ISSN 1727-1584

КОФАНОВ А.В. ПРИМЕНЕНИЕ СОВРЕМЕННЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ПРИ ПРОВЕДЕНИИ ОРУЖИЕВЕДЧЕСКИХ ИССЛЕДОВАНИЙ
Рассмотрены теоретические и практические аспекты использования компьютерных технологий при проведении оружиеведческих исследований.

***

KOFANOV A.V. APPLICATION MODERN INFORMATION TECHNOLOGY INVESTIGATION OF FIREARMS
This article analyzes the theoretical and practical aspects make use of computer technology investigation of firearms.

УДК 681.3

Л.Г. ЧЕРНИШ, канд. техн. наук, доц.
О.К. ЮДІН, канд. техн. наук

Інститут діагностичних систем Національного авіаційного університету

ЗАГАЛЬНИЙ ПІДХІД ДО ПОБУДОВИ СИСТЕМ ВІДДАЛЕНОГО АДМІНІСТРУВАННЯ, АВТОМАТИЧНОГО ОНОВЛЕННЯ І СУПРОВОДУ ПРОГРАМНИХ ПРОДУКТІВ

Розглянуто систему віддаленого адміністрування, автоматичного оновлення і супроводу програмних продуктів; визначені загальні підходи до їх побудови, досліджена можливість використання в якості серверних модулів таких систем системних служб Windows NT/2000/XP.

Розвиток у нашій державі відносин власності, визнання інформації як об'єкта права власності та підвищення цінності інформації, викликав вдосконалення адміністративно-технічного управління інформаційними ресурсами та базами даних підприємств і організацій, які є розподіленими не тільки технічно, але і в аспекті територіального місця розташування. Сьогодні виникла гостра потреба щодо вдосконаленню методів та засобів віддаленого адміністрування і супроводу таких інформаційних ресурсів та баз даних.

В умовах, коли філії чи відокремлені підрозділи підприємства розташовані на великій відстані одна від одної, одним з основних каналів зв'язку та можливістю організації системи електронного управління між ними є мережа Інтернет. При цьому більшість підприємств використовують програмне забезпечення власної розробки, яке необхідно супроводжувати і періодично оновлювати. Крім того, виникає питання про організацію системи електронного документообігу і дієздатності програмного забезпечення стандартизованого щодо роботи та вимог даної організації чи підприємства.

Зрозуміло, що в такій ситуації в кожній відокремленій структурі потрібен достатньо підготовлений системний адміністратор, який буде виконувати перелічені задачі. Припустимо, що для виконання процедури інсталяції системи закритого документообігу необхідно розгорнути програмний продукт, адаптований до вимог зазначеної фірми. Продукт передається через Інтернет засобами електронної пошти, тому на стороні одержувача необхідно прийняти цей файл або сукупність файлів, розпакувати їх у випадку, якщо вони були упаковані, і встановити на всі комп'ютери локальної мережі або центральний сервер. Навіть для досвідченого співробітника виконання цієї задачі займе чимало часу, Тому з урахуванням того, що дані можуть передаватися багаторазово і періодично оновлюватися, у кожній філії необхідно мати співробітника, який займатиметься тільки встановленням файлової системи документообігу і синхронізацією версій для подальшого отримання користувачами оновлених документів і матеріалів. Безумовно, такий підхід не є раціональним.

1. Дистанційне оновлення та супровід програмного забезпечення.

Розглянемо приклад системи автоматичного оновлення, призначеної для дистанційного супроводу програмних продуктів, а також для віддаленого оновлення і настроювання програмного забезпечення. Означена система орієнтована на супровід спеціалізованого програмного забезпечення, яке використовується в процесі організації закритого документообігу та його супроводу [1, с.125].

До основних можливостей системи можна віднести:

- автоматичне копіювання і видалення файлів; встановлення і запуск на виконання програм на всіх машинах локальної мережі;
- формування пакетів оновлень і завантаження їх на сервер у мережі Інтернет;
- установку оновлень із сервера в мережі Інтернет.

При цьому інформація ущільнюється з метою зменшення її обсягу і передається в захищеному від читання і модифікації виді. Також система містить функції для віддаленого адміністрування машин: створення, зміни і видалення облікових записів користувачів, дозволів файлової системи одночасно на всіх машинах локальної мережі. Ця функціональність може бути зручна як для мережних адміністраторів, так і для керівників відокремлених підрозділів чи філій щодо впровадження системи контролю та доступу до інформаційних потоків та ресурсів у випадках, коли необхідно на якийсь час розширити повноваження облікових записів співробітників, щоб вони могли виконати ті або інші дії, а потім оновити їхні початкові права доступу.

ISSN 1727-1584

Слід зазначити, що як сервер оновлень можна використовувати будь-яку поштову скриньку на безкоштовному поштовому сервері, що робить використання даного продукту доступним для будь-якого підприємства. Крім того, завдяки досить ефективному ущільненню даних нема потреби мати виділену лінію доступу в Інтернет, достатньо звичайного модемного підключення до телефонної мережі.

З метою запобігання спроб несанкціонованого читання і модифікації інформації, переданої по поштових каналах зв'язку, усі файли, що прикріплюються до повідомлень, шифруються, і розраховується їхня контрольна сума. При отриманні файли розшифровуються, і перевіряється їхня контрольна сума. Пакет оновлення встановлюється тільки тоді, якщо контрольна сума розшифрованих даних збігається з обчисленою при відправленні.

Для шифрування використовується алгоритм потокового шифрування RC4; воно виконується засобами криптографічного програмного інтерфейсу Windows. Контрольна сума являє собою 32-розрядний циклічний надлишковий код (CRC). Ключ алгоритму шифрування зберігається всередині програмного файлу клієнтського модуля. Кожна інсталяція продукту має свій унікальний ключ, тому необхідно, щоб відправник і одержувач оновлень встановлювали свої копії продукту з одного інсталяційного диска. Хоча виконуваний файл клієнтського модуля ущільнений програмою-пакувальником, що істотно ускладнює отримання ключа шифрування з виконуваного файлу, для забезпечення безпеки ключа треба виключити доступ сторонніх осіб до інсталяції і встановлених копій програмного продукту.

Таким чином, один раз встановивши і настроївши модулі системи автоматичного оновлення, можна позбутися від необхідності вручну приймати і копіювати файли. Автоматизоване робоче місце оператора дозволяє з одного комп'ютера одержувати пакети оновлень і відразу ж встановлювати їх на всі машини локальної мережі. Розгортання системи автоматичного оновлення на комп'ютерах локальної мережі не представляє складності і може бути зроблено звичайним користувачем, що має в системі права адміністратора. Установка означеної системи виконується або власною інсталяційною програмою, або програмою установки продукту, компонентом якого вона є, тому що система автоматичного оновлення може поширюватися не тільки як окремий продукт, але й як компонент іншого програмного продукту, наприклад, оболонки для лабораторних робіт.

2. Модулі системи та процедури їх безпеки.

Система автоматичного оновлення складається з двох основних модулів: клієнтського і серверного, а також деяких допоміжних модулів, наприклад, модулю підсистеми ліцензування.

Клієнтський модуль встановлюється на комп'ютер адміністратора, що має доступ в Інтернет, і служить для управління системою автоматичного оновлення. Він логічно розділений на три підсистеми: прямого управління, формування оновлень і установки оновлень, і може працювати у відповідних режимах прямого управління, формування оновлень і установки оновлень. Модуль є автоматизованим робочим місцем адміністратора, за допомогою якого система як одержує оновлення з сервера оновлень, так і відправляє на нього ж оновлення, веде пошук у локальній мережі запущених серверних модулів і відправляє їм відповідні команди. Доступ до клієнтського модуля обмежений паролем – його запитує модуль під час запуску і продовжує роботу тільки у випадку успішної авторизації.

Серверний модуль приймає від клієнтського модуля команди і виконує їх; він встановлюється на кожний комп'ютер локальної мережі. Запускається цей модуль як системна служба при завантаженні операційної системи із системним обліковим записом і працює *в контексті безпеки системного облікового запису* незалежно від прав, з якими увійшов у систему користувач, і чи увійшов він взагалі.

Кожен процес оновлення в ОС Windows NT/2000/XP запускається в контексті безпеки якого-небудь облікового запису. Наприклад, коли користувач запускає виконуваний файл, він працює в контексті безпеки поточного облікового запису. Існує також можливість запуску процесу оновлення від імені іншого користувача після входу в систему під його ім'ям, в контексті його безпеки. У цьому випадку в системі виконуються ті дії, які дозволені даному користувачеві системною політикою безпеки і дозволами файлової системи. Тобто, наприклад, якщо користувач має право на створення файлу в системному каталозі, то і процес оновлення, запущений у контексті безпеки цього користувача, буде мати таку можливість.

Системні служби запускаються в контексті безпеки системного облікового запису (якщо не задане інше), вони мають повні, нічим не обмежені права доступу.

Тепер звернемо увагу ще на одну особливість Windows: якщо при запуску процесом оновлення зовнішнього додатка маркер безпеки не переданий йому явно (що відбувається тільки в особливих випадках), то дочірній процес успадковує контекст безпеки від батьківського процесу [2, с.45]. З урахуванням цієї особливості стає очевидною доцільність використання серверних модулів систем автоматичного оновлення саме як системних служб, що дозволяє не тільки виконувати будь-які дії за допомогою самих серверних модулів, але й запускати на виконання інші процеси оновлення в контексті безпеки системного облікового запису.

Після запуску запускається вбудований сервер TCP і сервер UDP, останній з яких служить для пошуку запущених серверних модулів у мережі клієнтським модулем, та який опитує мережу на предмет наявності запущених серверних модулів шляхом відправки клієнтським модулем по протоколу UDP на відповідний порт широкомовного пакету. Серверний модуль, одержавши такий пакет, відправляє IP-адресу машини, на якій він виконується, на адресу, з якого прийшов широкомовний пакет. Клієнтський модуль, таким чином, формує список адрес машин, на яких запущені серверні модулі. Потім цей список використовується при виконанні всіх операцій із серверними модулями в поточному сеансі роботи.

Даний спосіб опитування мережі на предмет наявності запущених серверних модулів можна вважати одним із найбільш ефективних. Одержавши відповідь від серверного модуля, клієнтський модуль вже точно знає, що на цій машині встановлений і запущений серверний модуль.

Режим прямого управління використовується, коли адміністратор виконує всі операції в межах однієї локальної мережі. При цьому клієнтський модуль відправляє серверним модулям команди і дані відповідно до дій, що виконує адміністратор.

Режими формування й установки оновлень незамінні при дистанційному супроводі продукту. Для роботи системи автоматичного оновлення в цих режимах потрібно підключення до мережі Інтернет. Відправлення й одер-

ISSN 1727-1584

жання оновлень відбувається з використанням стандартних поштових протоколів SMTP і POP3. Структура усіх оновлень приблизно однакова: оновлення являє собою поштове повідомлення; тема повідомлення містить короткий опис оновлення, що вводиться при формуванні оновлення; тіло повідомлення являє собою текстовий конфігураційний файл, що містить команду, яка має бути передана серверним модулям при установці оновлення, і при необхідності додаткові параметри команди (наприклад, ім'я каталогу призначення при копіюванні файлів). Якщо для виконання команди необхідні які-небудь додаткові дані (наприклад, архів з файлами при виконанні операції копіювання файлів), то вони прикріплюються до повідомлення у вигляді вкладеного файлу [3, с.256].

3. Підсистема внутрішнього ліцензування.

Одним із важливих компонентів системи автоматичного оновлення є підсистема ліцензування, що автоматизує процес генерації й установки ліцензійних ключів програмного забезпечення, прив'язаних до конкретного комп'ютера. Справа в тому, що програмні модулі більшості продуктів, супроводжуваних за допомогою системи автоматичного оновлення (наприклад, оболонка для лабораторних робіт), захищені від несанкціонованого копіювання системою захисту програмного забезпечення ASProtect. При використанні даної схеми захисту для кожної встановленої копії треба згенерувати ліцензійний ключ, який залежить від початкових констант, що знаходяться у файлі проекту ASProtect, текстової реєстраційної інформації та унікальних параметрів конкретної машини. Сформований ключ має бути розміщений у системному реєстрі.

Підсистема ліцензування дозволяє автоматизувати цей процес, значно спрощуючи роботу з захищеними програмними продуктами.

Таким чином, у даній статті на конкретному прикладі ми розглянули принципи побудови систем віддаленого адміністрування, автоматичного оновлення і супроводу програмних продуктів. З цього можна зробити наступні висновки:

1. Система має складатися з двох частин: серверної, яка розміщується на кожній машині, і клієнтської, яка встановлюється на одній машині і служить для управління серверними модулями за допомогою команд.

2. Всередині локальної мережі найкраще передавати команди і дані по протоколу TCP, бо він забезпечує гарантовану доставку даних.

3. Опитування машин у локальній мережі щодо наявності запущених на них серверних модулів найкраще здійснювати, відправляючи широкомовний пакет UDP і приймаючи відповіді серверних модулів. Після цього можна скласти список адрес, з яких прийшла відповідь, і працювати з ними по протоколу TCP. Системні функції опитування мережі незручні тому, що вони не завжди знаходять машини в мережі, і після виявлення кожної машини потрібно робити перевірку, чи запущений на ній серверний модуль.

4. В якості серверного модуля краще використовувати не звичайний процес, а системну службу, оскільки вона:

- запускається автоматично при завантаженні системи поза залежністю входу користувача у систему;
- працює в контексті безпеки системного облікового запису і тому може виконувати будь-як дії;
- дозволяє запускати на виконання інші процеси в контексті безпеки системного облікового запису.

5. Для обміну інформацією через мережу Інтернет зручно використовувати звичайні поштові сервери, які підтримують стандартні поштові протоколи SMTP і POP3, тому що це дозволяє обмінюватися інформацією без встановлення безпосереднього з'єднання двох комп'ютерів і при цьому дисковий простір на поштових серверах найчастіше доступно безкоштовний.

6. При пересиланні інформації з поштових каналів доцільно зашифровувати її для захисту від несанкціонованого доступу, а також контролювати цілісність даних, щоб унеможливити випадкову або навмисну їх модифікацію.

7. При пересиланні інформації через мережу Інтернет треба робити ущільнювати передані дані для зменшення їхнього об'єму і прискорення передачі, а також зниження фінансових витрат на пересилання оновлень.

8. Потрібно пам'ятати, що система автоматичного оновлення може порушити безпеку мережі, якщо доступ до неї зможуть одержати неавторизовані користувачі. Її використання має бути дозволене тільки тим користувачам, яким це потрібно для виконання їхніх задач. Треба обмежити загальний доступ користувачів до системи автоматичного оновлення і проводити їхню аутентифікацію, інакше несанкціоноване використання системи може принести значні збитки і понизити загальний рівень безпеки інформаційних ресурсів підприємства.

ЛІТЕРАТУРА

1. Зима В.М., Молдовян А.А., Молдовян Н.А. Безопасность глобальных сетевых технологий. -СПб.: БХВ - Петербург, 2000. -320 с.

2. Бернет С., Пэйн С. Криптография. Официальное руководство RSA Security. -М.: Бином-Пресс, 2002. –384 с.

3. Конеев В.Р., Беляев А.В. Информационная безопасность предприятия. -СПб.: БХВ-Петербург, 2003. -752 с.

Надійшла до редколегії 22.06.2005

ЧЕРНЫШ Л.Г., ЮДИН О.К. ОБЩИЙ ПОДХОД К ПОСТРОЕНИЮ СИСТЕМ ОТДАЛЕННОГО АДМИНИСТРИРОВАНИЯ, АВТОМАТИЧЕСКОГО ОБНОВЛЕНИЯ И СОПРОВОЖДЕНИЯ ПРОГРАММНЫХ ПРОДУКТОВ

Рассмотрена система отдаленного администрирования, автоматического обновления и сопровождения программных продуктов; определены общин подходы к их построению, исследована возможность использования в качестве серверных модулей таких систем системных служб Windows NT/2000/XP.

***

CHERNYSH L.G., JUDIN O.K. GENERAL APPROACH TO CONSTRUCTION SYSTEMS OF THE REMOTE ADMINISTRATION, AUTOMATIC UPDATING AND SUPPORT OF SOFTWARE

The system of the remote administration, automatic updating and support of software is considered; approaches to their construction are determined communities, the opportunity of use is investigated as server modules of such systems of system services Windows NT/2000/XP.