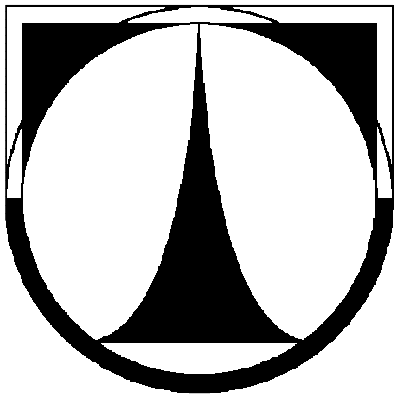
TECHNICKÁ UNIVERZITA V LIBERCI

Fakulta mechatroniky, informatiky a mezioborových studií



AUTOREFERÁT DISERTAČNÍ PRÁCE

Ústí n. L. 2013 Mgr. Jindřich Jelínek

TECHNICKÁ UNIVERZITA V LIBERCI
Fakulta mechatroniky, informatiky a mezioborových studií

Studijní program: P2612 Elektrotechnika a informatika
Studijní obor: 2612V045 Technická kybernetika

Autentizační mechanismy v distribuovaném prostředí a jejich aplikace
Authentication mechanisms in a distributed environments and their applications

Mgr. Jindřich Jelínek

Školitel: doc. RNDr. Pavel Satrapa, Ph.D.
Školící pracoviště: Ústav nových technologií a aplikované informatiky

Rozsah práce:
Počet stran: 105
Počet obrázků a grafů: 40
Počet tabulek: 6

ANOTACE

Disertační práce „Autentizační mechanismy v distribuovaném prostředí a jejich aplikace“ se zaměřuje na problematiku distribuovaných sítí založených na autentizačním protokolu RADIUS, jakou je například v současnosti velmi rozšířená síť *eduroam*. V práci jsou rozebrány dva hlavní směry inovace protokolu RADIUS.

V první části se práce zabývá vylepšením protokolu RADIUS za účelem zvýšení spolehlivosti činnosti distribuované počítačové sítě, která využívá k autentizaci uživatelů stávající implementaci protokolu RADIUS. Byl navržen nový algoritmus činnosti protokolu, který využívá k autentizaci uživatelů dostupné informace ze všech autentizačních serverů systému. Činnost nového algoritmu je simulována s využitím barevných Petriho sítí.

Druhá část práce se zaměřuje na inovaci protokolu RADIUS z hlediska bezpečnosti sítě na systémové úrovni. Práce navrhuje nový přístup k využití protokolu RADIUS Accounting pro předávání bezpečnostních informací o klientech. Zlepšení je založeno na novém systému výměny informací mezi RADIUS servery a spoluprací s nasazenými Intrusion Detection Systémy.

Výsledky této práce mohou přispět k celkovému zvýšení spolehlivosti a bezpečnosti distribuovaných sítí založených na protokolu RADIUS, protože navrhují řešení nevyřešených situací, které mohou nastat.

Klíčová slova

RADIUS protokol, *eduroam*, distribuovaná počítačová síť, IDS, autentizační mechanismus, Petriho sítě, CPN Tools

ABSTRACT

PhD thesis “Authentication mechanisms in a distributed environments and their applications“ focuses on issues of distributed networks based on the RADIUS authentication protocol, such as the currently widespread *eduroam* network. Two main directions of innovation of the RADIUS protocol are discussed in this work.

The first part of the thesis deals with improving the RADIUS protocol to increase reliability in the distributed computer networks using existing implementation of the RADIUS protocol for authentication of users. Operations of the new algorithm are simulated by colored Petri nets.

The second part focuses on innovation of the RADIUS protocol in terms of network security at the system level. We propose a new approach to use the RADIUS Accounting protocol for transmission of a security information about clients. The improvement is based on a new system of exchanging information between RADIUS servers and cooperating Intrusion Detection Systems.

The results of this work may contribute to the overall reliability and security of distributed networks based on the RADIUS protocol because it proposes solutions of unsolved situations which may occur.

Key words

RADIUS Protocol, Eduroam, Distributed Computer Network, IDS, Authentication Mechanism, Petri Nets, CPN Tools

OBSAH

Anotace ..... - 1 -

Abstract ..... - 2 -

1 Úvod ..... - 4 -

2 Cíle disertační práce ..... - 7 -

3 Protokol RADIUS ..... - 8 -

3.1 Vlastnosti a činnost protokolu ..... - 8 -

3.2 Typy a formát paketů ..... - 9 -

4 Návrh inovace protokolu RADIUS z hlediska spolehlivosti ..... - 11 -

4.1 Popis aktuálního algoritmu ..... - 11 -

4.2 Model vylepšeného protokolu ..... - 14 -

4.3 Ověření činnosti vylepšeného protokolu ..... - 18 -

5 Návrh inovace protokolu RADIUS z hlediska bezpečnosti ..... - 23 -

5.1 Základní východiska ..... - 23 -

5.2 Návrh řešení pro zlepšení bezpečnosti ..... - 25 -

5.3 Bezpečnostní zprávy a atributy ..... - 29 -

5.4 Příklad bezpečnostních politik systému ..... - 30 -

6 Závěr ..... - 31 -

Přehled publikační činnosti autora ..... - 32 -

Použité zdroje ..... - 32 -

1 ÚVOD

Rostoucí portfolio, kvalita a dostupnost služeb internetu vedou jeho uživatele ke snaze získat dostatečně rychlé připojení na libovolném místě. Kromě jiných možností lze zaznamenat rozvoj tzv. **distribuovaných sítí**. Jejich základní charakteristikou je, že se vyskytují na velkém území, jsou heterogenní, rozptýlené a mají různé "provozovatele" i technická řešení.

Příslušná oblast („doména", resp. jednoznačný identifikátor) sítě se označuje jako **realm.** Tyto sítě primárně slouží pro poskytování připojení k internetu a příp. intranetových služeb domovské sítě příslušnému uživateli, i když se fyzicky nachází na geograficky vzdáleném místě od této domovské sítě. Charakteristikou těchto vzájemně propojených sítí je obrovské množství potenciálních uživatelů, kteří mohou migrovat mezi jednotlivými dílčími oblastmi této distribuované sítě. Další charakteristickou vlastností obdobných sítí je **federativní uspořádání** připojených institucí[i]. Jednotlivé instituce zapojené v dané federaci rozdělujeme na **poskytovatele identit** a **poskytovatele služeb**. Poskytovatel identity je vždy vůči danému uživateli jen jeden. Síť poskytovatele identity uživatele pak označujeme jako *domovskou síť* tohoto uživatele. Vůči danému uživateli jsou sítě ostatních institucí, než síť poskytovatele identity (domovská síť), v roli poskytovatele služeb.

Reálně fungujícím příkladem distribuované sítě s federativní autentizací [1] je akademická bezdrátová síť ***eduroam***, kterou využijeme jako vhodné modelové prostředí pro nastíněné problémy a jejich řešení.

Motivací pro vznik sítě ***eduroam*** bylo umožnit uživateli jedné sítě přístup k internetu a případně ke službám své domovské sítě, i když k ní není fyzicky připojen. Organizátorem sítě ***eduroam*** v České republice je CESNET a participují na ní další připojené organizace.

Ze systémového hlediska jsou distribuční sítí ***eduroam***u veřejné sítě. V současnosti je to v ČR především síť CESNET2, nicméně systém byl navržen

[i] Federativním uspořádáním se rozumí fakt, že instituce zapojené do takové federace mají vlastní nezávislou správu své sítě, přičemž v souvislosti s provozováním společné distribuované sítě spolu navzájem spolupracují na základě nějakých společně definovaných pravidel [2].

tak, aby mohl pracovat nad libovolnou (i nedůvěryhodnou) sítí. Bezpečnostní roli v rámci ***eduroam*** zajišťuje autentizační a autorizační infrastruktura (AAI). Zásadní pozici v tomto hraje systém vzájemně propojených RADIUS serverů jednotlivých organizací (členů federace) založený na autentizačním protokolu RADIUS. Významnou úlohu mají také další autentizační protokoly, které zajišťují autentizaci uživatele při komunikaci s přístupovým bodem bezdrátové sítě (viz dále). Systém distribuované bezpečnosti je postaven především na protokolech IEEE 802.1X a RADIUS, viz kapitola 3.

Důležitým dokumentem, popisujícím činnost sítě ***eduroam***, je takzvaná **Roamingová politika** [2], která upravuje vztahy mezi jednotlivými členskými institucemi české ***eduroam*** federace. Tento dokument definuje jednotlivé role institucí v ***eduroam*** federaci, upravuje připojení a odpojení členských institucí, řešení bezpečnostních incidentů, pravidla pro uchovávání auditních informací apod.

Základní role v ***eduroam*** federaci podle [2] jsou:

- správce ***eduroam*** federace,
- poskytovatel identity,
- poskytovatel zdrojů,
- uživatel.

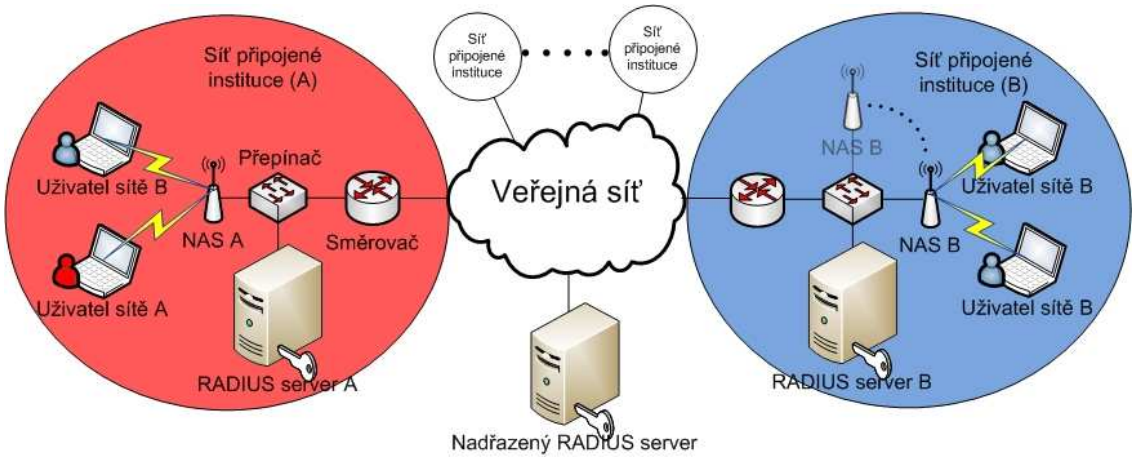
Jednotlivé role mají definovaná práva a povinnosti. Zjednodušené schema sítě ***eduroam*** je patrné z obr. 1.

Správce federace je odpovědný za koordinaci dění ve federaci, připojování a odpojování členů federace, dodržování pravidel, připojení k mezinárodní federaci ***eduroam***, správu nadřazených RADIUS serverů a jejich fungování. Dále provádí logování informací o autentizačním provozu a technickou podporu pro členy federace.

Poskytovatel identity je zobrazen na obr. 1 jako instituce A nebo B a jeho úkolem je vést databázi uživatelů sítě ***eduroam***, které eviduje ve své organizaci, a provádět jejich autentizaci ve vztahu ke všem členům federace. Dále provozuje své autentizační servery a zajišťuje jejich napojení na národní autentizační servery a zabezpečenou činnost. Samozřejmou součástí činností

poskytovatele identity je logování informací o autentizaci, řešení bezpečnostních incidentů apod.

Poskytovatel zdrojů je instituce, která v rámci federace nabízí své služby. Jedná se především o poskytnutí konektivity, připojení k intranetovým aplikacím apod. Služby jsou poskytnuty pro daného uživatele pouze v případě jeho kladné autentizace u poskytovatele identity, jinak je přístup ke službám zamítnut. A to bez rozdílu toho, zda uživatel zadal nesprávné autentizační údaje, nebo došlo k technickým problémům na straně poskytovatele identity. Samozřejmou součástí činností poskytovatele zdrojů je logování informací o autentizačních informacích, řešení bezpečnostních incidentů apod.



obr. 1 Schéma distribuované sítě *eduroam*

Uživatel je na obr. 1 zobrazen jak pro domovskou síť A (červený), tak pro domovskou síť B (modrý). Uživatel musí mít právní vztah k poskytovateli identity a musí se řídit povinnostmi definovanými Roamingovou politikou a dalšími pravidly poskytovatele indentity a poskytovatelů zdrojů. Služby, které jsou poskytovány sítí ***eduroam***, jsou bezplatné, a tedy na ně není právní nárok, ale jsou poskytovány jako „best effort“. Přesný rozsah služeb pro uživatele definují pravidla příslušného poskytovatele služeb.

Z uvedeného je zřejmé, že jednotlivé logovací informace o autentizaci, o činnosti uživatelů a podobně jsou v systému ukládány distribuovaně bez vzájemného vztahu. Z Roamingové politiky dále plyne, že jejich ukládací doba je 6 měsíců a že si je jednotlivé subjekty poskytují ad hoc při řešení bezpečnostních incidentů. Stejně tak při technických problémech v síti nelze použít dostupné informace umístěné v jiném místě, než v domovské síti.

2 CÍLE DISERTAČNÍ PRÁCE

Mezi jednotlivými uzly v sítích s federativní autentizací (jako např. ***eduroam***) existuje komunikace na bázi protokolu RADIUS, přičemž tento protokol se také využívá pro částečné logování činností uživatelů a prvků sítě. Na systémové úrovni se v případě takové sítě jedná o distribuovanou databázi, která poskytuje svým uživatelům služby. Na služby sítě ***eduroam*** není nárok, a navíc je zřejmé, že v předloženém systému není zaveden žádný mechanismus pro podporu spolehlivosti, tedy například při výpadku autentizačního serveru není služba dostupná. To odpovídá deklarované filozofii sítě na úrovni „best effort“, což může být do budoucna omezujícím faktorem pro další rozvoj sítí s federativní autentizací.

Problémy mohou vznikat také při pokusech uživatelů zneužít k nepovoleným účelům či jinak napadnout síť poskytovatele služeb nebo jeho síť využít k útokům na jiné sítě. O takovém chování uživatele se poskytovatel identity tohoto uživatele nemusí vůbec dozvědět, natož aby mohl účinně proti němu zasáhnout.

Obecným cílem této práce je **nalezení mechanismů pro zvýšení spolehlivosti a bezpečnosti protokolu RADIUS** v distribuovaných sítích s federativní autentizací a využít přitom prostředí modelové sítě ***eduroam***.

V souvislosti s tím bude třeba **navrhnout úpravu protokolů a/nebo algoritmů zúčastněných prvků**, případně interních bezpečnostních dokumentů provozovatelů distribuovaných sítí (Roamingové politiky) v souvislosti s výše uvedenými mechanismy pro podporu spolehlivosti a bezpečnosti distribuovaných sítí s federativní autentizací, včetně případného rozšíření vazby mezi poskytovateli zdrojů a identit a se zohledněním ochrany soukromí uživatelů daných sítí.

Dílčím cílem práce je najít vhodný algoritmus pro řešení problému s výpadkem domovského autentizačního RADIUS serveru, který zajistí autentizaci uživatele z jiného autentizačního serveru po dohodě mezi uzly a navrhnout inovaci protokolu RADIUS v tomto směru. Předložený algoritmus by měl být využitelný i v síti s velkým množstvím uzlů a měl by být schopen činnosti v asynchronním distribuovaném systému [3]. V této souvislosti je třeba najít vhodný simulační

nástroj a ověřit činnost nalezeného algoritmu ve spolupráci s protokolem RADIUS v simulovaném prostředí.

Dalším dílčím cílem je navrhnout, jak vylepšit protokol RADIUS o možnost sledování chování uživatelů v distribuované síti s federativní autentizací se zaměřením na bezpečnost systému, a s využitím volitelných atributů protokolu RADIUS vyřešit, jak předávat tyto informace mezi jednotlivé autentizační servery.

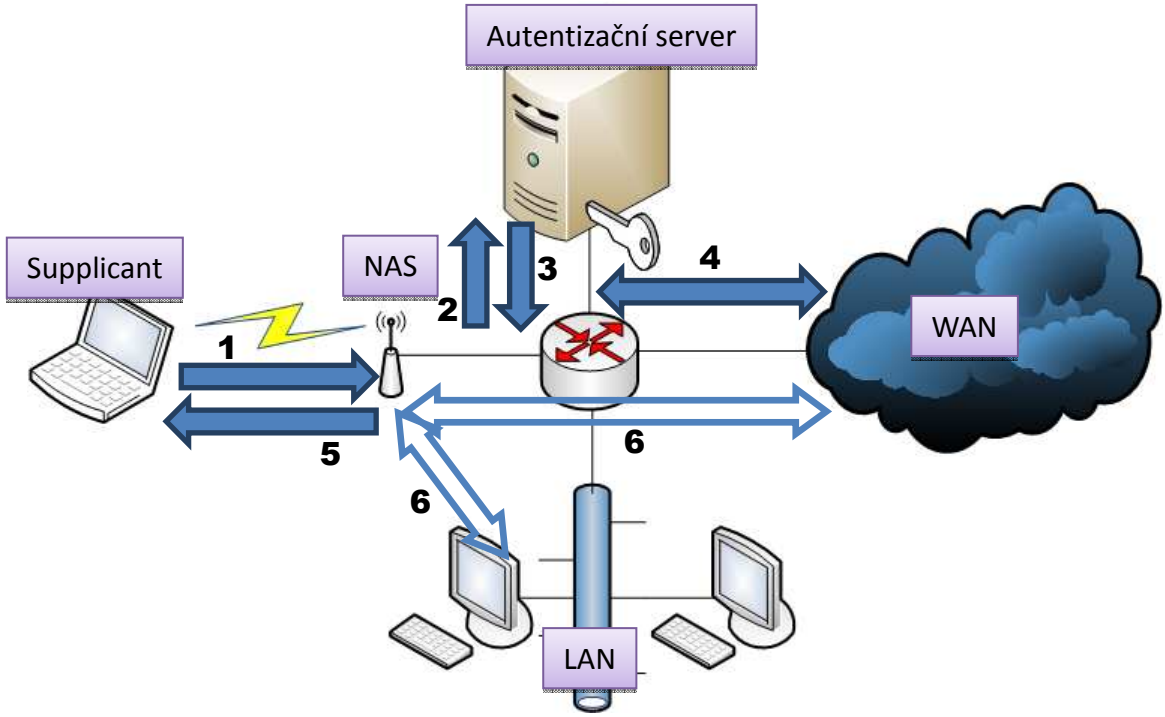
3 PROTOKOL RADIUS

3.1 Vlastnosti a činnost protokolu

Protokol RADIUS (Remote Access Dial-in User Server) je distribuovaný autentizační protokol typu klient/server, který pochází z roku 2000 od společnosti Livingston Enterprises. Je to protokol podporující technologii AAA, přičemž autentizace a autorizace jsou shrnuty v RFC2865 [3] a auditování je v samostatném RFC2866 [4]. Protokol podporuje spolupráci s protokoly TACACS+ a Kerberos a je součástí nejrůznějších systémů, které požadují poměrně vysoký stupeň zabezpečení. Výhodou tohoto protokolu – kromě velkého rozšíření – je také otevřenost standardu. V rámci činnosti protokolu RADIUS vystupují čtyři základní subjekty, viz obr. 2.

Jedná se o uživatele, který požaduje přístup do sítě a který je označován jako **supplicant** (prosebník). Dále zde je **klient**, kterým je příslušný přístupový server NAS (např. přístupový bod sítě WiFi). Neposledním je **autentizační server**, jenž obsahuje serverovou část systému RADIUS, a je na něm provozována **databáze** klientů, kteří mají mít přístup do sítě, vůči které je prováděna autentizace. Protokol RADIUS pracuje nad protokolem UDP [5] (port 1812 či 1645), pomocí kterého probíhá přenos zpráv mezi přístupovým serverem a zabezpečovacím serverem. Jak již bylo naznačeno výše, propojeny jsou autentizace s autorizací, přičemž accounting lze provozovat odděleně. Server přijímá od klientů autentizační informace (které získají protokolem PPP od supplicantů) a posílá jim zpět rozhodnutí o autentizaci (kladné nebo

záporné). Autentizace probíhá na základě uživatelského jména a hesla, které je zasíláno zabezpečené pomocí algoritmu MD5 [6].



obr. 2 Přístup do sítě s využitím protokolu RADIUS

Na obr. 2 je schematicky znázorněn průběh autentizace. V prvním kroku požádá supplicant o autentizaci příslušný NAS protokolem PPP-EAP, tento požadavek předá NAS protokolem RADIUS příslušnému RADIUS serveru (bod 2), který jej buď vyřídí sám (body 3 a 5) nebo jej předá k vyřízení příslušnému dalšímu RADIUS serveru podle realmu uživatele (body 4 a 5). V dalším kroku je pak v případě kladné autentizace otevřen požadovaný port NAS. Tím je umožněna uživateli komunikace do LAN či WAN (bod 6).

3.2 Typy a formát paketů

Do zprávy transportního protokolu UDP nebo TCP je zabalena vždy právě jedna RADIUS zpráva (viz obr. 3) a cílový port je nastaven na 1812, přičemž při odpovědi jsou cílový a zdrojový port prohozeny.

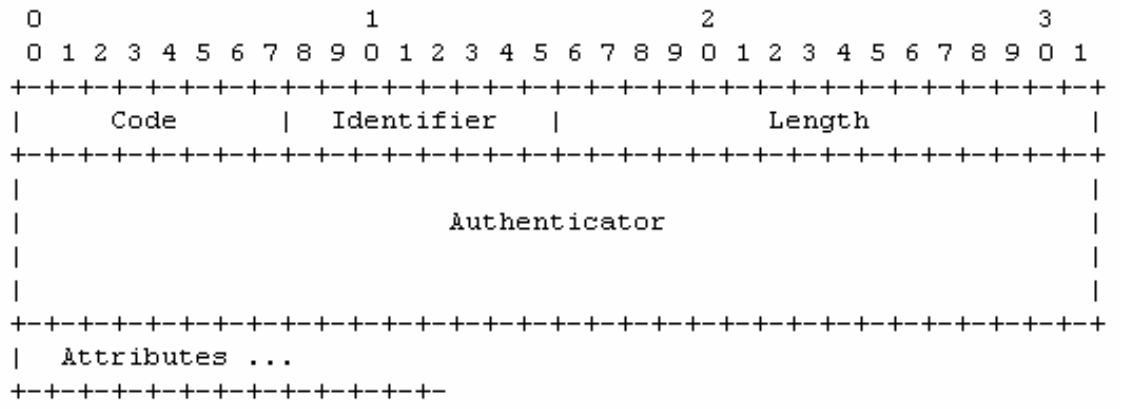
Pole uvedená na obr. 3 budou přenášena zleva doprava. Protokol RADIUS disponuje až 255 typy paketů (pole Code může obsahovat hodnoty 1-255). Registrací jednotlivých typů paketů a přidělováním jejich čísel se zabývá

IANA [8]. V současné době je obsazeno přibližně padesát typů paketů, zbytek je volný, výjimečně rezervovaný.

Není smyslem této práce uvádět celý výčet typů paketů, zde je výběr následujících nejzajímavějších (uvedené číslo je decimální hodnota pole Code):

1 Access-Request
2 Access-Accept
3 Access-Reject
4 Accounting-Request
5 Accounting-Response
10 Accounting-Message
11 Access-Chalenge

Vzhledem k jejich označení není zřejmě nutné tyto typy paketů detailněji popisovat; accounting pakety využívá RADIUS accounting server, access pakety jsou pak použity standardním RADIUS protokolem.



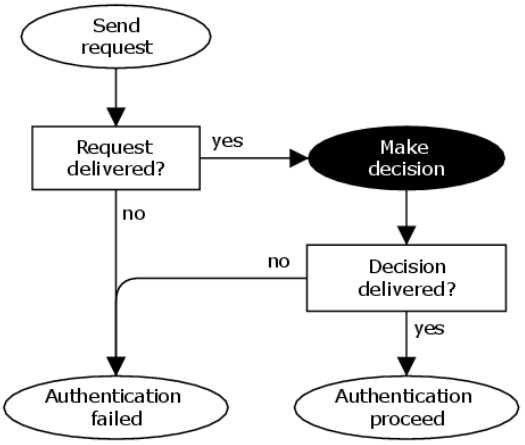
obr. 3 Formát zprávy protokolu RADIUS (převzato z [3])

Podobně jako lze v protokolu RADIUS definovat nové typy paketů, je možné definovat také jednotlivé atributy. Protokol nabízí opět celkem 255 možných atributů. Obsazených je aktuálně přibližně 140 atributů, zbytek je převážně volný.

4 NÁVRH INOVACE PROTOKOLU RADIUS Z HLEDISKA SPOLEHLIVOSTI

4.1 Popis aktuálního algoritmu

Protokol RADIUS pracuje v distribuovaném prostředí tak, že autentizační požadavek uživatele předá k vyřešení domovskému autentizačnímu serveru tohoto uživatele prostřednictvím nespolehlivé počítačové sítě. Autentizační požadavek odešle server-odesílatel, ale domovský server uživatele jej nemusí vůbec obdržet v případě, že přenosová trasa je dočasně nedostupná nebo je domovský autentizační server mimo provoz (tyto případy označme souhrnně pojmem „**chybové stavy komunikace**“). Autentizační protokol RADIUS je součástí aplikační vrstvy podle modelu ISO/OSI a v jeho konstrukci obvykle nejsou nástroje, které by tyto chybové stavy komunikace ošetřovaly. V tomto směru se RADIUS spoléhá na protokoly nižší vrstvy.




```
DO send request
IF request delivered THEN
       DO make decision
       IF decision delivered THEN
        RETURN authentication proceed
       ELSE RETURN authentication failed
ELSE RETURN authentication failed
```

obr. 4 Diagram a pseudokód stávajícího algoritmu

Algoritmus chování protokolu RADIUS je názorně zobrazen na obr. 4. V případě doručení požadavku na autentizaci domovský autentizační RADIUS server požadavek porovná se svou databází uživatelů. Verifikuje uživatelské jméno a heslo a podle výsledku buď požadavek akceptuje, nebo jej zamítne. Své rozhodnutí poté obdobným způsobem odešle zpět serveru-odesílateli. Pokud rozhodnutí serveru-odesílateli dorazí, považujeme proces autentizace za úspěšný (bez ohledu na to, zda uživatel byl autentizován nebo byl jeho pokus

zamítnut). I v případě doručování rozhodnutí však může dojít k selhání přenosové cesty.

Jednou z nevýhod stávajícího řešení je selhání autentizace, pokud dojde k chybovému stavu komunikace. Systém je v současnosti nastaven tak, že pokud je domovský autentizační server nedostupný nebo nereaguje v časovém limitu, server-odesílatel požadavek na autentizaci klienta zamítne, protože autentizace na vzdáleném serveru selže. Toto pravidlo je definováno na straně 4, bod 4.3.1 platné Roamingové politiky [2]. Dále bude stručně uveden námi navržený algoritmus, který tento problém minimalizuje a zvyšuje spolehlivost systému, více je v kapitole 5 disertační práce.

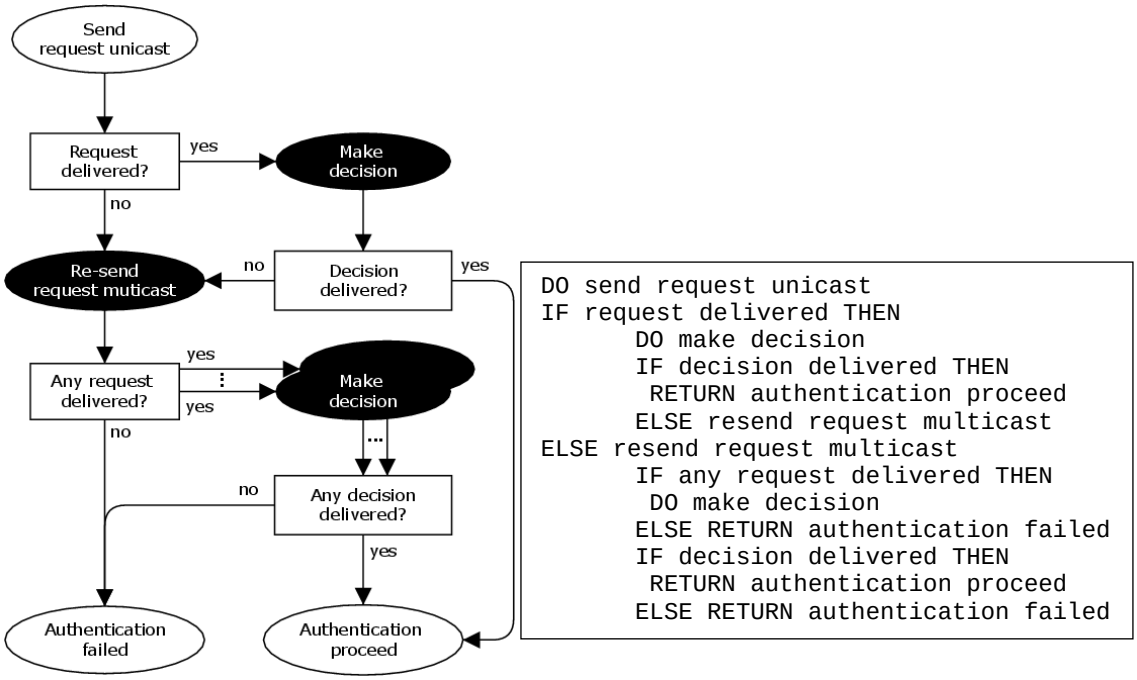
4.1.1 Popis vylepšeného algoritmu

Princip řešení je založen na faktu, že distribuovaná síť s federativní autentizací může být tvořena mnoha servery. Autentizační informace o uživateli tak může být uložena nejen v jeho domovském serveru (v serveru poskytovatele identity), ale i na jiných serverech (tedy – z hlediska daného uživatele – serverech poskytovatelů služeb). K uložení autentizační informace na jiný než domovský server dojde tehdy, když uživatel využije tento autentizační server poskytovatele zdrojů k přihlášení do sítě.

Tento server se obrátí na domovský server poskytovatele identity uživatele a po případné úspěšné autentizaci si informaci uloží do zvláštní databáze (viz dále), jak bylo popsáno v předchozím odstavci. Hlavní myšlenka vylepšení protokolu RADIUS uvažuje s možností využít autentizační informace uživatele uložené na všech dostupných serverech, kde by se mohly nacházet, nikoliv pouze na serveru poskytovatele identity. Vhodnou aplikací tohoto záměru do praxe může dojít ke snížení autentizačních selhání zejména u uživatelů, kteří využívají velký počet poskytovatelů zdrojů (tedy relativně hodně „cestují“).

Námi navržený algoritmus při výskytu chybového stavu komunikace kontaktuje nějakou formou určené servery v dané doméně (nejlépe všechny) a pokusí se provést autentizaci uživatele pomocí jejich informací. Výběr oslovených serverů bude závislý na dohodě mezi jednotlivými poskytovateli služeb. Algoritmus popsaného chování je zobrazen na obr. 5. Oslovené servery standardním

způsobem na žádost reagují tak, jako by jim byla primárně určena. Nicméně, vzhledem k tomu, že nejsou správci realmu uživatele, o jehož autentizaci se žádá, nemohou použít databázi uživatelů, kterou vedou v roli poskytovatelé identity. Pro rozhodnutí musí použít databázi uživatelů, kteří jejich služby využili jako poskytovatele zdrojů. Tuto databázi označme „**cache databáze**“, protože záznamy v ní by měly sloužit pro opakované žádosti o autentizaci a měly by mít časově omezenou platnost.



obr. 5 Diagram a pseudokód vylepšeného algoritmu

Po provedení rozhodnutí oslovené servery odešlou serveru-odesílateli své stanovisko. Server-odesílatel nějakým způsobem doručené odpovědi vyhodnotí a odešle Supplicantovi konečnou odpověď. Způsob vyhodnocení může být různý – od „hlasování“ všech zúčastněných až po direktivní rozhodnutí serveru-odesílatele. Příslušnou instanci nového algoritmu zodpovědnou za výše uvedené rozhodování označme pojmem **adjudikátor**. Některé možnosti realizace adjudikátorů budou popsány v odstavci 4.2.2.

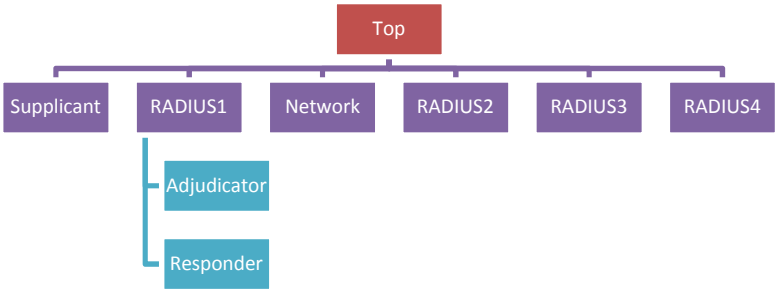
Navržený způsob řešení problému nebude vyžadovat změnu protokolu RADIUS jako takového, resp. nebude vyžadovat změnu jiných protokolů. Cíle lze dosáhnout výše popsanou změnou algoritmu chování koncových prvků, tedy úpravou softwarové implementace protokolu RADIUS a doplněním nového prvku – cache databáze.

Předem lze dovodit, že tento způsob fungování povede k většímu zatížení sítě a zpoždění reakce na požadavek o autentizaci, ale nejspíše významně sníží možnost celkového selhání autentizace. Pro ověření těchto předpokladů a jejich přibližnou kvantifikaci byl vytvořen model vylepšeného protokolu a na tomto modelu byly provedeny experimenty.

4.2 Model vylepšeného protokolu

4.2.1 Základní popis

Model protokolu s výše navrženým algoritmem byl vytvořen v barevných Petriho sítích [7], [8] s pomocí aplikace CPN Tools [9] a byl publikován viz [C, D]. Model je přiložen k této práci jako softwarové přílohy B.1 – B.3. Jedná se o hierarchický model, který má tři úrovně. Schéma s barevným zohledněním hierarchie sekcí je na obr. 6.

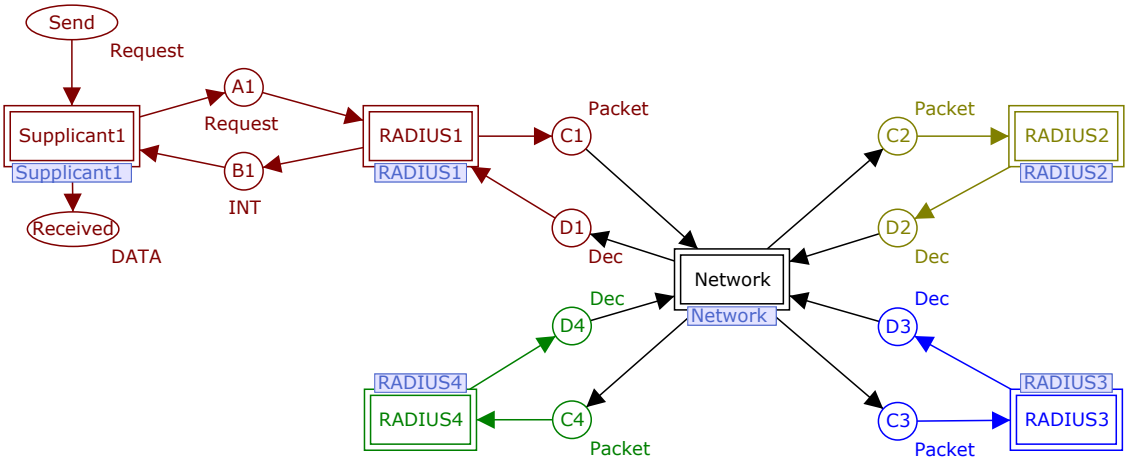


obr. 6 Schéma hierarchického modelu

Zde je vidět šest základních sekcí modelu – *Supplicant1*, *RADIUS1* - *4* a *Network*. Sekce *RADIUS1* se dělí na dvě subsekce *Adjudicator*, která slouží pro rozhodování, a *Responder*, jenž generuje automatické záporné odpovědi.

Jednotlivé sekce a subsekce jsou popsány v disertační práci – subkapitola 5.4. Důležitá subsekce *Adjudicator* bude popsána dále.

Schéma modelu na úrovni *Top* je uvedeno na obr. 7, kde obdélníkové objekty označují jednotlivé základní sekce modelu a jejich vzájemné propojení pomocí míst *A1* – *D4*. Místa *Send* a *Received* jsou součástí sekce *Supplicant1* a na úrovni *Top* jsou umístěna pro přehlednou kontrolu činnosti modelu.



obr. 7 Schéma modelu (úroveň Top)

4.2.2 Subsekce Adjudicator

V disertační práci je podrobně uveden popis všech sekcí. Nejdůležitější součástí vylepšeného serveru je subsekce Adjudicator, ktrerá je součástí sekce RADIUS1 a kterou zde stručně uvedeme.

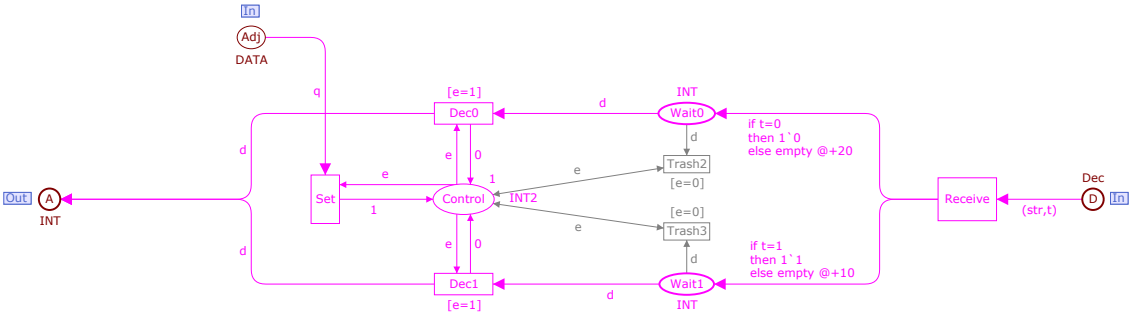
V případě, že systém obdrží více odpovědí, musí je nějakým způsobem zpracovat a rozhodnout. Za to zodpovídá právě rozhodovací subsekce **adjudikátor**. Adjudikátor představuje parametrizovatelnou složku algoritmu, kterou lze přizpůsobit požadavkům konkrétní situace. Ne všude musí být adjudikátor stejný, naopak umožňuje vyjádřit lokální politiku konkrétního poskytovatele služeb.

V této práci byly vytvořeny a ověřeny tři modelové případy adjudikátorů. Označovány budou jako **simple**, **base** a **vote**. V této subkapitole budou jednotlivé adjudikátory popsány z hlediska návrhu a činnosti. Adjudikátor má klíčový vliv na chování modelu jako celku, takže výsledky experimentů s jednotlivými adjudikátory budou popsány v subkapitole 4.3.

4.2.2.1 Simple adjudikátor

Tento adjudikátor obsahuje dvě cesty, obr. 8. Jednu pro kladné a druhou záporné odpovědi. Adjudikátor lze nakonfigurovat různě. V našem případě je pomocí časových konstant model nastaven tak, že záporné odpovědi čekají v místě 0, zda nepřijde alespoň jedna odpověď kladná. Ta projde bez většího zpoždění přes přechod *Dec1*, kde nastaví místo *Control* tak, že záporné

odpovědi budou zahozeny. Systém tedy preferuje kladnou autentizaci. Vstupní místo *Adj* slouží pouze pro nastavení adjudikátoru do výchozího stavu.



obr. 8 Simple adjudikátor

Oblast lze ale přepracovat i jinak, například lze preferovat zápornou autentizaci. Může se také stát, že jednou z příchozích odpovědí bude odpověď domovského serveru. Tato odpověď má však nyní stejnou „váhu“ jako odpovědi ostatních serverů.

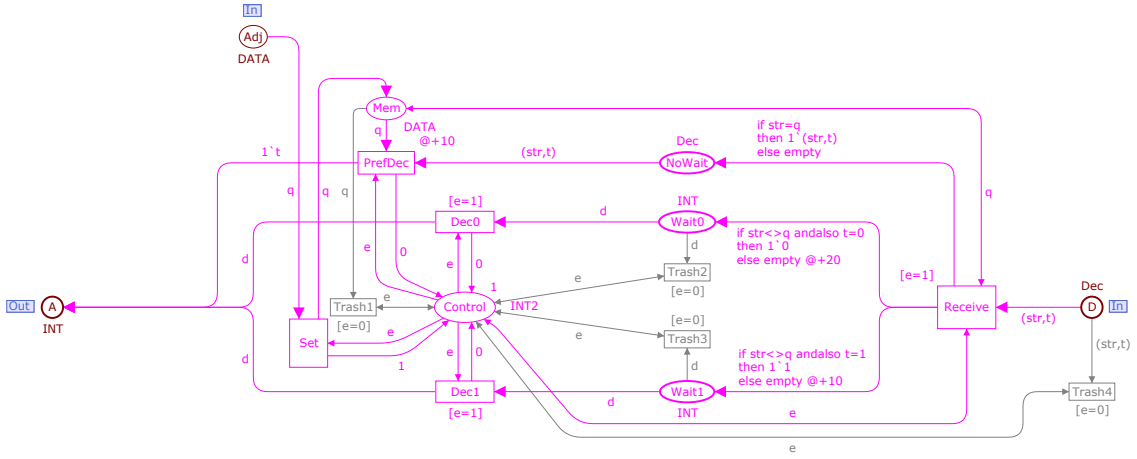
Z uvedeného faktu vzniká **bezpečnostní riziko autentizace neaktuálního účtu**. To znamená, že v určitých situacích může systém povolit autentizaci uživatele, kterou by jeho domovský server (pokud by byl funkční) nepovolil. Může se to stát zejména v případě, že daný uživatel si změní heslo, ale po nějakém (relativně krátkém) čase použije z nějakého důvodu pro autentizaci původní heslo (např. „chybou ve své hlavě“ nebo to za něho udělá útočník). Výpadek jeho domovského serveru způsobí, že systém se pokusí uživatele autentizovat proti cache databázím ostatních RADIUS serverů, které však mohou mít uložen záznam o uživateli ještě s původním heslem (tedy neaktuální účet). Toto heslo však může být kompromitované, a tak tato situace je potenciálním bezpečnostním rizikem[ii]. Je však otázkou, zda je toto riziko natolik značné (muselo by dojít k sérii náhodných jevů, aby došlo ke skutečnému ohrožení uživatelského účtu), než aby byl tento způsob činnosti adjudikátoru označen za nepoužitelný.

Závěrem je třeba upozornit na obecnou skutečnost, že nastavení doby platnosti cache záznamu ovlivňuje chování systému jako celku. Vhodná doba expirace cache záznamů by mohla být náplní dalšího rozvoje tohoto tématu a nových experimentů.

[ii] popis tohoto rizika a jeho minimalizace je v popsána v kapitole 6 disertační práce.

4.2.2.2 Base adjudikátor

Base adjudikátor se schová podobně jako adjudikátor Simple. Klíčovým rozdílem je však fakt, že primárně preferuje odpověď od domovského serveru, pokud taková přijde. V tom případě jsou ostatní odpovědi zahozeny. Odpovědi od domovského serveru jsou téměř bez zpoždění propuštěny k odchozímu místu *A*, zatímco ostatní odpovědi čekají, zda nějaká odpověď domovského serveru dorazí. Časovými konstantami na hranách směrem k místům *Wait0* a *Wait1* je dosaženo toho, že adjudikátor sekundárně preferuje kladné autentizace před zápornými. Abychom dosáhli toho, že adjudikátor bude preferovat odpovědi domovského serveru, je nutné, aby se do něho dostala informace, kterému domovskému serveru byl prvotní požadavek vlastně směřován. Toho se dosáhne tím, že z místa *Adj* přes přechod *Set* je do místa *Mem* tato informace předána ve formě řetězce s hodnotou „realm“.



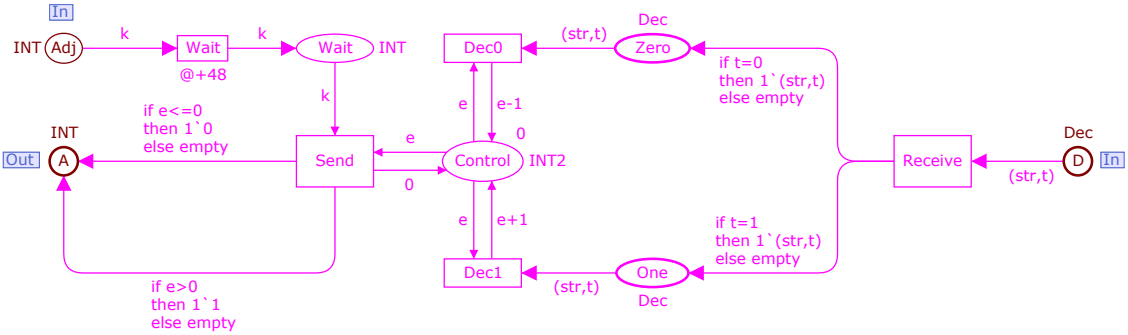
obr. 9 Base adjudikátor

Této informace pak využívá přechod *Receive*, který vstupující pakety třídí dle toho, zda pocházejí od domovského serveru či nikoliv.

Takto navržený adjudikátor dává přednostní šanci domovskému serveru, pokud se po ztrátě paketu nebo dočasném výpadku znovu zapojí do rozhodovacího procesu, povolit nebo zamítnout autentizaci uživatele. V případě, že domovský server nereaguje ani na opakovanou výzvu, riziko autentizace uživatele zastaralým heslem, jak bylo popsáno v předchozím odstavci, přetrvává.

4.2.2.3 Vote adjudikátor

Ve třetím případě byl navržen „hlasovací“ adjudikátor. Tento se od předchozích liší tím, že sám generuje kladnou nebo zápornou autentizaci a mohl by tudíž i převzít funkci subsekce *Responder* (z důvodu unifikace sekce *RADIUS1* s předchozími řešeními to však není provedeno). Hlasovací adjudikátor generuje odpověď na základě hlasování jednotlivých serverů, přičemž všechny servery mají v tomto případě stejnou váhu hlasu. Stejně tak odpovědi (kladné / záporné) mají stejnou váhu. Nepřijde-li v čekací lhůtě (viz přechod *Wait*) žádná odpověď nebo je kladných i záporných odpovědí stejně, vygeneruje adjudikátor zamítavé stanovisko. Nevýhodou tohoto řešení je fakt, že adjudikátor musí čekat dostatečně dlouho na pokud možno co největší množství odpovědí. Po provedení simulací a jejich vyhodnocení v subkapitole 4.3 bude patrné, že se jedná o časově nejpomalejší způsob řešení.



obr. 10 Vote adjudikátor

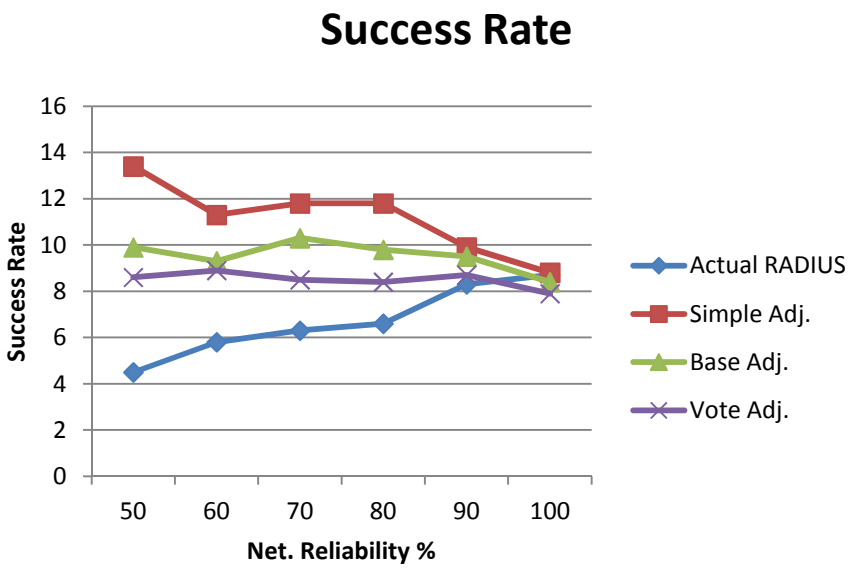
4.3 Ověření činnosti vylepšeného protokolu

Cílem předloženého modelu je simulovat činnost několika variant vylepšeného protokolu RADIUS v distribuovaném prostředí. Modely umožňují ověřit činnost vylepšení v různých konfiguracích a nastavení specifických parametrů (například časových konstant, pravděpodobností apod.), jak bylo naznačeno výše. Parametry a konfiguraci modelů je možné měnit a ověřovat tak hypotézy o chování počítačové sítě, například předpoklad, že s klesající mírou spolehlivosti sítě bude vylepšený RADIUS dosahovat lepších výsledků při autentizaci uživatele.

V disertační práci je popsán způsob měření jednotlivých níže uvedených parametrů a také jsou uvedeny a popsány další parametry modelu. Naměřená data jsou v příloze C disertační práce.

4.3.1 Úspěšnost autentizace uživatele

Tento parametr ukazuje úspěšnost autentizace pro sto požadavků o autentizaci pseudonáhodně vygenerovaných z dat umístěných v sekci *Supplicant*. Tato data jsou vždy pro všechny varianty modelu shodná. Model tedy vygeneruje náhodnou kombinaci uživatelského jména, realmu a hesla a tuto kombinaci zašle k autentizaci. Pokud je tato kombinace vstupních dat umístěna v databázi některého z autentizačních serverů (a je doručena), je autentizace považována za úspěšnou. Výhodou vylepšeného modelu je, že má možnost pokusit se o autentizaci na základě totožných vstupních dat opakovaně. Počet úspěšných pokusů se může zdát nízký, ale je třeba si uvědomit, že se jedná o pseudonáhodně sestavené kombinace vstupních dat.



graf 1 Úspěšnost autentizace uživatele

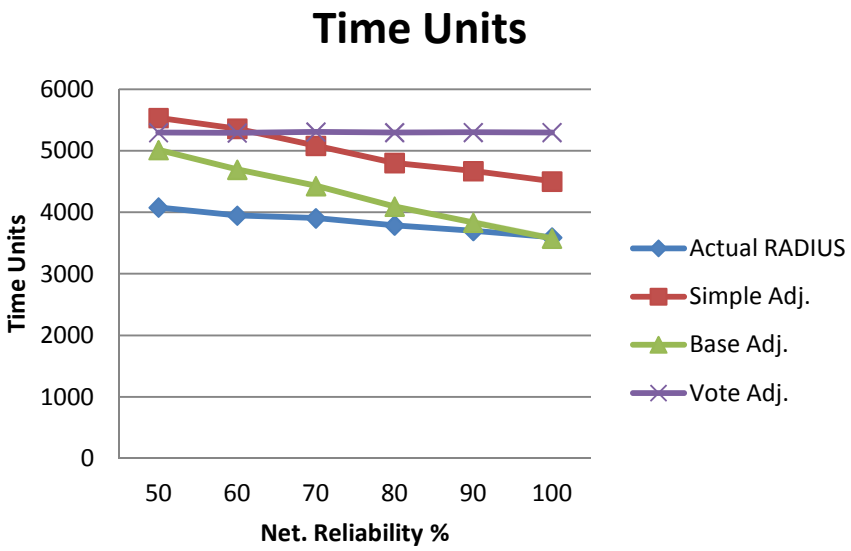
Z grafu 1 je patrné, že aktuální verze protokolu RADIUS má s klesající spolehlivostí sítě přibližně lineárně klesající úspěšnost autentizace. Vylepšený algoritmus protokolu naopak **vykazuje s klesající spolehlivostí sítě lineárně stoupající úspěšnost autentizace** (zejména pro Simple adjudikátor). Toto zásadně rozdílné **chování lze vysvětlit zvyšujícím se využíváním cache**

databází jednotlivých poskytovatelů služeb při klesající spolehlivosti sítě. Protože s klesající spolehlivostí sítě dochází k častějším výpadkům přenosu dat, autentizační server poskytovatele služeb častěji opakuje výzvu o autentizaci a tím se zvyšuje šance na úspěšnou autentizaci. Prodlužuje se však doba autentizace a zvyšuje se počet paketů v síti.

Dosažené chování vylepšeného RADIUS protokolu nicméně může být výhodou při jeho nasazení v sítích s nízkou nebo výrazně kolísavou spolehlivostí (např. geograficky rozlehlé bezdrátové sítě v rozvojových zemích, bezdrátové sítě ve frekvenčně zarušených prostředích apod.).

Vylepšený protokol s Vote adjudikátorem má spíše konstantní průběh měřeného parametru. To je zřejmě dáno především množstvím hlasujících subjektů (tedy rozhodovacích RADIUS serverů), které je poměrně nízké. Výhodu při nasazení tohoto typu adjudikátoru by měli uživatelé, kteří relativně hodně „cestují“ mezi sítěmi a tedy mají šanci získat větší množství kladných hlasů.

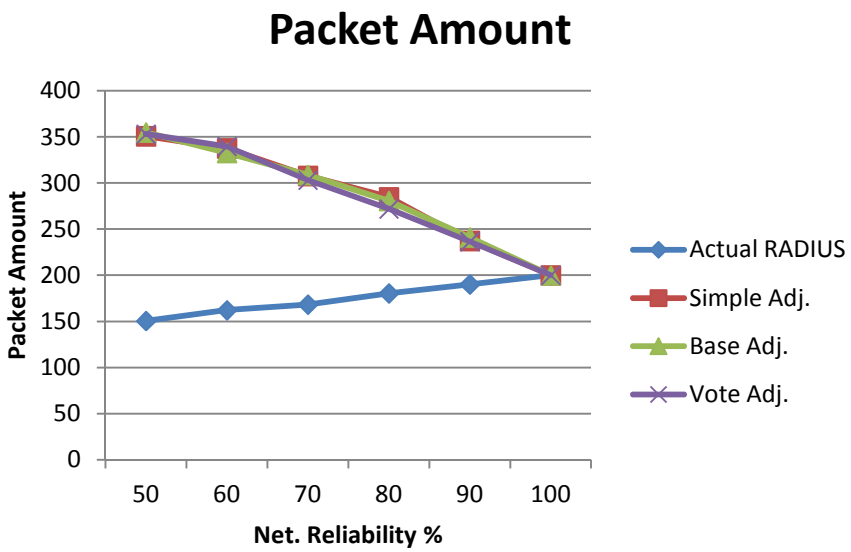
Za zmínku stojí výsledky pro hodnotu spolehlivosti sítě 100%, kdy všechny varianty protokolu pracují podle aktuálního algoritmu a jejich výsledky by tak měly být shodné. Jejich nevýznamná rozdílnost je dána pouze chybou měření, která byla u jednotlivých měření stanovena, přičemž předložené výsledky jsou v rámci přípustné míry tolerance.



graf 2 Úspěšnost autentizace

4.3.2 Doba trvání autentizačního procesu

Doba trvání autentizačního procesu je parametr, který udává celkovou dobu trvání autentizace pro sto pseudonáhodně vygenerovaných požadavků o autentizaci. Hodnota je uvedena v časových jednotkách, které jsou součástí CPN Tools. Srovnáním s reálnou činností protokolu by pak bylo možné získat skutečný čas. Z grafu 2 je vidět, že kromě Vote adjudikátoru mají všechny varianty protokolu tendenci s rostoucí spolehlivostí sítě lineárně snižovat časovou náročnost procesu autentizace. Base adjudikátor má pro hodnotu spolehlivosti sítě 100% dokonce přibližně shodnou časovou náročnost jako aktuální RADIUS protokol. To je dáno tím, že v Base adjudikátoru není třeba čekat na odpovědi ostatních serverů, pokud reaguje domovský server. V Simple adjudikátoru je čekání na případné další reakce zavedeno a z toho důvodu je z grafu patrný konstantní rozdíl od Base adjudikátoru. Naproti tomu Vote adjudikátor má pevně stanovenou dobu čekání na „ukončení hlasování“, takže jeho charakteristika musí být konstantní, což jej znevýhodňuje vůči ostatním variantám pro použití ve spolehlivějších sítích.



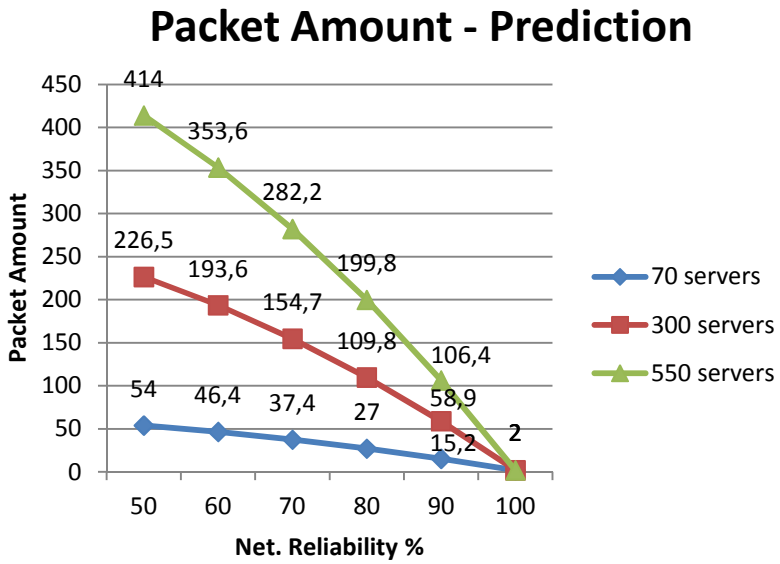
graf 3 Počet přenesených paketů – naměřeno

4.3.3 Počet přenesených paketů

Tento parametr patří mezi nejdůležitější. V podstatě ukazuje, jak velké zatížení sítě při nasazení vylepšeného RADIUS protokolu můžeme očekávat (graf 3).

Metodika měření byla nastavena tak, že započteny byly odchozí pakety ze subsekce *Network* (a to v obou směrech). Chybové pakety, které se cestou v subsekci *Network* „ztratily“, se nezapočetly. Z výsledků uvedených v grafu pak plyne, že nezáleží na navrženém typu adjudikátoru, podstatná je pouze spolehlivost sítě. Pro uvažovanou nejnižší spolehlivost 50% dojde ke zvýšení přenosu paketů o cca 2,3násobek. Pro spolehlivost sítě 100% ke ztrátám paketů nedochází, a tak pro sto autentizačních požadavků a k nim náležejících odpovědí je počet přenesených paketů vždy právě 200.

Na základě naměřených dat (viz graf 3) je možné vyvodit empirický vztah mezi jednotlivými parametry sítě (viz subkapitola 5.5.5 disertační práce), který umožní predikovat počty přenesených paktů v rozsáhlejších sítích.



graf 4 Počet přenesených paketů - předpoklad

Z uvedených výsledků empirického vztahu, které činí i pro poměrně rozsáhlé sítě (na úrovni států) řádově stovky přenesených paketů (tedy řádově stonásobky stávajícího stavu), je zřejmé, že nebude docházet k neúměrnému nárůstu počtu přenesených paketů a to ani pro případné nízké spolehlivosti sítě (viz graf 4).

4.3.4 Diskuse o dosažených výsledcích

Z výše uvedených měření je patrné, že vylepšený RADIUS protokol má ve srovnání s aktuálním protokolem poněkud odlišné chování. Zatímco

v aktuálním RADIUS protokolu parametr úspěšnost autentizace s klesající spolehlivostí sítě přibližně lineárně klesá, vylepšený protokol vykazuje opačný trend. Je zjevné, že aktuální protokol není vhodný pro síťová prostředí, kde lze očekávat nízkou spolehlivost. Naopak ze zjištěných výsledků se dá předpokládat, že vylepšený protokol je pro prostředí s nespolehlivými sítěmi mnohem vhodnější. Navržený protokol sice vykazuje o něco delší prodlevy při řešení autentizačních požadavků (přibližně až o 30-35%, viz grafy v subkapitole 5.5 disertační práce), nejedná se ale o zásadní zpoždění, které by uživatele mohlo odradit od používání služeb sítě s nasazeným vylepšeným protokolem, neboť zpoždění je stále v řádu desetin sekundy.

Vylepšený protokol naopak v souladu s předpokladem vykazuje zvýšení počtu přenesených paketů až o cca 200% oproti aktuálnímu protokolu. Toto zvýšení je nepřímo závislé na spolehlivosti sítě. Z tohoto faktu je možné usoudit, že by nasazení vylepšeného protokolu mohlo ohrozit fungování sítě tím, že při snižování spolehlivosti sítě (např. při přetížení směrovačů) by vylepšený RADIUS protokol zahlcoval systém dalšími pakety s požadavky na autentizaci a tím by roztočil spirálu vedoucí ke kolapsu sítě. Toto riziko by však nemělo hrozit při implementaci vylepšeného protokolu RADIUS, který bude využívat protokol TCP, což je i ve stávajících implementacích běžné.

5 NÁVRH INOVACE PROTOKOLU RADIUS Z HLEDISKA BEZPEČNOSTI

5.1 Základní východiska

Uživatelé distribuovaných sítí mohou měnit své chování ve vztahu k bezpečnosti jednotlivých částí sítě (připojených institucí) nebo sítě jako celku, například jinou než domovskou sít mohou zneužívat k útokům na vnitřní zdroje této sítě nebo na externí sítě.

V předchozí kapitole bylo navrženo rozšíření protokolu RADIUS pro zlepšení spolehlivosti. Předložené řešení však umožňuje při splnění poměrně extrémních podmínek autentizaci na základě neaktuálního účtu To by mohlo umožnit

přístup do systému uživateli, kterému byla tato možnost poskytovatelem identity odebrána (například z důvodu spáchání bezpečnostního incidentu).

Je tedy třeba rozšířit protokol RADIUS o možnost zavádět zprávy přenášející informace o jednotlivých uživatelských účtech a chování uživatelů. Tento nástroj bude nutné doplnit o systém umožňující částečně automatickou formu sledování bezpečnostně-relevantní činnosti uživatelů v sítích jednotlivých členů federace. Informace o uživatelích v systému už nyní mohou shromažďovat jednotlivé zainteresované RADIUS servery v rámci svých účtovacích informací, nicméně systém účtování byl před lety navržen především z důvodu ekonomického provozu sítě a tedy se zaměřoval především na získání podkladů pro zpoplatnění uživatele za služby související s použitím sítě, proto se nejeví jako vhodný pro sledování bezpečnostně-relevantní činnosti uživatelů a bude třeba jej rozšířit a vhodně propojit s jiným nástrojem pro odhalování bezpečnostních incidentů, mezi které patří především Intrusion Detection Systémy [10].

Číslo výstrahy	Označení výstrahy	Popis výstrahy
0	Attempted-admin	pokus o získání administrátorských práv
1	Attempted-user	pokus o získání uživatelských práv
2	Successful-admin	úspěšné získání administrátorských práv
3	Successful-user	úspěšné získání uživatelských práv
4	Web-application-attack	útok na webovou aplikaci
5	Attempted-dos	pokus o DOS
6	Denial-of-service	odhalení DOS
7	Successful-dos	DOS

tab. 1 Tabulka závažných výstrah

Systémy IDS se pro výše naznačené problémy ukazují jako vhodné, například pro to, že mají jednoznačně definované formáty výstrah (například hojně rozšířený **IDS Snort** [11]) a tyto výstrahy zaznamenávají textově do souboru logu (např. s názvem `alert.log` apod.). Vzhledem k textovému charakteru výstrah IDS je možné využít je pro předávání bezpečnostních informací v rámci protokolu RADIUS tak, že zejména ty nejzávažnější z nich (definované v tab. 1) budou předány společně s uživatelským jménem potenciálního útočníka do accounting systému protokolu RADIUS.

Ten je po vytvoření a implementaci nových atributů (zavedeny dále) bude moci předávat mezi členy federace. Závažné výstrahy byly definovány podle atributů systému IDS Snort, které byly subjektivně považovány za nebezpečné. Na základě zkušeností z praxe lze případně závažné atributy předefinovat.

5.2 Návrh řešení pro zlepšení bezpečnosti

Tato část práce byla částečně publikována v [A] a prezentována na [B].

5.2.1 Varianty komunikace mezi RADIUS a IDS

V rámci disertační práce jsou nastíněny možnosti spolupráce mezi protokolem RADIUS a IDS nasazeným v konkrétní síti. Jednotlivé strategie přicházející v úvahu stručně popisuje a zdůvodňuje odstavec 6.4.1 práce. Mezi obecné strategie lze zařadit tři základní přístupy:

- **Metoda dotazování na aktuální stav (Pull strategie)**

RADIUS protokol se dotazuje na aktuální stav zvoleného IDS v pravidelných časových intervalech. Strategie je jednoduchá na implementaci a pro dále zkoumané řešení dostatečně efektivní. Navíc nevyžaduje zásahy do dalších entit kromě protokolu RADIUS.

- **Metoda subscribe-publish (Push strategie)**

RADIUS protokol se registruje u IDS a při vzniku události je automaticky informován o změně stavu. Strategie vyžaduje zásahy do dalších entit kromě protokolu RADIUS a její přínosy nemohou vyvážit relativní složitost její implementace.

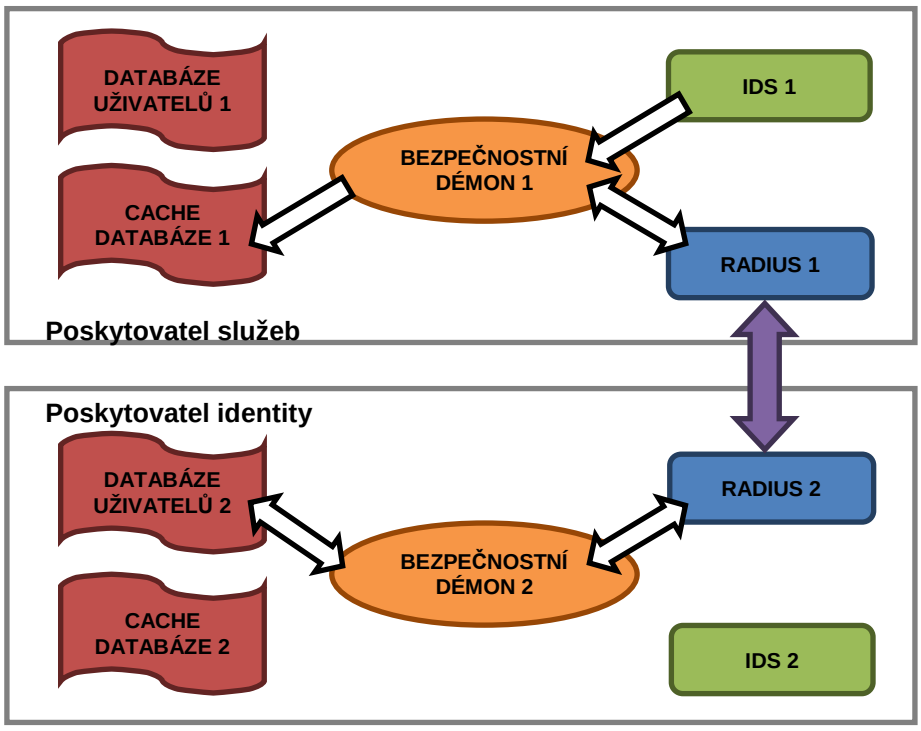
- **RADIUS jako softwarový agent v multiagentním IDS systému**

RADIUS protokol spolupracuje se skupinou IDS instancí (agentů) při poskytování optimálního monitoringu bezpečnostních událostí a při jejich předávání mezi agenty vzájemně. RADIUS by tedy nebyl pouze konzumentem informací, ale mohl by příslušnému IDS poskytovat bezpečnostní informace získané z externích systémů. Toto řešení spolupráce je nejzajímavější, avšak náročné na implementaci, protože předpokládá nový pohled na IDS, na protokol RADIUS, na spolupráci mezi nimi a tvorbu nového multiagentního systému.

Nasazení této strategie by však přineslo významné benefity pro celkovou bezpečnost počítačových systémů. Rozvoj předložené myšlenky může být tématem dalšího směřování výzkumu, nicméně rozsah nastíněné problematiky se nachází mimo rámec práce.

5.2.2 Aplikace zvoleného řešení a zavedení nových atributů

Předávání vybraných výstrah z logovacího souboru do protokolu RADIUS accounting bude prováděno automatickým způsobem, přičemž existující možnosti byly naznačeny výše. Případný zásah administrátora by měl být zúžen jen na schválení předložených omezení uživatelů před odesláním dalším



obr. 11 Princip předávání bezpečnostních informací

součástem federace. Pro svou relativní jednoduchost a snadnou implementaci do protokolu RADIUS byla jako mechanismus předávání informací mezi nasazeným IDS a protokolem RADIUS zvolena tzv. Pull strategie, viz výše. Za získávání informací z IDS instance bude v rámci vylepšené implementace protokolu RADIUS zodpovědná nová entita, tzv. **bezpečnostní démon** (viz subkap. 6.5.3 práce). Tento bezpečnostní démon bude ve stanovených intervalech prohledávat databázi výstrah příslušného IDS a vytěžovat informace podle klíčových slov výstrah (tab. 1, sloupec 2) zjištěné IDS. Přehled vztahů

mezi prvky uvažovaného konceptu je na obr. 11. Dále démon vygeneruje odpovídající bezpečnostní zprávu protokolu RADIUS Accounting opatřenou novými bezpečnostními atributy navrženými v tab. 2. Na přijímací straně (tedy na serveru-příjemci, za kterého považujme server poskytovatele identity daného uživatele) bude úkolem vylepšené implementace protokolu (bezpečnostního démonu) podle přijatého uživatelského jména zavést restrikce pro daného uživatele, například jej dočasně nebo trvale vyřadit z možnosti využívat služeb dané federace (pravidla určí lokální či federační politika, viz subkapitola 5.4).

Navržený systém se zaměřuje na řešení následujících případů:

1. Uživatel způsobí bezpečnostní incident v síti poskytovatele služeb,
2. Uživatel způsobí bezpečnostní incident v síti svého poskytovatele identity,
3. Poskytovatel identity se rozhodne pro omezení uživatelského účtu z jiného důvodu,
4. Uživatel provede změnu hesla svého účtu a tuto změnu je třeba propagovat členům federace (z důvodu případného odstranění neplatného hesla z jejich databází), přičemž vlastní heslo se nepřenáší.

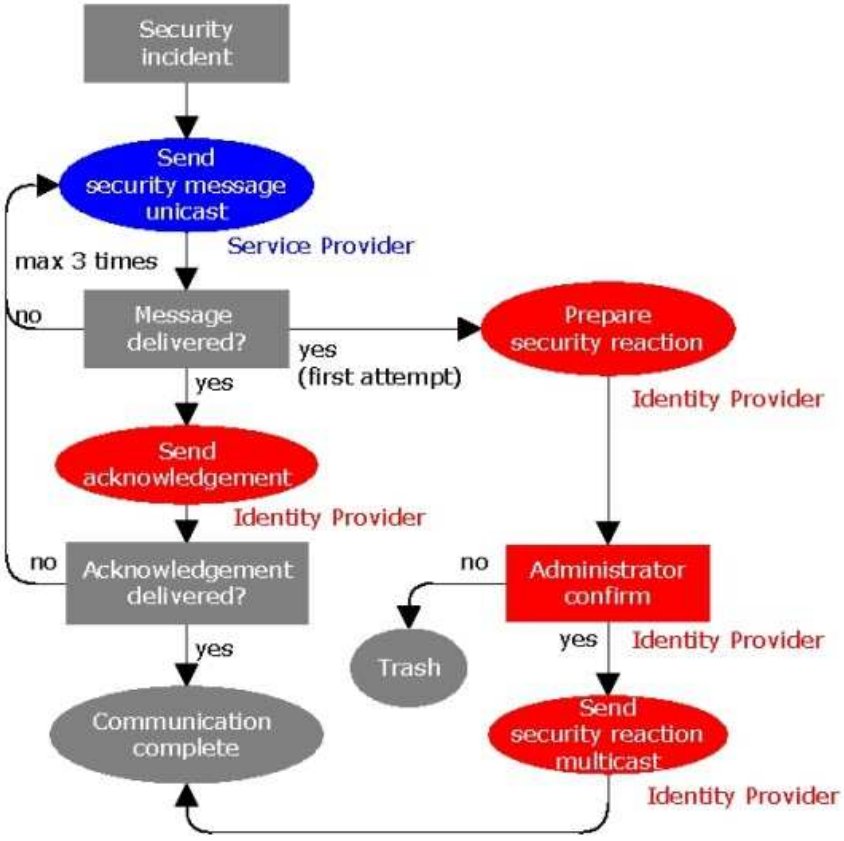
Pro řešení těchto případů budou navrženy atributy, viz tab. 2. Popis atributů je uveden v disertační práci – subkapitola 6.5.

Číslo	Označení atributu	Popis atributu
145	Sec-Exchange	zapíná příjem bezpečnostních informací
146	Sec-Alert	předává bezpečnostní upozornění
147	Sec-Restriction	informuje o omezení už. účtu
148	Sec-Restriction-Period	informuje o délce omezení už. účtu
149	Sec-Restriction-Reason	informuje o důvodu omezení už. účtu
150	Sec-PassChange	informuje o změně hesla už. účtu

tab. 2 Definice nových atributů protokolu RADIUS

Jednou z nejdůležitějších bezpečnostních situací, kterou disertační práce řeší, je uvedena výše jako **případ 1**. Uvažujeme, že bezpečnostní incident nastal v síti, kterou lze vůči uživateli, který jej způsobil, označit jako síť poskytovatele služeb. Bezpečnostní zprávu o incidentu generuje RADIUS server poskytovatele služeb, v jehož síti bezpečnostní incident nastal, a předává ji k řešení serveru poskytovatele identity příslušnému podle realmu uživatele,

který incident způsobil, a to standardní cestou formou unicast zprávy podle realmu uživatele. Zjednodušený diagram činnosti algoritmu je na obr. 12. Odeslaná bezpečnostní zpráva obsahuje atribut `Sec-Alert` s hodnotou, která zařazuje způsobený incident, a atribut `User-Name`, který jako hodnotu obsahuje jméno uživatelského účtu. Po přijetí zprávy bezpečnostní démon poskytovatele identity odešle potvrzovací zprávu odesílajícímu serveru obsahující atribut `Sec-Exchange` s hodnotou `3` a atribut `User-Name`. Pokud odesílající server tuto zprávu neobdrží, opakuje zaslání bezpečnostní zprávy znovu (nikoliv však nekonečně, například třikrát).



obr. 12 Diagram činnosti algoritmu pro zasílání bezpečnostních zpráv

Dále bezpečnostní démon poskytovatele identity zajistí připravení reakce na bezpečnostní incident (restrikce na uživatelský účet) v souladu s interní bezpečnostní politikou poskytovatele identity, viz subkap. 5.4. Z procedurálního hlediska následuje rozeslání informace o restrikci uživatelského účtu nejlépe formou multicast zprávy všem členům federace. Zpráva obsahuje povinně atributy `Sec-Restriction` a `User-Name` a volitelně atributy `Sec-Restriction-`

`Period` a `Sec-Restriction-Reason`. Rozeslání těchto zpráv však může trvat několik hodin i několik dní, protože připravená reakce na bezpečnostní incident může vyžadovat potvrzení administrátorem serveru.
Další výše uvedené případy jsou popsány v disertační práci – subkapitola 6.4.2

5.3 Bezpečnostní zprávy a atributy

Navržené řešení inovace protokolu klade na stávající verzi systému RADIUS nové požadavky. S návrhem nových funkcionalit protokolu souvisí také potřeba nových nástrojů, které protokol bude nezbytně potřebovat, aby mohl navrženým požadavkům dostát. Mezi tyto nástroje patří zejména skupina nových atributů, které dovolí přenášet dosud nevyžadované informace. Z logiky fungování protokolu plyne skutečnost, že atributy musí být při komunikaci součástí některého typu zprávy protokolu RADIUS (viz subkapitola 3.2). Stávající nabídka typů zpráv je podle IANA [12] poměrně široká. Nabízí se existující typ zprávy `Accounting-Message`, ale vzhledem k přehlednosti, a pro případ budoucího nárůstu atributů bezpečnostního typu, považujeme za vhodnější zavést nový typ zprávy (bezpečnostní).
Zprávy jsou v rámci protokolu RADIUS definovány hodnotou pole **Code** viz subkapitola. 3.2. Hodnoty tohoto pole registruje IANA, přičemž k termínu vzniku této práce byla volná například hodnota 35. V dalším textu budeme předpokládat, že nově zavedenému typu zprávy byla přidělena hodnota Code = 35. Je tedy možné definovat v rámci standardního formátu zpráv protokolu RADIUS nový typ bezpečnostní zprávy:

35 Security-Message

Tento typ zpráv může obsahovat atributy `User-Name`, `Sec-Exchange`, `Sec-Alert`, `Sec-Restriction`, `Sec-Restriction-Period`, `Sec-Restriction-Reason` a `Sec-PassChange`.

Nově navržené **atributy bezpečnostního typu** (viz tab. 2) budou sloužit především pro výměnu bezpečnostních informací mezi členy federace. V disertační práci – subkapitola 6.5 – jsou tyto bezpečnostní atributy definovány ve standardním formátu podle RFC 2865 a detailně popsány včetně komunikačních procedur v systému.

5.4 Příklad bezpečnostních politik systému

V rámci navrženého systému je možné omezovat jednotlivým uživatelům přístup do sítě. Není pochybností o tom, že tento systém musí být nastaven transparentním způsobem tak, aby uživatelům sítě bylo předem jasné, za jakých podmínek k omezení může docházet, a tedy jaké sankce v případě porušení pravidel hrozí. Není záměrem práce nastavit obecně platná pravidla, neboť jsou to poskytovatelé identit, kteří nesou za registraci svých uživatelů zodpovědnost. Tedy poskytovatelé identit by především měli mít zájem na používání navrženého systému a na nastavení odpovídajících pravidel a sankcí. **Navržené bezpečnostní politiky** je tedy možné chápat jako **příklad či doporučení** k nastavení individuálních pravidel jednotlivých poskytovatelů identit (nicméně bylo by vhodné používat u jednotlivých poskytovatelů identit pravidla obdobná).

Jedním z hlavních cílů je zabránit opakovaným útokům, které nečiní uživatel vědomě, ale činí je např. vir, který počítač uživatele zahrne do botnetu. V tomto případě má být hlavním smyslem restrikce donutit uživatele provést individuální bezpečnostní opatření. Vhodné je tedy kratší odpojení uživatele od služeb, spojené s informováním (např. „přes Váš účet byl proveden útok..., prosím spusťte antivir“). Po ukončení restrikce by byla při dalším útoku provedena trvalejší restrikce (s informací, kde se může uživatel informovat dál).

Číslo výstrahy	Označení výstrahy	Koeficient sankce k_s
0	Attempted-admin	3,0
1	Attempted-user	2,0
2	Successful-admin	3,0
3	Successful-user	2,0
4	Web-application-attack	1,0
5	Attempted-dos	1,0
6	Denial-of-service	1,0
7	Successful-dos	1,0

tab. 3 Návrh sankcí za porušení pravidel

Při restrikci uživatele navrhujeme vycházet z navržených bezpečnostních incidentů a časového omezení uživatelského účtu na násobky doby, kterou označme jako **základní dobu** (ZD). Hodnotu základní doby stanovme empiricky na tři dny, což je zřejmě běžná doba, za kterou stihne uživatel sjednat nějakou

nápravu věci. Za jednotlivé incidenty způsobené uživatelem poprvé by byla zavedena **restrikce na násobky základní doby** navržené v tab. 3 jako **koeficient k_s**.

Při opakování incidentu stejným uživatelem by se doba restrikce prodlužovala, což by mělo působit výchovně při neplnění povinností uživatele.

Vhodný způsob prodlužování doby restrikce by mohl vycházet z následující funkce:

$$t_r = 2^{n-1} \times k_s(L) t_b$$

kde

- t_r je celková doba restrikce ve dnech
- n je počet opakování útoků za určenou dobu (např. za jeden rok)
- t_b označuje základní dobu restrikce
- L je typ útoku $L \in \{0, 1, \dots, 7\}$, viz tab. 3 (číslo výstrahy)
- k_s je funkce mapující typ útoku na koeficient trvání restrikce $(k_s : \{0, 1, \dots, 7\} \rightarrow R)$, viz tab. 3.

6 ZÁVĚR

V souladu s definovanými cíli práce byly dosaženy následující hlavní výsledky:

1. Byl navržen algoritmus pro zajištění autentizace při výpadku domovského autentizačního serveru uživatele – subkapitola 5.3 práce,
2. Navržený algoritmus byl simulován s použitím barevných Petriho sítí a byla ověřena jeho schopnost úspěšně řešit předložený problém v rozsáhlých sítích s nízkou spolehlivostí – subkapitola 5.4 práce,
3. Bylo ověřeno na vytvořeném modelu, že algoritmus je schopen činnosti v asynchronním distribuovaném prostředí [13] – subkapitola 5.5 práce,
4. Byl navržen způsob řešení výměny informací o bezpečnostních událostech spojených s uživateli s využitím volitelných atributů protokolu RADIUS a systémů IDS – subkapitoly 6.4, 6.5 a 6.6 práce.

Práce je zaměřena na analýzu problémů distribuovaných sítí s federativní autentizací založených na protokolu RADIUS a na hledání řešení předložených problémů a jejich ověření na modelu. Přirozeným pokračováním práce, které má následovat, je dotažení návrhu do funkční softwarové implementace, což

není jen záležitost problematiky počítačových sítí, ale je třeba zapojit do týmu odborníky na návrh a tvorbu softwarových aplikací.

Mezi přímé problémy práce patří ověření vlivu parametrizace cache databází jednotlivých poskytovatelů služeb (zejména délka trvání záznamu) na úspěchu autentizace uživatele. V tomto směru by patrně bylo nemalým přínosem rozšíření systému předávání informací o uživatelích na obecnou distribuovanou správu uživatelů. V praxi to znamená zavedení dalších nových atributů protokolu RADIUS Accounting a rozšíření činnosti bezpečnostního démonu.

Poměrně rozsáhlou a zajímavou problematikou může být záležitost týkající se spolupráce mezi IDS a protokolem RADIUS v rámci multiagentních systémů, jak bylo naznačeno v odstavci 5.3.1.

PŘEHLED PUBLIKAČNÍ ČINNOSTI AUTORA

[A] Jelínek J., Satrapa P.: Návrh inovace protokolu RADIUS z hlediska bezpečnosti, In: sborník příspěvků 12. ročníku doktoradské konference, Hradec Králové, 2012, ISBN 978-80-7435-185-3

[B] Jelínek J., Satrapa P.: Návrh inovace protokolu RADIUS z hlediska bezpečnosti, příspěvek na 12. ročníku doktoradské konference, Hradec Králové, 10.5.2012

[C] Jelínek J., Satrapa P., Fišer J.: Simulation of enhanced RADIUS protocol in Colored Petri nets, In: Proceedings of 11th International Scientific Conference Informatics 2011, Rožňava, ISBN 978-80-89284-94-8

[D] Jelínek J., Satrapa P., Fišer J.: Simulation of enhanced RADIUS protocol in Colored Petri nets, příspěvek na konferenci, Informatics 2011, 11th International Scientific Conference, Rožňava, 17.11.2011

[E] Jelínek J., Satrapa P.: Simulation of RADIUS protocol in Colored Petri nets, In: Proceedings of Networking 1 – Theory and Practice, ŽU Žilina, 2011, ISBN 978-80-554-0494-3

[F] Barilla J., Jelínek J., The Mathematical Model of the Chemical Phase of Radiobiological Mechanism, WDS05 Proceeding of Contributed Papers, Part III, 620-624, Praha 2005

POUŽITÉ ZDROJE

[1] Sova, M. *Federativní přístup k autentizaci.* Liberec : TU Liberec, 2005.

[2] CESNET, z. s. p. o. Roamingová politika, verze 2.0 ze 14.7.2009. *eduroam.cz.* [Online] [Citace: 26. únor 2010.] www.eduroam.cz.

[3] Tanenbaum, A. S. a Van Steen, M. *Distributed Systems: Principles and Paradigms (2nd Edition).* - : Prentice Hall, 2006. 978-0132392273.

[4] Rigney, C. a kol. *RFC2865 - Remote Authentication Dial In User Service (RADIUS).* Livingston : The Internet Society, 2000. RFC2865.

[5] —. *RFC2866 - RADIUS Accounting.* Livingston : The Internet Society, 2000. RFC2866.

[6] Postel, J. *RFC768 - User Datagram Protocol.* místo neznámé : USC/Information Sciences Institute, 1980. RFC 768.

[7] Rivest, R. *RFC1321 - The MD5 Message-Digest Algorithm.* - : MIT Laboratory for Computer Science and RSA Data Security, Inc., 1992. RFC1321.

[8] Internet Corporation For Assigned Names and Numbers. Internet Assigned Numbers Authority (IANA). *Internet Assigned Numbers Authority (IANA).* [Online] [Citace: 11. 10 2012.] http://www.iana.org/.

[9] Petri, C. A. *Kommunikation mit Automaten.* Bonn : University of Bonn, 1962.

[10] Jensen, K. a Kristensen, L. M. *Coloured Petri Nets: Modelling and Validation of Concurrent Systems.* Berlin Heidelberg : Springer-Verlag, 2009. 978-3-642-00283-0.

[11] Westergaard M., Verbeek H.M.W. CPN Tools Homepage. *CPN Tools.* [Online] [Citace: 6. 4 2011.] http://cpntools.org/.

[12] Endorf C., Schultz E., MelanderJ. *Intrusion Detection & Prevention.* Emeryville : McGraw-Hill, 2004. 0-07-222954-3.

[13] Roesch, M. Snort. [Online] SourceFire. [Citace: 20. 11 2011.] http://www.snort.org/.

Mgr. Jindřich Jelínek
Autoreferát disertační práce
2013