Bezpečnostní výzvy internetu věcí z pohledu praxe

Marek Šottl, Karel Medek 17.8.2017

IoT jako pojem

Je samotný pojem IoT postačující?

- Pojem IoT se stává podobným fenoménem jako před lety pojem Cloud. Je často využíván, bez jasné specifikace technologie a stává se spíše Marketingovým pojmem.
- Důležitost některých aspektů se pro různé oblasti implementace (včetně bezpečnosti) významně liší.
- Samotný pojem tedy označuje spíše přístup a trend než řešení.
- Aktuálně je přijímáno dělení IoT zařízení do tří oblastí segmentů:

IoT a bezpečnost

1 Mezera v technologiích

Nedostatečná složitost IoT

Nedostatek nových technologií pro End to End komunikaci.

Technologie se rozvíjí rychleji než uživatel.

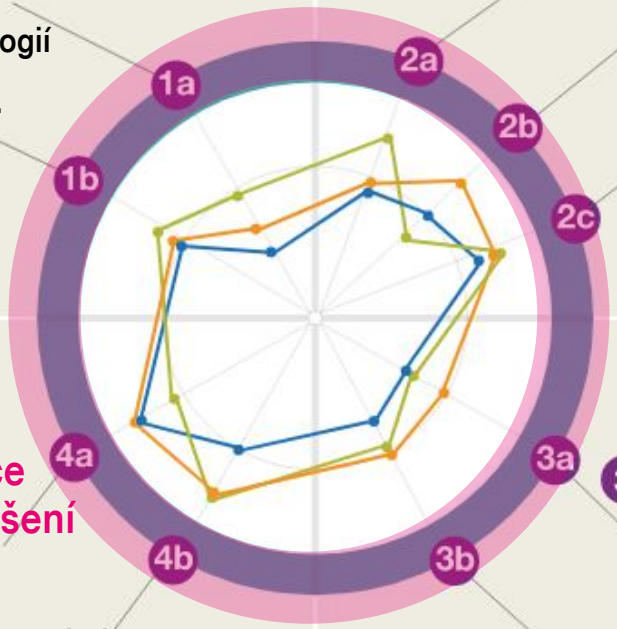
2 Nevyzrálé bezpečnostní standardy

Proprietární standardy výrobců

Technologie se pomalu odrážejí v regulatorice

Nemožnost definovat vynucení standardů

Dosavadní zkušenosti z Deutsche Telekomu naznačují, že zde zmíněné mezery jsou v praxi spíše širší, než jak je neznačeno.



3 Nemožnost vidět plnou hodnotu v IoT security

Nedostatek vhledu do technologií

Nedostatek znalostí koncového uživatele.

4 Obtížná monetizace bezpečnostních rešení

Zákazník obyčejně nechce platit bezpečnost

Společnosti vyrábějící HW mají problém přesunout se do SW řešení.

http://www.mckinsey.com/industries/semiconductors/our-insights/security-in-the-internet-of-things

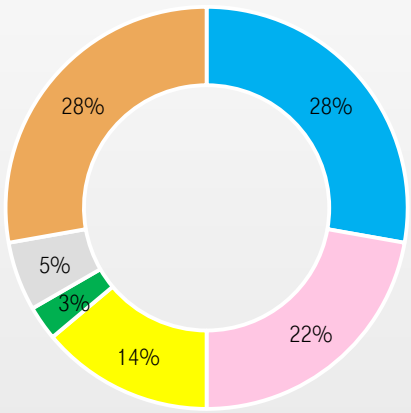
Bezpečnost IoT v číslech

Dosavadní zkušenosti

43%

Organizací očekává nějakou formu nasazení IoT

Typy zranitelností



- Odhalení informací
- Kryptografie
- Konfigurace
- Síťová bezpečnost
- Injekce
- Další

+40% instalací chytrých budov ročně

70% procent aplikačních útoků na IoT zařízení v penetračních testech

Brickerbot - Dropbear, nalezen na 21 milionech zařízení

Počet IoT zařízení se za poslední dva roky zdvojnásobil

Chytrý dům

Zařízení

Brikerbot

Typické hrozby v jednotlivých vrstvách IoT

KLIENT

Hardcoded údaje
Dekompilace
Injektáž

CLOUD

Autentizační útoky
Zastaralé UI knihovny
SQL injekce

API

REPLAY útoky
DoS útoky
Obcházení business logiky

TRANSPORT

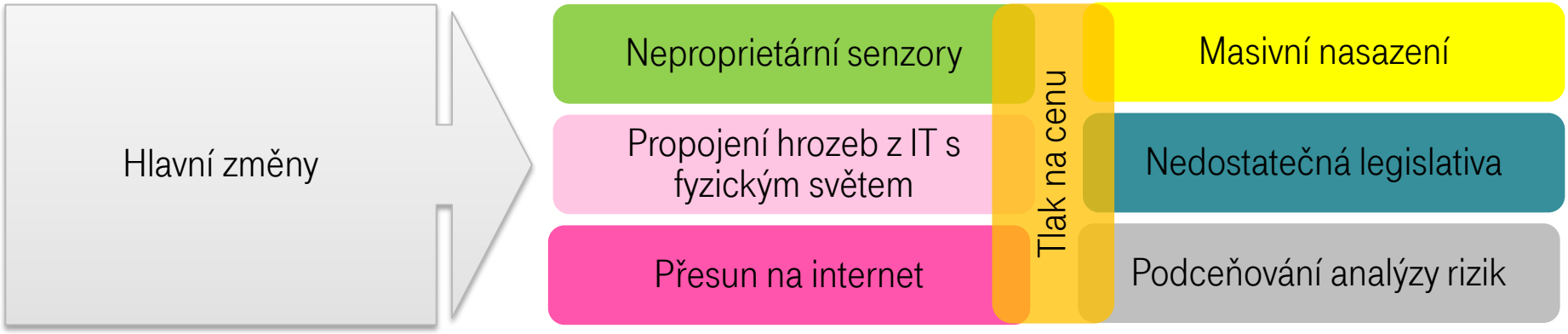
Spoofing
Denial of service
Man in the middle útoky

SENZOR

Podvržení firmware
Změna konfigurace

IoT jako evoluční a nikoli revoluční aspekt

Internet věcí je tu s námi již dlouho



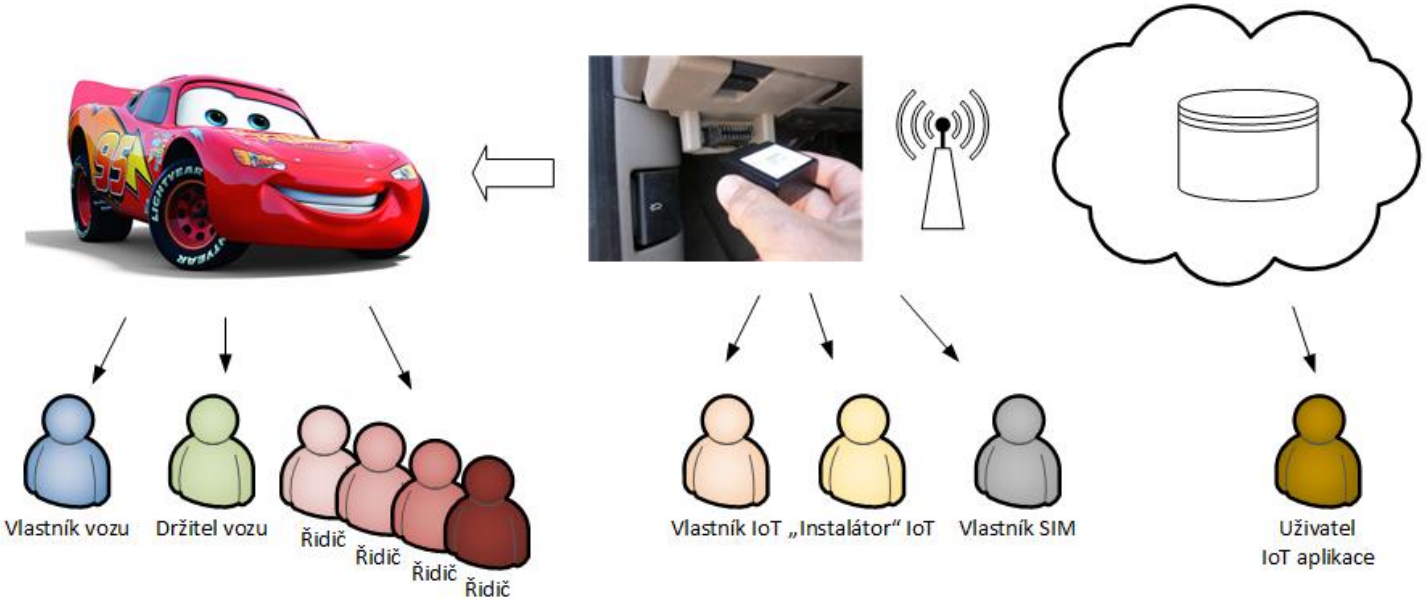
Pokus se zaměříme např. na technologický aspekt, tak :

Internet věcí je de facto komunikace mezi dvěma stroji.

- Problémy s replay útoky na REST rozhraní nebo bezdrátovou komunikaci.
- Chybějící vrstvená ochrana pro SOAP rozhraní, kde může být problém s šifrováním a výkonem. (Využívání WS proxy)
- Android malware není mýtem – Například problém knihovny Androidu, zvaný Stagefright. Co když takový Malware využije IoT ?
- Zranitelnosti iOS klienta jakou jsou injekce a únik dat z interního uložiště.
- Nezměrné možnosti DoS útoku pomocí IoT infrastruktury.

IoT z pohledu legislativy

Elementární případ „chytrého auta“ prodávaného např. v USA.



Položme si základní otázky, známe na ně odpověď?

- Kdo má právo přijmout nebo zamítnout použití IoT v automobilu?
- Uživatel může/musí/smí/nesmí mít právo zcela vypnout zařízení?
- Když bude zařízení prolomeno a nebo uniknou data – kdo bude informovat a kdo bude informován?
- Kdo je vlastníkem neanonymizovaných dat a má právo je využívat a nechat smazat?
- Kdo je zodpovědný za to, pokud se pomocí zranitelnosti v IoT platformě poškodí auto, nebo dojde ke zranění řidiče?
- Kdo je zodpovědný za update firmware v IoT?


Klient

Klienti - evaluace bezpečnosti

Mobilní aplikace na Google zařízeních

- Burp suite / ZapProxy / Fiddler – aplikační proxy
- Genymotion, **Android studio** / sdk tools – virtualizace
- **APK, Dex2Jar, JD-gui, LINT** – Dekompilace a statická analýza
- **Drozer** – Framework pro testování bezpečnosti aplikací a procesů Android.
- Certificate pinning: Problém většiny nástrojů pro testování bezpečnosti. **Android-SSL-TrustKiller** může obejít SSL / TLS vrstvy.

Klienti - evaluace bezpečnosti

Mobilní aplikace Apple

- **Burp suite / ZapProxy / Fiddler** – aplikační proxy
- **FileDP, Filemon** – systémy pro audit souborového systému a oprávnění.
- **Needle** – Framework na penetrační testování iOS
- **Cycript** – Interakce s běžícími aplikacemi v systémech iOS nebo Mac OS X pomocí hybridní syntaxe Objective-C ++ a JavaScriptu. Perfektní nástroj pro úpravu běžících procesů. Užitečné pro vývojáře a penetrační testery.
- Source code review frameworky (**CLANG/LLVM, Source clear)**

Firmware

LIFE IS FOR SHARING.

Bezpečnost správy zařízení v IoT síti

Vybrané problémy:

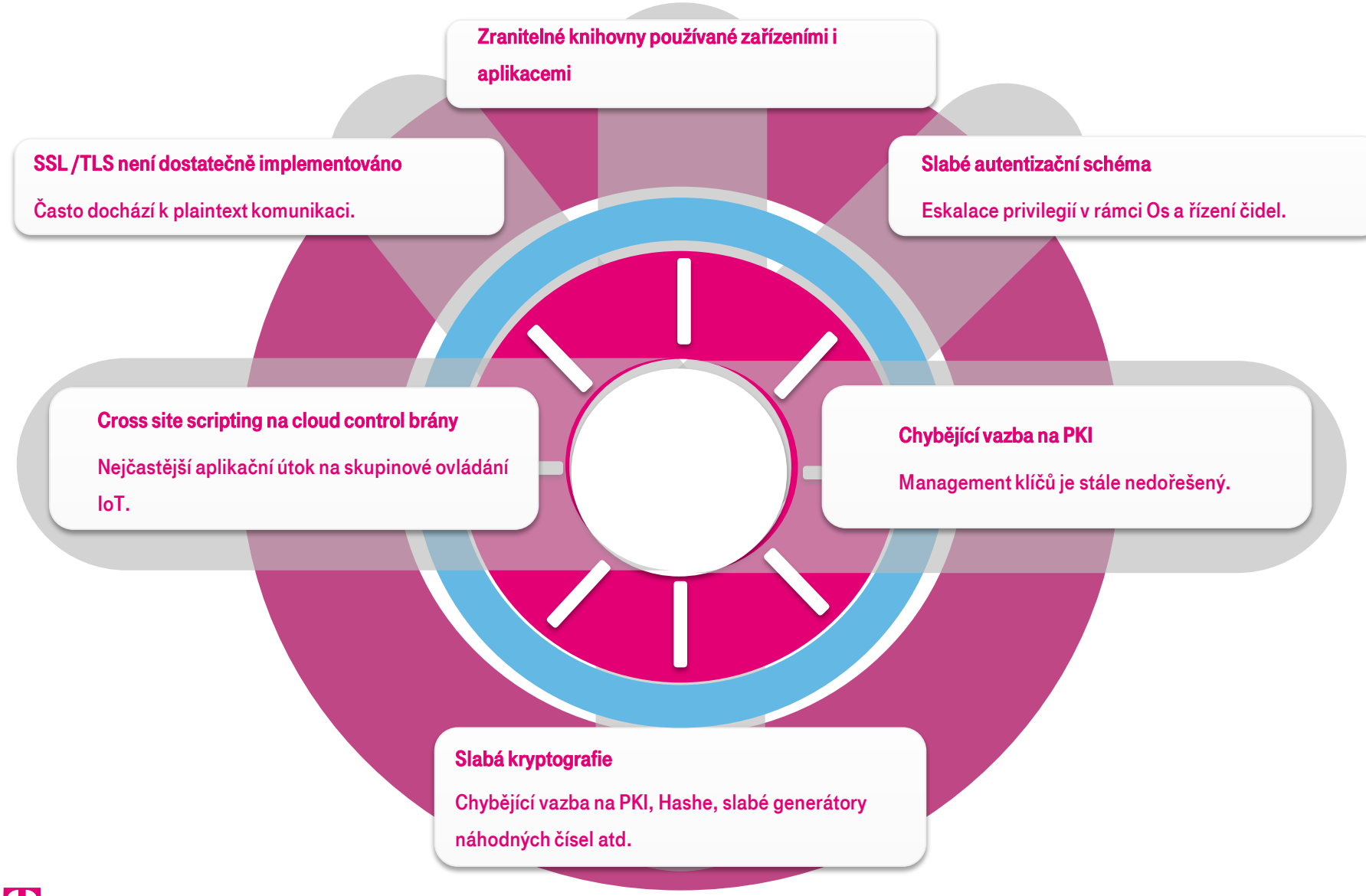
1. Často je Firmware chráněn slabým heslem.
2. OTA update nejsou korektně podepisovány a šifrovány. (Relevantní pro operátory).
3. Nedostupnost FW, rychlost update, vyjednávání s výrobcem.
4. Při útoku MITM je vnutit vlastní upravený FW, který používá všechny funkcionality IoT zařízení.

Možná řešení:

- Podepisování updatů a konfigurace pomocí se silným algoritmem. (Certifikát s signaturou alespoň SHA2 a kontrolní součet CRC16)
- Jakákoliv změna v konfiguraci a Firmware musí být chráněna vůči neoprávněné modifikaci.
- Provádění kontroly bezpečnosti konfigurace (tzv. Configuration review - Lynis, Nipper studio, Nessus)
- Patch management.
- Testování síly hesla pro přístup k konfiguračním souborům.

Cloud control

Typické útoky na IoT platformu



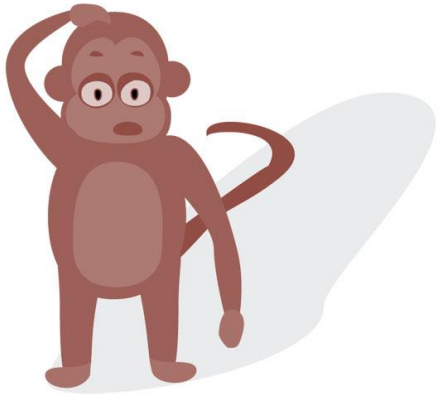
Infrastruktura

LIFE IS FOR SHARING.

Infrastruktura

Vybrané problémy pro některé typy sítí:

- Otevřené nepotřebné služby jako SSH, Telnet nebo UDP porty pro defaultní služby.
- Vnořené účty nebo defaultní od výrobců, které není možné smazat.
- Odhalení informací o účtech využívaných službami třetí stran jako je GPS, nebo obslužný cloud.
- GPS spoofing a podvržení pozice senzorů.
- DNS spoofing – DNS resolving není nijak chráněn.



Možná řešení:

- Port scan zařízení a kontrola otevřených služeb.
- Kontrola účtů a jejich oprávnění.
- Používání ochrany jako je DNSsec pro DNS řešení IoT, využívání PKI jako prostředků zajištění důvěrnosti přenášených dat.
- Kontrola business logiky a senzorů na straně back-endu. (Business processing engine)