Crypto-World

Informační sešit GCUCMP
ISSN 1801-2140

Ročník 9, číslo 2/2007 **15. únor 2007**

2/2007

Připravil: Mgr. Pavel Vondruška

Sešit je přednostně distribuován registrovaným čtenářům.
Starší sešity jsou dostupné na adrese
http://crypto-world.info
(1230 registrovaných odběratelů)

Obsah : str.

A. Najväčšia tma je pod lampou – STEGANOGRAFIA
Časť I.

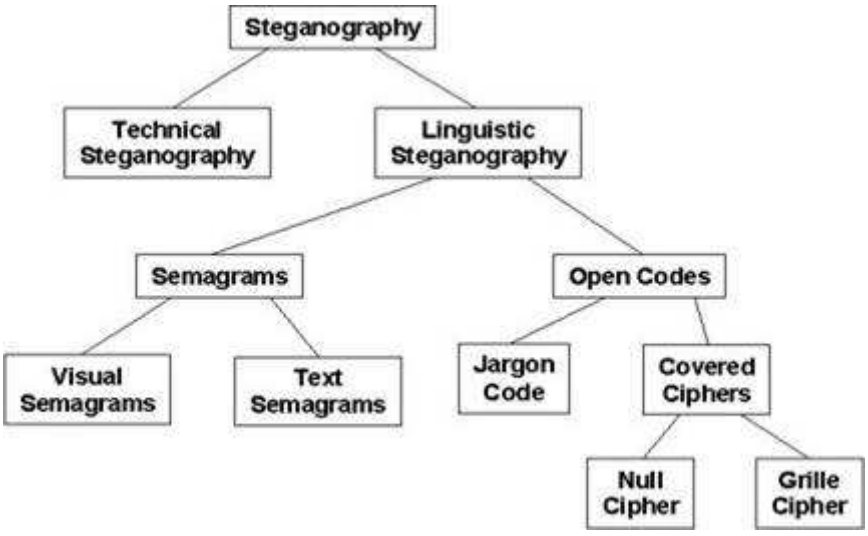
Roman Cinkais, VošonSpšo – IT, MFF UK
http://atrey.karlin.mff.cuni.cz/~cinky
e-mail: roman.cinkais@gmail.com

Obsah

1. Úvod

Steganografia je umenie ako ukryť alebo zakryť správu. Účel steganografie je kamuflovať(podviesť) komunikáciu – utajiť existenciu správy pre tretiu stranu. Tým sa líši od kryptografie. Niektorí autori však považujú steganografiu ako formu kryptografie odkedy je tajná komunikácia považovaná za tajné písance (Bauer 2002).

Aj keď termín steganografia sa začal používať na konci 15-teho storočia, použitie steganografie siaha až do dávnej minulosti. V staroveku boli správy skrývané na zadnú stranu voskových tabuliek (zaliali sa voskom a nebolo ich vidieť), na králičí žalúdok, alebo boli vytetované na hlavu otroka (a čakalo sa kým mu dorástli vlasy). Neviditelný atrament sa používa po stáročia – dnes už skôr pre zábavu ale takisto pre špionáže teroristov. Mikrobody a mikrofilmy, neoddeliteľná súčasť vojny a špionážnych filmov, sa začali používať až po vytvorení fotografií. (Arnold 2003; Johnson 2001; Kahn 1996; Wayner 2002).



Obrázok 1. Klasifikácia steganografických techník (prispôsobené podľa Bauera 2002).

Steganografia ukrýva nejakú správu, ale nie fakt, že medzi oboma partiami prebieha komunikácia. Steganografický proces všeobecne zahŕňa vloženie utajovanej správy na transportné médium nazývané **nosič**. Tajná správa je vložená (zabudovaná) do nosiča a vytvára takzvané **steganografické médium**. Steganografický kľúč môže byť použitý pre kódovanie skrývanej správy a/alebo pre vygenerovanie náhodnej steganografickej schémy.

V skutočnosti:
steganografické médium = ukrývaná správa + nosič + steganografický kľúč

Obrázok 1 na predchádzajúcej stránke, ukazuje obvyklú systematiku steganografických techník (Arnold 2003; Bauer 2002).

- **Technická steganografia (Technical steganography)** využíva vedecko-technické metódy na ukrytie správy, ako je napríklad použitie neviditeľného atramentu alebo mikrobodov a ostatných veľkosť redukujúcich metód.

- **Lingvistická (jazyková) steganografia (Linguistic steganography)** ukrýva správu do nosiča v nie veľmi zreteľnom spôsobe a je ďalej triedená na semagramy a otvorené kódy.

- **Semagramy (Semagrams)** ukrývajú správu pomocou symbolov a znakov. **Vizuálny (obrazový) semagram (Visual semagrams)** využíva nevinne vyzerajúce objekty alebo veci, s ktorými sa stretávame každý deň, ako napríklad čmárance alebo ukladanie vecí na stôl v určitom poradí alebo na webovú stránku, na to, aby sa správa dostala k druhej strane. **Textový semagram (Text semagrams)** ukrýva správu modifikovaním vzhľadu textu na nosiči, napríklad jemné úpravy vo veľkosti a typu písma, pridávanie extra medzier, alebo odlišné ozdobenie písma v dopise.

- **Otvorené kódy (Open codes)** ukrývajú správu na pravú správu nosiča tak, že to nič netušiacemu pozorovateľovi nepríde zreteľné. Takáto správa na nosiči sa niekedy nazýva vyložená alebo jasná komunikácia, zatiaľ čo ukrývaná správa je utajovaná komunikácia. Táto kategória sa ešte delí na žargónové kódy a skryté šifry.

- **Žargónové kódy (Jargon codes)**, ako napovedá názov, používajú jazyk, ktorý ovláda len istá skupina ľudí a je nezrozumiteľný pre ostatných. Žargónové kódy zahrňujú warchalking (symboly používané na indikovanie prítomnosti a typu signálu bezdrôtovej siete [Warchalking 2003]). iné terminológie, alebo prostú komunikáciu, ktorá prevádza špeciálny zmysel nejakého faktu, ktorý je známy len konkrétnej osobe. Podmnožinou žargónových kódov sú **pokynové kódy (Cue codes)**, kde určité dopredu dohodnuté frázy plnia svoj zmysel.

Obrázok 2. Grille cipher.

- **Skryté alebo ukryté šifry (Covered ciphers)** ukrývajú správu otvorenú na nosič tak, aby ju bolo možné obnoviť len niekým, kto pozná tajomstvo, ako to bolo ukrývané. **Zamrežová šifra (Grille cipher)** využíva vzor (šablonu), ktorý je používaný na pokrytie správy nosiča. **Nulová šifra (Null cipher)** ukrýva správu na základe nejakej preddefinovanej množine pravidiel, ako napríklad „čítaj každé piate slovo“ alebo „čítaj tretie písmeno v každom slove“.

Zväčšovaním množstva dát ukladaného na počítač a posielaním jeho obsahu po sieti nie je prekvapujúce, že steganografia vstupuje do digitálneho veku. Steganografia na počítači a na sieti umožnuje ukrývať nejaký typ binárnych súborov do iného binárneho súboru. Obrázok a audio súbor sú dnes najviac používané nosiče.

Steganografia poskytuje niektoré veľmi užitočné a zaujimavé funkcie v digitálnom svete, z čoho je najviac používaný digitálny **watermarking**. V takejto aplikácii môže autor vložit ukrývanú správu do súboru, takže neskôr môže pomocou toho potvrdiť vlastníctvo daného súboru. Napríklad maliar by mohol poslať prostredníctvom internetu svoje originálne dielo. Ak niekto ukradne tento súbor a bude tvrdiť, že obraz je jeho, maliar môže neskôr bez problémov dokázať vlastníctvo, pretože on jediný je schopný obnoviť watermark (Arnold 2003; Barni 2001; Kwok 2003). Aj keď je watermarking konceptuálne podobný steganografii, väčšinou má rozdielne technické smery.

Steganografia podporuje množstvo nelegálnych aplikácií, najviac známe je napríklad ukrývanie ilegálnych nahrávok, finančných podvodov, priemyslových špionáži, a komunikácie medzi členmi nejakej teroristickej alebo zločinnej organizácie (Hosmer a Hyde 2003).

2. Nulová šifra

Historicky sú nulové šifry spôsobom, ako ukryť správu do inej bez použitia komplikovaného algoritmu. Ukážeme si príklad jednu z najjednoduchších nulových šifier:

PRESIDENT'S EMBARGO RULING SHOULD HAVE IMMEDIATE NOTICE. GRAVE SITUATION AFFECTING INTERNATIONAL LAW. STATEMENT FORESHADOWS RUIN OF MANY NEUTRALS. YELLOW JOURNALS UNIFYING NATIONAL EXCITEMENT IMMENSELY.

APPARENTLY NEUTRAL'S PROTEST IS THOROUGHLY DISCOUNTED AND IGNORED. ISMAN HARD HIT. BLOCKADE ISSUE AFFECTS PRETEXT FOR EMBARGO ON BYPRODUCTS, EJECTING SUETS AND VEGETABLE OILS.

Nemecká ambasáda vo Washingtone, DC, poslala túto správu v telegrame do centrály v Berlíne počas prvej svetovej vojny (Kahn 1996). Keď prečítame prvé písmeno z každého slova v prvej správe a druhé písmeno z každého slova v druhej správe, dostaneme nasledujúci skrytý text:
PERSHING SAILS FROM N.Y. JUNE 1

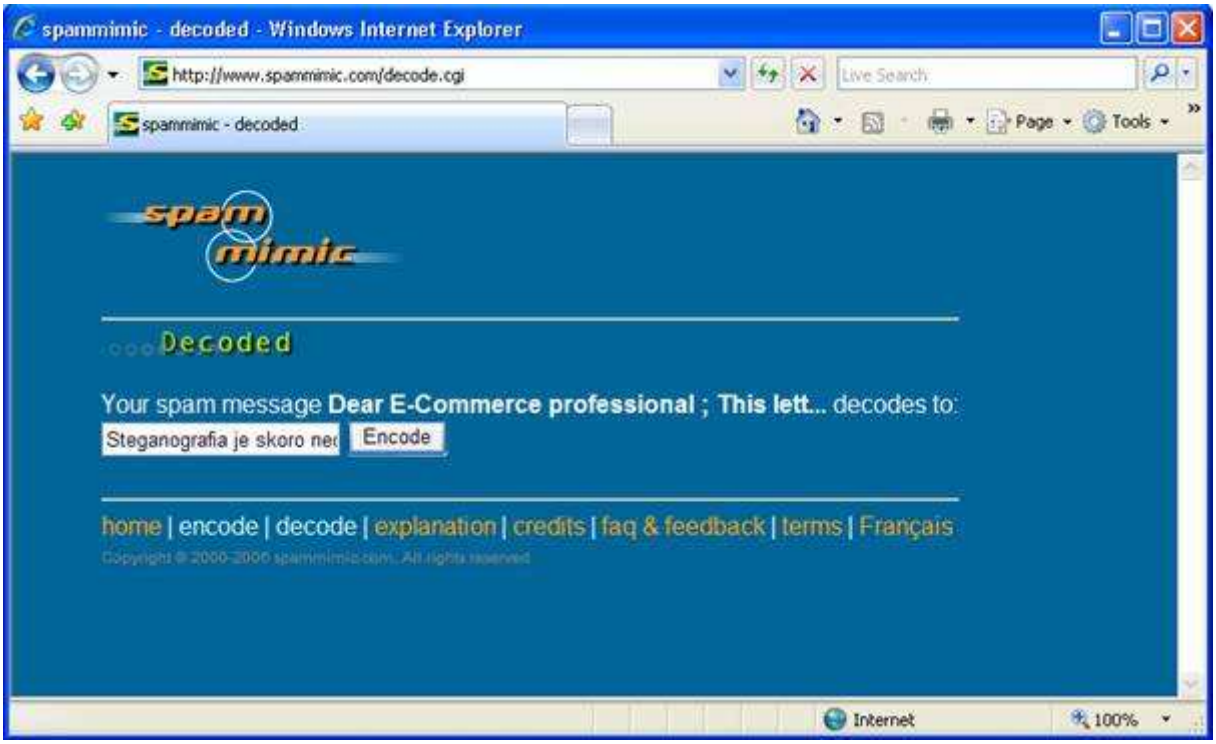
Na internete je spam potenciálnym nosičom pre ukrývanú správu. Skúste zvážiť nasledujúci text:

Dear E-Commerce professional ; This letter was specially selected to be sent to you . This is a one time mailing there is no need to request removal if you won't want any more . This mail is being sent in compliance with Senate bill 1916 , Title 6 ; Section 304 . Do NOT confuse us with Internet scam artists ! Why work for somebody else when you can become rich as few as 94 months ! Have you ever noticed most everyone has a cellphone and nobody is getting any younger ! Well, now is your chance to capitalize on this . WE will help YOU use credit cards on your website & use credit cards on your website ! You are guaranteed to succeed because we take all the risk ! But don't believe us . Prof Jones of Wisconsin tried us and says "I was skeptical but it worked for me" . We are a BBB member in good standing ! DO NOT DELAY - order today . Sign up a friend and you get half off ! Thanks ! Dear Salaryman , This letter was specially selected to be sent to you ! We will comply with all removal requests . This mail is being sent in compliance with Senate bill 1618 ; Title 4 , Section 302 ! Do NOT confuse us with Internet scam artists ! Why work for somebody else when you can become rich within 82 weeks ! Have you ever noticed nearly every commercial on television has a .com on in it & people love convenience . Well, now is your chance to capitalize on this ! We will help you use credit cards on your website & SELL MORE ! You can begin at absolutely no cost to you . But don't believe us . Mrs Ames of Iowa tried us and says "Now I'm rich, Rich, RICH" . We assure you that we operate within all applicable laws . Do not delay - order today . Sign up a friend and you get half off ! Thanks . Dear Business person , This letter was specially selected to be sent to you ! We will comply with all removal requests . This mail is being sent in compliance with Senate bill 2616 ; Title 8 ; Section 306 ! Do NOT confuse us with Internet scam artists ! Why work for somebody else when you can become rich inside 39 weeks . Have you ever noticed most everyone has a cellphone and people love convenience . Well, now is your chance to capitalize on this . WE will help YOU SELL MORE and deliver goods right to the customer's doorstep . The best thing about our system is that it is absolutely risk free for you . But don't believe us ! Mrs Simpson who resides in Wisconsin tried us and says "I've been poor and I've been rich - rich is better" ! We are a BBB member in good standing ! We BESEECH you - act now ! Sign up a friend and your friend will be rich too . Thanks ! Dear Friend ; This letter was specially selected to be sent to you . We will comply with all removal requests ! This mail is being sent in compliance with Senate bill 1622 ; Title 3 ; Section 303 ! This is not multi-level marketing . Why work for somebody else when you can become rich inside 79 days . Have you ever noticed most everyone has a cellphone and society seems to be moving faster and faster . Well, now is your chance to capitalize on this . We will help you process your orders within seconds & deliver goods right to the customer's doorstep . The best thing about our system is that it is absolutely risk free for you . But don't believe us . Ms Simpson of Mississippi tried us and says "Now I'm rich many more things are possible" . We assure you that we operate within all applicable laws ! Do not delay - order today ! Sign up a friend and your friend will be rich too ! Cheers .

Táto správa vyzerá ako typický spam, ktorý je väčšinou ignorovaný a vyradený z e-mailovej schránky. Správa bola vytvorená cez spam mimic. Je to webová stránka, ktorá konvertuje krátku textovú správu do textového bloku vyzerajúceho ako typický spam prostredníctvom idey gramaticky založenej mimiky (spam mimic 2003; Wayner 2002). Tretia strana nezistí nič všimaním si rozostupu medzier alebo gramatických chýb. Jedničky a nuly sú kódované voľbou slov. Ukrytá správa v spame hore je:

Steganografia je skoro neodhaliteľná.

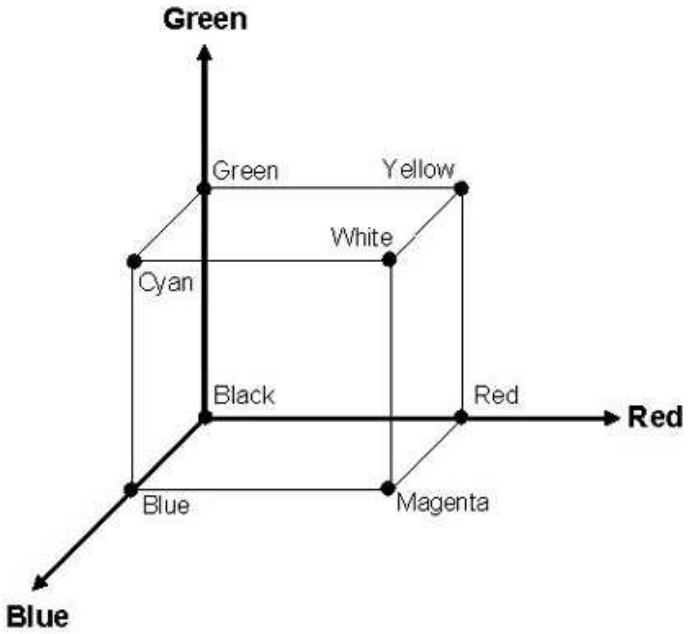
Na ukrytie správy do digitálneho súboru používajúc nulové šifry nepotrebujeme žiadne špeciálne nástroje. Obrázok alebo text môže byť ukrytý pod iným obrázkom napríklad v súbore aplikácie PowerPoint. Správa môže byť ukrytá vo vlastnostiach súboru typu Word, v komentároch na webovej stránke, alebo v ďalších rôznych formátových vlastnostiach, ktoré sú ignorované prehliadačom (Artz 2001). Správa môže byť grafický uložená v dokumente nastavením farby písma na farbu pozadia a umiestnením nejakého obrázka na pozadie. Adresát potom získa správu ďalšou zmenou farby textu (Seward 2004). To všetko sú rozhodne slabé mechanizmy, ale takisto môžu byť veľmi efektívne.



Obrázok 3. Webová aplikácia spam mimic.

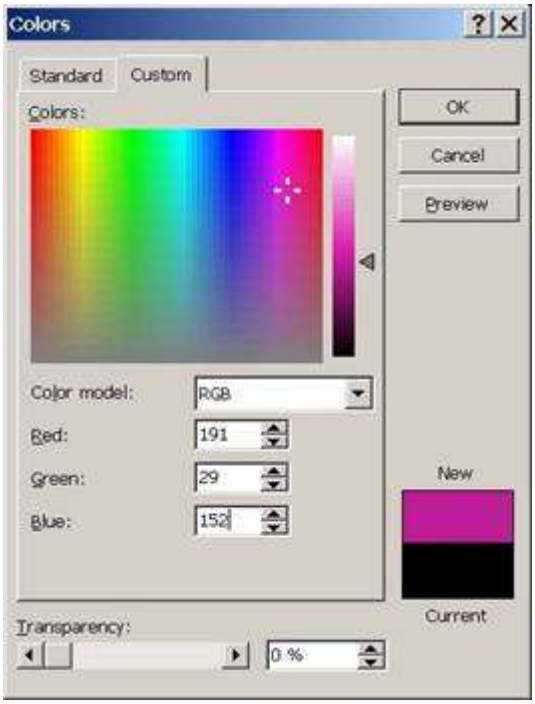
3. Digitálny obrázok a audio

Mnoho súčasných digitálnych steganografických techník využíva grafické obrázky alebo audio súbory ako nosič média. Je poučné sa pozrieť ako funkuje kódovanie obrázkov a audio súborov predtým, ako budeme hovoriť o tom, akým spôsobom pracuje steganografia a steganoanalýza s týmito nosičmi.



Obrázok 4. Schéma RGB.

Obrázok 4 znázorňuje rozloženie **RGB** farieb, kde každú farbu reprezentuje nejaká intenzita z každej farebnej komponenty – červená (red), zelená (green), modrá (blue). Absencia všetkých farieb dáva farbu čiernu, znázornené ako prienik všetkých farieb v nule. Mix 100 percent z každej farby dáva farbu bielu. Ostatné farby získame podobne.



Obrázok 5. Ukážka RGB stupňov vo vybranej farbe.

Obrázok 5 ukazuje intenzitu RGB pri nejakej náhodnej farbe. Každá komponenta je určená jedným bajtom, takže hodnoty pre každú farbu sú v škále od 0 do 255 . Na obrázku je konkrétny odtieň (fialová farba) označený takto: červený stupeň 191 (hex BF), zelený stupeň 29 (hex 1D), modrý stupeň 152 (hex 92). Teda fialová farba by bola kódovaná 24 bitmi ako 0xBF1D98. Táto 24-bitová kódovacia schéma podporuje 16,777,216 (2^24) unikátnych farieb (Curran a Bailey 2003; Johnson a Jajodia 1998A).

Dnes už väčšina aplikácii, ktoré pracujú s digitálnymi obrázkami podporuje 24-bitové farby (24-bit true color), kde každý element obrázka (pixel) je kódovaný do 24 bitov zahrňujúcich tri RGB bajty ako sme si ukázali vyššie. Ostatné aplikácie používajú kódovanie farieb do 8 bitov na každý pixel. Tieto schémy takisto používajú 24-bitové farby, ale pri tom využívajú paletu, ktorá označuje aké farby sú používané v obrázku. Každý pixel je kódovaný v 8 bitoch, kde hodnota ukazuje na hodnotu v 24 bitoch na palete. Z tohto dôvodu táto metóda podporuje len 256 (2^8) farieb. Voľba kódovania farieb má prirodzene vplyv na veľkosť obrázka (nie rozmer ale data uložené na disku). 640 x 480 pixelový obrázok, ktorý používa 8-bitové farby môže zaberať približne 307 KB (640 x 480 = 307,200 bajtov), zatiaľ čo 1400 x 1050 pixelový obrázok používajúci 24-bitové farby potrebuje 4.4 MB (1400 x 1050 x 3 = 4,410,000 bajtov).

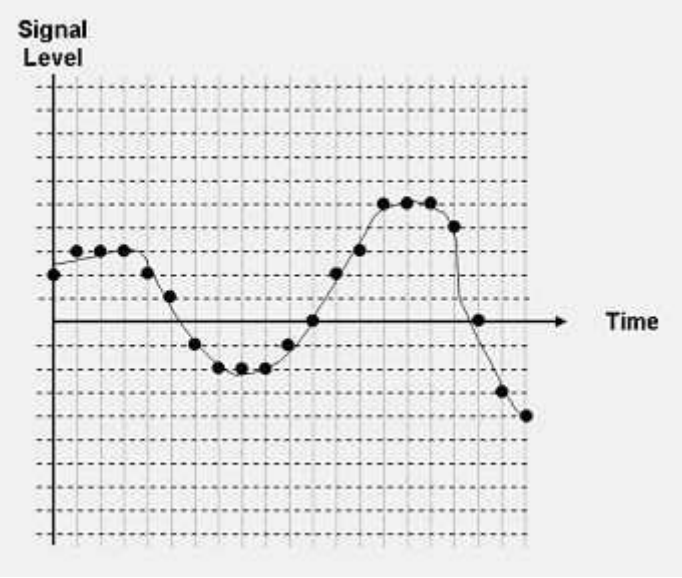
Farebné palety a 8-bitové farby obvykle používali formáty obrázkov **Graphics Interchange Format (GIF)** a **Bitmap (BMP),** ale dnes to už nemusí byť pravda. Obidva formáty môžu využívať aj viacbitovú reprezentáciu pixelov. GIF a BMP sú označované ako formáty s bezstratovou kompresiou, pretože obraz získaný po kódovaní a kompresii je bit po bitu identický originálu (Johnson and Jajodia 1998A).

Joint Photographic Experts Group (JPEG) formáty používajú individuálnu kosínusovu transformáciu radšej ako kódovanie bit po bite. V JPEG súbore je obraz rozdelený do 8 x 8 blokov pre každú samostatnú farebnú komponentu. Cieľom je nájsť bloky, kde množstvo zmien v hodnotách pixelov (energia, the energy) je nízka. Ak stupeň energie je príliš vysoký, blok je rozdelený na 8 x 8 podblokov, až kým energia nie je dostatočne nízka. Každý blok (alebo podblok) je zmenený na 64 individuálnych kosínusových transformáčných koeficientov, ktoré vytvárajú svietivosť (jasnosť (brightness), nejasnosť (darkness) a kontrast(contrast)) a farebnosť (color) tej konkrétnej časti obrázka. JPEG je formát so stratovou kompresiou, pretože obraz získaný z komprimovaného JPEG súboru je vizuálne skoro rovnaký, ale nie identický s originálom (Johnson a Jajodia 1998A; Monash University 2004; Provos a Honeyman 2003).

Audio kódovanie zahrňuje konvertovanie analogového signálu do bitového toku. Analogový zvuk – hlas a hudba – je reprezentovaný sínusovými vlnami v rozličných frekvenciách. Ľudské ucho dokáže vnímať frekvenciu v rozsahu od 20 do 20 000 Hz (cyklus/sekunda). Zvuk je analogový teda je to spojitý signál. Ukladanie zvuku digitálne vyžaduje aby spojitá zvuková vlna bola skonvertovaná do množiny vzorov, ktoré môžu byť reprezentované sekvenciou núl a jedničiek.

Analogovo-digitálna (analog-to-digital) konverzia je ukončená vytvorením vzoru z analogového signálu (pomocou mikrofónu alebo iného audio detektoru) a skonvertovaním tohto vzoru na stupeň napätia. Toto napätie je potom prevedené na numerickú hodnotu, ktorá používa schému nazývanú **modulácia pulzov (pulse code modulation)**. Prístroj, ktorý vykonáva túto konverziu je nazývaný kóder-dekóder (coder-decoder) alebo jodnoducho kodek (codec, väčšinou sa používa v zmysle PCM + kompression algorithm).

Modulácia pulzov obstaráva iba aproximáciu originálneho analogového signálu, ako znázorňuje obrázok 6. Ak je napríklad stupeň analogového zvuku zmeraný na 4.86 stupňa, bude to skonvertované na 5 pomocou modulácie pulzov. Toto sa nazýva **chyba hromadenia (quantization error)**. Rozdielne audio aplikácie majú definované iné čísla ako stupne modulácie pulzov, takže táto chyba je skoro nepostrehnuteľná pre ľudské ucho. Telefónna sieť konvertuje každý hlasový záznam do 8-bitovej hodnoty (0-255), zatiaľ čo hudobné aplikácie používajú hlavne 16-bitové hodnoty (0-65,535) (Fries and Fries 2000; Rey 1983).



Obrázok 6. Jednoduchá modulácia pulzov (signal level = stupeň signálu).

Analogové signály musia byť vzorkované minimálne v dvakrát väčšej miere ako je frekvencia komponentu signálu, aby originál mohol byť korektne reprodukovaný zo vzorkov samostatne. V telefónnej sieti je ľudský hlas prenášaný s frekvenciou 0-4000 Hz (hoci len nejakých 400-3400 Hz je v skutočnosti používaných), a preto je hlas vzorkovaný 8000krát za sekundu (8 kHz, sample rate, frekvencia vzorkovania). Hudobne aplikácie predpokládajú celé spektrum ľudského ucha a používajú skoro vždy 44.1 sampling rate (samozrejme môžu používať aj iné vzorkovanie) (Fries a Fries 2000; Rey 1983).

Rýchlosť prenosu nekomprimovanej hudby môže byť ľahko vypočítaná z frekvencie vzorkovania (44.1 kHz), modulácie pulzov (16 bits), a z počtu zvukových kanálov (stereo má počet kanálov 2). Teda dostávame 1,411,200 bitov za sekundu. Tým by jedno-minutový audio súbor (nekomprimovaný) mohol zaberať 10.6 MB (1,411,200*60/8 = 10,584,000). Veľkosť audio súborov sa v skutočnosti zmenšuje pomocou rôznych kompresných techník. Jedna očividná metóda je redukovať počet kanálov na jeden, alebo redukovať frekvenciu vzorkovania, v niektorých prípadoch až na 11 kHz. Rôzne kodeky používajú vlastné kompresné schémy. Všetky tieto redukujúce spôsoby ale znižuju kvalitu zvuku.

Tabuľka 1. Niektoré bežné digitálne audio formáty (Fries and Fries 2000).

Audio formát	**Prípona súboru**	**Kodek**
AIFF (Mac)	.aif, .aiff	Pulse code modulation (alebo iné)
AU (Sun/Next)	.au	µ-law (alebo iné)
CD audio (CDDA)	n/a	Pulse code modulation
MP3	.mp3	MPEG Audio Layer III
Windows Media Audio	.wma	Microsoft proprietary
QuickTime	.qt	Apple Computer proprietary
RealAudio	.ra, .ram	Real Networks proprietary
WAV	.wav	Pulse code modulation (alebo iné)

Konec prvej časti.

B. XML a bezpečnost
Část II.

RNDr. Dagmar Brechlerová, Ústav informatiky AV ČR, v. v. i.,
Oddělení medicínské informatiky a KIT PEF ČZU
(Dagmar.Brechlerova@seznam.cz)

XACML

XACML (Extensible Access Control Markup language) je iniciativa vedená skupinou OASIS [3], je určená na vyjádření **bezpečnostní politiky pro přístup** (autentizaci a autorizaci) k XML dokumentům a datovým zdrojům. Souvisí se SAML (viz dále) a to tak, že SAML poskytuje mechanismus pro šíření autentizačních a autorizačních informací mezi servery a službami, zatímco **XACML je autentizační a autorizační informací.** Idea XACML je ta, že XML dokument nebo samotný SOAP vzkaz může popisovat politiku přístupu, tj. kdo má mít přístup k čemu atd.
Cílem je **standardizovat jazyk pro popsání autentizace a přístupových politik** v XML syntaxi. Standardní jazyk pro kontrolu přístupu vede k nízkým nákladům, protože není potřeba vyvíjet jazyk pro určitou aplikaci nebo psát politiky kontroly přístupu ve více jazycích. Pomocí XACML je možné vytvářet politiky kontroly přístupu z těch, které byly vytvořeny jinými stranami. XACML definuje slovník pro specifikaci předmětu, práv subjektu a podmínek. Jeden standardní jazyk pro řízení kontroly přístupu může nahradit několik jiných jazyků jednotlivých aplikací.

V kostce: XACML je jazyk pro řízení přístupu, poskytuje syntaxi (definovanou v XML) pro řízení přístupu ke zdrojům.
XACML je standard OASIS, který popisuje jednak **jazyk pro politiku a jednak jazyk pro řízení přístupu založený na dotaz / odpověď** (obojí je napsané v XML). XACML (extensible access control markup language) je tedy jazyk založený na XML. Jazyk politiky je použit na vyjádření politiky řízení přístupu – popisuje obecné požadavky řízení kontroly přístupu. A má standardní rozšiřitelné body pro definování nových funkcí, datových typů, kombinační logiky atd. Je zde tedy možno definovat, kdo může kdy dělat co. Jazyk dotaz / odpověď umožňuje vyjádřit dotaz, zda speciální akce může být dovolena (vyžádána) a interpretovat výsledek. Odezva (reakce) vždy zahrnuje odpověď, zda požadavek může být povolen, za použití 4 hodnot:

Permit - povolit
Deny - zakázat
Inderterminate - neurčené, vyskytuje se chyba nebo chybí nějaké hodnoty a nemůže být určena odpověď
Not Applicable – žádost nemůže být odpověděna touto službou

V typickém XACML scénáři **subjekt** (tj. uživatel nebo pracovní stanice) chce udělat nějakou akci na speciálním zdroji. Subjekt podá žádost entitě, která chrání zdroj (např. web server, souborový systém atd.). Tato entita se nazývá **PEP** (Policy Enforcement Point). PEP zformuluje dotaz (za použití XACML jazyka) založený na atributech subjektu, akci, požadovaném zdroji a dalších informacích náležejících dotazu. PEP potom pošle tento dotaz

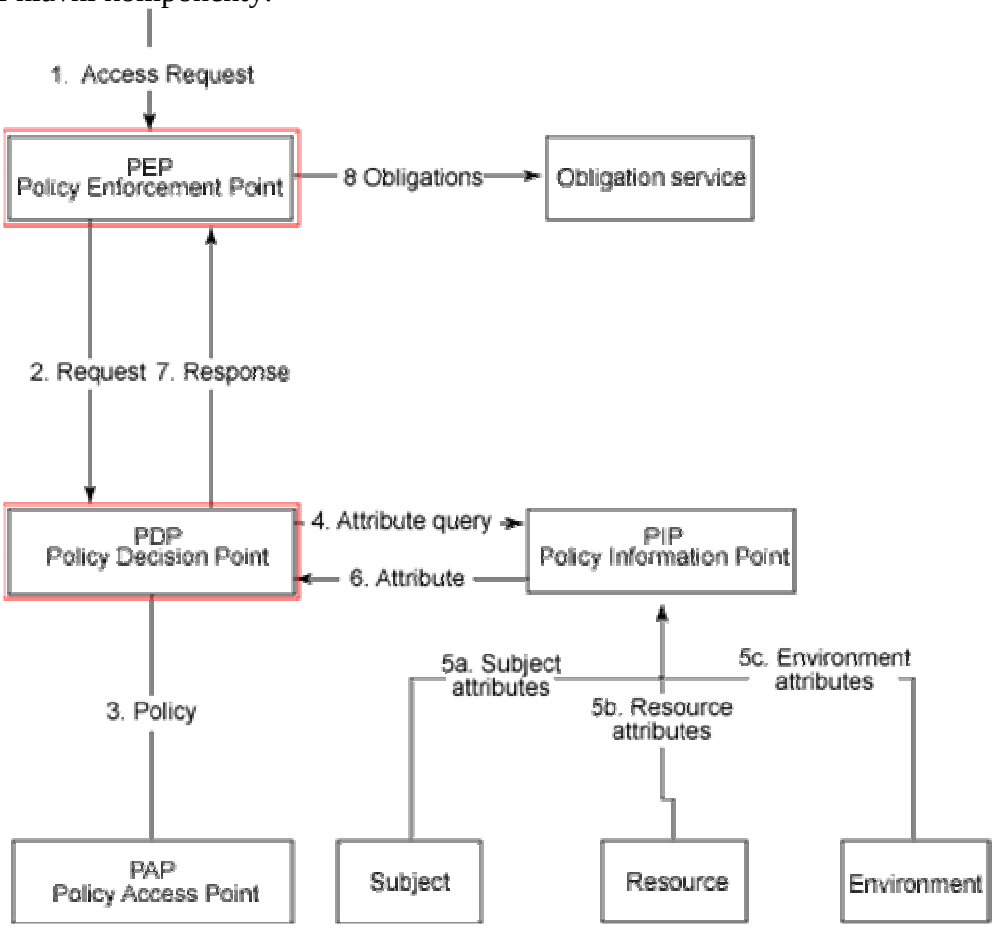
PDP (Policy Decision Point), který se podívá na dotaz a nějakou politiku, kterou aplikuje na dotaz a přijde s odpovědí, zda může být přístup povolen. Odpověď vyjádřená v XACML jazyku je vrácena PEP, který pak povolí nebo zakáže přístup. PEP i PDP mohou být buď v jednotlivé aplikaci nebo mohou být distribuovány na několika serverech. Navíc k poskytnutí dotaz / odpověď a jazyku politik, XACML také poskytuje další části tohoto vztahu, speciálně nalezení politiky, která se aplikuje pro daný dotaz a ověření, zda porovnáním žádosti a dané politiky je přístup povolen nebo ne.

XACML má mnoho výhod nad jinými jazyky (existuje mnoho proprietárních a pro nějakou aplikaci specifických jiných jazyků) pro politiku řízení přístupu

1. Jeden standardní jazyk pro řízení kontroly přístupu může nahradit několik jiných jazyků jednotlivých aplikací. Použitím standardního jazyka se bude užívat něco, co užívá široká komunita expertů a uživatelů, nebudou se muset stále znovu zavádět nové jazyky, bude snazší spolupracovat s jinými aplikacemi používajícími stejný standardní jazyk.

2. Je to generické. To znamená, že místo pokoušet se o accesss control pro speciální prostředí nebo speciální zdroj, může to být užito v jakémkoliv prostředí. Může být napsána jedna politika, která může být užita mnoha různými druhy aplikací a pokud je užit jeden společný jazyk, management politik je snazší.

XACML hlavní komponenty:



3. Je to distribuované tj. může se napsat politika, která se po řadě odvolává na jiné politiky, které se vyskytují v libovolném okolí. Výsledkem je to, že místo „managování“

monolitické politiky různí lidé nebo různé skupiny mohou mít svoje politiky a XACML ví, jak zkombinovat výsledky z jednotlivých politik do jednoho řešení.

4. Je to mocný nástroj - je zde mnoho cest, jak jazyk rozšířit, mnoho prostředí. Mnoho datových typů, funkcí, pravidel, atd. Jsou zde různá pravidla, jak kombinovat výsledky různých politik. Dále pracovní skupiny pracují na rozšíření a profilaci XACML do dalších standardů jako SAML a LDAP, které zvýší množství cest pro použití XACML:

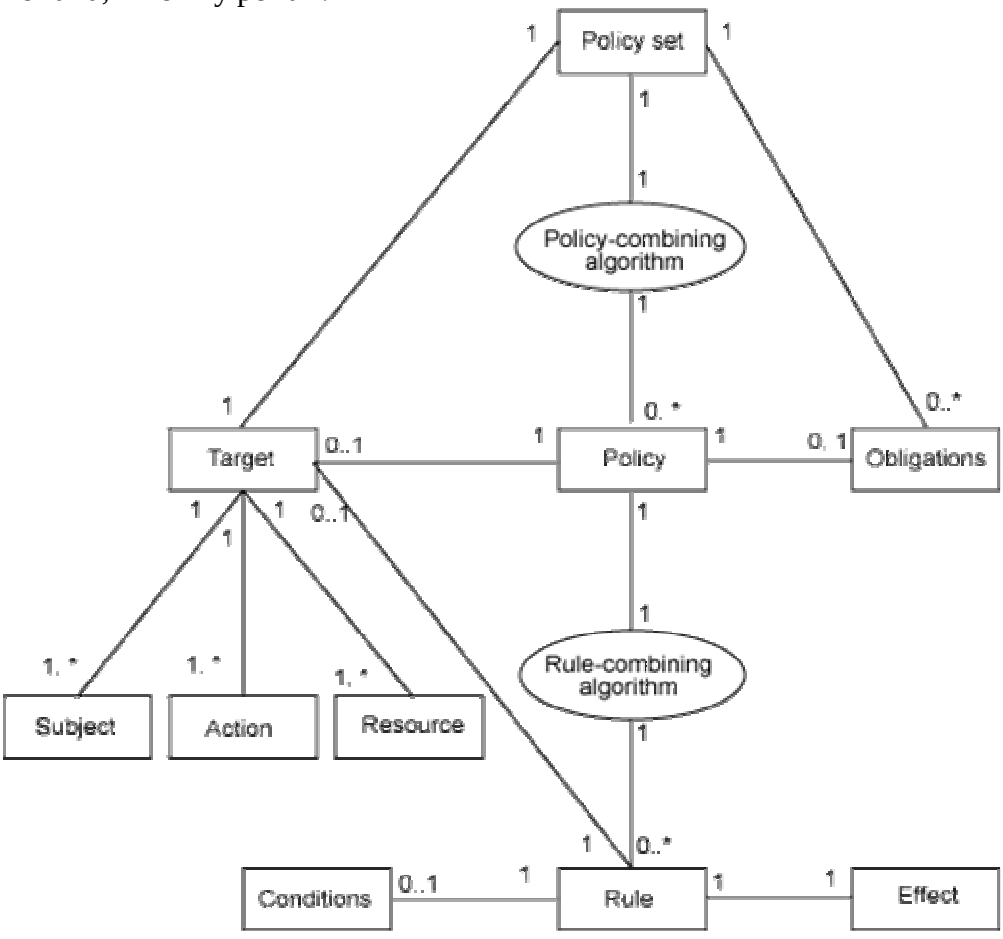
Jedna XACML politika může pokrýt mnoho zdrojů, to zabrání nekonsistentním politikám. XACML dovoluje jedné politice odkazovat na jiné, to je důležité pro velké organizace.

Dále je uvedena diskuse ohledně XACML politiky, která demonstruje standardní rysy jazyka. XACML je velmi bohatý jazyk, takže jsou ukázány pouze některé rysy. Další informace jsou ve specifikaci.

Politika a množina politik

Kořenem XACML politik je Politika (Policy) nebo Množina politik (PolicySet). Množina politik je kontejner, který může obsahovat další politiky (Policy) nebo množinu politik (PolicySet). Nebo odkazy na politiky v okolí. Politika reprezentuje jednotlivou politiku řízení přístupu, vyjádřenou pomocí množiny pravidel (set of Rules). Každý XACML dokument s politikou obsahuje právě jednu politiku nebo set politik jako „kořenový XML tag“.

Politika, množiny politik:



Protože Politika nebo Množina Politik může obsahovat násobné politiky nebo pravidla (Rules), každé z nich může vyhodnocovat různé rozhodnutí ohledně přístupu, XACML potřebuje nějakou cestu, způsob, jak uvést v soulad tato různá rozhodnutí. To je dáno pomocí Kombinačních Algoritmů (Combining Algorithms). Každý z těchto algoritmů vyjadřuje odlišnou cestu pro kombinování více rozhodnutí do jednoho. Je zde Policy Combining Algorithm - kombinační algoritmus pro množinu politik (Policy Set) - a Rule Combining Algorithm (používá ho Policy). Příkladem toho je Deny Overrides Algorithm, který říká, že bez ohledu na to, jestliže nějaké vyhodnocení vrací Deny (zakázáno) a jiné povoleno, výsledek je zakázáno. Tyto kombinační algoritmy jsou užívány k vybudování komplexní politiky, je zde 7 standardních algoritmů, ale můžeme si postavit také svoje další, pokud je potřeba.

Cíle a pravidla (Targets, Rules)

Částí, kterou potřebuje XACML PDP udělat, je najít politiku, kterou bude aplikovat na danou žádost. Aby to mohl PDP XACML udělat, poskytuje XACML další rys zvaný Target. Target je množina zjednodušených podmínek pro Subjekt (Subject), Zdroje (Resources) a akci (Action), které se musejí setkat, sjednotit, aby je PolicySet, Policy nebo Rules aplikovaly na daný dotaz. Tyto používají Boolovské funkce, aby porovnaly hodnoty nalezené v dotazu (v žádosti) s těmi, které jsou obsaženy v Targetu. Jestliže jsou všechny hodnoty Targetu splněny, potom jeho připojené (sdružené) PolicySet, Policy nebo Rules jsou aplikovány na žádost.

Navíc, aby se to dalo dobře aplikovat, Target informace také poskytuje způsob, kterak indexovat politiky, což je užitečné, jestliže máme nahromaděno mnoho politik a je třeba rychle najít tu jednu, která se aplikuje. Např. politika může obsahovat Target, který se aplikuje pouze na žádost o specifickou službu. Pokud je žádost právě na tuto službu, PDP bude vědět, kam se podívat na politiku, která se aplikuje na tuto žádost, neboť politiky jsou indexovány podle jejich Target omezení. Také ale může Target specifikovat, že se aplikuje na kterýkoliv dotaz.

Pokud je Policy nalezena a je ověřeno, že se dá aplikovat na žádost, její Rules jsou vyhodnocena. Policy může mít libovolný počet Rules, která obsahují ústřední logiku XACML politiky. Srdcem většiny Rules je Condition (Podmínka), což je boolovská funkce. Jestliže vyhodnocení Condition je True, je vrácen určitý efekt pravidla (Rule'sEffect), což je hodnota Permit nebo Deny a je spojena s vyhodnocením pravidla. Vyhodnocení Condition také může vrátit chybu (Indeterminate) nebo se může objevit, že Condition nemůže být vyhodnoceno (Not Applicable). Condition může být velmi komplexní, postaveno z vyhodnocení vnitřních vestavěných neboolovských fukcí a atributů.

Attributes, Attribute Values, Functions

Běžně se XACML zabývá atributy. Atributy jsou pojmenované hodnoty známých typů, které mohou obsahovat veřejný identifikátor nebo datum a čas. Speciálně, atributy jsou charakteristické pro subjekty (Subjects), zdroje (Resource), akce (Action) nebo pro prostředí (Environment), ve kterém je dotaz (žádost) činěn. Jméno uživatele, jeho bezpečnostní úroveň, soubor, ke kterému chce subjekt přistupovat, čas a den to jsou všechno hodnoty atributů. Když je požadavek poslán od PEP k PDP, tento požadavek je založen téměř pouze na

atributech, a potom jsou porovnány s hodnotami atributů v politice, která dělá rozhodnutí o přístupu.

Policy (politika) rozlišuje hodnoty atributů z žádosti nebo z jiných zdrojů na základě 2 mechanismů: AttributeDesignator a AttributeSelector. AttributeDesignator umožní policy, aby specifikovala atributy s daným jménem a typem a potom se PDP podívá na hodnoty v žádosti nebo někde jinde, pokud nemohou být nalezeny v žádosti. Jsou 4 druhy designatorů pro každý druh atributů v žádosti: Subject, Resource, Action, Environment. Protože atributy subjektu se mohou dělit do různých kategorií, SubjectAttributeDesignator také specifikuje kategorii. AttributeSelector dovoluje politice podívat se na hodnoty atributu pomocí dotazu XPath. Datový typ a XPath výraz jsou poskytnuty a mohou být použity na řešení hodnoty buď ve vyžadovaném dokumentu nebo někde jinde.

Jak AttributeDesignator tak AttributeSelector mohou vracet násobné hodnoty (protože jich může být více se hodících buď v žádosti nebo někde jinde), proto XACML poskytuje speciální attribut zvaný Bag. Bagy jsou neuspořádané kolekce (sbírky), které povolují duplikáty. Designátor nebo Selector vždy vrací Bag, dokonce i pokud je vrácena jenom jedna hodnota. V případě, že není učiněna žádná shoda, je vrácen prázdný bag, ačkoliv designator nebo selector mohou vrátit návěští, které hlásí chybu.

Pokud je vrácen nějaký Bag s hodnotami atributů, tak jejich hodnoty potřebují být porovnány nějakým způsobem s očekávanými hodnotami, aby mohlo být učiněno rozhodnutí. To je učiněno pomocí mocného systému funkcí. Funkce mohou pracovat s kombinacemi hodnot atributů a mohou vracet jakýkoliv druh atributu, který je systémem očekáván. Funkce také mohou být Vložené, takže máme funkce, které operují uvnitř jiných funkcí. A tato hierarchie může být dosti komplexní. Dále je možnost napsat uživatelské funkce.

Pokud budeme stavět tuto hierarchii funkcí, je nutno si uvědomit, že většina těchto funkcí pracuje na nějakém speciálním typu proměnné jako je string nebo integer, zatímco designátor a selektor vždy vracejí Bagy. Proto XACML definuje množinu standardních funkcí, které akceptují Bag určitého druhu a vracejí jednu hodnotu pokud je v Bagu právě jedna hodnota nebo mohou vracet chybu, pokud jev Bagu více hodnot nebo žádná..

Příklad politiky

Dále je příklad jednoduché politiky (Policy), která používá rysy diskutované výše. Její Target říká, že tato Policy je aplikována pouze na žádosti pro server „Simple Server“. Policy má pravidlo (Rule) s Targetem, který vyžaduje akci „Login“ a Condition, který je aplikován pouze, jestliže se Subject pokouší logovat mezi 9 ráno a 5 odpoledne. Tento příklad může být rozšířen tak, aby zahrnul další pravidla pro jiné akce. Pokud není první pravidlo aplikováno, pak je použito default Rule, které vždy vrací Deny (Rules jsou vyhodnoceny po řadě.)

```
<Policy PolicyId="SamplePolicy"
      RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:permit-
overrides">

   <!—Tato  Policy  se aplikuje pouze na zadost pro the SampleServer -->
   <Target>
```

```
    <Subjects>
      <AnySubject/>
    </Subjects>
    <Resources>
      <ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
        <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">SampleServer</AttributeValue>
        <ResourceAttributeDesignator
DataType="http://www.w3.org/2001/XMLSchema#string"
                              AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"/>
      </ResourceMatch>
    </Resources>
    <Actions>
      <AnyAction/>
    </Actions>
  </Target>
 <!—Toto Rule se podívá, zda se smí Subject prilogovat -->
  <Rule RuleId="LoginRule" Effect="Permit">
    <!—Pouiziva se toto  Rule, pokud je akce  login -->
    <Target>
      <Subjects>
        <AnySubject/>
      </Subjects>
      <Resources>
        <AnyResource/>
      </Resources>
      <Actions>
        <ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
          <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">login</AttributeValue>
          <ActionAttributeDesignator DataType="http://www.w3.org/2001/XMLSchema#string"
                              AttributeId="ServerAction"/>
        </ActionMatch>
      </Actions>
    </Target>
    <!—Dovoluje se logovani pouze mezi 9am a 5pm -->
    <Condition FunctionId="urn:oasis:names:tc:xacml:1.0:function:and">
      <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:time-greater-than-or-equal"
        <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:time-one-and-only">
          <EnvironmentAttributeSelector
DataType="http://www.w3.org/2001/XMLSchema#time"
                                AttributeId="urn:oasis:names:tc:xacml:1.0:environment:current-
time"/>

        </Apply>
        <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#time">09:00:00</AttributeValue>
      </Apply>
      <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:time-less-than-or-equal"
        <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:time-one-and-only">
```

```
          <EnvironmentAttributeSelector
DataType="http://www.w3.org/2001/XMLSchema#time"
                                AttributeId="urn:oasis:names:tc:xacml:1.0:environment:current-
time"/>
        </Apply>
        <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#time">17:00:00</AttributeValue>
       </Apply>
     </Condition>

   </Rule>
   <!—Zde se daji vlozit jina Rules pro jine akce -->

   <!-- A final, "fall-through" Rule that always Denies -->
   <Rule RuleId="FinalRule" Effect="Deny"/>

 </Policy>
```

Příklad žádosti o přístup

Předpokládejme, že universita jménem University AB (UnivAB.cz) má politiku kontroly přístupu, která kterémukoli uživateli, jehož email patří do UnivAB.cz, umožní provést jakoukoli akci nad jakýmkoli zdrojem.

Takto podobně by vypadala žádost o rozhodnutí (anglicky decision request), v níž si uživatel Dagmar Brechlerova s adresou DB@UnivAB.cz chce přečíst záznam o studentovi XY UnivAB.:

```
<Request xmlns=... >
<Subject>
<Attribute AttributeId="urn:oasis: ... :1.0:subject:subjected"
DataType="urn:oasis:names:tc:xacml:1.0:data-type:rfc822Name">
<AttributeValue>DB@UnivAB.cz </AttributeValue>
</Attribute>
</Subject>
<Resource>
<Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:resource:ufspath"
DataType="http://www.w3.org/2001/XMLSchema#anyURI">
<AttributeValue>/UnivAB /record/student/XY</AttributeValue>
</Attribute>
</Resource>
<Action>
<Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
DataType="http://www.w3.org/2001/XMLSchema#string">
<AttributeValue>read</AttributeValue>
</Attribute>
</Action>

</Request>
```

SAML

SAML umožňuje přechod autentizačních a autorizačních informací mezi zúčastněnými stranami. SAML poskytuje tzv. „prosazení“ důvěry. Takže tato aplikace může prosadit, že jde o určitého uživatele a ten má navíc určitá privilegia. SAML dokument může být digitálně podepsán pomocí XML signature. SAML poskytuje distribuci informace mezi určitou platformou a organizací a je proto jedno, kolik bodů prochází.. Např. nějaký portál autentizuje Alici a ví, že Alice má určitou roli. Portálová aplikace toto připojí do tvrzení v SOAP zprávy s dotazem na další webovou službu. Další webová služba se podívá na portálovou identitu, ověří digitální podpis portálu a povolí nebo zakáže přístup uživatele vzhledem k jeho roli.

SAML je Security Assertion Markup Language of Structured Information: tento jazyk je vyvíjen OASIS. Cílem příslušné skupiny OASIS je vyvinout standard pro **výměnu autentizačních a autorizačních informací**. Jedním slovem SAML je konstrukce, systém založený na XML pro výměnu autentizačních a autorizačních informací.

Má 3 části:

1. definuje syntaxi a sémantiku XML zpráv obsahujících tvrzení (assertion) ve formě XML.

2. definuje protokoly žádostí a odpovědí mezi žádající a vydávající stranou pro výměnu bezpečnostních informací

3. definuje pravidla pro užití tvrzení se standardy pro transport, např. definuje jak SAML tvrzení můžeme transportovat ve zprávě SOAP přes http.

Tvrzení SAMLu neprovádějí autentizaci, ale slouží k obalení, zapouzdření tohoto procesu a jeho přenosu.

Použití SAMLu – 3 scénáře

Jediné přihlášení SSO
Distribuovaná transakce
Autorizační služba

Jediné přihlášení SSO
– uživatel se přihlásí na tom.com a je autentizován. Později se chce přihlásit na joe.com. Bez užití SSO by musel své údaje zadávat znovu. Pokud je užit SAML, pak joe.com pošle požadavek na tom.com s dotazem, zda se již uživatel na tom.com autentizoval. tom.com odpoví prohlášením, že ano, uživatel je autentizován. Poté joe.com zpřístupňuje své zdroje, aniž vyžaduje znovu přihlašovací informace.

Distribuovaná transakce
Uživatel použije přihlášení k nějaké službě na www.a1.cz a poté chce jinou službu od www.b1.cz. Uživatel poté může předat informace o svém profilu na www.a1.cz serveru www.b1.cz. Ten pošle tzv. SAML tvrzení serveru www.a1.cz, ve kterém bude chtít veškeré informace, které o uživatelovi má. www.a1.cz tyto informace pošle ve formě tzv. tvrzení.

Autorizační služba

Pomocí této služby je možno zasílat tvrzení, zda je někdo k něčemu autorizován, např. k platbě, objednání atd.

SAML assertion - tvrzení

Je to XML dokument, který prostě obsahuje bezpečnostní informace. Existují celkem 3 možnosti výroků o subjektu, což může být osoba nebo program tj. zde se užívá subjekt ve smyslu bezpečnostních modelů. Assertion může obsahovat všechny tyto výroky najednou nebo nemusí.
Jsou to autentizace, attribut a autorizace.
Dále jsou jednotlivé výroky ukázány.

1. Autentizace (anglicky authentication) — autentizační výrok říká, že uvedený subjekt S byl autentizován konkrétními prostředky M v konktrétním čase T. Toto tvrzení je reprezentováno elementem <AuthenticationStatement>. Toto se používá pro umožnění SSO.

```
<saml:Assertion ...>
<saml:AuthenticationStatement
AuthenticationMethod="password"   (pomocí autentizace M- zde heslem)
AuthenticationInstant="2001-12-03T10:02:00Z">   (Čas T)
<saml:Subject>     (Subjekt  S)
<saml:NameIdentifier
SecurityDomain="sun.com"
Name="Sang" />
<saml:ConfirmationMethod>
http://...core-25/sender-vouches
</saml:ConfirmationMethod>
</saml:Subject>
</saml:AuthenticationStatement>
</saml:Assertion>
```

Tedy autentizační výrok říká, že subjekt Sang v bezpečnostní doméně sun.com byl autentizován v čase T 3. prosince 2001. Jako prostředek autentizace bylo užito jméno a heslo.

2. Atribut (Attribute) výrok. Tvrzení, že uvedený subjekt Sang je svázán s atributy A, B a tedy s odpovídajícími hodnotami a, b atd. Attribute výrok je použitelný pro distribuovanou transakci a autorizační službu.

```
<saml:Assertion ...>
<saml:AttributeStatement>
<saml:Subject>..Sang..</saml:Subject>
<saml:Attribute
AttributeName="PaidStatus"    atribut A
AttributeNamespace="http://smithco.com">
<saml:AttributeValue>  s hodnotou a
PaidUp
```

```
</saml:AttributeValue>
</saml:Attribute>
<saml:Attribute
AttributeName="CreditLimit"    atribut B
AttributeNamespace="http://smithco.com">
<saml:AttributeValue>   s hodnotou b
<my:amount currency="USD">500.00
</my:amount>
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
</saml:Assertion>
```

Subjekt Sang je spojen se 2 atributy. První má jméno Paid Status s odpovídající hodnotou paidup. Druhý má jméno Credit Limit s odpovídající hodnotou 500.0.

3. **Rozhodnutí o autorizaci (anglicky Authorization Decision)**

Žádost o povolení přístupu typu A uvedeného subjektu S k uvedeným zdrojům R byla povolena nebo zamítnuta. O tomto rozhoduje vydávající autorita. Rozhoduje o tom na základě přítomnosti evidence E žádající strany. Zdroj R může být webová služba nebo webová stránka. Toto tvrzení je reprezentováno elementem <AuthorizationDecisionStatement>:

```
<saml:Assertion ...>
<saml:AuthorizationDecisionStatement
Decision="Permit"  povolit žádost
Resource="http://jonesco.com/rpt_12345.html">  na zdroj R
<saml:Subject>... Sang ...</saml:Subject>     subjekt S je Sang
<saml:Actions
ActionNamespace="http://...core-25/rwedc"> druh přístupu A zde read
<saml:Action>Read</saml:Action>
</saml:Actions>
</saml:AuthorizationStatement>
</saml:Assertion>
```

Zde tedy zdroj je webová stránka s adresou http://jonesco.com/rpt_12345.html. Zde po obdržení SAML assertion request obsahující nějaký druh evidence E asserting strana vydá request, který indikuje, že Sang může číst tuto stránku.

Liberty Alliance Project

Byl definován skupinou korporací s cílem ochránit soukromí zákazníků a definovat standard pro federální síťovou identitu (USA) pro SSO přes sítě, domény, organizace atd. Jde tedy o to, že se dá tímto způsobem dát záruka o identitě.
Je možno se jednou přihlásit a dalším členům ve skupině se pak už uživatelé dál hlásit nemusejí. Zahrnuje SAML, XML Encryption, XML Signature. [1]

Spolupráce těchto iniciativ

Jak již bylo dříve uvedeno, SAML vyměňuje autentizační a autorizační informace, tj. jedná se o velmi důležitý druh informací, které je nutno zajistit proti cizímu zásahu případně i proti vyzrazení. Proto tvrzení SAML mohou být digitálně podepsána pomocí XML Signature a pro zajištění utajení mohou být stejná tvrzení zašifrována pomocí XML Encryption. Veřejný klíč použitý k digitálnímu podpisu a šifrování může být ověřen a registrován pomocí XKMS, neboť právě XKMS definuje důvěryhodné služby pro management kryptografických klíčů.

Strana vydávající tvrzení SAML může využít XACML k definování politiky kontroly přístupu jako základ pro manipulaci s požadavky na tvrzení SAML [5].

Alice použije XML digitální podpis a XML šifrování k podepsání a zašifrování objednávky, která má formu XML dokumentu. Tento dokument pak odešle dodavateli Bobovi, nejspíše protokolem SOAP, jehož struktura hlavičky je definována buď ve WS-Security nebo ve standardu ebXML Message Service. Příjemce dokumentu Bob může využít XKMS k vyhledání a kontrole veřejného klíče, který patří Alici. Také ale může použít jiných mechanismů. Po ověření, že klíč je důvěryhodný, Bob ověří a dešifruje objednávku.

Závěr

V oblasti XML dochází v posledních letech k významným činům na poli bezpečnosti. Některé tyto iniciativy jsou teprve na úrovni vývoje, jiné jako např. XML podpis a XML šifrování jsou již i implementovány v produktech. Dá se očekávat, že tyto nové možnosti zvýší bezpečnost webových služeb a umožní některé doposud těžko řešitelné akce jako např. selektivní podepisování záznamů o pacientech, studentech apod.

Některé z výše uvedených bezpečnostních technologií jsou teprve ve stádiu normalizace, jiné ve stadiu návrhu. Jiné jsou již i implementovány. Nejdále je zatím XML podpis, rychlý rozvoj je dále u šifrování, v poslední době 2005-2006 jsou také nové pokroky u XACML. Vzhledem k zájmu o tuto oblast je možno očekávat velmi rychlý pokrok a nasazení v nejbližší době.

Tato práce vznikla za podpory projektu 1ET200300413 AV ČR -
Informační technologie pro rozvoj kontinuální sdílené péče o zdraví.

Literatura

[1] http://xml.coverpages.org/ni2002-07-16-a.html

[2] http://www.w3.org/Signature/

[3] http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml

[4] http://www-106.ibm.com/developerworks/xml/library/x-xmlsecuritysuite/index.html

[5] http://www.w3.org/TR/xmlenc-core/

[6] http://www-106.ibm.com/developerworks/xml/library/x-seclay1/

C. Přehled dokumentů ETSI v oblasti elektronického podpisu, časových razítek a kvalifikovaných certifikátů Shrnutí roku 2006 a začátek roku 2007

Připravil Vladimír Sudzina, Ministerstvo informatiky ČR, (vladimir.sudzina@micr.cz)

Na stránkách ETSI - Evropský institut pro normalizaci v telekomunikacích (European Telecommunications Standards Institute) byly zveřejněny v roce 2006 a začátkem letošního roku nové verze technických specifikací a technických zpráv. V závorce u jednotlivých dokumentů jsou data, kdy byl daný dokument publikován, případně v jaké fázi se momentálně nachází.

Informace jsou určené především pro poskytovatele certifikačních služeb a další odborníky v oblasti certifikačních autorit.

Technické specifikace (TS):

ETSI TS 102 904 V1.1.1 (2007-01-12) Electronic Signatures and Infrastructures; Profiling for Electronic Signatures based on ETSI TS 101 903

ETSI TS 101 734 V1.1.1 (2007-01-12) Electronic Signatures and Infrastructures; Profiling for Electronic Signatures based on ETSI TS 101 733

ETSI TS 102 231 V2.1.1 (2006-03-10) Electronic Signatures and Infrastructures (ESI); Provision of harmonized Trust-service status information

ETSI TS 102 176-1 V1.3.1 (Drafting stage, TB adoption of WI 2006-09-01)

Electronic Signatures and Infrastructures (ESI) Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms

ETSI TS 102 176-2 V1.3.1 (Drafting stage, TB adoption of WI 2006-09-01)

Electronic Signatures and Infrastructures (ESI) Algorithms and Parameters for Secure Electronic Signatures; Part 2: Secure channel protocols and algorithms for signature creation devices

ETSI TS 102 042 V1.2.3 (2006-12-08) Electronic Signatures and Infrastructures (ESI) Policy requirements for certification authorities issuing public key certificates

ETSI TS 101 903 V1.3.2 (2006-03-07) XML Advanced Electronic Signatures (XAdES)

ETSI TS 101 862 V1.3.3 (2006-01-06) Qualified Certificate profile

ETSI TS 101 861 V1.3.1 (2006-01-27) Time stamping profile

ETSI TS 101 733 V1.7.3 (2007-01-11) Electronic Signatures and Infrastructures (ESI) CMS Advanced Electronic Signatures (CAdES)

ETSI TS 101 456 V1.4.2 (2006-12-14) Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates

ETSI TS 101 456 V1.4.1 (2006-02-02) Electronic Signatures and Infrastructures (ESI) Policy requirements for certification authorities issuing qualified certificates

Technické zprávy (TR):

ETSI TR 102 458 V1.1.1 (2006-04-20) Electronic Signatures and Infrastructures (ESI); Mapping Comparison Matrix between the US Federal Bridge CA Certifcate Policy and the European Qualified Certificate Policy (TS 101 456)

ETSI TR 102 438 V1.1.1 (2006-03-06) Electronic Signatures and Infrastructures (ESI); Application of Electronic Signature Standards in Europe

ETSI TR 102 437 V1.1.1 (2006-10-03) Electronic Signatures and Infrastructures (ESI); Guidance on TS 101 456 (Policy requirements for certification authorities issuing qualified certificates)

Pro vyhledávání dokumentů a zjišťování stavu rozpracovanosti jednotlivých dokumentů je možné používat např. adresu

http://webapp.etsi.org/WorkProgram/SimpleSearch/QueryForm.asp ,

případně pro vyhledávání podle klíčových slov využít odkaz

http://pda.etsi.org/pda/queryform.asp .

ETSI (sídlo v Sophia Antipolis, Francie, založen v roce 1988) je neziskovou organizací, jejímž posláním je vypracovávat normy ETSI EN (telekomunikační řady), normy ETSI ES (normy nižší úrovně), technické specifikace (ETSI TS), technické zprávy (ETSI TR), zvláštní zprávy (ETSI SR), technické základy pro předpisy (ETSI TBR), dřívější telekomunikační normy (ETSI-ETS) a předběžné telekomunikační normy (ETSI I-ETS), technické zprávy ETSI (ETSI-ETR) a pokyny ETSI (ETSI EG) v oblasti telekomunikací a elektronických komunikací.

D. O čem jsme psali v únoru 2000 – 2006

Crypto-World 2/2000

Crypto-World 2/2001

Crypto-World 2/2002

Příloha: Program pro naše čtenáře : "Hašák ver. 0.9" (viz. letem šifrovým světem) hasak.

Crypto-World 2/2003

Crypto-World 2/2004

Crypto-World 2/2005

Crypto-World 2/2006

E. Závěrečné informace

1. Sešit

Crypto-World je oficiální informační sešit "Kryptologické sekce Jednoty českých matematiků a fyziků" (GCUCMP). Obsahuje články podepsané autory. Případné chyby a nepřesnosti jsou dílem P.Vondrušky a autorů jednotlivých podepsaných článků, GCUCMP za ně nemá odbornou ani jinou zodpovědnost.
Adresa URL, na níž můžete najít tento sešit (zpravidla 3 týdny po jeho rozeslání) a předchozí sešity GCUCMP, denně aktualizované novinky z kryptologie a informační bezpečnosti, normy, standardy, stránky některých členů a další související materiály:
http://crypto-world.info

2. Registrace / zrušení registrace

Zájemci o e-zin se mohou zaregistrovat pomocí e-mailu na adrese pavel.vondruska@crypto-world.info (předmět: Crypto-World) nebo použít k odeslání žádosti o registraci elektronický formulář na http://crypto-world.info. Při registraci vyžadujeme pouze jméno a příjmení, titul, pracoviště (není podmínkou) a e-mail adresu určenou k zasílání kódů ke stažení sešitu.
Ke zrušení registrace stačí zaslat krátkou zprávu na e-mail pavel.vondruska@crypto-world.info (předmět: ruším odběr Crypto-Worldu!) nebo opět použít formulář na http://crypto-world.info. Ve zprávě prosím uveďte jméno a příjmení a e-mail adresu, na kterou byly kódy zasílány.

3. Redakce

E-zin Crypto-World

Redakční práce:	Pavel Vondruška
Stálí přispěvatelé:	Pavel Vondruška
	Jaroslav Pinkava
Jazyková úprava:	Jakub Vrána
Přehled autorů:	http://crypto-world.info/obsah/autori.pdf
NEWS	Vlastimil Klíma
(výběr příspěvků,	Jaroslav Pinkava
komentáře a	Tomáš Rosa
vkládání na web)	Pavel Vondruška
Webmaster	Pavel Vondruška, jr.

4. Spojení (abecedně)

redakce e-zinu	ezin@crypto-world.info ,	http://crypto-world.info
Vlastimil Klíma	v.klima@volny.cz ,	http://cryptography.hyperlink.cz/
Jaroslav Pinkava	Jaroslav.Pinkava@zoner.cz ,	http://crypto-world.info/pinkava/
Tomáš Rosa	t_rosa@volny.cz ,	http://crypto.hyperlink.cz/
Pavel Vondruška	pavel.vondruska@crypto-world.info ,	http://crypto-world.info/vondruska/index.php
Pavel Vondruška,jr.	pavel@crypto-world.info ,	http://webdesign.crypto-world.info
Jakub Vrána	jakub@vrana.cz ,	http://www.vrana.cz/