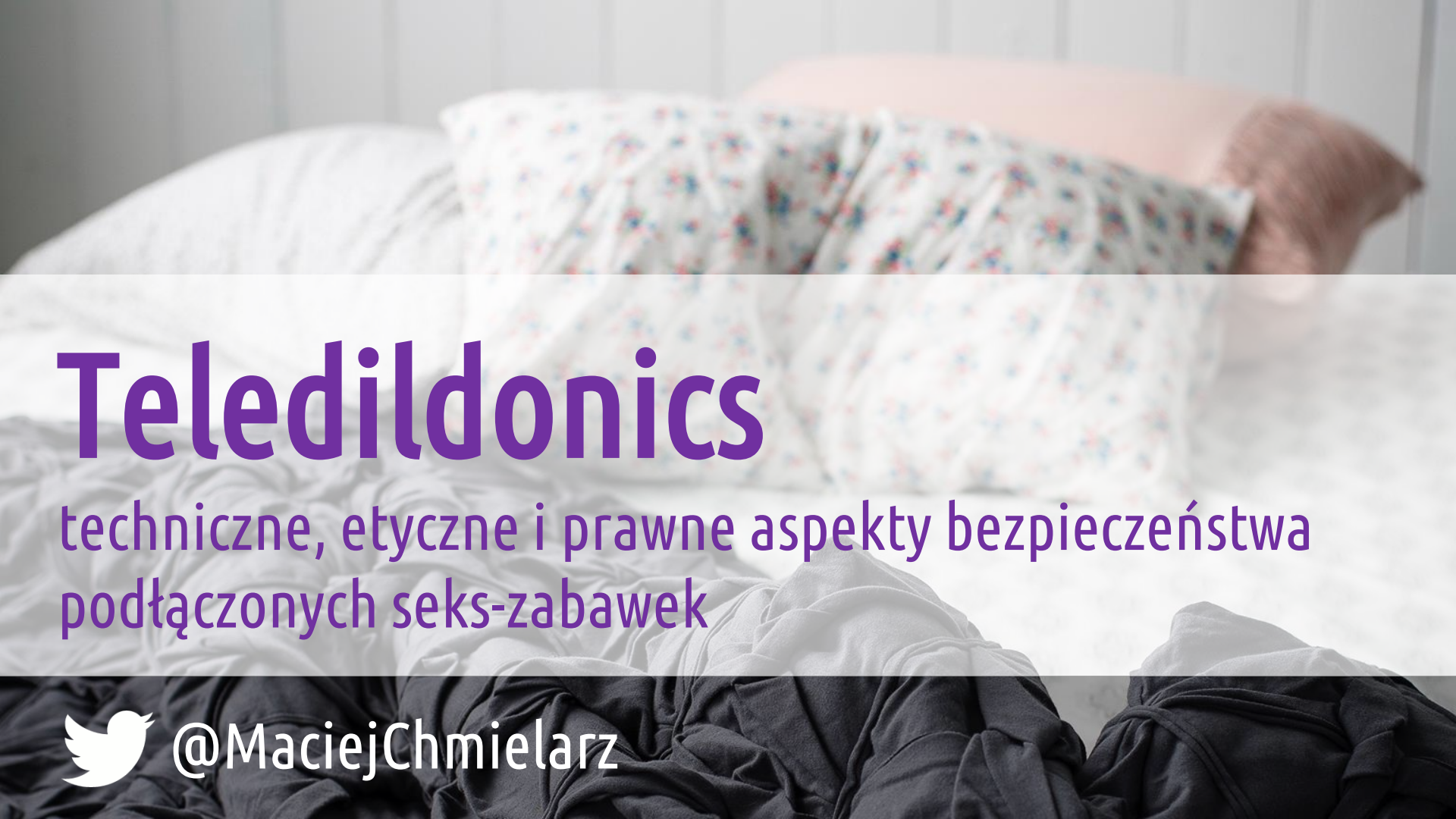


Teledildonics

techniczne, etyczne i prawne aspekty bezpieczeństwa podłączonych seks-zabawek

@MaciejChmielarz

Tamagotchi

maciej@chmielarz.it

Gululu

Fot. materiały producenta

maciej@chmielarz.it

Gululu

maciej@chmielarz.it

maciej@chmielarz.it

We-Vibe

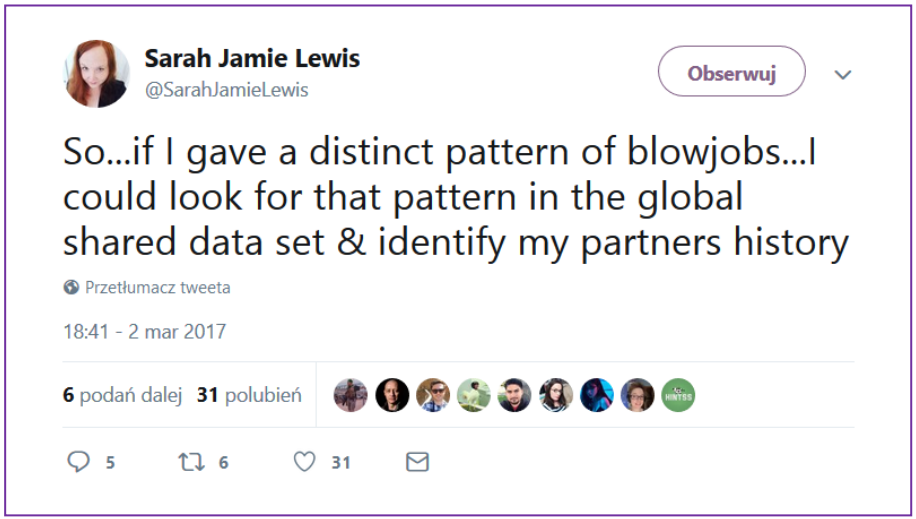
- 2016, DEF CON, g0ldfisk & follower
- Dane przesyłane na serwery We-Vibe:
  - Temperatura urządzenia (co minutę)
  - Tryb i intensywność wibracji (przy zmianie)
- 3,75 mln $ odszkodowania w ramach ugody w procesie zbiorowym

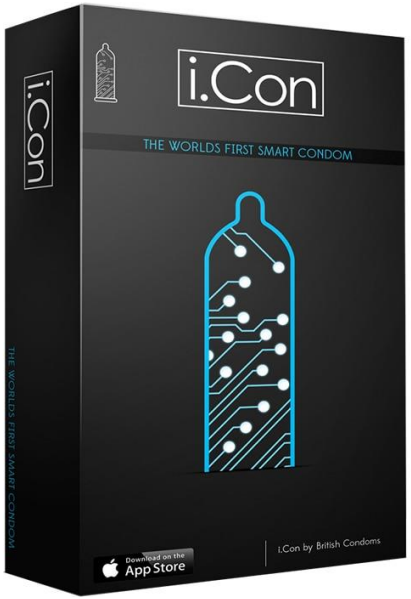
Fot. materiały producenta

maciej@chmielarz.it

i.Con

- Zbiera dane na temat aktywności seksualnej użytkownika

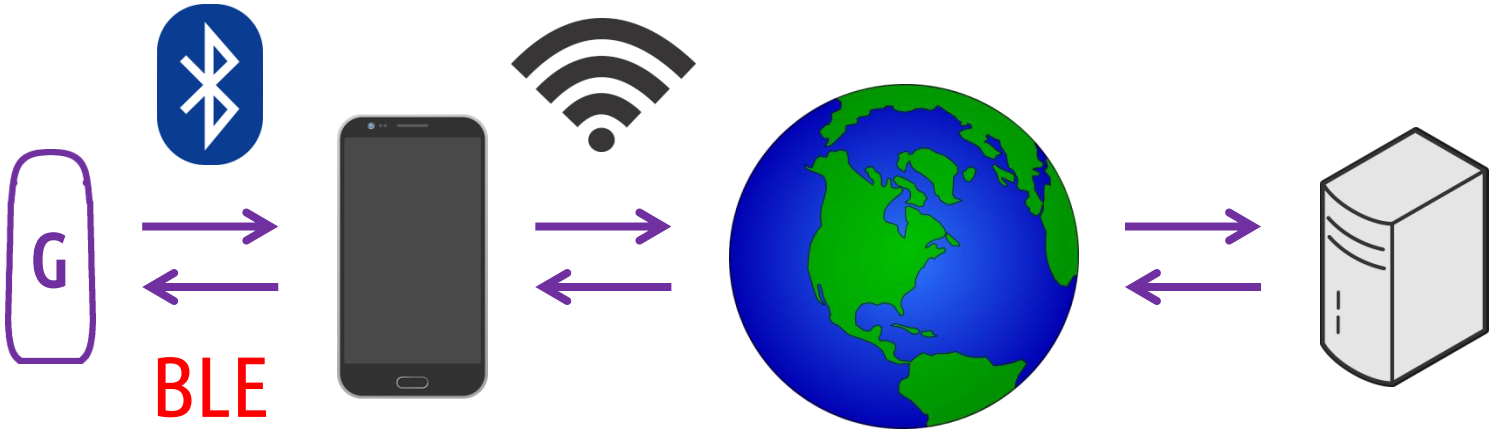




Źródło: materiały producenta

maciej@chmielarz.it

Połączenie



maciej@chmielarz.it

Lovense

- Niezabezpieczone połączenie BLE
- Przejęcie kontroli nad urządzeniem
  - 2017.09, PenTestPartners, BLE sniffing
  - 2017.10, merlos, dekompilacja APK
- Bagatelizowane przez producenta

Fot. materiały producenta

maciej@chmielarz.it

Vibratissimo

- Niezabezpieczone połączenie BLE
- Przejęcie kontroli nad urządzeniem
  - 2018.02, SEC Consult, BLE sniffing
- Dużo więcej problemów po stronie backendu i aplikacji mobilnej

Fot. materiały producenta

maciej@chmielarz.it

Art. 191. § 1.

Kto stosuje przemoc wobec osoby lub groźbę bezprawną w celu zmuszenia innej osoby do określonego działania, zaniechania lub znoszenia, podlega karze pozbawienia wolności do lat 3.

maciej@chmielarz.it

Art. 197. § 2.
Kto przemocą, groźbą bezprawną lub podstępem doprowadza inną osobę do poddania się innej czynności seksualnej (...), podlega karze pozbawienia wolności od 6 miesięcy do lat 8.

maciej@chmielarz.it

Vibratissimo

- 2018.02, SEC Consult
- Problemy po stronie backendu:
  - Jawne dane dostępowe do bazy danych
  - Dostępny na zewnątrz phpMyAdmin
  - Hasła przechowywane tekstem jawnym

Fot. materiały producenta

maciej@chmielarz.it

Vibratissimo

- 2018.02, SEC Consult
- Problemy po stronie aplikacji mobilnej:
  - Żądania uwierzytelnione loginem i hasłem (TLS)
  - Zdjęcia dostępne bez autoryzacji (DOR)
  - Przewidywalne linki do „szybkiej kontroli” (liczba), bez potwierdzenia
  - Reflected XSS w linkach do „szybkiej kontroli”

Fot. materiały producenta

maciej@chmielarz.it

DEMO

maciej@chmielarz.it

Dziękuję za uwagę

@MaciejChmielarz maciej@chmielarz.it