

УДК 303.7

Петелін Д.Д.¹, Зайко Т.А.²

¹ студ. гр. КНТ-142м НУ «Запорізька політехніка»

² канд. техн. наук, доц. НУ «Запорізька політехніка»

СИСТЕМИ ВІЗУАЛІЗАЦІЇ SCADA

Системи диспетчеризації, керування та збору даних – SCADA (Supervisory Control and Data Acquisition) є основним та найбільш перспективним методом автоматизованого керування складними динамічними системами та процесами у життєво важливих та критичних, з точки зору безпеки та надійності, областях.

SCADA-системи в ієрархії програмно апаратних засобів промислової автоматизації знаходяться на верхньому рівні. Якщо спробувати стисло охарактеризувати основні функції, то можна сказати, що SCADA-система збирає інформацію про технологічний процес, забезпечує інтерфейс з оператором, зберігає історію процесу і здійснює управління процесом в тому об'ємі, в якому це необхідно.

Залежно від складності керованого технологічного процесу, а також вимог до надійності, SCADA-системи будуються по одній з наступних архітектур:

- автономні. При використанні даної архітектури система складається з однієї або декількох робочих станцій оператора, що не «знають» один про одного. Всі функції системи виконуються на одній (декількох незалежних) станцій. Переваги – простота. Недоліки – низька відмова стійкість, не забезпечується істинність даних (історичні дані можуть відрізнятись між різними станціями).

- клієнт-серверні. В даному випадку система виконується на сервері, а оператори використовують клієнтські станції для моніторингу та управління процесом. Високонадійні системи будуються на базі подвійного або потрійного резервування серверів і дублювання клієнтських станцій оператора, дублювання здійснювати підключення до мережі сервер-сервер і клієнт-сервер. При даній архітектурі вже можливо поділ функцій SCADA-системи між серверами. Наприклад, збір даних і управління ПЛК виконується на одному сервері, архівування даних – на другому, а взаємодія з клієнтами – на третьому.

- розподілені. При використанні архітектури розподіленої системи управління (PCY) обчислення здійснюються на декількох взаємопов'язаних обчислювальних пристроях, часто з функцією взаємного резервування. Розподілені SCADA-системи з взаємним резервуванням відрізняються підвищеною надійністю.

Системи SCADA, які об'єднують децентралізовані об'єкти, такі як енергетичні, нафтові, газові трубопроводи, системи розподілу води та збору стічних вод, були розроблені, щоб бути відкритими, надійними і легко керованими. Перехід від пропріетарних технологій до більш стандартизованих та відкритих рішень разом із збільшенням кількості з'єднань між системами SCADA, офісними мережами та Інтернетом зробив їх більш уразливими для типів мережних атак, які відносно поширені в комп'ютерній безпеці. Було опубліковано попередження про уразливості, яке містило інформацію про те, що не пройшли перевірку автентичності користувачі можуть завантажувати конфіденційну інформацію про конфігурації, включаючи хеши паролів, системи індуктивного автоматичного запалювання, використовуючи стандартний тип атаки, забезпечує доступ до TomcatEmbedded. Таким чином, безпека деяких систем на основі SCADA була поставлена під сумнів, оскільки вони розглядалися як потенційно уразливі для кібератак.

Підвищений інтерес до вразливостей SCADA призвів до того, що дослідники виявили проблеми в комерційному проектуванні SCADA-систем і більш загальні наступальні методи, представлені для загального співтовариства безпеки. У SCADA системах з електричними і газовими утилітами вразливість великої встановленої бази дротяних і бездротових послідовних каналів зв'язку в деяких випадках усувається шляхом застосування пристроїв з шипами в кабельній мережі, які використовують аутентифікацію і шифрування розширеного шифрування, а не замінюючи всі існуючі вузли.

Найпоширеніші типи вразливостей SCADA-систем: вразливості аутентифікації вузлів в результаті «слабких» паролівних налаштувань (Authentication). Уразливості шифрування через використання «слабких» криптографічних алгоритмів і систем управління ключами (Key Management); уразливості через помилки конфігурації SCADA-систем, часто виробник системи встановлює неоптимальні політики безпеки або за замовчуванням встановлює адміністративні права доступу; уразливості, викликані відсутністю оновлень безпеки для різних версій SCADA-систем або несвоєчасністю їх установки; уразливості програмно-апаратних компонент, що дозволяють використовувати DoS-атаки для автоматичного виконання протоколів аварійних або позаштатних ситуацій, завершення або «зависання» програм, експлуатації в системі шкідливого коду.

Використання інформаційних систем і технологій пов'язано з певною сукупністю ризиків. Оцінка ризиків, перш за все, необхідна для контролю ефективності діяльності цих систем в області інформаційної безпеки, прийняття цільових заходів і створення економічно – ефективних заходів для захисту системи. Важливо пам'ятати, що добросовісно виконана і ретельно

проведена перша оцінка може істотно полегшити подальшу діяльність, зв'язану з забезпеченням безпеки системи.

Шкала якісної оцінки захищеності варіюється наступним чином:

- 0-25% – низький рівень захищеності системи;
- 26-75% – середній рівень захищеності системи;
- 76-100% – високий рівень захищеності системи.

Як правило, такі уразливості пов'язані з помилками програмістів – виробників SCADA. Помилка в програмі може дозволити зловмиснику використовувати відкриті порти для запуску шкідливого коду в системі, проведення DoS-атаки для переповнення розміру буферу даних і т.п.

Одним із способів захисту від вразливостей, а відповідно й від атак, що ґрунтуються на них, є вчасне виявлення та усунення проблем, що пов'язані з безпекою. Тому необхідно використовувати методи/підходи, на основі яких буде перевірятись та оцінюватись стан захищеності SCADA системи. Також, такі перевірки є важливими з точки зору попередження атак на систему при вчасному виявленні та виправленні слабких місць, що наявні в системі.