How to securely build your own IoT embedded systems: from design to execution and assessment

Vito Rallo – Jean-Georges Valle – Adriaan Neijzen

PwC, Woluwegarden - Woluwedal 18 B - 1932 BRUSSELS
{vito.rallo, jean-georges.valle, adriaan.neijzen}@pwc.com

Abstract

The Internet of Things (IoT) is the next Internet revolution that aims at interconnecting devices that we use on a daily basis e.g. household appliances, wearables, cars, cameras, and sensors. Enabling the IoT can be done by introducing new smart devices, or by equipping legacy devices with sensors to accommodate them with smart capabilities. But how secure are these IoT appliances? And why limit yourself to commercial off-the-shelf devices if you can design and build them yourself?

Our workshop will (1) guide all participants through all steps that are required to build their own Internet of Things enabling embedded systems and (2) give an introduction on the assessment of security and exploitation of vulnerabilities in embedded systems.

Our, very practically oriented, workshop will consist of a presentation that briefly explains all required steps to build and assess the security of embedded systems and a guided hands-on lab session in which all participants will actually program and exploit their own basic, but smart temperature sensor.

The presentation will provide the participants with all the means to design their own IoT-enabling embedded systems and will focus on how to transfer ideas into real plans and designs. We will elaborate on how to gather information on the required electronics, where to buy them, how to use their datasheets and we will even teach the audience how they can design, print and test their ideas on self-designed PCBs. Topped off with some of our lessons learned and practical tips ‘n tricks, the main presentation will provide the audience with everything they need to know to start building.

The guided and hands-on lab session will even take everything a step further. We will provide the participants with an already assembled version of the smart temperature sensor we have designed during the presentation and we will go into writing and flashing our own bare-metal ARM firmware.

After we have all successfully created our first embedded system, we will move towards a basic firmware analysis and exploitation session by flashing our temperature sensor board with custom made, but vulnerable firmware. This will allow us to assess our embedded system by reverse engineering the firmware with Radare and gdb and exploit it using basic shellcode.

Please note that this workshop is the full version of '*How to assess the security of IoT enabling embedded systems*', which is also submitted as a 2 hour workshop.

Detailed outline of the workshop

The outline of our workshop with presentations and guided labs will be as follows:

- Who are we and what will participants learn in this workshop (10 min, presentation)
- Phase 1: planning, design and assembling – or how to transfer your idea into a real product? (50 min, presentation and demos):
    - What makes an idea a good idea? What is achievable and what are the limiting factors?
    - How to know which electronics to buy? How to select the most appropriate sensors, storage equipment and microcontrollers?
    - How to read and use datasheets to put all pieces together?
    - How to design and order your own PCB?
    - How to assemble and solder electronics? What are the required tools and equipment?
- Phase 2: firmware - or how to program and flash your own bare-metal ARM firmware? (30 min, guided lab session)
    - Required tools and equipment?
    - How to find and use external hardware abstraction layers, libraries, etc?
    - How to create and use makefiles?
    - How to connect via serial interfaces to embedded systems?
    - How to flash bare-metal ARM firmware to your chip?
- Phase 3: exploitation – or how to assess and exploit embedded systems by reverse engineering firmware with Radare and gdb? (2h30, guided lab session)
    - What are the typical attack vectors? What are common vulnerabilities in IoT devices?
    - How to dump and analyse firmware?
    - How to use Radare2 and gdb to reverse engineer firmware?
    - How to write basic shellcode to exploit the found vulnerabilities?
    - How to protect against exploitation?

What will the attendees learn?

This workshop will provide the attendees with all required knowledge to (1) start building their own Internet of Things enabling embedded systems and (2) do basic security assessments of IoT appliances.

List of facilities required

The following facilities will be required to host this workshop:

- Projection equipment to at least project one laptop at a time (preferably two):
    - One Windows laptop hosting the presentation
    - One Linux laptop used for the guided labs

For each participant, the following has to be foreseen (can also be provided by the instructors):

- STM32L100RCT6 ARM Cortex M3 development board + USB cable
- Our custom designed and already assembled victim board
- Pre-configured USB stick with Linux operating systems and the required tools and files
- USB to serial adapter (e.g. based on the FTDI FT232RL chip)

Each participant will have to bring the following:

- Laptop with 3 USB ports and capable to boot via USB

Previous experience

This training have been given for the first time during the BSides LasVegas security conference in 2017. An extended version of this workshop is regularly given internally within PwC for our international colleagues. Next to this, the instructors have a lot of experience with presentations and/or workshops given at several (international) conferences (BruCON, Hardwear.io, IoTBE, etc.)

Bio Vito

Vito works as Senior Manager (Security Consulting) for PwC. He has worked in IT for more than 15 years and brings a value of 9 years' Security experience with a background of Intrusion Prevention, System Hardening, Software Security, Mobile Security and excellence in Ethical Hacking. Vito had the opportunity to develop his profile by leading a global cyber security assessment team and facing technical edge projects providing consultancy for corporates and financial institutions. He holds Ethical Hacking, IT professional and networking certifications, enjoys speaking at security events and is experienced in assisting companies with Security Assessments, Threat Modelling and Remediation.

Vito previously worked as a leader and an ethical hacker for IBM in the Cyber Security Assessment and Response team. He had an international exposure performing delivery of Infrastructure, Web Application and Mobile Security Assessments (pentest), steering the team and ensuring quality results and customer satisfaction.

By growing his knowledge over the years and facing challenging projects, he became a recognized asset in Mobile Hacking, presented on several security events and authored various methodology documents, checklists and assets adopted by the internal IBM community of practices.

Bio Jean-Georges

Jean-Georges is a Senior Technology Consultant within PwC since April 2015.

He is passionate about IT security and new technologies and is a titular of a Master in information system security (2008).

He has worked in highly heterogeneous environments, service and industrial type with both deep technical (administrator in a hosting business), organizational (security auditor in a French Ministry, acting CISO in a BNP Paribas Branch) and governance skills.

Jean-Georges specialised in secure infrastructure systems design, audit and management, policy implementation and adherence audits, KPIs, KRIs and hacking and mitigation techniques.

Jean-Georges have build multiple security conferences badges (BRUCon, Cyberskool)

Bio Adriaan

Adriaan is a Senior Associate within PwC's Cyber & Privacy department. He started his professional career at PwC in 2016. Despite his economic background, Adriaan developed a very strong interest in the technical aspect of cyber and information security during his studies. Through a large amount of self-study in addition to his education, he continued to explore these technical aspects. Eventually, this growing interest drove him to pursue a career as penetration tester. Within PwC, Adriaan focuses primarily on infrastructure-related assessments. Since joining PwC, he has gained experience in conducting red teams, internal and external intrusion tests, threat analysis based on publicly available information (OSINT) and system configuration and hardening assessments. In addition, he also developed specific competencies in assessing the security of VoIP and videoconferencing systems and has performed a number of physical and wireless security assessments. During his career at PwC, Adriaan has also helped develop and presented an interactive hacking demonstration called the Hacking Experience. Due to presenting the Hacking Experience numerous times in front of sizeable and/or international audiences, he has become very comfortable and enjoys public speaking on a multitude of topics.