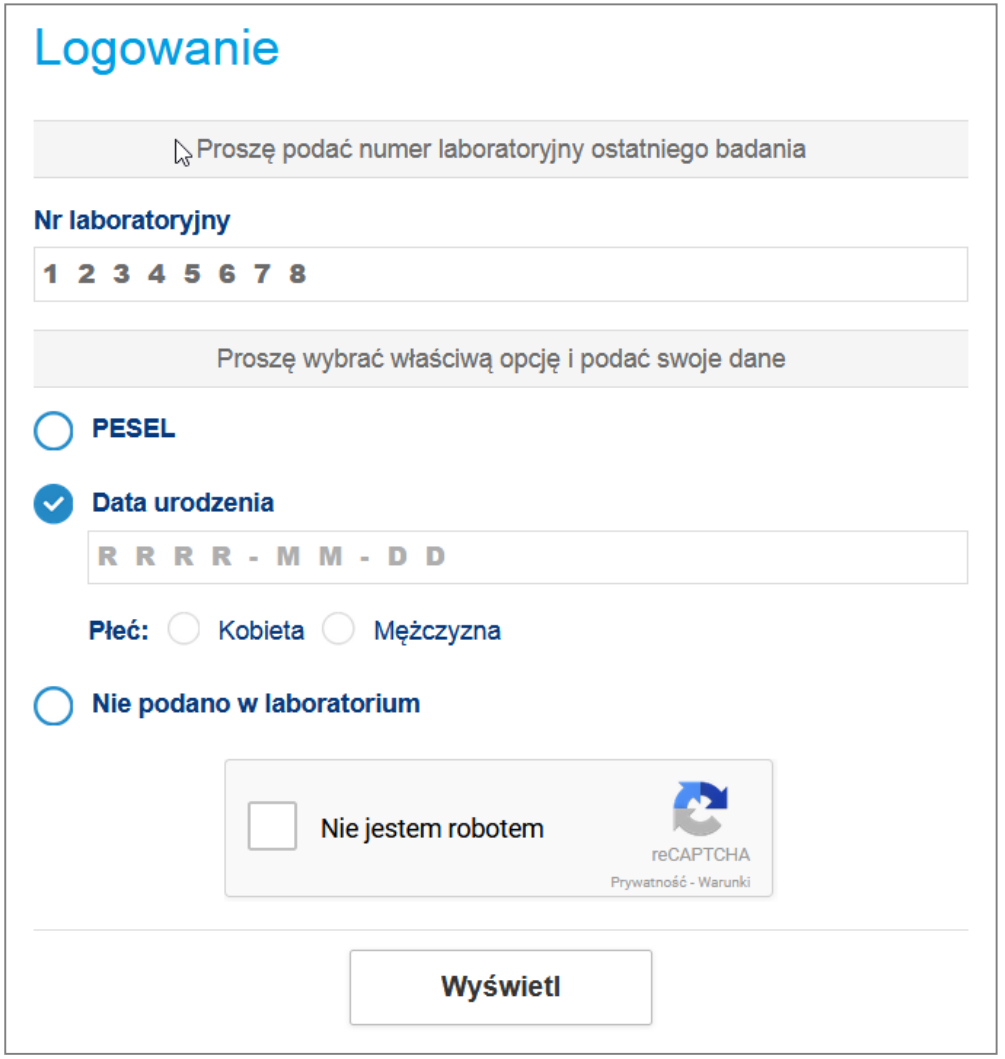
Tomografy komputerowe

- Sierpień 2017, rekomendacja ICS-CERT dot. podatności wykrytych w tomografach komputerowych Siemens z systemem Windows 7
- Cztery podatności możliwe do wykorzystania zdalnie
- Zdalne wykonanie kodu przez:
  - Wstrzyknięcie kodu przez żądanie HTTP do Microsoft Web Server na porcie 80 lub 443 oraz HP Client Automation Service na porcie 3465
  - Wykonanie kodu poza granicą buforu pamięci przez żądanie do HP Client Automation Service
  - Wykonanie kodu bez uprawnień przez żądanie do HP CAS

Siemens CT

Źródło: DHS ICS-CERT [11], fot. Siemens

Laboratoria medyczne




```
$('input[name="nr_lab"]').change(function () {
    var nr = $(this).val();
    if (nr.length < 8) {
        $('input[type="radio"]').iCheck('disable');
    } else if (nr.length == 8) {
        $('input[name="wybor"]').iCheck('enable');
    } else {
        $(this).val(nr.substring(0, 8));
    }
});
$('input[name="nr_lab"]').keyup(function () {
    $(this).change();
});
$('input[name="nr_lab"]').change();
```

- Czy nr laboratoryjny da się przewidzieć?
- Czy wystarczy dla sprawdzenia wyniku?

Źródło: opracowanie własne

maciej@chmielarz.it

Laboratoria medyczne

Źródło: opracowanie własne

maciej@chmielarz.it

Laboratoria medyczne

- Dla trzech osób numery laboratoryjne były w zakresie czterech liczb
- Wszyscy dokonaliśmy pełnej rejestracji i opcja „Nie podano w laboratorium” zwracała informację „Wynik niegotowy”
- Sprawdzenie wyniku było możliwe po podaniu numeru laboratoryjnego oraz daty urodzenia
- Czy to wystarczające zabezpieczenie?

Źródło: opracowanie własne

maciej@chmielarz.it

Ransomware / malware

- Szpitalne sieci komputerowe nie są „kuloodporne”:
  - Grudzień 2011, Gwinnett Medical Center, Lawrenceville (USA), atak malware
  - Luty 2016, Hollywood Presbyterian Medical Center, LA, atak ransomware
  - Marzec 2016, Baltimore's Union Memorial Hospital (USA), atak ransomware
  - Kwiecień 2017, Erie County Medical Center, Buffalo (USA), atak ransomware
  - Maj 2017, NHS w Anglii i Szkocji, atak ransomware WannaCry
  - Sierpień 2017, NHS Lanarkshire (Szkocja), atak ransomware

Źródło: inf. medialne

maciej@chmielarz.it

Opóźniony dostęp

- 2017, wpływ maratonów na losy pacjentów kardiologicznych
- Dane zbierane w latach 2002-2012, 11 maratońskich miast
- Transport karetką dłuższy średnio o 4 min 24 sek (32%)
- 30-dniowa śmiertelność wyższa o 3,3 punktu procentowego

Źródło: The New England Journal of Medicine [12], fot. Adrian Grycuk CC-3.0

maciej@chmielarz.it

I Am The Cavalry

Źródło: I Am The Cavalry [13]

maciej@chmielarz.it

Koszty badań

- Niektóre urządzenia słabo dostępne, drogie (MRI) lub wymagają pozwoleń (rentgen)
- Używane pompy infuzyjne na eBay < $100
- Możliwe pozyskanie za darmo do badań
- Udostępnianie na konferencjach

Źródło fot.: WhiteScopeIO [14]

Bibliografia

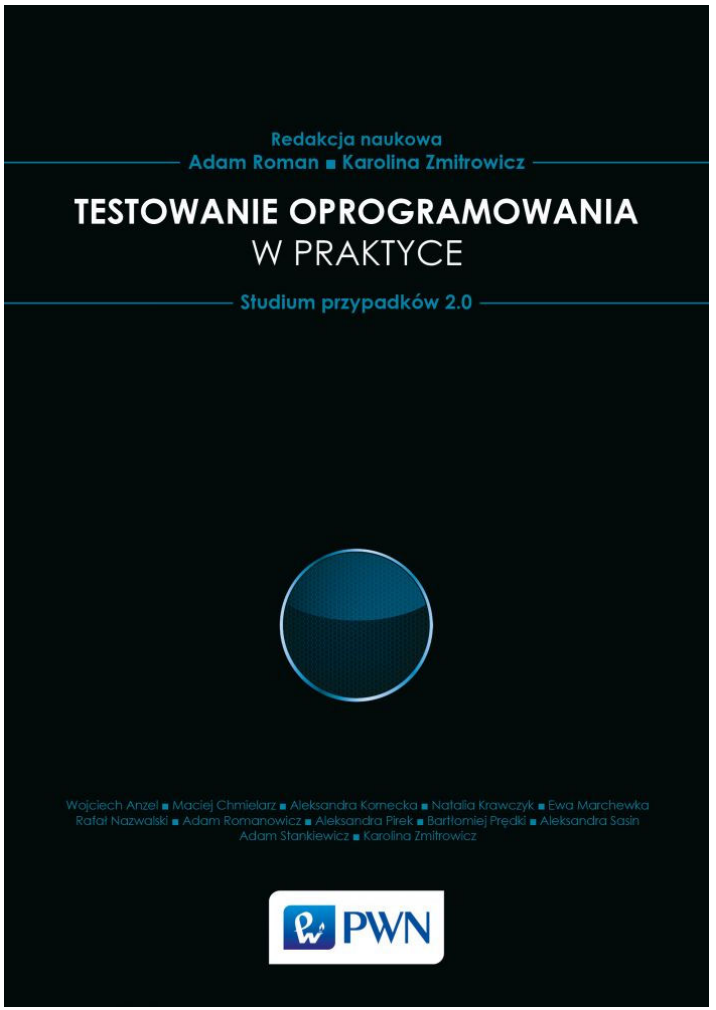
1. Jerome Radcliffe - Hacking Medical Devices for Fun and Insulin: Breaking the Human SCADA System
   https://media.blackhat.com/bh-us-11/Radcliffe/BH_US_11_Radcliffe_Hacking_Medical_Devices_WP.pdf
2. R7-2016-07: Multiple Vulnerabilities in Animas OneTouch Ping Insulin Pump
   https://blog.rapid7.com/2016/10/04/r7-2016-07-multiple-vulnerabilities-in-animas-onetouch-ping-insulin-pump/
3. Bloomberg Businessweek - It's Way Too Easy to Hack the Hospital
   https://www.bloomberg.com/features/2015-hospital-hack/
4. Symbiq Infusion System by Hospira: FDA Safety Communication - Cybersecurity Vulnerabilities
   https://www.fda.gov/safety/medwatch/safetyinformation/safetyalertsforhumanmedicalproducts/ucm456832.htm
5. Billy Rios - Infusion Pump Teardown
   https://www.youtube.com/watch?v=pq9sCaoBVOw
6. Smiths Medical Medfusion 4000 Wireless Syringe Infusion Pump Vulnerabilities
   https://ics-cert.us-cert.gov/advisories/ICSMA-17-250-02
7. Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses
   http://scholarworks.umass.edu/cgi/viewcontent.cgi?article=1067&context=cs_faculty_pubs
8. On the (in)security of the Latest Generation Implantable Cardiac Defibrillators and How to Secure Them
   https://www.esat.kuleuven.be/cosic/publications/article-2678.pdf

maciej@chmielarz.it

Bibliografia

9. Firmware Update to Address Cybersecurity Vulnerabilities Identified in Abbott's (formerly St. Jude Medical's) Implantable Cardiac Pacemakers
   https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm573669.htm
10. Go Ahead, Hackers. Break My Heart.
    https://www.wired.com/2016/03/go-ahead-hackers-break-heart/
11. Siemens Molecular Imaging Vulnerabilities
    https://ics-cert.us-cert.gov/advisories/ICSMA-17-215-02
12. Delays in Emergency Care and Mortality during Major U.S. Marathons
    https://www.ncbi.nlm.nih.gov/pubmed/28402772
13. Anatomy of a Medical Device Hack
    https://www.youtube.com/watch?v=FnvcocyI4pI
14. Understanding Pacemaker Systems Cybersecurity
    http://blog.whitescope.io/2017/05/understanding-pacemaker-systems.html

maciej@chmielarz.it



maciej@chmielarz.it

@MaciejChmielarz