ФОРМИРОВАНИЕ ЭКСПЕРТНЫХ ЗНАНИЙ ДЛЯ РАЗРАБОТКИ ЗАЩИЩЕННЫХ СИСТЕМ «ИНТЕРНЕТ ВЕЩЕЙ»

Бушуев С.Н.,
д.т.н., профессор, ЗАО «НПП ТЕЛДА»,
Десницкий В.А.,
к.т.н., лаборатория проблем компьютерной безопасности, СПИИРАН

Санкт-Петербург, Россия

Проектирования систем Интернет вещей

- Специализированное назначение устройств
- Особенности устройств
  - Специфичные угрозы ИБ
  - Ресурсопотребление → производительность → функциональность
  - Автономность → энергопотребление & степень встраиваемости в систему верхнего уровня
  - Мобильность
  - Физические характеристики
  - Компонентно-ориентированная структура устройств → внутр. связи
  - Стоимостные ограничения
- Сложность проектирования:
  - Анализ и учет ограничений устройств
  - Слабая формализация и структуризация области знаний ИБ

Устройства систем Интернет вещей

- Автомобили
  - Контроль двигателя, АКП, АБС и др.
- Авиация
  - Управление полетом, системы диспетчерского контроля и др.
- Связь
  - Коммутация, цифровые ресиверы, мобильные телефоны, маршрутизаторы, IP телефония, КПК и др.
- Бытовая техника
  - Кондиционеры, холодильники, СВЧ печи и др.
- Коммерческая техника
  - Автоматизированный контроль, кассовые аппараты, системы управления запасами и др.







Релевантные работы

- Ключевые проблемы проектирования систем Интернет вещей:
  - *Hwang D.D., Schaumont P., Tiri K., Verbauwhede I. Securing Embedded Systems // IEEE Educational Activities Department, IEEE Security and Privacy, volume 4, number 2, 2006, pp. 40-49.*
  - *Ravi S., Raghunathan A., Kocher P., Hattangady S. Security in Embedded Systems: Design Challenges // ACM Transactions on Embedded Computing Systems,Vol.3,No.3, 2004, pp.461-491.*
  - *Kocher P., Lee R., Mcgraw G., Ravi, S. Security as a new dimension in embedded system design // Proceedings of the 41st Design Automation Conference (DAC '04) , 2004, pp.753-760.*
  - *Knezevic M., Rozic V., Verbauwhede I. Design Methods for Embedded Security // Telfor Journal, Vol. 1, No. 2, 2009.*
  - *Koopman P. Embedded System Security // IEEE Computer, No. 7, 2004.*
  - *Henzinger T.A., Sifakis J. The Embedded Systems Design Challenge // LNCS Vol. 4085, Springer Berlin Heidelberg, 2006, pp. 1-15.*
- Модели проектирования систем Интернет вещей :
  - Moyers B.R., Dunning J.P., Marchany R.C., Tron J.G. Effects of Wi-Fi and Bluetooth Battery Exhaustion Attacks on Mobile Devices // Proceedings of the 43rd Hawaii International Conference on System Sciences (HICSS'10), IEEE Computer Society, 2010, pp.1-9.
  - *Rein A., Rudolph C., Ruiz J.F. Building Secure Systems Using a Security Engineering Process and Security Building Blocks // Zertifizierung und modellgetriebene Entwicklung sicherer Software (ZeMoSS-Workshop), 2013, http://subs.emis.de/LNI/Proceedings/Proceedings198.html*
  - *Nadjm-Tehrani S., Vasilevskaya M. Towards a Security Domain Model for Embedded Systems // 13th IEEE International High Assurance Systems Engineering Symposium, IEEE, 2011.*
  - *Mana A., Ruiz J.F. A Security Modelling Framework for Systems of Embedded Components // 13th IEEE International High Assurance Systems Engineering Symposium, IEEE, 2011*
  - *Rudolph C. Security Engineering and Modelling of Set-top Boxes // RISE'12, Workshop on Redefining and Integrating Security Engineering at ASE/IEEE International Conference on Cyber Security 12, IEEE, 2012*

Процесс проектирования систем Интернет вещей

- *Роль эксперта в обл. ИБ:*

I. формирование модель нарушителя → требования защиты → шаблоны защиты → базовые компоненты защиты (КЗ), их реализация/интеграция

II. возможные виды конфликтов и аномалий в политиках безопасности и между КЗ

III. возможные виды аномалий в данных от сенсоров системы → виды ограничений на данные в системе для их проверки в процессе мониторинга аномалий

Задачи исследования

Задачи:

1. Выявление экспертных знаний (ЭЗ) в области ИБ систем Интернет вещей
   - В т.ч.: знания о нарушителях ВУ, КЗ, требованиях и ограничениях, информационных потоках (ИП), разновидностях аномальных данных и др.
2. На основе ЭЗ разработка частных методик и программных инструментов проектирования и анализа

Основные источники ЭЗ:

- Существующие информационно телекоммуникационные системы: STB (Technicolor), MD (Mixed-mode), TMN (Ruag)
- Научно-исследовательские работы в области

Онтологическое представление ЭЗ (классы и отношения):

- Формализация ЭЗ, уточнение семантики
- Входные данные для автоматизации проектирования, верификации и принятия решений защиты ВУ

Примеры экспертных знаний

Предмет ЭЗ	Примеры ЭЗ	Применение ЭЗ
Проблемы защиты ВУ (Embedded security design challenges) Известные модели нарушителей ВУ	Работы в обл.: [Ravi'04], [Kocher'04], [Henzinger'06], [Hwang'06], [Knezevic'04], [Eby'07],, [Burleson'12], и др. Модели нарушителя [Rae'03], [Grand'04], [Abraham'91]	Методика верификации спецификаций ВУ на предмет выявление потенциальных атак на ВУ
Информация о КЗ ВУ, требованиях и ограничениях и Эвристика порядка учета нефункциональных требований	Спецификация нефункциональных и функциональных требований	Инструмент принятия решений комбинирования КЗ Конфигуратор КЗ ВУ
Типовые конфликты между КЗ ВУ	Три типа конфликтов КЗ	Методика выявления конфликтов КЗ ВУ
Информация о системе и информационных потоках (ИП) Знания о типовых конфликтов и аномалиях ИП	Правила запрета и разрешения ИП вида rule:=(aFlow, true/false) aFlow := (Us, Ns, Is, Ut, Nt, It, T)	Методика и программный инструмент верификации ИП на основе SPIN
Возможные виды аномалий в данных от сенсоров системы Ограничения системы для проведения мониторинга аномалий Способы осуществления типовых атак на сенсоры	Ограничения бизнес-логики целевой системы Ограничения, исходя из совокупной структуры системы с учетом предыдущей истории показаний сенсора Ограничения, вследствие естественных технических условий эксплуатации устройств системы	Программный генератор компонентов мониторинга аномалий с проверкой нужного набора ограничений на данные в системе

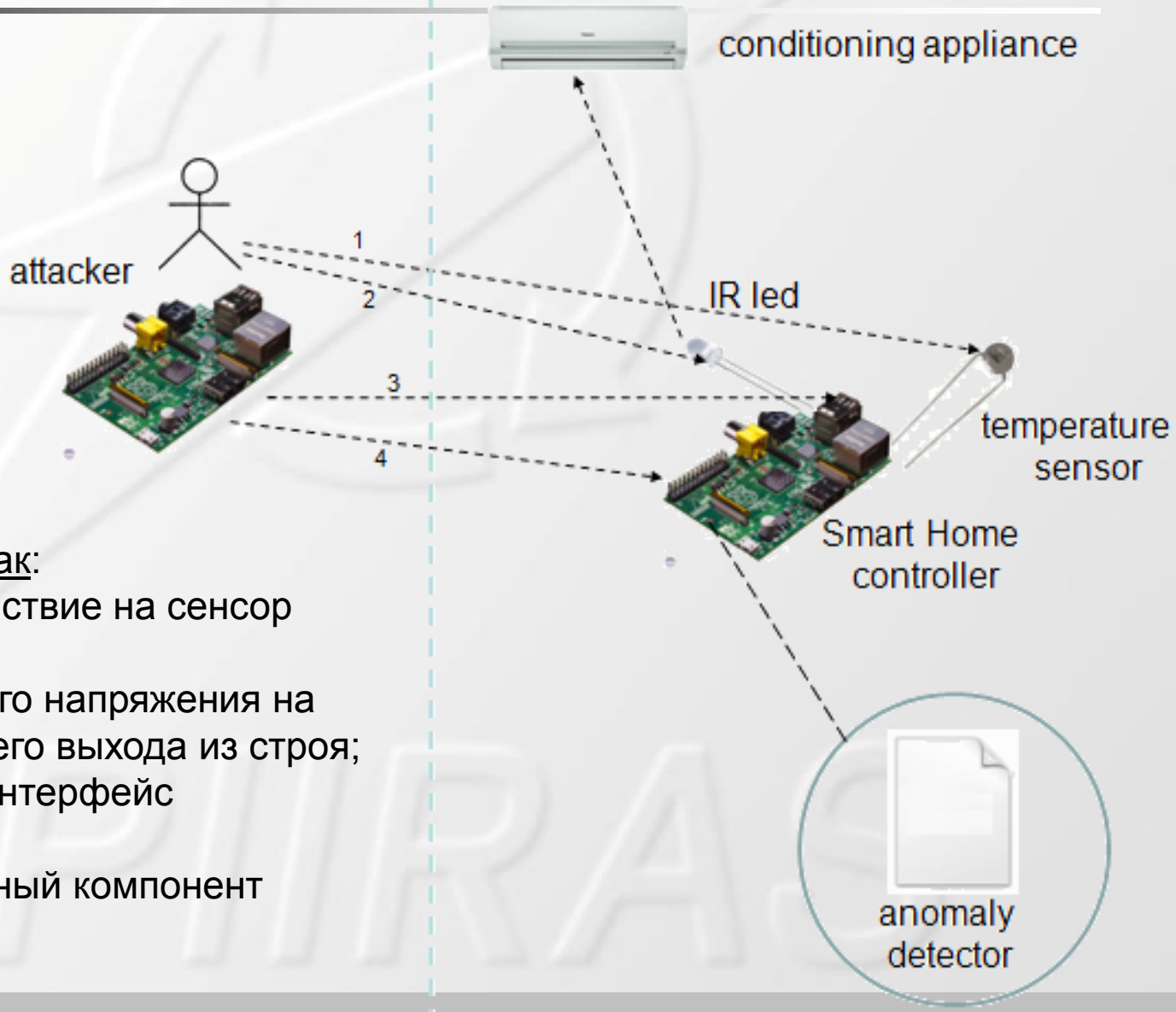
Мониторинг аномальных данных

Мониторинг организуется на основе экспертных знаний – ограничений на данные в системе и ожидаемых действий атакующего

Типы ограничений	Примеры ограничений
1. Ограничения бизнес-логики конкретной системы Умный дом	- в соответствии с целевыми требованиями температура внутри помещения Умного дома не должна превышать 30 градусов Цельсия и быть ниже 5 градусов - предельно-допустимая концентрация угарного газа (CO) не должна превышать порогового значения соответствующих санитарных норм
2. Ограничения, исходя из совокупной структуры системы, как результат связей между отдельными частями системы в процессе ее интеграции	- если два или более сходных сенсоров показывают принципиально разные значения (в предположении об отсутствии причин для такого отличия), то это считается аномалией, и на основе этого можно сделать вывод о возможной атаке как минимум на один из этих сенсоров
3. Ограничения, исходя из течения времени	- сенсор освещенности и термометр вне помещения Умного дома показывает заведомо не корректные значения освещенности и температуры для данного времени года с учетом геоинформационных данных о его месторасположении (в том числе неожиданные изменения/колебания температуры)
4. Ограничения с учетом предыдущей истории показаний сенсора	- сенсор движения в офисе перестал выдать сведений (или некорректные сведения) о передвижении сотрудников в рабочее время, что является возможным признаком того, что сенсор был атакован и неработоспособен с целью осуществления незаконного проникновения в дальнейшем
5. Ограничения, вследствие естественных технических условий эксплуатации электронных компонентов системы и/или ее подсистемы защиты	- величина электрического напряжения, подаваемого на аппаратный pin встроенного устройства не должно превышать 5 (или 3) вольта - ограничения в результате технически допустимых границ значений сенсора, например, граничные значения температуры, заявленные производителем термистора

Прототип системы Умный дом для задачи обнаружения аномальных данных

Фрагмент системы Умный дом с использованием Raspberry Pi – контроль температурного режима помещения



Исследуемые виды атак:

(1) физическое воздействие на сенсор температуры;
(2) подача повышенного напряжения на ИК-светодиод для его выхода из строя;
(3) атака на Ethernet-интерфейс контроллера;
(4) атака на программный компонент детектор аномалий

Заключение

- Дальнейшая работа:
  - Уточнение ЭЗ для компонентов проектирования, верификации и тестирования в части мониторинга аномальных данных в системе
  - Разработка инструмента проектирования - генератора компонентов мониторинга аномальных данных в зависимости от ограничений целевой системы

Контактная информация

Десницкий Василий Алексеевич (СПИИРАН)

desnitsky@comsec.spb.ru

http://comsec.spb.ru/Desnitsky

Благодарности

Работа выполнена при финансовой поддержке РФФИ (13-01-00843, 14-07-00697, 14-07-00417, 15-07-07451), программы фундаментальных исследований ОНИТ РАН (контракт №2.2), проекта ENGENSEC программы Европейского Сообщества TEMPUS и Министерства образования и науки Российской Федерации (соглашение № 14.604.21.0033, уникальный идентификатор соглашения RFMEFI60414X0033; соглашение № 14.604.21.0137, уникальный идентификатор соглашения RFMEFI60414X0137; соглашение № 14.604.21.0147, уникальный идентификатор соглашения RFMEFI60414X0147).

ВОПРОСЫ?