УДК 004.056

Системи виявлення вторгнень в системи автоматичного управління підприємств на основі аналізу аномалій

Якименко М.С., доцент кафедри вищої математики та фізики, к.ф.-м.н., доцент
mykola.yakymenko@gmail.com
Кіровоградський національний технічний університет, м. Кіровоград

В останній час у захисті інформації все більшу актуальність набувають системи виявлення вторгнень (Intrusion detection system, IDS) та системи запобігання вторгнень (Intrusion prevention system, IPS). В даній роботі звертається увага на важливість наявності систем виявлення вторгнень та, зокрема, деякі види таких систем, що базуються на виявленні аномалій.

Крім загальної потреби захисту інформації в комп'ютерних системах і мережах на сьогодні в умовах інформаційної війни вторгнення в роботу підприємств несе небезпеку не тільки безпеці даних, але й роботі фізичних пристроїв. Останнім часом, зважаючи на все більшу автоматизацію, великій небезпеці підлягають енергогенеруючі, енергорозподіляючі компанії, безпеці яких приділяється багато уваги [1]. Наприклад, вторгнення в системи 3-х українських обленерго 23 грудня 2015 року призвели до відключення електроенергії не менше, ніж у 230 тис. споживачів. Ця подія привернула багато уваги у світі, так як це був перший відомий випадок успішної кібератаки на об'єкти електроенергетичної галузі.

Згідно попередніх висновків [2] розслідування, яке проводилося українськими органами сумісно із представниками ICS-CERT, та іншими міжнародними експертами, було встановлено, зокрема, що від першого втручання (за допомогою зловмисних макросів у офісних документах) до самої атаки пройшло близько півроку, протягом яких зловмисниками проводилося розвідка системи, її картографування і створення закладок. Після атаки енергопостачання було відновлено протягом кількох годин, проте автоматичні вимикачі, в яких була змінена прошивка, вийшли з ладу на значно довший час і перемикалися тривалий час в ручному режимі.

Слід відмітити, що системи захисту комп'ютерної мережі однієї із атакованих організацій, «Прикарпаттяобленерго», були (за свідченням експертів, що проводили розслідування) кращими, ніж у деяких енергорозподільчих компаніях США, що ще раз підтверджує думку, що ефективною може бути тільки побудова комплексної багаторівневої системи захисту.

В подібних ситуаціях значну користь можуть приносити системи виявлення втручань (Intrusion detection system, IDS) [3]. Не торкаючись питань розташування систем виявлення втручань (мережні чи вузлові) розглянемо їх класифікацію за методом аналізу. Виділяють 2 типи IDS: системи, що засновані на виявленні зловживань (з тих, які входять до бази даних), та на виявленні аномалій при статистичному аналізі роботи системи. Більш поширеними серед програмних продуктів є методи першої групи, але вони чутливі до регулярного оновлення баз виявлення (т.зв. вразливість нульового дня), поліморфних змін коду тощо. В реальності системи виявлення вторгнень є гібридними і поєднують як методи аналізу, засновані на виявлені зловживань, так і методи виявлення аномалій.

Перспективними виглядають системи виявлення вразливостей, що базуються на виявленні аномалій поведінки компонент системи. Інтенсивно використовуються методи [4], які використовують елементи штучного інтелекту, машинне навчання (штучні нейронні мережі, метод опорних векторів, кластерний аналіз, Байєсовські мережі, генетичні алгоритми), методи big data, а також їх поєднання. Ще однією групою є методи, засновані на нечіткій логіці [5].

Всі методи другої групи [6] є досить гнучкими до виявлення нових видів атак, проте вимагають налаштовувань під конкретну систему, часто мають велику кількість фальшивих спрацьовувань, все ще споживають багато апаратних ресурсів, вимагають часу для вивчення «нормального» стану системи.

Враховуючи хаотичну будову трафіку із властивостями самоподібності [7] запропоновано досліджувати параметри хаотичних систем, такі як, наприклад, фрактальна розмірність, параметр

Херста [8, 9], показник Ляпунова [10]. Основна ідея цих методів полягає у визначенні наскільки вказані параметри відрізняються у «нормальному» та «аномальному» станах.

Тісно пов'язаними з останніми є методи, що використовують моделювання трафіку нелінійними динамічними системами за допомогою методів теорії детермінованого хаосу [11, 12]. В роботі [12] для виявлення аномалій в роботі системи в умовах зовнішніх перешкод використовується модель брюсселятора. Для покращення роботи доцільним також є використання інших моделей динамічних систем для виявлення різних видів атак.

Для підвищення ефективності роботи систем захисту на підприємствах слід проводити більш широке запровадження тестів на проникнення, використання яких важливе також при роботі систем виявлення аномалій для перевірки адекватності різних видів моделей, може бути корисним в роботі комплексних IDS із методами машинного навчання.

Список літератури

1. Pasqualetti F. Attack detection and identification in cyber-physical systems / F. Pasqualetti, F. Dorfler, F. Bullo // Automatic Control, IEEE Transactions on. — 2013. — Vol. 58, No. 11. — P. 2715–2729
2. Alert (IR-ALERT-H-16-056-01) cyber-attack against ukrainian critical infrastructure / [Електронне джерело]. – 2016. – Режим доступу: https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01
3. Sharma S. Intrusion detection system: a review / S. Sharma, R. Gupta // International Journal of Security and Its Applications. — 2015. — Vol. 9, No. 5. — P. 69–76
4. Большев А. К. Алгоритмы преобразования и классификации трафика для обнаружения вторжений в компьютерные сети: авторефер. дисс. на соискание научн. степени канд. техн. наук: спец. 05.13. 19–методы и системы защиты информации, информационная безопасность / А. К. Большев. – Санкт-Петербург, 2011. – 36 с
5. Корченко А. Г. Построение систем защиты информации на нечетких множествах / А.Г. Корченко. — К.: МК-Пресс, 2006
6. Agrawal S. Survey on anomaly detection using data mining techniques / S. Agrawal, J. Agrawal // Procedia Computer Science. — 2015. — Vol. 60. — P. 708–713
7. Fiore U. Network anomaly detection with the restricted Boltzmann machine / U. Fiore, F. Palmieri, A. Castiglione, A. De Santis // Neurocomputing. — 2013. — Vol. 122. — P. 13–23
8. Sheluhin O. Detection of anomalies in network traffic using the methods of fractal analysis in real time / O. Sheluhin, A. Pankrushin // T-Comm-Телекоммуникации и Транспорт. — 2014. — Vol. 8, No. 8. – P.108-112
9. Басараб М. А. Обнаружение аномалий в информационных процессах на основе мультифрактального анализа / М.А. Басараб, И.С. Строганов // Вопросы кибербезопасности. — 2014. — No. 4 (7). – С. 30-40
10. Ren X. Fractal Lyapunov exponent based anomaly detection of network traffic. / X. Ren, H. Wan, others // International Journal of Advancements in Computing Technology. — 2012. — Vol. 4, No. 11. – P. 275-282
11. Palmieri F. Network anomaly detection through nonlinear analysis / F. Palmieri, U. Fiore // Computers & Security. — 2010. — Vol. 29, No. 7. — P. 737–755
12. Семенов С.Г. Аппроксимация технологии функционирования компьютерной системы в условиях внешних воздействий моделью брюсселятора с возмущениями в виде динамического хаоса / С.Г. Семенов, А.Ю. Можаев, С.Ю. Гавриленко // Системи обробки інформації. — 2014. — No. 4. — С. 188–191