International Scientific Conference 20 UNITECH 26

INTERNATIONAL SCIENTIFIC CONFERENCE
19-21 November 2026
GABROVO

АНАЛИЗ НА ВИДОВЕТЕ КИБЕР АТАКИ СРЕЩУ УСТРОЙСТВА В SMART HOME

инж. Милен Ивайлов Василев[1], инж. Пламен Тихомиров Тихов[1], инж. Ганчо Любомиров Танев[1]

[1]катедра КТТ, ФЕЕ, ТУ - Габрово, ул. Х. Димитър 4, гр. Габрово, България
**кореспондиращ автор: milensskii@icloud.com*

ANALYSIS OF TYPES OF CYBERATTACKS AGAINST SMART HOME DEVICES

eng. Milen Ivaylov Vasilev[1], eng. Plamen Tihomirov Tihov[1], eng. Gancho Lubomirov Tanev[1]

[1]department CET, FEE, Technical University of Gabrovo, H. Dimitar Str.4, Gabrovo, Bulgaria
**Corresponding author: milensskii@icloud.com*

Abstract
Smart homes represent a revolutionary trend in how we control and automate our living environments. From heating and lighting control systems to video surveillance and home automation, smart devices have become an integral part of modern life. However, the integration of technology into our homes brings about new cybersecurity challenges and risks. This article outlines the various types of cyberattacks to which devices in a smart home environment are vulnerable. It demonstrates a specific type of cyberattack that can affect smart homes and discusses ways to prevent and manage such threats.

Keywords: Cyberattacks, Smart Home Devices; Aircrack-ng.

ВЪВЕДЕНИЕ

В последните години кибер защита заема все по-голямо място в общата система на сигурността като реален проблем, а не като сценарий от научнофантастичен филм. Проявленията на киберзаплахите, както и техните източници, са навсякъде около нас и вече са дефинирани и класифицирани, но все още са непознати за повечето хора [1, 3].

Като отговор на реално съществуващите опасности в информационното пространство са създадени редица стандарти за кибернетична сигурност, прилагането на които намалява риска в тази област. Те са разработени както от държавни, така и от неправителствени организации; непрекъснато се разработват нови стандарти и е сериозно предизвикателство да бъдат намерени и приложени тези, които най-добре ще отговорят на изискванията на отбраната.

Терминът „smart home” или „умен дом” по същество се състой в това да се управляват различни електроуреди или механизми от дадено лице на разстояние или управлението им да се автоматизира според зададени различни критерии. Управлението може разчита на входната информация от различни сензори [2, 4]. Тя може да бъде само информативна и да не служи пряко за създаване на някакво събитие. Тази информация може да бъде съхранявана локално или на централен

Print ISSN: 1313-230X, Online ISSN: 3033-1404

сървър. Възможно е управление на база на предварително зададен часови график или само на изрична команда от разстояние.

Целта на разработката е да се извърши сканиране и изследване на ефира, да се открият всички устройства и мрежи в обхвата на скенера, и да се търсят уязвимости в криптирането на безжичните мрежите и устройствата, които комуникират в тях. На базата на това да се реализира примерна кибер атака към устройствата и да се анализира тяхната уязвимост.

ИЗЛОЖЕНИЕ

Въздушното хакване (aircracking) е техника за откриване на безжични мрежи и проникване в тях, като се използва уязвимост в криптирането на мрежата. Тази техника може да бъде използвана за незаконни цели, като кражба на лична информация или злоупотреба с мрежата.

Въздушното хакване използва уязвимост в криптирането на безжичната мрежа, за да се открие паролата й. Това става чрез изпращане на множество заявки за автентикация към мрежата, като се използва различен ключ за всяка заявка. Когато мрежата отговори на заявките, хакерът може да използва тези отговори, за да изчисли паролата на мрежата. След като хакерът е открил паролата на мрежата, той може да се свърже към нея и да използва интернета, както и да получи достъп до всички устройства, свързани към мрежата. Това може да включва компютри, телефони, телевизори и други устройства.

Съществуват много инструменти за въздушно хакване, като някои от тях са: Aircrack-ng, Wireshark, Cain and Abel, Kismet. Като за целите на нашето изследване ще използваме Aircrack-ng (фиг.1). Това е един от най-известните инструменти за въздушно хакване. Той може да открие паролата на безжична мрежа, като използва уязвимост в криптирането на мрежата.



***Фиг. 1**. Aircrack-ng*

Aircrack-ng е мрежов софтуерен пакет, състоящ се от детектор, снифър на пакети, WEP и WPA / WPA2-PSK крекер и инструмент за анализ за 802.11 безжични LAN [5]. Той работи с всеки контролер за безжичен мрежов интерфейс, чийто драйвер поддържа режим на суров мониторинг и може да подуши 802.11a, 802.11b и 802.11g трафик. Пакетите се пускат за Linux и Windows.

Aircrack-ng е разклонение на оригиналния проект Aircrack. Той може да бъде намерен като предварително инсталиран инструмент в много Linux дистрибуции, фокусирани върху сигурността, като Kali Linux или Parrot Security OS, които споделят общи атрибути, тъй като са разработени по един и същ проект (Debian).

Aircrack е инструмент за откриване на безжични мрежи и проникване в тях, като се използва уязвимост в криптирането на мрежата. Тази техника може да бъде използвана за незаконни цели, като кражба на лична информация или злоупотреба с мрежата. Ще разгледаме как работи Aircrack, какви са неговите функции и как може да бъде използван за откриване на уязвимости в безжичните мрежи.

Aircrack използва уязвимост в криптирането на безжичната мрежа, за да се открие паролата й. Това става чрез изпращане на множество заявки за автентикация към мрежата, като се използва различен ключ за всяка заявка. Когато мрежата отговори на заявките, Aircrack

може да използва тези отговори, за да изчисли паролата на мрежата.

След като Aircrack е открил паролата на мрежата, той може да се свърже към нея и да използва интернета, както и да получи достъп до всички устройства, свързани към мрежата. Това може да включва компютри, телефони, телевизори и други устройства.

Aircrack има много функции, които могат да бъдат използвани за откриване на уязвимости в безжичните мрежи. Някои от тези функции включват:

- Откриване на безжични мрежи: Aircrack може да открие всички безжични мрежи в дадена област.
- Откриване на уязвимости в мрежата: Aircrack може да открие уязвимости в криптирането на мрежата, които могат да бъдат използвани за откриване на паролата на мрежата.
- Анализ на трафика на мрежата: Aircrack може да записва трафика на мрежата и да го анализира, за да се открият проблеми в мрежата.
- Филтриране на трафика: Aircrack може да филтрира трафика на мрежата, за да се покажат само определени видове трафик, като например трафик от определен IP адрес или протокол.
- Декодиране на протоколите: Aircrack може да декодира протоколите на мрежата, за да се покажат данните, които се предават през мрежата.
- Съхранение на данни: Aircrack може да съхранява данните, които са записани по време на анализа на мрежата, за да могат да бъдат анализирани по-късно.

Криптирането на мрежата може да затрудни атаките, открити с помощта на Aircrack, като прави откриването на данните по-трудно.

Целта ни е да уловим ръкостискането за удостоверяване на WPA / WPA2 и след това да се използва aircrack-ng, за да се разбие предварително споделеният ключ.

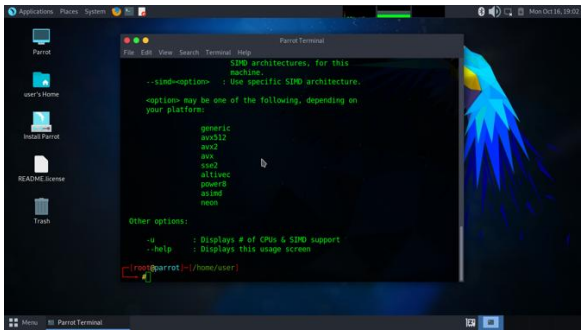
Това може да се направи активно или пасивно. "Активно" означава, че ще ускориме процеса, като премахнеме удостоверяването на съществуващ безжичен клиент. "Пасивно" означава, че просто ще чакаме безжичен клиент да се удостовери в WPA / WPA2 мрежата. Предимството на пасивното е, че всъщност не се нуждаеме от възможност за инжектиране и по този начин може да се използва Windows версията на aircrack-ng.

Ето основните стъпки, през които ще преминем:

- ✓ Стартиране на безжичния интерфейс в режим на монитор на конкретния AP канал;
- ✓ Стартиране airodump-ng на AP канал с филтър за bssid за събиране на ръкостискане за удостоверяване;
- ✓ Използване на aireplay-ng за деудостоверяване на безжичния клиент;
- ✓ Стартиране aircrack-ng, за да разбиеме предварително споделения ключ с помощта на ръкостискането за удостоверяване.

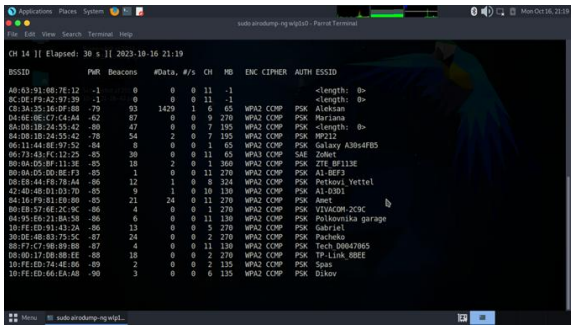
След като сме реализирали чрез настройки и команди посочените по-горе стъпки правим експеримент от който постигаме следните резултати.

На фиг.2, активираме „monitoring mode”, за да може да видим наличните мрежи.



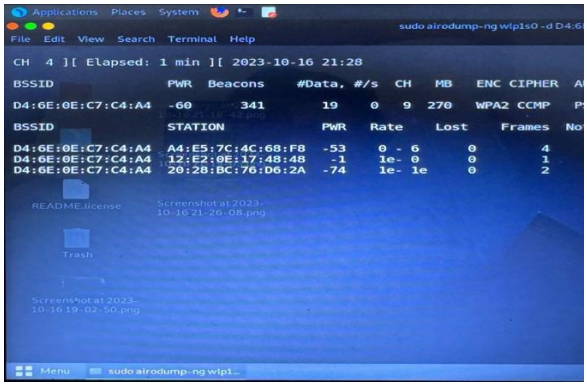
***Фиг. 2**. Работен екран на „monitoring mode” Aircrack-ng*

След активирането на „monitoring mode” виждаме наличните мрежи и техните MAC addresses – Фиг. 3.



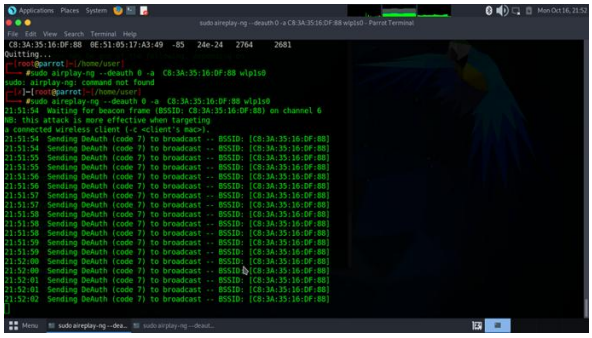
***Фиг. 3**. Работен екран на сканираните мрежи*

След като си изберем мишена сканираме по MAC address и виждаме какви и колко устройства са свързани безжично – Фиг. 4.



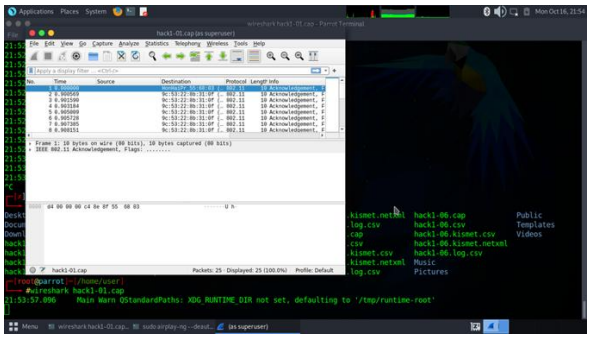
***Фиг. 4**. Работен екран с MAC address*

След като изберем мишена тестваме връзката ни с него (все едно пускаме пинг) – Фиг. 5.



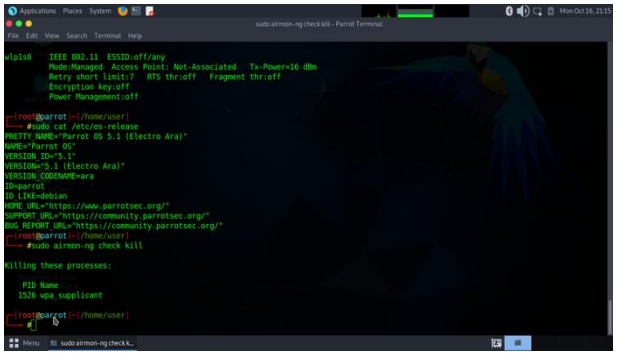
***Фиг. 5**. Работен екран за тестване на връзка с устройството*

Следва отговор от свързаните безжични клиенти и имаме достъп до файловете на примерната мишена – фиг. 6.



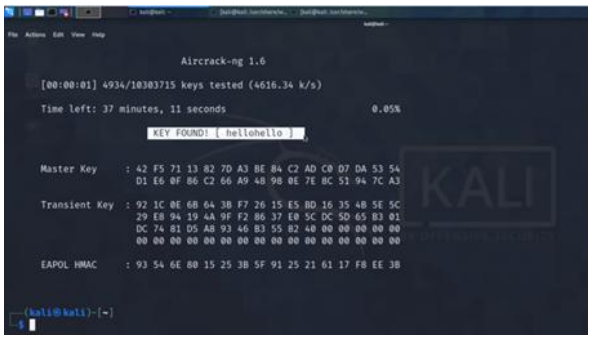
***Фиг. 6**. Работен екран показващ достъп до файловете*

А от тук вече можем и да извлечем файлове от мишената – фиг. 7



***Фиг. 7**. Работен екран с извличане на информация и файлове*

Когато разархивираме файла и го стартираме виждаме паролата – фиг. 8 и времето, за което е успял да прихване паролата.



***Фиг. 8.** Работен екран с маркирата парола на устройството*

ЗАКЛЮЧЕНИЕ

В заключение, сигурността на смарт домовете е един от най-важните аспекти на технологичния напредък и начина ни на живот. Разгледахме различни видове кибернетични атаки, както и как да ги предотвратим и управляваме. Също така разгледахме важни аспекти на информационната, екологичната и физическа сигурност на смарт домовете.

Сигурността на смарт домовете изисква усилия от страна на производителите, регулаторите, образователните институции и най-вече потребителите. Само съвместната работа и постоянни усилия могат да осигурят, че смарт технологиите ще продължат да обогатяват и улесняват нашия живот, без да подлагат нашата сигурност и поверителност на риск.

Следователно, е от съществено значение да продължим с научните изследвания и иновациите в областта на киберсигурността и смарт технологиите. Постоянната адаптация към новите технологии и заплахи, както и усъвършенстването на стандартите за сигурност, са ключови защитни мерки. В същото време, образованието на потребителите трябва да бъде акцентирано, за да се увеличи осведомеността за рисковете и най-добрите практики в областта на сигурността на смарт домовете.

Само чрез съвместните усилия на индустрията, академичната общност, регулаторите и потребителите можем да гарантираме, че смарт домовете ще продължат да бъдат напредни и сигурни, и че технологичният напредък ще бъде използван за наше благо и сигурност. В бъдеще, трябва да продължим да изследваме нови методи и технологии, които да укрепят сигурността на смарт домовете и да осигурят устойчивост срещу нарастващите заплахи от кибер атаки.

БЛАГОДАРНОСТИ: *Този доклад и изследванията в него са реализирани по проект „Изследване на интелигентни методи, архитектури и технологии за защита на данни в комуникационните мрежи“, договор НИП2026-22/2026г. към УЦНИТ при ТУ – Габрово.*

ЛИТЕРАТУРА

[1] Fritzing - https://fritzing.org/home/.
[2] PHP Manual - https://www.php.net/, 2020.
[3] How Home Automation Market Will Generate Huge Revenue Opportunities? - https://fresnobserver.com/how-home-automation-market-will-generate-huge-revenue-opportunities/2717/.
[4] Smart Home Automation Market Size: http://latestmarketresearchupdate.blogspot.com/2018/11/smart-home-automation-market-size-worth.html.
[5] Aircrack-Ng: https://www.aircrack-ng.org/downloads.html.