ČESKÁ TECHNICKÁ NORMA

ICS 35. 100. 00
Červen 1999

Informační technologie - Propojení otevřených systémů - Bezpečnostní struktury otevřených systémů: Struktura integrity

ČSN

ISO/IEC 10181-6

36 9694

idt lTU-TX. 815: 1995

Information technology - Open Systems Interconnection - Security frameworks for open systems: Integrity framework

Technologies de l'information - Interconnexion de systèmes ouverts (OSI) - Cadres pour la sécurité dans les systèmes ouverts: Cadre général d'intégrité

Informationstechnik - Kommunikation Offener Systeme - Rahmenrichtlinien für IT Sicherheit in Offener Systemen: Rahmenrichtlinien für die Integrität

Tato norma je českou verzí mezinárodní normy ISO/IEC 10181-6: 1996. Mezinárodní norma ISO/IEC 10181-6: 1996 má status české technické normy.

This standard is the Czech version of the International Standard ISO/IEC 10181-6: 1996. The International Standard ISO/IEC 10181-6: 1996 has the status of a Czech Standard.

Anotace obsahu

Tato mezinárodní norma se zabývá integritou dat při sběru, přenosu a managementu informací. Definuje základní pojetí integrity dat, identifikuje možné třídy mechanismů integrity, identifikuje dílčí služby pro každou z těchto tříd mechanismů integrity, identifikuje management potřebný к podpoře těchto tříd mechanismů integrity, zabývá se interakcí mechanismů integrity a podpůrných služeb s ostatními bezpečnostními službami a mechanismy. Zaměřuje se na zajištění integrity prostřednictvím mechanismů, které nespoléhají výhradně na řízení přístupu.

Národní předmluva

Citované normy

ISO/IEC 7498-1: 1994 zavedena v ČSN EN ISO/IEC 7498-1 Informační technologie - Základní referenční model - Základní model (36 9614)

ISO/IEC 8073: 1992 zavedena v ČSN EN 28073 Informační technologie - Telekomunikace a výměna informací mezi systémy - Propojení otevřených systémů - Protokol pro zajištění transportní služby v režimu se spojením (36 9619), nahrazena ISO/IEC 8073: 1998 dosud nezavedenou

ISO 7498-2: 1989 zavedena v ČSN ISO 7498-2 Systémy na spracovanie informacií - Propojenie otvořených systémov (OSI) - Základný referenčný model - Časť 2: Bezpečnostná architektúra (36 9615)

ISO/IEC 9979: 1991 zavedena v ČSN ISO/IEC 9979 Datové kryptografické techniky. Postupy pro registraci kryptografických algoritmů (36 9781)

ISO/IEC 10181-1: 1996 zavedena v ČSN ISO/IEC 10181-1 Informační technologie - Propojení otevřených systémů - Bezpečnostní struktury otevřených systémů: Přehled (36 9694)

ISO/IEC 10181-2: 1996 zavedena v ČSN ISO/IEC 10181-2 Informační technologie - Propojení otevřených systémů - Bezpečnostní struktury otevřených systémů: Struktura autentizace (36 9694)

ISO/IEC 10181-3: 1996 zavedena v ČSN ISO/IEC 10181-3 Informační technologie - Propojení otevřených systémů - Bezpečnostní struktury otevřených systémů: Struktura řízení přístupu (36 9694)

ISO/IEC 10736: 1995 zavedena v ČSN ISO/IEC 10736 Informační technologie - Telekomunikace a výměna informací mezi systémy - Bezpečnostní protokol transportní vrstvy (36 9245)

ISO/IEC 11577: 1995 zavedena v ČSN ISO/IEC 11577 Informační technologie - Propojení otevřených systémů - Bezpečnostní protokol síťové vrstvy (36 9246)

Upozornění na národní přílohu

Do této normy byla doplněna národní příloha NA, která obsahuje vysvětlivky к textu a slovník použitých termínů.

Vypracování normy

Zpracovatel: Ing. Vladimír Pračke, IČO 40654419

Technická normalizační komise: TNK 20 Informační technologie

Pracovník Českého normalizačního institutu: Ing. Jitka Procházková

MEZINÁRODNÍ NORMA

Informační technologie - Propojení otevřených	ISO/IEC 10181-6
systémů - Bezpečnostní struktury otevřených	První vydání

systémů: Struktura integrity 1996-09-15

ICS 35. 100. 01

Deskriptory: data processing, information interchange, network interconnection, open systems interconnection, communication procedure, protection of information, security techniques

Obsah

Strana

ČSN ISO/IEC 10181-6

Předmluva

ISO (Mezinárodní organizace pro normalizaci) a IEC (Mezinárodní elektrotechnická komise) tvoří specializovaný systém světové normalizace. Národní orgány, které jsou členy ISO a IEC, se podílejí na vývoji mezinárodních norem prostřednictvím technických komisí, zřízených dotyčnou organizací a zabývajících se určitou oblastí technické činnosti. Technické komise ISO a IEC spolupracují v oblastech společných zájmů. Práce se zúčastňují i mezinárodní komise, vládní i nevládní, s nimiž ISO a IEC navázalo pracovní styk.

ISO a IEC ustavily v oblasti informační technologie společnou technickou komisi, ISO/IEC JTC 1. Návrhy mezinárodních norem, přijaté společnou technickou komisí, se rozesílají národním orgánům ke schvalování. Vydání mezinárodní normy vyžaduje souhlas alespoň 75 % hlasujících národních orgánů.

Mezinárodní norma ISO/IEC 10181-6 byla připravena Společnou technickou komisí ISO/IEC JTC 1 Informační technologie, subkomisí SC 21 Propojení otevřených systémů, správa dat a otevřené distribuované zpracování, ve spolupráci s ITU-T. Identický text je publikován jako Doporučení ITU-T X. 815.

ISO/IEC 10181 se skládá z následujících částí se společným názvem Informační technologie - Propojení otevřených systémů - Bezpečnostní struktury otevřených systémů:

- Část 1: Přehled
- Část 2: Struktura autentizace
- Část 3: Struktura řízení přístupu
- Část 4: Struktura nepopiratelnosti
- Část 5: Struktura důvěrnosti
- Část 6: Struktura integrity
- Část 7: Struktura bezpečnostního auditu a alarmů

Přílohy A až D této části ISO/IEC 10181 jsou pouze pro informaci.

ČSN ISO/IEC 10181-6

Úvod

Mnoho aplikací otevřených systémů má bezpečnostní požadavky, které závisí na integritě dat. Tyto požadavky mohou zahrnovat ochranu dat používaných pro zajištění jiných bezpečnostních služeb, jako je autentizace, řízení přístupu, důvěrnost, audit a nepopiratelnost, které mohou, pokud je útočník schopen je modifikovat, omezit nebo anulovat efektivitu těchto služeb.

Vlastnost, že data nebyla pozměněna nebo zničena neautorizovaným způsobem, se nazývá integrita. Toto doporučení | mezinárodní norma definuje obecnou strukturu pro zajištění služeb integrity.

1 Předmět normy

Toto doporučení | mezinárodní norma se zabývá aplikací bezpečnostních služeb v prostředí otevřených systémů, přičemž termín "otevřený systém" zahrnuje takové oblasti jako databáze, distribuované aplikace, otevřené distribuované zpracování a OSI. Bezpečnostní struktury se zaměřují na definování prostředků pro zajištění ochrany systémů a objektů uvnitř systémů a na interakce mezi systémy. Bezpečnostní struktury se nezabývají metodologií konstrukce systémů nebo mechanismů.

Bezpečnostní struktury se zabývají datovými prvky a posloupnostmi operací (ale nikoliv prvky protokolů), které jsou použity κ získání specifických bezpečnostních služeb. Tyto bezpečnostní služby se mohou aplikovat na komunikující entity systémů stejně jako na data vyměňovaná mezi systémy a na data spravovaná systémy.

Toto doporučení | mezinárodní norma se zabývá integritou dat při sběru, přenosu a managementu informací:

1) definuje základní pojetí integrity dat;

2) identifikuje možné třídy mechanismů integrity;

3) identifikuje dílčí služby pro každou z těchto tříd mechanismů integrity;

4) identifikuje management potřebný κ podpoře těchto tříd mechanismů integrity;

5) zabývá se interakcí mechanismů integrity a podpůrných služeb s ostatními bezpečnostními službami a mechanismy.

Tuto strukturu může využívat mnoho různých typů norem, včetně:

1) norem, které zahrnují pojetí integrity;

2) norem, které specifikují abstraktní služby obsahující integritu;

3) norem, které specifikují používání služby integrity;

4) norem, které specifikují prostředky κ poskytnutí integrity v architektuře otevřených systémů; a

5) norem, které specifikují mechanismy integrity. Tyto normy mohou používat tuto strukturu takto:

- normy typu 1), 2), 3), 4) a 5) mohou využívat názvosloví této struktury;

- normy typu 2), 3), 4) a 5) mohou využívat dílčí služby, definované v článku 7;

- normy typu 5) mohou být založeny na charakteristikách mechanismů definovaných v článku 8.

Některé postupy, popsané v této bezpečnostní struktuře, prosazují integritu aplikací kryptografických technik. Tato struktura není závislá na použití specifických kryptografických nebo jiných algoritmů, i když určité třídy mechanismů integrity mohou záviset na vlastnostech konkrétního algoritmu.

POZNÁMKA - Ačkoliv ISO nenormalizuje kryptografické algoritmy, normalizuje v ISO/IEC postupy, používané pro jejich registraci.

Integrita, kterou se toto doporučení | mezinárodní norma zabývá, je integrita vymezená neměnností hodnoty dat. Toto pojetí (neměnnost hodnoty dat) zahrnuje všechny instance, ve kterých jsou různé reprezentace hodnoty dat považovány za ekvivalentní (jako např. různé zakódovaní stejné hodnoty dle ASN. 1). Jiné formy invariance jsou vyloučeny.

Používání termínu data v tomto doporučení | mezinárodní normě zahrnuje všechny typy datových struktur (jako soubory nebo skupiny dat, posloupnosti dat, souborové systémy a databáze).

Tato struktura se zabývá zajištěním integrity těch dat, která jsou považována za přístupná pro zápis pro potenciální útočníky. Proto se zaměřuje na zajištění integrity prostřednictvím mechanismů, jak kryptografických, tak jiných než kryptografických, které nespoléhají výhradně na řízení přístupu.