УДК 681.518.5

Банах Р. І.

Аспірант кафедри захисту інформації Національного університету «Львівська політехніка», Львів, Україна

ВИЗНАЧЕННЯ ПАРАМЕТРІВ КЛЮЧА МЕТОДУ АВТЕНТИФІКАЦІЇ WPA/WPA2 ДЛЯ СИСТЕМИ-ПРИМАНКИ МЕРЕЖІ СТАНДАРТУ IEEE 802.11

Актуальність. Відкритим є питання правильності конфігурування систем-приманок, особливо це стосується систем-приманок, які імітують бездротові мережі, оскільки їх клієнти є мобільними, а контрольована зона часто не є обмеженою. Неправильна конфігурація системи-приманки може стати безкорисним навантаженням у середині автоматизованої системи, особливо це стосується систем-приманок для бездротової мережі стандарту IEEE 802.11. Система-приманка із низьким чи відсутнім рівнем захисту може викликати підозру у досвідченого зловмисника, у гіршому ж випадку вона стане легкою здобиччю порушників метою яких є лише доступ до ресурсу Інтернет. З іншого боку, використання системи-приманки із максимальним рівнем захисту також не має сенсу, оскільки така модель стане неприступною фортецею для зловмисника.

Найбільш захищеними вважаються точки доступу на яких використовується метод автентифікації WPA/WPA2, застосування якого, імовірно, дасть впевненість зловмиснику у тому, що він атакує легітимну систему.

Метою роботи є розробка діагностичної моделі для систем-приманок бездротових мереж стандарту IEEE 802.11 для умовного захисту якої використовується метод автентифікації WPA/WPA2. Така модель допоможе оцінити поточну конфігурацію точки доступу на імовірність використання відомих вразливостей методу автентифікації WPA/WPA2 з боку зловмисників потрібного рівня підготовленості.

Метод. Запропоновано метод оцінки кваліфікованості зловмисника та його технічної оснащеності шляхом підбору параметрів ключа WPA/WPA2 для системи-приманки у бездротовій мережі стандарту IEEE 802.11. Реалізація даного методу дозволить досягти зменшення навантаження на систему-приманку, що передусім створить ілюзію автентичності для зловмисника. Запропоновано метод розподіленої атаки грубої сили на метод автентифікації WPA/WPA2, який забезпечує діагностику стійкості ключа системи-приманки у мережі Wi-Fi. Проведено порівняння апаратної віртуалізації з віртуалізацією на рівні операційної системи за однакових умов у рамках атаки грубої сили на механізм автентифікації WPA/WPA2.

Результати. Отримано оптимальні умови для проведення розподіленої атаки грубої сили у віртуальному середовищі, що дає змогу відносно швидко оцінити рівень захищеності системи-приманки.

Висновки. Запропоновано метод оцінки стійкості ключа для методу автентифікації WPA/WPA2 мережі стандарту IEEE 802.11 для взаємодії зі зловмисником потрібного рівня кваліфікації і наявного у нього технічного забезпечення. Подальший розвиток отримав метод оцінки захищеності бездротових мереж стандарту IEEE 802.11 за допомогою методу аналізу ієрархій. Запропоновано середовище для проведення оцінки умовної захищеності системи-приманки із умовами застосування масштабованості даної технології; метод генерування словників для проведення оцінки захищеності систем-приманок, який дозволить уникнути повторення ключів і, тим самим, пришвидшить отримання результатів.

Ключові слова: IEEE 802.11, Wi-Fi, система-приманка, оцінка захищеності, метод аналізу ієрархій.

НОМЕНКЛАТУРА

Wi-Fi – загальновживана назва для стандарту IEEE 802.11 передачі цифрових потоків даних по радіоканалу;

WPA – (англ. Wi-Fi Protected Access) – протокол безпеки для захисту бездротових мереж;

АС – автоматизована система;

МОІ – метод оцінки ієрархій (англ. Analytic Hierarchy Process, AHP);

СП – система-приманка;

PSK – (англ. Pre-Shared key) – ключ, який є попередньо розділений між двома вузлами за допомогою певного безпечного каналу;

AES – (англ. Advanced Encryption Standard) – також відомий під назвою Rijndael – симетричний алгоритм блочного шифрування;

SOHO – (англ. Small office / home office) – назва сигменту ринку, який відноситься до категорії (1 – 10 працюючих);

SSID – (англ. Service Set Identifier) – унікальне найменування роздротової мережі, що відрізняє одну мережу стандарту IEEE 802.11 від іншої.

PKCS – стандарт криптографії з відкритим ключем;

PBKDF2 – (англ. Password-Based Key Derivation Function) – стандарт форматування ключа на основі паролю;

HMAC – (скорочення від англ. hash-based message authentication code) – код перевірки автентичності повідомлень, який використовує хеш функцію;

SHA1 – (англ. Secure Hash Algorithm 1) – алгоритм криптографічного хешування, описаний в RFC 3174;

D – позначення загального словника для атаки грубої сили;

d – позначення поточного словника;

l – позначення набору комбінацій у словнику;

S – швидкість перебору ключів за одиницю часу;

t_{BF} – час перебору словника методом грубої сили;

N – вагова матриця методу аналізу ієрархій.

ВСТУП

Бездротові комп'ютерні мережі стандарту IEEE 802.11 є найцікавішим для зловмисників, оскільки для передавання даних використовують радіохвилі, які розповсюджуються за законами фізики, а контролювати поведінку радіохвиль є дуже затратним рішенням. Це означає, що контрольована зона в даному випадку є не вагомою з точки зору захисту.

DOI 10.15588/1607-3274-2018-1-13

Серйозну проблему створює те, що користувачі бездротових мереж є мобільними. Вони можуть з'являтись і зникати, змінювати місце розташування і не є прив'язаними до фіксованих точок входу. Для під'єднання лишень потрібно перебувати у зоні покриття конкретної бездротової мережі.

У інформаційній безпеці, окрім протистояння «атака-захист» практикується і «атака-контратака». У парі «напад-захист» практикується покрокова стратегія, а саме – зловмисник користується певною вразливістю у захисті до поки вона не буде виявлена і закрита, після чого він знаходить нову вразливість, і так до нескінченості. У випадку стратегії «атака-контратака» сторона захисту грає на випередження, вивчаючи дії та можливості зловмисника. Реалізація такої ідеї лежить в основі використання віртуальних приманок. Мета їх функціонування – піддатись атаці або несанкціонованому дослідженню зі сторони зловмисників, що згодом дозволить вивчити їх стратегію та визначити перелік засобів, за допомогою яких можуть бути нанесені удари по стратегічних об'єктах мережі.

Та не правильна конфігурація системи-приманки (СП) може стати безкорисним навантаженням у середині автоматизованої системи (АС), особливо це стосується СП для бездротової мережі стандарту IEEE 802.11. СП із низьким чи відсутнім рівнем захисту може викликати підозру у досвідченого зловмисника, у гіршому ж випадку вона стане легкою здобиччю порушників, метою яких є лише доступ до ресурсу Інтернет. З іншого боку, використання СП із максимальним рівнем захисту також не має сенсу, оскільки така модель стане не приступною фортецею для зловмисника.

Метою даної роботи є розроблення методу оцінки стійкості ключа для метода автентифікації WPA/WPA2 СП для бездротової мережі стандарту IEEE 802.11, порівняти стратегії тестування ключа та обґрунтувати вибір середовища для роботи даного методу.

1 ПОСТАНОВКА ЗАДАЧІ

Очікуваним результатом даного дослідження є отримання шкали складності P_k ключа WPA/WPA2 для СП бездротової мережі стандарту IEEE 802.11 для кінцевого користувача на основі критеріїв a_{ij} матриці N, добутої методом аналізу ієрархій. Результатом правильної конфігурації СП виступають дані тесту t_{BF}, що прогнозує час перебору ключа за допомогою атаки грубої сили. Тест проводиться на основі даних зі словника D, а саме поточного словника d_i, результатом якого є набір $l_i - l_{i-1}$ унікальних ключів $l = \{k_1, k_2, ..., k_n\}$, та швидкості перебору ключів S, яка заміряється із певної еталонної системи. Порівнюючи даний метод за допомогою методів повної віртуалізації та віртуалізації на рівні операційної системи, буде вибрано середовище для проведення розподіленої атаки грубої сили, що дозволить знайти оптимальний метод оцінки умовної захищеності СП.

2 ОГЛЯД ЛІТЕРАТУРИ

Оцінка захищеності комп'ютерних систем та мереж вимагає великої уваги, особливо ця оцінка набуває цінності, якщо підкріпляється фактичними даними і цифрами [1]. Найбільшої уваги потребують бездротові мережі, оскільки в них важко запровадити контрольовану зону. В роботі [2] запропоновано метод оцінки захищеності бездротових мереж, який базується на методі оцінки ієрархій (MOI, англ. Analytic Hierarchy Process, AHP). Та зі збільшенням кількості елементів у системі збільшується і похибка в оцінці захищеності комп'ютерних мереж. Вплив великої кількості факторів (об'єкти, атрибути і т. д), описаних в роботі [3], не дозволяє отримати точності в результатах. Зрештою, є імовірним виникнення нової вразливості в програмному чи апаратному забезпеченні яке використовуються в АС. Тому, задля досягнення точності в оцінці захищеності необхідно розділяти компоненти у комплексних системах. До прикладу, в бездротових мережах Wi-Fi існує деяка кількість методів захисту, деякі з них можуть використовуватись в комбінації між собою. Кожен з методів має свій час і складність подолання.

Схожу проблему можна спостерігати і у системах, які імітують роботу автентичних систем. Вони функціонують задля відвернення уваги від справжніх систем, а метою їх роботи є збір і обробка інформації про методи та засоби порушників. Види, особливості функціонування, переваги та недоліки, а також методи інтегрування таких систем в АС, описано в роботі [4]. В роботі [5] описується систематизація методів та засобів аналізу СП в процесі зламу комп'ютерних систем чи мереж і пропонуються рекомендації щодо організації розслідування зламу, вибору засобів та аналізу подій.

Кожна комп'ютерна система володіє певними характеристиками і в кожної є свої вразливості і, відповідно, методи захисту. Не є виключенням і бездротові мережі стандарту IEEE 802.11 [6]. Застосування систем приманок в мережах Wi-Fi також має певні особливості і дуже часто СП у бездротових мережах вважаються інструментом зловмисника. В роботах [7-8] пропонується кардинально інший підхід до реалізації приманок у бездротових мережах, а саме застосування незалежних сенсорів у мережах стандарту IEEE 802.11 для ідентифікації вторгнень і забезпечення взаємодії зловмисника із СП.

Не вирішеним є питання створення системи, яка би оцінювала СП на складність подолання її захисту, що би дозволило гнучко підбирати конфігурацію відносно вартості інформації в системі, яка захищається, і очікувань щодо кваліфікованості зловмисника. Така постановка задачі вимагає аналізу вимог щодо системи, яка оцінює, а саме середовища розгортання та методів взаємодії із СП [9].

3 МАТЕРІАЛИ І МЕТОДИ

Як відомо, метод автентифікації WPA2 на сьогодні є найстійкішим до атак, та, все ж існують методи його подолання. Існує дві модифікації даного методу WPA2 Personal та WPA2 Enterprise. Різниця між WPA2 Personal та WPA2 Enterprise полягає у тому, що ключі шифрування алгоритму AES зберігаються у різних місцях. WPA2 Personal використовується здебільшого у Small or Home Office (SOHO) мережах. Ключ у механізмі WPA2 Personal є однаковим для всіх користувачів. Для корпоративних застосувань використовується динамічний ключ, індиві-

дуальний для кожного користувача. За генерацію пар логін-пароль у WPA2 Enterprise відповідає спеціальний сервер, здебільшого RADIUS.

Протокол WPA2-PSK (Pre-Shared key) дозволяє мобільним пристроям обмінюватись даними з точками доступу за допомогою методу шифрування AES. У криптографії PSK – це ключ, який попередньо ідентифікується між двома вузлами за допомогою певного безпечного каналу, перш ніж він буде використаний. PSK отримується з ключа, використовуючи стандарт формування ключа на основі паролю PBKDF2 із алгоритмом хешування SHA1 як псевдовипадковою функцією. PSK є 32 байтним (256 бітним), часто відображається у вигляді 64 шістнадцяткових символів.

Стандарт PBKDF2 у свою чергу описується стандартом PKCS#5. У цьому випадку пароль повинен бути довжиною від 8 до 63 символів. Символи конвертуються у машинний код за допомогою таблиці кодування ASCII, а отже у паролі можуть використовуватись лише ці символи.

У PBKDF2 бінарний пароль використовується як ключ до функції HMAC. В якості солі використовується ім'я точки доступу (SSID). Сіль із значенням лічильника використовується для початкового входу в функцію HMAC. Після цього попередні вихідні дані використовуються як вхідні допоки не відбудеться повторення 4096 HMAC. На жаль, він повертає дані у форматі 256 біт, в той час як SHA1 всього лиш повертає 160 біт.

Вихідні дані функції PBKDF2 і є PSK. PSK використовується безпосередньо як і Pairwise Master Key (PMK) у чотиристоронньому процесі рукостискання (1):

$$PSK = PBKDF2(HMAC-SHA1 \mid Passphrase \mid SSID \mid 4096 \mid 256). \quad (1)$$

Паролі, які використовують рядові споживачі сучасного обладнання Wi-Fi зазвичай є не складними. Це може бути комбінація цифр від одиниці до дев'яти, літер на клавіатурі які розташовані поряд, чи дата народження. Сьогодні існує велика кількість згенерованих словників із не складними фразами, які використовуються рядовими користувачами. Такі словники можна знайти у відкритому доступі в мережі Інтернет, а також у спеціальних операційних системах, таких як Black Arch, ArchStrike, Kali Linux та ін.

Загальна кількість символів, яка може бути використана при створенні ключа дорівнює 95 (табл. 1).

На основі проаналізованих популярних словників, автором формулюються найбільш доцільні комбінації наборів на основі таблиці 1 (табл. 2).

Для того, щоб отримати доступ до мережі зловмиснику необхідно перехопити пакет рукостискання і запустити процес дешифрування. Операція дешифрування паролю відбувається за допомогою центрального або графічного процесорів.

Після того, як відбувся перебір за словником і в ньому пароль не було знайдено, очевидно, що потрібно використати наступний словник. Якщо це словник, у якому не збільшується довжина ключа, але збільшується кількість символів з яких будуть генеруватись ключі, то логічно виключати ті комбінації, які вже були присутні у попередніх словниках (2):

$$D = \sum_{i=1}^{n} d_i = l_i - l_{i-1}, \quad (2)$$

де D – загальний словник, d – поточний словник, l – набір ключів у словнику (3):

$$l_i = \{k_1, k_2 ... k_n\}, \quad (3)$$

де k – ключ.

Існує імовірність, що в базовому словнику ключа не буде знайдено. У цьому випадку повинен бути згенерований новий словник. Після базового словника логічно, що наступним має бути словник, у якому забезпечено мінімальну довжину ключів і найменший набір символів з таблиці 1. Це може бути словник, який складається лише з цифр. Як видно з (2), ті ключі, які вже було використано в базовому словнику, не повинні перевикористовуватись.

Якщо було опрацьовано словник, у якому 10^8 варіантів ключів, згенерованих з мінімального набору символів, ключ не буде знайдено, тоді наступний словник буде згенеровано із кількістю ключів 10^9 і з тим же ж мінімальним набором символів (тобто, це символи від 000000000, до 999999999). Для цього потрібно розгорну-

Таблиця 1 – Символи доступні для задання ключа у методі автентифікації WPA/WPA2

№	Набір символів	Кількість символів у наборі	Може використовуватись у словнику, як атомарна одиниця
1	[0-9]	10	+
2	[a-z]	26	+
3	[A-Z]	26	+
4	Спеціальні символи (`~!@#$ %^&*()+-=/|<>[]'"\.,?:;{})	32	+
5	Пробіл	1	-

Таблиця 2 – Комбінація символів на основі таблиці 1

№	Комбінація символів	Кількість символів у наборі
1	[0-9] + [a-z]	36
2	[0-9] + [A-Z]	36
3	[a-Z] + [A-Z]	52
4	[0-9] + [a-Z] + [A-Z]	62
5	[0-9] + [a-Z] + [A-Z] + спеціальні символи	94
6	[0-9] + [a-Z] + [A-Z] + спеціальні символи + пробіл	95

то в 10 разів більше обчислювальних ресурсів для пошуку ключів із тою ж швидкістю. В іншому випадку, замість збільшення розміру ключа можна збільшувати кількість символів у наборі, тобто змінювати варіанти з таблиці 1.

Час, за який буде витрачено на підбір ключа за словником можна визначити за формулою (4):

$$t_{BF} = \frac{C_d}{S}, \tag{4}$$

де C_d – кількість ключів у словнику, а S – швидкість перебору, отримана за допомогою інструменту aircrack-ng із застосуванням прапорця – S.

Для того, щоб обійти захист технології Wi-Fi із методом автентифікації WPA2, окрім необхідних знань зловмисник повинен володіти певною обчислювальною потужністю. Проведення лобової атаки на пароль здійснюється за рахунок центрального процесора (ЦП), або графічного процесора (ГП). Швидкість роботи ГП у проведенні лобової атаки є значно вищою, але не кожен комп'ютер оснащується дискретною графічною карткою. Для пришвидшення лобової атаки, дана задача може виконуватись розподілено в кластері комп'ютерів.

Рівень захищеності приманки, яка імітує певну систему, не повинен бути значно вищим за рівень та можливості зловмисника, який очікується до взаємодії. Тобто, чим складніший ключ, тим потужнішою обчислювальною технікою потрібно володіти.

Введемо поняття обчислювальної одиниці, якою будемо вважати певний ресурс, який повинен виконати операцію перебору одного словника d_i.

Як вже було згадано, для лобової атаки можна використовувати розподілені системи. Сьогодні задля оптимізації використання обчислювальних ресурсів використовуються різні типи комп'ютерної віртуалізації. Серед них повна, часткова, пара-віртуалізація і віртуалізація на рівні ОС. Розглянемо такі два типи віртуалізації, як повна віртуалізація і віртуалізація на рівні операційної системи, яка ще також називається контейнеризацією.

Згідно з дослідженнями компанії IBM технологія віртуалізації KVM на операційній системі SUSE Linux Enterprise 11 збільшує споживання ресурсів в загальному на 15%. Також при використанні віртуалізації додаткові витрати у споживанні процесорного часу становлять на 3–4% більше, аніж без застосування віртуалізації.

У технології контейнеризації гіпервізор не використовується, що зменшує навантаження на апаратне забезпечення. Усі контейнери функціонують на базі лише серверного ядра. Для кожного контейнера створюється своє окреме, ізольоване середовище.

Як вже будо згадано вище, будь-яка технологія ізоляції приносить додаткові витрати. У випадку контейнеризації ці витрати складають від 0,1%–1%, за рахунок того, що використовуються прості перетворення. Наприклад ізоляція PID процесів виконується за допомогою додавання 4-байтного ідентифікатора, який позначає, якому контейнеру належить процес.

На рис. 1 наведено принципову відмінність між контейнеризацією та віртуалізацією.

Для перевірки умовної захищеності системи приманки велике значення має швидкість обробки даних, а отже перевага буде віддаватись технології, яка справляється із задачами перебору за словником швидше.

Задля оцінки складності подолання захисту методу автентифікації WPA/WPA2 зробимо його оцінку за рахунок коефіцієнтів методу аналізу ієрархій на основі таких критеріїв, як довжина ключа та кількість можливих символів у словнику. Даний метод дозволяє отримати співвідношення шкал від парних порівнянь із невеликим відхиленням [10–12]. В якості коефіцієнтів використовується фактичне вимірювання або суб'єктивна думка. На виході отримується співвідношення ваг та індекс узгодженості.

У стандартному виконанні методу аналізу ієрархій здійснюється оцінка будь-якої групи характеристик за допомогою шкали коефіцієнтів від 1 до 9. Кожна із характеристик порівнюється між собою, і виводиться матриця ваги кожного з елементів по відношенню одне до одного (5):

$$N = \begin{vmatrix} 1 & a_{12} & \cdots & a_{1n} \\ a_{12}^{-1} & 1 & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{1n}^{-1} & a_{2n}^{-1} & \cdots & 1 \end{vmatrix}. \tag{5}$$

З матриці N знаходяться суми коефіцієнтів для кожного стовпця (6), для подальшої нормалізації матриці N (7):

$$S_i = \sum_{i=1}^{n} a_i = a_{i1} + a_{i2} + ... + a_{in}. \tag{6}$$

а б

Рисунок 1 – Схематичне зображення відмінності між контейнеризацією та віртуалізацією:
а – віртуалізація; б – контейнеризація

$$|N| = \begin{vmatrix} \frac{1}{S_1} & \frac{a_{12}}{S_2} & \cdots & \frac{a_{1n}}{S_n} \\ \frac{a_{12}^{-1}}{S_1} & \frac{1}{S_2} & \cdots & \frac{a_{2n}}{S_n} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{a_{1n}^{-1}}{S_1} & \frac{a_{2n}^{-1}}{S_2} & \cdots & \frac{1}{S_n} \end{vmatrix}. \quad (7)$$

Просумувавши коефіцієнти кожного рядка нормалізованої матриці і розділивши суму на кількість коефіцієнтів рядка за допомогою (8), можна отримати вагу кожного з оцінюваних елементів:

$$x = \begin{bmatrix} \sum \frac{row_1}{n} \\ \sum \frac{row_k}{n} \\ \cdots \\ \sum \frac{row_k}{n} \end{bmatrix}. \quad (8)$$

Сума усіх ваг повинна бути рівною 100%, а отже, щоб отримати відсоткове значення складності ключа певної довжини, потрібно додати його вагу до суми попередніх.

4 ЕКСПЕРИМЕНТИ

У виведенні базового словника для лобової атаки було використано ресурс операційної системи Kali Linux. Kali Linux – це операційна система сімейства Linux, яка базується на дистрибутиві Debian, є безкоштовною і знаходиться у вільному доступі. Прямим призначенням даної операційної системи є тестування на проникнення. Але окрім тестувань власних систем не виключено, що такі операційні системи можуть використовуються зловмисниками для атак.

Автором було проаналізовано словники, які поставляються з операційною системою Kali Linux, і знаходяться у директорії /usr/share/wordlists. Дані словники фільтруються таким чином, щоб з них виключались усі слова-комбінації які менші за 8 символів, і ті, які не складаються із символів системи кодування ASCII цілком. Дані словники інтегруються в один, з якого виключаються не унікальні слова-комбінації (Лістинг 1).

Лістинг 1. Виведення базового словника для проведення лобової атаки на пакет рукостискання методу автентифікації WPA/WPA2 у операційній системі Kali Linux

```
cat dirbuster/*.txt fern-wifi/* rockyou.txt
fasttrack.txt metasploit/*.lst metasploit/*.txt
| grep ........ | grep -P -v “[^[:ascii:]]” |
sort –unique
```

Звичайно ж кожне тестування залежить від типу апаратного забезпечення, конфігурації програмного забезпечення. Автором було досліджено швидкість обчислення ключа для методу автентифікації WPA2 з попередньо перехопленого пакету «рукостискання».

Дослід проводився у контейнері віртуальної машини CoreOS, якій було виділено 1 Гб оперативної пам’яті і одне ядро процесора Intel Core i5-4590 з тактовою частотою 3,3 ГГц.

Попередньо було здійснено тестування за допомогою команди aircrack-ng – *S*, яка дозволяє здійснити замір швидкості лобової атаки у співвідношенні ключів за секунду.

5 РЕЗУЛЬТАТИ

Після виконання команди з лістингу 1 і підрахувавши кількість ключів, отримуємо значення C_d = 9801317.

Замір швидкості лобової атаки на двох різних системах віртуалізації і контейнеризації було проведено по 10 разів, результати представлено у табл. 3 та на рис. 2.

Використаємо формулу (5) і обчислимо середню швидкість для віртуалізації:

$$\overline{S}_V = \frac{922+956+954+955+927+911+949+947+933+912}{10} = 936{,}6.$$

Використаємо формулу (5) і обчислимо середню швидкість для контейнеризації:

$$\overline{S}_C = \frac{1053+1038+1038+1041+1031+1032+1038+1038+1054+1036}{10} = 1039{,}9.$$

Володіючи даними про кількість ключів у базовому словнику і швидкість з якою опрацьовуються ключі можемо скористатись формулою (4) і знайти приблизний час за який буде здійснено перебір усього базового словника:

$$t_{BF} = \frac{9801317}{1039{,}9} \approx 9425\,\text{сек.}$$

Якщо ж у базовому словнику ключ не буде знайдено, то пошук ключа буде розпочато із восьмисимвольного словника. Як вже було згадано вище, WPA2 дозволяє задати ключ довжиною від 8 до 63 символів, що еквівалентно 56 варіантам довжини ключа. Це означає, що кількість варіантів буде збільшено в десятеро при переході на наступний словник, а отже й потужності буде затребувано в десятеро більше.

Щоб застосувати метод аналізу ієрархій для даного дослідження, потрібно оцінити характеристики по відношенню одне до одного за шкалою від 1 до 9. Оскільки складність словника збільшується лінійно, тобто, щоразу у десять разів, то на відрізку від 1 до 9 ціною переходу від одного словника до іншого буде додавання до попереднього значення коефіцієнт 0,145454545 (рис. 3).

Таблиця 3 – Заміри швидкості перебору ключів за словником

Спроба / Тип віртуалізації	1	2	3	4	5	6	7	8	9	10
Повна віртуалізація (ключів/секунду)	922	956	954	955	927	911	949	947	933	912
Контейнеризація (ключів/секунду)	1053	1038	1038	1041	1031	1032	1038	1038	1054	1036

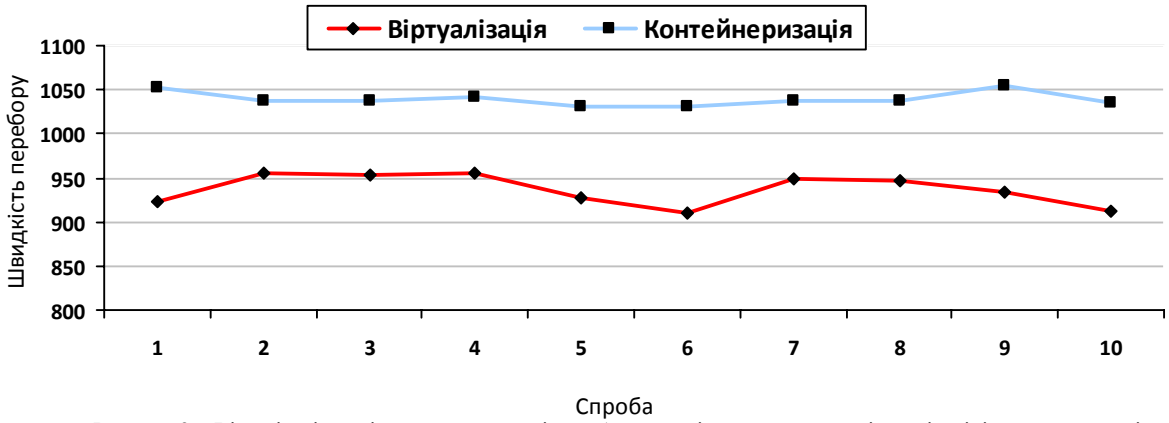

Рисунок 2 – Візуалізація порівняння швидкості перебору ключів за допомогою віртуалізації і контейнеризації

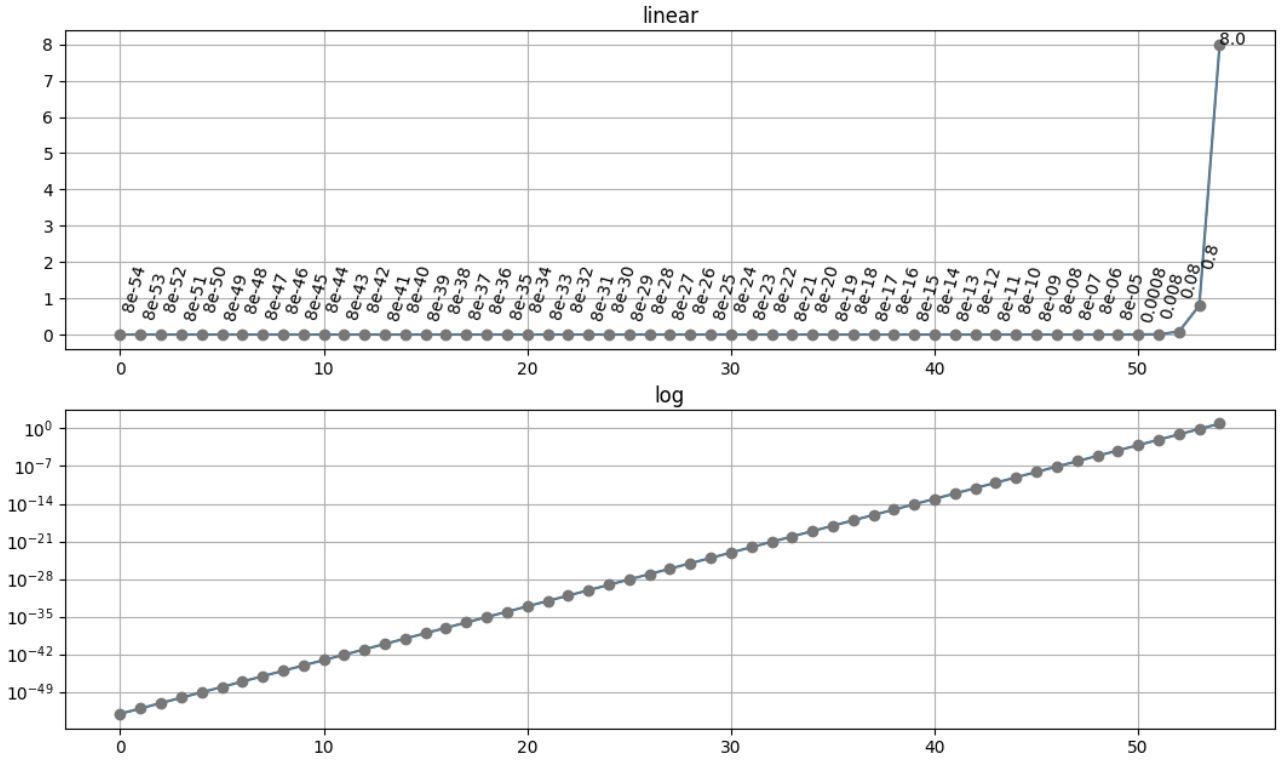

Рисунок 3 – Лінійне та логарифмічне представлення зміни складності словника у методі аналізу ієрархій

Використаємо формулу (6) для знаходження вагової матриці:

$$N = \begin{vmatrix} 1 & 1{,}145454545 & \cdots & 8{,}854545454 & 9 \\ 0{,}873015873 & 1 & \cdots & 8{,}709090909 & 8{,}854545454 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0{,}112936345 & 0{,}114822547 & \cdots & 1 & 1{,}145454545 \\ 0{,}111111111 & 0{,}112936345 & \cdots & 0{,}873015873 & 1 \end{vmatrix}.$$

Використаємо формулу (7) для знаходження суми коефіцієнтів для кожного рядка матриці N:

$$S = \begin{vmatrix} 280 \\ 271{,}873 \\ \vdots \\ 16{,}70776 \\ 15{,}67342 \end{vmatrix}.$$

Використаємо формулу (8) для знаходження нормалізованої матриці N:

$$|N| = \begin{vmatrix} \frac{1}{280} & \frac{1{,}145454545}{271{,}873} & \cdots & \frac{8{,}854545454}{16{,}70776} & \frac{9}{15{,}67342} \\ \frac{0{,}873015873}{280} & \frac{1}{271{,}873} & \cdots & \frac{8{,}709090909}{16{,}70776} & \frac{8{,}854545454}{15{,}67342} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \frac{0{,}112936345}{280} & \frac{0{,}114822547}{271{,}873} & \cdots & \frac{1}{16{,}70776} & \frac{1{,}145454545}{15{,}67342} \\ \frac{0{,}111111111}{280} & \frac{0{,}112936345}{271{,}873} & \cdots & \frac{0{,}873015873}{16{,}70776} & \frac{1}{15{,}67342} \end{vmatrix}$$

Застосуємо формулу (9) для отримання ваги кожного з оцінюваних елементів. Для отримання значень у відсотках матрицю x помножимо на 100.

$$x = \begin{vmatrix} 0{,}003011 \\ 0{,}003127 \\ \vdots \\ 0{,}051451 \\ 0{,}053967 \end{vmatrix} \cdot 100\% = \begin{vmatrix} 0{,}3011 \\ 0{,}3127 \\ \vdots \\ 5{,}1451 \\ 5{,}3967 \end{vmatrix}.$$

Тобто, вага словника із ключами довжиною у 8 символів складає 0,3011%, вага словника із ключами довжиною в 9 символів складає 0,3128%, вага словника із ключами довжиною в 63 символи складає 5,1451%, а вага словника із ключами довжиною в 64 символи складає 5,3967%.

Як вже було зазначено, довжина ключа не є єдиним критерієм оцінки його складності. Набір символів присутніх у словнику є також важливим критерієм. На основі таблиць 1 та 2 можемо зробити висновки про те, які комбінації символів у словниках є логічними для використання. Максимальна кількість символів, які можуть бути використані в паролі становить 95, тобто 95 символів складає 100%. Відповідно до цього отримуємо таблицю 4.

6 ОБГОВОРЕННЯ

Як можемо бачити, один контейнер опрацює базовий словник приблизно за дві з половиною години, коли віртуальній машині для цієї ж операції знадобиться приблизно три години. А отже, можемо зробити висновок, що контейнеризація є кращим варіантом для проведення розподіленої лобової атаки на ключ методу автентифікації WPA/WPA2 технології бездротового зв'язку Wi-Fi. З використанням контейнеризації продуктивність зростає приблизно на 11%.

Задля правильної оцінки умовної захищеності системи-приманки важливо, щоб система, яка проводить таку оцінку, якомога точніше відтворювала поведінку зловмисника. Звичайно ж, ні в якій системі не можливо врахувати людський фактор, та все ж певне наближення є можливим.

Особа яка атакує певну систему в будь-який момент може вирішити, що подальше продовження атаки є не доцільним, через час, який йде на дешифрування ключа, чи коштів, які вже вкладені в обчислювальну потужність.

Найпростішим варіантом з якого починають зловмисники – це використовувані ключі, що найбільше використовуютьсякористувачами. До такими ключами може бути інформація, яка несе в собі якусь логіку, наприклад, дані про саму ж точку доступу, її власника чи місце, де вона знаходиться. Тому очевидно, що атаку варто починати зі словника, який містить в собі таку інформацію.

Якщо у базовому словнику ключа не буде знайдено, то для обробки буде взятий найпростіший словник, згенерований лише з цифр від 0 до 9, довжина ключів в якому не перевищуватиме 8 символів. Процес підбору словника буде виконуватись до моменту, поки ключ не буде знайдений. Відповідно, чим складніший словник – тим більший ресурс буде виділено для пошуку ключа, і тим вищою буде оцінка захищеності умовного захисту системи-приманки. Найскладнішим буде словник, ключі якого генеруються з 95 різних символів таблиці ASCII, а довжина його складає 63 символи.

Власники бездротового обладнання Wi-Fi нечасто встановлюють складні паролі на доступ до мережі, і цим користуються зловмисники. Тому логічно, що атака не буде розпочата зі словника, у якому ключі є довжиною 63 символи. Складність ключа певної довжини буде дорівнювати сумі коефіцієнта його ваги з усіма попередніми. Відповідно до цього можемо вивести шкалу складності подолання методу автентифікації WPA2 для розміру ключа. Виключенням з правил може бути випадок, якщо зловмисник знає довжину ключа.

Перед тим, як обирати наступний словник, система оцінки повинна зробити вибір того критерію, який повинен бути змінений у наступному словнику – довжина ключів чи кількість символів, з яких можуть бути згенеровані ключі. Автором пропонується робити приорітетним словник, у якому середнім значенням від суми відсоткових співвідношень кількості символів і довжини ключа у наступних словниках є менше з двох варіантів (10):

$$P_k = \begin{cases} \dfrac{x_{k+1} + w_i}{2}, x_{k+1} + w_i < x_k + w_{i+1} \\ \dfrac{x_k + w_{i+1}}{2}, x_{k+1} + w_i > x_k + w_{i+1}. \end{cases} \quad (10)$$

Словник, на якому закінчується атака, і буде вважатись точкою для оцінки рівня кваліфікації і технічного оснащення зловмисника.

Даний підхід допоможе якнайшвидше провести оцінку рівня захищеності системи-приманки для бездротових мереж в яких використовуються методи автентифікації WPA/WPA2.

ВИСНОВКИ

Наукова новизна отриманих результатів полягає в тому, що вперше запропоновано метод оцінки стійкості ключа для методу автентифікації WPA/WPA2 мережі стандарту IEEE 802.11 для взаємодії зі зловмисником потрібного рівня кваліфікації і наявного у нього технічного забезпечення. Отримав подальший розвиток метод оцінки захищеності бездротових мереж стандарту IEEE 802.11 за допомогою методу аналізу ієрархій, оскільки було запропоновано метод оцінки не технології в цілому, а метод детальної оцінки методу автентифікації WPA2.

Практичне значення отриманих результатів полягає в тому, що запропоновано середовище для проведення оцінки умовної захищеності системи приманки із умо-

Таблиця 4 – Відсоткове співвідношення кількості символів у словниках

Кількість символів	95	94	62	52	36	32	26	10
Відсоткове представлення (w)	100	98,95	65,26	54,17	37,89	33,68	27,36	10,5

вами застосування масштабованості даної технології. Запропоновано метод генерування словників для проведення оцінки захищеності систем-приманок у бездротових мережах Wi-Fi, на яких використовується метод автентифікації WPA2, який дозволить уникнути повторення ключів і, тим самим, пришвидшить отримання результатів.

Перспективи подальших досліджень полягають в тому, що необхідним є створення детального механізму оцінки для інших методів автентифікації та механізмів захисту систем-приманок технології Wi-Fi.

ПОДЯКИ

Роботу виконано в рамках держбюджетної науково-дослідної теми Національного університету «Львівська політехніка» «Розвиток теоретичних засад створення комплексних систем безпеки автоматизованих і комунікаційних систем» (номер державної реєстрації 0115U006722).

СПИСОК ЛІТЕРАТУРИ

1. Lijuan Z. A Network Security Evaluation Method based on FUZZY and RST / Z. Lijuan, W. Qingxin // 2010 2nd International Conference on Education Technology and Computer (ICETC). 22–24 June 2010 : proceedings. – Shanghai, China : IEEE, 2010, P. 40–44.
2. Runfu Z. Security for Wireless Network Based on Fuzzy-AHP with Variable Weight / Z. Runfu, H. Lianfen, X. Mingbo // 2010 Second International Conference on Networks Security, Wireless Communications and Trusted Computing, 24–25 April 2010 : proceedings. – Wuhan, Hubei, China : IEEE, 2010. Vol. 2. – P. 490–493.
3. Ying-Chiang C. Hybrid Network Defense Model Based on Fuzzy Evaluation / C. Ying-Chiang, P Jen-Yi // The Scientific World Journal, 2014. – Vol. 2014. – P. 1-12.
4. Goel R. Wireless Honeypot: Framework, Architectures and Tools / R. Goel, A. Sardana, R. C. Joshi // International Journal of Network Security, 2013. – Vol. 15, No. 5. – P. 373–383.
5. Методи та засоби аналізу систем-приманок в процесі зламу / [В. Б. Дудикевич, А. З. Піскозуб, Н. П. Тимошик и др.] // Науково-технічний журнал «Захист інформації». – 2009. – № 1. – С. 27–31.
6. Ajah I. A. Evaluation of Enhanced Security Solutions in 802.11-Based Networks / I. A. Ajah // International Journal of Network Security & Its Applications (IJNSA). – 2014. – Vol. 6, No. 4. – P. 29–42.
7. Banakh R. External elements of honeypot for wireless network / R. Banakh, A. Piskozub, Y. Stefinko // Modern Problems of Radio Engineering, Telecommunications, and Computer Science: Proceedings of the XIIIth International Conference TCSET'2016. 23–26 February 2016 : proceedings. – Lviv-Slavsko, Ukraine : Lviv Publishing House of Lviv Polytechnic, 2016. – P. 480–482.
8. Banakh. R. Wi-Fi Honeypot as a service. Conception of business model / R. Banakh // Engineer of XXI century : VI inter university conference of students, PHD students and young scientists, 02 December 2016 : proceedings. – Bielsko-Biała, Poland : dr inż. Jacek Rysiński, 2016. – P. 59–64.
9. Morabito R. Hypervisors vs. Lightweight Virtualization: a Performance Comparison / R. Morabito, J. Kj ällman, M. Komu // 2015 IEEE International Conference on Cloud Engineering: First International Workshop on Container Technologies and Container Clouds, 19 March 2015: proceedings. – Tempe, Arizona : IC2E, 2015. – P. 386–393.

Стаття надійшла до редакції 20.04.2017.
Після доробки 23.05.2017.

Банах Р. И.
Аспирант кафедры защиты информации Национального университета «Львовская политехника», Львов, Украина

ОПРЕДЕЛЕНИЕ ПАРАМЕТРОВ КЛЮЧА МЕТОДА АУТЕНТИФИКАЦИИ WPA/WPA2 ДЛЯ СИСТЕМЫ-ПРИМАНКИ СЕТИ СТАНДАРТА IEEE 802.11

Актуальность. Открытым есть вопрос правильности конфигурации систем-приманок, особенно это касается систем-приманок, имитирующих беспроводные сети, поскольку их клиенты мобильны, а контролируема зона часто не ограничена. Неправильная конфигурация системы-приманки может стать бескорыстной нагрузкой в середине автоматизированной системы, особенно это касается системы-приманки для беспроводных сетей стандарта IEEE 802.11. Система-приманка с низким или отсутствующим уровнем защиты может вызвать подозрение у опытного злоумышленника, в худшем же случае она станет легкой добычей нарушителей, целью которых является лишь доступ к ресурсу Интернет. С другой стороны, использование системы-приманки с максимальным уровнем защиты также не имеет смысла, поскольку такая модель станет недоступной крепостью для злоумышленника.

Наиболее защищенными считаются точки доступа на которых используется метод аутентификации WPA/WPA2, применение которого вероятно даст уверенность злоумышленнику в том, что он атакует легитимную систему.

Целью работы является разработка диагностической модели для систем-приманок беспроводных сетей стандарта IEEE 802.11, для условной защиты которой используется метод аутентификации WPA/WPA2. Такая модель поможет оценить текущую конфигурацию точки доступа на вероятность использования известных уязвимостей метода аутентификации WPA/WPA со стороны злоумышленников нужного уровня подготовленности.

Метод. Предложен метод оценки квалифицированности злоумышленника и его технической оснащенности путем подбора параметров ключа WPA/WPA2 для системы-приманки в беспроводной сети стандарта IEEE 802.11. Реализация данного метода позволит достичь уменьшения нагрузки на систему-приманку, прежде всего создаст иллюзию подлинности для злоумышленника. Предложен метод распределенной атаки грубой силы на метод аутентификации WPA/WPA2, который обеспечивает диагностику устойчивости ключа системы-приманки в сети Wi-Fi. Проведено сравнение аппаратной виртуализации с виртуализацией на уровне операционной системы при одинаковых условиях в рамках атаки грубой силы на механизм аутентификации WPA/WPA2.

Результаты. Получены оптимальные условия для проведения распределенной атаки грубой силы в виртуальной среде, что позволяет относительно быстро оценить уровень защищенности системы-приманки.

Выводы. Предложен метод оценки устойчивости ключа для метода аутентификации WPA/WPA2 сети стандарта IEEE 802.11 для взаимодействия со злоумышленником нужного уровня квалификации и имеющегося у него технического обеспечения. Дальнейшее развитие получил метод оценки защищенности беспроводных сетей стандарта IEEE 802.11 с помощью метода анализа иерархий. Предложено среду для проведения оценки условной защищенности системы-приманки с условиями применения масштабируемости данной технологии; метод генерирования словарей для проведения оценки защищенности систем-приманок, который позволит избежать повторения ключей и, тем самым, ускорит получение результатов.

Ключевые слова: IEEE 802.11, Wi-Fi, система-приманка, оценка защищенности, метод анализа иерархий.

Banakh R. I.
Post-graduate Student of Information Security Department, Lviv Polytechnic National University, Lviv, Ukraine

AUTHENTICATION METHOD WPA/WPA2 KEY PARAMETERS' DEFINITION FOR IEEE 802.11 BASED HONEYPOT

Context. An issue of correct configuration of honeypots is still opened, especially it is about honeypots that simulate wireless networks as their clients are mobile and zone of control is not limited. Wrong configuration of honeypot may become its usage disinterested inside automated system especially it is applicable to honeypots for IEEE 802.11 wireless networks. Honeypot with open (no authentication) method or with low security may be suspicious for experienced attacker otherwise, it become easy prey for attackers whose goal is just access to Internet. On the other hand, usage of honeypot with strong security level make no sense as well, as this model will become unconquerable for attackers.

Most protected access points use authentication method WPA2, usage of which may assure attacker that he/she attacks legitimate system.

Objective. The goal of the researching work is to develop diagnostic model for honeypots in IEEE 802.11 wireless networks, which is conditionally secured by authentication method WPA/WPA2. Proposed model can help to assess possibility to leverage known WPA vulnerabilities by attacker on access point with given configuration.

Method. An evaluation method of attacker's qualification and its technical set of equipment in way of WPA/WPA2 encryption key selection for wireless honeypot is offered. Implementation of this method allows to reach load reduction on honeypot what will provide an illusion of system authenticity for attacker. Method of distributed brute force attack on authentication method WPA/WPA2 that provides diagnostic of Wi-Fi honeypot for encryption key resistance is offered. A Comparison between hardware virtualization and OS-level virtualization is provided under the identical conditions in scope of WPA2 handshake brute force task.

Results. Optimal conditions for providing brute force attack in virtual environment are obtained, what can give possibility to quickly assess security level honeypot. This information can be used to understand how qualified attacker should be.

Conclusions. A method of key perseverance assessment for authentication method WPA/WPA2 in IEEE 802.11 wireless network is proposed, for interaction with attacker with needed qualification level and computing resources. A method of IEEE 802.11 wireless networks security assessment using Analytics Hierarchy Process got further development. The scalable environment for honeypots assessment providing is offered. The method of wordlist generation and rotation that are delivered to assessment system is proposed, what can help to exclude key reduplication what in its turn will help to speedup of assessment results.

Keywords: IEEE 802.11, Wi-Fi, honeypot, security assessment, analytic hierarchy process.

REFERENCES

1. Lijuan Z., Qingxin W. *A Network Security Evaluation Method based on FUZZY and RST, 2010 2nd International Conference on Education Technology and Computer (ICETC), 22–24 June 2010 : proceedings*. Shanghai, China, IEEE, 2010, pp. 40–44.
2. Runfu Z., Lianfen H., Mingbo X. Security for Wireless Network Based on Fuzzy-AHP with Variable Weight, *2010 Second International Conference on Networks Security, Wireless Communications and Trusted Computing, 24–25 April 2010 : proceedings*. Wuhan, Hubei, China, IEEE, 2010, Vol. 2, pp. 490–493.
3. Ying-Chiang C., Jen-Yi P. Hybrid Network Defense Model Based on Fuzzy Evaluation, *The Scientific World Journal*, 2014, Vol. 2014, pp. 1–12.
4. Goel R., Sardana A., Joshi R. C. Wireless Honeypot: Framework, Architectures and Tools, *International Journal of Network Security*, 2013, Vol. 15, No. 5, pp. 373–383.
5. Dudykevych V. B., Piskozub A. Z., Tymoshyk N. P., Tymoshyk R. P., Dutkevych T. V. Metody ta zasoby analizu system-prymanok v procesi zlamu, *Naukovo-tehnichnyui zhurnal «Zahyst informatsii»*, 2009, No. 1, pp. 27–31.
6. Ajah I. A. Evaluation of Enhanced Security Solutions in 802.11-Based Networks, *International Journal of Network Security & Its Applications (IJNSA)*, 2014, Vol. 6, No. 4, pp. 29–42.
7. Banakh R., Piskozub A., Stefinko Y. External elements of honeypot for wireless network, *Modern Problems of Radio Engineering, Telecommunications, and Computer Science, Proceedings of the XIIIth International Conference TCSET'2016. 23–26 February 2016 : proceedings.* Lviv-Slavsko, Ukraine, Lviv Publishing House of Lviv Polytechnic, 2016, pp. 480–482.
8. Banakh R. Wi-Fi Honeypot as a service. *Conception of business model, Engineer of XXI century : VI inter university conference of students, PHD students and young scientists, 02 December 2016 : proceedings*. Bielsko-Biała, Poland : dr inż. Jacek Rysiński, 2016, pp. 59–64.
9. Morabito R., Kjä llman J., Komu M. Hypervisors vs. Lightweight Virtualization: a Performance Comparison, *2015 IEEE International Conference on Cloud Engineering: First International Workshop on Container Technologies and Container Clouds, 19 March 2015: proceedings.* Tempe, Arizona, IC2E, 2015, pp. 386–393.