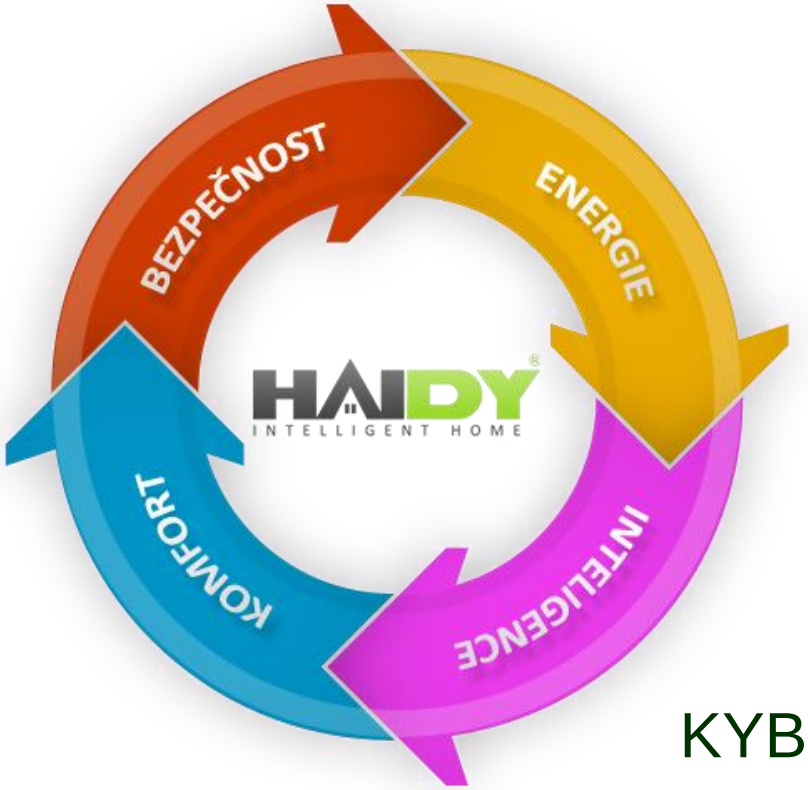


KYBERPSYCHO 2015

Tomáš Poláček
HAIDY a.s.

Internet věcí – přínosy versus rizika

- Aktuální stav internetu věcí (z pohledu uživatelů, z pohledu technologie)
- Možnosti dalšího vývoje v oblasti internetu věcí (HW, SW)
- Odpovědnost uživatele za své prvky IoT (autonomní rozhodování) – právní pohled
- Ochrana soukromí uživatele
- Bezpečnost prvků internetu věcí
- Osobní velký bratr (automatizace okolí uživatele) a korporátní velký bratr
- Jak může uživatel ovlivnit svoji bezpečnost

Aktuální stav internetu věcí

- Z pohledu uživatelů:
- Uživatel se bojí neznámého a má pocit, že bude nucen novou technologii využívat
- Obava o ztrátu soukromí (že internet věcí předá intimní data třetím stranám)
- Nechuť učit se novým věcem, obava o zhoršení bezpečnosti
- Lednice, kávovar - užitečnost vs. zbytečnost? (otázky smysluplnosti internetu věcí)
- Spotřební elektronika je často nespolehlivá (mrzne, zdržuje, přestává fungovat)

- Z pohledu technologie:
- Smart City (doprava, senzorové sítě – monitoring pohybu, spotřeby energie, parkování)
- Automatizace domácnosti (úspory energie, komfort, bezpečnost)
- Autonomní prvky (náramky, smartphone)
- Slepá ulička (time to market vs. kvalita produktu)
- Na výrobcích je úkol přinést produkty, které jsou smysluplné pro širokou veřejnost

Možnosti dalšího vývoje

- V současnosti jsme obklopeni velmi malým množstvím senzorů, toto se v blízké budoucnosti výrazně změní.
- Technologický pokrok – miniaturizace a integrace elektronických prvků (například akcelerometr + procesor + vysílač v jednom čipu)
- Neustálé snižování ceny prvků umožní monitorovat i drobné předměty jako je zubní kartáček nebo obalové materiály potravin.

- Co můžeme očekávat v blízké budoucnosti:

- Vzájemné informační propojení mezi následujícími prvky:

  mobil, boty, kolo, automobil, MHD, nábytek/byt/dům, budovy, město, obaly potravin

  Příklad: Dopravní nehoda, automobil vyhledá nejbližší osobu s kurzem první pomoci...

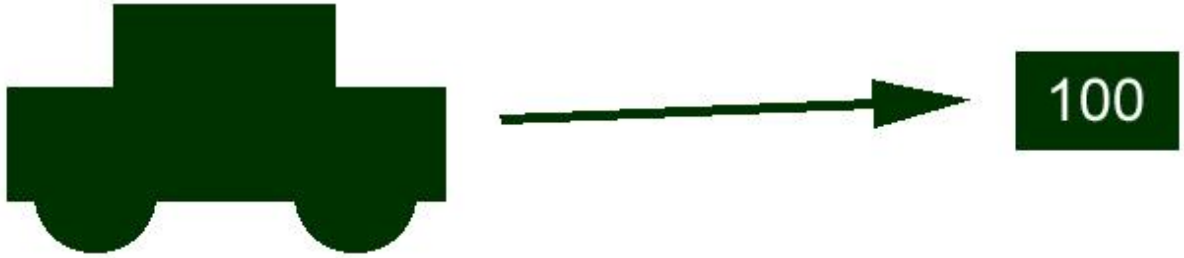
Odpovědnost za své prvky IoT

- Právní pohled na odpovědnost za autonomní rozhodování prvků IoT

- Autonomní rozhodování má několik logických vrstev:
  1. Uživatelská konfigurace (podmínkové akce) – zodpovědnost uživatele za nastavení
  2. Software uživatelského rozhraní
  3. Software měření a regulace
  3. Operační systém
  4. Hardware (senzory – přesnost a spolehlivost)

Ochrana soukromí uživatele

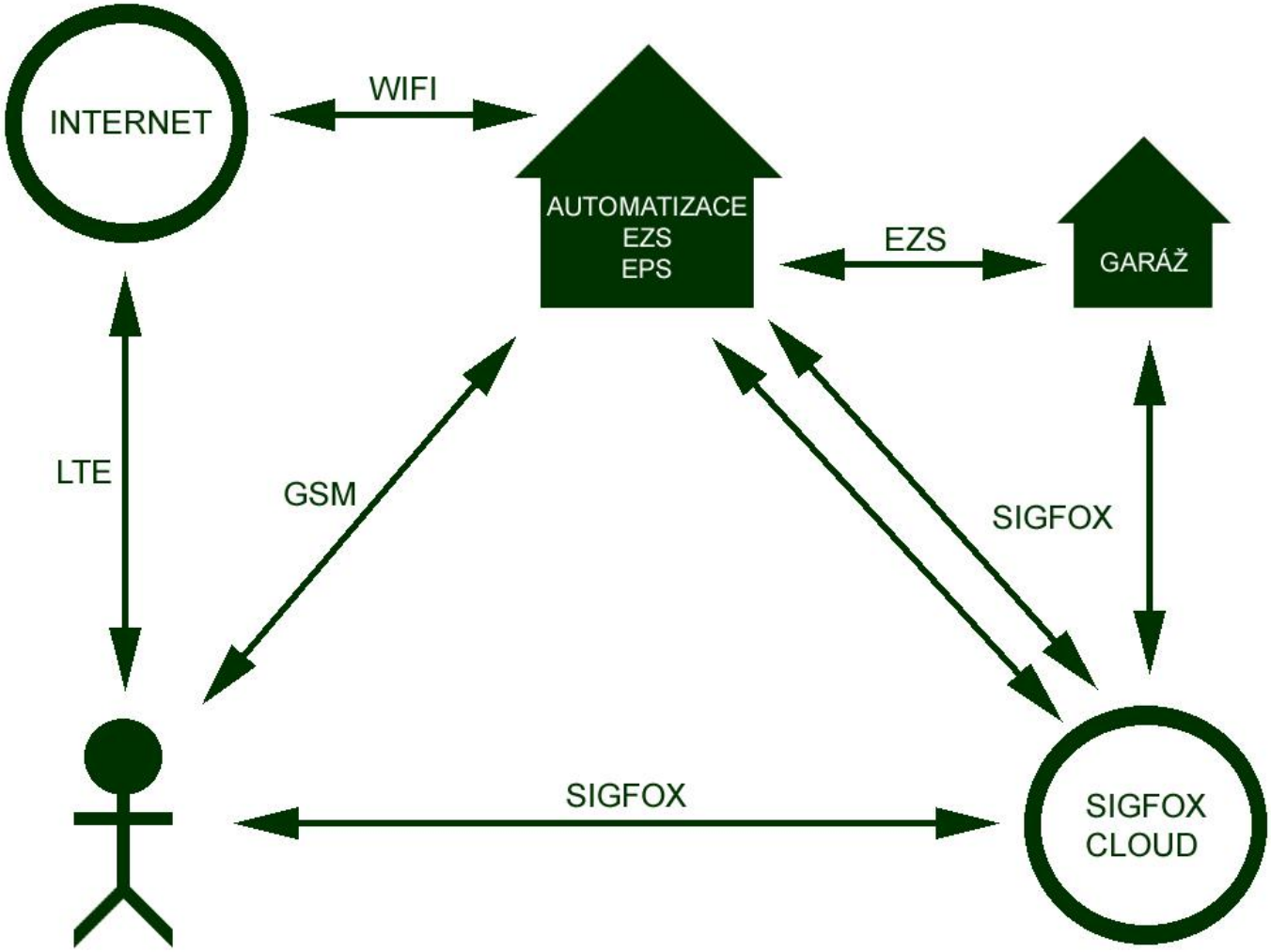
- Vývoj hardwaru s důrazem na eliminaci možných zadních dvířek
- Rozhodování může být na lokální úrovni (data se nemusí dostat do cloudu)
- Kde je hranice soukromí vs. bezpečnosti společnosti?! (chceme zadní dvířka?)
- Příklad: Automobil – sledování stylu jízdy autem, dopad na výši povinného ručení



Bezpečnost prvků internetu věcí

- Nejrozšířenější systémy budou nejvíc zajímavé pro hackery (miliony domů)
- I malé prvky internetu věcí můžou disponovat asymetricky šifrovanou komunikací
- Žádné vzdálené připojení není 100% bezpečné
- Diverzitní kanály a prvky umělé inteligence můžou výrazně zvýšit bezpečnost (např. auto se bude rozhodovat, komu umožní odjet)

HAIDY = Systém inteligentního bydlení



Velký bratr

- Korporátní velký bratr
- Cloud velkých korporací (e-mailové servery, sociální sítě a pod.)

- Osobní velký bratr
- Lokální cloud (sběr dat, jejich ukládání a rozhodování vždy ve fyzickém okolí uživatele)
- O uživateli sesbírá velké množství intimních dat, ale nepustí je ven, využije je pouze pro pomoc uživateli

Jak ovlivnit svoji bezpečnost

- Nekupovat výrobek, kterému nevěřím (vyvinout tlak na výrobce)
- Průběžně se informovat o možnostech zvýšení bezpečnosti (časopisy, rodina)
- Chovat se obezřetně a ověřovat si informace z různých zdrojů (nereagovat hned na výzvy)
- Sledovat nezávislé testy výrobků, které hodláme koupit
- Jakýkoli produkt používat s ohledem na riziko možné škody

- Mezi výrobci jsou rozdíly a solidní společnosti chtějí dodávat kvalitní a bezpečné výrobky

Děkuji Vám za pozornost