CEN/TR 16968 - **Electronic Fee Collection - Assessment of security measures for applications using Dedicated Short-Range Communication**

Application Area: Electronic Fee Collection (EFC)

Publication Year, Number of Pages: Published 2016, 44 pages

Extract Creation Year: 2016

Standard Topic Group: Zabezpečení a kontrola

Standard Topic: Systémová architektura

Topic Description: Analýza rizik v rámcí provozu mýtného systému a návrhy na odpovídající kroky k potlačení rizik a zajištění bezpečnosti.

Introduction, Explanation of Starting Points

Description of Architecture, Hierarchies, Roles, and Object Relationships

Indikace pozice subjektů bezpečnostní analýzy v rámci architektury EFC systému. Definice kvalitativních kritérií pro ohodnocení bezpečnostního rámce.

Description of Process / Function / Method of Use

Definice obecné metodiky pro bezpečnostní analýzu EFC systému. Popis jednotlivých požadavků na entity EFC systémů s ohledem na kvalitativní kritéria.

Description of Interfaces / APIs / System Structure

Protocol / Algorithm / Computation Definition

Definice postupu vedoucí od analýzy rizik k návrhu bezpečnostních opatření v rámci vývoje EFC systémů.

Definition of Data Representation / Physical Meaning

Dfinice významu jednotlivých datových elementů a parametrů.

Definition of Constants / Ranges / Restrictions

Introduction

Tato technická zpráva se snaží identifikovat rizika související s použitím DSRC a navrhnout odpovídající bezpečnostní kroky k jejich odstranění či minimalizaci. Na základě navrhnutých opatření rovněž indikuje nutnost vytvoření nových norem, pokud to dané opatření vyžaduje.

Poznámka: Extrakt uvádí vybrané kapitoly popisovaného dokumentu a přejímá původní číslování kapitol.

Application

Cílem popisovaného dokumentu je poskytnutí přehledových informací ohledně bezpečnosti použití DSRC coby základní technologie v rámci elektronických mýtných systémů (EFC). Tyto informace mohou být užitečné zejména pro potenciální subjekty pro výběr mýtného (instituce, jež vlastní a provozují elektronický mýtný systém) v rámci jejich rozhodovacího procesu ohledně použitých technologií (v tomto dokumentu lze nalézt aspekty, jež se týkají bezpečnosti užití DSRC). Vzhledem k rozsahu analýzy může být tato zpráva určena i pro poskytovatele služeb a výrobce zařízení (OBU či RSE).

1. Scope

Popisovaný dokument obsahuje analýzu hrozeb souvisejících s použitím DSRC v rámci aplikací EFC (způsob použití této technologie je předmětem několika různých norem – EN 15509:2014, ISO 12813:2015, ISO 13141:2015 a CEN/TS 16702-1:2014. V rámci analýzy jsou zohledňovány zejména následující aspekty:

- kontext (tj. zda jde o lokální mýtný systém, interoperabilní schéma či Evropskou službu elektronického mýtného – EETS)

- současné bezpečnostní algoritmy a opatření a jejich možnosti vzhledem k potenciálním budoucím hrozbám

- nové bezpečnostní opatření, doplňující ty existující

- důsledky bezpečnostních aspektů (rizik a opatření) na existující mýtné systémy

- důsledky bezpečnostních aspektů na již existující normy (jedná se zejména o normy související s DSRC) a jejich revizi či případně na návrhy norem nových

2. Associated Standards

Tato technická zpráva se zabývá oblastí, jež je zahrnuta v řadě norem a technických specifikací, z nichž klíčové jsou následující.:

ČSN EN ISO 14906 (01 8382) Elektronický výběr mýtného (EFC) – Stanovení aplikačního rozhraní pro vyhrazené spojení krátkého dosahu

ČSN P CEN/TS 16702-1 Elektronický výběr poplatků (EFC) – Bezpečné monitorování pro autonomní systémy výběru mýtného – Část 1: Kontrola shody

ČSN EN 15509 Elektronický výběr poplatků (EFC) – Aplikační profil interoperability pro DSRC

3. Terms and Definitions

Kapitola Termíny a definice obsahuje 15 termínů a definic souvisících s touto normou, z nichž nejdůležitější jsou následující:

přičitatelnost *(accountability)* – vlastnost, která zaručuje, že jednání entity lze jednoznačně přiřknout příslušné entitě

útok *(attack)* – pokus o zničení, vystavení hrozbě, vyřazení z činnosti, zcizení nebo získání neautorizovaného přístupu k aktivu nebo neautorizovanému použití aktiva

hacker *(hacker)* – uživatel počítače, který se snaží získat neoprávněný přístup k počítačovému systému jiného majitele nebo zneužít slabých míst v jeho systému

správa klíčů *(key management)* – generování, distribuce, skladování, použití a zrušení šifrovacích klíčů

předmět ohodnocení *(target of evaluation)* – produkt nebo IT systém, který je předmětem hodnocení bezpečnosti

Další termíny a zkratky z oboru ITS jsou obsaženy ve slovníku ITS terminology.

4. Abbreviations

Kapitola Zkratky obsahuje 18 zkratek souvisících s touto normou, z nichž nejdůležitější jsou následující:

AES- standard pokročilého šifrování *(Advanced Encryption Standard)*

TOE- předmět ohodnocení *(Target Of Evaluation)*

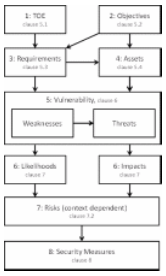
SM-CC- bezpečné monitorování kontrola shody *(secure monitoring compliance check)*

TVRA analýza hrozeb, zranitelnosti a rizik *(Threat, Vulnerabily, and Risk Analysis)*

Další termíny a zkratky z oboru ITS jsou obsaženy ve slovníku ITS terminology (www.ITSterminology.org).

4 Metoda

Tato kapitola popisuje metodologii (založena na metodě definované v ETSI/TS 102 165-1), jež byla použita při vzniku této technické zprávy. Jedná se o posloupnost deseti kroků, jež v kostce souvisejí s procesem identifikace hlavních zdrojů a cílů potenciálních hrozeb, návrhu účelu bezpečnostních mechanismů a požadavků od těchto odvozených, kalkulaci pravděpodobnosti a dopadu jednotlivých hrozeb a rizik, podrobnější identifikaci zdrojů a cílů, analýzu výdajů a detailním návrhem požadavků na bezpečnostní opatření. Jednotlivé kroky včetně posloupnosti jsou zobrazeny na Obrázku 1.



Obrázek 1 – TVRA metodologie použitá v této technické zprávě (obrázek 1 normy)

5 Bezpečnostní cíle a požadavky

Tato kapitola poskytuje podrobnou analýzu témat, jež jsou podrobněji rozepsána níže.

Předmět bezpečnostní analýzy (TOE) – Jedná se o identifikaci elementů, jichž se analýza přímo týká (OBU a RSE). Jsou zde identifikována rozhraní, se kterými souvisejí potenciální bezpečnostní hrozby (viz Tabulka . č. 1).

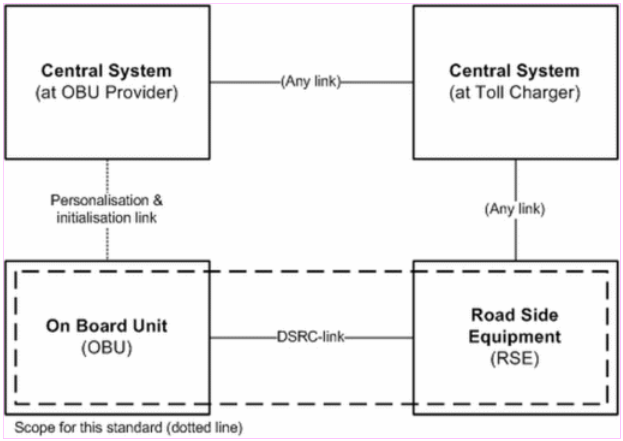


Figure 2 — TOE

Obrázek 2 – Identifikace rozhraní (obrázek 2 normy)

Bezpečnostní cíle – Jsou zde specifikovány jednotlivá bezpečnostní kritéria a cíle, jež jsou v následujícím procesu analýzy zohledněny. Jedná se zejména o cíle zohledňující aspekty důvěrnosti, dostupnosti, přičitatelnosti a integrity dat.

Funkční požadavky týkající se bezpečnosti – Tato sekce obsahuje specifikace požadavků, jež reflektují cíle a kritéria uvedená v sekci předchozí. Jsou zde rovněž zohledněny role, kterých se jednotlivé požadavky týkají:

- subjekt pro výběr mýtného – požadavky týkající se důvěrnosti, dostupnosti, přičitatelnosti, integrity dat

- OBU – požadavky týkající se důvěrnosti,

- poskytovatel služby – požadavky týkající se dostupnosti, přičitatelnosti, integrity dat

Identifikace zdrojů – Jedná se o výpis funkčních a datových zdrojů (např. komunikační protokol, algoritmus pro kalkulaci bezpečnostního klíče či aplikační data, jež jsou předmětem komunikace mezi OBU a RSE), jež souvisejí s cílem bezpečnostní analýzy zohledňující jednotlivé funkční elementy EFC systému – tj. OBU a RSE.

6 Analýza hrozeb

Tato kapitola poskytuje přehlednou tabulku s popisem jednotlivých bezpečnostních hrozeb a beroucí v potaz následující kritéria:

- zranitelnost – kombinace identifikovaného slabého místa v systému, s nímž souvisí jedna či více hrozeb, které jsou v důsledku schopny této slabosti zneužít

- důsledek – odkazuje na narušení funkčních požadavků, způsobené danou hrozbou

Tato analýza nezkoumá v důsledku roli v EFC systému, jež může být danou hrozbou poškozena.

7 Kvalitativní analýza rizik

Tato kapitola poskytuje podrobnou analýzu jednotlivých rizik či hrozeb (registr rizik) definovaných v předchozí kapitole. Jsou zde podrobně popsány použité metodiky ohodnocení jednotlivých atributů rizik a hrozeb a také faktory, jež je nutné brát v potaz při tvorbě registru rizik. Následující tabulka poskytuje seznam hrozeb s ohodnocením jednotlivých atributů týkajících se pravděpodobnosti, dopadu a míry rizika.

Tabulka 1 – Souhrn rizik/hrozeb (tabulka 13 normy)

Threat	Low risk context			High risk context		
	Likelihood	Impact	Risk	Likelihood	Impact	Risk
T1 Access credentials key recovery	Unlikely	Low	Minor	Likely	High	**Critical**
T2 Authentication key recovery	Possible	Low	Minor	Possible	Medium	**Major**
T3 OBU can be cloned	Possible	Low	Minor	Possible	High	**Critical**
T4 OBU can be faked	Unlikely	Low	Minor	Likely	High	**Critical**
T5 Authentication of OBU data can be repudiated	Possible	Low	Minor	Likely	High	**Critical**
T6 Application data can be modified after the transaction	Unlikely	Low	Minor	Possible	Medium	**Major**
T7 Data in VST is not secure	Unlikely	Low	Minor	Possible	Medium	Minor
T8 DSRC communication data can be eavesdropped	Unlikely	Medium	Minor	Unlikely	Medium	Minor
T9 Correctness of application data are repudiated	Unlikely	Low	Minor	Possible	High	**Major**
T10 Master key can be obtained from RSE	Extremely unlikely	High	Minor	Unlikely	High	Minor

8 Návrhy na nová bezpečnostní opatření

Tato kapitola uvádí nová bezpečnostní opatření pro hrozby, jejichž míra rizika byla určena na středně vážnou a kritickou. Vzhledem k tomu, že většina těchto hrozeb souvisí s kryptografií, týkají se všechna navržená opatření současných bezpečnostních mechanismů DSRC. V rámci návrhu bezpečnostních opatření obsahuje tato kapitola seznam možných opatření asociovaných k jednotlivým hrozbám (viz Tabulka č. 2).

Tabulka 2 – Hrozby a možná bezpečnostní opatření (tabulka 14 normy)

Threat	Possible countermeasures
T1 Access credentials key recovery	AES, randomization of RndOBU and RndRSE, increasing the diversification space
T2 Authentication key recovery	AES, randomization of RndOBU and RndRSE, disallow empty attribute list, MAC enlargement, MAC randomization
T3 OBU can be cloned	AES, transaction-counter
T4 OBU can be faked	AES, transaction-counter
T5 Authentication of OBU data can be repudiated	AES
T6 Application data can be modified after the transaction	AES, encrypted attributes over the air
T9 Correctness of application data are repudiated	AES

Na základě seznamu všech možných opatření jsou v této sekci uvedena doporučená souhrnná opatření, jež ve svém funkčním konceptu pokrývají i výše uvedené hrozby.

9 Důsledky navržených opatření

Tato kapitola prezentuje možné dopady a důsledky navržených opatření z několika perspektiv. Jedná se zejména o současnou situaci a úroveň realizace hrozeb v rámci existujících elektronických mýtných systémů používajících DSRC, legislativní i nelegislativní dokumenty zaměřující se na specifikaci EETS, důsledky na jednotlivé role v rámci elektronických mýtných systémů (zejména z pohledu certifikačního procesu, autentizačních mechanismů a interoperability).

10 Doporučení

Tato kapitola obsahuje několik finálních doporučení týkajících se zejména oblasti norem. Jsou zde uvedeny doporučení pro revizi následujících norem: ISO 14906, EN 15509, ISO 12813, ISO 13141, CEN/TS 16702-1. Veškeré změny souvisí s již existujícími bezpečnostními mechanismy DSRC.

Příloha A (informativní) Současný stav kryptovacího algoritmu DEA

Příloha A obsahuje přehledovou rešerši ke kryptovacímu algoritmu DEA, spolu s referencemi na odpovídající normy, jež tento algoritmus využívají a/nebo definují.

Příloha B (informativní) Bezpečnostní aspekty vztahující se k DSRC v EFC

Příloha B obsahuje aspekty, jež je doporučeno brát v potaz např. v rámci implementace elektronického mýtného systému, resp. technologie, na níž bude systém založen (tedy DSRC). Týkají se zejména aspektu zranitelnosti v rámci užití norem souvisejících s DSRC – EN 15509, ISO 14906, ISO 12813, ISO 13141 a CEN/TS 16702-1.