ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РЕСПУБЛИКИ КАЗАХСТАН

ҚазҰТЗУ ХАБАРШЫСЫ

ВЕСТНИК КазНИТУ

VESTNIK KazNRTU

№ 5 (135)

АЛМАТЫ 2019 ОКТЯБРЬ

ISSN 1680-9211

Учредитель:

Казахский национальный исследовательский технический университет
имени К.И. Сатпаева

Регистрация:

Министерство культуры, информации и общественного согласия
Республики Казахстан № 951 – Ж "25" 11. 1999 г.

Основан в августе 1994 г. Выходит 6 раз в год

Адрес редакции:

г. Алматы, ул. Сатпаева, 22,
каб. 609, тел. 292-63-46
Nina. Fedorovna. 52 @ mail.ru

[8] Варвак П.М., Варвак Л.П. Метод сеток в задачах расчета строительных конструкций. М.: Стройиздат. – 1977. – 160 с.

[9] Дарков А.В., Шапошников Н.Н. Строительная механика. М.: Высшая школа, – 1986. – 607 с.

[10] Ахмедиев С.К., Филиппова Т.С., Орынтаева Г.Ж., Доненбаев Б.С. Аналитические и численные методы расчетов машиностроительных и транспортных конструкции и сооружений. Караганда: КарГТУ. – 2016. –158с.

Ахмедиев С.К., Хабидолда О., Жолмагамбетова Б.Р., Мәдібайқызы Ж., Сахтаганов А.З.

Сатылы-айнымалы көлденең қиманың консоль өзегінің күйін қалыптастыру

Түйіндеме: Аталған жұмыста ұзындығы бойынша сатылы-айнымалы иілімді қаттылықты консоль өзегінің иілімдік деформацияланған күйін зерттеу жүргізілген. Ұқсас конструкциялар түрлі электр тарату желілерінің және т.б құрылыста кеңінен қолданылады.

Көптеген осындай міндеттерді шешу әдістерінің арасында n=10, 20 қолығында жиі желілік тормен ақырғы айырымдар сандық әдісі ұсынылады.

Сырткы жүктеме мен айнымалы иілімді қаттылықты ескеруге мүмкіндік беретін рұқсат етілетін есептеу матрицалары алынған. Зерттеу нәтижелері бойынша өзектің ұзындығы бойынша тор тізбектерінде иілулер алынған. Аналитикалық және басқа сандық әдістермен алынған нәтижелрді салыстыру жүргізілген.

Бұл жұмыстың ғылыми және қолданбалы нәтижелері қатты деформацияланатын дене механикасында кең қолданыс табады.

Түйінді сөздер: сырткы әсерлер, сатылы-айнымалы қима өзегі, жел жүктемесі, орын ауыстырулар, иілім, ақырғы айырымдар әдісі.

УДК 004.05

M.Y. Aidyn, Sh.Zh. Mussiraliyeva
(Al-Farabi Kazakh National University, Almaty, Kazakhstan
Email: {aidynme, mussiraliyevashasure@gmail.com)

VULNERABILITY ANALYSIS OF GSM NETWORK IN KAZAKHSTAN BY APPLYING OSMOCOM PROJECT

Abstract. This article analyzes the security level of Kazakhstani GSM and GPRS networks using the OsmocomBB project, which aimed at the free (Open Source) implementation of the GSM protocol stack. In order to perform the experimental work, a stand was assembled consisting of two mobile devices that work on the basis of the Calypso chipset, 2 USB-UART converters, 2 mini jack 2.5 mm TRS. Ubuntu OS 14.04 was chosen for work. OsmocomBB was used to understand the processes of the GSM system, as well as to implement the following attacks: listening to any information from the GSM network; locating the existing mobile base station in the selected square, finding out what the mobile base station broadcasts; identifying temporary names of cellular tower subscribers (TMSI); cloning it into our phone (in order to connect to the network instead of the original subscriber); intercepting SMS; and decoding by using rainbow tables and Kraken utility. During the study, the possibility of these attacks on local GSM networks was assessed. All information presented on this article is intended for educational purposes only.

Key words: mobile networks, gsm hacking, privacy, network vulnerability, osmocom, hardware exploitation

М.Е. Айдын, Ш.Ж. Мусиралиева
(Al-Farabi Kazakh National University, Almaty, Kazakhstan {aidynme, mussiraliyevash}@gmail.com)

ПРИМЕНЕНИЕ ПРОЕКТА OSMOCOM ДЛЯ АНАЛИЗА УЯЗВИМОСТЕЙ GSM СЕТЕЙ В КАЗАХСТАНЕ

Аннотация. В статье анализируется безопасность казахстанских GSM и GPRS сетей с использованием проекта OsmocomBB, целью которого является свободная (Open Source) имплементация стека протоколов GSM. Для выполнения экспериментальных работ был собран стенд состоящий из 2 мобильных устройств, которые работают на базе чипсета Calypso, 2 USB-UART конвертера, 2 mini jack 2.5 mm TRS, для работы была выбрана ОС Ubuntu 14.04. OsmocomBB использовался для понимания процессов системы GSM, а также для реализации следующих атак: прослушивание любой информации из GSM сети; определение существующих мобильных базовых станции в выбранном квадрате, выяснить о чем вещает мобильная базовая станция; идентификация временных имен абонентов сотовой вышки (TMSI); клонирование его в наш телефон, в целях подключения к сети вместо исходного абонента; перехватить SMS; расшифрование с помощью радужных таблиц и утилиты Kraken. В ходе исследования, возможность этих атак на местных GSM сетей была оценена. Вся информация, представленная на этой статье, предназначена только для образовательных целей.

Ключевые слова: мобильные сети, gsm-взлом, конфиденциальность, сетевая уязвимость, osmocom, аппаратная эксплуатация.

Введение

В течение последних двух десятилетий мобильные устройства, такие как смартфоны стали вездесущими [1]. Сфера охвата систем мобильной связи, начиная с Глобальной системы мобильной связи второго поколения (2G / GSM) и Универсальных систем мобильной связи третьего поколения (3G / UMTS), распространилась на все уголки мира. Мобильная связь является важным краеугольным камнем в жизни подавляющего большинства людей и обществ на этой планете. Последнее поколение в этой эволюции, системы четвертого поколения «Long Term Evolution» (4G/LTE) широко используются. Прогнозируется, что количество подписок LTE в мире вырастет с 1,73 млрд. (конец 2016 г.) до 4,33 млрд. (конец 2021 г.), когда LTE будет составлять более 52% всех мобильных подписок.

В то время, как по всему миру идет процесс отключения сетей от 2G, мобильные операторы Казахстана пока не планируют идти на этот шаг из-за большого количества абонентов, которые пользуются кнопочными телефонами [7]. К тому же, в начале апреля 2016 года в Казахстане вступил в силу запрет на использование государственными служащими на рабочих местах смартфонов, то есть разрешены устройства поддерживающие только 2G связь.

Ранние системы 2G, как было известно, имели несколько уязвимостей [1]. Например, отсутствие взаимной аутентификации между мобильными пользователями и сетью означало, что злоумышленник мог установить поддельные базовые станции и убедить законные мобильные устройства подключиться к нему. Чтобы минимизировать воздействие пользовательских идентификаторов (известных как Международный идентификатор мобильного абонента или IMSI) в беспроводных сигнальных сообщениях, системы 2G ввели использование временных мобильных идентификаторов абонентов. Однако в отсутствие взаимной аутентификации поддельные базовые станции использовались в качестве «ловушек IMSI» для сбора IMSI и отслеживания перемещений пользователей.

Обзор литературы

В 2017 году используя проект Osmocom, исследователи UnicornTeam, одной из трех исследовательских команд альянса инновационных исследований в области кибербезопасности – 360 Technology, продемонстрировали новую уязвимость в CSFB (Circuit Switched Fallback) в сети 4G LTE и подробно описали в работе «Inside Radio: An Attack and Defense Guide» [8]. Данная атака, названная «Ghost Telephonist», позволяет злоумышленнику выдавать себя за жертву. Последствия этой атаки включают в себя: (1) Злоумышленник может выдать себя за вызываемого абонента и получить содержимое входящих вызовов или SMS. (2) Злоумышленник может выдать себя за абонента и инициировать вызов/SMS другим. (3) Злоумышленник может получить номер телефона жертвы, а затем использовать номер телефона, чтобы осуществить следующую атаку, например, сбросить пароль интернет-аккаунта жертвы. Эти эксплуатации могут нацеливаться на выбранную или случайную жертву. Жертва не будет знать об атаке, поскольку поддельная базовая станция не используется и не происходит повторный выбор соты. Исследователи внедрили собственную полосу частот на основе OsmocomBB и проверили уязвимость с помощью собственных телефонов в сети двух операторов. Эксперименты подтверждают, что уязвимость действительно существует.

Также в 2018 году исследователи из Рурского университета продемонстрировали актуальные уязвимости в работе «Breaking LTE on Layer Two» [4]. В работе представлен комплексный анализ безопасности второго уровня и определены три вектора атак. Впервые представлены пассивные атаки с отображением идентификаторов, которая сопоставляет изменчивые идентификаторы радиосвязи с более длительными сетевыми идентификаторами, что позволяет идентифицировать пользователей внутри ячейки и служит отправной точкой для последующих атак. Во-вторых, демонстрировали, как пассивный злоумышленник может злоупотреблять распределением ресурсов в качестве побочного канала для выполнения идентификации веб-сайтов, которая позволяет злоумышленнику изучать веб-сайты, к которым пользователь обращался. Также, описана атака ALTER, которая использует тот факт, что пользовательские данные LTE зашифрованы в режиме счетчика (AES-CTR), но не защищены целостностью, что позволяет изменять полезную нагрузку сообщения [12]. В качестве демонстрации концепции показаны, как активный злоумышленник может перенаправить DNS-запросы, а затем выполнить спуфинговую атаку DNS. В результате пользователь перенаправляется на вредоносный веб-сайт. Экспериментальный анализ демонстрирует реальную применимость всех трех атак и подчеркивает угрозу открытых векторов атак на протоколах второго уровня LTE.

Методы и инструменты

Архитектура сотовой связи

Технология GSM основана на методах передачи с множественным доступом с временным разделением (TDMA), в то время как его радиоинтерфейс работает в диапазонах 900 МГц и 1,8 ГГц в Европе, а также в США на частотах 850 МГц и 1,9 ГГц [2]. Схема архитектуры GSM изображена на рисунке 1. Мобильная станция (MS) содержит карту мобильного телефона и модуля идентификации абонента (SIM) и взаимодействует с базовой приемопередающей станцией (BTS) по радиоинтерфейсу. BTS отвечает за радиопокрытие данной географической области, в то время как контроллер базовой станции (BSC) поддерживает радиосвязи с MS и наземные соединения с фиксированной частью сети (базовой сетью). И BTS, и BSC составляют подсистему базовой станции (BSS), которая управляет радиотрактом GSM. Зона обслуживания GSM разделена на области местоположения (LA), где каждый LA включает в себя одну или несколько радиоячеек. Каждая LA и радиоячейка имеют уникальный идентификатор, называемый кодом зоны расположения (LAC) и Cell-ID, соответственно. Базовая сеть GSM в основном включает в себя домашний регистр местоположения / центр аутентификации (HLR / AuC), регистр местоположения посетителей (VLR) и центр коммутации мобильной связи (MSC). HLR / AuC - это база данных, используемая для управления постоянными данными мобильных пользователей, а также хранит информацию о безопасности, связанную с идентификацией абонентов. VLR является базой данных зоны обслуживания, которую посещает MS, и содержит всю связанную информацию, необходимую для обработки услуги MS. MSC является сетевым элементом, отвечающим за услуги с коммутацией каналов, и обеспечивает подключение к телефонной сети общего пользования (PSTN).

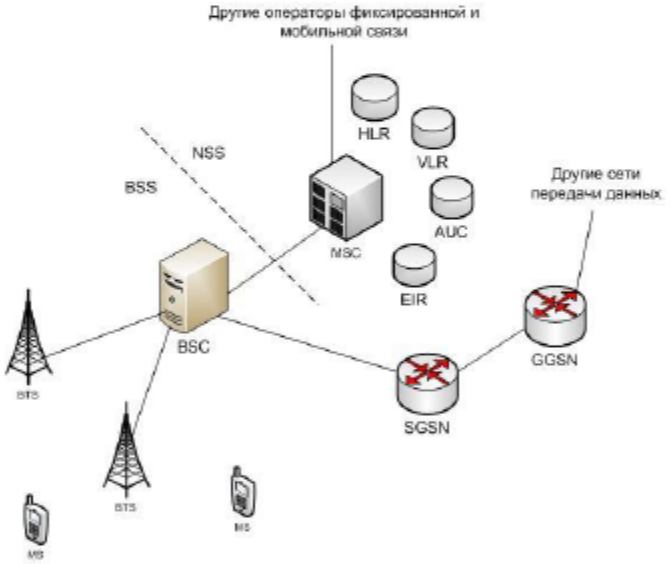

Рис.1. Схема архитектуры GSM

Идентификаторы в GSM

Одной из главных задач сети GSM является определение местоположения абонента [9]. Для этого используются специальные идентификаторы, представляющие собой некоторые уникальные номера.

Рассмотрим каждый идентификатор. В дальнейшем это будет необходимо для понимания основных процессов, происходящих в сети GSM.

- IMSI [250001234567890] – международный идентификатор мобильного абонента записан в SIM-карте

- MSISDN [79001234567] – телефонный номер мобильного абонента, привязанный к IMSI в инфраструктуре оператора

- TMSI [0x12bc34fa] – временный идентификатор мобильного телефона назначается случайным образом каждому мобильному устройству в пределах определенной территории

- IMEI [351986061639790] – международный идентификатор мобильного оборудования, уникален для каждого мобильного телефона

Стек протокола GSM

Стек протоколов состоит из 3 уровней [3]. Уровни 1 и 2 являются физическим и канальным уровнями. Слой 3 состоит из 3 частей. Это известно как уровень сообщения или сигнализации. Физический уровень определяет, как данные передаются от одного объекта другому через физическую транспортную среду. Транспортный уровень между MS и BSS является радиолинией. Физический уровень между BSS и MSC - это протокол уровня MTP 1 набора протоколов SS7 [10]. Канальный уровень обеспечивает обнаружение и исправление ошибок. Протокол LAPD используется по радиоинтерфейсу. Протокол MTP уровня 2 из набора протоколов SS7 используется через A-интерфейс. Три разные части уровня сообщений управляют ресурсами сотовой радиосети: 1. Управление радиоресурсами (RR) 2. Управление мобильностью (MM) 3. Управление вызовами (CM). Стек протокола GSM подробно изображена на рисунке 2.

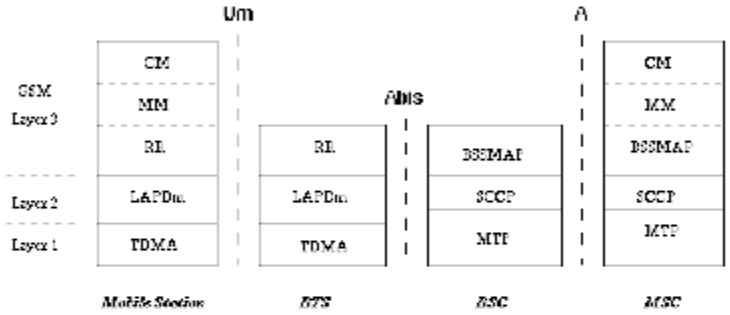

Рис. 2. Стек протокола GSM

Экспериментальный стенд

Был собран экспериментальный стенд, состоящий из 2 мобильных устройств, которые работают на базе чипсета Calypso, 2 USB-UART конвертера, 2 mini jack 2.5 mm TRS, для работы была выбрана ОС Ubuntu 14.04.

Телефон

Osmocom-bb реализует клиентскую часть протокола GSM. Для этого используются телефоны на базе чипсета calypso и mediatek. Для эксперимента был выбран телефоны, которые изображены на рисунке 3.

Рис. 3. Motorola C118 и Motorola C123

USB конвертер и Mini jack 2.5 mm

Наиболее стабильным USB-TTL конвертером является CP2102. Для возможности работы на нестандартных скоростях необходимо перепрошить устройство.

Motorola на базе чипсета calypso поддерживает обычный трёхконтактный (TRS) minijack 2.5 mm. Чтобы присоединить конвертер к Mini jack нужно подключить следующим образом:

TXD – наконечник, RXD – середина, GND - нижняя часть. Выбранные устройства показаны на рисунке 4.

Рис. 4. USB-TTL CP2102 и Mini jack 2.5 mm

Программного обеспечение
В качестве операционной системы был выбран Ubuntu 14.04 32bit.

Результаты и анализ. Вся информация, представленная на этой статье, предназначена только для образовательных целей. Была собрана библиотека: libosmocore – основная библиотека проекта, кросс-компилятор и OsmocomBB. На рисунке 5 можно увидеть телефон работающий в режиме Layer 1.

Рис. 5. Подключенный к компьютеру Motorola C118 в режиме Layer 1

Определяем какие мобильные базовые станции есть в округе
После того, как прошивка загрузилась, в выводе терминала будет системная информация о ближайшей базовой станции. Есть возможность менять канал (ARFCN). С вышкой можно синхронизироваться, если нажать на «кнопку вызова», тогда будет выдано ещё больше информации, которые изображены на рисуноке 6.

Рис. 6. Системная информация о ближайшей базовой станции

Здесь MMC (Mobile Country Code) - код страны, MNC (Mobile Network Code) - код оператора, LAC (Location Area Code) - код локальной зоны. LAC - это объединение некоторого количества базовых станций, которые обслуживаются одним контроллером базовых станций (BSC). cell id - идентификатор базовой станции [13].

Учитывая то, что телефон подключён к сети для экстренных вызовов, можно определить примерное местоположение телефона.

Перехват SMS

Используя уже известный ARFCN, запускаем команду gr-gsm для записи трафика. После, начинаем анализировать трафик с помощью программы Wireshark. Необходимо убедиться, какой алгоритм шифрования применяет оператор сотовой связи. В программе Wireshark раскрываем пакет Ciphering Mode Command, поле Algorithm identifier. В данном случае это - алгоритм шифрования A5/1.

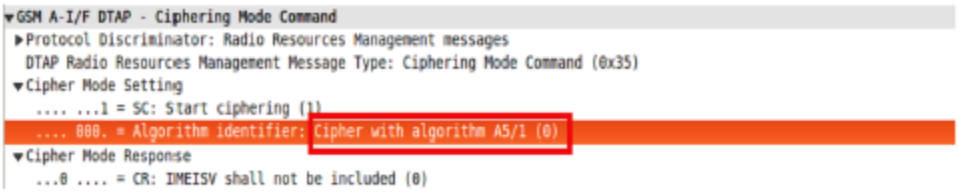

Рис. 6. Ciphering mode command

Шифрование A5/1 не является гарантией защиты данных – при помощи радужных таблиц и утилиты Kraken ключ шифрования можно найти буквально за несколько минут в 90 процентах случаев [5]. В случае успешного нахождения ключа шифрования программа выдаст ключ с параметром *MATCHED*. Запускаем программу Wireshark на просмотр трафика локальной петли и декодируем файл радиоэфира, задав ключ шифрования. Переходим в программу Wireshark, и находим GSM_SMS. На рисунке 7 можно увидеть информацию с номером отправителя и текстом сообщения.

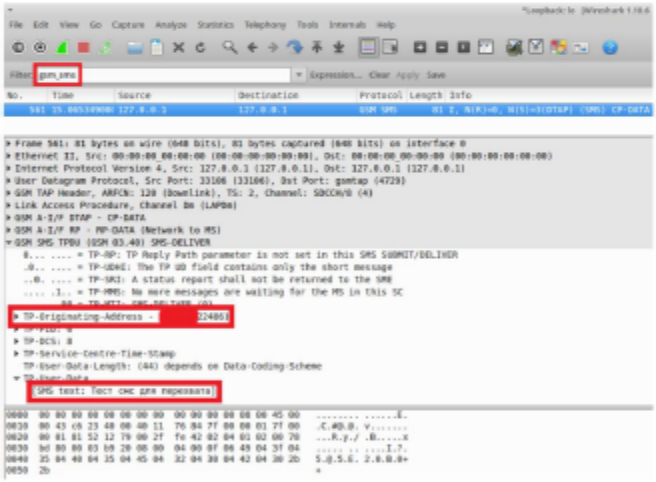

Рис. 7. Информация с номером отправителя и текстом сообщения

Идентификация TMSI абонентов сотовой вышки

Когда новый абонент GSM включает свой телефон в первый раз, его IMSI передается на AuC в сети [6]. После чего абоненту назначается временная идентификация мобильного абонента (TMSI). IMSI редко передается по этой точке, если это не является абсолютно необходимым. Это препятствует тому, чтобы потенциальный перехватчик идентифицировал пользователя GSM по их IMSI. Пользователь продолжает использовать тот же TMSI, в зависимости от того, как часто происходят обновления местоположения. Каждый раз, когда происходит обновление местоположения, сеть назначает новый TMSI для мобильного телефона. TMSI хранится вместе с IMSI в сети. Мобильная станция использует TMSI для сообщения в сеть или во время инициирования вызова [11]. Точно так же сеть использует TMSI, чтобы общаться с мобильной станцией. Регистр местонахождения посетителя (VLR) выполняет назначение, администрирование и обновление TMSI. Когда он выключен, мобильная станция сохраняет TMSI на SIM-карте, чтобы обеспечить его доступность при повторном включении.

Анализируя трафик с помощью программы Wireshark можно обнаружить TMSI абонента. Поскольку назначение TMSI отправляется после того, как шифрование включено, доступ между TMSI и подписчиком не могут быть получены неавторизованными пользователями.

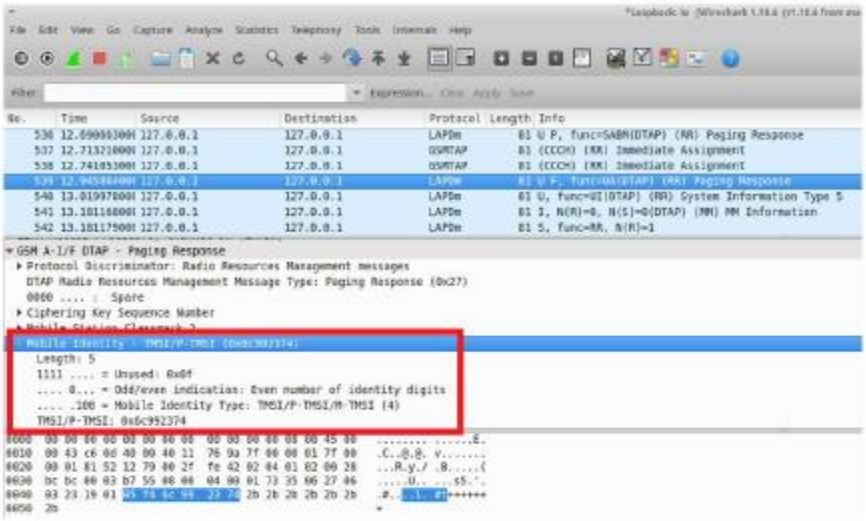

Рис. 8. TMSI абонента

В дальнейшей работе попробуем с помощью TMSI идентифицировать настоящие имена абонентов сотовой вышки (IMSI), и клонировать TMSI и подключиться к сети вместо исходного абонента.

Заключение. GSM и GPRS являются устаревшими системами, которые широко используются и вероятно, будут оставаться актуальными в течение длительного времени, но их защита устарела. Реализуя стек протоколов GSM на стороне MS, работающий на платформе на основе Calypso, позволяет глубоко контролировать сторону сети мобильного телефона.

В этой работе были проанализированы несколько типов атак, которые стали возможны благодаря проекту OsmocomBB с акцентом на систему GSM.

Еще много работы можно сделать над проектом OsmocomBB. Например, потестировать атаку «Ghost Telephonist», полностью клонировать TMSI абонента сети и др.

Глобальное улучшение проекта может принести пользу исследованиям в области безопасности GSM и GPRS. Надеемся, что он будет расти и стимулировать операторов, а также производителей оборудования для повышения безопасности своих продуктов.

ЛИТЕРАТУРА

[1] Altaf S., Ravishankar B., Practical Attacks Against Privacy and Availability in 4G/LTE Mobile Communication Systems [Текст]. / NDSS. – 2016.

[2] Pönsgen, Francois Louis, GSM and GPRS Security Using OsmocomBB [Текст]. / NTNU. – 2015.

[3] Christoforos Ntantogian, Grigoris Valtas, Nikos Kapetanakis, Faidon Lalagiannis, Georgios Karopoulos, Christos Xenakis, Attacking GSM Networks as a Script Kiddie Using Commodity Hardware and Software [Текст]. / 0302-9743. – 2015.

[4] David Rupprecht, Katharina Kohls, Thorsten Holz, Breaking LTE on Layer Two [Текст]. / IEEE S&P'19. – 2018.

[5] Уязвимости 2G. Режим доступа: https://radio-secure.ru/secure/2g/20-2g#f — Загл. с экрана. — Яз. рус. (дата обращения: 01.03.2019).

[6] The MiTM Mobile Contest: GSM Network Down at PHDays V. Режим доступа: http://blog.ptsecurity.com/2015/07/the-mitm-mobile-contest-gsm-network.html — Загл. с экрана. — Яз. анг. (дата обращения: 01.03.2019).

[7] Мировой тренд отказа от 2G. Режим доступа: https://tengrinews.kz/kazakhstan_news/mirovoy-trend-otkaza-2G-stoit-volnovatsya-obladatelyam-327751/ — Загл. с экрана. — Яз. рус. (дата обращения: 01.03.2019).

[8] Yang, Qing, Huang, Lin, Inside Radio: An Attack and Defense Guide [Текст]. / Springer Beijing. – 2018.
[9] Active analysis of a gsm call through. Режим доступа: osmocom-bb https://payatu.com/active-analysis-gsm-call-osmocom-bb/ — Загл. с экрана. — Яз. анг. (дата обращения: 01.03.2019).
[10] Как работает радиоинтерфейс в GSM-сетях. Режим доступа: https://habr.com/ru/post/268127/ — Загл. с экрана. — Яз. рус. (дата обращения: 01.03.2019).
[11] Karl Norrman, Mats Naslund, Protecting IMSI and User Privacy in 5G Networks [Текст]. / 9th EAI International Conference on Mobile Multimedia Communications. – 2016.
[12] Raheem Beyah, Bing Chang, Yingjiu Li, International Conference on Security and Privacy in Communication Networks [Текст]. / Springer International Publishing. – 2018.
[13] Скрытые аспекты безопасности в GSM-сетях. Режим доступа: https://alien-roger.livejournal.com/22266.html — Загл. с экрана. — Яз. рус. (дата обращения: 01.03.2019).

Айдын М.Е., Мусиралиева Ш.Ж.

Osmocom жобасын Қазақстандағы GSM желілерінің осалдықтарын талдау үшін қолдану

Резюме.Бұл мақалада GSM және GPRS желілерінің қауіпсіздігі OsmocomBB жобасын қолдану арқылы талданады. Эксперименттік жұмыстарды орындау үшін Calypso чипсеті нұсқасы негізінде жұмыс істейтін 2 мобильді құрылғы, 2 USB-UART түрлендіргіші, 2,5 мм TRS 2 шағын ұясы, Ubuntu 14.04 операциялық жүйесі таңдалды. OsmocomBB GSM жүйесінің процестерін түсіну үшін, сондай-ақ келесідей шабуылдарды жүзеге асыру үшін пайдаланылды: GSM желісінен кез-келген ақпаратты тыңдау; таңдалған аумақта қолданыстағы мобильді базалық станцияны анықтау; мобильдік базалық станцияның таратқан хабарын анықтау; Ұялы абоненттерінің уақытша атауларын (TMSI) анықтау; бастапқы абоненттің орнына желіге қосылу үшін таңдалған телефонға оны көшіру; SMS-ті жолай ұстау; Kraken утилитасын пайдалану арқылы декодтау. Зерттеу кезінде жергілікті шабуылдардың GSM желілеріне ықтималдығы бағаланды. Осы мақалада ұсынылған барлық ақпарат тек білім алу мақсаттарына арналған.

Кілттік сөздер: ұялы желілер, gsm, құпиялылық, желідегі осалдық, osmocom, аппараттық жұмыс.

УДК 65.01.005

Болегенова С.А., Шортанбаева Ж.К., Көпжасар М.Ж.
(Әл-Фараби атындағы Қазақ Ұлттық Университеті, Алматы, Қазақстан)

ҚАЛДЫҚТАР МӘСЕЛЕСІ ЖӘНЕ БҰЛ МӘСЕЛЕНІ ЖЕДЕЛ ШЕШУДЕГІ ISO 14001 СТАНДАРТЫНЫҢ РӨЛІ

Түйін. Мақалада еліміздегі және шетелдегі қалдықтар мәселесі және олардың шешу мүмкіндіктері, сонымен қатар бұл мәселемен айналысу барысында ISO 14001 халықаралық стандартының мүмкіншіліктері жөнінде қысқаша анықтамалар келтірілген. Қалдықтардың халықаралық анықтамасы мен жиі кездесетін түрлері келтірілген. Мемлекеттің экологиялық жағдайын төмендететін факторлар анықталып, оларды шешу үшін зерттеу жүргізілген. Сондай-ақ, кәсіпорындарда экологиялық саясатты тиімді басқару үшін қажетті жағдай жасауға қызмет ететін ISO 14001 стандарты және де экологиялық кодекс бойынша олардың қоршаған орта алдындағы міндеттері қысқаша келтірілген.

Түйінді сөздер: ISO 14001, кәсіпорын, қалдық, стандарт, Біріккен Ұлттар Ұйымы (БҰҰ), Халықаралық стандарттау ұйымы (ИСО), Экологиялық менеджмент жүйесі, экологиялық кодекс.

Қазіргі заманда қалдықтарды басқару және оларды қайта өңдеу мәселесі уақыт өткен сайын маңыздылығын арттырып келеді. Бұл мәселенің маңыздылығы соншалықты адамзатың өзінің қолымен жасаған заттары адамзаттың өзіне кері әсерін тигізуде.Қалдық дегеніміз не? Планетамызды экологиялық және тағы басқа аппаттардан құткару үшін не істей аламыз? Қалдықтарды басқарудағы халықаралық стандарт ISO 14001-ның рөлі қандай?

Қалдықтардың халықаралық мойындалған анықтамасы: қалдықтар - ұлттық заңнамаға сәйкес шығарылатын, жоюға арналған немесе жоюға жататын заттар. Сонымен қатар Қазақстан Республикасының Мемлекеттік «ҚР СТ ИСО 14050-2010» стандарты бойынша қалдықтың анықтамасы: қалдықтар – иегерінің белгілі бір мақсатта пайдаланатын немесе одан құтылғысы келетін заттары мен бұйымдары. ЕСКЕРТУ. Бұл анықтама Қауіпті қалдықтарды трансшекаралық тасымалдауды және оларды жоюды бақылау туралы Базель конвенциясынан алынған (1989 ж., 22 наурыз), алайда осы стандартта бұл қауіпті қалдықтармен шектелмейді [ИСО 14040:2006] [1]. Қалдық дегенімізде біздің көз алдымызға ең бірінші кезекте өздігінен ыдырау уақыты өте көп пластмасс заттар келеді. Бірақ қалдықтар тек қана мұндай заттардан ғана емесбаска да көптеген заттардан тұрады.

СОДЕРЖАНИЕ

Науки о Земле

Технические науки

Физико-математические науки

Химико-металлургические науки