УДК 004.056

БЕЗОПАСНОСТЬ БЕСПРОВОДНОЙ СЕНСОРНОЙ СЕТИ

Бабенко В. (Университет ИТМО)
Научный руководитель – кандидат технических наук, доцент Коржук В.М.
(Университет ИТМО)

В данном докладе описаны актуальные проблемы беспроводной сенсорной сети, конкретно Интернет-вещей. Представлен и описан эксперимент, который позволит установить оптимальную защиту для такого вида сети.

Введение. Число устройств, подключенных к Интернету, составляет сотни миллиардов. Поэтому необходимо уделять особое внимание вопросам безопасности в этой среде.

В данном докладе будет рассматриваться проблемы безопасности БСС и возможность их решения.

Основная часть.

В беспроводной сенсорной сети можно отметить проблемы ограничения мощности, качество обслуживания и безопасность.

В БСС существует большое количество угроз, например физическое вмешательство, захват управления, отказ в обслуживании, DDos и т.д.

Так же существует много способов решения этих проблем, например шифрование, поддержка управления ключами, и т.д.

БСС уязвима к разным атакам, так как имеет неуправляемую сеть внутри. Из-за широковещательного характера беспроводной сети имеется возможность прослушивания.

Атаки могут быть отсортированы по шифрованию и ограничению доступа. То есть ограничение доступа происходит с помощью алгоритма на узлах датчика, контролируя доступ. Шифрование достигается с использованием любого алгоритма криптографии.

Для обеспечения безопасности в области беспроводной сенсорной сети необходимо обеспечить безопасность каждого слоя сети и их целостную безопасность.

По данным исследования Мичиганского университета, выявлены три уязвимости:

- ✓ избыточные разрешения;
- ✓ небезопасные сообщения;
- ✓ передача конфиденциальной информации на сервера компаний.

Так же в качестве уязвимостей можно указать бекдоры – «черный ход», разработчики оставляют ход для себя, который позволяет получить полный доступ над всей сетью, к которым подключены устройства.

Защитится от данных уязвимостей возможно через регулярное обновление прошивки или ПО, использование двухфакторной аутентификации и т.д. Но в случае с физическим доступом, пользователь умного устройства не защитится от кражи конфиденциальной информации, например, через мерцание лампочки.

Выводы. По данной работе будет проводится эксперимент, где в качестве беспроводной сенсорной сети будет использоваться смартфон с программой для управления «умного» устройства (лампочка или розетка). Цель эксперимента в том, чтобы узнать к каким атакам уязвима данная сеть, протестировать методы защиты и выявить оптимальную и более эффективную защиту.

Бабенко В. (автор) Подпись

Коржук В.М. (научный руководитель) Подпись