Дослідження проблем інформаційної безпеки в інформаційно-телекомунікаційних мережах

Атаманюк А.В., Джулій В.М., Кльоц Ю.П.
Хмельницький національний університет

Інформаційно-телекомунікаційна мережа надає різні сервіси для організації соціальних взаємовідносин між користувачами (абонентами). На сьогоднішній день найбільш популярними з них є соціальні мережі. З бурхливим ростом кількості користувачів інформаційно-телекомунікаційних мереж виникають і проблеми безпеки в них.

Розглянемо існуючі проблеми інформаційної безпеки в інформаційно-телекомунікаційних мережах, які актуальні для даного дослідження:

1. Використання глобальної мережі Інтернет як розподіленої інформаційно-телекомунікаційної системи. Найбільш вразливими компонентами системи, що часто атакуються, є: сервери; робочі станції; середовище передачі інформації; вузли комутації. Типові інформаційні впливи зловмисників:

- Прослуховування мережевого трафіку. Щоб прослухати трафік (sniffing) мережевий адаптер переводиться в «безладний» режим. У цьому режимі адаптер перехоплює всі мережеві пакети, що проходять через нього, а не тільки призначені даною адресою, як в нормальному режимі функціонування-технології – ARP Spoofing (ARP-poisoning), MAC Flooding і MAC Duplicating. Перехоплення здійснюється з використанням мережевих моніторів, з яких найбільш функціональними є Sniffer Pro від компанії Sniffer Technologies, IRIS Network Traffic Analyzer від компанії EYE і TCP Dump.

Наслідки. Сучасні мережеві протоколи (TCP / IP, ARP, HTTP, FTP, SMTP, POP3 тощо) не мають механізмів захисту (дані передаються у відкритому вигляді). Зловмисник, що перехоплює трафік між сервером і будь-яким вузлом мережі, може заволодіти аутентифікаційними даними користувача (отримати пароль).

Протидія. Відомо ряд методів визначення наявності запущеного сніфера в мережі, наприклад метод пінга, метод ARP, метод DNS і метод пастки.

- Сканування вразливостей. Результатом роботи сканера є інформація про систему, що містить список мережевого обладнання, комп'ютерів з запущеними на них службами, версіями мережевого ПЗ (а отже і вразливостей, властивих даному ПЗ), облікові записи користувачів. Сканування вразливостей зазвичай є етапом, що передує атаку. Саме результати сканування дозволяють точно підібрати експлойти для здійснення безпосереднього НСД.

Виявлення. Само по собі сканування не є незаконним. Однак, якщо сканування з боку зовнішньої, по відношенню до системи, мережі звичайне

явище, то сканування комп'ютерів з внутрішньої мережі – безумовно, інцидент безпеки, що вимагає негайної реакції з боку мережевого адміністратора. Виявити кроки сканування можна, вивчаючи журнали реєстрації міжмережевих екранів (МЕ). Однак такий підхід не дозволяє своєчасно реагувати на подібні інциденти. Тому сучасні МЕ і системи виявлення вторгнень СВВ мають модулі (plug-in), що дозволяють виявити сканування в режимі реального часу. Деякі сканери вразливостей використовують оригінальні методи, що дозволяють здійснювати сканування максимально приховано. Наприклад, в Nmap існують можливості, що дозволяють значно ускладнити виявлення сканування для СВВ.

Протидія. Використання мережевих СВВ, або періодичне вивчення журналів реєстрації МЕ.

- Мережеві атаки. Мережеві атаки можна розділити на: атаки, засновані на переповненні буфера (overflow based attacks). Вони використовують вразливість системи, яка полягає в некоректній програмної обробці даних. При цьому з'являється можливість виконання шкідливого коду з підвищеними привілеями; атаки, спрямовані на відмову в обслуговуванні (Denial Of Service attacks). Атаки не обов'язково використовують вразливості в ПЗ системи, що атакується. Порушення працездатності системи відбувається через те, що дані, що їй посилають, призводять до значної витрати ресурсів системи. Найпростішим прикладом атаки цього типу є атака «Ping Of Death». Суть її в наступному: на комп'ютер жертви надсилається сильно фрагментований ICMP-пакет великого розміру. Реакцією ОС Windows на отримання такого пакету є повне зависання.

- Атаки, засновані на використанні вразливостей в ПЗ мережевих додатків – експлойти (exploit). Даний клас атак заснований на експлуатації різних дефектів в ПЗ. Експлойти є шкідливими програмами, що реалізують відому вразливість в ОС або прикладному ПЗ, для отримання НСД до вразливого хосту або порушення його працездатності. Для експлойтів характерна наявність функцій подавлення антивірусних програм і МЕ. Наслідки застосування експлойтів можуть бути самими критичними. У випадку отримання зловмисником віддаленого доступу до системи, він має практично повний (системний) доступ до комп'ютера. Наступні дії і збиток від них можуть бути такими: впровадження троянської програми, впровадження набору утиліт для приховування факту компрометації системи, несанкціоноване копіювання зловмисником даних з жорстких та зовнішніх носіїв інформації, створення на віддаленому комп'ютері нових облікових записів з будь-якими правами в системі для подальшого доступу як віддалено, так і локально, крадіжка файлів з хешами паролів користувачів, знищення або модифікація інформації, здійснення дій від імені користувача системи.

Протидія. МЕ і СОВ, встановлені на системі, що атакується, в деяких випадків не в змозі відобразити дію експлойтів. Для успішного відображення атак експлойтів засоби захисту необхідно оновлювати, оскільки механізм виявлення вторгнень заснований на розпізнаванні сигнатур вже відомих атак. Хоча є розробки, здатні за завіреннями розробників відображати невідомі атаки, практика показує, що вони все ще не ефективні.

- Шкідливі програми. Шкідливі програми – це комп'ютерна програма або переносний код, призначений для реалізації загроз інформації, що зберігається в мережі, або для прихованого нецільового використання ресурсів або якого іншого впливу, що перешкоджає нормальному функціонуванню мережі. До шкідливих програми відносяться комп'ютерні віруси, троянські коні, мережеві черв'яки тощо.

Протидія. Типовим методом протидії є застосування антивірусних засобів, що працюють в режимі реального часу (моніторів). Для виявлення троянських програм існує спеціалізоване програмне забезпечення.

2. Проблема забороненого контенту. Залежно від законодавства країни різні матеріали можуть вважатися нелегальними. У більшості країн заборонені: матеріали сексуального характеру за участю дітей і підлітків, порнографічний контент, описи насильства, в тому числі сексуального, екстремізм і розпалювання расової ненависті. В українському законодавстві кілька законів регулюють питання надання інформації про фізичних та юридичних осіб, а саме: Закон України «Про інформацію» від 02.10.92, що регулює відносини щодо одержання і поширення інформації; Закон України «Про захист персональних даних» від 01.06.2010, що визначає захист і обробку персональних даних; Закон України «Про доступ до публічної інформації» від 13.01.2011, який надає право на отримання інформації, що знаходиться у володінні розпорядників.

Аналогічно з концепцією забезпечення комплексного захисту об'єкта інформатизації, можна сформувати повну множину функцій захисту від забороненої інформації. Під функцією захисту (ФЗ) розуміється сукупність однорідних в функціональному відношенні заходів, що регулярно здійснюються в автоматизованих системах різними засобами і методами з метою створення, підтримки і забезпечення умов, об'єктивно необхідних для надійного захисту інформації.

Перелік повної множини функцій захисту від забороненої інформації в соціальних мережах:

1. Попередження умов виникнення забороненої інформації. Функція реалізується за допомогою нормативно-правових актів. Вона не може повністю виключити загрозу поширення забороненої інформації в соціальних мережах, так як в цілому ситуація з дотриманням законів незадовільна, а в інтернет-просторі загострюється через технічні складнощі.

2. Попередження безпосередньої прояви забороненої інформації. Функція реалізується за рахунок механізмів прогнозування поширення забороненої інформації в соціальній мережі.

3. Виявлення забороненої інформації, яка проявилася. Функція пов'язана з моніторингом ІТКМ на предмет забороненої інформації на сторінках абонентів. Як правило, для реалізації даного захисту використовується різні СОРМ (система оперативно-розшукових заходів). Дана ФЗ пов'язана з проблемами контекстного пошуку, а також необхідністю контролю над всією системою.

4. Попередження впливу на абонентів забороненої інформації, яка проявилася. Функція може бути реалізована за допомогою автоматичного пересилання повідомлення з попередженням про відповідальність за розповсюдження забороненої інформації, аж до блокування абонента. Блокування може здійснюватися легітимними засобами за наявності доступу до керування системи та нелегітимними – при його відсутності (зламання акаунта). ФЗ ділиться на дві функції. Перша пов'язана з попередженням абонентів, на сторінках яких була знайдена заборонена інформація, а друга – з розсилкою попереджень потенційним одержувачам забороненої інформації.

5. Виявлення впливу забороненої інформації на абонентів. Функція пов'язана безпосередньо з фіксацією процесу поширення забороненої інформації, може бути реалізована через контекстний аналіз повідомлень.

6. Локалізація, обмеження впливу забороненої інформації на абонентів. Функція реалізується через блокування абонентів, що поширюють заборонену інформацію, або абонентів – потенційних розповсюджувачів. Дана ФЗ опирається на попередні функції і для її ефективної реалізації необхідний контроль над системою.

7. Ліквідація наслідків виявленого впливу забороненої інформації на абонентів. Функція пов'язана з видаленням забороненої інформації з системи. Для реалізації даної функції також необхідний контроль над системою.

На основі проведеного аналізу функцій захисту видно, що найбільш ефективні функції – це перші функції, оскільки вони забезпечують захист на початкових етапах. Наведені функції захисту мають свої недоліки. Найбільш перспективною ФЗ інженерно-технічного напряму є $ФЗ_2$. На даному етапі, маючи інформацію про топології ІТКМ і потенційних розповсюджувачів забороненої інформації, можливе прогнозування процесу її поширення.

Одним з підходів до прогнозування загрози поширення забороненої інформації (ЗПЗІ) є моделювання, наприклад, з використанням моделей впливу, моделей просочування і зараження. Дані моделі, як правило, не враховують топологічні особливості мережі (розподіл ступенів зв'язності, кластерний коефіцієнт, середня довжина шляху). Взаємодія між абонентами в межах цих математичних моделей описується переважно гомогенним

графом, що при моделюванні великомасштабних мереж (більше 10 млн. вузлів) може дати похибку прогнозування загрози поширення забороненої інформації більше 30%. Крім того, дані підходи мають в основному теоретичний характер, практика їх використання не виходить за межі експериментів. Таким чином, дослідження, спрямовані на створення моделей та алгоритмів загрози поширення забороненої інформації, актуальні і мають теоретичне і практичне значення у вирішенні проблеми забезпечення інформаційної безпеки в системах і мережах телекомунікацій.

Прведене дослідження проблем інформаційної безпеки виявило, що крім проблем, пов'язаних з використанням глобальної мережі Інтернет як розподіленої інформаційно-телекомунікаційної системи, які досить добре відомі і можна вирішити, існує маловивчена проблема забороненого контенту, існуючі рішення малоефективні.

Ще однією важливою проблемою є великомасштабність ІТКМ, яка заважає отримати дані з імітаційної моделі за прийнятний час. Розв'язання цієї задачі полягає у створенні аналітичної моделі загрози поширення забороненої інформації в ІТКМ.

Перелік посилань

1. Биячуев, Т.А. Безопасность корпоративных сетей: учеб. пособие / Т.А. Биячуев; под ред. Осовецкого Л.Г. – СПб.: СПбГУ ИТМО, 2016.– 161 с.

2. Лукацький, А.В. Предотвращение сетевых атак: технологии и решения / А.В. Лукацкий. – СПб. : Экспрес Электроника, 2014. – 268 с.

3. Тропіна М. Дослідження соціальних мереж як нового феномену сучасного світу / М. Тропіна // Наукові записки Малої академії наук України. Серія «Педагогічні науки» : [зб. наук. праць ; редкол. : С.О. Довгий (голова), О.Є. Стрижак, О.В. Лісовий, І.М. Савченко та ін.]. — Київ : Національний центр «Мала академія наук України», 2019. — Вип. 16. – С. 57-63

Модель тренувального процесу та метод обробки музичних даних програмної системи генерування музичних творів із використанням штучного інтелекту

Бабич І.Р.
Науковий керівник – к.т.н., доцент Яшина О. М.
Хмельницький національний університет

В основі моделі тренувального процесу системи генерування музичного контенту лежить удосконалене розуміння музичної структури та чітке передбачення нотних даних із наданням можливості генерування поліфонічної музики (коли одна нота на один крок у часі[1]), що узгоджується із музичними правилами.