Virtuálne prostredia, komunikácia a viacfaktorová autentifikácia v organizačných jednotkách inštitúcie

Virtual environments, communication and multi-factor authentication in organizational units

Rastislav MUCHA — Miloslav MUCHA

Abstract
This contribution briefly mentions some of the possibilities of virtualization and multi-factor authentication with a significant role for the often overlooked SSH protocol. Short information on practical aspects of implementation and deployment at Slovak Agricultural University is also provided. Self-explanatory diagrams and pictures are included.

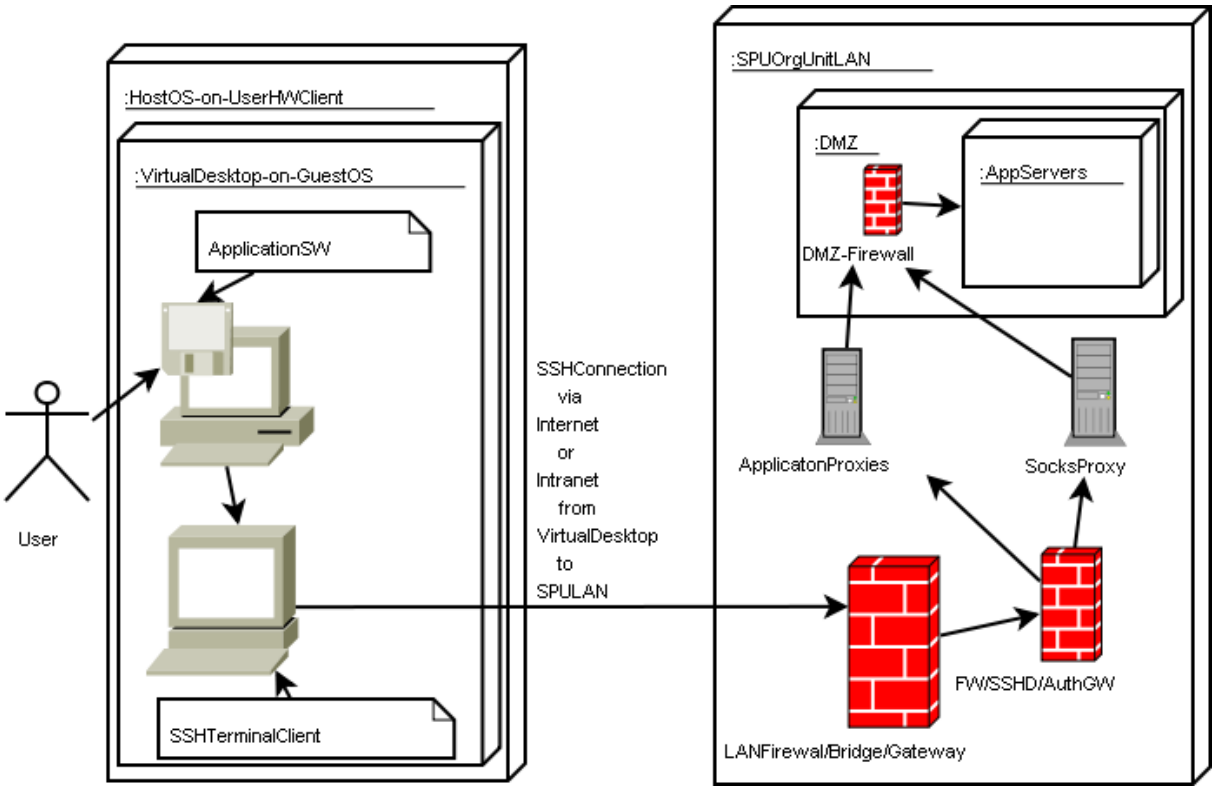
Keywords
Virtualization, QEMU, SSH, PuTTY, HTTP Proxy, Socks Proxy, Apache HTTP Server, Public Key Authentication, OpenBSD, FreeBSD, Multi-Factor Authentication

Úvod

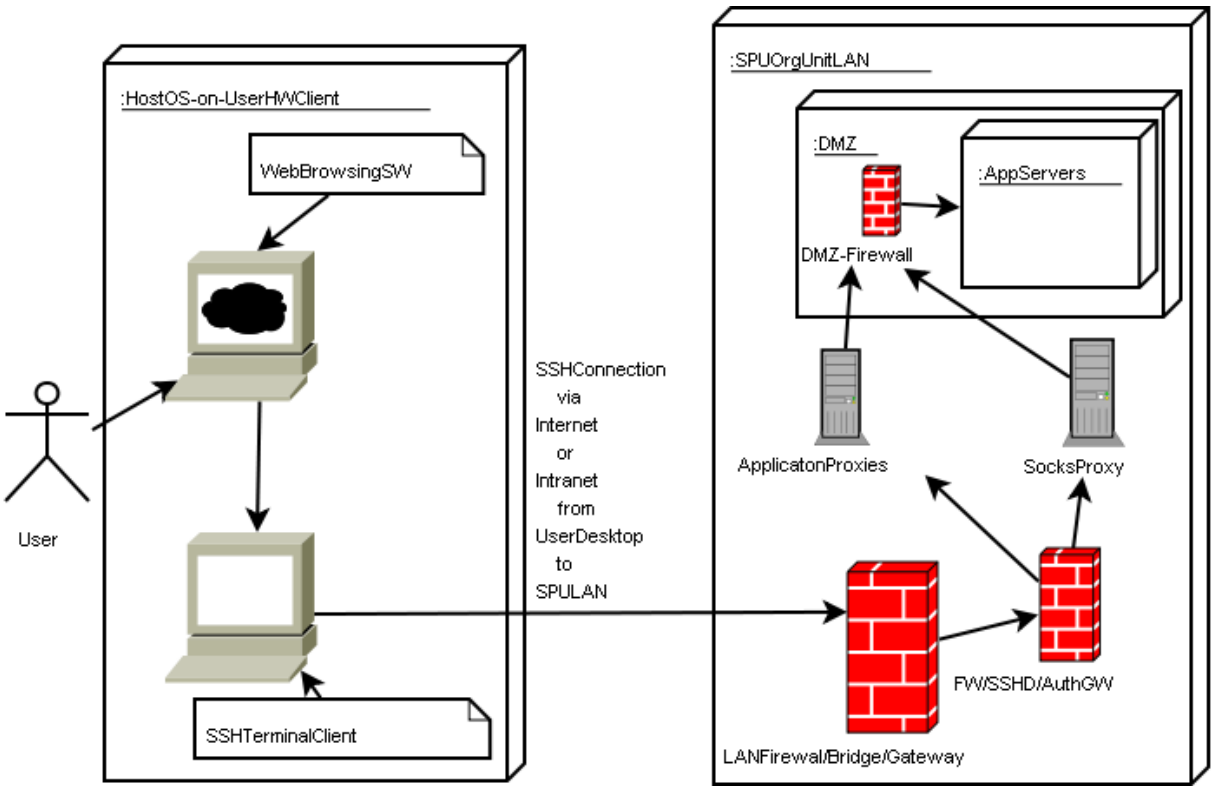
Zvyšovanie počtu používateľov IKT a zariadení pripájaných do sietí spôsobuje organizáciám problémy pri správe klientskych staníc (limitovanými počtami personálu IKT a obmedzenými zdrojmi), udržiavaní a rozširovaní portfólia poskytovaných služieb. Veľmi rýchlo rastú počty osôb s veľkými nárokmi ale minimálnymi znalosťami IKT v spojení s ignorovaním pravidiel a základných noriem slušného správania pri komunikácii. Často až 90% prenášaných dát v sieťach je spojených s aktivitami priamo nesúvisiacimi s činnosťou organizácií. Kontrolované zavádzanie aplikácii, zabezpečenie ich funkčnosti, prípadne pripájanie vlastných zariadení používateľov do LAN si vyžaduje transparentné spôsoby autentifikácie, tvorby spoľahlivých spojení a konfigurácie SW. Nielen podľa názoru autorov tohto príspevku, určitou cestou môže byť vytváranie virtuálnych prostredí (počítačov) spolu s viacfaktorovou autentifikáciu s využitím dostupných mechanizmov na báze kryptografie s verejným kľúčom.

Poznámky k virtualizácii a viacfaktorovej autentifikácii so zapojením protokolu SSH

Virtuálne prostredia spúšťané na hostiteľských koncových zariadeniach používateľov umožňujú realizáciu funkčných konfigurácií aplikačného a komunikačného SW aj v relatívne neznámom alebo „nepriateľskom“ prostredí. K typickým prípadom použitia môžeme zahrnúť „verejne“ prístupné IKT prostriedky bez priamej autentifikácie používateľov, vlastné zariadenia, návštevníkov, personálu a iných osôb spojených s činnosťou organizácie, pracovné stanice používateľov s obmedzenými kompetenciami a okruhom žiaducich aplikácií (napr. administratívny personál). Virtualizácia umožňuje aj separáciu pracovných činností a prostredia na „motiváciu“, „samovzdelávanie“, či „zábavu“ na rovnakom HW a tak znižuje riziko znefunkčnenia kritických aplikácií v nevhodnom čase, prípadne aj redukuje následky kompromitovania SW vybavenia stanice malware-om. Separácia virtuálneho prostredia od HW umožňuje aj zjednodušenie konfigurácie SW výberom vhodných a „univerzálne“ podporovaných virtuálnych zariadení. Virtualizácia poskytuje aj nástroj na sprevádzkovanie autentifikácie na „pozadí“ bez nutnosti „obťažovať“ používateľov „nadmernou“ interakciou (obr. 1). Protokol SSH poskytuje elegantné (žiaľ často veľmi málo známe alebo ignorované)



Obr. 1: Virtuálny desktop v prostredí hosťujúceho operačného systému poskytujúci grafické pracovné prostredie aplikácii spolu s prenosovým kanálom cez protokol SSH do LAN SPU.



Obr. 2: Aplikácia prístupná cez web rozhranie v prehliadači spolu s prenosovým kanálom cez protokol SSH (s využitím ľubovoľného dostupného SSH klienta) do LAN SPU.

prostriedky na autentifikáciu a tvorbu spoľahlivých, zabezpečených spojení k aplikáciám (presmerovanie portov, Socks-proxy, VPN) vrátane nenáročného vybudovania mechanizmov infraštruktúry na základe kryptografie s verejným kľúčom. SSH teda zďaleka nie je len nástrojom pre systémových administrátorov na vzdialenú správu serverov. V spojení s virtualizovaným desktopom je napr. možné zabezpečiť aj „automagické“ vytvorenie spoľahlivého komunikačného kanálu k aplikáciám v chránenej časti LAN (viď. napr. obr. 1), pričom sú zapojené viaceré autentifikačné faktory ako MAC adresa (prípadne virtuálna), IP adresa (prípadne vo VPN) a SSH autentifikácia verejným kľúčom (aj viacnásobne a v kombinácii). Spomínaný mechanizmus samozrejme funguje aj pri neprítomnosti virtuálneho prostredia, len používateľ prípadne „musí“ viac krát niekam kliknúť než v predošlom prípade a poskytovaná aplikácia môže byť citlivejšia na „neporiadok“ na používateľovom HW, čo je možné do určitej miery redukovať web-aplikáciami (viď. napr. obr. 2).

Praktická realizácia

Na obr. 3 je záznam demonštračnej ukážky autorizovaného pripojenia na informačný web z pohľadu používateľa virtualizovaného prostredia (OS Windows XP) s využitím SSH (PuTTY terminálový klient) autentifikácie verejným kľúčom.

Autorom sa ako nástroj na spúšťanie a tvorbu virtuálnych prostredí osvedčil Open Source HW emulátor QEMU [2] dostupný pre množstvo architektúr a operačných systémov. U aplikačných serverov už takmer desaťročie s úspechom využívame natívnu virtualizáciu vo forme jailov na platformách FreeBSD [3] a OpenBSD [5]. V poslednom období testujeme možnosti využitia OpenBSD s QEMU ako hostiteľského systému pre hosťujúci FreeBSD s natívnymi jailami pre aplikácie a im predradené proxy servre, napr. Apache [1].

Na transparentnú realizáciu SSH spojení sú na klientskej strane používané plink z PuTTY [7] a ssh z OpenSSH [6], pričom sshd z OpenSSH je exkluzívne využívaný aj na strane autentifikačných brán (v spojení s authpf a PF z OpenBSD), mostoch a serveroch. Mechanizmus zobrazený na obr. 2 je využívaný pre nadštandardný prístup na WiFi-sieť (802.11n) Fakulty záhradníctva a krajinného inžinierstva (FZKI) Slovenskej poľnohospodárskej univerzity (SPU) v lokalitách na Tulipánovej a Hospodárskej ulici a vo výpožičnom oddelení Slovenskej poľnohospodárskej knižnice (SlPK) na Štúrovej ulici v Nitre.

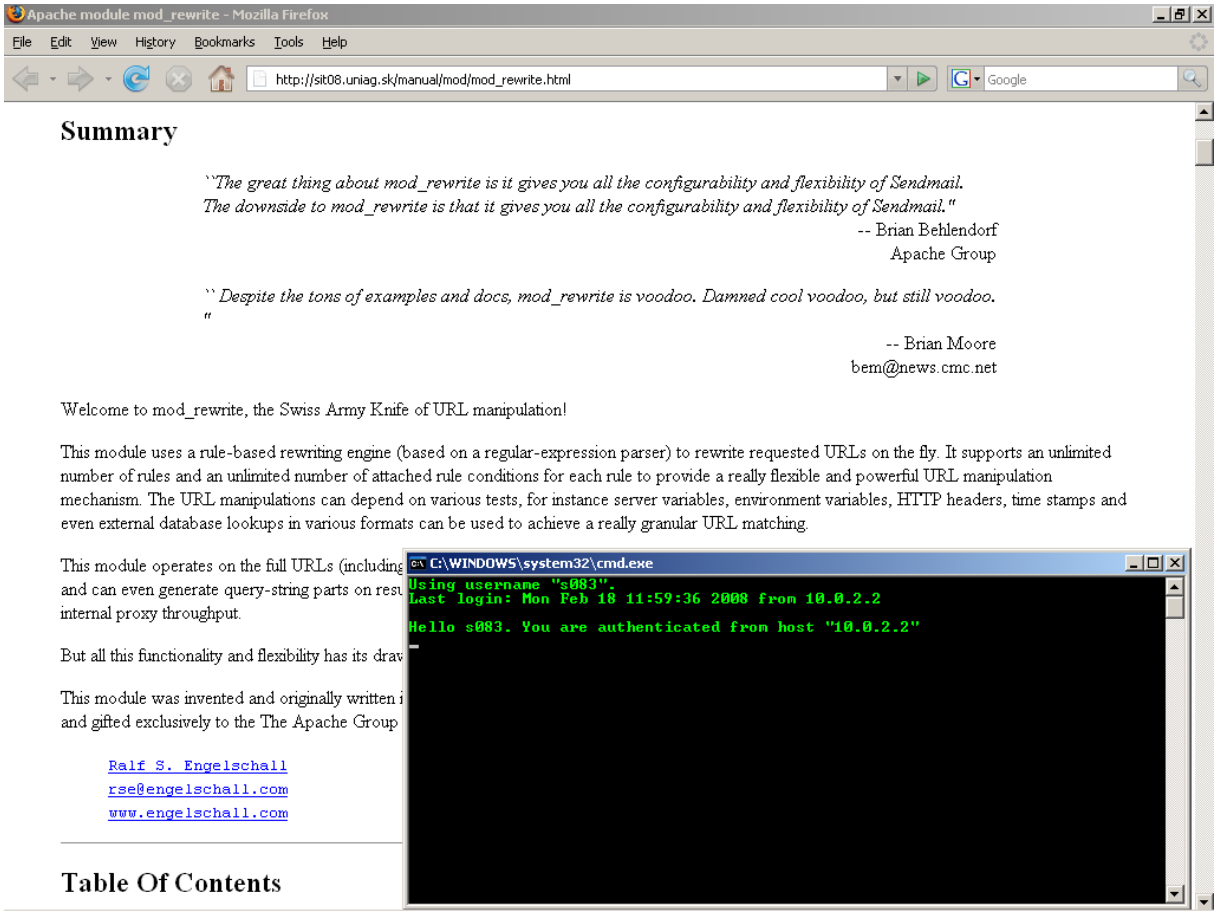
Sieť FZKI v objektoch na Tulipánovej a Hospodárskej ulici je segmentovaná podľa schémy na obr. 4 [4] tak na strane podsietí pre klientov, ako aj u demilitarizovaných zón (DMZ) serverov. Podobná segmentácia, v prepojení na tu spomínané nástroje, je postupne zavádzaná aj v SlPK.

Aplikačná infraštruktúra „schovaná“ na obr. 1—2 ako „AppServers“, ako bola budovaná a je v prevádzke na FZKI, je schematicky znázornená [4] na obr. 5 s tam popísanými redukciami.

Záver

Autori sa v tomto príspevku pokúsili naznačiť možnosti využitia virtualizácie a viacfaktorovej autentifikácie so zapojením protokolu SSH, vrátane poukázania na praktickú implementáciu a nasadenie v produkčnom prostredí v 3 lokalitách SPU. Veľká flexibilita, štandardnosť a kompletná zameniteľnosť jednotlivých prvkov, ktoré môžu byť buď zakúpené alebo zostavené vlastným úsilím z OpenSource komponentov sú výhodou predstavených riešení. Nevýhodou je pomerne malé povedomie o týchto možnostiach a to najmä u protokolu SSH. Žiadne technické riešenie, ani v spojení s maximálnym nasadením pracovníkov v oblasti IKT, ale nenahradí nedostatok inštitucionálnej kultúry, chýbajúcu podporu kompetentných článkov

riadenia, neexistujúce angažované komunity v organizácii a neochotu našej spoločnosti podporovať tvorivosť, vlastné projekty, výskum, vývoj, vzdelávanie a rozvoj nielen na konzum orientovanej kultúry.



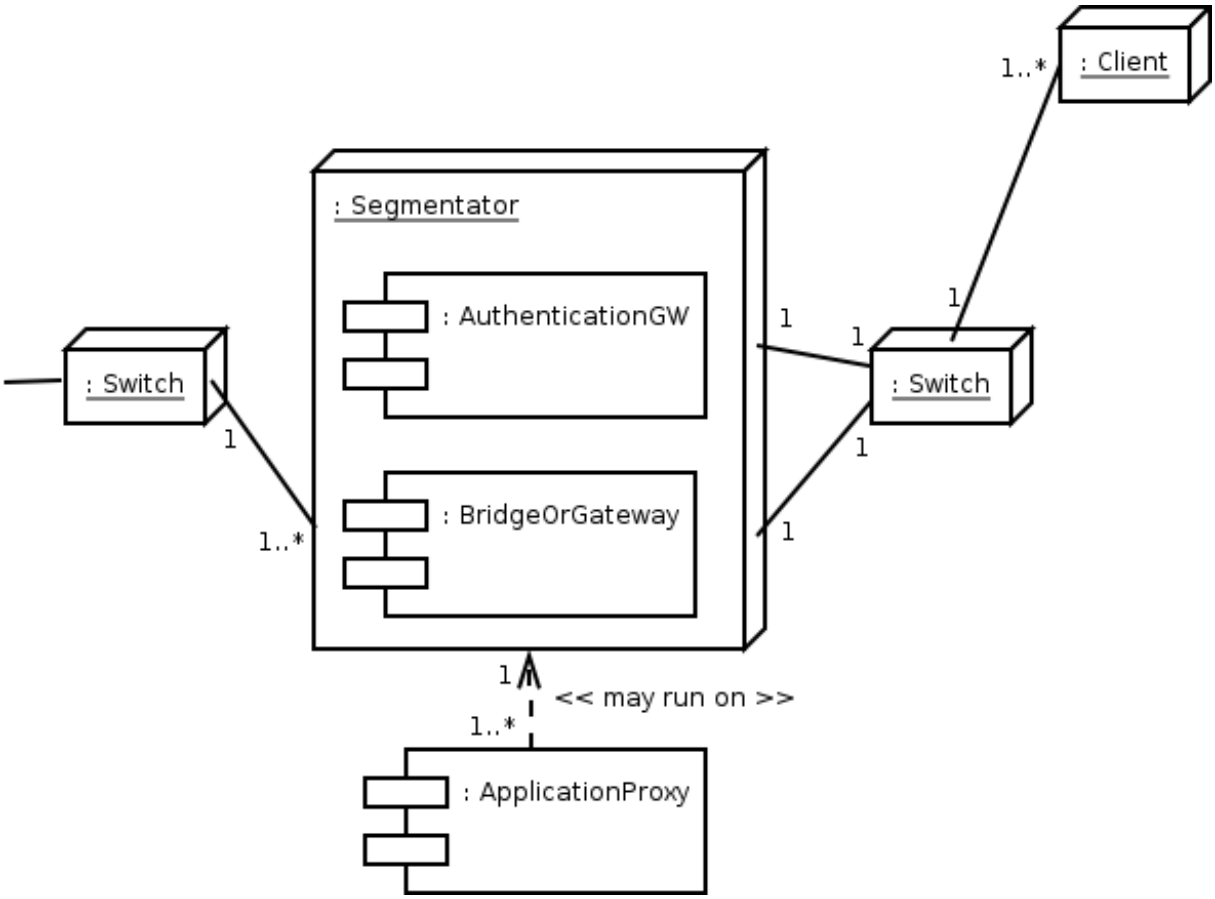
Obr. 3: Ilustrácia komunikácie autorizovaného používateľa autentifikovaného na základe viacerých faktorov, vrátane použitia kryptografického systému s verejným kľúčom (SSH public key authentication). Pripojenie na informačný web server cez autentifikačnú bránu a Socks proxy šifrovaným SSH kanálom. Informácia o úspešnej autentifikácii na prístupovej bráne je zobrazená vpravo dole.

Abstrakt

Tento príspevok naznačuje niektoré možnosti virtualizácie a viacfaktorovej autentifikácie so signifikantným zapojením často prehliadaného protokolu SSH. Stručné informácie k praktickým aspektom implementácie a nasadenia v podmienkach Slovenskej poľnohospodárskej univerzity sú tiež spomenuté. Samoilustračné diagramy a obrázky dopĺňajú text.

Kľúčové slová

virtualizácia, QEMU, SSH, PuTTY, HTTP proxy, Socks proxy, Apache HTTP server, autentifikácia verejným kľúčom, OpenBSD, FreeBSD, viacfaktorová autentifikácia



Obr. 4: Schéma možností nasadenia segmentačných opatrení a viacfaktorových kontrolných mechanizmov na firewalloch, mostoch (bridge) a autentifikačných bránach v chránenej LAN.

Literatúra

[1] Apache Foundation. 2008. Apache HTTP Server. [online]. [cit. 2008-02-06]. Dostupné na internete: <http://httpd.apache.org/>.

[2] Bellard, F. 2008. QEMU Open Source Processor Emulator. [online]. [cit. 2008-02-06]. Dostupné na internete: <http://fabrice.bellard.free.fr/qemu/>.

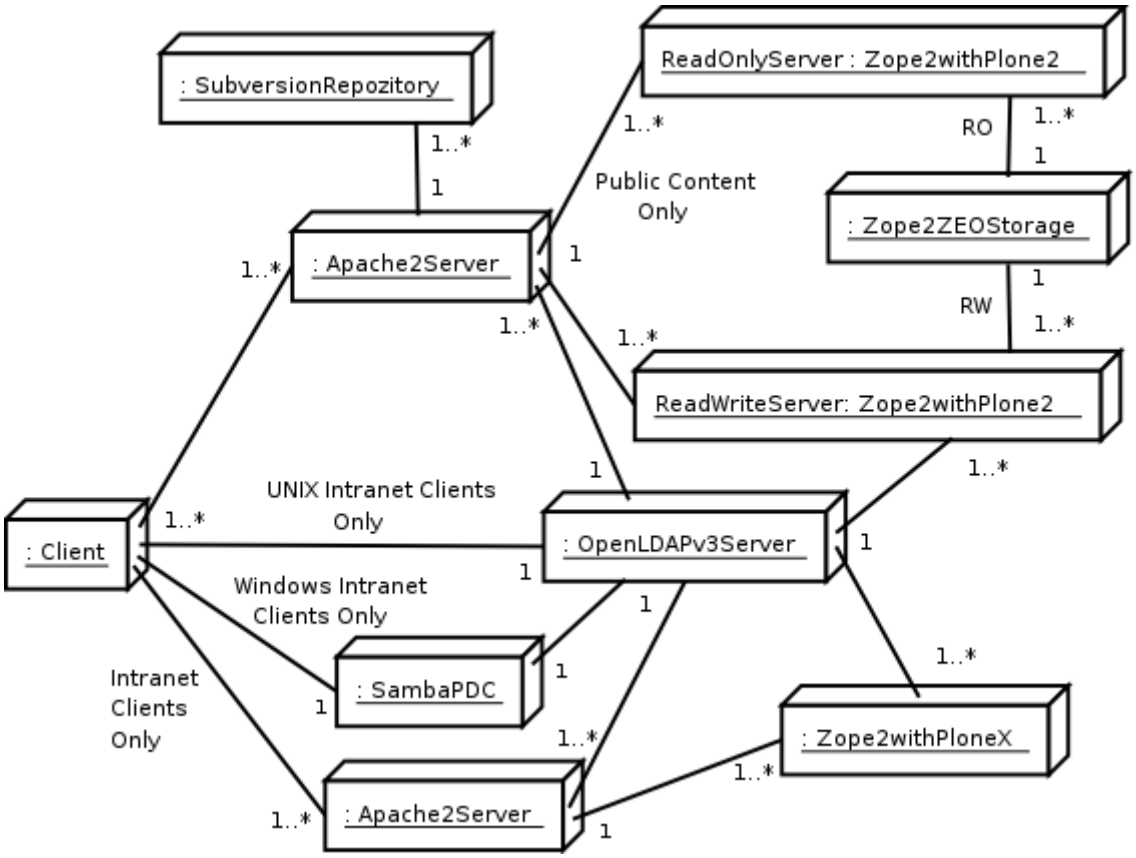
[3] FreeBSD Community. 2008. FreeBSD OS Resources. [online]. [cit. 2008-02-06]. Dostupné na internete: <http://www.freebsd.org/>.

[4] Mucha, M. — Mucha, R. 2006. Poznámky k optimalizácii prístupu k prostriedkom IKT. [online]. [cit. 2008-02-06]. Dostupné na internete: <http://fzki.uniag.sk/Members/mucha_m/>.

[5] OpenBSD Community. 2008. OpenBSD OS Resources. [online]. [cit. 2008-02-06]. Dostupné na internete: <http://www.openbsd.org/>.

[6] OpenSSH Team. 2008. OpenSSH Resources. [online]. [cit. 2008-02-06]. Dostupné na internete: <http://www.openssh.org/>.[6] OpenSSH Team. 2008. OpenSSH Resources. [online]. [cit. 2008-02-06]. Dostupné na internete: <http://www.openssh.org/>.

[7] PuTTY Team. 2008. PuTTY SSH Client Resources. [online]. [cit. 2008-02-06]. Dostupné na internete: <http://www.chiark.greenend.org.uk/~sgtatham/putty/>.



Obr. 5: Schéma nasadenia virtualizovaných aplikačných serverov (natívna virtualizácia na platformách FreeBSD a OpenBSD plus QEMU v prostredí OpenBSD) a autentifikačných opatrení v časti FZKI SPU LAN. Znázornená infraštruktúra bola budovaná od roku 2000 a dobudovaná v uvedenej podobe v rokoch 2005 až 2006. Je neustále aktualizovaná a udržiavaná v nepretržitej prevádzke až do dnešných dní. LDAP server a PDC nie sú momentálne spustené z organizačných dôvodov (chýbajúca podpora riadiacich štruktúr), časť adresárovej infraštruktúry je tak integrovaná priamo do aplikačných serverov alebo realizovaná inými mechanizmami.

Kontakt

Ing. Miloslav Mucha, CIKT FZKI SPU, Hospodárska 7, 949 76 Nitra, Slovakia, tel.: +421 37 641 5235, E-mail adresa: Miloslav.Mucha@uniag.sk