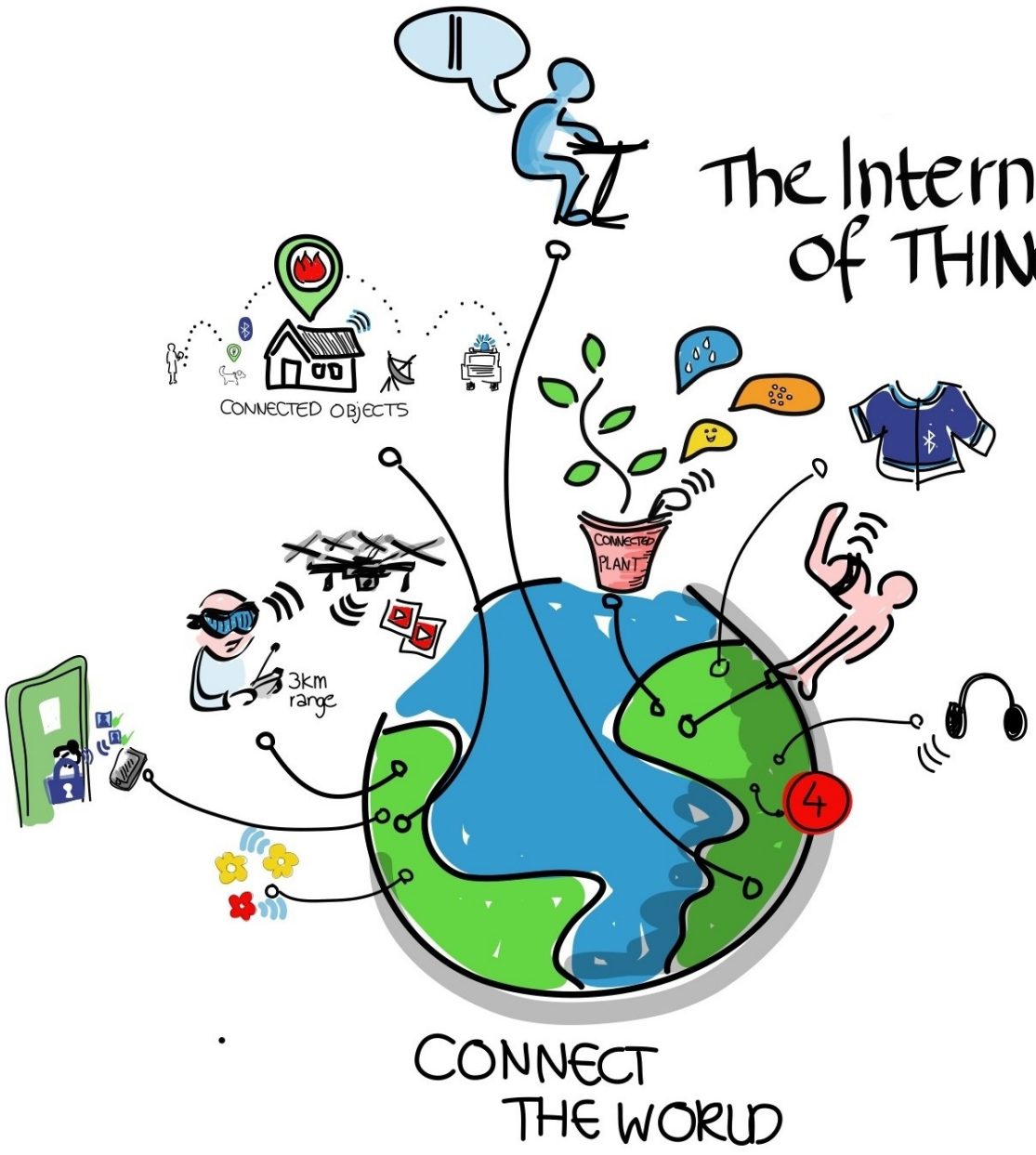
dr inż. Michał Grobelny

INTELIGENTNE URZĄDZENIA I MASZYNY – MOŻLIWOŚCI I ZAGROŻENIA

Internet przedmiotów

- Internet of Things (IoT)
- Internet of Everything (IoE) – Cisco
- Globalna sieć urządzeń wzajemnie się komunikujących bez ingerencji człowieka, wykorzystująca różne technologie komunikacji oraz nowoczesne sensory, kamery, oprogramowanie, bazy i centra danych



źródło: wikipedia.org

Obszary zastosowań

- inteligentne budynki
- samoprowadzące się pojazdy
- sprzęt gospodarstwa domowego
- aparatura medyczna
- urządzenia multimedialne i rozrywkowe
- monitorowanie środowiska i otoczenia
- komunikacja publiczna
- odzież i wiele innych

Stan obecny

- moda
- duży entuzjazm
- pokładane nadzieje
- popularność
- niepełne zabezpieczanie systemów inteligentnych
- kompetencje i świadomość użytkowników

Pierwszy cyberatak z IoT

Masowe rozsyłanie spamu odkryte przez Proofpoint, Inc.:

- 26 grudnia 2013 - 6 stycznia 2014
- 750 000 wiadomości (SPAM)
- użycie 100 000 urządzeń „inteligentych”:
  - domowe rutery
  - urządzenia multimedialne (multi-media center)
  - telewizory
  - co najmniej jedna lodówka

Prognozy

- w 2008 roku liczba urządzeń podłączonych do Internetu przekroczyła liczbę ludności
- w 2013 roku według Cisco podłączonych do Internetu było 13 miliardów urządzeń
- urządzenia i przedmioty podłączone do sieci w 2020 roku:
  - 26 miliardów według Gartnera
  - 50 miliardów według Cisco
  - ponad 200 miliardów według szacunków IDC

Aspekty techniczne

- bezpieczeństwo danych
- skuteczne mechanizmy ochronne
- mała moc obliczeniowa i niski pobór energii
- bezpieczna komunikacji
- blokada usług (DoS)
- unifikacja protokołów
- komunikacja bez udziału człowieka

Aspekty techniczne

- budowa fizyczna rozwiązań
- zastępowalność urządzeń
- autoryzacja i identyfikacja
- wykradnięcie konfiguracji
- klonowanie i podmiana urządzeń
- ingerencja w oprogramowanie
- aktualizacje

Aspekty społeczne

- bezpieczeństwo otoczenia i użytkowników
- kontekst danych i ich korelacja
- wypieranie człowieka przez urządzenia
- zanikanie umiejętności
- permanentna obserwacja
- uzależnienie od urządzeń
- użytkownik kontra system
- nowe sposoby komunikacji i izolacja

Czy jesteśmy gotowi na Internet przedmiotów?

Potencjalne korzyści

- wygoda
- odciążenie człowieka
- bezpieczniejsze otoczenie
- większa kontrola
- pogłębiona wiedza
- spontaniczna sieć komunikacyjna w sytuacji kryzysowej

Samokierujące się samochody

- zwiększenie bezpieczeństwa
- komunikacja car-to-car
- absurdy drogowe
- nowoczesny złodziej = haker
- uprawnienia organów ścigania
- blokada dróg bez udziału człowieka
- jedno kliknięcie do zablokowania floty
- odpowiedzialność prawna

Ochrona zdrowia

- aparatura medyczna i czujniki w ubraniu
- monitorowanie stanu pacjenta 24/7/365
- dostęp lekarza do danych
- automatyczne powiadamianie w sytuacjach kryzysowych
- informacje o stanie zdrowia i kondycji w niepowołanych rękach
- rozrusznik serca vs haker

Inteligentne budynki

- znaczne podniesienie komfortu mieszkania i pracy
- ekologia
- zdalne sterowanie domem lub biurem
- blokada usług
- prywatność zależna od algorytmu
- praca systemu a zagrożenie życia
- zmiana parametrów pracy

Urządzenia codziennego użytku

- automatyzacja życia
- lodówka inteligentna inaczej
- wszystkowiedząca toaleta
- co może mieć to wspólnego z ubezpieczeniem zdrowotnym?
- problem aktualizacji i jej zdalnego wykonania

Bezpieczeństwo firmy/instytucji i Internet przedmiotów

- inteligentne budynki
- wykorzystanie służbowe a prywatne
- włamanie do infrastruktury firmowej przez toster pracownika
- bezpieczeństwo danych firmowych
- służbowy pojazd samoprowadzący
- przenikanie się światów

Powszechność IoT problemem

- systemy dedykowane dla przeciętnego Kowalskiego
- konieczność masowej interakcji urządzeń i wymiany informacji
- jak odróżnić swojego od obcego
- bezpieczeństwo sensorów na polu, ulicy czy w centrum handlowym

Zaufanie do produktu

- coraz bardziej uzależniamy się od urządzeń inteligentnych pomimo, że coraz mniej wiemy o sposobie ich budowy i działania
- problem „time-to-market”
- klient testerem
- najłatwiej pozbyć się funkcji i rozwiązań, których nie widać

Jak pogodzić

bezobsługowość

(skrajną prostotę obsługi),

swobodę komunikacyjną

i

bezpieczeństwo?

Inteligentne urządzenia i maszyny –
możliwości i zagrożenia

dr inż. Michał Grobelny

DZIĘKUJĘ ZA UWAGĘ