Návrh komunikačného protokolu pre inteligentnú zásuvku

diplomová práca

Bc. Tomáš Kubla

Školiteľ: RNDr. Richard Ostertág PhD.

23. júna 2017

Ciele práce

- preskúmať najznámejšie protokoly pre komunikáciu medzi zariadeniami v inteligentných domácnostiach
- analyzovať bezpečnosť existujúceho riešenia inteligentnej zásuvky a prípadne určiť možné zraniteľnosti
- v prípade nájdenia zraniteľností navrhnúť bezpečný komunikačný protokol pre inteligentnú zásuvku

IoT - úvod

Internet vecí

- veľký rozmach
- priemysel aj domácnosti
- veľa riešení - zjednotenie a zjednodušenie $\rightarrow$ vznik štandardov
- smart home

IoT - štandardy

komunikačné stack-y, podobné TCP/IP

- rôzne dosahy
  - krátky - Bluetooth, IrDA, ZigBee, Z-Wave
  - dlhý - mobilné sieťe, WiFi (802.11n), LoRa
- bezpečnosť - napr. bluetooth (sprádovanie, potom E0)

IoT - chyby

- Prehľad útokov na smart home[1]
- OWASP - TOP 10
- Konkrétne útoky
  - X10 - bez šifrovania[2]
  - ZigBee - AES, ale potrebný *master key*[3]
  - Z-Wave - kľúč zašifrovaný, ale znova predzdieľaným kľúčom[4]

[1] Hacking the Neighbor's Home: How Secure are Proprietary Wireless Home Automation Protocols? (Jeroen Vollenbrock 2016)

[2] Pentesting over Power lines(Dave Kennedy, Rob Simon 2011)

[3] Killerbee: practical zigbee exploitation framework (Joshua Wright 2009 - ToorCon)

[4] Security evaluation of the Z-Wave wireless protocol (Behrang Fouladi, Sahand Ghanoun 2013)

IoT - inteligentná zásuvka

- meranie spotreby, vypínanie/zapínanie na diaľku
- rôzne vyhotovenia
  - redukcia

  - zabudované v stene[5]

[5] potreba odborníka pri inštalácii

Analýza bezpečnosti zásuvky

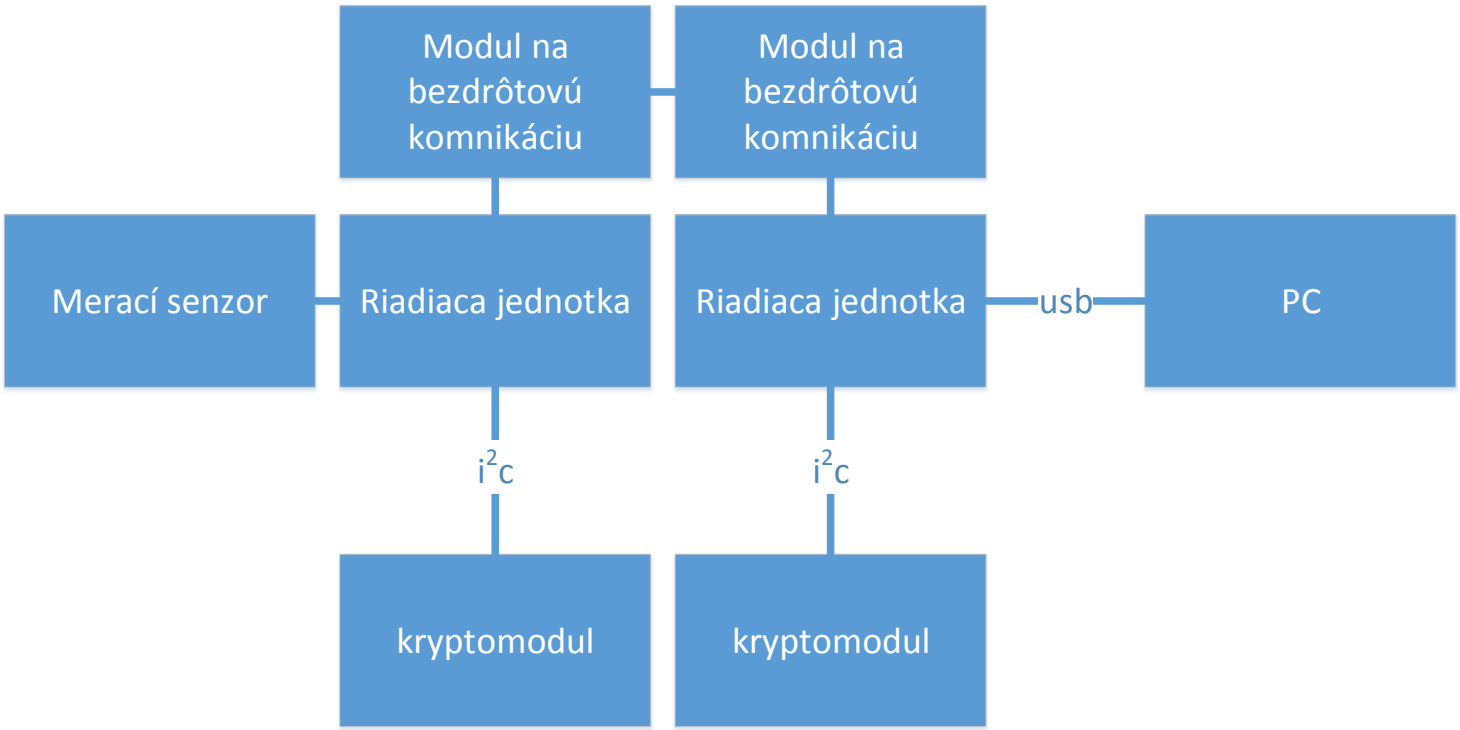
Úvod

- Vývojový tím na FEI
- Veľké dosahy (LoRa), v stene
- Šifrovanie dát - A7001 - NXP[6]

[6] Komunikácia cez I^2C, potreba podpisu NDA

Analýza bezpečnosti zásuvky

Úvod



- Odpočútie komunikácie

Analýza bezpečnosti zásuvky

Komunikácia

Packet	Start Time	R/W	ACK	Data
1	0.0239	W	0	0F
2	0.0319	W	0	1F
3	0.0322	R	0	01 00
4	0.0557	W	0	2F
5	0.0561	R	0	1E 00 B8 03 11 01 05 B9 02 01 01 BA 01 01 BB 0D 41 37 30 30 31 43 4D 20 32 34 32 52 31 BC 00
6	0.0745	W	0	FF
7	0.0748	R	0	01 CC
8	0.0829	W	0	00 0B 00 A4 04 00 05 41 37 30 43 4D 00

Analýza bezpečnosti zásuvky

Komunikácia

Packet	Start Time	R/W	ACK	Data
9	0.0921	Write	1	
10	0.1309	Write	0	07
11	0.1312	Read	0	01 07
12	0.1484	Write	0	02
13	0.1487	Read	0	07 02 02 05 01 02 90 00
14	0.1588	Write	0	10 0B 80 02 01 00 06 01 01 03 02 01 01

Analýza bezpečnosti zásuvky

Komunikácia

Packet	Start Time	R/W	ACK	Data
15	0.1680	Write	1	
16	0.2068	Write	0	07
17	0.2071	Read	0	01 07
18	0.2243	Write	0	02
19	0.2246	Read	0	03 12 69 82
20	0.2344	Write	0	20 1D 80 06 01 00 18 02 01 00 16 01 01 0C 10 2B 7E 15 16 28 AE D2 A6 AB F7 15 88 09 CF 4F 3C

Analýza bezpečnosti zásuvky

Komunikácia

Packet	Start Time	R/W	ACK	Data
21	0.2454	Write	1	
22	0.2842	Write	0	07
23	0.2845	Read	0	01 07
24	0.3017	Write	0	02
25	0.3020	Read	0	03 22 90 00
26	2.0019	Write	0	30 1D 80 10 01 00 18 02 01 00 0F 01 01 10 10 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

Packet	Start Time	R/W	ACK	Data
27	2.0129	Write	1	
28	2.0517	Write	0	07
29	2.0520	Read	0	01 07
30	2.0692	Write	0	02
31	2.0695	Read	0	06 32 0E 01 01 90 00
32	2.0796	Write	0	40 47 80 10 02 01 42 11 40 33 EA 33 EA 33 EA 33 EA 33 EA 33 EA 33 EA 33 EA 33 EA 33 EA 33 EA 33 EA 33 EA 33 EA 33 EA 33 EA 33 EA 33 EA 33 EA 33 EA 33 EA 33 EA 33 EA 33 EA 33 EA 33 EA 33 EA 33 EA 33 EA 33 EA 33 EA

Analýza bezpečnosti zásuvky

Komunikácia

Packet	Start Time	R/W	ACK	Data
33	2.0948	Write	1	
34	2.1337	Write	1	
35	2.1725	Write	0	07
36	2.1728	Read	0	01 07
37	2.1900	Write	0	02
38	2.1903	Read	0	45 42 12 40 F3 5A 3B B4 63 1A 37 C3 04 8D 41 4E 41 B0 58 6D C9 C2 EF 5C F3 F8 FE CF EA F6 1E D0 CE 21 70 1B 5B A9 4D F1 F4 5E DF 03 D5 10 C0 55 48 AC 84 8D CC EA 8B 1B C8 D5 5A AD B0 DC 85 F4 7C 90 38 2D 90 00
39	2.2062	Write	0	50 05 80 10 04 01 00

Analýza bezpečnosti zásuvky

Komunikácia

Packet	Start Time	R/W	ACK	Data
40	2.2148	Write	1	
41	2.2536	Write	0	07
42	2.2539	Read	0	01 07
43	2.2711	Write	0	02
44	2.2714	Read	0	03 52 90 00

Analýza bezpečnosti zásuvky

Sémantika komunikácie

Rozdelenie na časti/príkazy vďaka príznakom: neakceptovaný ACK bit + rovnaký prológ príkazov

- Predstavenie
  - A7001CM
- Inicializácia sedenia - definovanie použitia AES
  - AES-128
- Nahratie kľúča
  - 2B 7E 15 16 28 AE D2 A6 AB F7 15 88 09 CF 4F 3C
- Nahratie IV
  - 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
- Zaslanie nezašifrovaných dát
- Čítanie zašifrovaných dát
- Koniec sedenia

Návrh bezpečného komunikačného protokolu - hlavný cieľ našej práce

- Komunikačné entity
  - Zásuvka
  - Zberný bod
  - Servisné zariadenie
- Systém
  - Aspoň jeden zberný bod
  - Ľubovoľný počet zásuviek
  - Komunikácia len medzi jednou zásuvkou a zberným bodom/servisným zariadením
  - Prvotné spárovanie servisným zariadením

Špecifikácia komunikačného modelu

Aspekty ovplyvňujúce model

- Zamedzenie čítania kľúčov
- Montáž špecializovaným technikom
- Fyzický prístup k zariadeniu
- Bezpečnostné profily
- Riadenie komunikácie
- Dlhšia nedostupnosť
- Nešifrovaný ukladací priestor
- Kapacita ukladacieho priestoru
- Práca so zašifrovanými informáciami
- Aktuálny čas
- Použitie multicast-u a broadcast-u
- Synchronizácia v továrni
- Možnosti sekundárnej komunikácie

- Certifikáty
  - certifikát CA
  - certifikát zberného bodu
  - certifikát zásuvky
  - certifikát pre multicastové a broadcastové správy

  Tvorba podľa procesu CSR[7]
- Komunikačné sloty - štruktúra v pamäti
  - identifikátor slotu
  - certifikát partnera
  - typ
  - symetrický kľúč

[7] Certificate signing request

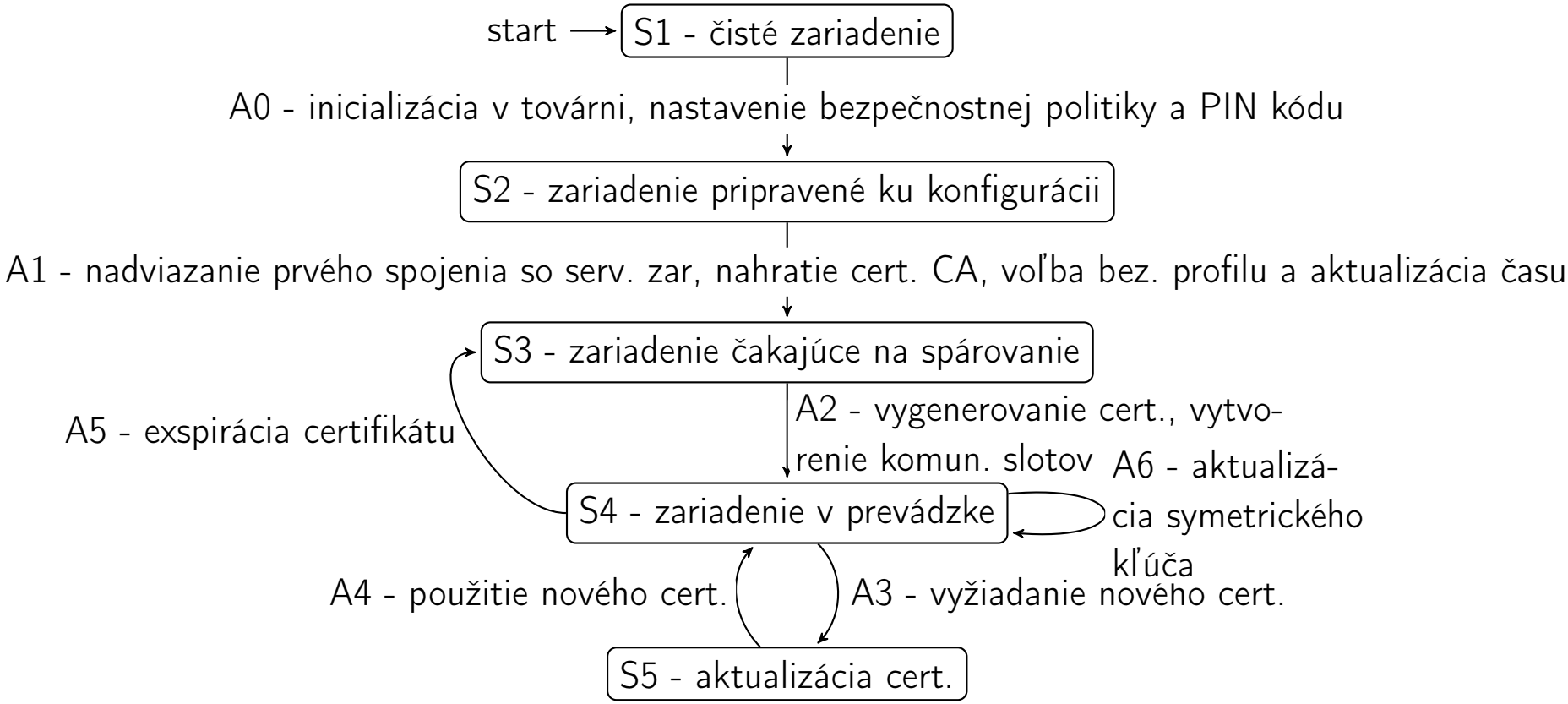
Štandardná komunikácia

- AES-128, AES-192, AES-256 - v závislosti od bezpečnostného profilu
- CBC mode
- Výplňová schéma - PKCS#7

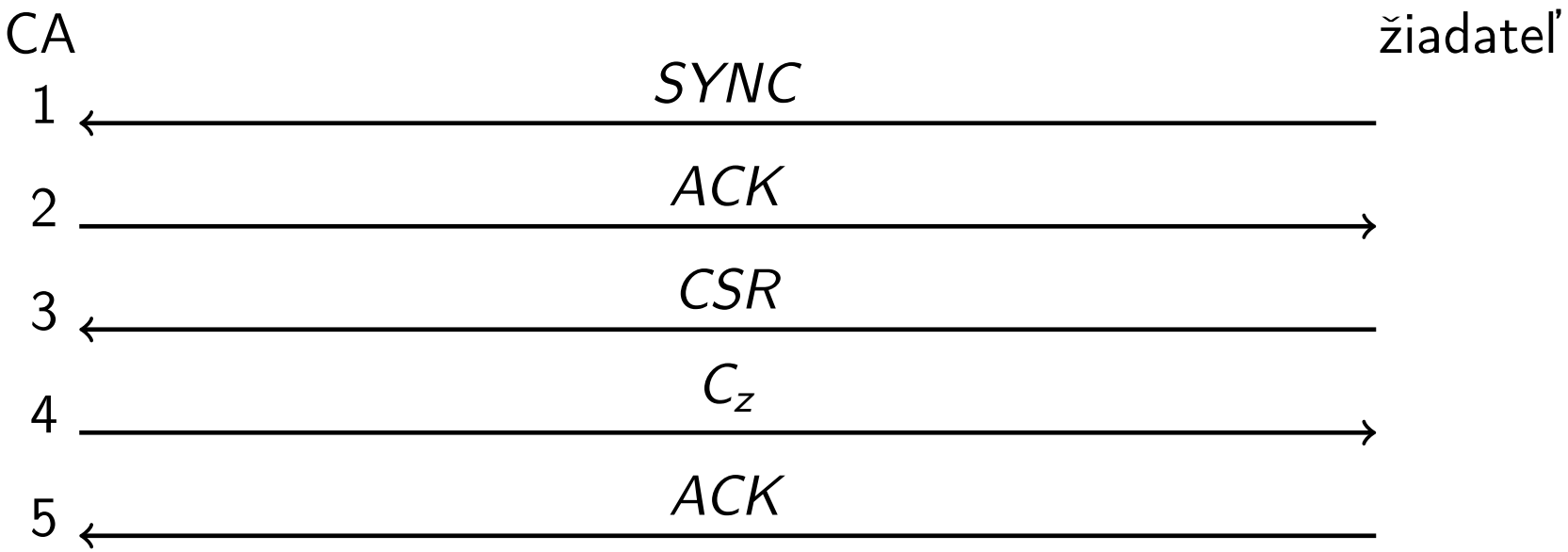
Nešifrované d.	Šifrované dáta				
ID slotu (4B)	*Príkaz (1B)*	*parameter 1*	*parameter 2*	*parameter 3*	...

Špecifikácia komunikačného modelu

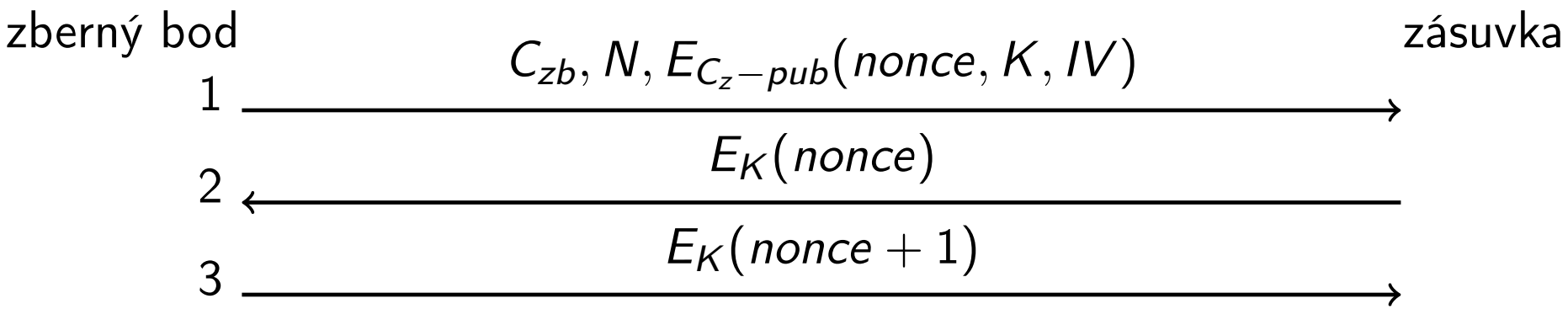
Protokol - životný cyklus



Proces generovania certifikátu



Proces tvorby slotu



Špecifikácia komunikačného modelu

Protokol - ďalšie

- Výnimočné udalosti
  - Výpadok času
  - Krátkodobá nedostupnosť
  - Dlhodobá nedustupnosť
- Broadcast a multicast sloty - ECB

Záver

- 6 mesiacov bez prístupu k dokumentácii
- Úspešné vytvorenie protokolu
- Použiteľný nie len pri zásuvkách
- Prínos v porovnaní s ostatnými
  - Profily
  - Scenár pri zaplnenom priestore - viac časových radov
  - Riešenie výpadku hodín
  - Multicast a broadcast správy
  - Aktualizácia a distribúcia kľúča

Ďakujem za pozornosť

Otázky oponenta

Ako bol návrh nového bezpečného komunikačného modelu overený?

- Plán použiť *OFMC: A symbolic model checker for security protocols*
- pre nedostatok času nerealizované

Otázky oponenta

Nový bezpečný komunikačný protokol kladie podstatne vyššie nároky na funkcionalitu riadiacej jednotky. Bol vykonaný odhad nárastu zložitosti riadiacej jednotky resp. celej inteligentnej zásuvky?

- Plne využiteľné aj s doteraz používanými komponentami
- Spotreba - vývojový tím má plán optimalizácie
- Časový faktor - bez dokumentácie nezistiteľné
- Časový faktor - subjektívny odhad
  - Inicializácia (úvodné spárovanie) - považujeme za zanedbateľnú - vykonáva sa jednorázovo
  - Aktualizácia certifikátu - považujeme za zanedbateľnú - nevykonáva sa časti
  - Nároky počas prevádzky
    - AES-128 - ešte rýchlejšie (na rozdiel od pôvodného protokolu, neinicializujeme šifrovanie pri každej skupine dát)
    - AES-192 a AES-256 - možno pomalšie pre kryptoelement (nezistiteľné), pre centrálnu jednotku bez zvýšenia výkonu

Otázky oponenta

Aká je ochrana systému inteligentných zásuviek a zberných bodov voči falošnej CA? Ako sa pri zmene CA na iný zberný bod prenesie privátny kľúč CA?

- Všetky elementy poznajú CA, ak by sa objavila falošná, overovanie by neprešlo (s. 50 - pri tvorbe slotov sa overuje, či majú entity spoločnú CA)
- Podvrhnutie možné len v úvodnej fáze, počas prevádzky nemožné
- Ak predsa - nemožnosť spárovania = technik hľadá dôvod
- Presun
  - nad rámec protokolu
  - nechávame na užívateľovi
  - potreba bezpečného presunu (s. 37)

Otázky oponenta

Na strane 51 sa hovorí o aktualizácii certifikátu. Čo tým má diplomant na mysli?

- Certifikát má platnosť
- Potreba nahratia nového dostatočné vopred
- Aktualizácia = včasná žiadosť o nový a jeho nahratie
- Dĺžka platnosti a požadovaný čas aktualizácie uvedený v tabuľke 3.1

Otázky oponenta

Z hľadiska čitateľnosti diplomovej práce by bolo vhodné uviesť vysokoúrovňový opis novéhobezpečného komunikačného modelu.

- Po podobných reakciách okolia súhlasím
- V čase písania práve - nepovažoval som za potrebné