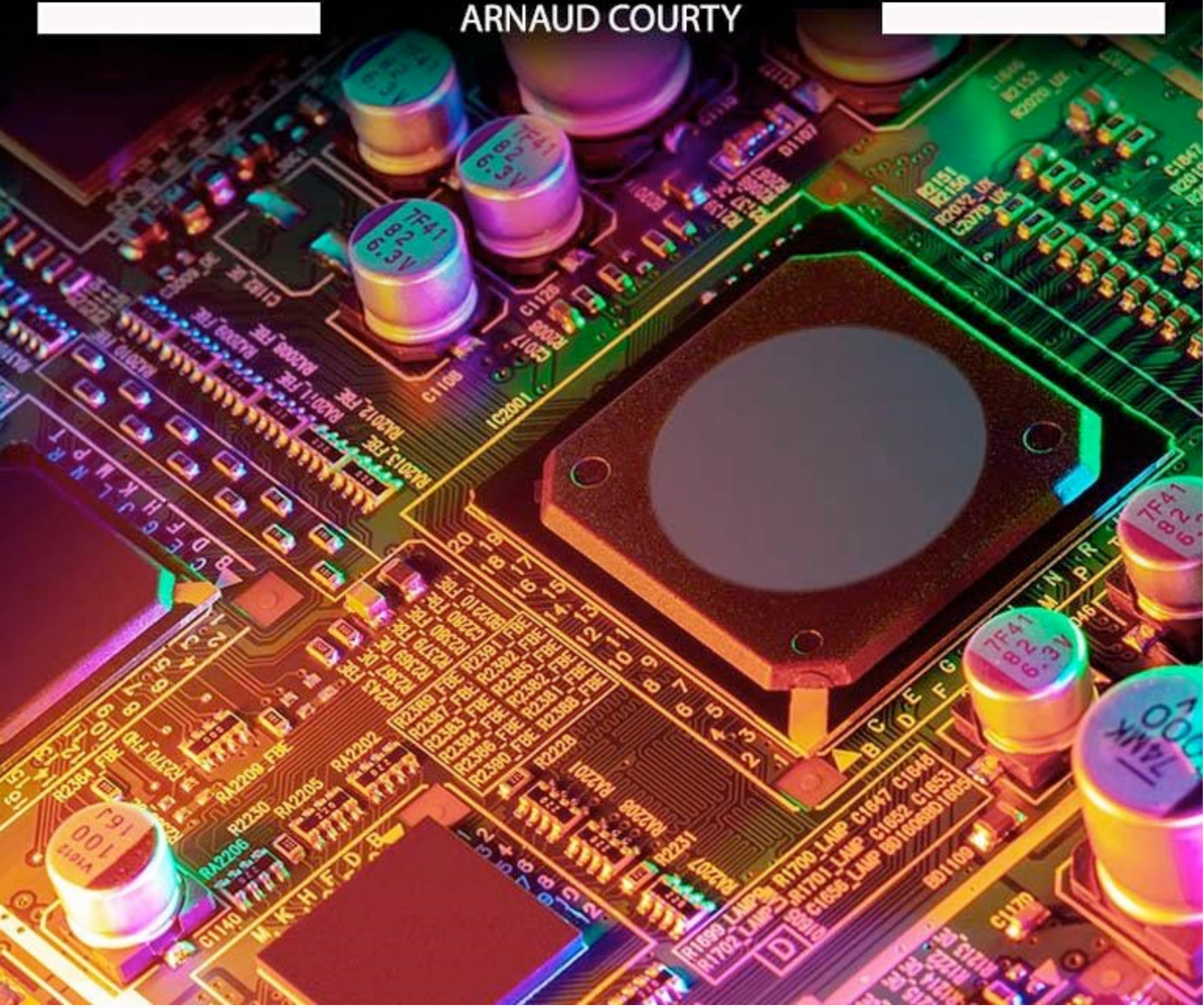
Course Brochure

Hakin9

IOT SECURITY - THE DVID CHALLENGE

ARNAUD COURTY



IoT Security - the DVID Challenge

IoT is a growing market and will be the future of our daily lives. Because of its emerging, there is no standard to steward the development process but there are many protocols and custom solutions to connect a hardware device to a cloud. Sometimes, middleware (like a smartphone application) could be encountered between the hardware and the cloud.

From my research, I would like to share my knowledge on IoT Security. This course is designed to help:

- IoT makers, in order to help them develop with security guidelines and view impact about security absence
- Security researchers, in order to help them to identify the most famous vulnerabilities and be trained with them
- IT Decision makers, in order to help them have the correct reflexes when IoT knocks on their IT door

This IoT course will explain IoT concepts, IoT construction and inside security holes. Each student will train themselves on a dedicated open sourced vulnerable board. They will be able to improve their skill to find vulnerabilities and learn how avoid them during development.

Because the board is owned by each student and will still be in the open sourced community, students could develop other training and get all new published content for free.

After completing the course, each student will be able to identify most famous IoT vulnerabilities, like plug his computer into debug interfaces, analyze outgoing exchange, try to understand used protocol and do some fun tricks with it. They also will be able to write a relevant audit report with vulnerability details and remediation.

About course tools: each student will get the Damn Vulnerable IoT Device (DVID) with extension board (Bluetooth), a USBasp to flash the device and USBuart to communicate with the board. For each training, the student will flash the device with the corresponding firmware and start to find the solution.

About the author: Arnaud Courty

As an IoT expert, my main mission is to evangelise companies to take care of security from the design step.

I work on internal and external offensive security analysis and assessment of security maturity of embedded systems upstream of their industrialization.

Since the beginning of IoT, I specialize in vulnerabilities research adapted to the embedded systems but also awareness of designers, developers and integrators. I take advantage of security events and working groups to campaign for a less vulnerable IoT world.

Prerequisites:

- Basic knowledge of web and mobile security
- Knowledge of Linux OS
- Basic knowledge of programming - Python

What attendees should bring:

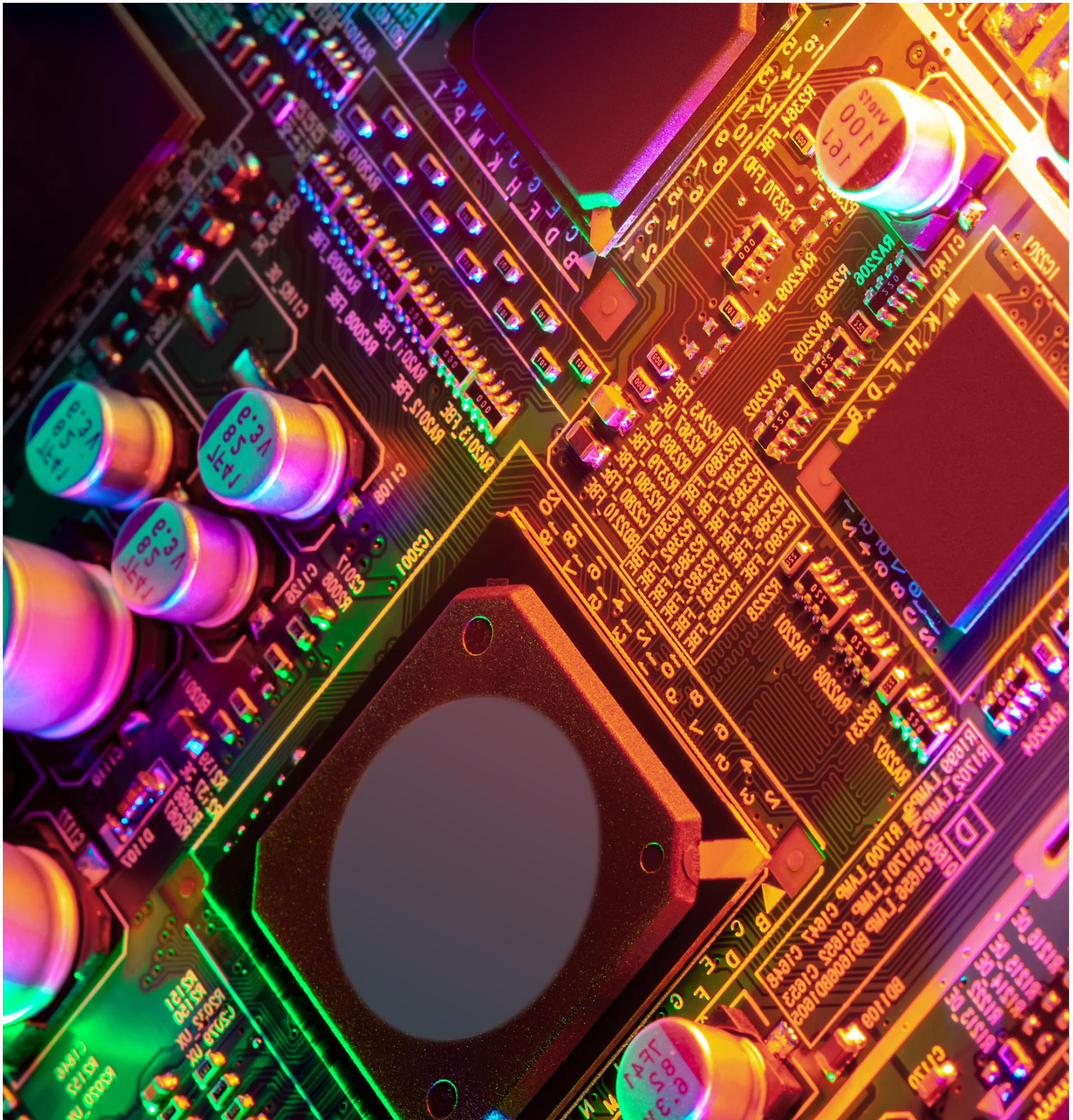
- Laptop with at least 50 GB free space
- 8+ GB minimum RAM (4+GB for the VM)
- External USB access (min. 2 USB ports)
- Administrative privileges on the system
- Virtualization software
- Android phone

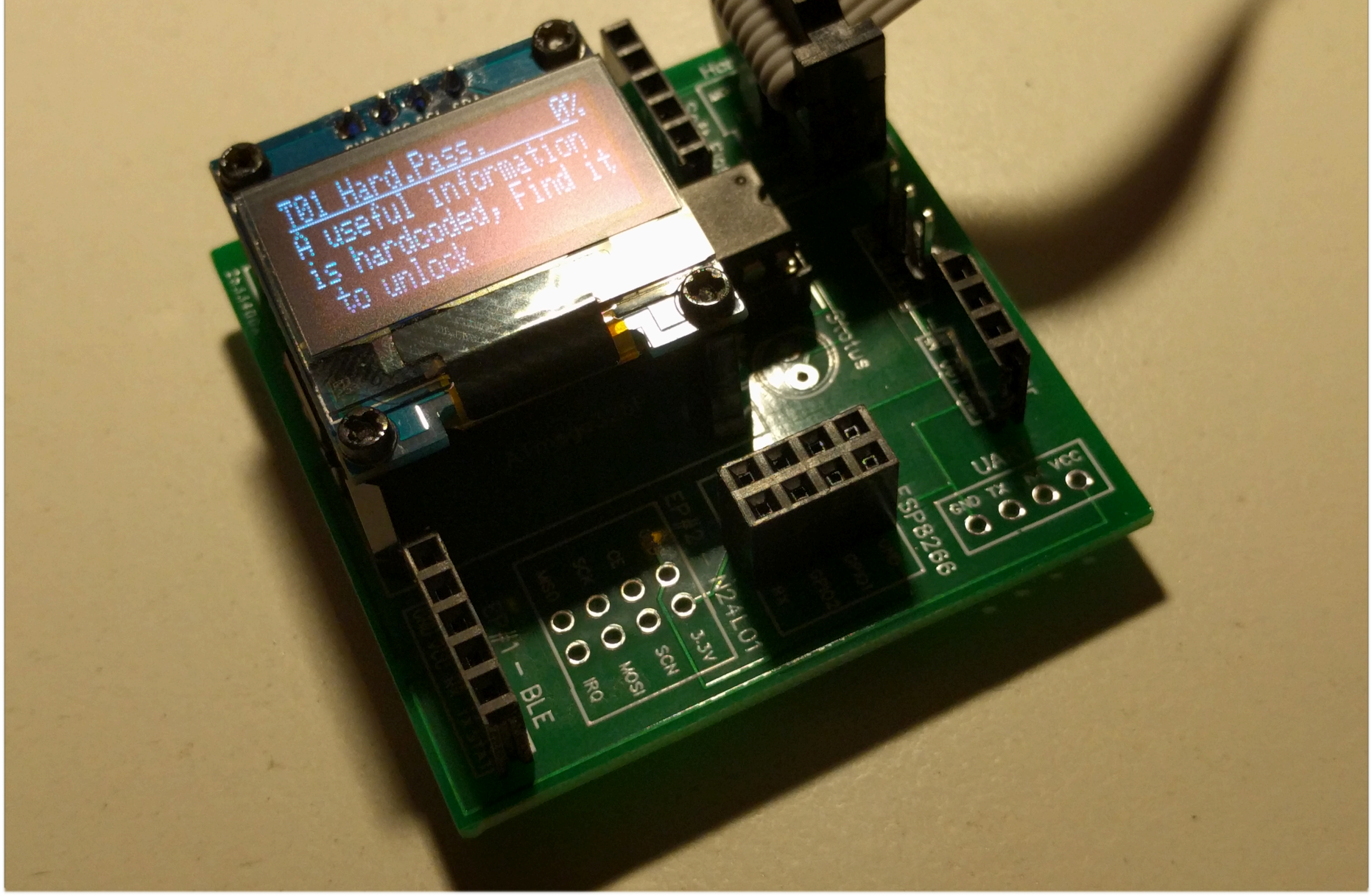
TABLE OF CONTENTS

1

The DVID board

The intentionally vulnerable device to help you learn IoT security





All content is open sourced and published here:

https://github.com/Vulcainreo/DVID

The DVID Open Sourced board

This IoT device is designed by myself and published as open source. The main objective is to provide to interested people a vulnerable board to improve their skill in IoT hacking.

The board core is composed of an Atmega328p and an OLED screen. For each training, a firmware could be flashed on the Atmega328p in order to offer a specific vulnerable environment.

There is also a connection port like UART, Bluetooth, 2,4Ghz and Wifi. In each training, a specific extension board must be plugged in to do the training.

Trainings need some attack tools like USBasp and USBuart. Many students may already have them.

In this course, firmware, objective and solution are provided free as open source. Moreover, I will provide more specific explanation only for this course.

**Schematic and component reference*: the student must buy everything himself, make the board and solder all components. This package will be provided free.

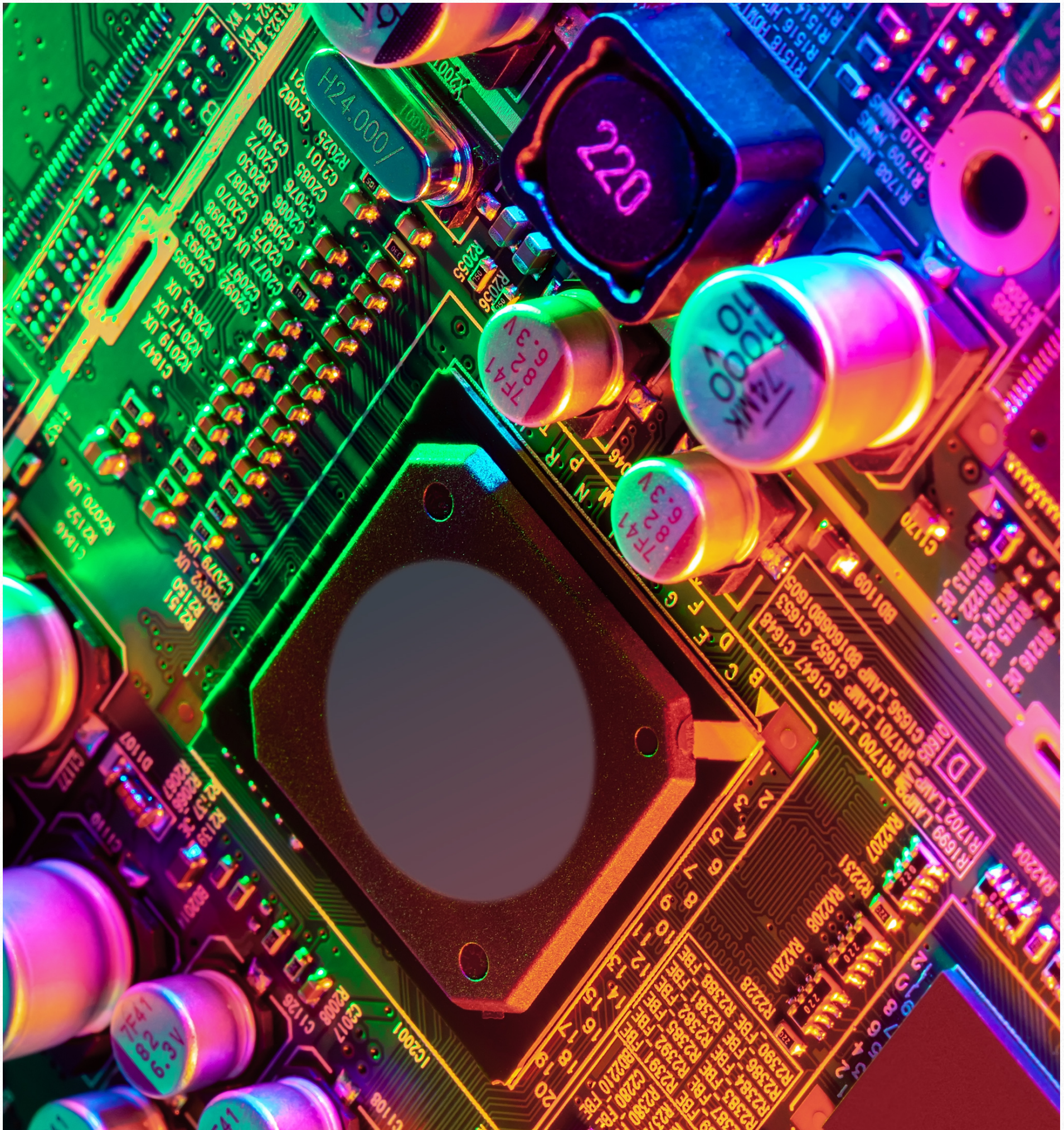
**Full package*: the student will receive everything needed for this course (soldered board, external board and attack tools).

As described before, some students may already have attack tools. They may wish to go further than the course by subscribing to Github alert on the DVID repository.

2

The Course Syllabus

What we plan to teach you



Time Organization

The course will be organized as this table. The estimated duration is 18 hours, with 7 hours of practical work, 11 hours of lectures. The course will finish with a 24h at home final exam.

Module	Total time	Details
Module 1 : Generalities	1 hours	(45mn) Course (15mn) Practical Work
Module 2 : Hardware and firmware attacks	6 hours	(3h) Course (3h) Practical Work
Module 3 : Middleware interactions	4 hours	(2h) Course (2h) Practical Work
Module 4 : Cloud interactions	4 hours	(3h) Course (1h) Practical Work
Module 5 : Audit methodology	3 hours	(2h) Course (1h) Practical Work
Exam : Audit an IoT device	24 hours	(3h) Vulnerabilities identification (2h) Vulnerabilities explotation (2h) Report writing

Module 1 : Generalities

This module will cover generalities about IoT. After a few reminders of protocols, we will discuss IoT architecture and discover the Practical Work board.

1. **A few reminders**

2. **Communication protocols**

    2.1. UAT

    2.2. JTAG

    2.3. SPI

3. **Generality**

    3.1. Security VS safety

    3.2. Security objectives and definition

    3.3. Embedded system life cycle

4. **Architecture**

    4.1. Hardware level

    4.2. Software level

    4.3. Communication level

    4.4. Security level

    4.5. Focus on SecBus architecture

5. **Discovering an IoT object (TP board)**

    5.1. Discovering methodology

    5.2. Hardware identification

    5.3. Gain information on Internet

    5.4. Making a schema

    5.5. Identify available attacks

Practical Work: Discover the Practical Work board DVID

1. Tools installation on student computer
2. Learning how flash the board with a Practical Work firmware

Project: Start to dev an IoT Device

1. Get started with Arduino IDE
2. Try to write a program to print text on the DVID screen
3. Try to write a program able to interact with serial

Module 2 : Hardware and firmware attacks

This module will cover hardware and firmware attacks. After discovering all available attacks, we will discuss and train vulnerabilities on the DVID board.

1. **Hardware attacks**
    - 1.1. Side channel attacks - Timing attacks
    - 1.2. Memory spying attacks
    - 1.3. On bus attacks
    - 1.4. Fault injections
    - 1.5. Hardware reverse engineering
2. **Well known vulnerabilities**
    - 2.1. Sensitive information on debug port
    - 2.2. Unencrypted firmware
    - 2.3. Weak algorithm
    - 2.4. Hardcoded sensitive information
3. **Countermeasures**

Practical Work - First board interaction

1. First interaction with the board (UART with Tx and RX)
2. Try to discover the password (password displayed on the console - student must write it on the serial TX connection to unlock)
3. Try to identify Tx pin on a signal analysis tool (tools aren't needed - it's based on provided picture) and try to get the correct password (two tries before board resetting)

Practical Work - Default password

1. Search on Internet for a default password (Mirai source code could be found on several Github repo)
2. Write a program to enumerate them (program asks the student for the password - there is no protection against brute force)
3. Student must try several passwords in order to find the correct one)

Practical Work - Hard-coded password

1. Try to extract onboard firmware with avrdude tool
2. Explore the firmware to get the hard-coded password
3. Try same with the provided hex file
4. Pass it on TX connexion to unlock

Practical Work - Buffer overflow

1. Write a Python program to explore the memory
2. Try to get the user password (the program said that a five entry table is set. Student could request each case by a number. Program must enumerate each number from 1 to 300 to identify ASCII content and get the password)

Practical Work: Weakness in algorithm

1. Students get a pseudo code of an algorithm. They must identify the weakness and write a program to exploit it
2. The firmware has brute force protection - students must be smart
3. Pass the correct password to unlock

Project: Escape from to DVID room

1. Stage 1: detect the cypher used to encrypt the firmware
2. Stage 2: try to detect with default password list
3. Stage 3: get the hard-coded credentials in the firmware
4. Stage 4: gain access to the console from the serial port with previous credentials

Module 3: Middleware interactions

This module will cover middleware interactions from hardware to cloud. After discovering a well known protocol, we will discuss and train about IoT usage and available attacks.

1. **Protocol discovering**
2. **MQTT**
   - 2.1. Presentation
   - 2.2. Attacks

Practical Work - MQTT sensor

1. Write a productor MQTT sensor that pushes every minute to officially broker the current time
2. Write a customer MQTT that subscribes to the previous MQTT time topic

Practical Work - MQTT Attacks

1. Find well known broker sensitive information published by users
2. Find a Shodan misconfigured MQTT Server

3. CoAP:

3.1. Protocol Presentation

3.2. Models

3.3. Message

Practical Work - COaP communication

1. Send a message to a well known server
2. Try to discover some resources

4. Radio Parking remote

4.1. Presentation

4.2. Attack methodology

Practical Work - Analysis of parking remote

1. Identify frequency based on hardware picture
2. Analysis of the recorded stream
3. Protocol Reverse engineering

5. Bluetooth Low Energy

5.1. Why such a difference between Bluetooth 2 and Bluetooth 3?

5.2. Advertising Concept

5.3. Characteristics & services Concept

5.4. Communication encryption

Practical Work - Decrypt the BLE exchange

1. Analyze the encrypted exchange between DVID and Android app
2. Get the key to decrypt stream
3. Get the code to unlock challenge

Practical Work: Discover advertising of DVID

1. Try to scan around BLE devices
2. Try to view in wireshark advertisement packets

Practical Work - Discover characteristics of DVID

1. Gattools
2. Bleah

Practical Work - Reverse engineering an IoT device

1. Get HCI exchange from Android
2. Try to replay characteristics

Project: Unlock the DVID door

1. Stage 1: analysis of BLE services and characteristics
2. Stage 2: identify opening characteristics
3. Stage 3: get HCI logs to see that it's a rolling code
4. Stage 4: reverse to Android APK to get the rolling code and find vulnerabilities
5. Stage 5: write a program to predict the next rolling code and open the door

Module 4 : Cloud interaction

This module will cover cloud interaction from a device or device through a middleware. After discovering well known vulnerabilities, we will discuss and train about IoT specific vulnerabilities.

1. Vulnerabilities identification

- 1.1. Injection
  - 1.1.1. SQL code injection
  - 1.1.2. NoSQL code injection
- 1.2. Broken authentication
  - 1.2.1. Session management
  - 1.2.2. Backdoor
- 1.3. Sensitive Data Exposure
- 1.4. Broken access control
  - 1.4.1. Vertical moving
  - 1.4.2. Horizontal moving
- 1.5. Security misconfiguration
- 1.6. Cross-site Scripting
- 1.7. Insecure deserialization
- 1.8. Using component well known vulnerabilities
- 1.9. Insufficient logging & monitoring

2. Rest API Analysis

- 2.1. JWT token
- 2.2. API keys
- 2.3. Method HTTP
- 2.4. Content type validation

2.5. Endpoint management

2.5.1. Error handling

2.5.2. Security Headers

2.5.3. Cross origin resource sharing

Practical Work: Vulnerabilities identification

1. Try to break the authentication
2. Default password
3. Predictable cookie
4. Try to direct access to sensible data
5. Try to exact session cookie from Cross Site Scripting

Module 5: Audit methodology and reporting

This module will cover the audit methodology and reporting. We will discuss making relevant reports and as exhaustive as possible on vulnerabilities identification

1. General information

1.1. Responsive disclosure

1.2. Authorization

1.3. Requirements

2. Audit methods

2.1. Penetration testing and Audit

2.2. Bug bounty

3. Analysis methodology

3.1. Hardware

Practical Work : Make a relevant report

1. From a vulnerability list, try to write associated risks
2. Try to make relevant remediation for given vulnerabilities

Exam: Audit an IoT device

In this exam, students will be in front of an IoT device. This device could be controlled by a Android application. This application pushes also on cloud the device status.

All learned skills about hardware analysis, middleware reverse or cloud exploration are needed to analyse the security of this IoT Device. Students must write a relevant report to show all findings and provide remediations on found vulnerabilities.

Exam general information:

This exam will have a 24 hour time limit. Student will have access to all slides and Internet.

Marks:

A list of designed vulnerabilities is set before the exam starts. The final mark is max 20 points:

1. First part for 10: 1 point for each vulnerability identified

2. Second part for 5: 0.5 point for each remediation associated of each identified vulnerability

3. Third part for 5: 2.5 on the technical summary and 2.5 on the executive summary

4. 10 bonus points for finding a 0-day :)

3

FAQ

DVID AND THE COURSE

What is the DVID?

The DVID (Damn Vulnerable Internet Device) is an intentionally vulnerable IoT device to help you learn about IoT security.

Do I need the DVID to do the course?

Yes. Without it you won't be able to do any practical work throughout the course, a big part of the content will refer directly to it as well.

How can I get the DVID?

You can order a pre-made device with us, or you can make one yourself (buy all components and solder them together). For all instructions see the course description.

Who makes the DVID?

The DVID is manufactured by the instructor of the course, Arnaud Courty.

Are the devices tested before shipping?

Yes. All boards are thoroughly tested before shipping, as well as all components and attack tools provided with the device.

Can I order the parts from Hakin9 and solder the board myself?

No, we don't offer part packages for retail customers. It is possible for group orders - see "Special orders" section.

SHIPPING

Does the price include shipping?

Yes.

What countries do you ship to?

Shipping will be done worldwide, but tracking will be available only for specific countries.

Will the package have tracking?

The packages will have tracking enabled, if they are shipped to the following countries:

Germany, Saudi Arabia, Australia, Austria, Belgium, Brazil, Canada, South Korea, Croatia, Cyprus, Denmark, Spain, Estonia, United States, Finland, Gibraltar, Great Britain, Hong Kong, Hungary, Ireland, Iceland , Israel, Italy, Japan, Latvia, Lebanon, Lithuania, Luxembourg, Malaysia, Malta, Norway, New Zealand, Netherlands, Poland, Portugal, Russia, Singapore, Slovakia, Slovenia, Serbia, Sweden, Switzerland.

Where will be the package shipped from?

France.

Where can I give my shipping address?

Since this is a special order, we will be contacting you by email with further instructions and more details.

When will the shipment be made?

Since the boards are manufactured just for this course, we will contact you with specific details. Between ordering parts, manufacturing, and shipping, it might take 30+ days to send the board your way. You will be notified when the shipment is made.

What if the package arrives damaged?

Please document the package and contact our e-Learning manager Marta at marta.strzelec@hakin9.org

What if the board arrives damaged?

Please document the board and contact our e-Learning manager Marta at marta.strzelec@hakin9.org

What if the package gets lost in shipment?

If you received a notice from us confirming that we've sent the package and the shipment does not arrive after a reasonable amount of time, please contact our e-Learning Manager Marta at marta.strzelec@hakin9.org

I AM A HAKIN9 PREMIUM SUBSCRIBER / IT PACK PREMIUM SUBSCRIBER / LIFETIME SUBSCRIBER

Do I still need to get the board?

Yes, the course is included in your subscription, but the board is not. Don't worry, we have a special product made just for you, where you can purchase the premade board independently from the course:

TU LINK

You can also manufacture the board yourself, if you're feeling up to it - see instructions in the course description.

Does the BOARD ONLY product include access to the course?

No. The BOARD ONLY product includes only the premade board and course access is not included. You have course access through your premium subscription.

If my subscription expires before the course starts but I order the board, do I keep access to the course?

No, you should either purchase a seat on the course, or renew your subscription.

Will I still have access to the course if I don't buy the board?

Yes, you will be able to view the training materials and see the assignments. However, you won't be able to perform any practical exercises from the course, unless you make the board yourself (instructions provided in the course description).

SPECIAL ORDERS

My University would be interested in enrolling our students in this course. Are there any discounts?

Educational institutions receive a discount for course enrollment. The price of the DVIDs (if you choose to order them as well) will not be discounted. Please contact our Product Manager Marta Sienicka at sienicka.marta@hakin9.org for further details.

My University has a premium subscription and would like to make a bulk order for the DVID. How can we make an order? Will we get a discount?

You can make a bulk order, but the price will not be discounted - the price of the DVID as offered on the website includes bare manufacturing and shipping costs. Please contact our Product Manager Marta Sienicka at sienicka.marta@hakin9.org for further details.

My University would like to make a custom order for naked boards and parts without soldering, and let the students do it themselves. Is that possible?

Yes, provided you meet certain criteria in regards to the amount of the packages you want. Please contact our Product Manager Marta Sienicka at sienicka.marta@hakin9.org for further details.

My company would like to enroll our employees in this course. How can we make an order?

Companies receive a discount for group course enrollment only. The price of the DVID (if you choose to order it as well) will not be discounted. Please contact our Product Manager Marta Sienicka at sienicka.marta@hakin9.org for further details.

My company has a group premium subscription and would like to make a bulk order for the DVID. How can we make an order? Do we get a discount?

You can make a bulk order, but the price will not be discounted - the price of the DVID as offered on the website includes bare manufacturing and shipping costs. Please contact our Product Manager Marta Sienicka at sienicka.marta@hakin9.org for further details.

My company would like to make a custom order for naked boards and parts without soldering, and let the students do it themselves. How can we make an order?

Yes, provided you meet certain criteria in regards to the amount of complete packages you want. Please contact our Product Manager Marta Sienicka at sienicka.marta@hakin9.org for further details.

RETURNS & REFUNDS

The package was damaged when it arrived. Will I get a refund or a replacement?

Please document the package and contact our e-Learning manager Marta at marta.strzelec@hakin9.org. We offer replacements if you meet the criteria for one.

The board arrived damaged, and was not working. Will I get a refund or a replacement?

Please document the board and contact our e-Learning manager Marta at marta.strzelec@hakin9.org. We offer replacements if you meet the criteria for one.

I bought the board, but I don't want it anymore. Can I return it and get a refund?

You can only return undamaged boards within 14 days of receiving them. You have to inform us of your intent to return within that timeframe, by email at marta.strzelec@hakin9.org

You are responsible for the return shipment and its cost. It should be made to a return address we provide. You must provide us with proof of shipment within 14 days of informing us of intent to return.

After we receive your return package, the board will be evaluated for damage, and if everything checks out, we'll reverse your payment and reimburse your shipping cost.

I bought the board + course package, but I don't want the board anymore. Can I return it, but keep the course?

Yes. You can only return undamaged boards within 14 days of receiving them. You have to inform us of your intent to return within that timeframe, by email at marta.strzelec@hakin9.org

You are responsible for the return shipment and its cost. It should be made to a return address we provide.

After we receive your return package, the board will be evaluated for damage, and if everything checks out, we'll reverse your payment.

I bought the board + course package, but I don't want the course anymore. Can I return it, but keep the board?

Yes, if you meet the criteria. For our return policy for on-line courses, please refer to our Terms of Service.

I bought the course, but I don't want it anymore. Can I get a refund?

Yes, if you meet the criteria. For our return policy for on-line courses, please refer to our Terms of Service.