УДК 62-503.5
Т.І. Лесишин
Тернопільський національний технічний університет імені Івана Пулюя, Україна

МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ СИСТЕМИ “РОЗУМНИЙ ДІМ”

T.I. Lesyshyn

METHODS AND MEANS OF INFORMATION PROTECTION OF THE “SMART HOME” SYSTEM

Розумні будинки, які використовують технологію Інтернету речей, надають унікальні можливості для автоматизації завдань та покращення зручності у нашому повсякденному житті. Зростання популярності цих технологій неухильно викликає занепокоєння щодо кібербезпеки та конфіденційності. Потреба в удосконаленні систем шифрування та розробці нових стратегій безпеки виникає з потенційної загрози витоку цінної інформації через бездротові сигнали. Важливість міцного криптографічного захисту, а також врахування факторів, таких як тимчасове маніпулювання трафіком та випадковість, підкреслюється сучасними атаками, такими як "шпигунство на основі FATS".

У сучасній ері передових технологій розумні пристрої стикаються з серйозним ризиком витоку конфіденційності та безпеки через появу атак бічного каналу. Зловмисники можуть використовувати систему через переконання в постійному витоку даних, що становить основу для цих атак. Дослідження пасивних та активних атак бічного каналу виявляє слабкості, які існують у стандартних компонентах розумних пристроїв.

Аналіз енергоспоживання та диференційний аналіз енергоспоживання - це дві техніки, які використовуються для виявлення чутливої інформації в пристроях за допомогою вивчення їхнього використання енергії. Спостерігаючи коливання у використанні енергії, можливо виявити тенденції та розрізняти алгоритми, в той час як SPA має здатність визначати техніки шифрування. Диференційний аналіз енергоспоживання є вдосконаленим підходом, який використовує статистичні методи для виправлення помилок та визначення ключів шифрування з більшою точністю.

Система знаходиться під загрозою фізичних маніпуляцій та розголошення інформації альтернативними каналами через аналіз помилок, електромагнітних характеристик та звукових характеристик. Дослідження часу та аналіз трафіку підкреслює використання інформації, пов'язаної з часом, та передачі сигналів для виявлення закономірностей та важливої інформації. Хакери можуть аналізувати комунікації системи та визначати її функціональність через ці атаки.

Сучасні дослідження в галузі безпеки розумного дому в бездротових мережах спрямовані на покращення конфіденційності та зменшення загальних затримок за допомогою використання вдосконалених схем захисту від атак FATS. Схема ConstRate, яка визначає послідовність вікон виконання для розподілу сигналів у мережевому трафіку, стала ефективним інструментом для оптимізації конфіденційності. Покращена схема ProbRate, заснована на експоненційному розподілі інтервалів очікування, дозволяє зберігати конфіденційність при зменшенні часових затримок. З свого боку, схема FitProbRate (FPR) використовує тест Андерсона-Дарлінга та пріоритетизацію фактичних пакетів для ефективного зменшення затримок системи.