ČESKÁ TECHNICKÁ NORMA

ICS 35.100.00

Duben 1998

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

ČSN
ISO/IEC 10181-2

36 9694

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

Technologies de l'information - Interconnexion de syst è mes ouvertes: Cadre général d'authentification

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

Authentifikation

Tato norma je českou verzí mezinárodní normy ISO/IEC 10181-2:1996. Mezinárodní norma ISO/IEC 101812:1996 má status české technické normy.

This standard is the Czech version of the International Standard ISO/IEC 10181-2:1996. The International Standard ISO/IEC 10181-2:1996 has the status of a Czech standard.

51917

Národní předmluva

Citované normy

ISO/IEC 10181-1:1996 zavedena v ČSN ISO/IEC 10181-1 Informační technologie - Bezpečnostní struktury pro otevřené systémy: Přehled (36 9694)

ISO 7498-2:1989 zavedena v ČSN ISO 7498-2 Systémy na spracovanie informacií - Propojenie otvorených 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 10116:1991 zavedena v ČSN ISO/IEC 10116 Informační technologie - Módy činnosti pro algoritmus n-bitové blokové šifry (36 9742)

Vypracování normy

Zpracovatel normy: Ing. Alena Hönigová, IČO 61470716

Technická normalizační komise: TNK 20 Informační technologie

Pracovník Českého normalizačního institutu: Ing. Jitka Procházková

MEZINÁRODNÍ NORMA
Informační technologie - Propojení otevřených systémů - Bezpečnostní struktury otevřených systémů: Struktura autentizace

ISO/IEC 10181-2
První vydání
1996-05-15

ICS 35.100

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

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 JTC 1. Návrhy

mezinárodních norem přijaté technickými komisemi se rozesílají členům ISO k hlasování. Vydání mezinárodní normy vyžaduje souhlas alespoň 75 % z hlasujících členů.

Mezinárodní norma ISO/IEC 10181-2 byla připravena společnou technickou komisí ISO/IEC JTC 1, *Informační technologie,* subkomise SC 21, *Propojení otevřených systémů, řízení dat a otevřené distribuované zpracování,* ve spolupráci s ITU-T. Identický text je publikován jako Doporučení ITU-T X.811.

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

- *1. část: Přehled*
- *2. část: Struktura autentizace*
- *3. část: Struktura řízení přístupu*
- *4. část: Struktura nepopiratelnosti*
- *5. část: Struktura důvěrnosti*
- *6. část: Struktura integrity*
- *7. část: Struktura bezpečnostního auditu*

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

Úvod

Mnoho aplikací má požadavky na bezpečnost, které mají za cíl ochránit je proti hrozbám, které se vyskytují při komunikaci informací. Některé obecně známé hrozby, spolu s bezpečnostními službami a mechanismy, které mohou být k ochraně proti nim použity, jsou popsány v Doporučení CCITT X.800 ISO 7498-2.

Mnoho aplikací otevřených systémů má bezpečnostní požadavky, které jsou závislé na správné identifikaci příslušných činitelů. Tyto požadavky mohou obsahovat ochranu aktiv a zdrojů před neautorizovaným přístupem. Pro tuto ochranu se mohou použít mechanismy řízení přístupu založené na identitě, a/nebo prosazení individuální zodpovědnosti udržováním auditních logů relevantních událostí, sloužících rovněž pro účely účtování nebo zpoplatňování.

Proces potvrzení identity se nazývá autentizace. Toto doporučení | mezinárodní norma definuje obecnou strukturu pro poskytování autentizačních služeb.

---

1 Předmět normy

Řada doporučení | mezinárodních norem pro bezpečnostní struktury otevřených systémů se zabývá aplikací bezpečnostních služeb v pořadí otevřených systémů, přičemž termín „Otevřené systémy" 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 nikoli prvky protokolů), které jsou používány k 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:

- definuje základní pojetí autentizace;

- identifikuje možné třídy autentizačních mechanismů;

- definuje služby pro tyto třídy autentizačních mechanismů; - identifikuje funkční požadavky na protokoly s cílem podporovat tyto třídy autentizačních mechanismů; a

- identifikuje všeobecné požadavky managementu na autentizaci.

Tuto strukturu může využívat několik různých typů norem včetně:

1) norem, které obsahují pojetí autentizace;

2) norem, které poskytují autentizační službu;

3) norem, které využívají autentizační službu;

4) norem, které specifikují prostředky k poskytnutí autentizace v architektuře otevřených systémů; a

5) norem, které specifikují autentizační mechanismy.

[Všimněme si, že služby, uvedené v b. 2), 3) a 4) mohou obsahovat autentizaci, ale jejich primární účel může být odlišný.]

Uvedené normy mohou použít tuto strukturu:

* normy typu 1), 2), 3), 4) a 5) mohou využít názvosloví této struktury;

* normy typu 2), 3), 4) a 5) mohou využít služby, definované v článku 7 této struktury; a

* normy typu 5) mohou být založeny na mechanismech definovaných v článku 8 této struktury.

Autentizace může být poskytnuta stejně jako jiné bezpečnostní služby pouze v kontextu definované bezpečnostní politiky pro konkrétní aplikaci. Definice bezpečnostních politik jsou mimo rámec tohoto doporučení ITU | mezinárodní normy.

Předmět tohoto doporučení | mezinárodní normy nezahrnuje specifikaci podrobností výměn protokolů,

které musejí být provedeny, aby se dosáhlo autentizace.

Toto doporučení | mezinárodní norma nespecifikuje speciální mechanismy k podpoře těchto autentizačních služeb. Další normy (jako ISO/IEC 9798) se zabývají specifickými autentizačními metodami podrobněji. Příklady takovýchto metod jsou kromě toho součástí dalších norem (jako ITU Dop. X.509 | ISO/IEC 9594-8), kde jsou řešeny specifické autentizační požadavky.

Některé z postupů popsaných v této struktuře dosahují bezpečnost aplikací kryptografických technik.

Tato struktura není závislá na použití konkrétních kryptografických nebo jiných algoritmů, i když určité třídy autentizačních mechanismů mohou záviset na konkrétních vlastnostech algoritmů, například na vlastnosti asymetrie.

POZNÁMKA - Ačkoliv ISO nenormalizuje kryptografické algoritmy, normalizuje v ISO/IEC 9979 postupy, používané pro jejich registraci.

-- Vynechaný text --