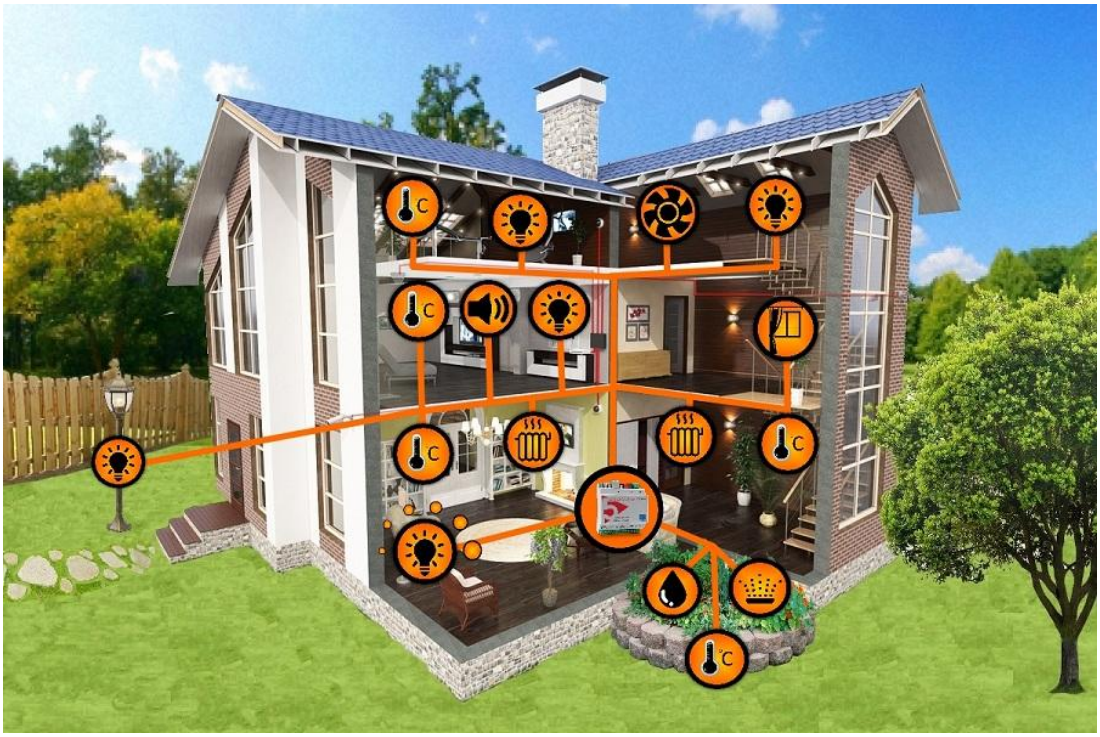
ЛЕКЦИЯ 7. УЯЗВИМОСТИ "УМНОГО ДОМА", IOT, ПРИНТЕРОВ. УЯЗВИМОСТИ ROOT-ПРАВ В УСТРОЙСТВАХ

7.1. «УМНЫЙ ДОМ»

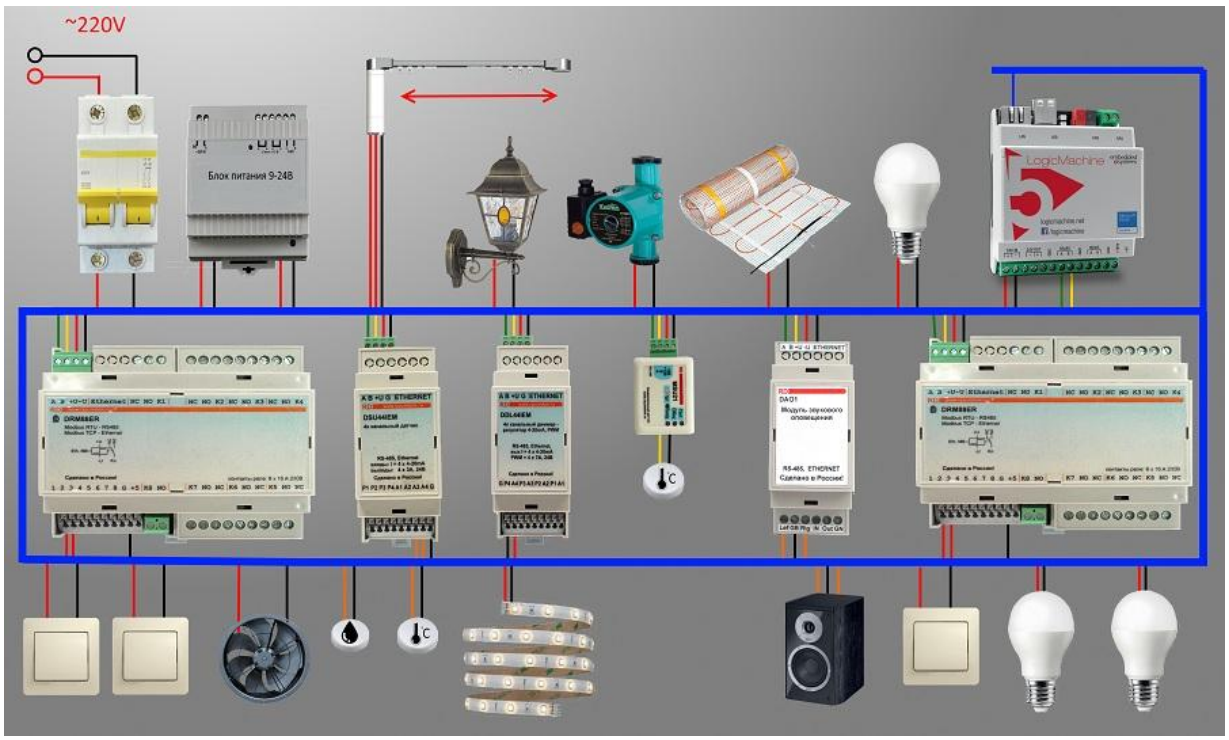
Установив систему “Умного Дома” в коттедже, можно взять под контроль практически все инженерные системы. Регулировка климата, света, штор, кондиционера, полив газона.

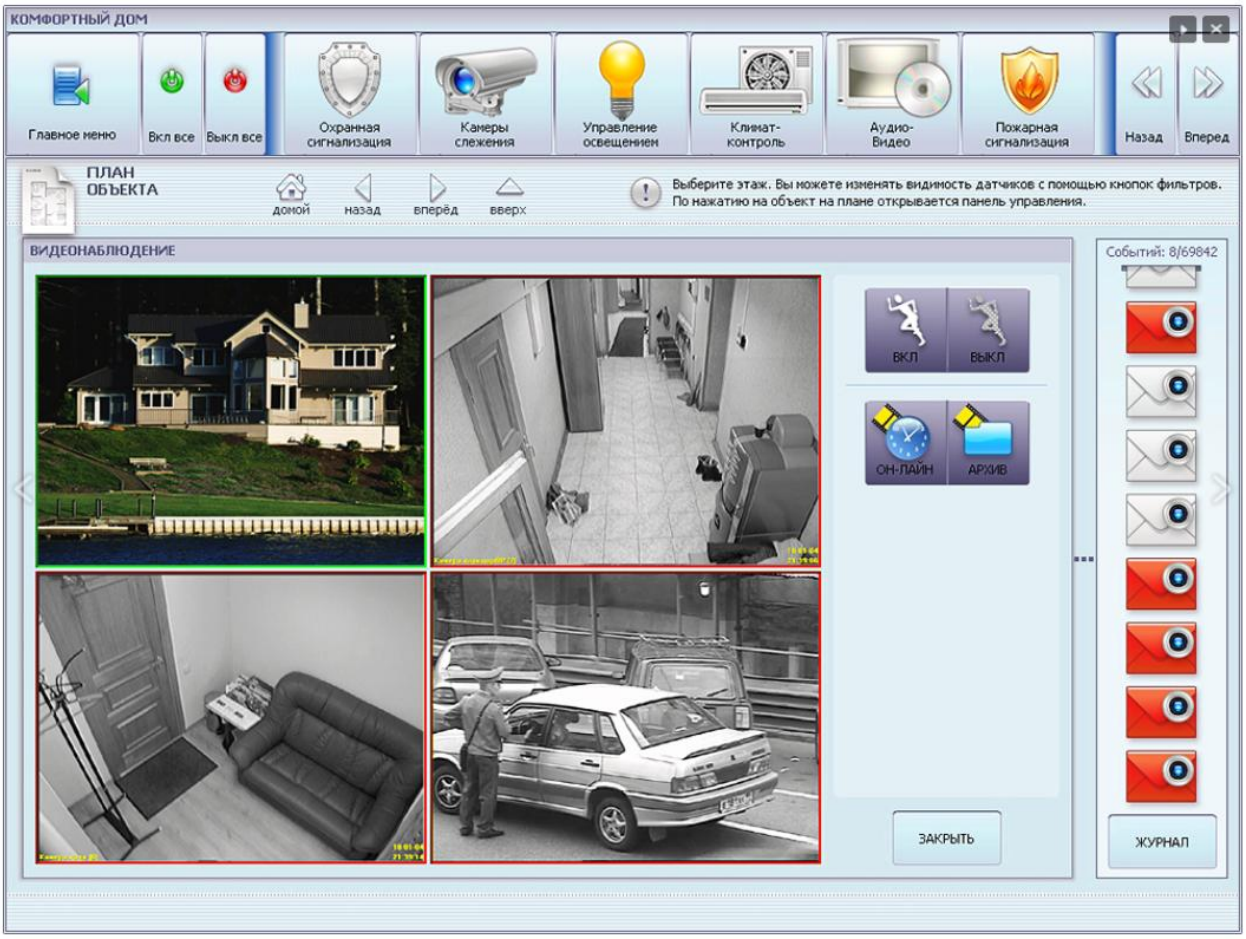


Автоматизированный дом на сегодняшний день не фантастика, а доступная для населения функция, которая может содержать в себе следующие параметры:

- Дистанционное управление освещением с планшета, смартфона, компьютер;
- Стандартное и ручное управление освещением с обычных или сенсорных выключателей;
- Автоматическое управление освещением по сценарию, в зависимости от времени;
- Плавное включение/выключение освещения;
- Выставление яркости света;
- Выставление скорости включения/выключения освещения;
- Имитация присутствия хозяев по заданной программе;
- Экономия электроэнергии;
- Экономия ресурса ламп;
- Ручное выставление режимов освещения;
- Управление температурой;
- Управление шторами;
- Управление поливом газона;
- Управление аудио оповещением.

Всё это находится на вашем компьютере, планшете, либо телефоне на базе IOS или Android.


~220V
Блок питания 9-24В
LogicMachine

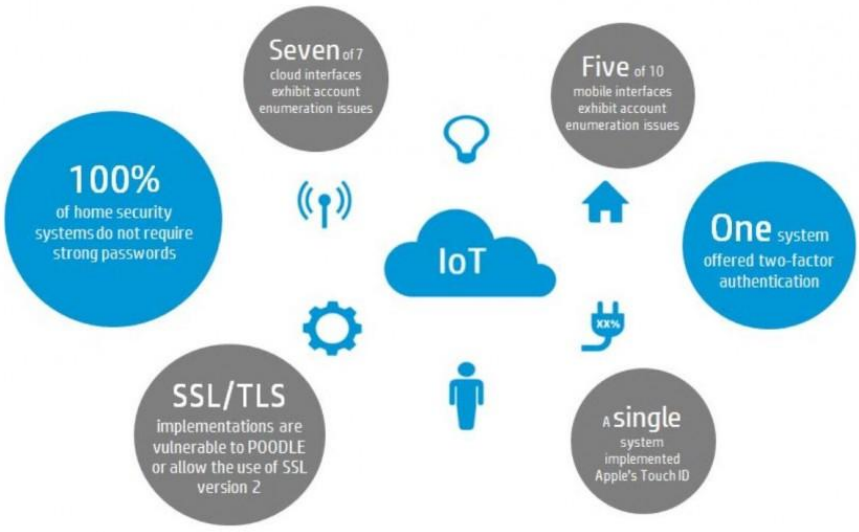

КОМФОРТНЫЙ ДОМ
Главное меню
Вкл все
Выкл все
Охранная сигнализация
Камеры слежения
Управление освещением
Климат-контроль
Аудио-Видео
Пожарная сигнализация
Назад
Вперед
ПЛАН ОБЪЕКТА
домой
назад
вперёд
вверх
Выберите этаж. Вы можете изменять видимость датчиков с помощью кнопок фильтров.
По нажатию на объект на плане открывается панель управления.
ВИДЕОНАБЛЮДЕНИЕ
Событий: 8/69842
ВКЛ
ВЫКЛ
ОН-ЛАЙН
АРХИВ
ЗАКРЫТЬ
ЖУРНАЛ

7.1.1. Уязвимости «умного дома»

Если вы решили защитить свой дом с помощью одной из новейших систем домашней безопасности, относящейся к классу "умных" и подключенных к Интернет решений, то вполне возможно, что вы станете даже менее защищенным и более уязвимым, чем раньше. Проведенные в последнее время разными компаниями тесты компьютерной безопасности таких систем показали, что несмотря на всю "разумность" таких устройств, практически все они не защищены от взлома хакерами.

Современные подключенные к Интернет системы домашней безопасности, как правило, соединяются через облако с мобильным устройством или веб-браузером пользователя, позволяя таким образом контролировать их работу. Подобная система состоит из множества различных устройств, таких как детекторы движения, контактные датчики, видеокамеры, "умные" замки, датчики утечки и присутствия. И, хотя все они предназначены для обеспечения домашней безопасности, последние исследования показали, что эти устройства имеют серьезные уязвимости, из-за чего возможность осуществлять мониторинг состояния дома и его окружения может иметь не только его владелец. Основная причина недостаточной защищенности подобных устройств - это отсутствие установленных стандартов для защиты "умных" домашних систем.

Недавно компания HP опубликовала отчет исследования параметров защищенности домашних охранных систем на примере 10 самых популярных систем безопасности для т.н. "умного подключенного дома". Специалисты компании смогли достаточно легко взломать все десять систем, воспользовавшись наличием целого ряда уязвимостей (слабая политика установки паролей, отсутствие блокировки аккаунтов, легко подбираемые имена пользователей), и удаленно собирать информацию о доме, включая информацию с видеокамер.



Исследователи нашли "пугающе большое количество проблем, связанных с идентификацией и авторизацией, а также с работой мобильных и облачных веб-интерфейсов". Что касается недостаточной защищенной аутентификации и авторизации, то:

- 100% систем позволяли использовать простые пароли;
- 100% систем нуждается в механизме блокировки аккаунта, который может предотвращать автоматизированные атаки;
- 100% систем не защищены от подбора аккаунта, позволяя преступникам угадать данные аутентификации и получить доступ;
- 4 из 7 систем, которые имеют камеры видеонаблюдения, предоставляют пользователю возможность предоставить видеодоступ дополнительным пользователям, что еще больше усугубляет проблему с подбором аккаунта;
- 2 системы предоставляли возможность передачи видео вообще без аутентификации;
- Только одна система требовала двухфакторную аутентификацию.

Очень важно для обеспечения защиты использовать правильно сконфигурированное шифрование передачи данных, но, по данным исследователей HP, в половине из протестированных систем конфигурация осуществлена неправильно, либо в них неправильно внедрена SSL/TLS. При этом 70% систем позволяли осуществлять неограниченную передачу данных аккаунта через незащищенный облачный интерфейс. Одна система обновляет ПО через FTP, что позволяет преступникам перехватить данные аккаунта и получить доступ на сервер обновлений с возможностью записи на него. Три из 10 систем позволяют пользователю при загрузке апгрейда решать, обновлять систему или нет.

Если доступ к видео пользователь получает через облачный Интернет или мобильное приложение, то это же видео из любого места в мире может смотреть преступник с помощью взломанного аккаунта. К сожалению, большинство пользователей поняло это только недавно, когда был осуществлен массовый взлом беспроводных "видео-нянь" и преступники пообщались через них с родителями или детьми. Владельцы примерно 73 тысяч камер были ошеломлены, когда сайт Insecam показал собранные со

всего мира картинки из камер видеонаблюдения, которые стали доступны для просмотра каждому желающему.

Компания HP умышленно не назвала производителей систем, которые были протестированы во время исследований. Если эти продукты или их производители будут публично поименованы, то это может вызвать массовый возврат устройств и другие проблемы для компаний. Это никому не нужно, поскольку ровно такие же проблемы существуют у всех остальных систем. Специалисты HP подготовили секретный список советов, которые были предоставлены производителям. При этом они предупредили, что если в течение 120 дней эти уязвимости не будут ликвидированы или публично отклонены, то список таких продуктов будет опубликован.

7.2. УЯЗВИМОСТИ IoT

Все упомянутое выше справедливо и для продуктов, относящихся к сфере Интернета вещей, производителям которых также рекомендовано обратить внимание на эту проблему, иначе в будущем они столкнутся с непредсказуемой реакцией потребителей. Вернее, вполне предсказуемой, но очень неприятной.

В своем предыдущем отчете, исследователи HP указали на примерно 25 уязвимостей, присущих протестированным домашним устройствам класса IoT, которые также не были поименованы. В списке проверенных компанией приборов были Smart TV, вебкамеры, "умные" термостаты, интеллектуальные электрические розетки, контроллеры садовых разбрызгивателей, замки, домашняя сигнализация, гаражные открывающие устройства, контрольные хабы и даже "умные" весы. Каждое из этих устройств имело функцию контроля с помощью смартфона и большинство из них было подключено к облачному сервису.

Аналогичное исследование провела компания Synack, которая провела тестирование 16 "умных" устройств. Каждое из них (за исключением одного) было "взломано" аналитиками компании менее, чем за 20 минут. Этим отличным от других устройством был детектор дыма Kidde.

В отличие от HP, эта компания предъявила общественности список исследованных устройство:

Камеры	Dropcam, D-Link, Foscam, Simplicam, Withings
Термостаты	Nest, Ecobee, Lyric, Hive
Детекторы дыма и CO	Nest, Kidde, FirstAlert
Контроллеры домашней автоматизации (хабы)	Revolv, SmartThings, Control4, Iris

Наиболее слабо защищенными устройствами в этом списке оказались камеры - каждая из проверенных систем имела проблемы с шифрованием данных и защищенностью паролей. Наименее проблемной из них оказалась камера Dropcam.

Что касается термостатов, наиболее защищенным оказался Nest, хотя и у него оказалась слабая система защиты паролей. Остальные системы оказались в этом смысле существенно хуже.

Хотя детектор Kidde оказался самым защищенным устройством среди всех исследуемых гаджетов, остальные продукты из этой категории не смогли показать себя хорошо. Особенно неудачным оказался датчик FirstAlert.

Детектор дыма Kidde

Последней исследуемой категорией стали хабы - наиболее технологически сложные устройства, к которым подключаются все остальные приборы, входящие в систему домашней автоматизации. Самым надежным оказался Iris, у которого относительно слабым местом оказалась недостаточно хорошая защита паролей. Остальные устройства имеют серьезные проблемы в сфере безопасности, начиная от сервисов и незащищенной архитектуры.

Общий вывод специалистов Synack - "защита "умных" систем домашней автоматизации ужасна". По их мнению, ситуация в отрасли напоминает 90-е годы в компьютерной индустрии, когда та только создавалась и никто особенно не задумывался о необходимости защиты.

Чтобы хоть как-то снизить уровень незащищенности этих устройств эксперты советуют по возможности больше использовать проводные соединения, включить во всех системах автоматическое обновление системного ПО и использовать сложные пароли.

Сегодня пространство Интернета вещей - это что-то вроде Дикого Запада, где каждый делает, что хочет и бежит туда, куда хочет, а домашние системы безопасности и прочие "умные" устройства очень далеки от того уровня безопасности, который все хотели бы видеть.

7.2.1. Виды уязвимостей IoT

Большую угрозу несёт управление устройств с помощью межмашинного взаимодействия. Ни одну написанную человеком программу нельзя считать стопроцентно точной; для неё пишутся различные патчи для исправления ошибок. Такая же участь ждёт датчики в интернет устройствах. И с углублением роли данных устройств в жизни людей будет увеличиваться угроза безопасности всех данных, даже самых незначительных на первый взгляд. Необходимо оценивать любую утекающую информацию, так как резюмирование её составляющих может представлять опасность для жизни как физических, так и юридических лиц (крупнейших компаний).

В таком случае ещё оказывается важным защищать критически важную инфраструктуру, такую как сеть электропередачи. Необходимо подготовить базу для неожиданного аварийного случая, а также правильное соотношение для открытости и

встроенной избыточности.

Одним из самых опасных направлений атаки, является DDoS-атака. Её цель представляет из себя захват системных ресурсов и затруднение доступа к ним добросовестных пользователей. Так 21 октября 2016 года в США была совершена серия DDoS-атак, которая привела к глобальному нарушению интернет-деятельности. Поскольку она была направлена на систему доменных имён (DNS), которая получает информацию о доменах, многие повседневные активности, такие как социальные сети или онлайн покупки, стали недоступны на некоторое время.

Основные информационные потоки злоумышленников были направлены на сервера компании Dyn, являющейся главным поставщиком DNS-услуг для таких крупнейших компаний, как Twitter, Pinterest, Reddit, GitHub, Etsy, Tumblr, Spotify, PayPal и Verizon. Осуществление таких атак стало возможным благодаря подключению к незащищённым цифровым устройствам: роутерам и камерам видеонаблюдения. Хоть они и не являются мощными компьютерами, но способны генерировать огромные объёмы паразитической информации для серверов, особенно при одновременном подключении.

В январе 2014 года в журнале Forbes кибержурналист Джозеф Стейнберг (англ. Joseph Steinberg) опубликовал список связанных с Интернетом приборов, которые «шпионят» за нами буквально в наших домах. В их числе телевизоры, кухонная техника, камеры. Очень ненадёжна компьютерная система автомобилей, которая контролирует тормоза, двигатель, замки, капот, вентиляцию и приборную панель; эти части системы наиболее уязвимы для злоумышленников при попытках получения доступа к бортовой сети. Также атака может быть произведена удалённо по Интернету . Хакерами была продемонстрирована возможность дистанционного управления электрокардиостимуляторами. Позднее они научились получать доступ к инсулиновым помпам и имплантируемым кардио-дефибрилляторам.

Компания Hewlett Packard провела масштабное исследование в 2015 году, в котором сообщается, что 70 % устройств IoT имеют уязвимости в безопасности своих паролей, существуют проблемы с шифрованием данных и с разрешением доступа, и 50 % приложений для мобильных устройств не обмениваются данными.

Лаборатория Касперского — компания, специализирующаяся на производстве программного обеспечения для защиты информации, провела испытания на объектах, подключенных к IoT, и обнаружила, что видеоняни могут быть взломаны для перехвата видео и кофемашины, которые передают информацию в незашифрованном виде, могут сохранять пароль сети Wi-Fi, к которой были подсоединены.

7.3. УЯЗВИМОСТИ ПРИНТЕРОВ

Подключенные к интернету принтеры содержат уязвимости в системе безопасности, которые позволяют совершать кражу паролей, дают возможность получить контроль над принтерами, а также отправленными в печать документами, хранящимися в памяти устройства.

Злоумышленник может получить доступ к энергонезависимой памяти (NVRAM) устройства, что даёт ему возможность завладеть хранящейся на нём информации. Более того, уязвимости в популярных многофункциональных принтерах позволяют получить пароли к локальным серверам SMB, FTP, LDAP, SMTP и POP3, поскольку настройки «умных» устройств предусматривают подключение к ним. С помощью других уязвимостей злоумышленник также способен вывести из строя принтер целиком или некоторые его компоненты.

Злоумышленник может вмешаться в очередь заданий принтера (print job), используя протокол коммуникации JetDirect (подключение по сети) и особенности интерпретатора PCL / PJL. Можно провести атаку типа «отказ в обслуживании» и вывести принтер из

строя, так что он потребует перезагрузки вручную. Кроме того, можно получить доступ к содержимому чужих документов в памяти принтера.

Список производителей, выпускающих принтеры с поддержкой JetDirect: Canon, Fujitsu, HP, Konica Minolta, Lexmark, Xerox, Sharp, Kodak, Brother, Samsung, Toshiba, Ricoh, Kyocera Mita, Lanier, Gestetner, Infotek, OCE, OKI.

Тысячи подключённых к интернету и уязвимых сетевых принтеров доступны через поиск Google. Поисковик проиндексировал их и показывает результат по грамотно составленному поисковому запросу.

7.3.1. Уязвимость сетевых принтеров Samsung, Dell, Brother

Специалист в области информационной безопасности Нейл Смит (Neil Smith) обнаружил в ряде принтеров Samsung скрытую встроенную программу, позволяющую удалённо подключиться к принтеру, менять его настройки и управлять печатью. Это самый настоящий «бэкдор», созданный разработчиком для удобства работы специалистов техподдержки.

Очевидно, из соображений безопасности, компания не афишировала существование подобного функционала. Аналогичная программа присутствует и в принтерах производства Dell, что связано с их взаимными контрактами на производство.

Работает этот бэкдор по видоизменённому протоколу SNMP, который не видим в списке соединений и продолжает работать, даже если отключить SNMP в настройках принтера.

После того, как информация о бэкдоре попала в интернет, появление рабочих эксплойтов для эксплуатации уязвимости — лишь вопрос времени. Конечно, основной путь применения — не столько перехват данных, вы водимых на печать, сколько неавторизованное исполнение произвольного кода с правами администратора в чужой сети. Компания Samsung считает, что успеет выпустить заплатку для этой уязвимости раньше, чем хакеры найдут способ это сделать.

Порядка 700 принтеров компании Brothers предоставляют полный несанкционированный доступ к своей панели администратора через интернет. Уязвимость затрагивает различные модели принтеров Brother, в том числе DCP-9020CDW, MFC-9340CDW, MFC-L2700DW, MFC-J2510 и пр. Проблема заключается в отсутствии пароля администратора в ряде принтеров Brothers. В настоящее время уязвимые устройства можно с легкостью обнаружить с помощью поисковых систем Shodan или Censys.

Поэксплуатировав данную уязвимость, удаленный злоумышленник может изменить пароль на устройстве, загрузить вредоносную прошивку и настроить уязвимые принтеры на отправку копий распечатанных документов на сервер злоумышленника.

7.3.2. Уязвимость сетевых принтеров HP

В настоящее время к интернету подключены тысячи принтеров с гигабайтами внутренних хранилищ, наиболее часто это устройства производства компании Hewlett-Packard. Злоумышленники получают доступ к принтерам HP через порт 9100 и используют их в качестве FTP-серверов. С помощью инструментов с открытым исходным кодом они загружают на принтер файлы, доступные через браузер по адресу http://<Printer_IP_Address> /hp/device /<File_Name>.

Принтеры корпоративного класса обычно включены 24 часа в сутки и даже в спящем режиме могут играть роль хранилища. Перед хакером открывается море возможностей. Злоумышленник может хранить на чужом принтере вредоносные страницы и скрипты, а также связывать их с потенциальными жертвами. Такие принтеры могут

быть отличными репозиториями.

Группа исследователей по информационной безопасности из Колумбийского университета сообщила об уязвимости в принтерах компании Hewlett Packard (HP). Специалисты уточнили, что эксплуатируя брешь в безопасности устройства, удаленный пользователь способен не только скомпрометировать целевую систему, но и спровоцировать пожар.

В ходе демонстрации исследователи показали, как взломанный принтер беспрерывно нагревал термоэлемент, что, в конечном счете, привело к задымлению помещения и обугливанию хранящейся внутри бумаги. Как отметили исследователи, та же уязвимость позволяет потенциальному злоумышленнику выполнить произвольный код на целевой системе. Проблема в том, что принтеры, подключенные к сети Интернет, самостоятельно находят и скачивают обновления для своей прошивки, и передать принтеру зараженный файл под видом обновления достаточно просто.

7.3.3. Желтые точки

Жёлтые точки (также Machine Identification Code (MIC), принтерная стеганография) — метки, ставящиеся многими цветными лазерными принтерами на каждую печатаемую страницу. Приглядевшись, скопление точек можно увидеть по всей странице в местах расположения текста или изображений, на расстоянии примерно 2,5 мм друг от друга.

Точки едва видны невооруженным глазом и содержат в себе информацию о серийном номере принтера, а также дате и времени печати. Они обычно наносятся краской жёлтого цвета, благодаря чему незаметны на белой бумаге. Точки легче разглядеть, если подсветить бумагу фонариком. Размещение данных точек является видом стеганографии. Подтверждено использование данного метода в принтерах, выпускаемых под торговыми марками Brother, Canon, Dell, Epson, Hewlett-Packard, IBM, Konica, Kyocera, Lanier, Lexmark, NRG, Panasonic, Ricoh, Savin, Toshiba, Xerox.

Введение данной меры, согласно комментариям производителей, являлось частью сотрудничества с правительством, конкурирующими производителями и консорциумом банков, направленного на борьбу с фальшивомонетничеством.

В 2005 году люди из Electronic Frontier Foundation взломали коды, использовавшиеся в принтерах Xerox DocuColor, и опубликовали руководство по их декодированию.

Хотя Electronic Frontier Foundation опубликовал результаты своего исследования только в 2005 году, принтеры использовали данную технологию и раньше. Удалось обнаружить метки на отпечатках, изготовленных в девяностых годах.

7.4. Уязвимости root-прав в устройствах

Получение прав суперпользователя, в народе известное как «рутование», позволяет получить полный контроль над устройством. Обладая правами суперпользователя на устройстве, можно сделать практически все что угодно. Поэтому и существует огромное количество приложений (в том числе и в официальном магазине Google Play), требующих root-права для работы.

Чаще всего такие права нужны для того, чтобы делать нечто такое, что в Android обычно сделать невозможно — например, ограничивать сетевую активность некоторых или всех приложений, удалять надоевшие предустановленные приложения, разгонять процессор и так далее.

Наличие у владельца устройства прав суперпользователя в системе нарушает главные принципы безопасности. То есть получение root — это по сути взлом операционной системы вашего планшета или смартфона вашими же руками.

В обычной ситуации все приложения работают в изолированных средах (так называемых «песочницах», sandbox) и не могут получить доступ к другим приложениям или к системе. Но, обладая правами суперпользователя, приложение может выйти из своей изолированной среды и получить полный контроль над устройством.

При наличии прав суперпользователя приложения могут творить на устройстве все, что им заблагорассудится, — например, просматривать, изменять или удалять любые файлы, в том числе необходимые для работы устройства.

Стоит учитывать, что даже в легитимных, «чистых» приложениях бывают ошибки. Так что неприятности могут произойти в том числе «не специально», а просто из-за того, что разработчики где-то что-то не так сделали.

Также следует иметь в виду, что часто в результате «рутования» теряется гарантия устройства. А иногда в процессе получения прав root можно нарушить работу устройства так, что оно превратится в натуральный кирпич, вообще не подающий никаких признаков жизни, — и деньги вам за него не вернут.

Для вредоносных приложений после получения прав суперпользователя наступает полное раздолье. Собственно, многие из троянов для Android как раз и пытаются всеми силами «получить рута». Если же пользователь сделал это самостоятельно — это просто подарок для разработчиков зловреда.

Что могут делать мобильные трояны при наличии прав суперпользователя:

- воровать пароли из браузера — именно это делал банковский троян Tordow;
- скрытно покупать приложения на Google Play — этим промышляют трояны Guerrilla и Ztorg;
- подменять адреса в браузере — такой идеальный фишинг реализован в трояне Triada;
- скрытно устанавливать приложения, в том числе в системные разделы;
- модифицировать прошивку так, что даже после сброса устройства до заводских установок троянец останется на устройстве.

Некоторые троянцы-вымогатели используют права суперпользователя для того, чтобы надежней закрепиться в системе.

Стоит отметить, что в большинстве указанных случаев зловреды способны сами получить права суперпользователя на устройстве с помощью использования уязвимостей в системе. Но некоторые зловреды используют уже существующие права. Кроме того, порядка 5% зловредов проверяют наличие прав рута на устройстве — например, так делает мобильный троян Obad.