УДК 004

© Мельникова Н. С.[1], 2007

СИСТЕМИ КЕРУВАННЯ ПРАВАМИ ДОСТУПУ ДО ІНФОРМАЦІЇ

Подано короткий огляд систем керування правами доступу до інформації: ERM і DRM.

The brief browse of the rights management systems is represented.

Зі швидким поширенням Інтернету, швидкість і легкість обміну цифровими даними зросла, разом із числом потенційних сторін, які можуть обмінюватися даними. Це також означає, що захист даних більше не обмежується комп'ютером, що містить оригінальні дані, або корпоративними системи мережевого захисту. До того ж, захист даних застосовується не тільки до доступу до даних, але й до того, що користувач може робити з даними [1]. Тому розвиток систем керування доступом до інформації посідає важливе місце в житті сучасного суспільства адже кожен підприємець і просто звичайний користувач комп'ютера бажає, щоб його інформація була захищена від розповсюдження.

Керування правами доступу до інформації (RM) припускає, що механізм політики безпеки нерозривно пов'язаний із захищеним цифровим контентом, незважаючи на його місцезнаходження. Цифрові права доступу — це правила, що визначають те, що конкретним користувачам, що працюють за відповідними комп'ютерами, дозволено робити з тими або іншими цифровими документами. А виконання цих правил здійснюється через механізми, прив'язані до конкретного документа або програмному контейнеру, що його містить. Оскільки ці повноваження назавжди пов'язані з документом, вони зберігаються й при передачі даних по мережі, і при копіюванні їх у буфер, і при занесенні в базу даних або при простому збереженні на жорсткий диск ноутбуків.

Керування правами доступу містить у собі набір документів, що регулюють їхній життєвий цикл, правила політики безпеки й методи кодування. Воно передбачає опис набору підтримуваних цифрових об'єктів — наприклад, документів САПР, електронних таблиць й аудіофайлів; ідентифікацію користувачів або комп'ютерів, взаємодіючих із цими об'єктами, створення правил використання об'єктів і т.д.

Сфера керування правами поширюється як на споживчий ринок, так і на корпоративний. Побутові засоби DRM широко використовуються для захисту цифрових матеріалів, що продаються, таких, як мелодії для мобільних телефонів, цифрова музика й відео, а також потоковий широкомовний контент. Такі технології вбудовані, наприклад, у цифрові аудіопродукти компанії Apple і різноманітні формати Windows Media компанії Microsoft, тоді як системи ERM,

[1] Українська академія друкарства.

відомі також під абревіатурою E-DRM (Enterprise DRM), є корпоративним механізмом захисту інформації. ERM-системи розгортаються, як правило, для захисту конфіденційної корпоративної інформації, доступ до якої повинен бути обмежений вузьким колом користувачів, переважно з керівного складу. Крім того, використання ERM гарантує повний контроль за роботою рядових користувачів з корпоративними даними.

Засновниками технології керування правами доступу стали кілька невеликих постачальників-новаторів, за якими пішли й великі галузеві компанії. Всі вони прагнуть запропонувати ERM-систему, що з'єднує в собі вбудоване кодування, контроль за використанням даних на робочих місцях, фільтрацію даних і керування політикою безпеки. Ці системи допоможуть забезпечити дотримання правил використання даних всіма співробітниками й запобігти випадковому витоку важливої інформації через мережу.

Реально захист інформації повинен здійснюватися на клієнтській системі, і це принципово новий рівень у розвитку технології забезпечення безпеки даних. Наприклад, механізми сканування контента на предмет вмісту вірусу повинні запускати додаток з підтримкою ERM, оскільки тільки воно має права на розшифровку даного контента. Можна зробити й по-іншому, постачивши RM-функціями антивірусне ПЗ на настільних системах і на централізованих міжмерсжевих екранах. Однак всі ці підходи на рівні виробника ще тільки мають бути реалізовані [2].

Сьогоднішні ERM-пропозиції різняться по своїх основних цільових завданнях й архітектурі. Так, деякі рішення базуються на програмних агентах, які можуть застосовуватися до самих різних додатків, ведучи моніторинг додатка ззовні, замість того, щоб вбудовуватися в його код. У цьому випадку може знадобитися додатковий користувацький інтерфейс для керування правами. У той же час RM-розробки, орієнтовані на фірмові платформи прикладного ПЗ, навпроти, використовують для забезпечення захисту API-інтерфейси або вбудовані в додатки функції.

Популярність систем ERM помітно виросла після того, як Microsoft в 2003 р. увійшла на цей ринок зі своєю пропозицією Rights Management Services for Windows Server (RMS) і зробила його ключовим елементом своєї стратегії безпеки. Створюючи платформу керування правами, Microsoft прагнула до створення цілої екосистеми для розробки RM-додатків на базі продуктів третіх фірм, що дозволяє вибудовувати самі різні прикладні системи, — наприклад, для офісної автоматизації (як, наприклад, пакет Office Professional з RM-підтримкою), САПР, інфраструктури обміну повідомленнями й т.д. Платформа складається із загального набору API і серверів (на базі сервера RMS), які розробники ПЗ можуть використовувати для додавання RM-функцій у нові й існуючі додатки. На відміну від постачальників, що пропонують агенти, таких, як Liquid Machines й SealedMedia, технології Microsoft потрібне широке визнання й сильна підтримка з боку співтовариства розробників.

Компанія Liquid Machines зробила мудрий вибір на користь удосконалювання своєї лінії продуктів за рахунок включення правил політики безпеки сервера RMS. Такий підхід дозволив Liquid Machines скористатися деякими можливостями новаторського користувацького інтерфейсу, підтри-

муючи при цьому взаємодію з потужними засобами Microsoft для керування політикою безпеки. Скоріше всього Liquid Machines продовжить поступово розширювати свою архітектуру, щоб охопити й інші бази даних для керування правами доступу.

Один з піонерів у цій області, компанія Authentica, недавно (на початку 2006 р.) була куплена компанією EMC з метою посилення впливу останньої на корпоративному ринку керування контентом. Після чого EMC оголосила про те, що за цим піде посилення її пакета керування документами eRoom можливостями продукту Secure Documents фірми Authentica, що повинне забезпечити безперервний захист корпоративної інформації. Така динаміка розвитку цілком природна, і прикладу EMC швидше за все підуть й інші постачальники.

Уже в багато версій ПЗ Reader компанії Adobe убудовані RM-засоби, але керування політикою захисту інформації у свою технологію LiveCycle вона додала тільки в останні кілька років.

Список основних ERM-постачальників завершує компанія SealedMedia. Маючи, очевидно, найбільша кількість клієнтів, вона прагнула створити архітектуру на базі агентів, легку в розгортанні що має мінімальний вплив на клієнтські системи. Вони забезпечують безперервний захист інформації не тільки всередині організації, але й при взаємодії з партнерами, у процесі пересилання їм тих або інших даних.

Електронна пошта з RM-функціональністю дозволить адміністраторам ввести обмеження на те, що співробітник може робити з повідомленнями. Так, конфіденційні оголошення можуть містити правила, наприклад, у такій комбінації: «тільки для читання співробітниками», «заборона на переадресацію» й «обмежений строк використання, видалити через три дні». Клієнтське ПЗ ERM і дозволяє користувачам читати повідомлення, але запобігає його пересиланню. І незважаючи на місцезнаходження повідомлення через три дні ERM-система його «анулює» і робить «нечитабельним» для всіх цілей усюди й одночасно. Більше того, ERM-клієнти запобігають й іншим способам витоку інформації, такі, як друкування повідомлення, копіювання/вставка, «знімок екрана» і т.д.

Для ефективності DRM повинні бути враховані юридичні інтереси як користувачів, так і власників авторських прав. Досить імовірно, що всі привілейовані використання, які очікують користувачі, не можуть бути враховані в автоматичній системі й, можливо, може бути потреба звертання користувача до ліцензійного сервера/розповсюджувача для одержання права привілейованого використання даних (наприклад журнал запитів про право вибірки з документа). Однак, така система буде вимагати, щоб третя сторона засвідчила й акредитувала користувачів (наприклад користувач є акредитованим журналістом), які не використовуються в поточних реалізаціях (виконаннях) систем DRM. Оскільки DRM має можливість дуже щільно (жорстко) контролювати дотримання авторських прав, законодавство може нейтралізувати такі кроки.

Є три фактори, які відрізняють різні структури захисту даних: присутність віртуальної машини (VM), форма контролю й стиль поширення.

Перший рівень відмінності — присутність віртуальної машини (VM), яка описується як «програмне забезпечення, що працює на вершині уразливого обчислювального середовища й використовує функції контролю для забезпечення засобів захисту й керування доступом і використанням цифрової інформації

Друга відмінність у вигляді елемента керування, що використовується. Форма керування – правила управління використання DRM захищених даних. Форми керування діляться на три типи: форма фіксованого контролю, впроваджений контроль і зовнішній контроль [3].

При фіксованому контролі віртуальна машина має визначені функції контролю, запропоновані для DRM даних [4, 5]. Хоча фіксована форма контролю не підходить для загальних додатків систем DRM, вона може успішно використатися в інших системах керуваннями правами. Наприклад, ядро Linux має систему, щоб простежити, чи є модулі, що завантажують незалежно (подібно драйверам пристрою) — GPL, сумісними чи ні [6].

Впроваджені й зовнішні форми контролю добре адаптуються до потреб користувача. При впровадженій формі контролю DRM дані прибувають із впровадженим елементом керування. Це може бути зроблено формуванням елемента контролю й роботи в оточенні захисту. При зовнішній формі контролю DRM захищені дані й елементи керування прибувають окремо. Явна перевага такої системи полягає в тому, що єдиний установлений елемент керування (контролю) може використовуватися для визначення прав на різні однотипні роботи. З іншого боку, зовнішні елементи контролю звичайно втримуються на мережному сервері й до них потрібен доступ щораз, коли звертаються до роботи DRM [7], дозволяючи тим найдужчий контроль за дотриманням прав. Обидві ці системи можуть, крім того, комбінуватися з фіксованою формою контролю. Багато хто із сьогоднішніх систем DRM використовують одну із цих двох систем; музичний магазин Apple iTunes, наприклад, використовує впроваджений елемент керування (Apple Fairplay) на музиці, об'єднаний з основним фіксованим елементом керування на музичному плеєрі iTunes. З іншого боку, Microsoft рекомендує використання комбінації впровадженого й зовнішнього елементів керування при поширенні музики й фільмів з DRM Windows Media Player 9 й WMA й WMV медіа форматів [8].

Третя відмінність складається в процесі поширення. Проводиться диференціація між відправленням повідомлення й зовнішнім архівом. У системі відправлення повідомлення, дані – передаються між відправником й одержувачем по прямому каналі зв'язку, типу електронної пошти. При зовнішньому архіві одержувач вибирає дані із центрального архіву. Обидві системи використовуються в системах DRM і вибір системи поширення не обов'язково впливає на захист даних.

Найсучасніші DRM системи, подібно Apple iTunes, використовують віртуальні машини програмного забезпечення для DRM елементів керування.

Microsoft Right Management Services (RMS) — кращий приклад операційного рівня DRM системи. Система RMS охоплює три частини: DRM диспетчер (контроль) клієнтської сторони, пакет програмного забезпечення, що дозволяє розробляти додатки DRM і серверний модуль (forWindows 2003

Server) для керування (адміністрування) DRM захищених робіт. Клієнтський модуль RMS приписує права, запитувані RMS додатками й доступний для всіх Microsoft Windows 98SE і більш пізніх версій операційних систем Microsoft. Однак RMS не є ще повним рішенням (не повністю розроблено, не вирішує всіх проблем, завдань) і цілеспрямоване тільки на роботу усередині підприємства.

Отже, поданий короткий огляд про те, що являють собою системи керування правами доступу до інформації. Технічно дуже важко здійснювати привілейовані права на використання, як цього вимагає закон про авторське право й жодна із сучасних систем не здійснює всі необхідні привілейовані використання. Однак, такі системи як, наприклад, Fairplay використовувана Apple's iTunes Music Store, зуміли знайти рівновагу (баланс) між очікуваннями користувачів і забезпеченням достатнього захисту авторських прав.

Microsoft's RMS має потенціал, щоб стати стандартом для здійснення керування правами; воно забезпечує гнучкість: дозволяє як слабкий DRM контроль для споживчих послуг, і сильний DRM контроль, що потрібно для захисту документів підприємства. RMS також має потенціал у загальному механізмі підписання ліцензій і цифрових контрактів. Однак, багато чого із цих додатків не може бути здійснено, якщо RMS не створить новий механізм для аутентифікації користувача, тому що сучасні механізми або мають занадто багато обмежень, або занадто багато проблем захисту.

Література

1. Windows rights management services: Protecting electronic content in financial, healthcare, government and legal organizations, 2003.

URL:http://www.microsoft.com

2. http://www.ccc.ru

3. *PARK, J., SANDHU, R., AND SCHIPALACQUA, J.* Security architectures for controlled digital information dissemination. In Proceedings of the 16th Annual Computer Security Applications Conference (2000).

4. *MULLIGAN, D., HAN, J., AND BURSTEIN, A.* How DRM based content delivery systems disrupt expectations of «personal use». In Proceedings of the 2003 ACM workshop on Digital Rights Management (2003), ACM, pp. 77-89.

5. *BECHTOLD, S.* Digital rights management in the united states and europe. IVir, Buma/Stemra — Copyright and the Music Industry: Digital Dilemmas

6. *BECHTOLD, S.* Reconciling DRM technology with copyright limitations. IVir, Buma/Stemra — Copyright and the Music Industry: Digital Dilemmas

7. *ROSENBLATT, B.* DRM for the enterprise, 2004

8. MICROSOFT. Microsoft windows media data session toolkit, 2003