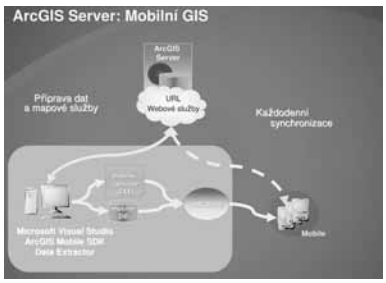
Jitka Jiravová

ArcGIS Mobile

ArcGIS Mobile umožňuje vývojářům vytvářet jednoduché a výkonné GIS aplikace pro mobilní klienty. Mobilní aplikace ArcGIS Serveru přispívají ke zvýšení produktivity a informovanosti pracovníků v terénu.

ArcGIS Mobile tvoří „software developer kit“ (SDK), který se instaluje spolu s ArcGIS Serverem. Pomocí SDK mohou vývojáři vytvářet geocentrické aplikace, které poskytují základní funkcionalitu GIS včetně zobrazení a navigace v mapě, podpory GPS nebo editace geografických dat. ArcGIS Mobile SDK se používá i pro rozšíření původně negeografických aplikací (např. CRM nebo systémy pro automatizaci prací v terénu) o možnosti GIS.



Pomocí ArcGIS Mobile můžete

- s využitím jednoduchých vývojářských nástrojů vytvářet mobilní aplikace šité na míru uživatelům,
- využívat data z geodatabáze při různých úrovních konektivity na internet,
- nasazovat aplikace na mobilních zařízeních (smartphone, Pocket PC, Tablet PC atd.).

Více informací o ArcGIS Mobile najdete na adrese **http://www.esri.com/software/arcgis/arcgismobile/.**

Ing. Jitka Jiravová, ARCDATA PRAHA, s.r.o.

David Ondřich

ArcIMS a bezpečnost

Část třetí

Ve třetím dílu našeho seriálu o zabezpečení ArcIMS se zaměříme na řízení přístupu k jednotlivým datovým zdrojům a také si povíme něco o možnostech správy uživatelů. Seriál totiž v průběhu vzniku poněkud nabobtnal, a proto jsem se rozhodl, že jej oproti původnímu plánu rozšířím minimálně ještě o jeden díl, který celý věnujeme možným útokům na ArcIMS a bezpečnosti dat.

V minulém dílu jsme rozebrali možnosti, které vícevrstvá architektura ArcIMS poskytuje pro rozdělení jednotlivých komponent v rámci DMZ (demilitarizované zóny) a vnitřní sítě. Připomeňme, že neexistuje obecně vhodné „bezpečné“ uspořádání, vždy záleží na konkrétní situaci, nicméně pro většinu obvyklých případů lze za nejvhodnější schéma pokládat uspořádání s transparentním proxy serverem v DMZ a kompletním ArcIMS ve vnitřní síti (zejména slouží-li jako datový zdroj geodatabáze, kterou není vhodné exponovat v otevřené síti). Také jsme v minulé části probrali komunikační protokoly a porty, na kterých jednotlivé komponenty ArcIMS komunikují.

Základní možnosti řízení přístupu

Řízením přístupu se pro potřeby tohoto seriálu rozumí jakýkoliv způsob určování dostupných prostředků, které mají mít jednotliví uživatelé systému k dispozici. Řízení přístupu proto zahrnuje jak samotné rozdělování uživatelů (je-li jaké), tak přidělování

jednotlivých služeb nebo prostředků, které mají mít k dispozici.

Často se používá dvojice termínů autentizace a autorizace, která se často plete a kterou řada lidí používá, aniž by přesně vymezili, co se kterým termínem myslí. Pokud v tomto seriálu použiji termín autentizace, pak mám na mysli ověření identity toho kterého uživatele. Pro ověření identity lze obecně použít nejrůznější metody, od nejobvyklejšího uživatelského jména a hesla přes použití ověřovacího klíče (karty) až po stále více používané biometrické metody (otisk prstu nebo celé ruky, snímek sítnice oka). Pod termínem autorizace rozumím ověření práva daného uživatele použít požadovaný prostředek, tedy např. přidělení práva použít danou službu ArcIMS. Autorizace předpokládá, že aplikace (server, systém) zná uživatelovu identitu a již o ní nepochybuje (neověřuje ji), pouze zjišťuje, zda má uživatel právo použít daný zdroj (službu, aplikaci, rozhraní). U jednodušších aplikací je obvykle autentizace s autorizací spojena do jednoho kroku, kdy se přihlášením do aplikace (ověření identity) automaticky předpokládá, že uživatel má právo danou aplikaci použít (ověření práv).

Samotný ArcIMS nabízí několik jednoduchých možností, jak řízení přístupu zajistit. Další (podrobnější) možnosti se dají zajistit buď použitím speciálních nástrojů mimo ArcIMS, nebo prostřednictvím vlastních doplňků (které je třeba naprogramovat). Pojďme se podívat na základní možnosti, které ArcIMS poskytuje. Jádrem tohoto připraveného řízení přístupu je tzv. základní HTTP autentizace, která je definovaná pro HTTP protokol a je dostupná ve většině používaných webových prohlížečů.

ACL soubor

Zkratka ACL představuje *Access Control List*, což je obvyklý termín pro soubor pravidel, kterými se má řídit program nebo operační systém při řízení přístupu (např. podrobnější přidělování práv v souborovém systému v operačním systému). Tento soubor má v případě ArcIMS podobu konfiguračního souboru ve formátu XML, který není nepodobný kontrolním souborům AXL. Rozdíl mezi AXL a ACL soubory je především v tom, že AXL soubory používá aplikační server ArcIMS, zatímco přístupový ACL soubor je určen pro servlet konektor, který přidělování práv k jednotlivým službám hlídá.

Abychom si o ACL souboru učinili představu, podíváme se na vlastnosti, které je možné jeho prostřednictvím nastavit (bude se nám to totiž hodit i v příští části, neboť servlet konektor prostřednictvím tohoto konfiguračního souboru umožňuje ovládat i vlastnosti poskytovaných služeb). Soubor by se měl jmenovat **`aimsacl.xml`** a musí se nacházet v takovém místě ve filesystému, kde se k němu dostane servlet kontejner. Obvykle se tento soubor dává do stejného adresáře, ve kterém se nachází konfigurační soubor **`Esrimap_prop`**; v souboru **`Esrimap_prop`** se také nastavuje použití ACL souboru, konkrétně povolením **`authenticate=True`** a nastavením **`aclFileName=$CESTA/aimsacl.xml`**. Soubor má kořenový element **`AIMSACL`**, který může obsahovat jedině dceřiné elementy **`USER`** (na velikosti písmen záleží).

Každý výskyt elementu **`USER`** v souboru představuje jedno pravidlo, kterým se servlet konektor bude při zpracování požadavků řídit. Vlastnosti pravidel se nastavují pomocí atributů (vlastností) elementu **`USER`**, přičemž těchto atributů může být osm:

- **`name`** – uživatelské přihlašovací jméno,
- **`password`** – uživatelské heslo,
- **`services`** – seznam služeb, které uživatel smí použít,
- **`roles`** – seznam rolí, které uživatel zastává pro Metadata Server,
- **`active`** – příznak, zda je uživatel aktivní,
- **`expiration`** – datum a čas, kdy uživatelský účet vyprší,
- **`forbiddentags`** – seznam zakázaných elementů v ArcXML,
- **`trustedclients`** – seznam povolených klientských IP adres.

V jednotlivých atributech je možné použít „hvězdičkovou konvenci“, tzn. např. je možné určit, že k některé službě mají mít přístup všichni uživatelé pomocí nastavení **`name="*"`** nebo některý z uživatelů (superuživatel) má mít přístup ke všem službám (**`services="*"`**). Atribut **`password`** je povinný, pokud pravidlo neobsahuje **`name="*"`**, atributy **`name`** a **`services`** jsou povinné vždy.

Ostatní atributy jsou volitelné a jejich prostřednictvím je možné nastavit další vlastnosti účtu: atributem **`active`** se nastavuje platnost, jakékoli kladné číslo představuje příznak, že účet je aktivní, 0 znamená, že uživatel je neaktivní a nemůže se přihlásit. Atributy **`services`**, **`roles`**, **`forbiddentags`** a **`trustedclients`** mohou obsahovat seznamy, kde se jako oddělovač jednotlivých položek používá čárka (**`,`**). Atribut **`roles`** obsahuje přidělení rolí potřebných pro použití (a hlavně administrování) ArcIMS Metadata Serveru (kterým se zde dále nebudeme zabývat). Atributem **`expiration`** je možné nastavit okamžik vypršení uživatelského účtu, např. při publikování služby s časově omezenou platností. Atributem **`forbiddentags`** se budeme podrobně zabývat v příštím pokračování seriálu, zde uvedu pouze konstatování, že se jedná o jakýsi filtr, který blokuje výskyt některých elementů („tagů“) v ArcXML komunikaci mezi klientem a serverem. Poslední atribut, **`trustedclients`**, umožňuje přidělit jednotlivým účtům seznam povolených IP adres, ze kterých je možné se připojit. V tomto atributu není možné použít hvězdičkovou konvenci, ale je možné pomocí znaku pomlčka (–) přiřadit rozsah adres, ze kterých se lze připojit.

ACL soubor umožňuje tedy poměrně jednoduše nastavit širokou škálu jednotlivých pravidel – ať už pro jednotlivé uživatele, nebo pro jednotlivé služby. Přesto má tento soubor několik nedostatků, které se v některých situacích mohou jevit jako zásadní. Především je to skutečnost, že je nutné restartovat servlet kontejner (typicky Tomcat), pokud se mají promítnout změny provedené v ACL souboru (servlet konektor čte tento soubor pouze při nastartování). To nemusí vadit, pokud se soubor nemění příliš často. Je samozřejmě možné vynutit restart servlet kontejneru i programově, ale obvykle to vyžaduje práva administrátora systému (nebo účtu, pod kterým kontejner běží). Druhým vážným nedostatkem je skutečnost, že uživatelská hesla jsou uložena v obyčejné textové podobě přímo v souboru, který při výchozí instalaci ArcIMS může číst kterýkoliv uživatel v systému. To lze částečně omezit nastavením příslušných přístupových práv daného souboru, ale na skutečnosti, že hesla jsou uložena v nijak nezašifrované podobě, to nic nemění. Třetím nedostatkem je fakt, že atribut **`trustedclients`** umožňuje nastavit pouze IP adresy klientských počítačů a nikoliv doménová jména, tento přístup se tedy nedá použít pro sítě s dynamicky přidělovanými adresami (pokud je potřeba omezit přístup jen na některé klientské počítače a ne na celý segment sítě). Tyto nedostatky se dají částečně omezit využitím druhého podporovaného způsobu řízení přístupu, který se ACL souboru velmi podobá – ACL databáze.

Pro úplnost informací o ACL souboru dodávám, že na webových stránkách ESRI (**http://support.esri.com/**) je možné stáhnout jednoduchou aplikaci pro editaci ACL souboru, která se jmenuje *ArcIMS Service ACL Editor* a je k dispozici pro operační systémy typu UNIX i Microsoft Windows.

ACL databáze

V podstatě stejně jako v případě ACL souboru je možné nastavit přístupová práva pomocí dvou tabulek v databázi, ke které je možné se připojit pomocí protokolu JDBC (*Java DataBase Connection*). Ovladače pro tento způsob připojení jsou k dispozici pro drtivou většinu existujících relačních databází.

V databázi je třeba připravit dvě tabulky: první z nich, které se říká uživatelská, musí obsahovat alespoň tři sloupce pro určení uživatelské identity; druhá, která se nazývá tabulka práv, definuje jednotlivá pravidla pro daného uživatele. Tabulky se mohou jmenovat libovolně (je tedy možné použít/upravit již existující tabulky s uživatelskými účty, pokud nějaké takové existují), nicméně pro názvy jejich sloupců je třeba dodržet daná pravidla. Uživatelská tabulka, nazvu ji např. **`ims_users`**, musí obsahovat alespoň tři sloupce:

- **`userid`** – identifikátor uživatele, typ VARCHAR(32),
- **`username`** – login uživatele, typ VARCHAR(64),
- **`password`** – heslo, typ VARCHAR(64).

Sloupeček s identifikátorem se ve skutečnosti může jmenovat libovolně, přesto doporučuji toto označení, které je jednoznačné. Datové typy jednotlivých sloupců mohou být analogické v dané RDBMS (např. VARCHAR2, TEXT apod.). Pro uživatelské jméno je možné použít hvězdičkovou konvenci, tj. je možné vytvořit záznam s **`username`** nastaveným na **`*`**, pak může sloupeček **`password`** zůstat prázdný (v ostatních případech jsou všechny tři sloupce povinné).
Tabulka práv, nechť se jmenuje např. **`ims_privileges`**, musí obsahovat alespoň tyto sloupce:

- **`userid`** – identifikátor uživatele, typ VARCHAR(32),
- **`service`** – název služby, typ VARCHAR(64),
- **`active`** – příznak aktivního účtu, typ INTEGER,
- **`roles`** – seznam rolí pro Metadata Server, typ VARCHAR(1024),
- **`expiration`** – datum vypršení účtu, typ DATE,
- **`tclients`** – seznam povolených klientských IP adres, typ VARCHAR(1024),
- **`ftags`** – seznam zakázaných ArcXML elementů, typ VARCHAR(1024).

Pro sloupeček s identifikátorem platí, že se musí jmenovat stejně jako v tabulce uživatelů. Pro datové typy opět platí výše zmíněné. Ostatní sloupce jsou analogické jednotlivým atributům v ACL souboru s tím rozdílem, že pro přiřazení jednotlivých služeb jednomu uživateli je třeba použít více záznamů v tabulce práv (tj. sloupec **`service`** může obsahovat pouze název jedné služby). Sloupečky **`roles`**, **`tclients`** a **`ftags`** mohou opět obsahovat seznamy rolí, resp. klientských IP adres a zakázaných elementů v ArcXML. Povinné sloupce jsou **`userid`**, **`service`** a **`active`**.

Nastavení jednotlivých práv se provádí vytvořením odpovídajících záznamů v obou tabulkách tak, aby byly svázány přes (jednoznačný) identifikátor uživatele. Na tabulky je možné klást některá databázová omezení, např. právě jednoznačnost **`userid`** nebo jeho použití jako FOREIGN KEY v tabulce práv. Naplnění tabulek je třeba provést externí aplikací nebo prostředky samotné databáze (např. řádkového klienta).

Aby vše fungovalo, je třeba ještě správným způsobem nastavit konfigurační soubor **`Esrimap_prop`**. Stejně jako v případě ACL souboru je třeba povolit použití autentizace pomocí **`authenticate=True`**, namísto **`aclFileName`** ovšem nastavíme **`useJdbc=True`** a podle konfigurace navíc nadefinujeme následující proměnné:

- **`jdbcDriver`** – JDBC ovladač pro připojení k databázi, např. **`oracle.jdbc.driver.OracleDriver`**,
- **`jdbcUrl`** – připojovací řetězec k databázi, např. **`jdbc:oracle:thin:@database.organizace.cz:1521:schéma`**,
- **`jdbcUser`** – DB účet pro připojení,
- **`jdbcPassword`** – heslo DB účtu,
- **`jdbcUserTable`** – jméno uživatelské tabulky, v našem příkladu **`ims_users`**,
- **`jdbcPermTable`** – jméno tabulky práv, v našem příkladu **`ims_privileges`**,

- **jdbcUidColumn** – název sloupečku s identifikátorem uživatele, v našem příkladu **userid**.

Použití ACL tabulek zmenšuje hlavní nevýhody souborového seznamu omezení, i když některé zcela neodstraňuje. Servlet kontejner není třeba restartovat po každé změně seznamu oprávnění (je to ovšem nutné, pokud se změní schéma tabulek). Hesla se uchovávají v obyčejném textu, ale velmi snadno lze omezit přístup k příslušné tabulce. Obsah tabulek v databázi je možné měnit nezávisle na samotném ArcIMS, je tedy možné navrhnout i takový systém, který bude pravidelně hlídat aktuální IP adresy klientských počítačů a nastavovat je v příslušných pravidlech v tabulce práv. Naopak nevýhodou tabulkového seznamu pravidel je poněkud složitější konfigurace a nutnost JDBC propojení mezi servlet kontejnerem a databází s tabulkami (což může představovat bezpečnostní riziko, např. vzhledem k umístění jednotlivých vrstev ArcIMS).

Pokročilé techniky řízení přístupu

Ostatní techniky, které umožňují nějakým způsobem řídit přístup k ArcIMS a jeho službám, mají společné to, že k jejich realizaci je zpravidla nutné nějaké programování s výjimkou velmi speciální techniky (která se ale nepoužívá příliš často). Tato technika se jmenuje *aliasing* (přejmenování) servlet konektoru a je vhodné ji použít tam, kde nevadí, že se k ArcIMS nepřipojí žádný klient typu ArcGIS Desktop (nebo je to přímo žádoucí).

Po instalaci servlet konektoru je tento konektor dostupný na adrese, která končí řetězcem **/servlet/com.esri.esrimap.Esrimap** a kterou očekává většina standardních klientů ArcIMS. Tuto adresu je velmi snadné změnit, a to dokonce několika způsoby. Jednak je to možné nastavením tzv. *servlet mappingu* v souboru **web.xml** v adresáři **$TOMCAT/webapps/servlet/WEB-INF** – prostým nastavením klíče **url-pattern** na jinou hodnotu, než je výchozí **/com.esri.esrimap.Esrimap**. Druhou snadnou metodou je prosté přejmenování adresáře **servlet** (nebo deployment servlet konektoru pod jiným názvem). Dalším způsobem je nastavení servlet kontejneru v hlavním konfiguračním souboru **web.xml**. Dejme tomu, že chceme z nějakého důvodu přejmenovat výchozí servlet konektor např. na **/aplikace/muj.konektor**. Přejmenujeme (pro testovací účely raději zkopírujeme) adresář **servlet** na **aplikace** a v souboru **$TOMCAT/webapps/aplikace/WEB-INF/web.xml** nastavíme v elementu **servlet-mapping** vlastnost **url-pattern** na **/muj.konektor**. Po restartu servlet kontejneru bude konektor dostupný na požadované adrese. ArcIMS Administratorem se k němu dokážeme připojit zadáním plné adresy (tedy včetně nového názvu konektoru) do políčka *ArcIMS Site URL* v dialogu *Open Site*. HTML klient se k našemu konektoru připojí, pokud do konfiguračního souboru **ArcIMSparam.js** do proměnné **esriBlurb** zadáme nový řetězec namísto původního. Tímto způsobem je také možné vytvořit kopii servlet konektoru (nebo více kopií), která je dostupná na nestandardní adrese, a přesměrováním různých klientů řídit přístup k jednotlivým službám ArcIMS.

Ostatní způsoby, jak řídit přístup k jednotlivým službám ArcIMS, je nutné připravit programově nebo prostřednictvím jiných prostředků než samotného ArcIMS (např. pokud je k zabezpečení ArcIMS použit transparentní proxy server, je možné nakonfigurovat jej tak, aby zároveň sloužil jako autentizační brána; stejnou funkčnost poskytují některé typy firewallů). Tyto programové techniky sice vyžadují hlubší pochopení principů autentizace prostřednictvím webových technologií, na druhou stranu umožňují daleko jemnější nastavení požadovaných vlastností nebo přizpůsobení řízení přístupu existujícím systémům (např. systém jednotného přihlášení v rámci organizace, tzv. *single-sign-on*, nebo použití ověřovacích protokolů LDAP či Kerberos). Tyto způsoby používají buď knihoven ostatních konektorů ArcIMS (Java, .NET, ColdFusion, ActiveX) nebo nějakým prostřednictvím pracují s technologií servletů (tzv. servletové filtry).

Pokračování

V příštím dílu se podíváme na slibovaná kouzla pomocí zakázaných elementů jazyka ArcXML a také se konečně dostane na dlouho slibované útoky proti ArcIMS a způsoby, jak se jim bránit. Protože už je víc než jasné, že původně zamýšlený rozsah seriálu se zvětší, budu jen rád za informace, co byste ještě chtěli o bezpečnosti v souvislosti s ArcIMS vědět.

Mgr. David Ondřich, ARCDATA PRAHA, s.r.o. Kontakt: dond@arcdata.cz