CEN ISO TS 17574 - **Elektronický výběr poplatků – Směrnice pro systém bezpečnosti**

Aplikační oblast: Elektronický výběr poplatků (EFC)

Rok vydání normy a počet stran: Vydána 1.7.2005, 72 stran

Zavedení normy do ČSN: originálem

Rok zpracování extraktu: 2008

Skupina témat: Zabezpečení a kontrola

Téma normy: Návod pro analýzu a specifikaci bezepčnostních aspektů EFC systémů

Charakteristika tématu: Návod pro tvorbu bezpečnostních profilů a jejich požadavků jímž musí elektronický mýtný systém vyhovovat.

Úvod, vysvětlení východisek

Popis architektury, hierarchie, rolí a vztahů objektů

Definice vztahů mezi jednotlivými učástníky služny elektronického mýtného z ohledem na bezpečnost. Nástin architektury z hlediska zabezpečení.

Popis procesu / funkce / způsobu použití

Popis kroků tvorbu bezpečnostního profilu pro systém elektronického mýtného. Specifikace výstůpů bezpečnostní analýzy systému.

Popis rozhraní / API / struktury systému

Definice protokolu / algoritmu / výpočtu

Definice reprezentace dat / fyzikálního významu

Definice konstant / rozsahů / omezení

Úvod

Tato technická specifikace je pokynem pro zpracování a posouzení specifikace požadavků na zabezpečení, označovaných jako profily zabezpečení (Protection Profiles (PP)). Profilem zabezpečení (PP) se míní sada bezpečnostních požadavků pro kategorii výrobků nebo systémů, které splňují určité potřeby. Typickým příkladem by byl PP pro palubní zařízení (OBE) používané v systému EFC, který by byl sadou bezpečnostních požadavků nezávislých na implementaci pro OBE splňující potřeby zabezpečení operátorů a uživatelů.

Po zpracování EFC/PP, jej lze mezinárodně zaregistrovat organizací, která jej zpracovala tak, aby se ostatní operátoři nebo země, které chtějí služby zabezpečení systému EFC rozvinout, mohli odkázat na již existující registrované profily EFC/PP.

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

Užití

Doporučuje se, aby operátoři EFC nebo ŘSD či MD ČR používali tento pokyn pro zpracování svých vlastních EFC/PP, neboť by bezpečnostní požadavky měly být popsány z pohledu operátora a/nebo organizací operátorů.

1. Předmět normy

Tato specifikace používá jako příklad zpracování a posouzení specifikace požadavků na zabezpečení (profil zabezpečení) OBE s kartou s integrovaným obvodem (obvody) (ICC), na kterém popisuje jak strukturu profilu, tak navrhovaný obsah. K popisu specifikace hojně využívá obrázků.

Na obrázku 1 normy je popsán kontext a místo, jaké má tato specifikace v architektuře zabezpečení EFC. Hlavní účelem profilu zabezpečení PP je analyzovat bezpečnostní prostředí určitého subjektu a poté stanovit požadavky splňující opatření proti hrozbám, což je výstupem analýzy bezpečnosti prostředí. Zkoumaný subjekt se nazývá Cíl posouzení (Target of Evaluation (TOE)), zde jako příklad OBE s ICC.

Zpracování profilu zabezpečení EFC/PP spočívá v těchto krocích:

1. Zpracování úvodu;

2. Zpracování popisu cíle posouzení, který zařadí subjekt (nebo rozhraní) do kontextu, z něhož vyplývají určitá bezpečnostní rizika;

3. Zpracování popisu bezpečnostního prostředí výrobků EFC nebo rozhraní, ve kterém musí být konkrétně popsána analýza ohrožení bezpečnosti a bezpečnostní politika.

4. Zpracování cílů zabezpečování s údaji, do jaké míry a jakým způsobem se bezpečnostní potřeby mají naplnit

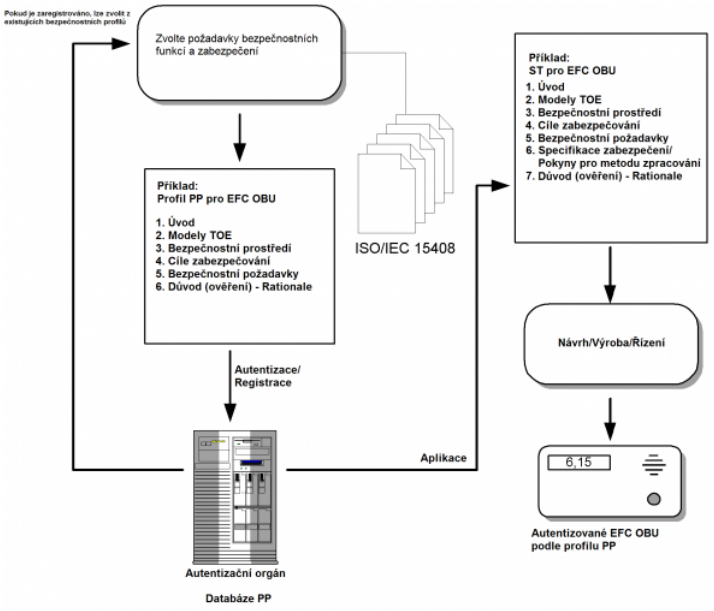
5. Zpracování bezpečnostních funkčních požadavků a požadavků zabezpečení pomocí funkčních požadavků z ISO/IEC 15408. Bezpečnostní funkční požadavky udávají, co se musí provést s TOE a prostředím TOE, aby se splnily cíle zabezpečování. Požadavky na zabezpečení udávají stupeň spolehlivosti předpokládaný v bezpečnostních funkcích TOE.

6. Zpracování důvodu/ověření (rationale), ve kterém by se měly zkontrolovat cíle zabezpečování a bezpečnostní požadavky.

Cílem zabezpečení (Security Target (ST)) se míní sada požadavků a specifikací, která se použije jako základ pro posouzení zkoumaného TOE. Zatímco PP lze vnímat jako požadavky operátora EFC, ST je určeno pro účely dokumentace dodavatele a také shody výrobku a splnění PP pro dané TOE, např. OBE.

Norma ukazuje zjednodušenou formou příklad vazeb mezi operátorem EFC, dodavatelem zařízení EFC a posuzovatelem, viz obrázek 3 normy.

Obrázek 4 zobrazuje cíl zabezpečení ST, které slouží jako základ při návrhu současných bezpečnostních funkcí pro výrobky EFC. Pro příklad je uveden níže.



Obrázek 1 – Příklad návrhu založeném na profilu zabezpečení PP (obrázek 5 normy)

TOE pro EFC je omezeno na EFC specifické entity a rozhraní jako jsou uživatelé, poskytovatelé služeb a spojení (komunikační linky DSRC nebo mobilní síť CN) mezi uživateli a poskytovateli služeb, které jsou základem systémů EFC, jak uvádí schéma obrázku 5.

Obrázek 1 ukazuje entity zapojené do rozhraní zpoplatnění, např. uživatele, poskytovatele služby a nečestné strany, která se snaží profitovat falšováním segmentů nebo celé komunikace.

2. Souvisící normy

Profily zabezpečení jsou stanoveny v ISO/IEC 15408 a ISO/IEC PDTR 15446. Zejména pro čtenáře přílohy A je zapotřebí seznámení s normou ISO/IEC 15408, která stanovuje sadu požadavků na bezpečnostní funkce a zabezpečení relevantních výrobků a systémů IT.

3. Termíny a definice

Norma uvádí 32 termínů a definicí, z nichž ty podstatné pro pochopení tohoto extraktu jsou uvedeny níže.

3.1 požadavek zabezpečení *(assurance requirement)* bezpečnostní požadavky pro zajištění důvěryhodnosti při implementaci funkčních požadavků

3.2 audit *(audit)* rozpoznání chyb jako protiprávní (protizákonný) systém či přístup; dále se jedná o záznam a analýzu informací a událostí spojených s bezpečnostními aktivitami tak, aby bylo docíleno řízení bezpečnosti v souladu s bezpečnostní politikou EFC

3.9 utajení *(confidentiality)* prevence proti úniku informací k neověřeným osobám, stranám a/nebo procesům

3.10 hodnocení úrovně důvěryhodnosti (EAL) *(evaluation assurance level (EAL))* úroveň důvěryhodnosti pro hodnocení bezpečnosti jednotlivých produktů i celého systému

3.21 důvod (ověření) *(rationale (verification))* proces stanovující, že produkt v každé fázi životního cyklu splňuje všechny požadavky specifikované v předchozí fázi

3.25 zabezpečený aplikační modul *(secure application module (SAM))* modul, který je určený pro uložení algoritmů, relevantních klíčů, postupů zabezpečení a informací pro ochranu aplikace tak, že neoprávněný přístup není možný; aby toto mohlo být dosaženo, modul je fyzicky, elektricky a logicky zabezpečen

3.28 cíl zabezpečení *(security target ST)* skupina bezpečnostních požadavků a specifikací, které tvoří bázi pro vyhodnocení identifikovaných TOE

3.30 cíl posuzování *(target of evaluation TOE)* produkt bezpečnosti informací nebo systém pro posouzení zabezpečení

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

4. Symboly a zkratky

Kapitola 4 uvádí 21 zkratek.

5 Přehled profilu zabezpečení PP

Tato kapitola je uvedena skladba profilu zabezpečení a jeho kontext, které jsou blíže popsány na příkladu v příloze A.

Příloha A (informativní) Postup tvorby dokumentů

A.1 Úvod

Článek A.1.1 upozorňuje, že většina obsahu této přílohy je příkladem způsobu, jak zpracovat bezpečnostní požadavky pro zařízení EFC; v tomto konkrétním případě je to čipová karta s klíčovými daty potřebnými pro elektronický výběr poplatků. Článek A.1.2 uvádí identifikační údaje dokumentu, článek A.1.3 popis TOE, článek A.1.4 shodu s ISO/IEC 15408 a článek A.1.5 přehled TOE.

A.2 Cíl posuzování (TOE)

Článek A.2.1 uvádí cíle a metodiku TOE, článek A.2.2 funkce TOE a článek A.2.3 strukturu TOE.

A.3 Bezpečnostní prostředí

Článek A.3.1 uvádí provozní prostředí TOE, článek A.3.2 možnosti ohrožení bezpečnosti a článek A.3.3 bezpečnostní politiku provozované entity

A.4 Cíle zabezpečování

Na možnosti ohrožení bezpečnosti, uvedené v článku A.3.2, jsou cíle zabezpečování stanoveny z hlediska obou aspektů – technických možností, které vycházejí ze systémů EFC nebo provozního prostředí, a možností řízení provozu.

Článek A.4.1 uvádí cíle/možnosti technického zabezpečení, pro ukázku je uvedeno torzo tabulky A.2.

Tabulka 1 – Příklad cílů zabezpečování TOE (tabulka A.2 normy)

č.	Hrozby	Cíle zabezpečování			
		Řízení	Prevence	Detekce	Náprava
1	Padělání a změny OBU (média) (analýza OBU, padělání média OBU a instalace ilegálních transakcí při komunikaci s RSE	Řízení jednotky informací (Opatření proti manipulaci)	Identifikace/ autentizace Pověření k přístupu	Ochrana dat (autentizace zprávy)	Řízení uživatele (záznam do blacklistu)
2	Padělání a zfalšování dat OBU (Padělání údajů vozidla v OBU za účelem snížení poplatků)	Řízení provozu (Kontrola údajů vozidla se smlouvou na služby EFC a data jsou zkontrolována také zařízením na straně infrastruktury.)	Spolehlivost dat (šifrovací funkce) Řízení data platnosti (Kontrola platnosti dat)	Ochrana dat (autentizace zprávy)	Řízení uživatele (záznam do blacklistu)

A.5 Bezpečnostní požadavky

Článek A.5.1 uvádí přehled ISO/IEC 15408, článek A.5.2 funkční požadavky na TOE a článek A.5.3 posouzení zabezpečení TOE.

A.6 Důvod ověření/efektivity

Článek A.6.1 uvádí obecnou charakteristiku článku A.6 a to, že obsahy Profilů zabezpečení jsou zkontrolovány pro stanovení nezbytnosti a míry naplnění bezpečnostních požadavků na TOE. Kontrolované položky jsou tyto:

- všechna bezpečnostní prostředí jsou pokryta;
- cíle zabezpečování by měly zcela splňovat bezpečnostní požadavky;
- Bezpečnostní požadavky by měly implementovat cíle zabezpečování.

Článek A.6 uvádí důvod/ověření (rationale) pro všechny položky popsané v článcích A.1 až A.5. Článek A.6.2 obsahuje důvod síly funkcí, článek A.6.3 důvod pro požadavky na zabezpečení, článek A.6.4 důvod pro požadavky na řízení/ provoz, článek A.6.5 důvod pro metodiku zabezpečení

Příloha B (informativní) Příklady metody posuzování analýzy ohrožení

Tato příloha obsahuje informativní příklad metody posuzování analýzy ohrožení.

Článek B.1 třídí možné hrozby na záměrné (útoky), administrativní a náhodné. Záměrnými jsou podvodné použití zařízení, změna nasbíraných dat a „odposlouchávání“ osobních dat a jejich zneužití. Administrativní hrozby jsou Vniknutí do databáze smluvních odběratelů/uživatelů, Únik osobních dat do sítě, podvodný přístup do systémových databází nebo k řídicím funkcím sítě. Náhodnými hrozbami jsou ty, které jsou zapříčiněny provozními chybami a chybami při přenosu dat.

Článek B.2 uvádí klasifikaci posouzení rizik do pěti úrovní, článek B.3 uvádí vlastní posouzení a možnosti protiopatření.

Příloha C (informativní) Abstrakt z dokumentu „Definice hrozeb a řízení zabezpečení pro rozhraní zpoplatnění v elektronickém výběru poplatků“

Tato příloha je abstraktem z dokumentu CEN/TC278 N780 „Definice hrozeb a řízení zabezpečení pro rozhraní zpoplatnění v elektronickém výběru poplatků“.

Článek C.1 obsahuje úvodní charakteristiky a bezpečnostní rámec (tj. požadavky, služby a mechanismy zabezpečení), článek C.2 popisuje předmět dokumentu, článek C.3 uvádí model EFC (shodný s obrázkem 5), článek C.4 obsahuje cíle a požadavky ochrany soukromí, článek C.5 uvádí analýzu hrozeb včetně obrázku C.2 (shodného s obrázkem 6) a popisuje tři oblasti, do kterých může negativně zasáhnout Nečestná strana: do segmentu uživatele (palubního zařízení), do segmentu poskytovatele služeb (zařízení na straně infrastruktury) a do komunikace mezi těmito dvěma segmenty.

Pro segment uživatele se jedná o manipulaci s hardwarem nebo softwarem uživatele (např. čipovou kartou), napodobování segmentu uživatele imitováním jeho funkcí (nedotýká se hardwaru) a popřením využití služby podvodným uživatelem.

Nečestný poskytovatel služeb může využít stejných hrozeb, např. popře, že obdržel platbu za poskytnuté služby.

Specifikace dále popisuje čtyři možnosti ohrožení komunikace mezi uživatelem a poskytovatelem služeb nečestnou stranou: Odposlouchávání za účelem zneužití informací, Manipulace s vyměňovanými daty (např. pro snížení placené částky), útok vracející odposlechnutou komunikaci (znovupřehrání zpráv – pokus o platbu pomocí certifikátů z předchozích plateb) a Zabránění komunikaci např. vysláním rušícího signálu).

Článek C.6 obsahuje bezpečnostní služby. Pro přehlednost je uvedena celá tabulka C.1.

Tabulka 2 – Bezpečnostní služby jako opatření proti bezpečnostním hrozbám (tabulka C.1 normy)

Obecná hrozba	Bezpečnostní služba	Popis bezpečnostní služby
Manipulace se segmentem	Integrita segmentu	Poskytuje ochranu před fyzickou manipulací se segmentem.
Napodobení segmentu	Autentizace smluvního partnera	Potvrzení, že partner je tím, za koho se vydává.
	Autentizace původu dat	Potvrzení, že zdroj dat je ten, za co se vydává.
Popření	Neodmítnutí s prokázáním původu	Příjemci dat je doručeno potvrzení původu dat.
	Neodmítnutí s prokázáním doručení	Odesilateli dat je doručeno potvrzení o doručení dat.
Odposlouchávání	Spolehlivost	Vlastnost, že údaj není dostupný nebo ukázán neautorizovaným jednotlivcům, entitám nebo procesům.
Manipulace	Integrita dat	Vlastnost, že data nebyla změněna nebo poškozena autorizovaným způsobem.
Znovupřehrání	Časový přehled	Informace závislá na čase ve zprávě obsahující integritu dat.

Dále článek uvádí bezpečnostní profily, mechanismy a jejich standardizaci.

Příloha D (informativní) Vzájemná dohoda pro sjednocení hodnocení bezpečnostních kriterií (CCRA)

Článek D.1 obsahuje obecnou charakteristiku vzájemné dohody pro sjednocení hodnocení bezpečnostních kriterií (CCRA). Článek D.2 uvádí seznam jednotlivých organizací dohody CCRA a článek D.3 seznam registrovaných profilů zabezpečení PP. Tento seznam registrovaných profilů zabezpečení lze v současnosti nalézt na http://www.commoncriteriaportal.org/pp.html.

Souvisící termíny

- mezinárodní registrátor
- odpovědnost
- personalizační karta
- platnost
- požadavky na záruku
- profily ochrany
- poskytovatel přepravní služby; poskytovatel dopravních služeb
- předmět hodnocení
- síla funkce
- soukromí
- správa klíčů
- výběrčí mýtného; subjekt pro výběr mýtného
- informační technologie
- bezpečnostní funkce TOE
- bezpečnostní hrozba
- bezpečnostní politika
- centrální komunikační jednotka
- centrální zařízení
- certifikace
- cíl zabezpečení
- dohoda o uznání společných kritérií
- dostupnost
- důvěrnost
- globální navigační satelitní systémy
- hodnocení úrovně důvěryhodnosti
- zdůvodnění; ověření