ČESKA TECHNICKÁ NORMA

ICS 35. 100. 01

Červen 1999

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

ČSN

ISO/IEC 10181-5

36 9694

idt ITU-TX. 814: 1995

Information Technology - Open Systems Interconnection - Security frameworks for open systems: Confidentiality framework

Technologies de l'information - Interconnexion de systèmes ouverts (OSI) - Cadres généraux pour la sécurité des systèmes ouverts: Cadre général de confidentialité

Informationstechnik - Kommunikation Offener Systeme - Rahmenrichtlinien für IT Sicherheit in Offenen Systemen: Vertraulichkeit

Tato norma je českou verzí mezinárodní normy ISO/IEC 10181-5: 1996. Mezinárodní norma ISO/IEC 10181-5: 1996 má status české technické normy.

This standard is the Czech version of the International Standard ISO/IEC 10181-5: 1996. The International Standard ISO/IEC 10181-5: 1996 has the status of a Czech Standard.

© Český normalizační institut, 1999

Podle zákona č. 22/1997 Sb. smějí být české technické normy rozmnožovány

a rozšiřovány jen se souhlasem Českého normalizačního institutu.

56082

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 8473-1: 1994 zavedena v ČSN ISO/IEC 8473-1 Informační technologie - Protokol pro poskytování síťové služby v režimu bez spojení: Specifikace protokolu (36 9658), nahrazena ISO/IEC 8473-1: 1998 dosud nezavedenou

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

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

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

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

Vypracování normy

Zpracovatel: Ing. Alena Hönigová, IČO 61470716

Technická normalizační komise: TNK 20 Informační technologie

Pracovník Českého normalizačního institutu: Ing. Jitka Procházková

ČSN ISO/IEC 10181-5

MEZINÁRODNÍ NORMA

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

ISO/IEC 10181-5

První vydání 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

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 navázalo pracovní styk.

ISO a IEC ustavily v oblasti informační technologie společnou technickou komisi, ISO/IEC JTC1. Návrhy mezinárodních norem přijaté technickými komisemi se rozesílají členům ISO κ hlasování. Vydání mezinárodní normy vyžaduje souhlas alespoň 75% z hlasujících členů.

Mezinárodní norma ISO/IEC 10181-5 byla připravena Společnou technickou komisí ISO/IEC JTC1 Informační technologie, subkomise SC 21 Propojení otevřených systémů, řízení dat a otevřené distribuované zpracování, ve spolupráci s ITU-T. Identický text je vydán jako Doporučení ITU-T X. 814.

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 E této části ISO/IEC 10181 jsou pouze pro informaci.

Úvod

Mnoho aplikací otevřených systémů má bezpečnostní požadavky, které závisí na zamezení odhalení informací. Tyto požadavky mohou zahrnovat ochranu informací používaných při poskytnutí dalších bezpečnostních služeb jako je autentizace, řízení přístupu nebo integrita, které mohou, jsou-li známy útočníkovi, omezit nebo anulovat efektivnost těchto služeb.

Důvěrnost je vlastnost, že informace není dostupná nebo není zpřístupněna neautorizovaným

jednotlivcům, entitám nebo procesům.

Toto doporučení | mezinárodní norma definuje obecnou strukturu pro poskytnutí služeb důvěrnosti.

1 Předmět normy

Toto doporučení | mezinárodní norma o bezpečnostních strukturách otevřených systémů se zabývá aplikací bezpečnostních služeb v prostředí otevřených systémů, kde termín "otevřené systémy" zahrnuje takové oblasti jako jsou databáze, distribuované aplikace, otevřené distribuované zpracování a OSI. Bezpečnostní struktury se zabývají definováním prostředků pro zajištění ochrany systémů a objektů uvnitř systémů a interakcí 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 používány 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 důvěrností informací při jejich vyhledávání, přenosu a managementu:

1) definuje základní pojetí důvěrnosti;

2) identifikuje možné třídy mechanismů důvěrnosti;

3) klasifikuje a identifikuje dílčí služby pro každou z těchto tříd mechanismů důvěrnosti;

4) identifikuje management požadovaný κ podpoře těchto tříd mechanismů důvěrnosti;

5) zabývá se interakcí mechanismu důvěrnosti a podpůrných služeb s dalšími bezpečnostními službami a mechanismy.

Tuto strukturu může využívat řada různých typů norem, včetně:

1) norem, které obsahují toto pojetí důvěrnosti;

2) norem, které specifikují abstraktní služby zahrnující důvěrnost;

3) norem, které specifikují používání služby důvěrnosti;

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

5) norem, které specifikují mechanismy důvěrnosti. Tyto normy mohou používat tuto strukturu následovně:

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

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

- normy typu 5) mohou být založeny na třídách mechanismů definovaných v článku 8 této struktury.

Stejně jako další bezpečnostní služby může být důvěrnost zajištěna pouze v kontextu bezpečnostní politiky definované pro konkrétní aplikaci. Definice specifických bezpečnostních politik není předmětem tohoto doporučení | mezinárodní normy.

Není věcí tohoto doporučení | mezinárodní normy specifikovat podrobnosti výměn protokolů, které je nutné provést, aby se dosáhlo důvěrnosti.

Toto doporučení | mezinárodní norma nespecifikuje konkrétní mechanismy κ podpoře těchto služeb důvěrnosti ani všechny podrobnosti týkající se služeb a protokolů pro bezpečnostní management. Generické mechanismy podporující důvěrnost jsou popsány v článku 8.

Některé z postupů popsaných v této bezpečnostní struktuře dosahují důvěrnost aplikací kryptografických technik. Tato struktura není závislá na použití specifických kryptografických nebo jiných algoritmů, i když určité třídy mechanismů důvěrnosti mohou záviset na vlastnostech konkrétního algoritmu.

POZNÁMKA - Ačkoliv ISO nenormalizuje kryptografické algoritmy, normalizuje postupy použité κ jejich registraci v ISO/IEC 9979: 1991, Postupy pro registraci kryptografických algoritmů.

Tato struktura se zabývá zajištěním důvěrnosti, je-li informace vyjádřena daty, κ nimž mají potenciální útočníci přístup pro čtení. Zahrnuje rovněž důvěrnost toku provozu.