УДК 004.056.523+004.354.7
DOI: 10.31673/2409-7292.2024.010012

Нємкова О. А., Чура Н. Р.

ОЦІНКА ПАРАМЕТРІВ МОДЕЛІ СИМУЛЯЦІЇ АВТЕНТИФІКАТОРІВ МІКРОКОНТРОЛЕРІВ

Мікроконтролерні технології є основою для інтелектуальних пристроїв, тому питання кібербезпеки важливі при забезпеченні обміну інформацією між ними. Оскільки ці пристрої утворюють різноманітні інтелектуальні системи, автентифікація стає ключовим аспектом кібербезпеки. Цей процес розрізняє легітимні пристрої від нелегітимних, що дозволяє легітимним пристроям отримувати доступ до ресурсів системи та відхиляти запити від нелегітимних. Сьогодні виникає задача вибору фактору автентифікації для великої кількості однотипних електронних пристроїв в інформаційній системі. Мета цього дослідження – з'ясувати можливість підходу симуляції "біометричного" шаблону автентифікації в програмний спосіб. Для вирішення мети потрібно реалізувати симулятор шаблонів з властивостями біометрики мовою програмування, виконати оцінку розподілу відстаней між парами шаблонів та оцінити параметри генерованих послідовностей з точки зору ймовірності брутфорсу. В даному дослідженні запропоновано рішення задачі, яке поєднує ідеї біометричного фактора та можливості швидкої програмної генерації автентифікаторів для мікроконтролерів. Робота присвячена оцінці параметрів моделі симулятора динамічних бітових шаблонів автентифікації на основі генератора псевдовипадкових імпульсних Пуасонівських послідовностей. У роботі висвітлено основні принципи функціонування симулятора та переваги використання динамічних шаблонів для забезпечення кібербезпеки електронних пристроїв, побудованих на основі мікроконтролерів. Виконано оцінки основних параметрів моделі симулятора. Результати роботи важливі для розвитку безпеки електронних систем та засобів автентифікації в контексті кібербезпеки мікроконтролерів.

Ключові слова: кібербезпека, автентифікація мікроконтролерів, динамічні бітові шаблони, модель симулятора, генератор псевдовипадкових імпульсних Пуасонівських послідовностей.

Вступ

Мікроконтролерні технології є основою для інтелектуальних пристроїв, тому питання кібербезпеки важливі при забезпеченні обміну інформацією між ними. Оскільки ці пристрої утворюють різноманітні інтелектуальні системи, автентифікація стає ключовим аспектом кібербезпеки. Цей процес розрізняє легітимні пристрої від нелегітимних, що дозволяє легітимним пристроям отримувати доступ до ресурсів системи та відхиляти запити від нелегітимних.

Існують кілька різних факторів до автентифікації [1]. Перший фактор - це знання, яке базується на введенні правильного паролю для підтвердження легітимності суб'єкта (пристрою чи людини). Наприклад, для пристроїв таким паролем може бути їх MAC-адреса мережевої карти. Однак такий пароль є статичним, що створює ризик його перехоплення або застосування техніки брутфорсу – підбору паролю методом послідовного перебору варіантів.

Другим фактором є підтвердження легітимності шляхом володіння унікальною річчю, такою як токен або електронний ключ. Наприклад, деякі комп'ютерні програми вимагають під'єднання токена до персонального комп'ютера для забезпечення інформаційної безпеки. Аналогічно до цього для людини може бути використаний цифровий електронний підпис (ЕЦП), що часто використовується для підтвердження особистості в мережі Інтернет. Недоліками цього підходу є можливість втратити токен або обмеження часу дії ЕЦП, а також складність надання їх у потрібний момент часу.

Третім фактором є використання біометричних даних, таких як відбитки пальців або голосу, для підтвердження легітимності. Початково цей підхід був розроблений для людей, але згодом його почали застосовувати і до електронних пристроїв, включаючи мікроконтролери. Виявилося, що для створення унікального шаблону автентифікації можна використовувати різні фізичні характеристики, такі як спектр електромагнітного випромінювання або електричні наведення (шуми) [2-7]. Експериментальні дослідження показали, що цей підхід дозволяє з високою точністю відрізняти серійні пристрої. Перевагами цього методу є його динамічність та практична неможливість підробки. Однак недоліками є необхідність спеціалізованого обладнання для вимірювання та складність обробки отриманих

даних, а також можливість помилок автентифікації. Для автентифікації мікроконтролерів та інтегральних схем також застосовують методики, що основані на фізично не клонованих функціях (PUF) [8, 9]. Таким чином, виникає задача вибору фактору автентифікації для великої кількості однотипних електронних пристроїв в інформаційній системі. В даному дослідженні запропоновано рішення задачі, яке поєднує ідеї біометричного фактора та можливості швидкої програмної генерації автентифікаторів для мікроконтролерів.

Аналіз літератури

Під час технологічних процесів виготовлення інтегральних схем відбуваються випадкові відхилення від заданих параметрів: концентрацій донорних чи акцепторних домішок, геометрії транзисторів, товщини оксидного шару або інші технологічні неточності. Це призводить до неоднаковості кожного мікроскопічного транзистора інтегральних схем ТТЛ (транзисторно-транзисторної логіки) [10], що у свою чергу впливає на значення порогових напруг транзисторів, швидкості наростання та спадання фронтів імпульсів, різних затримок у розповсюдженні сигналів в залежності від шляху та інше. Ці неконтрольовані явища використовують для ідентифікації цифрових пристроїв. Наприклад, виробники FPGA Xilinx і Altera (Intel) використовують PUF у якості вбудованого не клонованого ідентифікатора ПЛІС (програмована логічна інтегральна схема) [11, 12].

Фізично не клоновані функції на основі затримки сигналу (кільцеві генератори) використовують неоднаковість часу проходження декількох копій одного сигналу через задані конфігурації симетричних шляхів. Запитом, що задається у двійковому вигляді, у даному випадку є конфігурація шляхів, відповіддю є результат порівняння затримок часу розповсюдження сигналів [13]. Фізично не клоновані функції на основі стану статичної пам’яті (SRAM) використовують унікальність значень бітів, що зберігаються у кожному елементі пам’яті. В результаті скидання стану елементів пам’яті (польових транзисторів) спостерігається зміна значень (0 або 1), для кожного чипа це унікальна конфігурація [14].

Одна з основних проблем наведеного прикладу PUF на основі статичної пам’яті є нестабільність деяких значень стану, що вимагає застосування кодів корекції похибок. Друга проблема полягає у старінні польових транзисторів з плаваючим затвором, що призводить до зміни ідентифікатора чипа. Нова технологія автентифікації чипів розроблена в компанії Toshiba. За основу взято випадковий телеграфний шум (RTN – Random Telegraph Noise) в транзисторах, який виникає внаслідок дефектів ізоляційного матеріалу [15]. Даний вид PUF на основі RTN стійкіший за попередніх до електричних навантажень, фактичні дані вимірів можна використовувати більше мільйона разів. Toshiba розробляє технологію взаємної автентифікації для пристроїв IoT шляхом зняття відбитків PUF у напівпровідникових чіпах для найшвидшого впровадження з метою створення більш безпечних систем IoT. Toshiba не розкриває деталей використання RTN з метою автентифікації, але, виходячи з загальної характеристики даного виду шуму [16, 17] – зосередження спектральної густини в області низьких частот (≈1 Гц) – можна очикувати, що процедура автентифікації буде досить тривалою, що накладає обмеження на швидкодію електронних пристроїв.

Аналіз літератури показав, що дослідники зосереджують зусилля на способах реалізації факторів “біометричної” автентифікації електронних пристроїв, які потребують значних зусиль, до того ж при такому підході можуть виникнути помилки першого та другого роду.

Мета та завдання дослідження

Мета дослідження – з’ясувати можливість підходу симуляції “біометричного” шаблону автентифікації в програмний спосіб. Для вирішення мети потрібно реалізувати симулятор шаблонів з властивостями біометрики мовою програмування, виконати оцінку розподілу відстаней між парами шаблонів та оцінити параметри генерованих послідовностей з точки зору ймовірності брутфорсу.

Результати дослідження

Побудова "біометричного" шаблону автентифікації саме для мікроконтролерів на основі вимірів електромагнітних полів чи електричних наведень ускладнена, оскільки не всі

© Нємкова, О. А., & Чура, Н. Р. (2024). Оцінка параметрів моделі симуляції автентифікаторів мікроконтролерів. Сучасний захист інформації, 1(57), 103–107. https://doi.org/10.31673/2409-7292.2024.010012.

сімейства мікроконтролерів мають вбудовані аналогово-цифрові перетворювачі (АЦП), і часто плати використовуються без металевих корпусів, що може вплинути на параметри сигналу шумів через зовнішні наведення. Фактично, єдиним можливим підходом для створення таких шаблонів є використання фізично не клонованих функцій. Для кожного сімейства мікроконтролерів потрібно розробляти індивідуальні методи реалізації PUF, тому цей підхід не є універсальним.

Підхід, який описаний в даному дослідженні, наступний. Потрібно виконати симуляцію "біометричного" шаблону автентифікації пристрою в програмний спосіб. Таким чином сформовані шаблони мають мати властивості динамічності (жодний з симульованих шаблонів не має повторюватись за час функціонування конкретного пристрою), при порівнянні довільної пари шаблонів одного пристрою за вибраною відстанню D_{intra} вони мають несуттєво відрізнятись один від одного, тоді як при порівнянні пари довільних шаблонів від різних пристроїв відстань D_{inter} має бути суттєво більшою, а саме $D_{intra}<<D_{inter}$. При цьому хибно позитивні та хибно негативні помилки автентифікації відсутні.

Підґрунтям для такого підходу слугують результати експериментів для реальних бітових шаблонів внутрішнього електричного шуму персональних комп'ютерів (ПК), які були розраховані з нормалізованої функції автокореляції записів шуму [6]. В експериментах довжина бітових шаблонів була взята 1000 біт. Було з'ясовано, що бітові шаблони сигналу шуму містять приблизно однакову кількість нульових бітів «0» та одиничних бітів «1». При порівнянні пари поточних шаблонів шуму (отриманих в реальному часі) одного ПК виявилося, що вони збігаються по більшості позицій бітів. Лише кілька позицій мали інвертовані біти. Позиції інвертованих бітів не збігалися для різних пар шаблонів. Порівняння бітових шаблонів шуму в реальному часі двох різних ПК показало набагато меншу схожість. Відстані Хемінга між шаблонами шуму різних ПК були в 5–10 разів більші порівняно з аналогічними відстанями для одного ПК. Розроблений генератор псевдовипадкової імпульсної послідовності Пуассона дозволив змоделювати ці властивості бітових шаблонів. Однакові біти в шаблоні змодельовані нульовими бітами, а біти, що відрізняються в парі шаблонів – одиничними бітами.

Прообраз симулятора був запропонований в дослідженні [18]. Шаблоном автентифікації слугує бітовий рядок, який утворений шляхом прямої суми двох псевдовипадкових пуасонівських послідовностей. Перша послідовність {A} моделює невеликі варіації між шаблонами одного пристрою, друга послідовність {B} відповідає за відстані між різними пристроями. В якості метрики використана відстань за Хемінгом. Алгоритм генерації псевдовипадкових пуасонівських послідовностей дозволяє забезпечити в середньому певну кількість одиничних бітів на 1000 біт за рахунок вибору початкових параметрів. Даний алгоритм успішно проходить тести NIST, період повторення такої послідовності оцінений як мільярд бітів.

На основі підходу [18] було розроблено програмне забезпечення для реалізації симулятора, мова програмування Python. Середня кількість одиничних бітів на 1000 бітів пуасонівської послідовності для розробленого генератора визначається керуючим кодом G. Якщо G=10 000, то в середньому кількість одиничних бітів буде дорівнювати 10, а кількість нульових бітів складе 990. Якщо G=100 000, то одиничних бітів буде відповідно 100, а нульових бітів - 900. Послідовність {A} формується із згенерованої пуасонівської послідовності для параметра G=10 000, а послідовність {B} відповідно для G=100 000. Результати моделювання {A xor B} дають наступні характеристики розподілу відстаней для ста шаблонів при довжині бітового шаблону L=1000 біт, табл.1.

Таблиця 1

Характеристики розподілу відстаней між парами шаблонів

Розподіл відстаней	Середнє значення відстані	Стандартне відхилення	Мінімальне значення	Максимальне значення
D_{intra} (для одного пристрою)	23	6	12	39
D_{inter} (для різних пристроїв)	205	5	189	215

Отримані результати задовольняють вимогам на співвідношення середніх значень відстаней $D_{intra}<<D_{inter}$, з таблиці 1: 23<<205. Також області відстаней D_{intra} та D_{inter} не перетинаються: 39<<189. З чого слідує, що дана модель не має помилкових спрацювань, таких як хибно позитивні та хибно негативні помилки.

Оцінка ймовірності успішного брутфорсу пов'язана з довжиною бітового шаблону. В послідовності {A} для однієї бітової одиниці потрібно забезпечити 100 бітів довжини шаблону. Чим менше буде унікально розташованих бітових одиниць, тим простіше зловмиснику буде підібрати потрібний варіант. Отже, для даної моделі бітових шаблонів довжина L може бути оцінена з точки зору ймовірності успішного брутфорсу. Підрахунок кількості варіантів $P(lAB,L)$ розташування lAB одиничних бітів на L позиціях відбувається за виразом, де lAB – сумарна кількість одиничних бітів послідовностей {A} і {B}

$$P(lAB,L) = L!/(L-lAB)! \quad P(110,1000) = 1000!/(1000-110)! \tag{1}$$

Розрахунок за допомогою онлайн калькулятора виразу (1), який працює за наближеною формулою Стірлінга, для значень lAB=110 і L=1000 дає оцінку кількості варіантів $2\cdot10^{327}$. Це дуже велика кількість варіантів для атаки брутфорсу, тому ймовірність $p(lAB,L)$, яка обернена до кількості варіантів $P(lAB,L)$, буде надзвичайно малою.

Інша ситуація буде, коли зловмиснику вдасться якимось чином перехопити декілька бітових шаблонів від одного пристрою. Тоді в нього буде часткова інформація про незмінні біти, які забезпечує послідовність {B}. В такому випадку кількість варіантів підбору бітового шаблону буде значно меншою порівняно з попередньою оцінкою (1)

$$P(lA,L) = L!/(L-lA)! \tag{2}$$

де lA – кількість одиничних бітів послідовності $\{A\}$.

Розрахунок за допомогою онлайн калькулятора дає оцінку кількості варіантів $2\cdot10^{30}$ для L=1000. Таку кількість варіантів також практично неможливо перебрати за час тривалості сесії. Залежність кількості варіантів $P(lA,L)$ (оцінка величини) від довжини шаблону L для оцінки (2) представлена в таблиці 2. Дані таблиці 2 дають можливість оцінити необхідну довжину бітового шаблону, виходячи з потреб конкретної інформаційної системи.

Таблиця 2

Оцінка кількості варіантів перебору для атаки брутфорсу на бітовий шаблон

Довжина шаблону L, біт	Кількість одиничних бітів послідовності $\{A\}$ на довжині L	Кількість варіантів перебору для атаки брутфорсу
1000	10	$2\cdot10^{30}$
900	9	$3\cdot10^{27}$
800	8	$2\cdot10^{23}$
700	7	$8\cdot10^{19}$
600	6	$5\cdot10^{16}$
500	5	$3\cdot10^{13}$
400	4	$2\cdot10^{10}$
300	3	$3\cdot10^{7}$
200	2	$2\cdot10^{4}$
100	1	$1\cdot10^{2}$

Потужність роботи симулятора визначається кількістю можливих унікальних автентифікаторів – бітових шаблонів. Якщо прийняти за довжину шаблону L=1000 біт, то можна організувати 10^6 шаблонів для послідовності $\{A\}$ і таку саму кількість для послідовності $\{B\}$ з використанням генератора псевдовипадкових імпульсних послідовностей Пуассона для двох значень керуючого кода G. Кількість унікальних бітових шаблонів буде

© Нємкова, О. А., & Чура, Н. Р. (2024). Оцінка параметрів моделі симуляції автентифікаторів мікроконтролерів. Сучасний захист інформації, 1(57), 103–107. https://doi.org/10.31673/2409-7292.2024.010012.

визначатися величиною 10^{12}. Яким чином розподілити ці шаблони між пристроями інтелектуальної системи – вирішується безпосередньо виходячи з вимог на кількість пристроїв та кількість автентифікацій для кожного пристрою.

Висновки

Для практичного використання симульованих бітових шаблонів планується розробити модуль автентифікації мікроконтролера, який буде побудований за клієнт-серверною архітектурою, але теоретично можливе використання таких шаблонів в децентралізованих мережах. Також потрібно розробити спосіб безпечної передачі шаблону в поточній сесії для використання його як автентифікатора у наступній сесії. Отже, в роботі виконано оцінки основних параметрів моделі симулятора на основі характеристик розподілу відстаней між парами шаблонів. Наведено рекомендації для вибору довжини бітових шаблонів. Результати роботи можуть мати важливе значення для розвитку безпеки електронних систем та засобів автентифікації в контексті кібербезпеки мікроконтролерів.

Перелік посилань

1. Authentication. URL: https://en.wikipedia.org/wiki/Authentication.
2. Wang, X., Zhang, Y., Zhang, H., Wei, X., Wang, G. Identification and authentication for wireless transmission security based on RF–DNA fingerprint. EURASIP Journal on Wireless Communications and Networking. 2019. URL: https://link.springer.com/article/10.1186/s13638–019–1544–8.
3. Chouchang, Y., Alanson, P. Sample EM–ID: Tag–less Identification of Electrical Devices via Electromagnetic Emissions. Proc. of 2016 IEEE International Conference on RFID (RFID). Orlando, FL, USA. 2016.
4. Suh, E. G., Srinivas, D. Physical Unclonable Functions for Device Authentication and Secret Key Generation. Proc. of Design Automation Conference. San Diego, California, USA. 2007. 6 p.
5. Toshiba Develops Mutual Authentication Technology for IoT Devices by PUF Fingerprinting Using Variations in Semiconductor Chips, 14 Jun. 2018. URL: http://www.toshiba.co.jp/rdc/rd/detail_e/e1806_02.html.
6. Sikora, A., Nyemkova, E., Lakh, Y. Accuracy Improvements of Identification and Authentication of Devices by EM-Measurements. IDAACS-SWS 2020 - 5th IEEE International Symposium on Smart and Wireless Systems within the International Conferences on Intelligent Data Acquisition and Advanced Computing Systems, Proceedings, 2020.
7. Banakh, R., Piskozub, A., Opirskyy, I. Detection of MAC spoofing attacks in IEEE 802.11 networks using signal strength from attackers' devices. Advances in Intelligent Systems and Computing, 2019, v. 754. URL: https://link.springer.com/chapter/10.1007/978-3-319-91008-6_47.
8. Holcomb, D. E., Burleson, W. P., Fu, K. Power–up sram state as an identifying fingerprint and source of true random numbers. Computers, IEEE Transactions. 2009. Vol. 58. No. 9. P. 1198–1210.
9. Böhm, C., Hofer, M. Physical Unclonable Functions in Theory and Practice. Springer Science & Business Media. 2012. 270 p.
10. Sparsh, M. A Survey Of Architectural Techniques for Managing Process Variation. ACM Computing Surveys, (Association for Computing Machinery). 2016. Vol. 48. No. 4. 31 p.
11. Graham, P. Xilinx to add PUF security to Zynq devices. 2016. URL: https://www.xilinx.com/about/security–working–group–2016.html.
12. Altera Reveals Stratix 10 with Intrinsic–ID's PUF technology. 2015. URL: https://www.intrinsic–id.com/altera–reveals–stratix–10–with–intrinsic–ids–puf–technology/
13. Suh, E. G., Srinivas D. Physical Unclonable Functions for Device Authentication and Secret Key Generation. Proc. of Design Automation Conference. San Diego, California, USA. 2007. 6 p.
14. Holcomb, D., Burleson, W., Fu, K. Power–up SRAM State as an Identifying Fingerprint and Source of True Random Numbers. IEEE Transactions on Computers. 2008. Vol. 58. Is. 9. P. 1198-1210.
15. Toshiba Develops Mutual Authentication Technology for IoT Devices by PUF Fingerprinting Using Variations in Semiconductor Chips, 14 Jun. 2018. URL: http://www.toshiba.co.jp/rdc/rd/detail_e/e1806_02.html.
16. Kirton, M. J., Uren, M. J., Collins, S., Schulz, M., Karmann, A., Scheffer, K. Individual defects at the Si: SiO2 interface. Semicond. Sci. Technol. 1989. Vol. 4. P. 1116–1126.
17. Realov, S., Shepard, K. L. Analysis of random telegraph noise in 45–nm CMOS using on–chip characterization system. IEEE Trans. Electron Devices. 2013. Vol. 60. No. 5. P. 1716–1722.
18. Maksymovych, V., Nyemkova, E., Justice, C., Shabatura, M., Harasymchuk, O., Lakh, Y., Rusynko, M. Simulation of Authentication in Information-Processing Electronic Devices Based on Poisson Pulse Sequence Generators. Electronics 2022, 11(13), 2039; URL: https://doi.org/10.3390/electronics11132039.

Надійшла 09.02.2024