УДК 004.056

ВРАЗЛИВОСТІ СИСТЕМ КЕРУВАННЯ

В. В. Чужда[1, a], С. А. Смирнов[1]

[1] *Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Фізико-технічний інститут*

Анотація

В доповіді розглядаються актуальні вразливості, виявленні в системах керування. Також звертається увага на ПІД-регулятори, а саме на основні помилки в їх реалізації, які можуть привести до вразливості системи керування перед нападником.

Ключові слова: ПІД-регулятори, кібербезпека, теорія керування

Вступ

В епоху поширення інтернету речей, безпілотних машин, та інших технологій, питання безпеки, приватності та надійності все частіше і частіше постають перед людьми. Збитки при реалізації загрози виростають з кожним роком, і, відповідно, необхідність в своєчасному усуненні загроз є завжди актуальною, – щоб підтвердити це, поглянемо на останні тренди в сфері захисту систем керування [1].

В ході конференції DefCon, що проходила в серпні 2016 року в Лас Вегасі (США), дослідник Ендрю Тірні показав, як можна зламати термостат. Після того, як він отримав контроль над ним (вставивши в нього SD-карту), температура піднялася до 99 градусів за Фаренгейтом (приблизно 37 градусів за Цельсієм), скасувати яку можна було тільки за допомогою PIN-коду. Термостат, підключений до IRC-каналу, вимагав біткоіни за отримання PIN-коду. Хоча це була всього лише демонстрація концепції, а до пристрою все ж був необхідний фізичний доступ, ми можемо зрозуміти, що атаки, з якими ми зіткнемося в найближчому майбутньому, будуть безпосередньо спрямовані на величезну кількість побутових пристроїв, підключених до Мережі. І це вже реальність, адже мільйони пристроїв з «Інтернету речей» були скомпрометовані. Бот-мережа LizardStressed, створена групою Lizard Squad, запустила руйнівну DDoS-атаку одночасно проти Playstation і Xbox, при цьому в основному вона складалася з подібного роду пристроїв. За даними Arbor Networks, більшість таких пристроїв є IP-камерами, і вони можуть бути зламані просто за рахунок перебору комбінацій «ім'я користувача - пароль», так званого «brute force». Оскільки багато користувачів не змінюють реєстраційні дані, встановлені виробниками за замовчуванням, то отримати до них доступ досить просто. Уже запускалися атаки до 400 Гбіт/сек. Інший улюблений пристрій, що використовується для подібного роду атак – це роутери, причому вони використовуються вже досить тривалий час.

В кінці вересня французька хостінг компанія OVH зіткнулася з масивної DDoS-атакою, що досягала 799 Гбіт/сек. А в кінці атаки трафік перевищив 1 Тбіт/сек. Дивлячись на дані, надані OVS, ми бачимо, що атака була запущена з 152000 пристроїв, а більшість з них належали до категорії «Інтернет речей» (IP-камери, відеореєстратори та ін.).

Що стосується автомобільної сфери, то дослідники з Університету Бірмінгема продемонстрували, як вони змогли зламати системи відкриття дверей на будь-яких автомобілях, проданих Volkswagen Group за останні 20 років. Через реверс інжиніринг, вони зуміли це зробити за допомогою криптографічного ключа, що використовується всіма машинами VW. Після отримання ключа їм довелося стояти на відстані 300 метрів від цільового автомобіля в очікуванні певної команди на радіопристрої, щоб перехопити інший ключ, унікальний для кожного автомобіля. Після отримання цієї інформації вони змогли легко клонувати пульт дистанційного керування, який відкриває і закриває двері машини.

Дослідники Чарлі Міллер і Кріс Валашек, які в минулому році показали, як можна віддалено зламати Jeep Cherokee, в цьому році пішли ще далі, показавши, як можна перехопити сигнали і відключити стоянкове гальмо, відключити кермо або по команді повернути його на будь-якій швидкості. На відміну від попередньої ситуації, щоб отримати контроль над машиною, їм довелося безпосередньо підключити до неї комп'ютер.

У вересні 2016 року китайські вчені з Keen Security Labs показали, як віддалено зламати машину Tesla, припарковану або таку, що перебуває в русі. Можна віддалено контролювати машину без фізичного контакту з нею: можна відкрити або закрити двері, при русі машини можна відкрити багажник, вони навіть змогли віддалено контролювати гальма. Вчені заздалегідь відправили інформацію виробникам, щоб

[a] v.14.15.24.32.34.43.a@gmail.com

вони змогли виправити виявлені проблеми в останній версії своєї прошивки.

Отже, зважаючи на сучасний стрімкий розвиток технологій систем керування, вразливості в них отримують все більшу і більшу важливість.

1. Досліджуванні вразливості

Вразливість гіроскопу

Вразливість виявлена працівниками університетів Мічигану та Південної Кароліни [2]. Вона полягає у відсутності валідації сигналів, отриманих від гіроскопу, вбудованого у телефони, пристрої інтернету речей, дронів та інші технічні засоби. За допомогою навмисних акустичних перешкод виникає можливість доставити певні цифрові значення до мікропроцесорів, або вбудованих систем.

Наприклад, використання цієї вразливості для перехвату керування над автомобілем. Атакуються не безпосередньо системи автомобіля, а телефон, який ним керує, а саме Samsung Galaxy S5, який має програмне забезпечення для дистанційного керування автомобілем. Користувач може нахилами смартфону змінювати напрям руху автомобіля. При атаці на телефон та підміні сигналу можна створити умови для ДТП, спрямовуючи автомобіль у потрібний нам напрямок.

В таблиці 1 наведений список акселерометрів, які на даний момент були протестовані на цю вразливість.

Табл. 1. Таблиця пристроїв, протестованих на наявність вразливості до інтерференції на частоті 110 ДБ

Модель сенсора	Вразливість
BMA222E	Вразливий
MIS2DH	Вразливий
IIS2DH	Вразливий
LIS3DSH	Вразливий
LIS344ALH	Вразливий
H3LIS331DL	Вразливий
MPU6050	Вразливий
MPU6500	Вразливий
ICM20601	Вразливий
ADXL312	Вразливий
ADXL337	Вразливий
ADXL345	Вразливий
ADXL346	Вразливий
ADXL350	Вразливий
ADXL362	Вразливий
SCA610	Невразливий
SCA820	Вразливий
SCA1000	Невразливий
SCA2100	Невразливий
SCA3100	Вразливий

Як протидіяти

Два найбільш ефективні методи протидії, – це:

1) Оточення акселерометру шумопоглинаючою піною.
2) Алгоритми ігнорування аномальних сигналів.

Можливість проведення даної атаки залежить від 3-х наступних факторів:

- Можливість доставки високо амплітудних та довільно модульованих акустичних перешкод в безпосередній близькості до сенсора.
- Знання резонансної частоти датчика.
- Знання методів обробки даних та алгоритму управління поведінкою цільової автономної системи.

Наразі не було помічено жодного випадку застосування даної вразливості.

Можливість помітити проведення атаки

Існує 2 підходи до виявлення атаки: виявлення порушень в даних та виявлення акустичної інтерференції. Наприклад, якщо акселерометр, установлений в електрокардіостимуляторі адаптивного темпу, очікує на вхід максимальну амплітуду прискорення, і якщо вхідне значення перевищує її, дані від сенсора можуть бути проігноровані.

У разі, коли той ж самий пристрій або система, які містять датчик, також містять мікрофон, мікрофон може безперервно контролювати навколишнє середовище акустичного шуму. Коли екологічний акустичний шум містить частотні компоненти, які відповідають резонансній частоті уразливого датчика, дані датчиків можуть бути проігноровані.

Вразливість систем аутентифікації

Співробітниками Інституту Технологій Джорджії було виявлено, що низка PLC, які наразі використовуються в більшій частині АСУ ТП, мають доволі низький рівень захисту системи аутентифікації [3]. Вони змогли написати першого в історії хробака-вимагача, який має назву LogicLocker. Він використовує рідні API сокетів Schneider Modicon M241 для сканування мережі на наявність доступних вразливих цілей, таких як MicroLogix 1400 або Schneider Modicon M221, інфікує їх, використовуючи вразливість аутентифікації, блокує доступ користувачам до легкого відновлення початкових налаштувань PLC. Після цих дій вони закладають логічну бомбу, яка змушує систему проводити небезпечні фізичні дії, при цьому ведеться пошук нових цілей для зараження. Тоді розпочинається процес вимагання викупу, і зазвичай, для того, щоб запобігти шкоді для населення, компанії набагато вигідніше просто заплатити викуп.

У таблиці 2 наведені деякі поширені PLC, компрометування яких було підтверджено на практиці.

Табл. 2. Таблиця пристроїв, протестованих на наявність вразливості

PLC Model	Shodan Count
MicroLogix 1400	1429
Schneider Modicon M221	250
Siemens S7-1200	167

При цьому важливо визначити в якому напрямку LogicLocker буде вести пошук нових цілей для

Рис. 1. Горизонтальне поширення

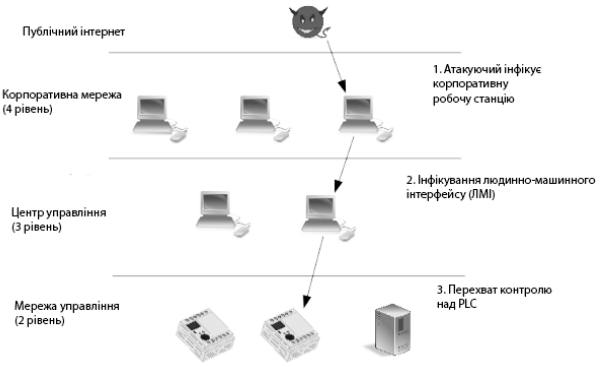

Рис. 2. Вертикальне поширення

Табл. 3. Таблиця пристроїв, протестованих на наявність вразливості

	Горизонтальний	Вертикальний
Переваги	Менша захищеність	Якісне поширення
	Більше контролю	Стандартний вірус
Недоліки	Менше поширення	Більше часу

зараження. Тут є 2 варіанти: горизонтально та вертикально. Схеми зараження показані на рис. 1 та рис. 2 відповідно.

Порівняємо ці два способи у вигляді переваг та недоліків в таблиці 3.

Можливі також комбінації цих двох методів.

Наступним кроком є блокування PLC від змін зі сторони оператора. Для цього є декілька шляхів, перерахуємо їх у таблиці 4.

Зміна паролю на випадковий є найпростішим рішенням, оскільки для того, щоб обминути це обмеження, доведеться витратити багато часу, окрім того, що для злому паролю доведеться писати програмне забезпечення, яке може викликати протест зі сторону розробника PLC. Перебір паролю, протестований на MicroLogix 1400, за умови, що RTT становить 1 мс, при кабелі довжиною 1 м, та при інших сприятливих умовах, займе 657 дні. Інші шляхи можуть включати читання статусів реєстрів в PLC, наприклад активні TCP з'єднання, для простежування спроб відновлення контролю та нанесення шкоди захисному обладнанню, якщо воно буде підключене. Також нападник може спробувати заблокувати PLC використовуючи перевагу обмежених ресурсів. Багато PLC мають обмеження на кількість активних TCP з'єднань, тобто нападник може їх всіх зайняти і таким чином заблокувати PLC. Нарешті він може просто змінити IP-адресу PLC, та номери портів які він прослуховує. Це принесе додаткову плутанину для захисників. Приклад використання вразливості: система очищення води. LogicLocker атакує систему, допустимо PLC яке керує якістю води є вразливим. Тоді LogicLocker змусить систему добавити більшу кількість хлору для очищування і заблокує пристрій. Тепер перед керівництвом виникає непроста ситуація – заплатити викуп, і 100 % запобігти шкоді людям, чи спробувати перехопити контроль, але на це піде невідомо скільки часу, і шкода буде нанесена з високою імовірністю. Логічно, що в даному випадку оптимальним є сплата викупу.

2. Проблеми в реалізації дискретних ПІД-регуляторів, які можуть привести то вразливостей

ПІД-регулятори є найпоширенішими у сучасному світі, згідно деяким даним їх частка серед регуляторів становить $90 \ldots 95\%$ [4, 5]. Однак при цьому, майже 30 % з них налаштовані невірно [6]. Далі розглянуто декілька з основних помилок.

Проблема 1

При використанні рекурентної дискретної схеми:

$$U(n-1) + Kp \cdot (E(n) - E(n-1)) + Ki \cdot E(n) +$$

$$+Kd \cdot (E(n) - 2 \cdot E(n-1) + E(n-2)) = U(n)$$

та при задані граничних значень виду

$$U(n) = \begin{cases} U_{\max}, & U(n) > U_{\max} \\ U_{\min}, & U(n) < U_{\min} \end{cases}$$

При досягненні цих значень регулятор перетворюється в диференційно-прискорюваний, через те, що пропадає інтегральна складова, в результаті якої потужність, яка подається, буде пропорційна зміні настановки або регульованої величини, а не пропорційна різниці між установкою та регульованою величиною.

Проблема 2

Розлянемо приклад реальної системи. Нехай у нас є лампочка з підключеною термопарою. Вона повинна загорітись при $T = 22°\text{C}$ градусах Цельсію, початкова температура $U_0 = 16°\text{C}$. Розпочинаємо процес: $U = 16.1, 16.4, 17, 18, \ldots, 24$, (засвітилась), $\ldots, 60$. На $60°\text{C}$ вона буде з певними коливаннями триматись. Задаємо наступне значення: $600°\text{C}$. Лампочка відразу тухне. Причина банальна, переповнення змінної. Перерахуємо: 540 нев'язка, частота 16 разів на секунду, коефіцієнт пропорційності 20. В результаті маємо: $540 \cdot 20 \cdot 16 = 172800$. Якщо ця змінна є 16-бітною знаковою, тоді отримуємо приблизно -8960.

Табл. 4. Шляхи блокування доступу

Підхід	Важкість	Слабкість
Пароль	Легко	Зазвичай обходяться
Блокування OEM	Легко	Зазвичай обходяться
Використання ресурсів	Сильніше блокування	Важко для реалізації
Зміна IP/портів	Найлегше	Легко знайти

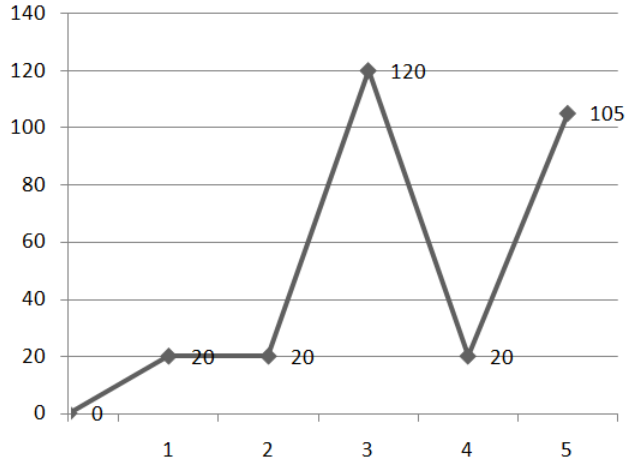

Рис. 3. Процес нагрівання

Проблема 3

Початкову ініціалізацію часто помилково проводять так: всі значення обнуляють, установку зчитують з флеш-пам'яті установки, очікуємо 1-ий цикл, зчитуємо нулі. Беремо отримані значення для 0. І тоді регулятор не працює. Причина: рекурентна формула відштовхується від змін в нев'язці. А якщо проініціювати нулем і загрузити моментальні дані, ми втрачаємо початкові умови. Тепер регулятор замість підтримання абсолютного значення температури на рівні, рівному абсолютній установці, починає тримати температуру, рівну стартовій плюс різниця установки. Наприклад: було 80°C, установили 200°C. Активний пристрій тримає 80°C. Змінюємо на 240°C, пристрій тримає 120°C.

Проблема 4

Наведемо графік процесу на рис. 3

1) $T_0 \to T_1$, $U_{st} = 20^\circ$ C, $U_0 = 0^\circ$ C.
2) $T_1 \to T_2$, $U_{st} = 20^\circ$ C, $U_0 = 20^\circ$ C.
3) $T_2 \to T_3$, $U_{st} = 600^\circ$ C, $U_0 = 20^\circ$ C.
4) $T_3 \to T_4$, $U_{st} = 20^\circ$ C, $U_0 = 120^\circ$ C.
5) $T_4 \to T_5$, $U_{st} = 100^\circ$ C, $U_0 = 20^\circ$ C.

І в результаті отримаємо 105°C замість 100°C. Причина такого полягає у наступному.

У випадку повної схеми, якщо обнуляти в процесі ітеративний процес, ми в тому числі обнуляємо накопичений інтеграл інтегральної складової. Однак у зв'язку з тим, що обнуляємо ми значно раніше, він встигає накопичитись за час довироботку залишку. І взагалі, збільшувати інтеграл на великих перегонах нелогічно, тому, що ціль інтегральної складової – вибрати нев'язку, яку не може обробити пропорційна складова окремо. Отже, якщо з певної причини Un було обмежено, схему необхідно переініціювати як тільки з'явилось враження, що схема повернулась в нормальний стан.

Висновки

При поширенні технологій, таких як гіроскопи, необхідно пам'ятати, що використовуватись вони будуть людьми, які можуть легковажно ставитись до своєї безпеки, тому введення додаткових обмежень для пристроїв керування є доцільним. Сучасні системи керування можуть стати легкою ціллю для нападника, якщо їхні системи аутентифікації будуть ненадійними, та можуть нанести значних збитків суспільству. Не зважаючи на тривале існування ПІД-регуляторів та їх зовнішню простоту, вони потребують уважного ставлення до їх реалізації.

Перелік використаних джерел

1. В 3 квартале 2016 года киберпреступления достигли новых высот // Блог компании Panda Security. — октябрь 2016. — URL: `https://habrahabr.ru/company/panda/blog/313166/`.
2. WALNUT: Waging Doubt on the Integrity of MEMS Accelerometers with Acoustic Injection Attacks / Ti. Trippel, O. Weisse, Xu. Wenyuan et al. // 2nd IEEE European Symposium on Security and Privacy (EuroS&P). — 2017. — URL: `https://spqr.eecs.umich.edu/papers/trippel-IEEE-oaklawn-walnut-2017.pdf`.
3. Formby D., Durbha S., Beyah R. Out of Control: Ransomware for Industrial Control Systems. — 2017. — URL: `http://www.cap.gatech.edu/plcransomware.pdf`.
4. A multi-layer architecture for distributed data acquisition / M. Bertocco, S. Cappellazzo, A. Flammini, M. Parvis // IMTC/2002. Proceedings of the 19th IEEE Instrumentation and Measurement Technology Conference (IEEE Cat. No.00CH37276). — IEEE, 2002. — P. 1261–1264.
5. Astrom K. J., Hagglund T. Advanced PID control. — Instrument Society of America, 2006.
6. Leva A., Cox C., Ruano A. Hands-on PID autotuning: a guide to better utilization. — IFAC Professional Brief, 2006. — URL: `http://www.ifac-control.org/publications/list-of-professional-briefs/pb_final_levacoxruano.pdf`.