УДК 004.056

А.В. Северинов[1], И.О. Жуков[2]

[1]*Харьковский университет Воздушных Сил им. И. Кожедуба, Харьков*
[2]*Харьковский национальный университет радиоэлектроники, Харьков*

ПОЛИТИКА БЕЗОПАСНОСТИ ПРИ РАЗВОРАЧИВАНИИ БЕСПРОВОДНОЙ СЕТИ

Рассматриваются вопросы безопасности в беспроводных сетях. Для устранения потенциальных угроз необходима разработка политики безопасности. Проводится анализ требований, а также основных компонентов политики безопасности в беспроводных сетях.

Ключевые слова: *угроза, политика безопасности, беспроводные сети.*

Актуальность проблемы

Существует множество потенциальных угроз безопасности в беспроводных локальных вычислительных сетях (WLAN): отказ в обслуживании (DoS), захват сеанса, сниффинг и другие. Одним из самых уязвимых мест является шифрование данных в беспроводных сетях Wi-Fi на основе протокола WEP (Wired Equivalent Privacy).

Все атаки на WEP основаны на таких недостатках, как возможность коллизий векторов инициализации и изменения кадров. Для всех типов атак требуется проводить перехват и анализ кадров беспроводной сети. В зависимости от типа атаки, количество кадров, требуемое для взлома, различно. С помощью программ, таких как Aircrack-ng, взлом беспроводной сети с WEP шифрованием осуществляется за несколько минут.

Еще одним недостатком доступность среды распространения сигналов WLAN. Из-за особенностей беспроводных сетей, в них сложно контролировать область доступности сигнала. В отличие от проводных сетей, это введёт к тому, что злоумышленник может перехватывать пакеты и управлять сетью из областей, расположенных вне контролируемой территории. WLAN также могут использоваться для создания программ или наборов программ, устанавливаемых злоумышленником на взломанном им компьютере после получения первоначального доступа с целью повторного доступа к системе (backdoors), для подключения к обычным сетям. Многие организации тратят тысячи и даже миллионы долларов для обеспечения защиты обычных сетей, обширно инвестируя в разработки VPN и других технологий. Однако достаточно одного беспроводного пользователя, связанного с обычной сетью, для успешного создания backdoor, обходящего системы защиты, позволяя хакеру получить доступ к закрытой сети. Политика безопасности беспроводной сети направлена на снижение или устранение возможных угроз.

Подходы в формировании политики безопасности в беспроводной сети рассмотрены в [1 – 4].

Целью статьи является построение политики безопасности для обеспечения защиты беспроводных сетей.

Требования политики безопасности в беспроводных сетях

Политика безопасности – совокупность руководящих принципов, правил процедур и практических приемов в области безопасности информации, которые регулируют управление, защиту и распределение ценной информации [1].

Политика безопасности не позволяет устранить все угрозы сетей стандарта 802.11, но ее внедрение существенно снижает их количество. Она устанавливает модель защиты для существующей или разрабатываемой сети. Политика безопасности предлагает набор правил и стандартов для пользователей, администраторов и менеджеров беспроводной сети. Для обеспечения функций защиты сети политика безопасности предполагает наличие должности начальника службы безопасности.

Для создания политики безопасности необходимо проведение оценки рисков в беспроводной сети. Оценка рисков предусматривает определения угроз и уязвимостей в системе и обязательна при борьбе с непредвиденными угрозами, издержками и затратами. Руководитель службы безопасности должен использовать меры защиты информации в сочетании с оценкой риска в 802.11 сетях. Оценка риска должна проводиться периодически для обеспечения точного набора потенциальных угроз.

Меры политики безопасности должны предусматривать разделение беспроводной и общей сетей (сегрегацию), чтобы нарушение безопасности в одной не влияло на другую. Сегрегация сети обеспечивает отделение WLAN сетей от проводных, которые являются менее уязвимыми для атак. Между общими и беспроводными сетями необходимо помещать фильтрующее устройство (подобно брандмауэру) для контроля и мониторинга трафика [2].

Установление подлинности является одним из основных элементов защиты Wi-Fi сетей и должно быть включено в их политику безопасности. Все пользователи WLAN обязаны подтвердить подлинность перед получением доступа к сети. Установление подлинности необходимо для ограничения доступа к закрытым ресурсам.

В политике безопасности должна быть определена форма взаимной аутентификации. При взаимном установлении подлинности клиент и сервер авторизуют друг друга. Взаимное установление подлинности, прежде всего, повышает безопасность, устанавливая подлинность сервера, а также уменьшает возможности мошенничества в сети. Другим фактором при выборе метода аутентификации должна быть простота реализации и администрирования. Некоторые формы установления подлинности, такие как Public Key Infrastructure (PKI), требуют тщательной разработки и администрирования. Политика безопасности может указывать меры по установлению подлинности, а также объекты и ресурсы, для которых требуется установление подлинности. Политика безопасности может разделить пользователей и уровни доступа по группам [3].

Средство для обеспечения конфиденциальности в беспроводных сетях должно быть определено в политике безопасности. Шифрование должно обеспечить безопасный канал связи, в котором будут циркулировать закрытые данные.

Политика безопасности должна определить стойкий метод шифрования для обеспечения безопасной передачи данных. Широко применяемый в сетях Wi-Fi метод шифрования WEP (Wired Equivalent Privacy) обеспечивает минимальную защиту и должен использоваться, если другое шифрование не возможно.

Основные компоненты политики безопасности в беспроводных сетях

Политика безопасности предусматривает введение лог файлов (специальных файлов, в которых протоколируются все действия пользователя на сервере) и учёт деятельности пользователей. Ведение лог файлов предусматривается политикой безопасности для обеспечения:

- контроля за пользователями;
- упрощения процесса настройки сети в случае возникновения неисправностей;
- упрощение вынесения ответственности за нарушение правил эксплуатации сети.

Лог файлы предусматривают идентификацию и отслеживание пути злоумышленника в случае проникновения в сеть. Они ведутся на беспроводных точках доступа (Wireless Access Point, WAP), брандмауэрах, разделяющих проводные и Wi-Fi сети, серверах. В политике безопасности должна быть определена частота просмотра лог файлов.

В политике безопасности беспроводных сетей необходима регламентация как логической, так и физической защиты WAP. Точки доступа должны быть расположены в физически защищенных областях. При изменении конфигураций точек доступа должна выполняться аутентификация администратора. Большинство WAP, после сброса, возвращаются к заданному по умолчанию небезопасному режиму. Большинство WAP позволяют создавать учетные записи пользователей. Учетные записи необходимо создавать для уменьшения риска несанкционированного доступа к WAP. Списки пользователей на подключение определяются политикой безопасности.

Беспроводные клиенты должны быть оборудованы персональным брандмауэром и антивирусным программным обеспечением. Из-за слабой защиты беспроводные клиенты становятся объектом для нападения и затем, однажды скомпрометированные, они используются как уязвимости для последующих нападений. Политика безопасности должна запрещать прямые (ad-hoc) беспроводные соединения, минуя точки доступа, маршрутизирующие трафик.

Политика безопасности должна предусматривать использование брандмауэров для уменьшения риска взлома беспроводного клиента. С помощью брандмауэров следует проводить регистрацию беспроводной деятельности. Политика безопасности должна требовать использования антивирусного программного обеспечения и обязательного обновления антивирусных баз. Политика безопасности должна предусматривать частоту обновления антивирусной базы [4].

В политике безопасности определяются инструменты для выполнения беспроводного сканирования, а также частота их выполнения. Беспроводное сканирование необходимо для определения местонахождение неправомочных точек доступа. Сканирования должны проводиться не менее чем один раз в неделю или, в крайнем случае, раз в месяц. В политике безопасности должно содержаться руководство как для проведения сканирования, так и устранения незаконных точек доступа.

Кроме того политикой безопасности предусматривается:

- статическая ARP адресация, усиливающая защиту, но при этом увеличивающая затраты времени на администрирование;
- проверка MAC адреса;
- статистическая IP адресация;
- определение схемы беспроводного сетевого идентификатора (SSID).

Политика безопасности может запретить широковещательную трансляцию SSID, с целью усложнения идентификации точек доступа.

Рекомендуется включить в политику безопасности беспроводных сетей систему обнаружения вторжения (Intrusion Detection System, IDS). Беспроводная IDS необходима для обеспечения защиту путем обнаружения незаконной беспроводной деятельности (нападения). Для обеспечения безопасности беспроводной сети политика безопасности должна включать комплекс мер как аппаратной, так и программной защиты [3].

Заключение

Для защиты данных в сети необходимо точное следование правилам и указаниям, изложенным в политике безопасности. Все сетевые операции и разработки должны соответствовать установленным в политике безопасности правилам. Таким образом, для уменьшения угроз безопасности в сетях Wi-Fi, снижения рисков утечки информации необходима разработка и неукоснительное соблюдение политики безопасности.

Список литературы

1. *ГОСТ Р ИСО/МЭК 15408*
2. *Основы построения систем и сетей передачи информации / В.В. Ломовицкий, А.И. Михайлов, К.В. Шестак, В.М. Щекотихин; под. ред. В. М. Щекотихина. – М.: Горячая линия-Телеком, 2005. – 228 с.*
3. *Бондаренко Сергей Васильевич. Социальная структура виртуальных сетевых сообществ : Дис. ... д-ра социол. наук : 22.00.04 : Ростов н/Д, 2004.*
4. *Интернет источник: http://itsec.com.ua/stat-i/raz-rabotka-politiki-bezopasnosti-v-besprovodnyx-setyax.html.*

Поступила в редколлегию 20.01.2011

Рецензент: д-р техн. наук, проф. В.А. Краснобаев, Харьковский национальный технический университет сельского хозяйства им. П. Василенко, Харьков.

ПОЛІТИКА БЕЗПЕКИ ПРИ РОЗГОРТАННІ БЕЗДРОТОВИХ МЕРЕЖ

О.В. Сєвєрінов , І.О. Жуков

Розглядаються питання безпеки у бездротових мережах. Для уникнення потенційних загроз необхідна розробка політики безпеки. Проводиться аналіз вимог, а також основні компонентів політики безпеки.

Ключові слова: *загроза, політика безпеки, бездротові мережі.*

APART SECURITY POLITIC OF WIRELESS NETWORKS

O.V. Severinov, I.O Zhukov

The main threats question of security information in wireless networks. For removal trust treats need development politic of security. Image analysis of demand and the main components of the security politic.

Keywords: *threat, security politic, wireless network.*