

ISO 16461 - Inteligentní dopravní systémy - Kritéria pro ochranu soukromí a integrity v rámci informačních systémů sondy vozidla

Aplikační oblast: [Komunikace \(CALM\)](#)

Rok vydání normy a počet stran: Vydána 2018, 18 stran

Rok zpracování extraktu: 2018

Skupina témat: CALM

Téma normy: CALM plovoucí vozidlo

Charakteristika tématu: ITS systémy - kritéria pro ochranu soukromí a integrity

Úvod, vysvětlení východisek
Stanovení kritérií pro ochranu soukromí a integrity dat
Popis architektury, hierarchie, rolí a vztahů objektů
Popis základního rámce stanovení kategorií ochrany soukromí a integrity dat plovoucích vozidel
Popis procesu / funkce / způsobu použití
Popis přiřazení do kategorií ochrany
Popis rozhraní / API / struktury systému
Definice protokolu / algoritmu / výpočtu
Definice reprezentace dat / fyzikálního významu
Definice konstant / rozsahů / omezení
Definice katalogových hodnot ochrany soukromí a integrity dat

Úvod

ISO 16461 (dále jen "popisovaný dokument") doplňuje normy týkající se problematiky plovoucích vozidel v oblasti ochrany soukromí a integrity.

Použití dat z plovoucích vozidel, tak jak je definováno v normě ISO 22837:2009 vyžaduje zavedení prvků ochrany soukromí osob, využívajících plovoucí vozidla.

Popisovaný dokument řeší následující okruhy problémů spojených s ochranou soukromí:

- Definice požadavků na ochranu soukromí při využití plovoucích vozidel;
- Definice společných vstupů při ochraně soukromí a integrity při sběru dat z plovoucích vozidel;
- Definice konfigurace ochrany plovoucích vozidel ve smyslu ochrany soukromí a integrity.

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

Užití

Popisovaný dokument stanoví postupy a principy ochrany soukromí a integrity při využití plovoucích vozidel a dat z plovoucích vozidel.

Pro orgány státní správy přináší norma pouze informace tak, aby získaly představu o postupech a principech ochrany soukromí a integrity při využití plovoucích vozidel a dat z plovoucích vozidel a mohly tyto znalosti použít při definování požadavků na dodavatele při přípravě zadávací dokumentace.

Pro výrobce telematických zařízení a jejich provozovatele je norma velice důležitá, protože definuje výrobcům a provozovatelům požadavky na implementaci systémů ochrany soukromí a integrity při implementaci systémů plovoucích vozidel a systémů sběru a zpracování dat z plovoucích vozidel.

1. Předmět normy

Tento dokument specifikuje požadavky na ochranu soukromí a ochranu integrity systémů plovoucích vozidel a dat z těchto plovoucích vozidel. Problematika ochrany soukromí a integrity je v dokumentu členěna na:

- Architekturu plovoucích vozidel v návaznosti na ochranu integrity dat a anonymitu plovoucích vozidel;
- Bezpečnostní kritéria a požadavky na plovoucí vozidla;
- Požadavky na správnost a anonymizaci generování a zpracování dat z plovoucích vozidel.

2. Související normy

Souvisejícími normami jsou zejména normy ze skupiny plovoucích vozidel a skupiny norem CALM:

ISO 22837:2009, *Vehicle probe data for wide area communication*

ISO 24100:2010, *Intelligent Transport Systems – Basic principles for personal data protection in probe vehicle systems*

3. Termíny a definice

Norma zavádí některé nové termíny; většina termínů a zkratk je uvedena v normách ISO 22837:2009 a ISO 24100:2010

data sondy (*probe data*) – soubor informací z vozidla

sběrač dat sondy (*probe data collector*) – zařízení, které přijímá data sondy, zpracovává je do tvaru informace ze sondy fúzí dat sondy a dalších doplňujících informací z jiných zdrojů

meziuložení dat sondy (*probe data retention*) – meziuložení surových dat

aplikace plovoucích dat (*probe information application*) – aplikace využívající data z plovoucích vozidel

příjemce informace z plovoucích vozidel (*probe information receiver*) – funkce příjmu informace z dat plovoucích sondy

zpráva z plovoucího vozidla (*probe message*) – strukturovaná datová zpráva z plovoucího vozidla

vytvoření balíčku se zprávou z plovoucího vozidla (*probe package creation*) – funkce, která zabalí data z plovoucího vozidla

příjem balíčku se zprávou z plovoucího vozidla (*probe package reception*) – funkce, která rozbalí data z balíčku se zprávou z plovoucího vozidla

přenos balíčku z plovoucího vozidla (*probe package transfer*) – funkce přenosu balíčku z plovoucího vozidla

vytvoření PDU sondy (*probe PDU creation*) – funkce vytvoření zprávy v PDU formátu (hlavička plus balíček), připravenost pro přenos

příjem PDU sondy (*probe PDU reception*) – funkce příjmu a rozbalení zprávy z PDU formátu (hlavička plus balíček)

přenos PDU sondy (*probe PDU transfer*) – funkce přenosu zprávy v PDU formátu (hlavička plus balíček)

systém plovoucích vozidel (*probe vehicle system*) – systém skládající se z plovoucích vozidel, která vysílají data sondy do datových center, která shromažďují a zpracovávají data z mnoha vozidel

ukládání zpracovaných dat sondy (*processed probe message retention*) – systém ukládání dat sondy

surová data senzoru (*raw sensor data*) – surová, nezpracovaná data ze senzoru

zpracování surových dat senzoru (*raw sensor data*) – zpracování surových dat ze senzoru do formátu dat sondy

vozidlový senzor (*vehicle sensor*) – zařízení ve vozidle, které měří vnější nebo vnitřní podmínky

Další termíny a zkratky z oboru ITS jsou obsaženy ve [slovníku ITS terminology](#).

4. Symboly a zkratky

V kapitole je uveden seznam důležitých zkratk uvedených v normě. Pro účely extraktu je tato množina dále omezena.

FPR Příslušný k do skupiny informací určených k zabezpečení (*Family Privacy Relevant*)

FPR_ANO Anonymní FPR (*Anonymity FPR*)

FPR_PSE Pseudoanonymní FPR (*Pseudonymity FPR*)

FPR_UNL Nepropojitelná FPR (*unlinkability FPR*)

FPR_UNO Neviditelná FPR (*Unobservability FPR*)

FPT_ITI Integrita exportované TSF-FPR (*Integrity of exported TSF FPR*)

PDR Příjem dat sondy (*Probe Data Retention*)

PIC Vytvoření informace ze sondy (*Probe Information Creation*)

PKI Veřejný klíč infrastruktury (*Public Key Infrastructure*)

PMC Vytvoření zprávy z vozidlové sondy (*Probe Message Creation*)

PMP Zpracování vozidlové sondy (*Probe Message Processing*)

PPC Vytvoření balíčku (*probe package creation*)

PPDR Uložení zpracovaných dat (*processed probe data retention*)

PPR Příjem balíčku (*probe package Reception*)

RSDP Zpracování surových dat (*Raw Sensor Data Processing*)

TSF Zpracování cílové bezpečnostní funkce (*Target of evaluation Security Functionality*)

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

5 Referenční architektura

5.1 Vazba na referenční architekturu ITS-S stanice

Kapitola definuje referenční architekturu systémů plovoucích vozidel. Na rozdíl od normy ISO 22837:2009 se nezabývá pouze částí plovoucích vozidel, ale celým řetězcem zpracování dat z plovoucích vozidel.

5.2 Kontextový model pro ochranu soukromí a integrity dat

Kontextový model ochrany dat je uveden na obrázku číslo 1.



Obrázek 1 - Základní rámce ochrany soukromí a integrity dat v systémech plovoucích vozidel (obrázek 1 normy)

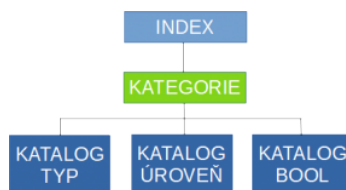
6 Základní rámec

6.1 Přehled

V této kapitole je provedena definice základního rámce ochrany soukromí a integrity dat pro jednotlivé stupně ochrany.

6.2 Struktura rámce

Struktura bezpečnostního rámce je uvedena na obrázku 2. V zásadě jde o to, že každé bezpečnostní úrovni je přiřazena kategorie, které odpovídají definovaná bezpečnostní kritéria z katalogu v normě ČSN ISO/IEC 15408-2:2005, Informační technologie -- Bezpečnostní techniky - kritéria pro hodnocení bezpečnosti IT -- Část 2: Bezpečnostní funkční komponenty.



Obrázek 2 -- Základní struktura rámce ochrany soukromí a integrity dat (obrázek 2 normy)

6.3 Indexy

Je definováno osm funkcí jako Index dle obrázků 1 a 2.

1. Zpracování surových dat
2. Uložení vozidlových dat
3. Tvorba zprávy vozidlových dat
4. Tvorba balíčku
5. Příjem balíčku
6. Zpracování vozidlové zprávy
7. Uložení zpracovaných vozidlových dat
8. Vytvoření informace z vozidlových dat.

Tyto funkce jsou předmětem stanovení způsobu zabezpečení v rámci popisované normy.

6.4 Rámce kategorií

V souladu s ISO/IEC 15408-2 jsou definovány následující kategorie v členění do takzvaných **rodin zabezpečení (třída FPR)**.

FPR_ANO Anonymní FPR (*Anonymity FPR*)

Tato rodina zajišťuje plnou anonymitu uživatele.

FPR_PSE Pseudoanonymní FPR (*Pseudonymity FPR*)

Tato rodina zajišťuje uživateli, že není identifikován, nicméně může být zpětně dohledán.

FPR_UNL Nepropojitelná FPR (*unlinkability FPR*)

Tato rodina zajišťuje uživateli, že může službu použít několikrát. Jednotlivá užití služby spolu ale nelze propojit.

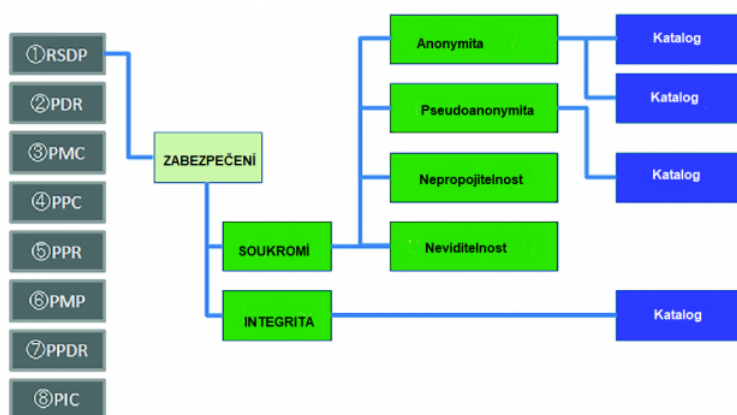
FPR_UNO Neviditelná FPR (*Unobservability FPR*)

Tato rodina zajišťuje, že uživatel může využít službu, aniž by třetí strana byla schopna identifikovat po užití služby.

FPT_ITI Integrita exportované TSF-FPR (*Integrity of exported TSF FPR*)

Tato rodina definuje pravidla pro ochranu před neautorizovanou modifikací dat.

Příklad zařazení jednotlivých rodin bezpečnosti (kategorií) k jednotlivým indexům (funkcím) je na obrázku číslo 3.



Obrázek 3 - Celkový rámec zabezpečení - příklad (obrázek 3 normy)

6.5 Aplikace jednotlivých způsobů zabezpečení v systémech plovoucích vozidel

V rámci této kapitoly jsou podrobně rozebrány možnosti zabezpečení jednotlivých rodin zabezpečení v rámci plovoucích vozidel.

7 Základní rámce

V rámci této kapitoly jsou tabulkovou formou přiřazeny jednotlivé katalogové hodnoty jednotlivým rodinám (kategoriím zabezpečení).