elektrorevue
ISSN 1213 - 1539

Rok / Year:	Svazek / Volume:	Číslo / Number:
2011	13	2

Univerzální rámec pro řízení přístupu v počítačových sítích

A universal frame of access control in computer networks

Karel Burda

burda@feec.vutbr.cz

Fakulta elektrotechniky a komunikačních technologií VUT v Brně.

Abstrakt: V článku je popsán univerzální rámec pro řízení přístupu v počítačových sítích, který vznikl v rámci projektu MŠMT 2C08002 - KAAPS. Navržený rámec umožňuje modulární konstrukci libovolně složitého přístupového systému o libovolné topologii. Navržený rámec má otevřený charakter, což dovoluje jeho další rozšiřování.

Abstract: In the paper, a universal frame of access control in computer networks is described. The proposed frame enables the modular construction of arbitrary complex access control system with arbitrary topology. The proposed frame has an open character, which enables its extension in the future.

Univerzální rámec pro řízení přístupu v počítačových sítích

Karel Burda

Fakulta elektrotechniky a komunikačních technologií VUT v Brně
Email: burda@feec.vutbr.cz

Abstrakt *– V článku je popsán univerzální rámec pro řízení přístupu v počítačových sítích, který vznikl v rámci projektu MŠMT 2C08002 - KAAPS. Navržený rámec umožňuje modulární konstrukci libovolně složitého přístupového systému o libovolné topologii. Navržený rámec má otevřený charakter, což dovoluje jeho další rozšiřování.*

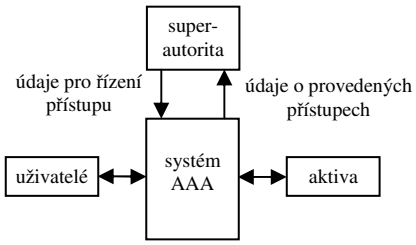
1 Úvod

Počítačové sítě umožňují svým uživatelům využívat různé služby. Poskytovatelé těchto služeb však potřebují přístup k poskytovaným službám regulovat. Účelem této regulace je nejčastěji potřeba zajistit důvěrnost poskytovaných informací nebo potřeba vynutit si platby za poskytované služby. Zmiňovaná regulace se nazývá řízení přístupu a jejím účelem je zajistit, aby poskytované informace nebo služby byly dostupné pouze těm zájemcům, kterým to poskytovatel služby povolil.

Počítačovou síť, jednotlivé počítače nebo síťová zařízení a jimi poskytované služby budeme nazývat počítačovými aktivy nebo zkráceně aktivy. Názvem systém AAA budeme označovat systém určený pro řízení přístupu uživatelů k počítačovým aktivům [1]. Zkratka AAA reprezentuje tři základní procesy vykonávané zmiňovanými systémy. Jedná se o autentizaci (anglicky "Authentication"), o autorizaci ("Authorization") a o účtování ("Accounting").

Správce nebo majitele aktiv budeme nazývat super-autoritou. Super-autorita rozhoduje o zařazení zájemců na seznam oprávněných uživatelů aktiv a stanovuje jejich přístupová práva. Před zařazením zájemce na seznam uživatelů aktiv musí proběhnout iniciační autorizace. V jejím rámci super-autorita se zájemcem sjedná jeho identitu (tj. jeho unikátní označení v rámci seznamu uživatelů aktiv), jeho přístupová práva a autentizační údaje. Autentizační údaje sestávají z dokazovacího faktoru a ověřovacího faktoru. Dokazovací faktor umožňuje uživateli dokázat jeho identitu a ověřovací faktor umožňuje systému AAA ověřit identitu uživatele. Příkladem dokazovacího faktoru je heslo uživatele, soukromý klíč uživatele, obraz otisku jeho prstu apod. Ověřovacím faktorem je například haš uživatelova hesla, veřejný klíč uživatele, popis markantů jeho prstu apod. V případě vzájemné autentizace se sjednají příslušné faktory pro oba směry autentizace.

Po iniciační autorizaci může žadatel získat přístup k aktivům prostřednictvím systému AAA. Systém AAA se logicky nachází mezi uživateli a aktivy (viz obr. 1). Zajišťuje uživatelům přístup k aktivům v souladu s jejich přístupovými právy a taktéž může pro super-autoritu shromažďovat informace o provedených přístupech. To dovoluje jednoznačné účtování služeb nebo bezpečnostní audit aktivit uživatelů.

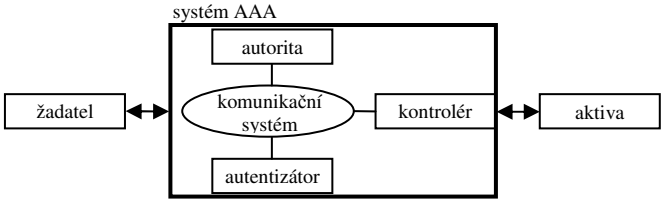


Obrázek 1: Místo systému AAA.

V systémech AAA lze definovat tři základní entity (viz obr. 2):

- kontrolér: entita, která žadatelům umožňuje přístup k aktivům,
- autentizátor: entita, která provádí ověření identity (autentizaci) žadatele,
- autorita: entita, která zajišťuje řízení systému AAA.

Systém AAA funguje následovně. Uživatel nejprve odešle do systému AAA žádost o přístup k aktivům. Následně proběhne autentizace, která proběhne formou komunikace mezi žadatelem a autentizátorem. V rámci této komunikace žadatel prokazuje skutečnost, že disponuje dokazovacím faktorem příslušného uživatele. Autentizátor si tuto skutečnost ověřuje pomocí ověřovacího faktoru, který bezpečným způsobem získal od super-autority. Zpravidla má tyto faktory uloženy ve své lokální databázi nebo je získává od autority. Autentizace může být i oboustranná. V tomto případě si žadatel a autentizátor v průběhu své komunikace stanoveným způsobem vyměňují role. Výstupem autentizace je zpráva o ověření identity žadatele, tzv. výsledek autentizace.



Obrázek 2: Struktura systému AAA.

Výsledek autentizace je předán autoritě. V případě pozitivního výsledku autorita zkontroluje, zda jsou splněny všechny další podmínky pro povolení přístupu a zjistí práva žadatele. Zpravidla je zjišťuje nahlédnutím do své lokální databáze nebo je odvozuje z pravidel stanovených super-autoritou. Na základě zjištěných práv žadatele a případně dalších kontextových informací (např. zatížení kontrolérů) vytvoří autorita dvě zprá-

vy - nařízení pro kontrolér a oprávnění pro žadatele (tzv. autorizace). Tyto dvě zprávy jsou bezpečným způsobem předány jejich adresátům. Nařízení jsou data určená kontroléru, která popisují přístupová práva žadatele a případně uvádějí další potřebné údaje (např. přiřazení IP adresy žadateli). Oprávnění jsou data určená žadateli, která obsahují informaci o poskytnutých právech a popřípadě i další informace (např. IP adresu kontroléru). Pokud je nutno mezi žadatelem a kontrolérem provést další autentizaci, tak nařízení i oprávnění obsahují potřebné autentizační faktory.

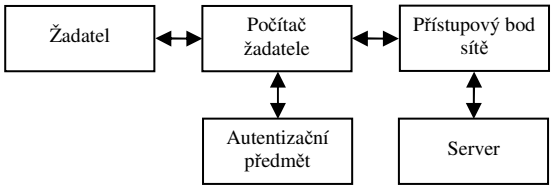
Žadatel obdrží od super-autority oprávnění a kontrolér obdrží nařízení. Na základě informací obsažených v těchto zprávách zahájí komunikaci, v jejímž rámci kontrolér umožní žadateli přístup k aktivům podle práv uvedených v nařízení. Pokud systém AAA zajišťuje i evidenci aktivit uživatelů (tzv. účtování), tak kontrolér zasílá buď autoritě nebo specializované entitě (tzv. účtovateli) informace o přístupech a případně i o jiných aktivitách daného žadatele (např. pokusy o neoprávněný přístup). Tyto informace jsou zpracovávány za účelem pozdějšího auditu nebo vyúčtování služeb.

2 Současný stav

V současné době se v počítačových sítích používá celá řada systémů AAA. K nejznámějším patří systémy založené na protokolech AAA. Jedná se zejména o protokol RADIUS [2] a o jeho nástupce Diameter [3]. Ve firemních sítích je rovněž značně rozšířen systém Kerberos [4]. Pro připojování uživatelských počítačů do lokálních kabelových sítí se používá přístupový systém podle standardu IEEE 802.1X [5] a v případě bezdrátových sítí je hojně používán systém AAA podle standardu IEEE 802.11i [6]. Pro přístup k webovým serverům se stále více používá systém OpenID [7]. Pro lokální řízení přístupu k aktivům jednotlivých počítačů se používá celá řada řešení (např. [8]), které využívají různé autentizační metody (např. autentizace pomocí biometriky, či předmětu).

Celkově lze konstatovat, že v současné době existuje celá řada systémů pro řízení přístupu. Tyto systémy používají různé komunikační protokoly a různé typy autentizace. Jsou určeny pro různé scénáře a specifikům těchto scénářů jsou přizpůsobeny. Důsledkem je pak skutečnost, že existující systémy AAA nejsou navzájem zastupitelné a obvykle nejsou schopny ani vzájemné spolupráce. Každý uživatelský počítač potom musí být hardwarově i softwarově vybaven tak, aby mohl fungovat v rámci stanovených systémů AAA. Různé systémy AAA také poskytují různou úroveň bezpečnosti. Pokud jeden počítač funguje ve více systémech AAA, tak vzniká riziko, že prostřednictvím méně bezpečného systému AAA může být kompromitován bezpečnější systém.

Současný stav řízení přístupu ilustruje obrázek 3. V tomto příkladu musí počítač žadatele nejprve umožnit žadateli, aby se z klávesnice počítače pomocí hesla autentizoval vůči svému autentizačnímu předmětu (např. USB tokenu). Poté počítač prostřednictvím tohoto tokenu uživatele autentizuje a umožní uživateli přístup k aktivům počítače. Dále musí proběhnout interakce se systémem AAA počítačové sítě, aby uživatel získal přes přístupový bod přístup do této sítě. Dále pak musí proběhnout další autentizační interakce s jednotlivými servery, ke kterým žadatel požaduje přístup. V každé z uvedených interakcí je použit jiný systém AAA, jiná autentizace a jiný způsob komunikace. To komplikuje návrh i provoz počítačových systémů a komplikuje i řešení jejich bezpečnosti.



Obrázek 3: Ilustrace současného stavu autentizace a autorizace v počítačových sítích.

3 Univerzální rámec řízení přístupu

Z hlediska systémů AAA lze v počítačových sítích identifikovat následující typy prvků:

- servery,
- počítače uživatelů,
- autentizační zařízení.

Servery poskytují vzdálené služby uživatelům (např. přístup do sítě, přístup k datům v databázi, autentizaci apod.). Počítače uživatelů poskytují uživatelům možnost využívat lokální služby (např. možnost napsat dokument) a možnost využívat vzdálené služby (vyžádání služby, zobrazení odpovědi na dotaz apod.). Autentizační zařízení umožňují uživatelům prokázat svoji identitu prvkům počítačové sítě.

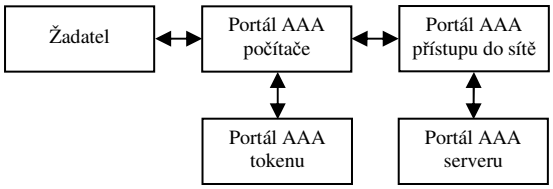
Každý z uvedených typů prvků počítačové sítě obsahuje nějaká aktiva. Aktivem serverů jsou poskytované služby, aktivem uživatelských počítačů jsou obvykle důvěrná data na počítači a zpracovatelské kapacity počítače a aktivem autentizačních zařízení jsou autentizační faktory uživatele. Pro řízení přístupu k uvedeným aktivům se proto nabízí myšlenka implementovat autonomní systém AAA do každého z uvedených typů prvků počítačové sítě. Autonomní AAA systém integrovaný do jediného zařízení se nazývá AAA portál [1]. Každý takový portál v sobě obsahuje všechny prvky systému AAA. Obsahuje autoritu, kontrolér, autentizátor a případně i účtovatele. Autentizátor provádí autentizaci protistrany i autentizaci vlastní, autorita povoluje přístup žadatele k aktivům, kontrolér tento přístup umožňuje a účtovatel vede evidenci o těchto přístupech.

Právě implementace portálu AAA do každého jednotlivého prvku počítačové sítě (tj. do serverů, uživatelských počítačů i autentizačních zařízení) je podstatou navrhovaného univerzálního rámce autentizace a autorizace. Výhodou navrženého rámce je jednotné a univerzální řešení řízení přístupu ke všem aktivům u všech prvků sítě. Předpokládáme, že jednotlivé portály budou mezi sebou komunikovat prostřednictvím speciálního protokolu řízení přístupu ("Access Control Protocol" - ACP). Zprávy protokolu umožní sjednání konkrétních aktiv pro přístup, sjednání typu autentizace, uskutečnění autentizace a také autorizaci. Portály AAA budou rovněž schopny zprávy protokolu ACP tranzitovat.

Zprávy protokolu ACP jsou přenositelné vybranými komunikačními protokoly prakticky v libovolné vrstvě. Zejména půjde o přenos zpráv protokolem TLS ("Transport Layer Security"), EAPoL ("EAP over LAN") a přes USB rozhraní.

Důvodem k preferenci uvedených protokolů je skutečnost, že budou k řízení přístupu používány nejvíce. Výhodou protokolu TLS je implicitní autentizace obou komunikujících stran založená na kryptografii s veřejným klíčem. Tento protokol tak bude používán zejména k zabezpečené komunikaci pomocí ACP protokolu mezi systémy AAA různých super-autorit. Protokol EAPoL je základní protokol k přenosu autentizačních zpráv protokolu EAP (Extensible Authentication Protocol) při řízení přístupu uživatelů do lokálních sítí. Protokol ACP má podobný formát zpráv jako EAP a proto bude protokolem EAPoL přenositelný. Na rozdíl od protokolu EAP však kromě samotné autentizace zajistí i další funkce, jako je sjednání aktiv, sjednání typu autentizace, přenos autorizačních zpráv apod. Komunikace přes USB rozhraní bude důležitá v případě nasazení autentizačních předmětů s uvedeným typem rozhraní. Portál počítače a portál k němu připojeného autentizačního předmětu spolu budou komunikovat zcela stejně jako by se jednalo o vzdálený přístup. Tím se zajistí univerzálnost navrženého řešení z hlediska lokální versus vzdálený přístup.

Výše uvedené řešení komunikujících portálů AAA dovoluje realizovat libovolné přístupové schéma, protože každé zařízení počítačové sítě může plnit v systému AAA libovolnou roli. Ilustrační příklad pro popis navrženého konceptu je uveden na obr. 4. Po připojení autentizačního předmětu (tokenu) uživatele do USB rozhraní počítače spolu začnou komunikovat portál AAA tokenu i počítače. Dojde ke sjednání aktiv (např. možnost práce na daném počítači), dále se sjedná typ autentizace (např. EAP-TLS), provede se autentizace a nakonec i autorizace. Pokud uživatel bude chtít zajistit přístup počítače do sítě, tak portál AAA počítače bude fungovat jako tranzitní uzel pro ACP protokol mezi portálem tokenu uživatele a portálu přístupového bodu do sítě. Tyto dva portály opět mezi sebou sjednají požadovaná aktiva (přístup počítače do sítě), dále se sjedná typ autentizace, provede se autentizace a nakonec i autorizace. Tím uživatel získal přístup do sítě. Předpokládejme nyní, že uživatel bude chtít získat přístup k aktivům nějakého serveru v síti, který požaduje autentizaci jak uživatele tak i počítače. Nejprve proto proběhne ACP protokol mezi portálem počítače a serveru. Na základě úspěšné autorizace se vybuduje šifrovaný TLS spoj mezi počítačem a serverem, který bude použit k běhu ACP protokolu mezi portálem tokenu a portálem serveru. Po následné autentizaci a autorizaci uživatele lze vybudovaný TLS spoj použít pro bezpečný přístup uživatele k aktivům serveru.



Obrázek 4: Ilustrace univerzálního rámce autentizace a autorizace v počítačových sítích.

Donedávna byl kritickým problémem výše popsaného návrhu problém implementace portálu AAA do autentizačních zařízení. Soudobá autentizační zařízení (mobilní telefony, handheldy nebo i čipové karty) však již mají dostatečnou výkonnost k implementaci portálu AAA.

Perspektivně by portály AAA měly být součástí jádra operačního sytému daného prvku. Optimální by bylo sdružení portálu AAA s referenčním monitorem ("reference monitor") [9] bezpečnostního jádra ("security kernel") operačního systému. Referenční monitor bezpečnostního jádra operačního systému řeší přístup uživatelů a procesů k lokálním datům a prostředkům daného prvku. Sdružení navrhovaného portálu AAA s referenčním monitorem by obecným způsobem řešilo přístup uživatelů i procesů jak k lokálním, tak i vzdáleným datům a prostředkům.

V případě operačních systémů, které referenční monitor nemají nebo by nebylo možné do jejich referenčního monitoru zasahovat, se nabízí možnost implementace portálu AAA do virtuálního stroje, na kterém bude daný operační systém běžet. Pokud by nějaká aplikace (např. webovský prohlížeč) požadovala komunikaci s nějakým vzdáleným serverem, tak by virtuální stroj toto volání zachytil a prostřednictvím svého portálu AAA by nejprve zajistil vzájemnou autentizaci obou stran a popřípadě zajistil také kryptografické klíče k navázání šifrované komunikaci mezi oběma autentizovanými stranami.

K praktické realizaci navrženého univerzálního rámce autentizace a autorizace bylo zapotřebí navrhnout dostatečně obecný protokol pro komunikaci mezi portály - protokol ACP. I když se na řízení přístupu obecně zúčastňuje více prvků (žadatel, autentizátor, autorita, kontrolér a účtovatel), tak protokol ACP navrhujeme realizovat jako dvoustranný, tj. komunikuje v něm vždy jen dvojice prvků. Zahrnutí dalších potřebných prvků se realizuje buď sekvenčním zřetězením více běhů protokolu ACP nebo vložením dalšího běhu protokolu do již probíhajícího běhu protokolu. Zmíněný přístup umožňuje jednoduší implementaci složitých interakcí, pro které je dvoustranný protokol ACP základním stavebním modulem.

Sekvenční přístup spočívá v tom, že iniciátor protokolu od druhého prvku získá nějaké aktivum (obvykle potvrzení nebo certifikát), které použije k získání dalšího aktiva v následujícím běhu protokolu. Tento přístup je použit například v protokolu Kerberos [4], kde se žadatel (ST) v prvním běhu protokolu navzájem autentizuje s autentizačním serverem (AS) a získá od něho autentizační faktor pro skupinový server (TGS). V následném druhém běhu protokolu se žadatel ST autentizuje vůči TGS a získá od něho autentizační faktor pro server požadované služby (SS). V posledním třetím běhu se žadatel ST autentizuje vůči serveru SS a získá tak nakonec přístup k požadované službě. Sekvenční zřetězení několika běhů protokolu ACP je výhodné v situaci, kdy iniciátor má k ostatním zúčastněným prvkům přímé (tj. jiným portálem nezprostředkované) síťové připojení.

Přístup vložením spočívá v tom, že při běhu protokolu ACP mezi dvojicí prvků jeden z těchto prvků inicializuje další běh protokolu ACP k jinému prvku. Data mezi těmito dvěma běhy protokolů jsou podle potřeby tranzitována. V rámci druhého běhu protokolu ACP je získáno nějaké aktivum, které umožní dokončit předchozí běh protokolu. Podstatu popsaného přístupu lze ilustrovat na protokolu podle standardu IEEE 802.11i [6]. Žadatel (ST) nejprve zahájí komunikační protokol vůči přístupovému bodu (AP). Ten na základě požadavku od ST spustí protokol k autentizačnímu serveru (AS). Prvek AP zprostředkovává komunikaci mezi ST a AS tak, aby se obě strany navzájem autentizovaly a odvodily autentizační faktory potřebné pro pozdější autentizaci mezi ST a AP. Prvek AS

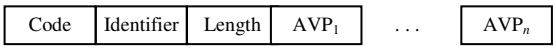
předá odvozené autentizační faktory do AP a tím je běh druhého protokolu ukončen. Prvky ST a AP dále pokračují v běhu prvního protokolu vzájemnou autentizací. Vkládání běhu protokolu je vhodné v situaci, kdy iniciátor může komunikovat jen prostřednictvím jiného portálu AAA. Typicky se jedná o připojení prvku do cizí sítě.

4 Protokol ACP

Protokol ACP ("Access Control Protocol") má zajistit flexibilní komunikaci pro potřeby autentizace, autorizace i účtování jak v počítačových sítích tak i v jednotlivých počítačových zařízeních (např. v počítačích). Protokol umožňuje zajistit komunikaci mezi více uzly, které se na dané transakci podílejí (např. mezi žadatelem z cizí sítě, domácí autoritou a externím autentizátorem). To se předpokládá řešit prostřednictvím ad-hoc sítě pro danou transakci. Transakční síť bude tvořena bezpečnými spoji (typicky TLS nebo fyzicky bezpečnými linkami), mezi kterými budou zprávy protokolu tranzitovat zúčastněné uzly. Uvedené spoje mohou být buď trvalé (typicky mezi prvky sítě jedné organizace) nebo dočasně jen pro potřebu dané transakce (typicky mezi prvky sítí různých organizací). Popsané řešení si vyžaduje síťovou adresaci, jednoduché směrování a možnost tranzitování zpráv.

Komunikace v rámci protokolu ACP probíhá mezi Iniciátorem a Adresátem. Iniciátor je uzel, který zahájil transakci, tj. o něco žádá. Nejčastěji žádá Adresáta o přístup k aktivům nebo o provedení autentizace. Transakci mohou zprostředkovávat jiné uzly, tzv. Zprostředkovatelé. Transakce na sebe mohou navazovat. To znamená, že uzel z jedné transakce se může stát Iniciátorem další transakce. Data ze zpráv těchto souvisejících transakcí mohou být mezi těmito transakcemi tranzitována. Příkladem je situace, kdy domácí autorita musí k autentizaci cizího žadatele otevřít novou transakci k cizí autoritě, která je schopna tohoto žadatele autentizovat.

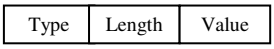
Formát zpráv protokolu ACP je záměrně podobný formátu zpráv protokolu EAP a ilustruje jej obrázek 5.



Obrázek 5: Formát zpráv protokolu ACP.

Popis polí zprávy protokolu ACP:

- Code (1 B): Toto pole odlišuje zprávu protokolu ACP od zprávy protokolu EAP. Odlišení je potřebné v prostředí, kde mohou být provozovány oba protokoly současně. Dále toto pole identifikuje typ zprávy. Binární formát pole je ve tvaru $x_7 x_6 x_5 x_4 x_3 x_2 x_1 x_0$, kde
  - $x_7 = 1$: indikuje zprávu protokolu ACP,
  - $x_6 x_5 x_4 x_3 = 0000$: zatím bez významu,
  - $x_2 x_1 x_0$: určují typ zprávy (viz dále).
- Identifier (3 B): Toto pole je identifikátor transakce v daném spoji. Každá transakce má svůj jedinečný identifikátor, který stanovuje Iniciátor. Aby jej nebylo nutné přenášet v každé zprávě a aby tranzitní uzly nemusely pokaždé analyzovat tělo zprávy, tak je identifikátor transakce přenášen jen v první zprávě transakce a zúčastněné uzly této transakci v každém spoji přiřadí unikátní Identifier. To umožní efektivnější zpracování zpráv v jednotlivých uzlech.
- Length (3 B): Toto pole udává celkovou délku zprávy v bitech. Maximální délka zprávy tak činí $(2^{24}-1)$ bitů ≈ 2MB.
- AVP (Attribute–Value Pair): proměnná se svojí hodnotou ve formátu protokolu ACP. Pole AVP mají formát uvedený na obrázku 6.



Obrázek 6: Formát pole AVP.

Popis polí AVP:

- Type (1 B): Toto pole identifikuje typ AVP.
- Length (2 B): Toto pole popisuje délku hodnoty Value v bajtech.
- Value (0 až 2^{16}-1 B): Toto pole popisuje hodnotu příslušného typu AVP. Velikost pole byla volena tak, že umožní bezproblémové přenosy fotografií (řádově kB), použití moderních kryptografických algoritmů (např. podpis o délce 2048 bitů) i transport celých EAP zpráv.

Tělo každé zprávy může nést více polí typu AVP. Typy AVP pro jednotlivé typy zpráv jsou volitelné. Tvůrce konkrétní implementace ACP protokolu tak má volnost, jakým způsobem bude řešit sjednávání aktiv, sjednávání autentizace, samotnou autentizaci i autorizaci.

V aktuální verzi protokolu ACP je definováno šest typů zpráv:

- Start. Tato zpráva je úvodní zprávou transakce. Odesílá ji vždy Iniciátor a může obsahovat požadované aktivum (pokud Iniciátor zná identifikátor tohoto aktiva) i typ autentizace (pokud Iniciátor zná identifikátor typu autentizace vyžadované Adresátem).
- Finish. Tato zpráva ukončuje transakci. Odesílá ji vždy Adresát. Obsahuje oznámení pro Iniciátora o poskytnutí/neposkytnutí aktiva a případné další údaje (např. certifikát). Zpráva Finish způsobuje v každém uzlu výmaz údajů potřebných k přenosu zpráv dané transakce.
- Offer. Tato zpráva je odesílána Adresátem. Je v ní uvedena nabídka dostupných aktiv nebo nabídka možných typů autentizace. Adresát ji odesílá, když mu požadované aktivum a typ autentizace nebyly sděleny ve zprávě Start.
- Specify. Tato zpráva je odesílána Iniciátorem v reakci na zprávu Offer. Iniciátor v ní volí z nabízených aktiv nebo z nabízených typů autentizace.
- Request. Tyto zprávy jsou odesílány Adresátem v rámci autentizace. Autentizaci zahajuje Adresát vysláním své první zprávy typu Request.
- Response. Tyto zprávy jsou odesílány Iniciátorem v rámci autentizace jako reakce na zprávy typu Request.

Tabulka 1 ilustruje schéma elementární transakce protokolu ACP. V prvním sloupci tabulky jsou uvedeny typy zpráv, které odesílá Iniciátor, druhý sloupec tabulky uvádí typy zpráv odeslané Adresátem a ve třetím sloupci jsou uvedeny doplňující poznámky k jednotlivým krokům protokolu. Každý krok reprezentuje jeden řádek zmiňované tabulky.

Tabulka 1: Schéma elementární transakce protokolu ACP.

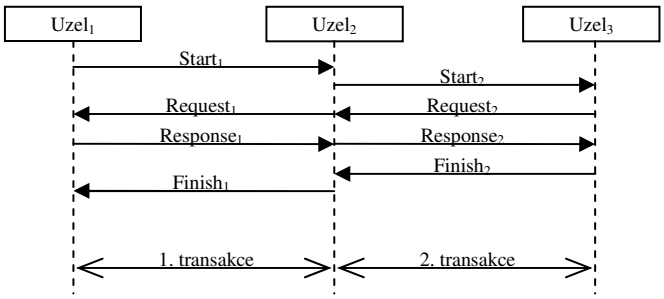
Iniciátor	Adresát	Poznámky
Start →		Zahájení transakce. Zahajuje vždy Iniciátor.
	← Offer	Sjednání požadovaného aktiva. Pokud Iniciátor požadované aktivum uvede již ve zprávě Start nebo existuje jediná možnost, tak může být vynecháno.
Specify →		
	← Offer	Sjednání typu autentizace. Pokud je správný typ autentizace uveden ve zprávě Start, tak může být vynecháno.
Specify →		
	← Request	Výměna autentizačních zpráv. Podle typu autentizace může být dvojic Request - Response více.
Response →		
	← Finish	Sdělení Adresáta o výsledku autorizace a o ukončení transakce.

V případě transakce mezi koncovými uzly bezpečného kanálu (např. v případě TLS kanálu mezi Autoritou a Kontrolérem nebo Kontrolérem a Účtovatelem), lze vypustit i výměnu zpráv typu Request - Response. V těchto případech lze elementární transakci redukovat na výměnu zpráv typu Start - Finish. Například v kanálu Autorita - Kontrolér obsahuje zpráva Start nařízení pro Kontrolér a zpráva Finish obsahuje hlášení Kontroléru o realizaci nařízení.

Elementární transakce lze propojovat a vytvořit transakce, na kterých se podílí více uzlů. Jak již bylo uvedeno, propojení transakcí může nastat zřetězením nebo vložením. Zřetězení transakce je takové propojení, kdy je nová transakce T_{i+1} zahájena až po skončení předchozí transakce T_i, přičemž Iniciátor nové transakce T_{i+1} využije výsledky z předchozí transakce T_i. Příkladem zřetězení transakce je případ, kdy se žadatel v první transakci autentizuje u externího autentizátoru, získá od něho podepsaný certifikát a tímto certifikátem se v následné transakci prokáže autoritě při žádosti o přístup k aktivům.

Vložení transakce je takové propojení, kdy je nová transakce T_{i+1} zahájena v průběhu jiné transakce T_i za účelem dokončení transakce T_i. Data ze zpráv těchto souvisejících transakcí mohou být mezi těmito transakcemi tranzitována. Vložení transakce je typické v případě, kdy Adresát musí k autentizaci Iniciátora využít jiný uzel. Princip vložení transakce ilustruje obrázek 7.

$Uzel_1$ žádá $Uzel_2$ ve zprávě $Start_1$ o určité aktivum a volí správný typ autentizace pro toto aktivum. Není proto zapotřebí uskutečnit výměny typu Offer - Specify a lze rovnou přejít k autentizaci $Uzlu_1$. $Uzel_2$ však tuto autentizaci nemůže provést a proto se připojí k příslušnému Autentizátoru, kterým je $Uzel_3$. Při vybudování připojovacího kanálu (typicky TLS kanálu) se oba koncové uzly navzájem autentizují. $Uzel_2$ v tomto novém kanálu otevírá svoji transakci (transakce číslo 2) vůči $Uzlu_3$. Adresát z 1. transakce je tedy nyní v pozici Iniciátora a $Uzel_3$ je v pozici Adresáta. Zpráva $Start_2$ obsahuje specifikaci požadovaného aktiva (tj. provedení autentizace $Uzlu_1$ a zaslání výsledku autentizace) a obsahuje i specifikaci správného typu autentizace. Není tak opět zapotřebí výměna zpráv Offer - Specify. $Uzel_3$ proto hned zahájí autentizaci vysláním zprávy $Request_2$. $Uzel_2$ vyjme příslušná AVP z této zprávy a umístí je do zprávy $Request_1$, která je zprávou 1. transakce. $Uzel_1$ odešle zprávu $Response_1$, $Uzel_2$ z této zprávy vyjme příslušná AVP a vloží je do zprávy $Response_2$, kterou zašle $Uzlu_3$. Ten provede autentizační výpočet a výsledek autentizace zašle ve zprávě $Finish_2$, kterou je 2. transakce zároveň ukončena. $Uzel_2$ na základě výsledku autentizace rozhodne o výsledku 1. transakce a tento výsledek zašle $Uzlu_1$ ve zprávě $Finish_1$.



Obrázek 7: Princip vložení transakce.

5 Závěr

Existující řešení řízení přístupu (RADIUS, Diameter, Kerberos apod.) používají různé komunikační protokoly, různé formáty zpráv a jsou určeny pro různé scénáře (přístup do sítě, přístup k serveru apod.). Důsledkem je skutečnost, že stávající systémy AAA nejsou navzájem zastupitelné a obvykle nejsou schopny ani vzájemné spolupráce. Každý uživatelský počítač proto musí být hardwarově i softwarově vybaven tak, aby mohl v rámci všech těchto systémů AAA fungovat. Existující systémy AAA navíc řeší pouze problematiku vzdáleného řízení přístupu. Lokální přístup je nutno řešit jinými způsoby.

Univerzální rámec pro řízení přístupu v počítačových sítích je založen na myšlence, že všechna zařízení počítačové sítě (servery, uživatelské počítače i autentizační zařízení) jsou vybavena autonomními portály AAA a že tyto portály jsou schopny prostřednictvím obecného protokolu ACP navzájem spolupracovat. Portál AAA řídí přístup jiných zařízení k aktivům daného zařízení a případně vyjednává i přístup z daného zařízení k aktivům jiných zařízení.

Popsaná myšlenka umožňuje z portálů AAA jednotlivých zařízení sestrojit libovolný distribuovaný systém AAA pro každou organizaci a každou situaci. Každé síťové zařízení má ve svém portálu implementován autentizátor, autoritu, kontrolér i účtovatele. Každé síťové zařízení tak může plnit v nějakém ad-hoc uspořádání libovolnou z uvedených rolí. Například portál počítače může vystupovat jako žadatel vůči nějakém serveru, ale v jiné situaci může naopak vystupovat jako systém AAA, který řídí přístup jiného počítače k datům svého majitele.

Pro zajištění komunikace mezi portály byl navržen protokol ACP. Vzájemným skládáním nebo vkládáním běhů protokolu ACP lze zajistit komunikaci pro prakticky libovolně

strukturovaný a libovolně složitý přístupový systém. Protokol ACP je zároveň z hlediska syntaxe otevřený a tak lze vytvářet přístupové systémy, jejichž bezpečnost je založena na různých kryptografických technikách. Pomocí volitelných AVP v něm lze vytvářet implementace založené na symetrické i asymetrické kryptografii i implementace založené na autentičnosti i důvěrnosti přenášených zpráv. Navazování i vkládání běhů protokolu umožňuje modulární a systematickou bezpečnostní analýzu komunikace navrženého přístupového systému.

V navrženém univerzálním rámci se předpokládá, že zprávy ACP protokolu bude možné přenášet různými komunikačními protokoly v různých vrstvách referenčního modelu OSI (RM-OSI). Portály AAA tak budou moci komunikovat prostřednictvím protokolu TLS, EAPoL, přes USB rozhraní apod. To dovoluje realizovat řízení přístupu v různých vrstvách RM-OSI i použití navrženého rámce v jiných aplikacích (např. v systémech řízení přístupu osob do budov). Zároveň to umožňuje sjednotit implementace pro řízení jak vzdáleného tak i lokálního přístupu.

Zprávy protokolu ACP umožňují sjednání konkrétních aktiv pro přístup, sjednání typu autentizace, uskutečnění autentizace a také autorizaci. Na rozdíl od stávajících řešení, které typ aktiv, typ autentizace i typ autorizace implicitně předpokládají, je režie protokolu ACP poněkud vyšší (vyšší průměrný počet zpráv na jednu transakci). Na druhou stranu protokol ACP nabízí pro řízení přístupu nové možnosti (např. žadatel si může vybírat přístup k jednomu z více nabízených aktiv, lze volit typ autentizace apod.).

Nevýhodou navrženého rámce je, že jeho nasazení vyžaduje poměrně významné zásahy do stávajících řešení. Jedná se zejména o to, že portály AAA by měly být implementovány jako součást bezpečnostního jádra operačních systémů. To bude poměrně pomalý a složitý proces, zejména u zařízení s omezeným výpočetním výkonem (např. autentizační předměty). Na druhou stranu se tím může podstatným způsobem zvýšit obecná bezpečnost počítačů i počítačových sítí.

Poděkování

Tento článek vznikl na základě podpory poskytnuté v rámci projektu MŠMT 2C08002 - KAAPS Výzkum univerzální a komplexní autentizace a autorizace pro pevné a mobilní počítačové sítě, rámec Národní program výzkumu II.

Literatura

[1] K. Burda: AAA systémy a protokoly. Elektrorevue, roč. 2009, č. 46, s. 1 - 7. <http://www.elektrorevue.cz/cz/clanky/informacni-techologie/0/aaa-systemy-a-protokoly/>

[2] C. Rigney, S. Willens, A. Rubens, W. Simpson: Remote Authentication Dial In User Service (RADIUS). [RFC 2865]. IETF 2000. <http://tools.ietf.org/html/rfc2865>

[3] P. Calhoun, J. Loughney, E. Guttman, G. Zorn, J. Arkko: Diameter Base Protocol. [RFC 3588]. IETF 2003. <http://tools.ietf.org/html/rfc3588>

[4] C. Neuman, T. Yu, S. Hartman, K. Raeburn: The Kerberos Network Authentication Service (V5). [RFC 4120]. IETF 2005. <http://tools.ietf.org/html/rfc4120>

[5] -: IEEE Standard for Local and metropolitan area networks. Port Based Network Access Control. [Standard IEEE 802.1X]. IEEE Computer Society, N. York 2004. <http://www.ieee802.org/1/pages/802.1x-2004.html>

[6] -: Medium Access Control (MAC) Security Enhancements. [Standard IEEE 802.11i]. IEEE Computer Society, N. York 2004. <http://standards.ieee.org/getieee802/ download/ 802.11i-2004.pdf>

[7] -: OpenID Authentication 2.0. OpenID 2007. <http://openid.net/specs/openid-authentication-2_0.html>

[8] -: OATH Reference Architecture, Release 2.0. Initiative for Open AuTHentication (OATH). OATH 2007. <http://www.openauthentication.org/webfm_send/1>

[9] Ch. Pfleeger, S. Pfleeger.: Security in computing. Prentice Hall, Upper Saddle River 2003.