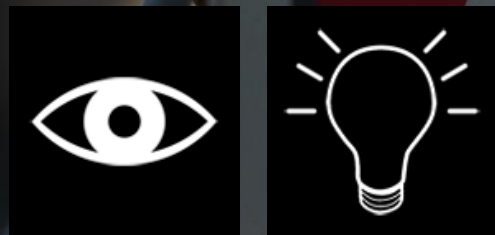


Internet of Threats

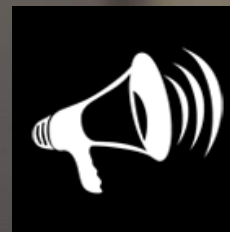
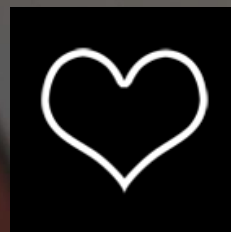
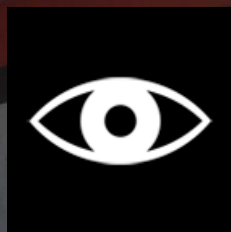
aneb proč se bát internetu věcí



Michal Altair Valášek

Development & Security Consultant, Altairis

michal.valasek@altairis.cz | www.aspnet.cz | www.secpublica.cz



IoT = Internet of ~~Things~~

Trash!



Threats

Platformy pro IoT

- **ARM + linuxové jádro**
 - „Raspberry Pi“
 - Typicky domácí routery, IP kamery atd.
 - Relativně komplexní systém
- **Jednoduché platformy bez OS**
 - „Arduino“
 - Typicky meteostanice, žárovky atd.
 - Jednoduchý systém s omezenými možnostmi
- **Real-time OS**
 - V IoT světě se používají relativně zřídka



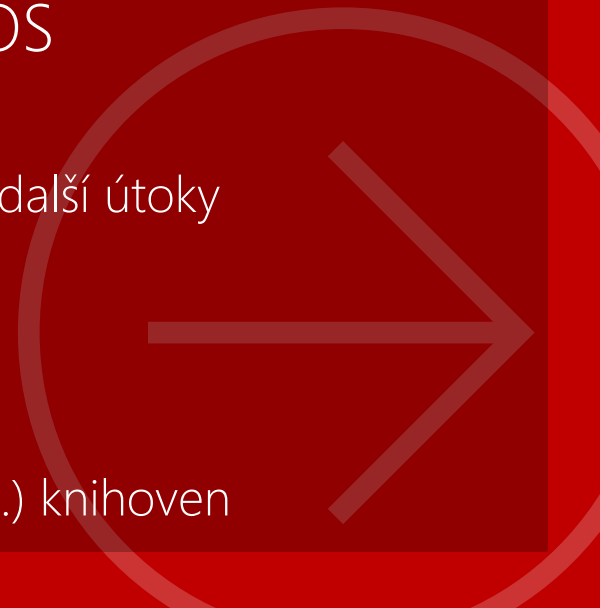
ARM + linuxové jádro

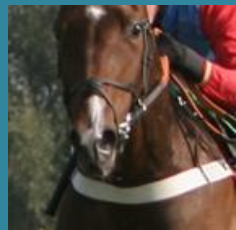
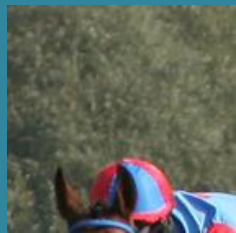
- Von Neumannovská architektura
 - Stejná paměť pro instrukce i data
- Na zařízení běží plnohodnotný operační systém
 - Výhody
 - Z hlediska vývojáře standardní stack
 - K dispozici běžné kryptografické knihovny atd.
 - Nevýhody
 - Velký attack surface – v podstatě plnohodnotný počítač
 - Velký potenciál pro zneužití k dalším útokům
 - Sdílená paměť znamená bezpečnostní riziko



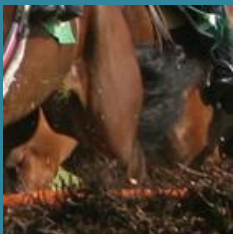
Jednoduché platformy bez OS

- Harvardská architektura
 - Oddělená paměť pro kód (EEPROM) a data (RAM)
- Na zařízení běží přímo kód aplikace, bez OS
 - Výhody
 - Menší attack surface, obtížná zneužitelnost pro další útoky
 - Levnější, menší spotřeba, RT/near-RT
 - Nevýhody
 - Obtížnější aktualizace firmware
 - Nedostupnost standardních kryptografických (aj.) knihoven






Typické problémy IoT



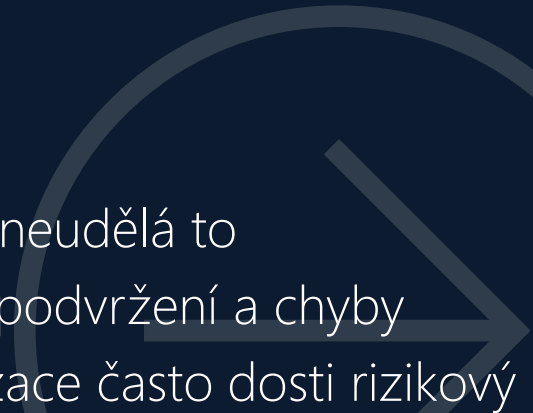
Typické problémy IoT

- Firmware a jeho bezpečná aktualizace
 - Nedostatečné zdroje entropie
 - Omezené kryptografické schopnosti
 - Nedostatečná rezistence vůči fyzickým lokálním útokům
 - Business – hackatonový syndrom
- 

Firmware a jeho bezpečná aktualizace

- Firmware je běžný SW, který obsahuje chyby
 - Je tedy nutné mít možnost ho aktualizovat
 - Což je ale nutné dělat bezpečným způsobem
- Co je bezpečný způsob
 - S minimálním, nejlépe žádným, zásahem uživatele
 - S ochranou proti modifikaci a podvržení

Problémy s aktualizací firmware

- Podpora poskytovaná výrobcem je většinou mnohem kratší, než životnost zařízení – EOL
 - Používají se zastaralé verze knihoven atd.
 - Nedostatečná diverzita ekosystému
 - Problematický proces aktualizace
 - Pokud uživatel musí aktualizovat firmware ručně, neudělá to
 - Pokud se firmware aktualizuje automaticky, hrozí podvržení a chyby
 - U jednodušších zařízení bez OS je proces aktualizace často dosti rizikový
- 

Nedostatečné zdroje entropie

- Kvalitní zdroj náhodnosti je nezbytným předpokladem úspěšné kryptografie (CSPRNG)
 - Počítač je ale inherentně neschopen vytvářet chaos
 - Potřebujeme externí zdroje
- IoT zařízení je často nemají, resp. ne v dostatečné kvalitě
- Často mají pevně daný stav, společný pro všechna zařízení svého druhu a totožný po restartu

Omezené kryptografické schopnosti

- Problém zejména u slabých zařízení bez OS
 - Malé množství operační paměti (kB)
 - Slabá výpočetní kapacita jako taková
 - Nejsme vesměs schopni dělat asymetrickou kryptografii
- U zařízení s OS jsou knihovny často zastaralé a/nebo špatně naimplementované
- Existují i specializované kryptografické čipy, ale:
 - Jsou drahé, takže se vesměs nepoužívají
 - Nejsou snadno dostupné mimo USA
- Problém s bezpečným úložištěm klíčů



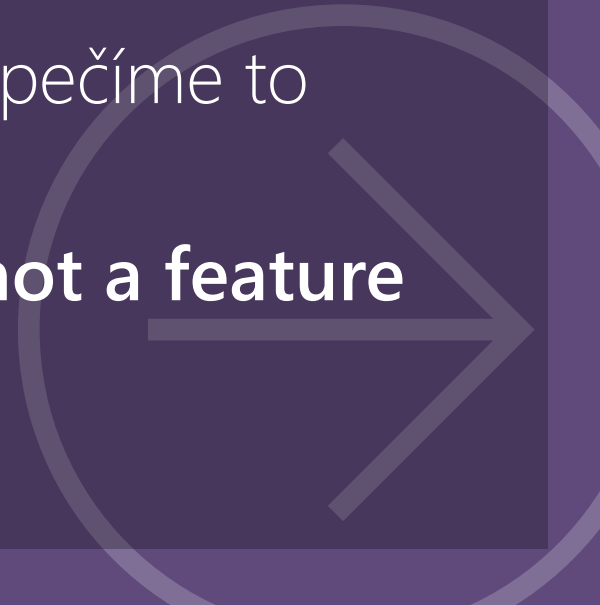
Lokální útoky

- **Není jednoduché firmware (a další data v EPROM) přečíst**
 - Ale není to ani nemožné – HaaS :-)
- **Je ale jednoduché je přepsat**
 - Pokud jsou fyzicky dostupné patřičné porty, což často jsou
 - Pak je triviální vytvořit vlastní firmware a rychle ho nahrát



Hackatonový syndrom

- Produkt musí být na trhu co nejdřív
 - Je důležité to udělat rychle, ne dobře
 - Nejdřív to naprogramujeme, zabezpečíme to později
 - To nefunguje: **Security is aspect, not a feature**
- Zákazníci bezpečnost nežadají



dotazy ?

www.aspnet.cz

www.rider.cz

facebook.com/rider.cz

twitter.com/ridercz

ask.fm/ridercz

youtube.com/altairiscz

michal.valasek@altairis.cz