VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
FACULTY OF INFORMATION TECHNOLOGY

ÚSTAV INTELIGENTNÍCH SYSTÉMŮ
DEPARTMENT OF INTELLIGENT SYSTEMS

NÁSTROJ PRO OCHRANU VÝKRESŮ AUTOCAD

TOOL FOR AUTOCAD SKETCHES PROTECTION

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE — **ADAM SMEJKAL**
AUTHOR

VEDOUCÍ PRÁCE — **Ing. DANIEL OVŠONKA**
SUPERVISOR

BRNO 2017

Zadání bakalářské práce/20165/2016/xsmejk19

Vysoké učení technické v Brně - Fakulta informačních technologií

Ústav inteligentních systémů Akademický rok 2016/2017

Zadání bakalářské práce

Řešitel: **Smejkal Adam**
Obor: Informační technologie
Téma: **Nástroj pro ochranu výkresů AutoCAD**
Tool for AutoCAD Sketches Protection
Kategorie: Bezpečnost

Pokyny:

1. Prostudujte a analyzujte princip ochrany citlivých dat s využitím systému pro řízení informací (Information Rights Management - IRM) ve firemním prostředí.
2. Prostudujte možnosti šifrování, bezpečného zobrazení dat a omezení uživatelských akcí (ochrana konstrukčních dat) z programu AutoCAD 2016.
3. Navrhněte a implementujte řešení IRM pro AutoCAD 2016 zaměřené na soubory v nativním formátu.
4. Řešení otestujte na poskytnutém testovacím vzorku dat od vedoucího.
5. Zhodnoťte řešení a diskutujte možnosti dalšího rozšíření.

Literatura:

- Liu, Simon, and Rick Kuhn. Data loss prevention. IT professional 12.2 (2010): 10-13.
- Al-Fedaghi, Sabah. A conceptual foundation for data loss prevention. System 16 (2011): 17.
- Dle doporučení vedoucího

Podrobné závazné pokyny pro vypracování bakalářské práce naleznete na adrese http://www.fit.vutbr.cz/info/szz/

Technická zpráva bakalářské práce musí obsahovat formulaci cíle, charakteristiku současného stavu, teoretická a odborná východiska řešených problémů a specifikaci etap (20 až 30% celkového rozsahu technické zprávy).

Student odevzdá v jednom výtisku technickou zprávu a v elektronické podobě zdrojový text technické zprávy, úplnou programovou dokumentaci a zdrojové texty programů. Informace v elektronické podobě budou uloženy na standardním nepřepisovatelném paměťovém médiu (CD-R, DVD-R, apod.), které bude vloženo do písemné zprávy tak, aby nemohlo dojít k jeho ztrátě při běžné manipulaci.

Vedoucí: **Ovšonka Daniel, Ing.**, UITS FIT VUT
Datum zadání: 1. listopadu 2016
Datum odevzdání: 17. května 2017

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
Fakulta informačních technologií
Ústav inteligentních systémů
612 66 Brno, Božetěchova 2

L.S.

doc. Dr. Ing. Petr Hanáček
vedoucí ústavu

Abstrakt

Cílem práce je vytvořit nástroj, který umožní chránit citlivá data výkresů tvořených v programu AutoCAD 2016 pomocí principů využívaných systémy pro správu přístupových práv k informacím, známých pod zkratkou IRM. Zabývá se studiem problematiky ochrany citlivých dat z širšího hlediska, principem fungování systémů IRM a analýzou vhodných metod pro rozšíření programu AutoCAD za účelem jeho zasazení do systému IRM v roli klientské aplikace.

Abstract

The main goal of this thesis is to develop a tool that helps to protect sensitive data in drawings created by AutoCAD 2016 using methods employed by information rights management systems (IRM). It studies general principles of data leak prevention, closely describes IRM systems and analyzes suitable methods to extend the functionality of AutoCAD with a goal of integrating it into an IRM system as a client application.

Klíčová slova

Prevence úniku citlivých dat, DLP, AutoCAD, správa přístupových práv k informacím, IRM, AD RMS

Keywords

Data leak prevention, DLP, AutoCAD, information rights management, IRM, AD RMS

Citace

SMEJKAL, Adam. *Nástroj pro ochranu výkresů AutoCAD.* Brno, 2017. Bakalářská práce. Vysoké učení technické v Brně, Fakulta informačních technologií. Vedoucí práce Ing. Daniel Ovšonka

Nástroj pro ochranu výkresů AutoCAD

Prohlášení

Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně pod vedením pana Ing. Daniela Ovšonky. Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

.....
Adam Smejkal
16. května 2017

Poděkování

Velmi rád bych poděkoval vedoucímu práce panu Ing. Danielu Ovšonkovi za jeho vstřícný přístup a cenné rady poskytnuté při řešení této práce.

Obsah

Kapitola 1

Úvod

S rostoucí mírou využití výpočetní techniky v rámci běžných firemních postupů se čím dál více ztěžuje zachování obchodních tajemství a vytrácí se kontrola firem nad pohybem citlivých údajů. V posledních letech se stále častěji objevují incidenty, kdy ztrátou velkého množství citlivých dat došlo k výraznému poškození dotčených organizací a v mnoha případech i osob, které do nich vložily svou důvěru. Tyto incidenty zdaleka nejsou způsobeny jen vnějšími narušiteli, naopak ve velké části případů nesou zodpovědnost právě ony organizace a jejich zaměstnanci.

Nutnost řešit tento problém dala za vznik odvětví zaměřenému na ochranu těchto údajů proti úniku či zneužití. Vzhledem k tomu, že většina informací je dnes tvořena a přenášena v elektronické podobě, je jeho pozornost zaměřena především na vývoj softwarových řešení a metod na ochranu dat v této podobě.

Tato práce navazuje na výše zmíněný trend a zaměřuje se na vývoj nástroje, který má za úkol chránit a ovládat přístup k citlivým dokumentům konstrukčních firem.

Pro vývoj efektivního řešení je vhodné si uvědomit, která data jsou považována za citlivá, odkud pochází motivace firem tyto data chránit, jaký je původ a charakter incidentů spojených s jejich únikem a jaké metody jsou pro jejich ochranu využívány. Této oblasti studia je věnována kapitola 2. Je zde vysvětlen pojem citlivých dat a ilustrována důležitost jejich ochrany jak z právního, tak finančního i morálního hlediska. Dále se kapitola zabývá studií incidentů spojených s únikem citlivých dat a obsahuje přehled známých přístupů k prevenci jejich výskytu.

Kapitola 3 je věnována studii systémů pro správu přístupových práv k informacím, známých pod zkratkou IRM (z anglického *Information Rights Management*). Těmto systémům je vyhrazena samostatná kapitola, jelikož využití jejich principů pro ochranu citlivých výkresů je hlavním předmětem této práce. V této kapitole lze nalézt obecnou charakteristiku technologií využívaných ke správě přístupových práv k informacím a je zde popsán princip, na jehož základě jsou data v těchto systémech běžně chráněna. Zvláštní pozornost je věnována jedné ze známých implementací systému IRM, tzv. Microsoft Active Directory Rights Management Services.

Analýza možností pro využití systémů IRM na ochranu dat konstrukčních firem je hlavním předmětem kapitoly 4. Analýza je zaměřena na program AutoCAD 2016, který je jedním z nejpoužívanějších programů v tomto odvětví. Dle poznatků z předchozích kapitol jsou zde určeny vlastnosti, o které je nutné program AutoCAD rozšířit pro jeho zasazení do systému IRM. Možnostem a úskalím implementace těchto rozšíření je věnován zbytek kapitoly.

Účelem kapitoly 5 je popsat a vysvětlit rozhodnutí učiněná při návrhu a implementaci nástroje. Jsou zde specifikovány případy užití a nastíněn způsob práce s navrženým systémem. Následuje přehled architektury výsledného systému, popis způsobu implementace jednotlivých komponent a zdůvodnění výběru použitých technologií a metod.

Kapitola 6 je věnována ověření, zda vytvořený nástroj splňuje kritéria definovaná při specifikaci požadavků a zda dostatečně pokrývá všechny navržené případy užití.

Závěrečná kapitola obsahuje shrnutí a zhodnocení výsledků práce a náměty pro budoucí rozšíření implementovaného systému.

Kapitola 2

Ochrana citlivých dat

Bezpečnostní standard SEC-501 pojem citlivá data definuje jako jakákoliv data, jejichž kompromitace porušením utajení, integrity nebo dostupnosti může mít zásadní dopad na zájmy dotčené strany, průběh programů organizace nebo soukromí jednotlivců. Míra citlivosti dat je zde uvedena jako přímo úměrná škodám, které mohou vzniknout jejich kompromitací. Jde tedy zejména o chráněné osobní údaje a data firem, jejichž únik by poškodil zájmy dotčené firmy či jejich zákazníků [1].

Osobní údaje jsou podle Úmluvy Rady Evropy č. 108 každou informací týkající se identifikované nebo identifikovatelné fyzické osoby. Pokud jsou takové informace uloženy v automatizovaných souborech dat, je třeba dle úmluvy učinit vhodná bezpečnostní opatření proti náhodnému nebo neoprávněnému zničení nebo náhodné ztrátě, jakož i proti neoprávněnému přístupu, změnám nebo šíření [2].

Do zvláštní kategorie spadají osobní údaje prozrazující rasový původ, politické názory, náboženské nebo jiné přesvědčení, jakož i údaje týkající se zdraví, pohlavního života nebo odsouzení za trestný čin. Takové informace smějí být zpracovávány automatizovaně jen tehdy, jestliže vnitrostátní právní řád stanoví vhodné záruky [2].

Citlivá data je tedy třeba chránit nejen z finančních důvodů, ale některé druhy dat je nutné chránit proti úniku nebo zneužití i z právního nebo morálního hlediska.

2.1 Členění dat

V oblasti ochrany citlivých dat se běžně rozlišuje mezi třemi různými stavy, ve kterých se data v průběhu svého životního cyklu mohou nacházet [3]. Pro snadnější pochopení následujících kapitol je nutné si tyto stavy představit.

Data v klidu (data-at-rest) Jedná se typicky o uložená data, která nejsou často využívána [4]. Mohou se nacházet například v archivech, na firemních síťových úložištích nebo odložena na pevném disku počítače. Citlivá data v tomto stavu jsou běžně chráněna pomocí šifrování a kontrolou přístupu k jejich umístění [3].

Data v pohybu (data-in-motion) Tento termín označuje data, která jsou v daném momentu přenášena po síti [4][5]. Patří sem například elektronická pošta, klient-klient (peer-to-peer) přenosy, FTP (file transfer protocol) a další způsoby síťové komunikace [5]. Tato data lze chránit například šifrováním přenosového kanálu [3].

Používaná data (data-in-use) Jedná se o aktivní data, se kterými uživatel v danou chvíli pracuje [3]. Jde například o soubory načtené v operační paměti, ve vyrovnávací paměti procesoru nebo zobrazené na obrazovce počítače [6].

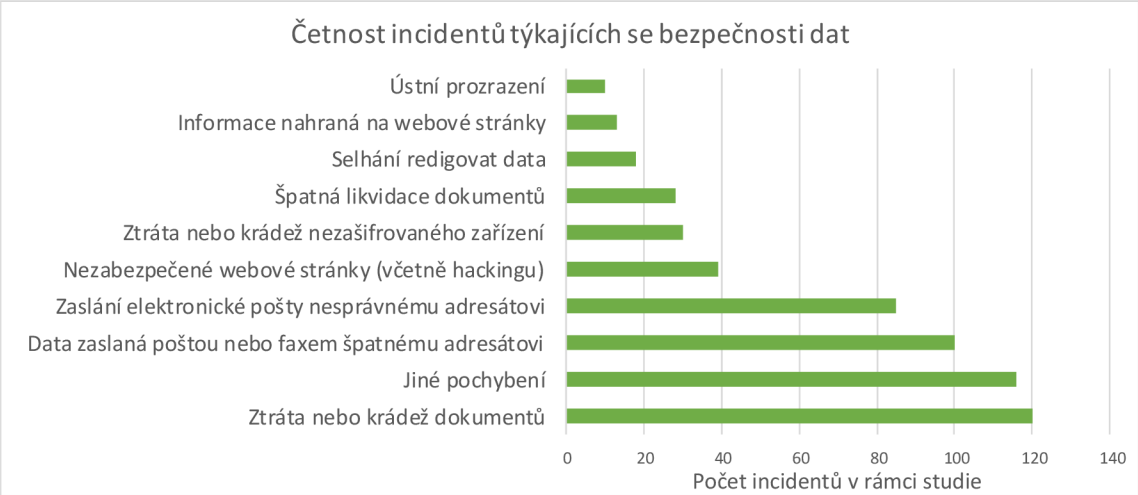
2.2 Únik citlivých dat

Únik citlivých dat je problém, jehož vážnost byla již nastíněna v úvodu kapitoly. Jedná se o incident, který zahrnuje neautorizované nebo nelegální zobrazení, přístup nebo získání citlivých dat jednotlivcem, aplikací nebo službou [7]. Takový incident je vážný problém například z finančních důvodů, kdy únikem citlivých dat může dojít k poškození reputace firmy a finančním ztrátám [8]. Jak již bylo dříve zmíněno, některé typy dat je třeba chránit i z legislativních důvodů, a to zejména osobní údaje [2].

Následující text je věnován analýze těchto incidentů, jelikož pro vývoj efektivního nástroje na ochranu citlivých dat je vhodné pochopit charakter problému, kterému má předcházet.

2.2.1 Četnost incidentů

Podle studie vykonané v září roku 2014 americkým Ponemon Institute, zaměřené na připravenost firem na úniky citlivých dat, celých 43 % respondentů přiznalo, že jejich firma byla v posledním roce postižena únikem dat. Jedná se tedy o navýšení o deset procent oproti předchozímu roku [9][10].



Obrázek 2.1: Graf incidentů týkajících se bezpečnosti dat dle typu incidentu [11].

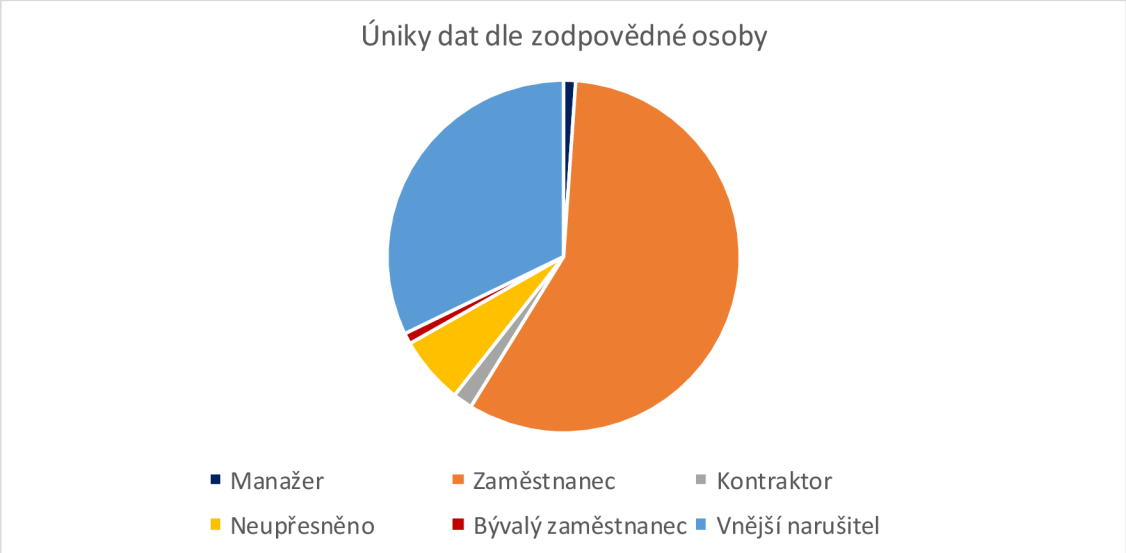
Podle statistik nezávislé britské organizace ICO byl ve druhém kvartálu roku 2015 zaznamenán rostoucí trend v počtu bezpečnostních incidentů, kde 33 % všech incidentů bylo způsobeno odesláním faxu nebo elektronické pošty špatnému adresátovi. Dalších 21 % incidentů se týkalo krádeže nebo ztráty dokumentů a 5 % bylo způsobeno ztrátou nebo odcizením nezašifrovaného zařízení [11]. Úplný přehled dat lze vidět na obr. 2.1.

Z výše uvedených statistik lze tedy konstatovat, že se jedná o rozsáhlý problém, který se dotýká značného množství firem. Obě provedené studie navíc zaznamenaly rostoucí trend v počtu nalezených incidentů.

2.2.2 Původ incidentů

Dle zprávy od InfoWatch Analytical Center bylo v první polovině roku 2015 65,1 % úniků dat způsobeno vnitřními narušiteli a 32,2 % vnějšími (ve 2,6 % případů se nepodařilo příčinu identifikovat). Dále 53,5 % úniků bylo neúmyslných a 44,1 % bylo způsobeno úmyslně [12].

Z celkových úniků bylo 58 % způsobeno současnými (57 %) a bývalými (1 %) zaměstnanci. Více než jedno procento náleží členům vedení firmy (manažeři a vedoucí oddělení) a za dvě procenta je zodpovědný personál externích kontraktorů, kteří měli přístup k interním citlivým datům [12]. Více informací lze vidět na obr. 2.2.



Obrázek 2.2: Graf úniků dat dle zodpovědné osoby [12].

Z výše uvedených informací je tedy zřejmé, že velká většina bezpečnostních incidentů spojených s únikem dat má původ uvnitř firmy a ve většině případů se jedná o pouhou chybu zaměstnance.

2.3 Softwarová řešení prevence úniku dat

Prevencí úniku dat se rozumí strategie pro zajištění citlivých dat proti úniku z firemních systémů [13]. Softwarová řešení pro prevenci úniku dat, také známá jako systémy DLP (z anglického data loss/leak prevention), jsou centralizované systémy pro správu dat, které identifikují, monitorují a chrání citlivé informace, spravují a vynucují firemní politiky, vynucují specifický tok dat a evidují incidenty spojené s úniky citlivých dat [4][14].

Kromě dedikovaných programových řešení, která jsou zaměřením této podkapitoly, se na prevenci úniku dat z určité části podílí i standardní bezpečnostní opatření jako je firewall, systémy pro odhalení průniku (anglicky intrusion detection systems) a antivirový software, který je schopný zabránit nejen útokům zvenčí, ale i útokům zevnitř (některá antivirová řešení v edici typu Enterprise nabízí např. možnost zakázat použití vybraných externích zařízení). Dalším příkladem může být i využití tzv. tenkých klientů (thin clients), kteří využívají architekturu klient-server, bez nutnosti ukládat jakákoliv citlivá data na samotném klientském počítači [3].

Ačkoli je tato práce zaměřena na softwarová řešení, prevence úniku dat není problém, který je možné plně vyřešit pouze softwarovými prostředky. Při uvažování nad celkovou bezpečností systému je nutné vzít v potaz i lidský faktor a informace, které se nevyskytují v elektronické podobě (vytisknuté dokumenty nebo jiná fyzická přenosová média a způsob nakládání s nimi). Programová řešení nemohou tyto aspekty plně pokrýt. Těžko řešitelné problémy jsou např. vyfocení obrazovky fotoaparátem, vynesení vytisknutých dokumentů osobou, která je pro jejich tisk autorizována nebo vyzrazení zapamatovaných informací. Softwarová řešení mohou ale poskytnout prostředky, které doplňují bezpečnostní mechanismy zabývající se těmito aspekty, např. šifrováním elektronických přenosových médií (ochrana proti krádeži a vynesení) nebo automatizovaným informováním uživatele o zavedených firemních bezpečnostních politikách při provádění potenciálně nebezpečných operací [15].

Systémy DLP lze klasifikovat podle následujících vlastností: stavu chráněných dat, místa nasazení, způsobů ochrany a akcí provedenou při detekci úniku [3]. Jejich popisu dle této klasifikace je věnován zbytek kapitoly.

2.3.1 Klasifikace dle stavu chráněných dat

Řešení DLP běžně rozlišují mezi třemi stavy dat: data v klidu, data v pohybu a používaná data. Tyto stavy byly detailně popsány v podkapitole 2.1. Kvalitní řešení by mělo pokrývat v určité míře bezpečnost dat ve všech uvedených stavech [5].

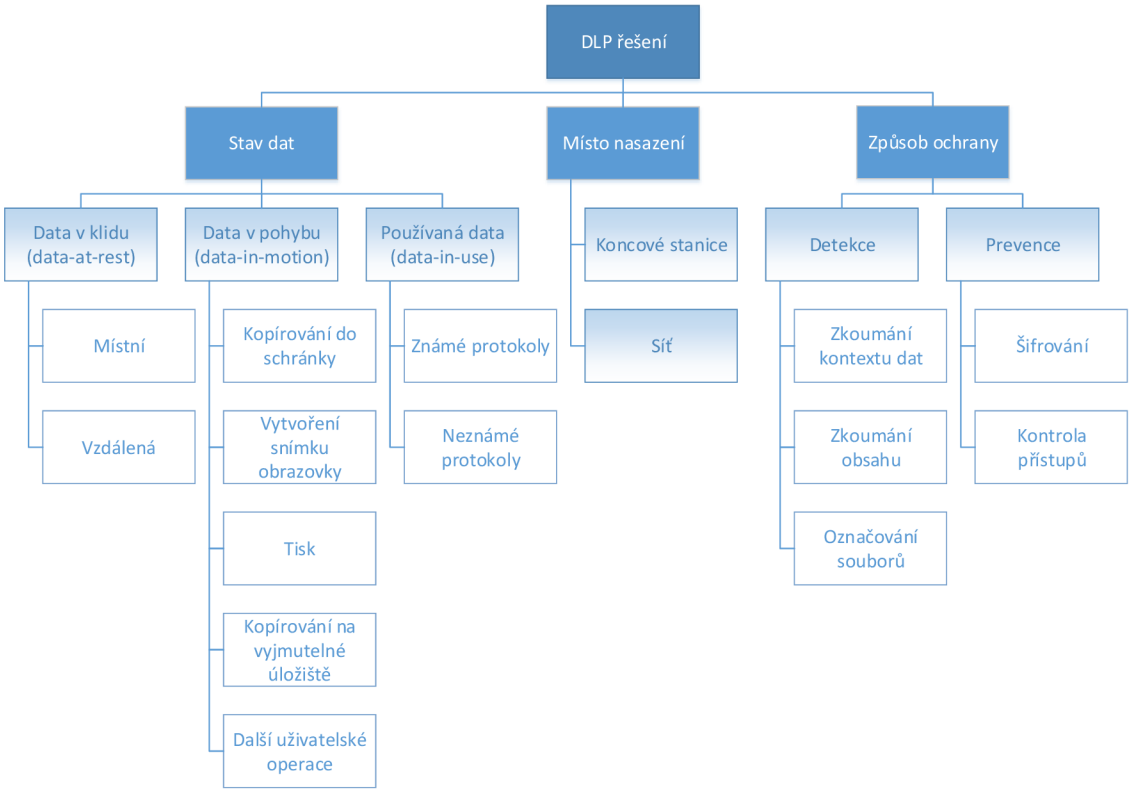
Ochrana dat v klidu Často používané metody pro ochranu dat v klidu (data-at-rest) zahrnují šifrování a kontrolu přístupu. Předpokladem pro využití těchto metod je nalezení dotčených dat, což bývá častou funkcí DLP programů. Například v případě nalezení dat na neautorizovaném serveru mohou být data automaticky smazána, zašifrována nebo může systém zaslat varování majiteli [3].

Pro nalezení citlivých dat jsou často využívány dedikované programy (tzv. *crawlers*), které se nasadí na koncové stanice. Tyto aplikace mají za úkol prohledávat datová úložiště a zaznamenávat umístění specifických informací dle nastavených politik [16].

Ochrana dat v pohybu Pro ochranu dat v pohybu (data-in-motion) jsou využívána řešení DLP, která monitorují a kontrolují síťový provoz. Jedná se o tzv. síťová řešení. Jejich účelem je naslouchat síťovému provozu ve snaze identifikovat přenášený obsah. V případě, že se jedná o data, která je podle nastavených politik zakázáno přenášet, může být přenos přerušen nebo podniknuta jiná akce [17].

Ochrana používaných dat Systémy DLP umístěné na koncových stanicích (endpoint DLP), jsou většinou využívány pro ochranu používaných dat (data-in-use), což jsou data, s kterými uživatel v danou chvíli interaguje. Tyto systémy většinou monitorují data během jejich použití v aplikacích a monitorují jejich tok v systému, například směrem na vyjmutelná úložiště. Jsou schopny zastavit únik dat hned v zárodku, například předtím, než jsou data vůbec vpuštěna na síť nebo než jsou zašifrována za účelem vynesení [3].

Nevýhodou řešení zaměřených na používaná data je nutnost jejich zavedení na všechna sledovaná zařízení, což není vždy možné. Překážkou může být například chybějící kompatibilita s operačním systémem, konflikt s jiným bezpečnostním programem (např. antivir) a jiné důvody.



Obrázek 2.3: Taxonomie systémů DLP [3].

2.3.2 Klasifikace dle místa nasazení

Existují dvě hlavní místa využívaná k nasazení produktů DLP: na koncových stanicích a na síťové úrovni [3].

Síťová řešení Řešení nasazená na síťové úrovni analyzují síťový provoz a podle nastavených bezpečnostních politik mohou blokovat podezřelou komunikaci a zasílat varování. Takový systém by měl být schopen monitorovat různá místa v síti, zatímco centrální server sbírá a analyzuje získaná data a aplikuje na ně nastavené bezpečnostní politiky [17]. Tyto systémy jsou zaměřené na ochranu dat v pohybu.

Řešení na koncových stanicích Řešení umístěná na koncových stanicích monitorují a ovládají přístup k datům. Systémy tohoto typu typicky chrání používaná data a data v klidu (viz podkapitola 2.1). Jejich výhodou je schopnost chránit data, i když je zařízení odpojeno od sítě nebo se nachází mimo budovu organizace. Bezpečnostní politiky bývají běžně uloženy na centrálním serveru, který je rozšiřuje na jednotlivé stanice [3].

2.3.3 Klasifikace podle způsobu ochrany

Přístupy k ochraně citlivých dat lze obecně rozdělit na reaktivní a preventivní [3]. Reaktivním přístupem se rozumí, že systém DLP detekuje bezpečnostní incidenty a reaguje na ně. Například při pokusu přenést soubor označený jako citlivý na nezabezpečené externí zařízení takový systém detekuje pokus o zahájení přenosu a může akci zablokovat nebo

provést jinou akci. V rámci tohoto přístupu se často využívá metod zkoumání kontextu dat (context-based inspection), zkoumání obsahu dat (content-based inspection) a označování souborů (content tagging) [3][17].

Systém aplikující preventivní přístup je schopen výskytu bezpečnostního incidentu přímo předejít, například pomocí kontroly přístupových práv k datům, použitím tenkých klientů nebo využitím šifrování [3].

Zkoumání kontextu dat Jedná se o přístup, který pro detekci incidentů využívá kontextu zkoumaných dat. Tím může být např. IP adresa zdroje a cíle při přenosu dat po síti, velikost dat, adresa příjemce a odesílatele ve zprávách elektronické pošty, přípony souborů, umístění dat nebo používaná aplikace [3].

Zkoumání obsahu Tento přístup detekuje úniky analýzou významu dat. Mezi často využívané metody patří [17]:

- analýza dat pomocí regulárních výrazů,
- porovnávání otisků položek v databázi – využívá hešování,
- porovnávání otisků citlivých souborů – také využívá hešování,
- porovnávání částí dokumentů – používá cyklické hešování,
- statistická analýza – využívá strojového učení a jiných statistických metod pro hledání podobností mezi chráněným a analyzovaným obsahem,
- slovníková/konceptuální analýza – využití kombinace slovníku výrazů a pravidel ve snaze odhadnout význam přenášených dat.

Kvalitní řešení využívající tento přístup by mělo být schopné nahlížet nejen do dokumentů uložených jako jednoduchý text, ale i například do archivů a jinak zahalených dokumentů [3].

Označování souborů Tento přístup využívá pro rozpoznání citlivého obsahu značek, které přidává k souborům obsahujícím chráněná data. Důležitá je schopnost tyto značky přenášet při kopírování, přesouvání, archivaci, šifrování souborů apod.

Kontrola přístupů Jedná se o preventivní přístup, kde řešení DLP má schopnost zamítnout přístup k chráněným datům nepovolaným uživatelům a povolit přístup jen tomu, pro koho jsou data určena [3]. Mezi tato řešení patří tzv. systémy pro správu přístupových práv k informacím. Detailní popis těchto řešení je obsažen v kapitole 3.

Kapitola 3

Systémy pro správu přístupových práv

Účelem systémů pro správu přístupových práv je poskytnout vydavateli kontrolu nad tím, kdo využívá jeho produkt, jakým způsobem je využíván a jak je dále sdílen [18].

Patří sem systémy pro správu digitálních práv (Digital Rights Management), zaměřené obecně na obsah digitálních médií, nebo systémy pro správu přístupových práv k informacím (Information Rights Management), které jsou podmnožinou systémů pro správu digitálních práv. Systémy pro správu přístupových práv k informacím jsou zaměřené na kontrolu informací a dokumentů, a tudíž jsou hlavním předmětem této kapitoly [18][19].

3.1 Správa digitálních práv

Správa digitálních práv, známá také pod zkratkou DRM (z anglického Digital Rights Management), je zastřešující pojem pro množinu technologií zaměřených na kontrolu digitálního obsahu, médií a zařízení proti neautorizovanému šíření a užití [20].

Vývoj těchto technologií byl nastartován rostoucím trendem digitálního šíření duševního vlastnictví, např. hudby, filmů, knih, dokumentů apod. Je v zájmu vydavatelů těchto dat, aby se jejich produkt využíval tak, jak bylo zamýšleno a nedošlo k úniku obchodních tajemství nebo ke ztrátě potenciálního zisku např. prostřednictvím nelegálního šíření obsahu chráněného autorským zákonem [18]. Pokusy o implementaci technologií DRM často naráží na velké množství překážek a nebyly dosud velmi úspěšné [18][19].

3.2 Správa přístupových práv k informacím

Jedná se o podmnožinu technologií pro správu digitálních práv (dále DRM), zaměřenou na ochranu a kontrolu dat ve firemním prostředí [18]. Známé zkratky označující tuto množinu technologií jsou ERM (z anglického Enterprise Rights Management) a IRM (Information Rights Management).

Na rozdíl od technologií DRM zaměřených na kontrolu produktů chráněných autorským zákonem (které ve svém poli působnosti kvůli množství překážek nezaznamenaly velký úspěch [18]), jsou technologie pro správu informačních práv (dále IRM) zaměřeny na mnohém lépe kontrolované a více uzavřené prostředí firem. Tento fakt, spojený s rozdílnými charakteristikami uživatelů dat chráněných těmito systémy, odstraňuje množství problémů, se kterými se potýkají pokusy o nasazení výše zmíněných DRM technologií [18][19].

Příkladem implementace systému IRM jsou např. Microsoft Active Directory Rights Management Services, Adobe LiveCycle[1], Seclore FileSecure[2], OpenText Documentum[3] a další. Tato podkapitola je zaměřena na typické vlastnosti systémů IRM. Jedné z konkrétních implementací, Active Directory Rights Management Services, je věnována samostatná podkapitola 3.3.

3.2.1 Klasifikace systémů IRM

Systémy pro správu přístupových práv k informacím jsou softwarová řešení zaměřená na prevenci úniku citlivých dat a ochranu proti jejich zneužití. Vysvětlení zde použitých pojmů lze nalézt v podkapitole 2.3.

Tyto systémy jsou schopny chránit data ve všech třech rozeznávaných stavech (data v klidu, data v pohybu a používaná data) a v průběhu jejich celého životního cyklu [21]. Data v klidu a data v pohybu jsou chráněna šifrováním na úrovni jednotlivých dokumentů. Obsah je rozšifrován jen pro zobrazení v kompatibilních aplikacích. Ochranu používaných dat zajišťuje skutečnost, že chráněné dokumenty lze zobrazit jen v aplikacích kompatibilních s daným systémem IRM. Tyto aplikace typicky blokují zakázané operace (např. kopírování do schránky, pořizování snímků obrazovky apod.) dle přístupových práv specifikovaných pro daný dokument [19].

Řešení IRM aplikují preventivní přístup k ochraně citlivých dat. Využívanými technikami jsou zejména šifrování a vynucení přístupových práv definovaných pro jednotlivé uživatele. Místem nasazení jsou jednotlivé koncové stanice. Více informací o architektuře těchto systémů je obsaženo v následující podkapitole.

3.2.2 Obecná architektura systémů IRM

Systémy IRM se na nejvyšší úrovni dají rozdělit na dvě hlavní součásti: klient a server. Klienti jsou aplikace kompatibilní s daným systémem. Tyto aplikace umí komunikovat se serverem, zobrazovat či upravovat chráněné dokumenty a vynucovat omezení specifikovaná pro daný dokument (zákaz tisku, kopírování do schránky apod.). Klientské aplikace jsou vysazeny na jednotlivých koncových stanicích a jejich prostřednictvím uživatel interaguje s chráněnými dokumenty [19]. Centrální server autentizuje uživatele a uděluje klientským aplikacím na jejich žádost přístup k chráněným dokumentům [19].

Častou součástí je manažerská konzole, kde je možné např. sledovat výskyt chráněných dokumentů, specifikovat přístupová práva k jednotlivým typům dokumentů, deaktivovat určitý dokument nebo blokovat uživatele [22].

3.2.3 Princip ochrany citlivých dat

Systémy IRM typicky chrání data prostřednictvím šifrování na úrovni jednotlivých dokumentů. Koncový uživatel nemá přístup ke klíči, který se využívá pro šifrování. Tento klíč je buď posílán na žádost klienta přímo z centrálního serveru (Adobe LiveCycle) nebo je obsažen v šifrované podobě v licenci, která je přibalena k chráněnému dokumentu a klíč je z ní extrahován centrálním serverem (Microsoft AD RMS) [19].

Získat přístup k chráněnému dokumentu je tedy možné jen prostřednictvím důvěryhodné kompatibilní aplikace (klienta), která je schopna komunikovat se serverem systému

[1] `http://www.adobe.com/products/livecycle.html`
[2] `http://www.seclore.com/`
[3] `http://www.opentext.com/campaigns/opentext-and-documentum`

IRM. Pokud autentizace uživatele vůči serveru proběhla v pořádku a dokument je stále platný, klientská aplikace obdrží klíč k danému dokumentu a je schopna jej rozšifrovat, zobrazit a provádět v něm úpravy. V některých implementacích nastává po určité době vypršení povolení, kdy se aplikace musí u serveru znovu autorizovat [19].

Úkolem klientské aplikace bývá dále omezovat specifické operace nad daným dokumentem (např. pokud je dokument pouze pro čtení nebo se jedná o dokument se zákazem tisku, kopírování do schránky apod.) [19][23]. Zakázané operace mohou být specifikovány např. v licenci přibalené k dokumentu nebo v odpovědi od serveru [19].

Každý pokus o přístup k chráněnému dokumentu tedy musí projít validací u centrálního serveru. Tato skutečnost umožňuje sledovat používání a pohyb chráněných dokumentů a podrobně spravovat kdo má přístup k jakým dokumentům, včetně kompletní deaktivace dokumentu nebo uživatele v systému.

3.3 Microsoft AD RMS

Příkladem implementace systému IRM je Microsoft AD RMS (Active Directory Rights Management Services). Tento systém byl vyvinutý společností Microsoft a v základní podobě je zaměřený zejména na sadu softwarových produktů Office [24]. Na rozdíl od mnoha uzavřených komerčních implementací Microsoft nabízí sadu vývojových nástrojů, která umožňuje třetím stranám vytvářet klientské aplikace kompatibilní s tímto systémem [25].

Zkratka AD znamená Active Directory, což je implementace adresářové služby vyvinutá firmou Microsoft pro doménové prostředí Windows. Tato adresářová služba se v systému AD RMS používá k autentizaci uživatelů [22].

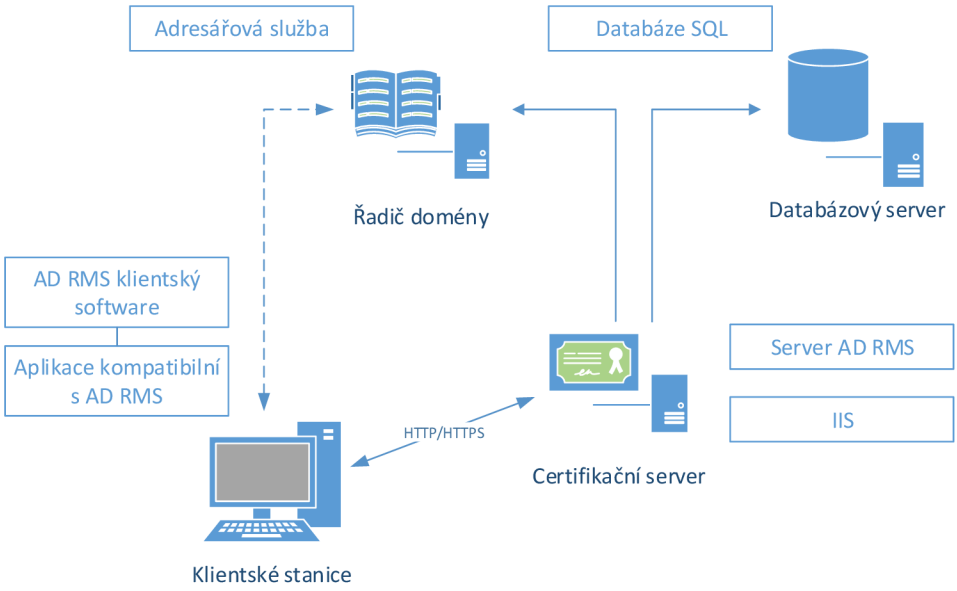
3.3.1 Architektura systému AD RMS

Základní architektura systému se skládá ze čtyř komponent: certifikační server, databázový server, adresářová služba a klientské stanice. Certifikační server vydává licence pro vytváření a přístup k chráněným dokumentům. Databázový server uchovává nastavení AD RMS, záznamy, certifikát serveru, privátní klíče a kopie certifikátů vydaných serverem. Adresářová služba je využívána klienty pro lokalizaci certifikačního serveru a pro autentizaci uživatelů. Poslední komponentou jsou klientské stanice, které mají nainstalovaný klientský software a aplikace kompatibilní se systémem AD RMS (tzv. RMS Enabled Applications). Tyto stanice jsou schopny komunikovat s certifikačním serverem a získat od něj licence k vytváření a použití chráněných dokumentů v kompatibilních aplikacích. Schéma základních komponent systému Microsoft AD RMS lze vidět na obr. 3.1 [22].

3.3.2 Princip ochrany dat pomocí systému AD RMS

V předchozí podkapitole byl popsán obecný princip ochrany dat pomocí systémů IRM. Následující text obsahuje podrobnější popis tohoto principu tak, jak je implementován v systému Microsoft AD RMS.

Než je možné vytvářet nebo pracovat s chráněnými dokumenty, je nutné autentizovat koncového uživatele v adresářové službě Active Directory a zařadit jeho stanici do certifikační hierarchie. Proces zařazení stanice do této hierarchie se nazývá aktivace a jeho výsledkem je řetěz certifikátů, jehož kořenem je certifikační autorita Microsoft a který končí podepsaným certifikátem stanice. Obdržený certifikát je jedinečným identifikátorem stanice [26]. Proces zařazení uživatele je obdobný [27].



Obrázek 3.1: Základní komponenty systému AD RMS [22].

Při vytvoření dokumentu s citlivými daty klientská aplikace vybere pro nový dokument vhodnou sadu přístupových práv pro potenciální uživatele dokumentu. Sadu zvolí buď automaticky nebo pomocí interakce s uživatelem (podle implementace konkrétní aplikace) [28]. Pro zjednodušení tohoto procesu lze v administraci systému AD RMS vytvořit šablony, které obsahují předem definované sady oprávnění pro skupiny uživatelů [28].

Klient následně zašifruje dokument pomocí symetrické šifry náhodně vygenerovaným klíčem, který spolu se zvolenou sadou oprávnění a dalšími informacemi vloží do tzv. *publishing license*. Poté si zažádá od serveru AD RMS tzv. *client licensor certificate*, což je certifikát obsahující asymetrický klíč, který klient použije k zašifrování vytvořené publishing license [28][29]. Zašifrovaný obsah dokumentu a vytvořená publishing license jsou poté spojeny a vloženy do jednoho souboru, čímž vzniká chráněný dokument [28].

Pokud chce někdo pracovat s takto chráněným dokumentem, musí pomocí klientské aplikace kontaktovat server AD RMS a zaslat mu přibalenou publishing license. Server ji dešifruje a vyhodnotí oprávnění daného uživatele vůči tomuto souboru. Pokud má uživatel oprávnění s dokumentem pracovat, server získá z publishing license symetrický klíč k obsahu dokumentu a zašle jej spolu s vyhodnocenou sadou oprávnění pro daného uživatele klientské aplikaci (tzv. *use license*). Tato aplikace dešifruje pomocí získaného klíče obsah dokumentu, zobrazí jej uživateli a vynutí jednotlivá oprávnění pro práci s dokumentem tak, jak jsou specifikována v obdržené use license [28][30][23].

3.3.3 Zahrnutí aplikací třetích stran do systému AD RMS

Jednou z výhod, která systém Microsoft AD RMS odlišuje od mnoha komerčních implementací systémů IRM, je zdarma nabízená oficiální sada nástrojů AD RMS SDK. Jedná se o sadu prostředků, které umožňují třetím stranám vytvářet klientské aplikace kompatibilní s tímto systémem. Toto umožňuje využít architekturu a technologie systému Microsoft AD RMS na ochranu libovolného typu dokumentů v aplikacích třetích stran [25].

Kapitola 4

Ochrana dat programu AutoCAD pomocí systémů IRM

Tato kapitola je věnována analýze možností ochrany cenných výkresů konstrukčních firem prostřednictvím systémů IRM se zaměřením na výkresy tvořené v programu AutoCAD.

AutoCAD je komerční aplikace pro 2D a 3D počítačový návrh vyvinutá v roce 1982 společností Autodesk [31]. Tento program byl zvolen z důvodu, že se jedná o jeden z nejznámějších a nejrozšířenějších programů v tomto odvětví. Velký tržní podíl tohoto produktu umožňuje zaměřit se na integraci pouze do jednoho programu, a přesto pokrýt velkou část rizik spojených s únikem dat, kterým jsou firmy v tomto odvětví vystaveny.

Z pohledu systému IRM je AutoCAD aplikací vysazenou na koncových stanicích, která je používána zaměstnanci pro vytváření a úpravu citlivých dokumentů. Jedná se tedy o klientskou komponentu.

Z předchozí kapitoly vyplývá, že pro zařazení klientské aplikace do systému IRM je nutné, aby byla schopna komunikovat s certifikačním serverem, vyžádat a získat od něj přístup k chráněným dokumentům, získat klíče pro vytvoření nových chráněných dokumentů a zprostředkovat autorizaci uživatele. Dále je nutné, aby aplikace byla schopna na základě odpovědi od certifikačního serveru rozšifrovat a bezpečně zobrazit chráněné dokumenty. V případě provedení úprav nebo při tvorbě nového dokumentů je nutné dokumenty zpětně zašifrovat. V případě, že systém umožňuje specifikovat podrobná přístupová omezení pro jednotlivé dokumenty, je třeba, aby aplikace byla schopna tyto omezení vynutit (např. zákaz kopírování, pořizování snímků obrazovky, otevření dokumentu jen pro čtení apod.) [23]. Více o úloze klientských aplikací v systémech IRM lze nalézt v kapitole 3.

AutoCAD 2016 výše zmíněnou funkcionalitu nenabízí a pro zařazení této aplikace do systému IRM je tedy nutné implementovat rozšíření, které požadované vlastnosti do tohoto programu doplní. Možnostem jeho implementace je věnován zbytek této kapitoly.

4.1 Bezpečné zobrazení chráněných dokumentů

Jednou z nutných vlastností klientské aplikace z pohledu systémů IRM je schopnost bezpečně rozšifrovat a zobrazit chráněné dokumenty. Bezpečným zobrazením je v tomto případě myšleno zobrazení chráněného dokumentu, kdy běžný uživatel nedokáže získat přístup k jeho rozšifrovanému obsahu jinak než zobrazením v aplikaci, kde je k přístupu autorizován. Není tedy vhodné, aby se zobrazený chráněný soubor během doby jeho používání např. nacházel na disku v rozšifrované podobě, odkud by jej mohl uživatel jednoduše zkopírovat.

Jelikož program AutoCAD umí v základní podobě pracovat pouze s nešifrovanými výkresy, je nutné jej o tuto funkcionalitu rozšířit. Pro dosažení tohoto cíle je nutné detekovat pokus o otevření zašifrovaného chráněného dokumentu uživatelem, provést autorizaci a získat přístup k dokumentu od certifikačního serveru. V případě úspěšného získání klíče je nutné programu předat k zobrazení rozšifrovaný obsah místo původního šifrovaného.

Dva možné přístupy prozkoumané v této analýze jsou využití oficiálního aplikačního rozhraní AutoCAD a zachycení a úprava chování systémových volání, které zprostředkovávají přístup k dokumentům. Analýza se zaměřuje na soubory s příponou DWG, což jsou soubory výkresů programu AutoCAD.

4.1.1 Využití aplikačního rozhraní AutoCAD

Společnost Autodesk poskytuje k programu AutoCAD aplikační rozhraní pro vývojáře doplňků třetích stran. Sada nástrojů a rozhraní, které se pro vývoj doplňků využívají, se nazývá ObjectARX (AutoCAD Runtime eXtension). K tomuto rozhraní existuje i varianta použitelná v prostředí .NET, tzv. AutoCAD .NET API [32].

Ačkoli toto rozhraní nabízí sadu funkcí pro otevření výkresů, všechny tyto funkce jsou schopny otevřít pouze nešifrované soubory umístěné v souborovém systému počítače, a tudíž nejsou vhodné pro zobrazení dešifrovaných dat, která se na disku nesmí jako soubor nacházet.

4.1.2 Zachycení systémových volání

Druhou a vhodnější možností, jak zachytit operaci otevření dokumentu uživatelem a případně podvrhnout otevíraný chráněný dokument za jeho rozšifrovaný obsah, je zavedení vlastní dynamicky linkované knihovny do procesu aplikace, buď pomocí metody zvané *DLL injecting* nebo prostřednictvím aplikačního rozhraní AutoCAD. Tato knihovna nahradí relevantní systémová volání vlastními funkcemi (tzv. *hooking*). Prostřednictvím takových funkcí je možné sledovat žádosti programu o přístup k souborům na disku a v případě, že se jedná o chráněný soubor, libovolně změnit parametry zachyceného volání, podvrhnout získaná data nebo žádost zablokovat (např. v případě odmítnutí přístupu k chráněnému dokumentu certifikačním serverem) [33].

Při využití tohoto řešení je možné narazit na problém s identifikací účelu jednotlivých systémových volání. Je nutné rozlišit, zda zachycená žádost o přístup k souboru na disku byla vyvolána pokusem uživatele o zobrazení dokumentu, nebo zda se jedná o automatickou akci prováděnou programem. Dobrým příkladem otevření souboru bez vědomí uživatele v aplikaci AutoCAD je načtení malého množství dat z každého souboru v seznamu nedávno použitých dokumentů po startu aplikace. Přístup k těmto souborům nebyl vyžádán uživatelem a ten by v tomto případě neměl být žádán o provedení autentizace za účelem přístupu k jejich chráněnému obsahu.

Z obr. 4.1 je patrné, že AutoCAD využívá pro načtení obsahu dokumentů pouze malou množinu základních systémových volání, jmenovitě funkce `CreateFileW`, `SetFilePointer`, `SetFilePointerEx` a synchronní variantu funkce `ReadFile`.

Funkce `CreateFileW` se nachází na počátku této sekvence a obsahuje v jednom z parametrů cestu k otevíranému dokumentu, protože se jedná o žádost k získání tzv. `HANDLE`, který se zasílá jako identifikátor souboru do ostatních funkcí, které s ním pracují [34]. V tomto bodě je tedy vhodné rozlišit, zda se jedná o chráněný soubor či nikoliv. Pokud ano, je možné se zde pokusit získat klíč k souboru od serveru IRM, rozšifrovat jeho obsah a uložit jej do paměti programu.

Modul	Funkce	Návratová hodnota
acdb20.dll	CreateFileW ("C:\Users\Adam\Documents\Drawing1.dwg", GENERIC_REA...	0x00000000000015d8
acdb20.dll	ReadFile (0x00000000000015d8, 0x00000051aaffcb40, 64, 0x00000051aaff...	TRUE
acdb20.dll	SetFilePointer (0x00000000000015d8, 128, 0x00000051aaffc604, FILE_BEGIN	128
acdb20.dll	ReadFile (0x00000000000015d8, 0x00000051aaffc620, 108, 0x00000051aaf...	TRUE
acdb20.dll	SetFilePointer (0x00000000000015d8, 24768, 0x00000051aaffc614, FILE_BE...	24768
acdb20.dll	ReadFile (0x00000000000015d8, 0x00000051aaffc640, 20, 0x00000051aaffc...	TRUE
AcSignCore1...	CreateFileW ("C:\Users\Adam\Documents\Drawing1.dwg", GENERIC_READ,	0x0000000000000e44
AcSignCore1...	ReadFile (0x0000000000000e44, 0x00000051aaffd654, 6, 0x00000051aaffd...	TRUE
AcSignCore1...	CloseHandle (0x0000000000000e44)	TRUE
AcSignCore1...	CreateFileW ("C:\Users\Adam\Documents\Drawing1.dwg", GENERIC_READ,	0x0000000000000e44
AcSignCore1...	SetFilePointer (0x0000000000000e44, 0, NULL, FILE_BEGIN)	0
AcSignCore1...	ReadFile (0x0000000000000e44, 0x00000051aaffd358, 16, 0x00000051aaff...	TRUE

Obrázek 4.1: Útržek z posloupnosti relevantních systémových volání prováděných programem AutoCAD 2016 při otevření výkresu za účelem jeho zobrazení.

V následujících voláních funkce `ReadFile`, což je žádost o načtení dat souboru podle předaného `HANDLE`, lze poté programu vracet dešifrovaný obsah uložený v paměti programu namísto šifrovaného, který se reálně v načítaném souboru nachází.

Volání `SetFilePointer` a `SetFilePointerEx` slouží k nastavení pozice čtení nebo zápisu v otevřeném souboru. Tato pozice se uchovává zvlášť pro každý `HANDLE` [34]. Pokud má podvržený dešifrovaný soubor jinou velikost než chráněný, je nutné chování této funkce náležitě upravit (např. když jde o nastavení pozice na konec souboru).

Vzhledem k tomu, že libovolný `HANDLE` může být po jeho uzavření recyklován systémem pro jiný objekt, je nutné zachytit i volání funkce `CloseHandle`, která jeho uzavření zprostředkovává [34]. Pokud `HANDLE` náleží souboru, pro který se právě podvrhují načítaná data, je potřeba jej přestat asociovat s tímto souborem.

Informaci, že dokument byl uzavřen a lze jej odstranit z paměti, je možné získat registrací události `DocumentDestroyed` nabízené v aplikačním rozhraní AutoCAD. Pokud je tato událost vyvolána a se souborem není v aplikaci asociován žádný otevřený `HANDLE`, tak aplikace s dokumentem přestala pracovat a je možné jeho dešifrovaný obsah odstranit.

Výše zmíněný problém detekce, zda žádost o přístup k souboru na disku byla vyvolána uživatelským otevřením dokumentu, lze řešit sledováním parametrů předaných funkci `CreateFileW`. Před otevřením dokumentu za účelem jeho zobrazení se spustí rutina, která použije tuto funkci se zvláštní a jedinečnou kombinaci parametrů, uvedenou v tabulce 4.1. Tuto kombinaci lze detekovat a vyhodnotit jako uživatelskou akci otevření dokumentu. Nevýhodou tohoto přístupu je, že není ze strany společnosti Autodesk garantováno, že toto chování bude zachováno i v budoucích verzích aplikace. Přítomnost tohoto chování byla ale ověřena na několika různých verzích programu AutoCAD.

Druhou možností detekce je registrace události `DocumentCreateStarted`, která je také nabízená v aplikačním rozhraní AutoCAD. Tato možnost je bohužel nespolehlivá. V případě otevření dokumentu prostřednictvím dialogu na výběr souborů chybí v informacích o události název otevíraného souboru, který je nutný pro kontrolu, zda jde o chráněný soubor, a pro doplnění kontextu k zachyceným systémovým voláním.

Parametr	Hodnota
dwDesiredAccess	GENERIC_READ | GENERIC_WRITE
dwShareMode	FILE_SHARE_READ
lpSecurityAttributes	NULL
dwCreationDisposition	OPEN_EXISTING
dwFlagsAndAttributes	FILE_ATTRIBUTE_NORMAL
hTemplateFile	NULL

Tabulka 4.1: Parametry jedinečného volání `CreateFileW`, které značí uživatelskou žádost o otevření výkresu.

4.2 Uložení dokumentů v šifrované podobě

Druhou z vlastností nutných pro zahrnutí klientské aplikace do systému IRM je schopnost zobrazený dokument uložit v chráněné podobě.

Jediným vhodným řešením pro rozšíření programu AutoCAD o tuto funkcionalitu, které bylo v rámci této analýzy nalezeno, je kombinace zachytávání systémových volání a využití aplikačního rozhraní programu.

Aplikační rozhraní AutoCAD umožňuje prostřednictvím doplňku zachytit provádění uživatelských příkazů. V případě, že by příkaz měl za následek uložení chráněného dokumentu v nešifrované formě (příkazy `QSAVE`, `SAVE`, `SAVEAS`, `CLOSE` a `QUIT`), je zde možné jeho provedení vetovat a spustit vlastní příkaz, který dokument uloží v chráněné podobě [35][36]. Bližší popis metody zachycení uživatelských příkazů se nachází v podkapitole 4.3.

Snadnou metodou pro uložení dokumentu v chráněné podobě je dočasné uložení výkresu do nešifrovaného souboru pomocí funkce `Database.SaveAs` nabízené v aplikačním rozhraní AutoCAD. Tento soubor lze následně zašifrovat a přesunout do cílového umístění. Nevýhodou tohoto řešení je, že po malou dobu se chráněný dokument nachází v souborovém systému v nešifrované podobě, odkud by mohl být zkopírován uživatelem. V případě pádu aplikace během šifrování by navíc mohlo dojít k trvalému úniku chráněných dat.

Vhodnější metodou pro uložení chráněného dokumentu je zachycení systémových volání `CreateFileW`, `SetFilePointer`, `SetFilePointerEx`, `WriteFile` a `CloseHandle`. Bližší popis většiny těchto funkcí, včetně metody jejich zachycení, lze nalézt v předchozí podkapitole.

Modul	Funkce	Návratová hodnota
acdb20.dll	CreateFileW ("C:\t\SavedDrawing.dwg", GENERIC_READ | GENERIC_WRITE, (	0x00000000000016cc
acdb20.dll	SetFilePointer (0x00000000000016cc, 128, 0x00000060989feba4, FILE_BEGIN	128
acdb20.dll	SetFilePointer (0x00000000000016cc, 0, 0x00000060989fe804, FILE_BEGIN)	0
acdb20.dll	WriteFile (0x00000000000016cc, 0x00000212c1b70a50, 256, 0x0000006098...	TRUE
acdb20.dll	WriteFile (0x00000000000016cc, 0x00007ff61eba8000, 160, 0x00000060989...	TRUE
acdb20.dll	WriteFile (0x00000000000016cc, 0x00007ff61eba8000, 1056, 0x0000006098...	TRUE
acdb20.dll	SetFilePointer (0x00000000000016cc, 416, 0x00000060989fe804, FILE_BEGIN	416
acdb20.dll	WriteFile (0x00000000000016cc, 0x00007ff61eba8000, 1056, 0x0000006098...	TRUE

Obrázek 4.2: Útržek z posloupnosti relevantních systémových volání prováděných při ukládání dokumentu funkcí `Database.SaveAs`.

Před vyvoláním funkce `Database.SaveAs` je možné si poznamenat výslednou cestu k souboru. Pokud se tato cesta poté vyskytne v parametru funkce `CreateFileW`, lze si uložit získaný `HANDLE` vázaný k tomuto souboru. Pokud se aplikace pokusí v rámci volání `WriteFile` o zápis do souboru prostřednictvím tohoto `HANDLE`, lze zapisovaný blok uložit do umístění v paměti namísto cílového souboru. Po dokončení funkce `Database.SaveAs` by se v paměti měl nacházet kompletní dokument, jehož data je poté možné zašifrovat a uložit v chráněné podobě do cílového souboru.

4.3 Omezení uživatelských operací

Další z nutných vlastností, o kterou je nutné program AutoCAD 2016 pro zasazení do systému IRM rozšířit, je schopnost omezit množinu proveditelných operací nad otevřeným dokumentem podle nastavených práv pro daného uživatele (viz podkapitola 3.2).

Pro vynucení těchto omezení je nutné identifikovat body v programovém toku aplikace (tzv. *usage restriction enforcement points*), ve kterých je nutné provést kontrolu příslušného přístupového práva pro daný dokument a podle výsledku prováděnou operaci uživateli zakázat nebo povolit [23].

Přehled relevantních nastavitelných přístupových práv k dokumentům v systému AD RMS a souvisejících uživatelských operací proveditelných v AutoCAD 2016 lze nalézt v tabulce 4.2.

Popis práva	**Související uživatelské operace**
zobrazení dokumentu	otevření výkresu
úprava dokumentu	uložení změn příkazy rodiny `SAVE`
vyjmutí rozšifrovaného obsahu z aplikace	pořízení snímků obrazovky, práce se schránkou, příkazy rodiny `EXPORT` a další
uložení v jiném chráněném formátu	–
tisk obsahu dokumentu	tisk výkresu příkazy `PLOT` a `3DPRINT`
zobrazení práv k dokumentu	–
změna práv k dokumentu	–

Tabulka 4.2: Souhrn nastavitelných práv pro práci s dokumentem v systému AD RMS a souvisejících uživatelských operací v AutoCAD 2016 [37][23][35][38].

Pokud uživateli nenáleží některé z výše zmíněných přístupových práv, je nutné nad daným dokumentem omezit možnost provádět související uživatelské operace.

4.3.1 Omezení operací pomocí aplikačního rozhraní AutoCAD

Naprostá většina uživatelských operací v programu AutoCAD se provádí pomocí příkazů zadávaných do příkazové řádky programu. Používání klávesových zkratek a nástrojů v grafickém rozhraní aplikace pouze generuje tyto příkazy, které se poté automaticky vloží do příkazové řádky.

Pomocí oficiálního aplikačního rozhraní programu AutoCAD lze vytvořit doplněk, který je schopen tyto příkazy blokovat. Jedním z možných způsobů blokace je zachycení události `DocumentLockModeChanged`, která je vyvolána v momentu, kdy prováděný příkaz žádá o exkluzivní přístup k dokumentu, tzv. *uzamčení*. V obsluze této události lze nahlédnout na

název právě prováděného příkazu a požadavek na zamčení vetovat, což má za následek přerušení operace. Nevýhodou této metody je, že lze aplikovat pouze na příkazy, které před svým provedením zamykají ovlivněný dokument [36]. Všechny výše zmíněné operace, které je nutné sledovat pro ochranu dokumentu, jsou ale touto metodou zachytitelné.

Druhou metodou je změna definice sledovaných příkazů pomocí příkazu `UNDEFINE` tak, aby byly obsluhovány doplňkem. Tento příkaz zruší původní definici libovolného příkazu, který může být poté nahrazen pomocí doplňku. Pokud je prováděná operace oprávněná, doplněk může poté spustit původní příkaz [35]. Hlavní výhodou tohoto řešení je jeho aplikovatelnost na všechny příkazy programu. Nevýhodou je, že původní definici je stále možné použít přidáním znaku tečky před název příkazu, což umožní znalému uživateli spustit i zakázané operace.

4.3.2 Operace nezachytitelné aplikačním rozhraním AutoCAD

Jedinou z významných uživatelských operací nalezených v této analýze, kterou nelze zachytit pomocí aplikačního rozhraní AutoCAD, je pořízení snímku obrazovky.

Jednou z možných metod blokace této operace je využití funkce `IpcProtectWindow` nabízené v sadě nástrojů AD RMS SDK popsané v oddíle 3.3.3. Mezi další metody patří blokace zpráv nebo kláves, které jsou zodpovědné za pořizování snímků obrazovky a zachytávání systémových volání `BitBlt`, `StretchBlt` a `GetDIBits`, které jsou využívány aplikacemi pro získání částí vykreslené obrazovky.

4.4 Analýza výstupních souborů

Při práci s výkresy vytváří program AutoCAD kromě souborů ve formátu DWG i několik dalších typů souborů. Úloha vytvořených vedlejších souborů, jejich dopad na ochranu citlivých dat a popis formátu výkresů DWG je předmětem následujícího textu.

4.4.1 Formát výkresů

DWG (z anglického *drawing*) je základním a nejpoužívanějším nativním formátem výkresů AutoCAD. Jedná se o uzavřený formát vlastněný společností Autodesk. Verze používaná v programu AutoCAD 2016 nese označení DWG 2013. Jeho částečná dokumentace je dostupná ze zpětné analýzy provedené třetími stranami, jako je např. Open Design Alliance [39].

Druhým formátem výkresů, se kterým lze v programu AutoCAD plnohodnotně pracovat, je formát DWF, který je určený pro sdílení dat mezi programy třetích stran. Specifikace tohoto formátu byla zveřejněna společností Autodesk a je volně dostupná [40].

4.4.2 Vedlejší soubory

Během práce s výkresem program automaticky vytváří několik vedlejších souborů. Jedná se o soubory s příponami DWL, DWL2, SV$ a BAK.

Soubory DWL a DWL2 slouží k uchování metadat o otevřeném dokumentu a po skončení práce s výkresem jsou automaticky odstraněny [41]. Tyto soubory neobsahují data výkresu a jsou tudíž z pohledu ochrany dat nezajímavé.

Soubory s příponou BAK jsou kopií dokumentu automaticky vytvářenou při každém uložení změn. Tyto soubory slouží pouze k zálohovacím účelům a jejich tvorbu je možné zakázat v nastavení programu. Při ukládání dokumentu pomocí aplikačního rozhraní je

možné se jejich tvorbě vyhnout použitím funkce pro uložení výkresu `Database.SaveAs`, která tyto kopie nevytváří.

Soubory s příponou SV$ jsou taktéž automaticky vytvářenou kopií výkresu. Jde o výsledek funkce automatického ukládání dokumentů, která v nastavených časových intervalech ukládá otevřený dokument do skrytého umístění za účelem obnovy v případě pádu programu. Tvorbě těchto dokumentů lze zabránit blokací příkazu `AUTO_SAVE`, který automatické uložení provádí.

4.4.3 Možnosti vytvoření obálky pro chráněná data

Pokud se uživatel pokusí otevřít šifrovaný dokument bez souvisejícího doplňku, aplikace pouze oznámí, že dokument není validní. Proto, pokud to formát souboru umožnuje, je vhodné chráněná data skrýt do jiného validního dokumentu, tzv. obálky. Tento dokument může obsahovat vysvětlení, že skrytý obsah dokumentu je chráněný a že bez vhodného doplňku jej není možné zobrazit. Při otevření dokumentu s nainstalovaným doplňkem se data této obálky ignorují a zobrazí se místo nich chráněný výkres. Ačkoli možností na vytvoření této obálky pro formát DWG je více, každá z nich s sebou nese velmi vážné nevýhody.

Podle specifikace zveřejněné organizací Open Design Alliance formát DWG neobsahuje sekci určenou pro vložení libovolných dat, kterou by bylo možné modifikovat přímým zásahem do uloženého souboru [42].

Pomocí aplikačního rozhraní AutoCAD je možné do databáze otevřeného dokumentu vložit větší množství libovolných dat prostřednictvím objektů `XData` a `XRecord`. Paměťový limit při použití objektů `XData` je 16 KB [43], což není pro uložení chráněných dat dostatečné. Ačkoli objekt `XRecord` nemá teoretický velikostní limit [44], jeho použití pro velká binární data se během analýzy ukázalo jako nespolehlivé. Po uložení a zpětném načtení dokumentu byla získaná data neúplná a způsobovala chybová hlášení při kontrole validity dokumentu příkazem `AUDIT`. Tento problém byl hlášen i dalšími členy vývojářské komunity [45]. Správného chování se podařilo dosáhnout rozdělením dat mezi mnoho malých objektů `XRecord`, což ale mělo velmi vážný dopad na rychlost načítání dat o velikosti přesahující několik MB.

Další možností nalezenou v této analýze je uložení chráněných dat na konec obalujícího dokumentu. Ačkoli tato skutečnost není dokumentována ve specifikacích formátu DWG [42], při načítaní souboru program AutoCAD nebere v potaz data přesahující velikost načítaného dokumentu a obálka se tedy zobrazí správně. Vážný problém ale nastane, pokud uživatel, kterému se obálka zobrazila, tento dokument uloží. Program AutoCAD v tomto případě nezachová chráněná data umístěná na konci obalujícího dokumentu a pravý obsah výkresu je ztracen.

4.5 Šifrování dat

V předchozím textu bylo často zmiňováno šifrování chráněných dat. Jelikož program AutoCAD neumí v základní podobě s šifrovanými daty pracovat, je pro zasazení programu do systému IRM nutné zavést vlastní metodu šifrování.

Jak bylo již zmíněno v oddílu 3.3.3, společnost Microsoft umožňuje pomocí sady nástrojů AD RMS SDK zasadit libovolnou aplikaci do systému AD RMS. Aplikační rozhraní nabízené v této sadě nástrojů umožňuje aplikacím komunikovat s klientským modulem systému AD RMS implementovaným v knihovně `Msipc.dll` (ve starší verzi rozhraní

`Msdrm.dll`) [46]. Tento modul poskytuje rozsáhlou sadu prostředků nutných pro zahrnutí libovolné aplikace do systému AD RMS, včetně funkcí pro šifrování dat. Mezi nabízené prostředky ve verzi sady 2.1 patří [47]:

- funkce pro šifrování celých souborů i bloků dat (`IpcEncrypt`),
- funkce pro dešifrování celých souborů i bloků dat (`IpcDecrypt`),
- sada funkcí pro získávání, vytváření a upravování licencí a šablon AD RMS,
- funkce pro ochranu oken při sejmutí snímku obrazovky.

Zde poskytnuté funkce podporují algoritmy RSA 2048 a SHA 256 pro asymetrické šifrování a vytváření podpisů. Pro šifrování obsahu dokumentů je použita symetrická šifra AES 128 [48].

Pro zasazení aplikace do systému AD RMS je nutné na šifrování dat využít nabízenou sadu nástrojů, jelikož šifrovací klíče nejsou v tomto systému klientským aplikacím přímo zpřístupněny. S šifrovacími klíči se zde pracuje pouze nepřímo, prostřednictvím objektů `IPC_KEY_HANDLE` [47].

Mezi další možnosti šifrování dat na platformě Windows patří například aplikační rozhraní CryptoAPI[1] od společnosti Microsoft nebo jiná řešení vyvinutá třetími stranami, jako je např. CryptLib[2], Crypto++[3] nebo Libgcrypt[4].

[1] `https://msdn.microsoft.com/en-us/library/windows/desktop/aa380255(v=vs.85).aspx`
[2] `http://www.cryptlib.com/`
[3] `https://www.cryptopp.com/`
[4] `https://gnupg.org/related_software/libgcrypt/`

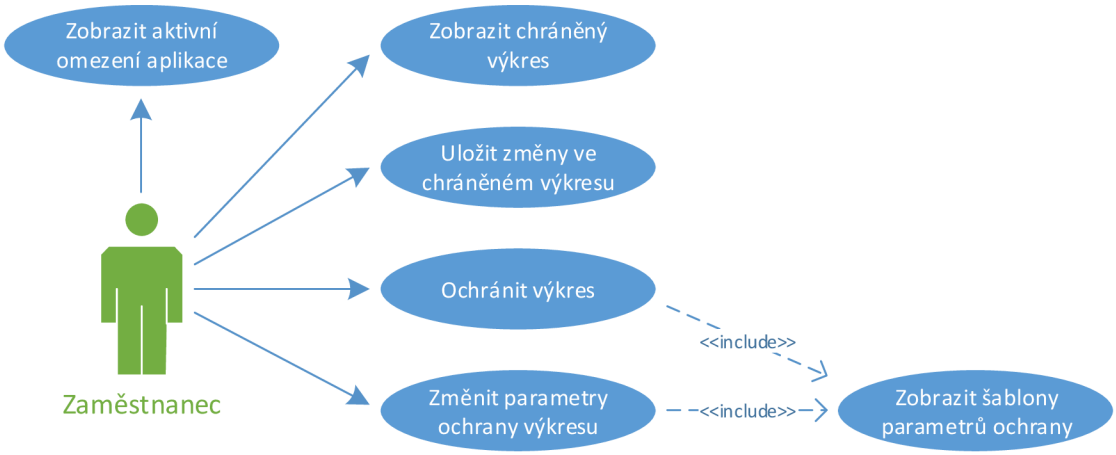
Kapitola 5

Návrh a implementace nástroje

Tato kapitola popisuje a vysvětluje rozhodnutí učiněná při návrhu a implementaci nástroje pro ochranu výkresů AutoCAD. Dále popisuje použité technologie a vybrané implementační detaily.

5.1 Případy užití

V případech užití vystupují dva hlavní aktéři, zaměstnanec a správce. Ze strany zaměstnance se případy užití vztahují zejména k práci s klientskou aplikací systému IRM umístěnou na koncových stanicích a jsou hlavním zaměřením implementovaného nástroje. Výčet případů užití ze strany zaměstnance lze vidět na obr. 5.1.



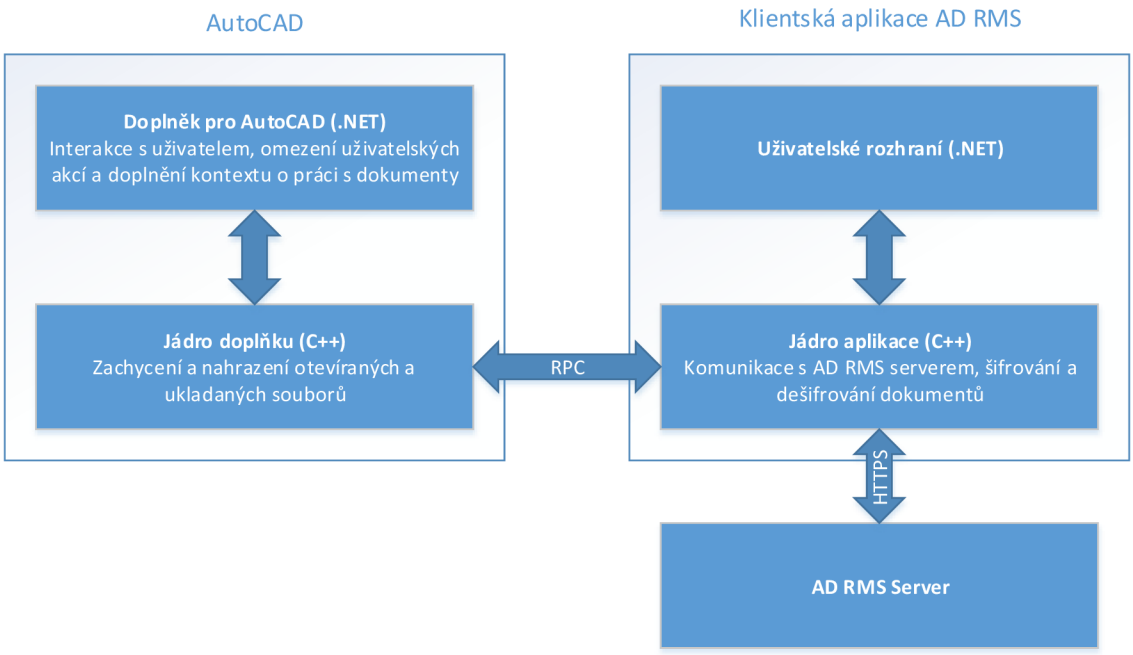
Obrázek 5.1: Diagram případů užití z pohledu zaměstnance.

Navržený systém umožní zaměstnanci klasifikovat a ochránit vytvořené dokumenty s citlivými daty dle jeho uvážení nebo podle zavedených firemních postupů. S chráněnými výkresy je možné dále pracovat pouze v souladu s parametry ochrany nastavenými pro daný výkres a provedené změny lze uložit jen v chráněné podobě. Parametry ochrany je pro jednoduchost možné zvolit pouze podle předem definovaných šablon. Tyto šablony jsou vytvářeny a spravovány správcem systému.

Případy užití ze strany správce se vztahují k práci s nastavovací konzolí a jsou pokryty systémem Microsoft AD RMS, který je detailně popsán v podkapitole 3.3. Zdůvodnění volby tohoto systému pro pokrytí serverové části řešení lze nalézt v oddíle 5.2.4.

5.2 Architektura řešení

Implementovaný systém se skládá z pěti hlavních součástí. Tyto součásti a vztahy mezi nimi jsou znázorněny na obr. 5.2.



Obrázek 5.2: Přehled hlavních komponent systému.

Komponenty umístěné na koncové stanici jsou rozděleny do dvou samostatných procesů. Proces aplikace AutoCAD (`acad.exe`) do sebe po spuštění automaticky zavede doplněk, který spustí inicializaci ostatních komponent. Komponenty klientské aplikace systému AD RMS jsou umístěny v samostatném spustitelném souboru (`IRMUserApplication.exe`) a běží v odděleném procesu. Důvodem pro toto rozdělení je požadavek, aby binární soubory klientských aplikací v systému AD RMS byly podepsány certifikační autoritou [49]. Komunikace s AD RMS serverem přímo z procesu aplikace AutoCAD by byla obtížná, jelikož její binární soubory jsou pod kontrolou aktualizačního systému Autodesk a jejich obsah se může změnit s každou aktualizací aplikace, což by mělo za následek znehodnocení podpisu a znemožnění komunikace se serverem.

Pro komunikaci mezi těmito procesy se využívá varianty protokolu RPC (*Remote Procedure Call*), určené pro lokální komunikaci mezi procesy běžícími na stejném stroji, tzv. protokol NCALRPC[1]. Prostředky pro implementaci tohoto typu komunikace jsou dostupné ve standardním aplikačním rozhraní systému Windows.

Detailní popis jednotlivých komponent, seřazených dle sledu jejich inicializace, lze nalézt v následujícím textu.

[1] `https://msdn.microsoft.com/en-us/library/windows/desktop/aa378665(v=vs.85).aspx`

5.2.1 Doplněk pro AutoCAD

Tato komponenta je dynamicky linkovanou knihovnou využívající variantu aplikačního rozhraní programu AutoCAD určenou pro platformu .NET. Pro její implementaci byl zvolen jazyk C#.

Hlavní úlohou doplňku je omezení uživatelských operací a úprava chování standardních příkazů programu AutoCAD v případě, že je zobrazen chráněný dokument. Pro dosažení této funkcionality využívá metodu vetování požadavků o uzamčení dokumentu, která je spolu se seznamem blokovaných příkazů popsána v podkapitole 4.3.

Kromě blokovaných operací je upraveno je chování příkazů, které mohou mít za následek uložení dokumentu v nechráněné podobě, jmenovitě `QSAVE`, `SAVE`, `SAVEAS`, `CLOSE` a `QUIT`. Při spuštění některého z těchto příkazů v kontextu chráněného dokumentu se příkaz zachytí a spustí se místo něj rutina pro uložení dokumentu ve chráněné podobě. Pro implementaci této rutiny byla zvolena metoda využívající zachycení systémových volání, která je detailně popsána v podkapitole 4.1.

Další úlohou této komponenty je přidání ovládacích prvků nástroje do uživatelského rozhraní programu AutoCAD. Do lišty rychlého přístupu a do hlavního menu jsou při inicializaci doplňku vloženy volby umožňující ochránění otevřeného dokumentu, změnu parametrů ochrany a zobrazení práv na práci s aktivním dokumentem.

Knihovna je zanesena do záznamů v registrech programu AutoCAD a po spuštění programu je automaticky načtena. Během své inicializace spustí inicializační rutinu následující komponenty, jádra doplňku.

5.2.2 Jádro doplňku

Druhou komponentou v pořadí inicializace je dynamicky linkovaná knihovna, jejíž hlavní úlohou je zprostředkovat bezpečné zobrazení a uložení chráněných dokumentů pomocí metody zachytávání systémových volání. Tato metoda je detailně popsána v kapitole 4 a následující text je proto věnován spíše vybraným implementačním detailům.

Tato komponenta je podobně jako výše zmíněný doplněk načtena do adresového prostoru AutoCAD. Z doplňku byla ale vyčleněna do samostatné knihovny implementované v jazyce C++. Kód psaný v tomto jazyce se kompiluje přímo do strojového kódu a je vhodnější pro práci s ukazateli, binárními daty a zachycenými systémovými voláními.

V průběhu inicializace komponenty je vytvořen nový proces klientské aplikace systému AD RMS. Každá instance programu AutoCAD má tedy svého vlastního dedikovaného klienta systému AD RMS, který obsluhuje její požadavky na práci s šifrovanými dokumenty.

Po dokončení inicializace tato komponenta čeká na požadavky od dříve zmíněného doplňku a na události detekované v zachycených systémových voláních. Pokud je v rámci systémového volání `CreateFileW` detekován pokus o zobrazení chráněného dokumentu, klientské aplikaci se prostřednictvím rozhraní RPC zašle požadavek na dešifrování souboru. Pokud je uživatel k zobrazení souboru oprávněný, knihovna zpět obdrží rozšifrovaná data dokumentu a sadu oprávnění pro práci s dokumentem, kterou je nutné při jeho zobrazení vynutit. V případě, že uživatel oprávnění nezíská, žádost o otevření souboru je zablokována a důvod se oznámí uživateli.

Otevřený chráněný dokument je poté reprezentován objektem třídy `CVirtualFile`, který obsahuje rozšifrovaná data dokumentu, seznam aktivních identifikátorů `HANDLE` vázaných k tomuto souboru, aktuální pozici čtení a zápisu pro každý svázaný `HANDLE` a získanou sadu oprávnění. Tento objekt je poté umístěn do kolekce `CVirtualFileCollection`, odkud je dostupný pro získání rozšifrovaných dat v obsluze zachycených systémových volání nebo

pro získání sady oprávnění pro práci s dokumentem. Po dokončení práce s výkresem je objekt odstraněn.

V případě získání žádosti o uložení výkresu se vytvoří nový objekt třídy `CVirtualFile` s prázdnou sekcí pro rozšifrovaná data. Tomuto objektu se poté nastaví příznak `Writeable`. Všechny pokusy o zápis dat do umístění asociovaného s tímto objektem se poté místo do cílového souboru zapíší do sekce pro rozšifrovaná data v objektu. Jakmile doplněk pro AutoCAD oznámí, že zápis dokumentu byl ukončen, rozšifrovaná data se zašlou prostřednictvím protokolu RPC klientské aplikaci, která je zašifruje podle zvolené šablony a uloží do cílového souboru. Objekt je poté z paměťového prostoru odstraněn.

Pokud se program pokusí zapsat data do zobrazeného chráněného dokumentu bez nastaveného příznaku `Writeable`, tak je zápis zablokován. Jedná se o druhou vrstvu ochrany proti přepsání šifrovaného souboru rozšifrovanými daty (první vrstvou je blokace příkazů určených pro uložení dokumentu).

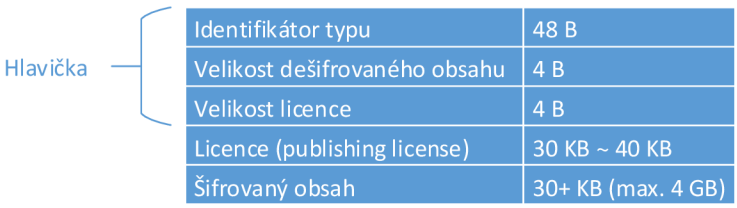
5.2.3 Klientská aplikace systému AD RMS

Úlohou klientské aplikace je komunikovat se serverem AD RMS, vytvářet a získávat dešifrovaný obsah chráněných dokumentů a komunikovat s uživatelem. Tato komponenta je z výše zmíněných důvodů umístěna v samostatném procesu. Proces je spuštěn při inicializaci jádra doplňku a jeho životnost je svázaná s rodičovským procesem aplikace AutoCAD. Jakmile je rodičovský proces ukončen, spojená klientská aplikace se též sama ukončí.

Aplikace je rozdělena na dvě části, jádro a uživatelské rozhraní. Jádro aplikace je implementováno jako dynamicky linkovaná knihovna v jazyce C++ kvůli snadnější práci s binárními daty a protokolem RPC. Pro tvorbu uživatelského rozhraní je použita technologie WPF (*Windows Presentation Foundation*) určená pro platformu .NET. Uživatelské rozhraní je implementováno v jazyce C#.

Při spuštění klientská aplikace obdrží identifikátor rodičovského procesu AutoCAD z parametrů příkazové řádky. Během inicializace uživatelského rozhraní se načte dynamická knihovna jádra aplikace, která spustí server implementující rozhraní RPC pro lokální komunikaci. Na tento server jsou poté od rodičovského procesu směrovány požadavky na vytvoření a rozšifrování chráněných dokumentů a zobrazení informací v uživatelském rozhraní. Připojení k serveru je povoleno pouze rodičovské aplikaci.

Hlavní třída klientské aplikace s názvem `CCore` využívá návrhový vzor jedináček (anglicky singleton) a je proto dostupná ze všech obslužných funkcí RPC serveru. Tato třída směruje přijaté požadavky do obslužných objektů. Nejdůležitějším z těchto objektů je třída `CRMSCommunicator`, která je zodpovědná za komunikaci se serverem AD RMS a práci s chráněnými dokumenty.



Obrázek 5.3: Formát chráněného dokumentu.

Formát chráněných souborů je znázorněn na obr. 5.3. Na začátku souboru se nachází identifikátor typu. Jedná se jedinečný řetězec znaků obsahující číslo verze formátu a slouží

pro rozpoznání chráněných dokumentů. Následují údaje o velikosti licence a dešifrovaného obsahu, které jsou nutné pro získání rozšifrovaných dat. Úloha licence (tzv. publishing license) v systému AD RMS je popsána v oddílu 3.3.2. Na konci dokumentu jsou umístěna šifrovaná data původního souboru.

Tvorba chráněného dokumentu Pro vytvoření nového chráněného souboru je nutné klientské aplikaci předat přes rozhraní RPC data nechráněného souboru a cestu pro uložení výsledného dokumentu. Aplikace poté získá od serveru AD RMS dostupné šablony parametrů ochrany a nechá uživatele některou z nich zvolit. Ze zvolené šablony následně pomocí funkce `IpcSerializeLicense` získá šifrovací klíč a výše zmíněnou licenci (publishing license). Data nechráněného souboru jsou poté zašifrována funkcí `IpcEncrypt` pomocí získaného klíče. Tyto data jsou spolu s licencí a hlavičkou zapsána do výsledného souboru. Funkce s prefixem `Ipc` jsou dostupné v sadě nástrojů AD RMS SDK.

Postup při uložení změn v chráněném souboru je obdobný. Změnou v procesu ochrany je, že klientské aplikaci je nutné navíc předat licenci, kterou má být soubor zašifrován. Výběr šablony ochrany uživatelem v tomto případě není nutný a je vynechán.

Získání dat z chráněného souboru Pro získání rozšifrovaných dat chráněného dokumentu je nutné zavolat funkci `RPC_DecryptFileData` obsaženou v rozhraní RPC klientské aplikace a specifikovat v jejích parametrech cestu k danému souboru.

Klientská aplikace po obdržení požadavku zkontroluje hlavičku dokumentu. Pokud je hlavička validní, získá ze souboru uloženou publishing license a zašle ji pomocí funkce `IpcGetKey` na AD RMS server. Pokud uživatel dosud nebyl za běhu aplikace autentizován, bude vyzván k zadání přihlašovacích údajů. Server poté způsobem blíže popsaným v podkapitole 3.3.2 vyhodnotí, zda je uživatel autorizován k přístupu k tomuto dokumentu. Pokud ano, funkce `IpcGetKey` vrátí klientské aplikaci klíč k šifrovaným datům. Aplikace následně rozšifruje chráněná data, získá pomocí funkce `IpcAccessCheck` sadu oprávnění pro práci s dokumentem a předá je zpět volajícímu funkce `RPC_DecryptFileData`.

5.2.4 AD RMS Server

Poslední komponentou systému je server AD RMS. Ve spolupráci s řadičem domény v implementovaném systému zajišťuje autentizaci a autorizaci uživatelů, správu šablon ochrany, uchovává klíče k šifrovaným licencím, umožňuje sledovat požadavky na přístup k dokumentům a mnoho dalšího. Detailní popis úlohy serveru v systému AD RMS lze nalézt v kapitole 3.

Pro pokrytí serverové části nástroje byl zvolen systém AD RMS z důvodu, že se jedná řešení, které je velmi jednoduché zavést v existujícím doménovém prostředí firmy. Jedná se pouze o další roli v řadiči domény, která využívá seznam uživatelů ze služby Active Directory. Navíc využitím tohoto systému se značně redukuje náročnost implementace nástroje, jelikož kompletně pokrývá úlohu serveru v systému IRM a pomocí sady nástrojů AD RMS SDK usnadňuje implementaci klientské části nástroje, zejména z pohledu šifrování, zabezpečené komunikace se serverem a správy šifrovacích klíčů.

Pro využití systému AD RMS je nutné zavést na koncové stanice klientský software služby AD RMS, jehož instalační balík je volně dostupný na webových stránkách společnosti Microsoft[2]. Pro implementaci nástroje byla využita verze klienta s označením 2.1. Detailní návod k instalaci a nastavení serveru AD RMS lze nalézt v příloze A.

[2] `https://www.microsoft.com/en-us/download/details.aspx?id=38396`

Překážkou pro využití tohoto systému v produkčním prostředí je nutnost podepsat binární soubory klientské aplikace certifikátem, který je nutné vyžádat od společnosti Microsoft [49]. Pro vývojové účely lze ale systém nastavit tak, aby využíval tzv. předprodukční hierarchii certifikátů. Binární soubory aplikace lze poté podepsat certifikátem, který je zahrnutý v sadě nástrojů AD RMS SDK [50].

5.3 Použité technologie

Pro usnadnění implementace některých částí nástroje byly použity již připravené a volně dostupné technologie.

EasyHook EasyHook je dynamicky linkovanou knihovnou využitou pro usnadnění zachytávání systémových volání (tzv. *hooking*) v implementaci třídy `CHookInstaller`. Knihovna je volně dostupná ke stažení na repositáři NuGet pod licencí MIT [51].

Microsoft AD RMS SDK Jedná se o sadu nástrojů volně nabízenou ke stažení na webových stránkách společnosti Microsoft[3]. Její využití pro implementaci nástroje bylo již detailně popsáno v předchozím textu.

Windows Presentation Foundation Tato technologie, určená pro tvorbu uživatelských rozhraní, je od verze 3.0 součástí platformy Microsoft .NET [52]. V rámci implementace byla zvolena pro jednoduchost jejího použití a moderní vzhled vytvořených rozhraní. V nástroji je využívána ke zobrazení dialogů pro komunikaci s uživatelem v rámci klientské aplikace systému AD RMS, která je blíže popsána v oddíle 5.2.3.

AutoCAD .NET API Jde o aplikační rozhraní obsažené v sadě nástrojů ObjectARX, které je nabízeno společností Autodesk k využití pro vývoj doplňků do programu AutoCAD [32]. Její využití v rámci implementovaného nástroje je popsáno v oddíle 5.2.1. Sada nástrojů je volně dostupná na webových stránkách společnosti Autodesk[4].

[3] `https://www.microsoft.com/en-us/download/details.aspx?id=38397`
[4] `http://usa.autodesk.com/adsk/servlet/item?siteID=123112&id=785550`

Kapitola 6

Testování nástroje

V této kapitole jsou představeny metody zvolené pro ověření správné funkčnosti implementovaného nástroje a je zde popsáno, jakým způsobem byly tyto metody aplikovány při testování výsledného řešení. Na konci kapitoly lze nalézt přehled výsledků testovací fáze.

6.1 Metodologie

Účelem testovací fáze je ověřit, zda vytvořená aplikace splňuje kritéria definovaná při specifikaci požadavků.

Pro zvolení vhodné metody testování je nutné vzít v potaz značnou provázanost dílčích komponent vyvinutého nástroje, kdy každá z komponent se podílí na realizaci i základních případů užití. Dále je nezbytné vzít v potaz závislost fungování nástroje na jeho integraci do programu AutoCAD a na očekávaném chování požadavků vůči systému AD RMS, kterého je možné dosáhnout pouze nasazením kompletního nástroje do cílového prostředí.

Z výše zmíněných důvodů bude tedy testování aplikace uskutečněno ověřením očekávaného chování programu při provedení série uživatelských scénářů. Tyto scénáře budou testovány nad kompletním řešením nasazeným do funkčního prostředí systému AD RMS.

Testovací scénáře jsou navrženy dle případů užití popsaných v podkapitole 5.1. Jejich kompletní seznam lze nalézt v příloze B. Každá série scénářů bude ověřena na vzorku dat poskytnutého vedoucím práce. Vzorek se skládá z pěti nechráněných souborů s různými charakteristikami:

1. výkres s malým objemem dat (méně než 50 KB),
2. výkres s velkým objemem dat (kolem 10 MB),
3. výkres s objemem dat, jehož zobrazení je na hranici schopností testovacího stroje (kolem 100 MB),
4. výkres ve formátu DWG 2010,
5. výkres ve formátu DWG 2007.

Obsah databáze objektů nacházející se v těchto výkresech je z pohledu testování nástroje bezpředmětný, jelikož implementované řešení s výkresy pracuje pouze na úrovni souborů.

6.2 Výsledky

Navržení testovacích scénářů a získání výsledků bylo provedeno autorem práce. V průběhu testování bylo ověřeno všech 37 navržených scénářů pro každý soubor poskytnutý v sadě vzorků dat, což dohromady činí 185 ověřených scénářů. Souhrn výsledků lze nalézt v tabulce 6.1.

Vlastnost výkresu	**Úspěch**	**Neúspěch**	**Celkem**	**Procento úspěšnosti**
Malý objem dat	34	3	37	91,9%
Velký objem dat	34	3	37	91,9%
Největší možný objem dat	34	3	37	91,9%
Formát DWG 2010	34	3	37	91,9%
Formát DWG 2007	34	3	37	91,9%
Celkem	**170**	**15**	**185**	**91,9%**

Tabulka 6.1: Souhrn výsledků testování.

Po dokončení testování byly neúspěšné scénáře analyzovány a program byl podle nich patřičně upraven. Nalezené problémy se týkaly chybného zobrazení uživatelských prvků a nesprávného mapování povolených operací nad chráněným dokumentem na odpovídající práva v systému AD RMS. Tyto problémy nebyly vázány na typ zobrazeného dokumentu a projevily se tedy u všech testovaných vzorků.

Po zavedení úprav bylo provedeno druhé kolo testování, které bylo dokončeno se stoprocentní úspěšností. Shrnutí jeho výsledků lze nalézt v tabulce 6.2.

Vlastnost výkresu	**Úspěch**	**Neúspěch**	**Celkem**	**Procento úspěšnosti**
Malý objem dat	37	0	37	100%
Velký objem dat	37	0	37	100%
Největší možný objem dat	37	0	37	100%
Formát DWG 2010	37	0	37	100%
Formát DWG 2007	37	0	37	100%
Celkem	**185**	**0**	**185**	**100%**

Tabulka 6.2: Souhrn výsledků druhého kola testování.

Kapitola 7

Závěr

Výsledkem této práce je plně funkční nástroj pro ochranu citlivých dat výkresů tvořených v programu AutoCAD 2016. Vytvořený nástroj rozšiřuje funkcionalitu tohoto programu způsobem, který jej umožňuje zasadit do role klientské aplikace v systému IRM.

Pro pokrytí serverové části systému bylo zvoleno již existující řešení s názvem Microsoft Active Directory Rights Management Services od společnosti Microsoft. Použití tohoto řešení značně usnadňuje nasazení nástroje do zavedeného doménového prostředí firmy, jelikož umožňuje využít stávající doménovou infrastrukturu pro autentizaci a správu uživatelských účtů. Další výhodou, kterou volba tohoto řešení přináší, je usnadnění implementace částí nástroje kritických pro bezpečnost, zejména díky zprostředkování bezpečné komunikace s certifikačním serverem a poskytnutím aplikačního rozhraní pro šifrování dat.

Hlavním předmětem implementační fáze bylo doplnění programu AutoCAD o vlastnosti, které jsou potřebné pro jeho zasazení do systému IRM. Pro efektivní dosažení tohoto cíle bylo nutné nastudovat problematiku ochrany citlivých dat z širšího pohledu a podrobně analyzovat princip fungování systémů IRM. Dále bylo nezbytné prozkoumat stávající možnosti programu AutoCAD a určit, o které vlastnosti je nutné tento program rozšířit.

Významnou částí práce byla realizace analyzační fáze, která byla zaměřena na nalezení vhodných způsobů implementace zmíněných rozšíření. V rámci této fáze byly nalezeny vyhovující metody na rozšíření programu AutoCAD o všechny požadované vlastnosti. Pro nalezení těchto metod bylo nutné analyzovat chování programu AutoCAD jak na úrovni základních systémových volání, tak z pohledu vysokoúrovňového aplikačního rozhraní nabízeného tímto programem.

Výsledné řešení je schopné zobrazit šifrované výkresy a uložit v nich provedené změny bez vystavení jejich chráněných dat nebezpečí úniku ze strany běžného uživatele. Rozšifrovaná data jsou během práce s výkresem skryta pouze v dočasné paměti programu. Zachycením a úpravou chování systémových volání využívaných programem AutoCAD jsou tomuto programu při práci se soubory podvržena dešifrovaná data místo šifrovaných, která se ve zpracovávaném souboru reálně nacházejí. Zobrazené výkresy jsou následně chráněny proti zneužití pomocí automaticky zavedeného doplňku, který implementuje mechanismus pro vetování operací, které nesmí být dle nastavených politik nad zobrazeným výkresem prováděny.

V závěrečné testovací fázi bylo ověřeno, že vytvořený systém dostatečně pokrývá všechny navržené případy užití a umožňuje práci se šifrovanými dokumenty způsobem běžným pro klientské aplikace systémů IRM.

Další vývoj nástroje by se mohl ubírat mnoha směry. Při implementaci a návrhu systému byl kladen důraz na oddělení obecných komponent a částí specifických pro program

AutoCAD. S drobnými úpravami by tedy bylo možné využít velkou část stávajícího řešení pro rozšíření podpory dalších typů aplikací.

Z pohledu uživatelské přívětivosti se nabízí rozšíření procesu ochrany dokumentů o možnost specifikovat libovolná přístupová práva uživatelem, místo spoléhání se pouze na správcem definované šablony. Pro snadnější vynucení zavedených firemních procesů by mohl být nástroj doplněn o schopnost automaticky chránit vytvářené dokumenty dle předem určené šablony.

Jednou z možných optimalizací by bylo snížení paměťové náročnosti programu dočasným ukládáním šifrovacích klíčů vázaných k zobrazeným výkresům a následným načítáním dat šifrovaných souborů v blocích a pouze na vyžádání.

Pro zvýšení bezpečnosti chráněných dat by bylo možné implementovat další překážky pro případného útočníka. Díky principu ochrany dokumentů systémem IRM není možné, aby narušitel získal přístup k rozšifrovaným datům chráněného souboru neoprávněně. Pokud je ale útočník oprávněn zobrazit rozšifrovaný obsah dokumentu a disponuje v operačním systému dostatečnými právy, tak by se za předpokladu pokročilých technických znalostí mohl pokusit o získání dalších práv na práci s dokumentem, včetně trvalého dešifrování souboru. Z tohoto pohledu je jedním ze slabých míst systému lokální meziprocesová komunikace mezi jednotlivými komponentami. Ačkoli implementovaný RPC server umožňuje pouze lokální komunikaci a již provádí jednoduchou autentizaci klientů, bylo by možné tento mechanismus posílit například šifrováním komunikace klíčem známým pouze autorizovaným komponentám.

Literatura

[1] VIRGINIA INFORMATION TECHNOLOGIES AGENCY. *Information Technology Resource Management Standard SEC501-09.1* [online]. Commonwealth of Virginia, December 8, 2016 [cit. 2017-05-09]. Dostupné z: `https://www.vita.virginia.gov/uploadedFiles/VITA_Main_Public/Library/PSGs/Information_Security_Standard_SEC501.pdf`.

[2] ČESKO. Sdělení Ministerstva zahraničních věcí ze dne 15. listopadu 2001 o přijetí úmluvy o ochraně osob se zřetelem na automatizované zpracování osobních dat. In: *Sbírka mezinárodních smluv*. Česká republika, 2001, částka 52, s. 2146-2165. ISSN 1801-0393. Dostupné z: `https://rm.coe.int/16802eb00f`.

[3] SHABTAI, A., ELOVICI, Y. a ROKACH, L. *A survey of data leakage detection and prevention solutions*. New York: Springer, SpringerBriefs in computer science. ISBN 978-146-1420-538.

[4] AL-FEDAGHI, S. A Conceptual Foundation for Data Loss Prevention. In: *International Journal of Digital Content Technology and its Applications*. 2011, **5**(3), 293-303. DOI 10.4156/jdcta.vol5.issue3.29. ISSN 1975-9339. Dostupné z: `http://www.aicit.org/jdcta/paper_detail.html?q=418`.

[5] LIU, S. a KUHN, R. Data Loss Prevention. In: *IT Professional*. 2010, **12**(2), 10-13. DOI 10.1109/MITP.2010.52. ISSN 1520-9202. Dostupné z: `http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5439507`.

[6] EY. Data loss prevention. *Insights on governance, risk and compliance* [online]. Ernst & Young, October 2011 [cit. 2017-05-10]. Dostupné z: `http://www.ey.com/publication/vwluassets/ey_data_loss_prevention/$file/ey_data_loss_prevention.pdf`.

[7] TEELING, M. What is a Data Breach? Definition, Costs & Security Around Data Breaches. In: *Veracode* [online]. March 26, 2012 [cit. 2017-05-10]. Dostupné z: `https://www.veracode.com/blog/2012/03/what-is-a-data-breach`.

[8] RIDDLE, D. Automating Data Protection, Disaster Recovery Creates Resilient Infrastructures. In: *Disaster Recovery Journal* [online]. © 2012 [cit. 2016-04-26]. Dostupné z: `https://www.techopedia.com/definition/29515/data-in-use`.

[9] PONEMON INSTITUTE. Is Your Company Ready for a Big Data Breach? The Second Annual Study on Data Breach Preparedness. *Experian* [online]. © 2014 [cit. 2016-04-26]. Dostupné z: `http://www.experian.com/assets/data-breach/brochures/2014-ponemon-2nd-annual-preparedness.pdf`.

[10] WEISE, E. 43% of companies had a data breach in the past year. *USA Today* [online]. 24. 10. 2014 [cit. 2016-04-26]. Dostupné z: http://www.usatoday.com/story/tech/2014/09/24/data-breach-companies-60/16106197/.

[11] INFORMATION COMMISIONER'S OFFICE. Data security incident trends. *ICO* [online]. © 2016 [cit. 2016-04-26]. Dostupné z: https://ico.org.uk/action-weve-taken/data-security-incident-trends/.

[12] INFOWATCH ANALYTICAL CENTER. Global Data Leakage Report, H1 2015. *InfoWatch Analytic Group* [online]. © 2015 [cit. 2016-04-26]. Dostupné z: http://infowatch.com/sites/default/files/report/infowatch_global_leakage_report_2015_h1.pdf.

[13] Data Loss Prevention (DLP). In: *WhatIs* [online]. © 2014 [cit. 2016-04-26]. Dostupné z: http://whatis.techtarget.com/definition/data-loss-prevention-DLP.

[14] Data Loss Prevention (DLP). In: *Techopedia* [online]. © 2016 [cit. 2016-04-26]. Dostupné z: https://www.techopedia.com/definition/25115/data-loss-prevention-dlp.

[15] BLACKWELL, C. A Security Architecture to Protect Against Data Loss. In: *Information Security and Digital Forensics*. 2010, 102-110. DOI 10.1007/978-3-642-11530-1_12. ISSN 1867-8211. Dostupné z: http://link.springer.com/10.1007/978-3-642-11530-1_12.

[16] ISACA. Data Leak Prevention. *ISACA* [online]. © 2010 [cit. 2016-04-26]. Dostupné z: http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Data-Leak-Prevention.aspx.

[17] SECUROSIS. Understanding and Selecting a Data Loss Prevention Solution. *Securosis* [online]. 21.10.2010 [cit. 2016-04-26]. Dostupné z: https://securosis.com/assets/library/reports/DLP-Whitepaper.pdf.

[18] PRETSCHNER, A., HILTY, M., SCHÜTZ, F. et al. Usage Control Enforcement: Present and Future. In: *IEEE Security*. 2008, **6**(4), 44-53. DOI 10.1109/MSP.2008.101. ISSN 1540-7993. Dostupné z: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=4588229.

[19] SCHRITTWIESER, S., KIESEBERG, P. a WEIPPL, E. Digital forensics for enterprise rights management systems. In: *Proceedings of the 14th International Conference on Information Integration and Web-based Applications*. New York, USA: ACM Press, 2012, 111-120. DOI 10.1145/2428736.2428756. ISBN 978-1-4503-1306-3. Dostupné z: http://dl.acm.org/citation.cfm?doid=2428736.2428756.

[20] EC-COUNCIL PRESS. *Computer forensics: investigating network intrusions and cybercrime*. Clifton Park, NY: Course Technology Cengage Learning, 2010. ISBN 14-354-8352-9.

[21] KUPPINGER, M. Information Rights Management: Microsoft gives it a new push – just in time to succeed. In: *Kuppingercole Analysts* [online]. 11. 8. 2013 [cit. 2016-04-26]. Dostupné z: https://www.kuppingercole.com/blog/kuppinger/information-rights-management-microsoft-gives-it-a-new-push-just-in-time-to-succeed.

[22] MICROSOFT. Basic AD RMS Architecture. *TechNet* [online]. August 1, 2009 [cit. 2017-03-12]. Dostupné z: https://technet.microsoft.com/en-us/library/ee256070(v=ws.10).aspx.

[23] PERLER, B. a BALDWIN, M. Security Best Practices for Azure Information Protection. In: *Microsoft Docs* [online]. 2017-2-23 [cit. 2017-03-20]. Dostupné z: https://docs.microsoft.com/en-us/information-protection/develop/security-guidelines.

[24] MICROSOFT. Active Directory Rights Management Services Overview. *TechNet* [online]. December 30, 2007 [cit. 2017-03-12]. Dostupné z: https://technet.microsoft.com/en-us/library/cc771627.aspx.

[25] MICROSOFT. About the AD RMS SDK. *Microsoft Developer Network* [online]. © 2017 [cit. 2017-03-12]. Dostupné z: https://msdn.microsoft.com/en-us/library/cc530374(v=vs.85).aspx.

[26] MICROSOFT. Activating a Computer. *Microsoft Developer Network* [online]. © 2017 [cit. 2017-03-17]. Dostupné z: https://msdn.microsoft.com/en-us/library/cc530377(v=vs.85).aspx.

[27] MICROSOFT. Activating a User. *Microsoft Developer Network* [online]. © 2017 [cit. 2017-03-17]. Dostupné z: https://msdn.microsoft.com/en-us/library/cc530378(v=vs.85).aspx.

[28] MICROSOFT. How AD RMS Works. *TechNet* [online]. August 2, 2012 [cit. 2017-03-17]. Dostupné z: https://technet.microsoft.com/en-us/library/jj590750(v=ws.11).aspx.

[29] MICROSOFT. Understanding AD RMS Certificates. *TechNet* [online]. December 30, 2007 [cit. 2017-03-18]. Dostupné z: https://technet.microsoft.com/en-us/library/cc753886(v=ws.11).aspx.

[30] MICROSOFT. AD RMS Applications. *Microsoft Developer Network* [online]. © 2017 [cit. 2017-03-18]. Dostupné z: https://msdn.microsoft.com/en-us/library/cc530383(v=vs.85).aspx.

[31] Autodesk, Inc. History. *FundingUniverse* [online]. [cit. 2017-03-16]. Dostupné z: http://www.fundinguniverse.com/company-histories/autodesk-inc-history/.

[32] AUTODESK. Autodesk Developer Network. *Autodesk* [online]. © 2017 [cit. 2017-04-12]. Dostupné z: http://usa.autodesk.com/adsk/servlet/index?siteID=123112&id=1911627.

[33] BREMER, J. X86 API Hooking Demystified. In: *Development & Security* [online]. July 2, 2012 [cit. 2017-04-12]. Dostupné z: http://jbremer.org/x86-api-hooking-demystified/.

[34] MICROSOFT. File Management Functions. *Microsoft Developer Network* [online]. © 2017 [cit. 2017-04-12]. Dostupné z: https://msdn.microsoft.com/en-us/library/windows/desktop/aa364232(v=vs.85).aspx.

[35] AUTODESK. Command Quick Reference. *Autodesk Help* [online]. © 2015, Last updated: November 3, 2015 [cit. 2017-03-20]. Dostupné z: http://help.autodesk.com/view/ACD/2016/ENU/?url=/view/ACD/2016/ENU/files/alphabetical-list-of-commands.html.

[36] WALMSLEY, K. Blocking AutoCAD commands from .NET. In: *Through the Interface* [online]. October 31, 2006 [cit. 2017-03-25]. Dostupné z: http://through-the-interface.typepad.com/through_the_interface/2006/10/blocking_autoca.html.

[37] MICROSOFT. Rights. *Microsoft Developer Network* [online]. © 2017 [cit. 2017-03-19]. Dostupné z: https://msdn.microsoft.com/en-us/library/hh535295(v=vs.85).aspx.

[38] PERLER, B., BALDWIN, M. a MOHANRAM, P. Understanding usage restrictions. In: *Microsoft Docs* [online]. 2017-2-23 [cit. 2017-03-20]. Dostupné z: https://docs.microsoft.com/en-us/information-protection/develop/understanding-usage-restrictions.

[39] EITELJORG, H., FERNIE, K., HUGGETT, J. et al. CAD: A Guide to Good Practice. In: *Guides to Good Practice* [online]. 17-01-2009, Revised 2011 [cit. 2017-04-14]. Dostupné z: http://guides.archaeologydataservice.ac.uk/g2gp/Cad_Toc.

[40] AUTODESK. *DXF Reference* [online]. Autodesk, Inc., February 2011 [cit. 2017-04-14]. Dostupné z: http://images.autodesk.com/adsk/files/autocad_2012_pdf_dxf-reference_enu.pdf.

[41] DWL2 file format description. *DataTypes.net* [online]. © 2017 [cit. 2017-03-16]. Dostupné z: https://datatypes.net/open-dwl2-files.

[42] OPEN DESING ALLIANCE. *Open Design Specification for .dwg files* [online]. Open Design Alliance, Inc., © 1998-2013 [cit. 2017-04-14]. Dostupné z: https://www.opendesign.com/files/guestdownloads/OpenDesign_Specification_for_.dwg_files.pdf.

[43] AUTODESK. Managing Extended Data Memory Use. *Autodesk Knowledge Network* [online]. Apr 14 2017 [cit. 2017-04-15]. Dostupné z: https://knowledge.autodesk.com/search-result/caas/CloudHelp/cloudhelp/2018/ENU/OARX-DevGuide/files/GUID-1290C815-0C57-4AC0-AC53-E90CF7F1DBF5-htm.html.

[44] AUTODESK. XRecord Object (ActiveX). *Autodesk Knowledge Network* [online]. Apr 28 2015 [cit. 2017-04-15]. Dostupné z: https://knowledge.autodesk.com/search-result/caas/CloudHelp/cloudhelp/2015/ENU/AutoCAD-ActiveX/files/GUID-AF9C01F7-5BD9-4AF8-AB63-F58A997A5258-htm.html.

[45] Binary Serialization to XRecord. In: *Autodesk Community* [online]. 04-21-2015 01:58 PM [cit. 2017-03-15]. Dostupné z: https://forums.autodesk.com/t5/net/binary-serialization-to-xrecord/td-p/5601969.

[46] MICROSOFT. AD RMS Client. *Microsoft Developer Network* [online]. © 2017 [cit. 2017-03-19]. Dostupné z: https://msdn.microsoft.com/en-us/library/cc530385(v=vs.85).aspx.

[47] MICROSOFT. Functions. *Microsoft Developer Network* [online]. © 2017 [cit. 2017-03-19]. Dostupné z: https://msdn.microsoft.com/library/hh535289.aspx.

[48] BAILEY, C. a BALDWIN, M. Comparing Azure Information Protection and AD RMS. In: *Microsoft Docs* [online]. 2017-3-6 [cit. 2017-03-22]. Dostupné z: https://docs.microsoft.com/en-us/information-protection/understand-explore/compare-on-premise.

[49] MICROSOFT. Creating an Application Manifest. *Microsoft Developer Network* [online]. © 2017 [cit. 2017-03-21]. Dostupné z: https://msdn.microsoft.com/en-us/library/cc530456(v=vs.85).aspx.

[50] MICROSOFT. Setting Up the Pre-production Development Environment. *Microsoft Developer Network* [online]. © 2017 [cit. 2017-03-22]. Dostupné z: https://msdn.microsoft.com/en-us/library/cc542540(v=vs.85).aspx.

[51] STENNING, J. *EasyHook* [online]. Copyright 2016 [cit. 2017-04-30]. Dostupné z: https://easyhook.github.io/.

[52] CHAPPELL, D. Introducing Windows Presentation Foundation. *Microsoft Developer Network* [online]. September 2006 [cit. 2017-03-30]. Dostupné z: https://msdn.microsoft.com/en-us/library/aa663364.aspx.

Přílohy

Příloha A

Návod k instalaci systému AD RMS

Tato příloha obsahuje stručný návod ke správnému nastavení a instalaci systému Microsoft AD RMS nutného pro spuštění implementovaného nástroje.

Prerekvizity

Pro instalaci systému AD RMS jsou nutné následující prerekvizity:

1. systém Microsoft Windows Server 2012 R2
2. funkční doménové prostředí

Návod k instalaci

Následující kroky popisují postup pro instalaci základní varianty systému AD RMS včetně přípravení klientské stanice a nastavení tzv. předprodukčního prostředí:

1. Nastavte instalaci tzv. předprodukčního prostředí.
   (a) Spusťte nástroj *Registry Editor*.
   (b) Najděte nebo vytvořte klíč `HKEY_LOCAL_MACHINE\Software\Microsoft\DRMS`.
   (c) Do klíče vložte položku typu `DWORD` s názvem `Hierarchy` a hodnotou 1.
2. Přidejte roli Active Directory Rights Management services.
   (a) V programu *Server Manager* zvolte položku *Add roles and features*.
   (b) Přejděte na druhý krok průvodce a označte *Role-based or feature-based installation*.
   (c) Vyberte cílový server pro instalaci role.
   (d) Ve výběru rolí označte *Active Directory Rights Management Services*.
   (e) Postupte na bod *Confirmation* a zvolte *Install*.
3. Proveďte konfiguraci role.
   (a) Po dokončení instalace zvolte *Perform additional configuration*.

(b) Přejděte na druhý krok průvodce a označte *Create a new AD RMS root cluster*.

(c) Zvolte *Use Windows Internal Database* on this server.

(d) Vytvořte běžný doménový uživatelský účet pro služby serveru AD RMS.

(e) V následujícím kroku průvodce vyberte vytvořený účet a zadejte přihlašovací údaje.

(f) Zvolte sílu šifrovacích algoritmů, doporučenou volbou je *Cryptographic Mode 2*.

(g) Označte *Use AD RMS centrally managed key storage*.

(h) Zadejte heslo pro obnovu tzv. Cluster Key.

(i) V bodě *Cluster Address* zvolte adresu virtuálního adresáře serveru AD RMS ve službě IIS.

(j) Postupte na bod *Confirmation* a zvolte *Install*.

4. Připravte klientskou stanici na funkci v předprodukčním prostředí.

   (a) Spusťte nástroj *Registry Editor*.

   (b) Najděte nebo vytvořte klíč `HKEY_LOCAL_MACHINE\Software\Microsoft\MSIPC`.

   (c) Do klíče vložte položku typu `DWORD` s názvem `Hierarchy` a hodnotou 1.

5. Nainstalujte klientský software systému AD RMS.

   (a) Stáhněte sadu nástrojů RMS SDK 2.1 z oficiálních webových stránek Microsoft[1].

   (b) Proveďte instalaci sady nástrojů.

   (c) Stáhněte instalační balíček klienta verze 2.1 z oficiálních webových stránek Microsoft[2].

   (d) Spusťte instalační balíček a proveďte instalaci.

   (e) Zkopírujte soubory `ipcsecproc_isv.dll` a `ipcsecproc_ssp_isv.dll` obsažené v sadě nástrojů v podadresářích `bin/x64` a `bin/x86`.

   (f) Soubory z adresáře `x64` vložte do instalačního adresáře 64 bitové verze klienta, typicky v `C:/Program Files`.

   (g) Soubory z adresáře `x86` vložte do instalačního adresáře 32 bitové verze klienta, typicky v `C:/Program Files (x86)`.

   (h) Zkopírované soubory přejmenujte tak, aby nahradily soubory `ipcsecproc.dll` a `ipcsecproc_ssp.dll` obsažené v obou instalačních adresářích.

[1] `https://www.microsoft.com/en-us/download/details.aspx?id=38397`
[2] `https://www.microsoft.com/en-us/download/details.aspx?id=38396`

Příloha B

Testovací scénáře

Prerekvizity:

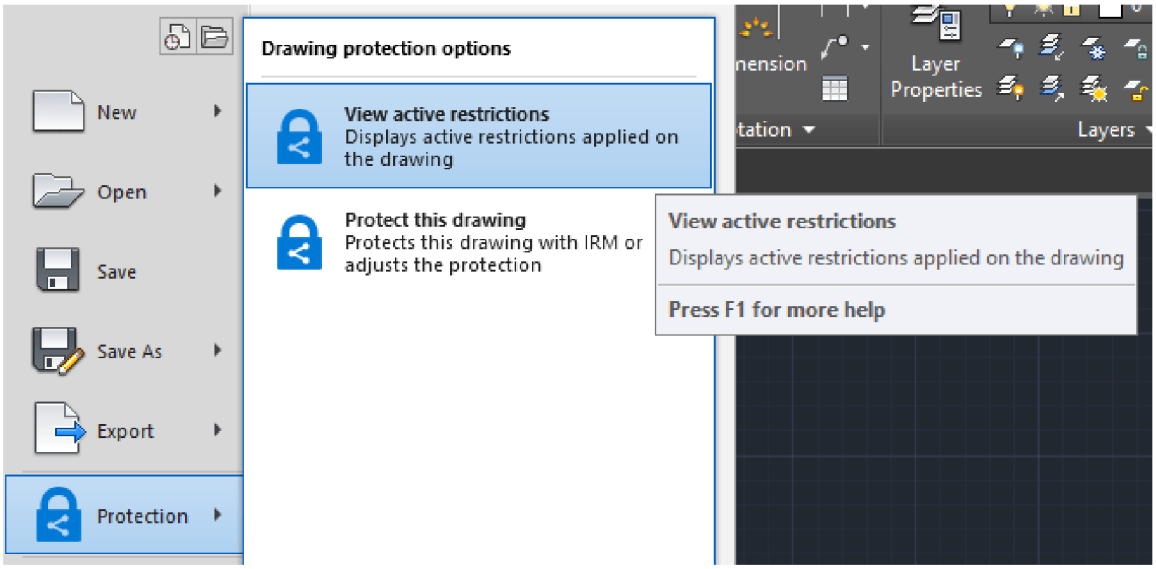
1. dva uživatelské účty v doméně
2. vytvořená *šablona ochrany 1* s právem pouze na čtení a zobrazení nastavených práv pro *uživatele A* a přidaným právem na zápis pro *uživatele B*
3. vytvořená *šablona ochrany 2* s právem na čtení pro *uživatele A* a bez specifikovaných práv pro *uživatele B*

Jednotlivé kroky a jejich očekávané výsledky jsou rozděleny do tří navazujících sezení a jsou uvedeny v tabulkách B.1, B.2 a B.3. Seznam kroků je navržen tak, aby efektivně pokryl následující sadu scénářů:

- otevření chráněného výkresu všemi známými způsoby
- interakce s všemi prvky uživatelského rozhraní nástroje
- ochránění výkresu
- zobrazení aktivních omezení aplikace
- změna parametrů ochrany výkresu
- uložení provedených změn ve výkresu všemi známými způsoby
- blokace zakázaných operací, včetně pořízení snímku obrazovky funkcí Print Screen

Krok	**Očekávaný výsledek**
Přihlášení pod účtem *uživatele A* a spuštění programu AutoCAD	Automatické načtení doplňku a zobrazení ikony zámku v liště rychlého přístupu
Otevření nechráněného výkresu z připravené sady vzorků	Zobrazení dokumentu
Rozbalení hlavní nabídky programu	Přítomnost položek *Protection*, *View Rights* a *Protect document*
Zvolení položky *View Rights*	Zobrazení okna s informací, že dokument není chráněný
Zvolení položky *Protect document*	Zobrazení dialogu pro autentizaci
Autentizace přihlašovacími údaji *uživatele A*	Zobrazení nastavených šablon ochrany
Výběr připravené *šablony 1* a zvolení tlačítka *Protect*	Výkres se uloží a otevře v chráněné podobě (*výkres X*)
Zvolení ikony zámku v liště rychlého přístupu	Zobrazení okna s výčtem práv na práci s výkresem, všechna jsou povolena
Uložení do nového umístění příkazem `SAVE`	Nový výkres se uloží v chráněné podobě (*výkres Y*)
Otevření právě uloženého výkresu přes hlavní nabídku	Chráněný výkres se správně zobrazí
Volba položky *Protect document*	Zobrazení nastavených šablon ochrany
Výběr připravené *šablony 2* a zvolení tlačítka *Protect*	Výkres se uloží a otevře v chráněné podobě
Vypnutí programu a odhlášení uživatele	Program se ukončí

Tabulka B.1: Sezení uživatele A.



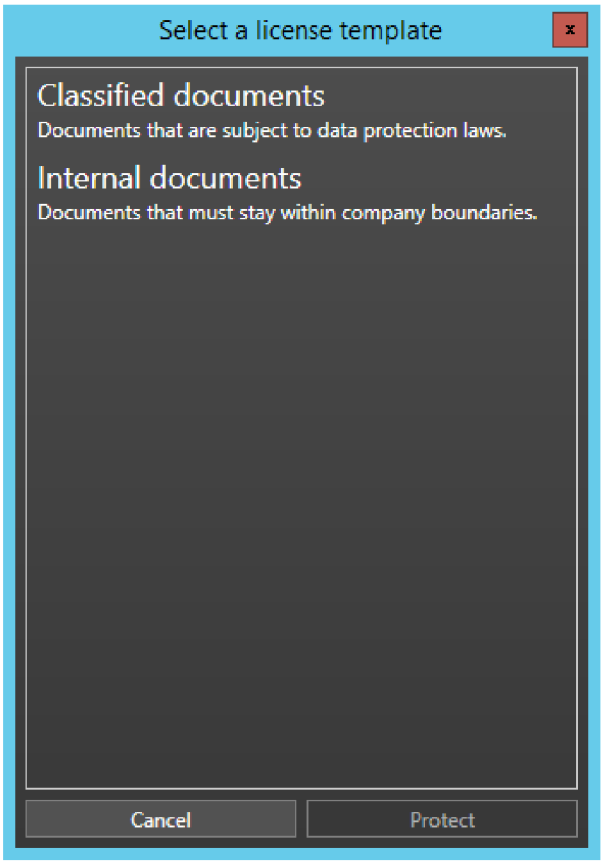
Obrázek B.1: Položky přidané do hlavní nabídky programu.

Krok	**Očekávaný výsledek**
Přihlášení pod účtem *uživatele B*	
Otevření chráněného *výkresu Y* poklepáním na soubor v Průzkumníku	Spuštení programu AutoCAD, automatické načtení doplňku a zobrazení dialogu pro autentizaci
Autentizace přihlašovacími údaji *uživatele B*	Přístup k dokumentu je odepřen a zobrazí se okno s odpovídající informací
Otevření chráněného *výkresu X*	Chráněný výkres se správně zobrazí
Zvolení položky *View Rights* v hlavní nabídce programu	Zobrazení okna s výčtem práv, povoleno je pouze čtení, zápis a zobrazení práv
Pokusit se o provedení zakázaných operací	Operace jsou zakázány a pro každou je zobrazeno odpovídající varování
Přepnutí na nechráněný dokument a pořízení snímku obrazovky	Okno aplikace je na snímku viditelné
Přepnutí zpět na chráněný dokument a pořízení snímku obrazovky	Okno aplikace je na snímku začerněno
Provedení změn a uložení příkazem `QSAVE`	Výkres se uloží a otevře v chráněné podobě
Uložení do nového umístění příkazem `SAVEAS`	Nový výkres se uloží otevře v chráněné podobě
Zvolení položky *View Rights* v hlavní nabídce programu	Zobrazení okna s výčtem práv na práci s výkresem, povoleno je pouze čtení a zápis
Provedení změn a uzavření výkresu	Zobrazení okna s varováním, že dokument má neuložené změny
Souhlas s uložením změn	Výkres se uloží v chráněné podobě a uzavře
Otevření právě uloženého výkresu přes nabídku *Recent Files*	Chráněný výkres se správně zobrazí a obsahuje změny z předchozího kroku
Vytvoření nového výkresu chráněného *šablonou 2*	Výkres se vytvoří, uloží a otevře v chráněné podobě (*výkres Z*)
Provedení změn v obou otevřených výkresech a ukončení programu	Zobrazení okna pro každý dokument s varováním, že výkres obsahuje neuložené změny
Odmítnutí uložení změn a odhlášení uživatele	Program se ukončí

Tabulka B.2: Sezení uživatele B.

Krok	**Očekávaný výsledek**
Přihlášení pod účtem *uživatele A*	
Otevření chráněného *výkresu Z* poklepáním na soubor v Průzkumníku	Spuštění programu AutoCAD, automatické načtení doplňku a zobrazení dialogu pro autentizaci
Autentizace přihlašovacími údaji *uživatele B*	Chráněný výkres se správně zobrazí
Zvolení položky *View Rights* v hlavní nabídce programu	Zobrazení práv je zakázáno a zobrazí se odpovídající hlášení
Provedení změn a pokus o uložení příkazy `QSAVE`, `SAVE` a `SAVEAS`	Operace jsou zakázány a pro každou je zobrazeno odpovídající varování
Uzavření výkresu	Výkres se uzavře bez možnosti uložit provedené změny
Otevření stejného výkresu přes nabídku *Recent Files*	Chráněný výkres se správně zobrazí a neobsahuje provedené změny
Provedení změn a ukončení programu	Program se ukončí bez možnosti uložit provedené změny

Tabulka B.3: Druhé sezení uživatele A.



Obrázek B.2: Dialog pro výběr šablony parametrů ochrany.