регламентували діяльність СБ України, залишила за цим державним органом лише функції спеціальної компетенції як правоохоронного органу.

У жовтні 1997 р. постановою КМУ № 1126 затверджена «Концепція технічного захисту інформації в Україні», яка визначала основи державної політики у сфері захисту інформації інженерно-технічними заходами і засобами. Реалізація Концепції забезпечувала єдність принципів формування і проведення державної політики в усіх сферах життєдіяльності особи, суспільства та держави. Зазначено, що необхідність розвитку ТЗІ зумовлена зростанням загроз для інформації, спричинених лібералізацією суспільних та міжнародних відносин, кризовим станом економіки, застосуванням технічних засобів оброблення інформації та засобів зв'язку іноземного виробництва, поширенням засобів несанкціонованого доступу до інформації та впливу на неї. На виконання положень «Концепції технічного захисту інформації в Україні», 16 лютого 1998 р. постановою № 180 Кабінетом Міністрів України затверджене «Положення про забезпечення режиму секретності під час обробки інформації, що становить державну таємницю, в автоматизованих системах». Це «Положення» визначило основи організації, завдання, права, обов'язки суб'єктів правовідносин та порядок забезпечення режиму секретності під час обробки секретної інформації в автоматизованих системах.

Забезпечення безпеки мікроконтролерних систем у робототехнічних комплексах

УДК 004.056

Гануля Роман , Козбур Ігор

Тернопільський національний технічний університет імені Івана Пулюя, Hanularoma@gmail.com Kozbur.igor@gmail.com

Актуальність проблеми. Мікроконтролерні системи є базовим рівнем керування у сучасних робототехнічних комплексах, включаючи промислові роботи, автономні системи та IoT-пристрої. Зростання кількості підключених пристроїв, а також інтеграція робототехніки у промислові та побутові сфери призводять до значного збільшення кіберзагроз, що можуть суттєво порушити роботу систем, викликати втрату даних або фізичну шкоду. Найпоширенішими проблемами є несанкціонований доступ до апаратного забезпечення, підміна прошивки, перехоплення та модифікація даних у комунікаційних каналах, а також атаки побічними каналами (side-channel attacks), що використовують інформацію про споживання енергії чи електромагнітне випромінювання. За даними NIST [1], більшість сучасних IoT-пристроїв мають критичні вразливості на рівні прошивки та автентифікації, що робить їх потенційною мішенню для атак на робототехнічні комплекси. З огляду на це, забезпечення безпеки мікроконтролерних систем є надзвичайно актуальним завданням, яке поєднує в собі апаратні, програмні та комунікаційні аспекти захисту.

Мета роботи. Метою цього дослідження є аналіз основних загроз безпеці мікроконтролерних систем у робототехнічних комплексах та визначення ефективних методів їх захисту. Крім того, робота спрямована на розробку та дослідження комплексного підходу, що поєднує апаратні та програмні засоби

безпеки з урахуванням специфіки робототехнічних систем, де критичною є робота у реальному часі та обмежені ресурси.

Основні загрози. До ключових загроз мікроконтролерних систем належать:

- фізичний доступ до мікроконтролера – зчитування пам'яті, спроби модифікації внутрішніх даних або заміна компонентів;
- атаки на прошивку (firmware tampering) – несанкціоноване змінення коду, що може призвести до функціональних збоїв або створення несанкціонованих каналів доступу;
- перехоплення даних у комунікаційних інтерфейсах (UART, SPI, I2C) – атаки, що дозволяють отримати або змінити інформацію, що передається між мікроконтролером та периферійними пристроями;
- атаки побічними каналами – використання енергоспоживання, електромагнітного випромінювання або акустичних сигналів для отримання конфіденційної інформації;
- недостатній криптографічний захист та контроль доступу – більшість вбудованих систем не забезпечують надійного шифрування або автентифікації, що збільшує ризик компрометації даних [2].

Методи забезпечення безпеки. Ефективний захист мікроконтролерних систем передбачає використання комплексного підходу, що включає:

- Апаратні механізми захисту – використання TrustZone або Secure Enclave, захист пам'яті (*Read-Out Protection*), контролери доступу до периферії;
- Криптографічний захист – шифрування даних за алгоритмами AES та RSA, цифровий підпис прошивки для підтвердження цілісності коду [3,4];
- Безпечне оновлення прошивки (Secure Boot) – перевірка автентичності та цілісності коду перед запуском, що запобігає виконанню зміненого або шкідливого програмного забезпечення [5];
- Захист комунікацій – використання протоколів TLS/DTLS для забезпечення безпечного обміну даними, автентифікація пристроїв у мережі, контроль доступу до критичних команд управління [6];
- Моніторинг та аудит безпеки – відстеження спроб несанкціонованого доступу, ведення журналів подій, оцінка ризиків на основі логів роботи системи.

Наукова новизна. У роботі запропоновано комплексний підхід до захисту мікроконтролерних систем у робототехнічних комплексах, що поєднує апаратні та програмні засоби безпеки з урахуванням обмежених ресурсів, необхідності роботи у реальному часі та специфічних вимог промислових та автономних роботів. Підкреслено важливість інтеграції різних рівнів захисту: фізичного, програмного та мережевого, а також адаптивного реагування на потенційні загрози.

Висновки. Мікроконтролерні системи у робототехнічних комплексах є критично важливими та водночас вразливими до широкого спектра кіберзагроз, включаючи фізичний доступ, модифікацію прошивки, перехоплення даних та атаки побічними каналами. Більшість сучасних вбудованих систем не забезпечують достатнього рівня криптографічного захисту та контролю доступу. Ефективний захист досягається шляхом комплексного підходу: апаратні механізми (TrustZone, Secure Enclave, Read-Out Protection), програмні засоби (шифрування даних, цифровий підпис прошивки, Secure Boot) та захищені комунікаційні протоколи (TLS/DTLS) з автентифікацією пристроїв. Впровадження цих методів підвищує надійність і стійкість систем до кібератак, а подальші дослідження повинні зосереджуватися на оптимізації захисту для ресурсно-обмежених мікроконтролерів, безпеку робототехнічних комплексів протягом усього життєвого циклу системи.

1. NISTIR 8259. Foundational Cybersecurity Activities for IoT Device Manufacturers. https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8259.pdf
2. OWASP IoT Top 10. https://owasp.org/www-project-internet-of-things/
3. ARM TrustZone Documentation. https://developer.arm.com/documentation/ 100690/latest
4. FIPS 197: Advanced Encryption Standard (AES). https://csrc.nist.gov/publications/detail/fips/197/final
5. Secure Boot. Trusted Computing Group. https://trustedcomputinggroup.org/ resource/secure-boot/
6. RFC 6347: Datagram Transport Layer Security (DTLS). https://datatracker.ietf.org/doc/html/rfc6347

Аналіз методів тестування генераторів псевдовипадкових чисел відповідно до стандартів NIST та ISO

УДК 004.056

Олег Гарасимчук

Національний університет "Львівська політехніка", oleh.i.harasymchuk@lpnu.ua

Генератори псевдовипадкових чисел (ГПВЧ) є невід'ємним елементом сучасних інформаційних систем. Їхнє застосування охоплює значно ширший спектр завдань, ніж традиційно прийнято вважати: від застосувань для моделювання різноманітних процесів до використання в задачах кібербезпеки [1]. Якість вихідних послідовностей ГПВЧ безпосередньо визначає достовірність результатів усіх перерахованих процесів. Хоча в криптографії до ГПВЧ пред'являються найвищі вимоги (необоротність, стійкість до відновлення стану, перевірка за NIST SP 800-22), аналогічна якість випадковості є критичною і для не-криптографічних завдань, де погані ГПВЧ призводять до нерепродукованих результатів фаззингу чи помилкових висновків ML-моделей.

Попри широке практичне застосування, методологія оцінювання якості ГПВЧ у не-криптографічних контекстах залишається недостатньо