Моделирование энерго-атак на автономные IoT-устройства

Санкт-Петербургский государственный университет телекоммуникаций
имени профессора М. А. Бонч-Бруевича (СПбГУТ),
Кафедра Защищенных Систем Связи

Десницкий Василий Алексеевич

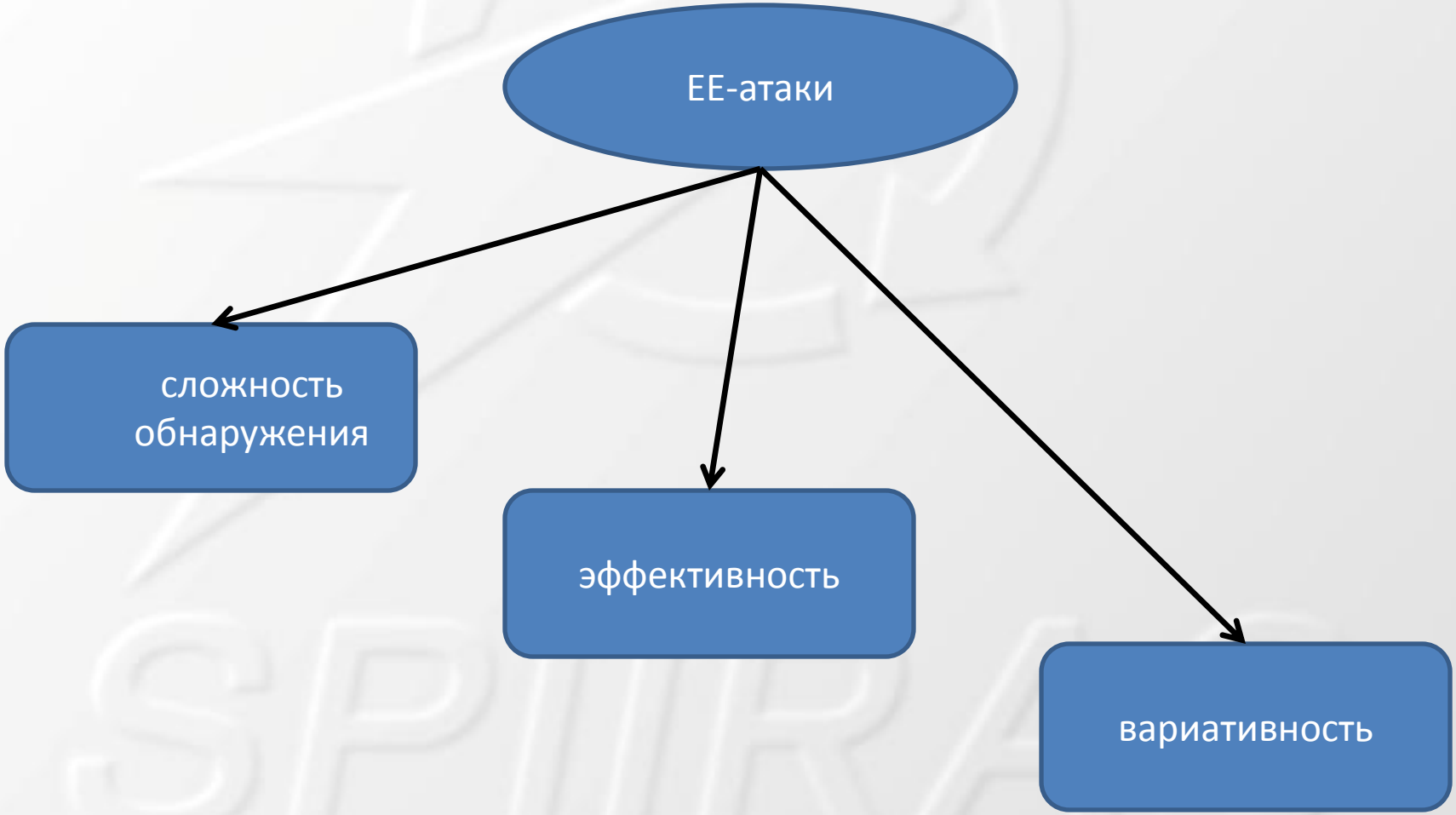
2018.03.22 РусКрипто 2018

Энерго-атаки на устройства IoT

- Атаки истощения энергоресурсов (Energy Exhaustion Attacks, EE-атаки)

- Автономность
- Беспроводные коммуникации

Особенности ERE-атак



Работы в предметной области

- Analysis of misusing mobile device batteries [Palmieri, et al., 2015], [Shin, et al., 2009], [Moyers, et al., 2010], etc.
- Energy resource exhaustion attacks in WSN, inc. *replay attacks*, *broadcast attacks*, etc. [Boubiche, et al., 2013], [Krishnan]
- Exploiting *MMS vulnerability* in battery exhaustion attack ERE attacks of mobile devices [Racic, et al., 2006]
- *Jamming attacks* [Karpagam, et al., 2013], [Periyanayagi, et al., 2011], etc.
- Denial-of-Sleep attacks in WSN, incl. *collision attack*, *overhearing attack*, *control packet overhead attack*, etc. [Goudar, et al., 2015], [Capossele, et al., 2016], etc.
- *Vampire attacks* in WSN [Farzana, et al., 2014]

Модели нарушителя IoT

Classification of intruder access type
Type$_0$ - no access (social engineering)
Type$_1$ - no direct access (TCP/IP based attacks from Internet)
Type$_2$ - remote access (Wi-Fi, IR, Bluetooth, etc.)
Type$_3$ - outward access (direct access to RS-232, I2C, etc.)
Type$_4$ - full access (tamper with microchip)

(Rae, et al.,03)

Classification of intruder capability levels
Level$_1$ - public accessed tools, well-known vulnerabilities
Level$_2$ - specialized tools, previously unknown vulnerabilities
Level$_3$ - group of intruders level 2 (unlimited resources)

(Abraham, et al.,91)

Разновидности EE-атак

- EE-атаки

Forced waking of a sleeping device (Denial-of-Sleep)

Growth of wireless traffic

Electromagnetic jamming

Misuse of a device

Атаки типа Denial-of-Sleep

Goal	Reducing the time of a sleep mode
Features	1. Presence of idle states of small energy consumption. 2. Using energy consuming wireless interfaces such as Bluetooth, Wi-Fi, etc. 3. Attack category <$Types_1$ & $Type_2$, $Level_1$ & above>
Actions	*idle mode* → *active mode*
Resources and possibilities	1. Superficial knowledge of Linux. Downloading and installing typical software. Capabilities of reproducing manuals. 2. Minimal time for deployment of a new attacking device is required after the precursive software and hardware preparation. 3. Typical laptop/single-board computer. 4. Rooted Android.
Conclusions	1. Indirect impact on the device (i.e. wirelessly). 2. Attack distance - wave frequencies and the power of the antenna of the intruder. 3. No need for an intruder to be authorized => complicates effective protection

Атаки увеличения беспроводного трафика

Goal	Increasing amounts of income/outcome data & decreasing their speed
Features	1. Typically devices transmit data not permanently. An attacker is to enlarge amounts of data transmitted and time of the transmission. 2. Attack category <$Types_1$&$Type_2$, $Level_1$&above>.
Actions	Intruder logs in to the device and starts messaging. To defeat authorization the one breaks the key or makes a replay attack by some past legitimate traffic.
Resources and possibilities	Basic knowledge on the target system. Typical laptop/single-board computer. Rooted Android.
Conclusions	Indirect impact (i.e. wirelessly). Attack distance - wave frequencies and the antenna of the intruder.

Jamming-атаки

Goal	To force the device to increase the signal power during the communication.
Features	Normally wireless modules try to transmit at the minimum power to reduce energy costs. Attack category <$Type_2$, $Level_2$&above>.
Actions	Electromagnetic noising on wireless data transmission channels.
Resources and possibilities	Tools to affect wireless channels. Location in a short distance from the device.
Conclusions	Indirect impact (i.e. wirelessly). Attack distance - wave frequencies and the antenna of the intruder.

Атаки неправомерного использования (untypical usage)

Goal	Waste energy by forcing the device to run some unnecessary functions.
Features	Attack category <$Type_0$ - $Type_4$, $Level_1$&above>.
Actions	- extra CPU load, - access to energy consuming memory, - packet transmission via communication channels, - multiple launch of applications, - breaking/bypass optimizations, - non-typical use of the software, - remote desktop session, etc.
Resources and possibilities	Penetration skills for direct/remote access to the device and run malware on it.
Conclusions	The attack assumes the deepest affection of the intruder to the device.

Эксперименты

- Вычисление эффективности EE-атак
- Proof-of-the concept

Case study 1

Smartphone LG Nexus 5

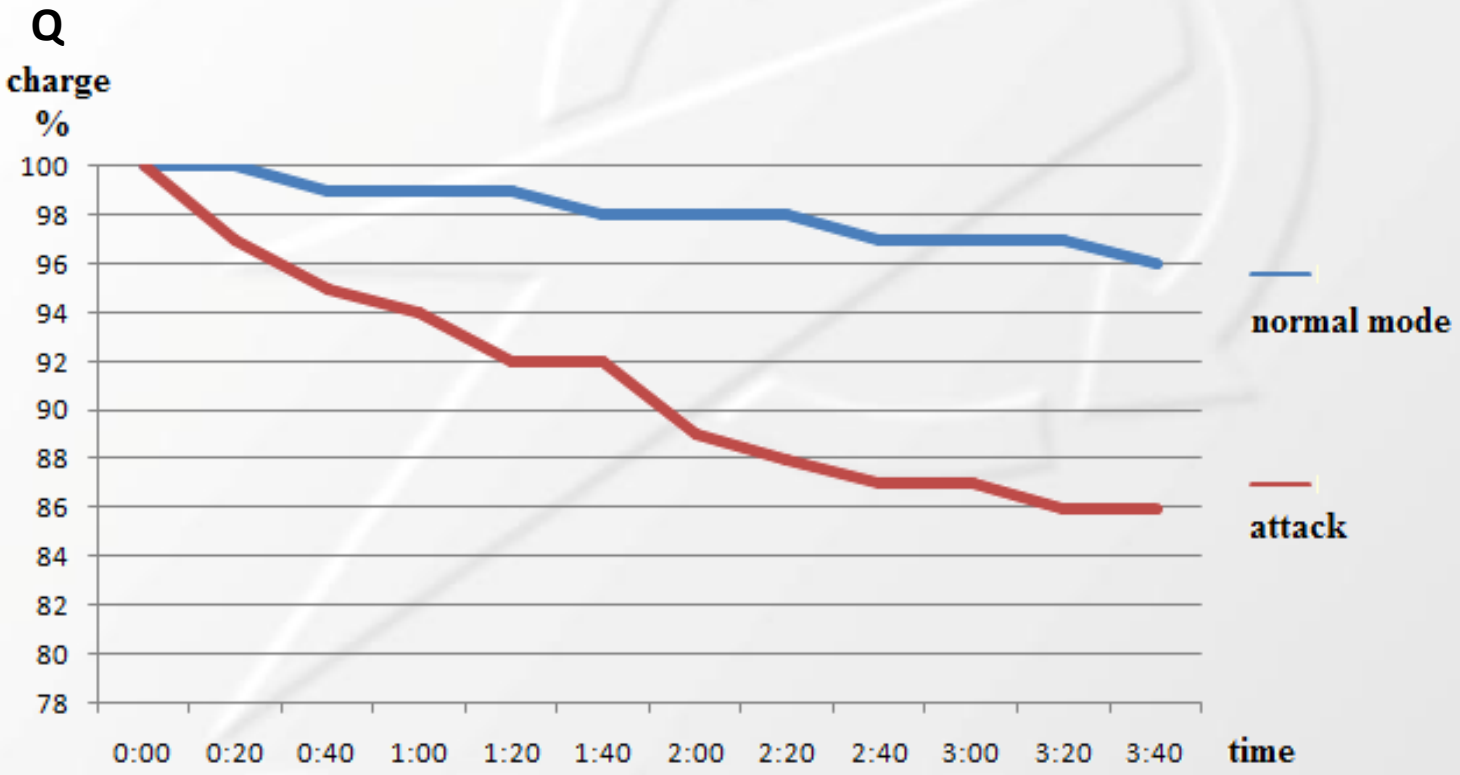
Case study 2

Wireless XBee module s2

Denial-of-Sleep attack

measurements

Case study 1: анализ EE-атаки

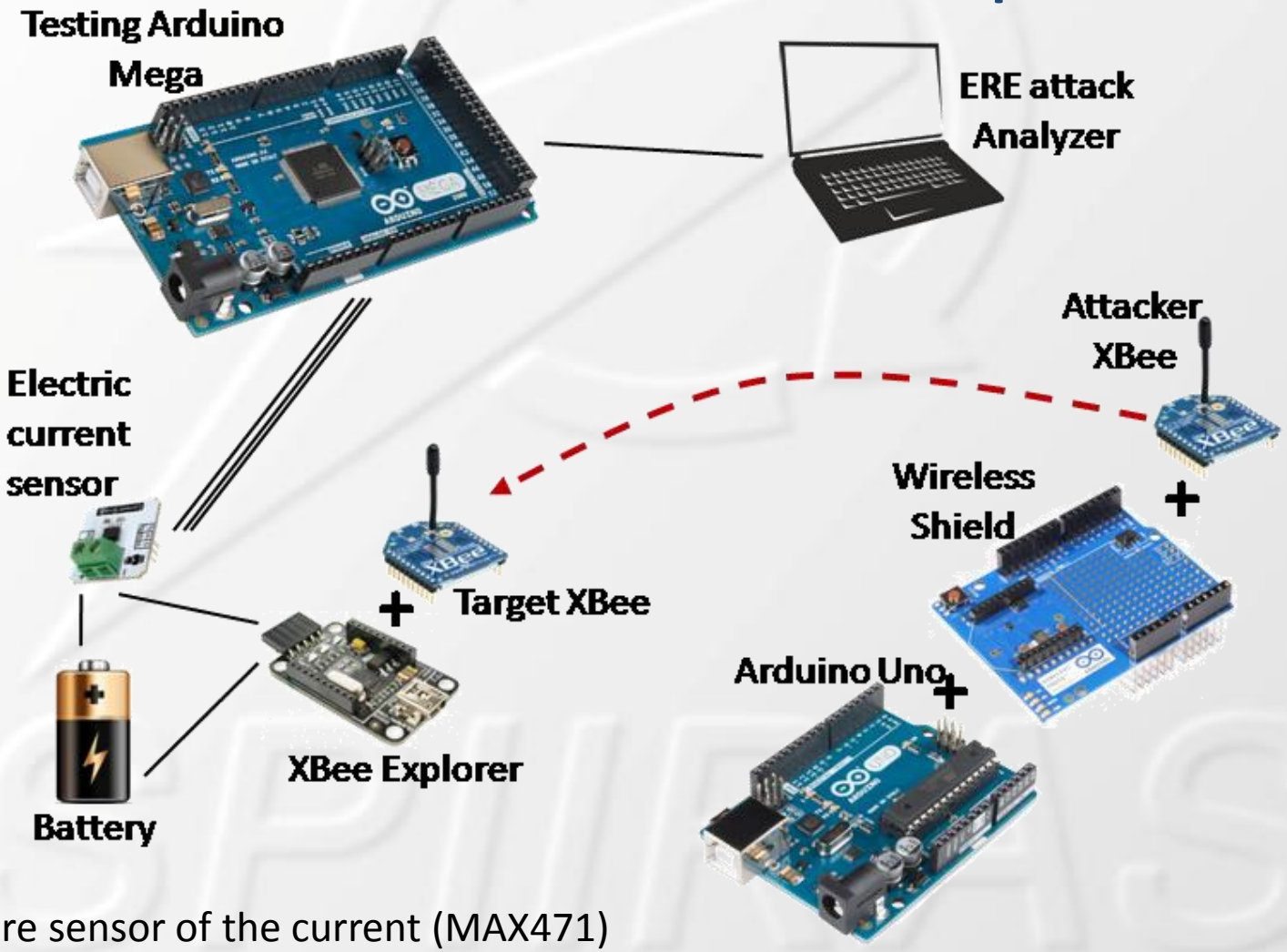


by reading *BatteryManager.EXTRA_LEVEL*

attack effectiveness:

$$E = \frac{delta(Q_A)}{delta(Q_N)} = 3.5$$

Case study 2: моделирование атаки типа Denial-of-Sleep



by hardware sensor of the current (MAX471)

Case study 2: анализ атаки

XBee config. parameters:

SM = 4 (cyclic sleep mode)
ST = 1000 *msec* (time before sleep)
SP = 10000 *msec* (cyclic Sleep Period)

Time gap, *msec*	0 – 1000	1000 – 11000
I_{IDLE}, *mA*	45	8
I_{ATTACK}, *mA*	51	51

Эффективность атаки:

$$E = I_{ATTACK} \cdot (t_2 - t_1) / \int_{t_1}^{t_2} I_{IDLE}(t)dt = 4.488$$

среднее значение

Заключение

- Вклад
  - Разработана аналитическая модель EE-атак
  - Проведены эксперименты на двух IoT case studies
  - Рассчитана эффективность атаки Denial-of-Sleep
  - Продемонстрирована выполнимость EE-атаки
- Направления будущих исследований
  - Обнаружение EE-атак
    - подход на основе машинного обучения

Контакты

Санкт-Петербургский государственный университет телекоммуникаций имени профессора М. А. Бонч-Бруевича (СПбГУТ), Кафедра Защищенных Систем Связи

Федеральное государственное бюджетное учреждение науки Санкт-Петербургский институт информатики и автоматизации Российской академии наук (СПИИРАН), Лаборатория проблем компьютерной безопасности

- desnitsky@comsec.spb.ru,
- http://comsec.spb.ru/desnitsky ,
- http://zss.sut.ru/desnitskiy

Работа выполняется при поддержке Гранта президента Российской Федерации № МК-5848.2018.9