CYBERSCHOOL
GRADUATE CYBERSECURITY
RESEARCH SCHOOL

MASTER'S IN COMPUTER SCIENCE
HARDWARE SECURITY MAJOR

DEGREE: Master's in Computer Science, Cybersecurity track

- **ECTS:** 120 ECTS
- **Duration:** 2 years, full-time
- **Academic curriculum run by:** Université de Rennes 1
- **Academic curriculum organised by:** CyberSchool
- **Place:** Beaulieu Campus, Rennes

TRAINING PROGRAMME OBJECTIVES

This major focuses on IoT's ecosystem security. Those electronic devices are prime targets for potential attackers.

The different courses offered in this specialisation allow students to discover the methods, tools, technical means necessary for the audit of embedded electronic systems. The key concepts of electronic architectures (hardware), interfaces with their external environments (Internet, Wifi, Radio Frequency Communication), embedded software and also vulnerabilities at all these levels, will be presented to students, as well as the theory necessary for the understanding of security challenges in these environments (Cryptography and associated mathematics, signal processing basis for example).

TEACHING ORGANISATION

The Master's degree is divided into 4 semesters, comprising lectures, tutorials and practicals. Students follow courses dedicated to the Hardware Security major, as well as courses shared with students from other CyberSchool specialisations.

Some of the teachings are done in English.

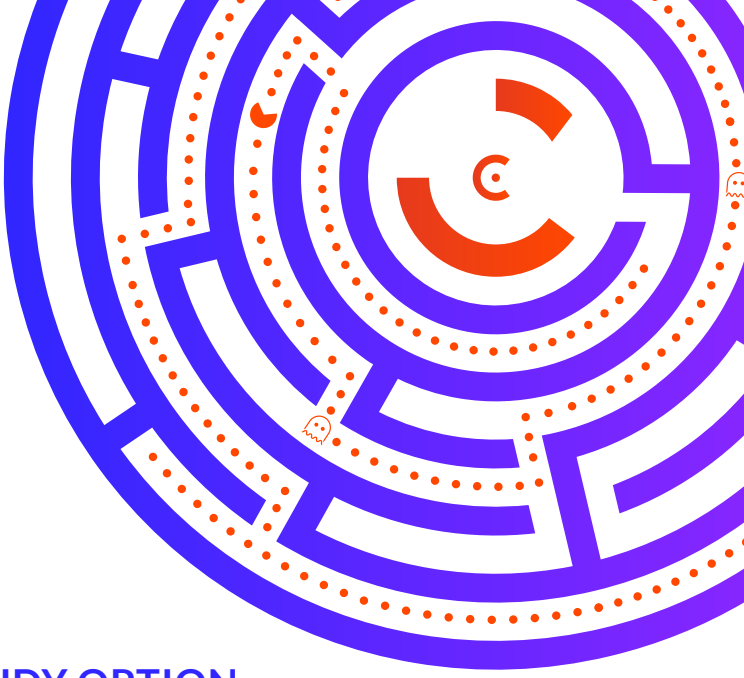
The teaching team is made up of IRISA (leading French IT lab) and internationally renowned cybersecurity research professors.

- A two-month in-company internship is carried out in the first year from may (optional).
- In the second year, students carry out a four-six month internship in a company or research laboratory from March. This internship can be carried out abroad. The master's year ends with a written report and an oral presentation in front of a jury.

More details on our website:
cyberschool.univ-rennes.fr

CYBERSCHOOL

GRADUATE CYBERSECURITY RESEARCH SCHOOL



WORK-STUDY OPTION

Students who choose the Hardware Security major are able to take their second Masters year as a work-study programme option, either through an apprenticeship or a professional-training contract.

ACQUIRED SKILLS

- Understand the security of IoT (Hardware, Software) environments.
- Be able to reverse engineer the software embedded in the IoT.
- Understand security best practices for embedded IoT or electronics environments.
- Know how to analyze the security of radio frequency communication protocols.
- Be able to participate in the process of securing IoT products and ecosystems.

PREREQUISITE

▸ Hold/or be in your final year of studies of a Bachelor of Computer Science or Electrical and Electronic Engineering.

▸ Selective training programme with admission upon application and file study.

CAREER OPPORTUNITIES

- Pentester or embedded systems auditor.
- Cybersecurity consultant in the field of IoT.
- Further study towards a PhD.

CONTACT US

CYBERSCHOOL
Pôle Numérique Rennes Beaulieu
263 Av. du Général Leclerc - CS 74205 - 35042 Rennes cedex
E : cyberschool@univ-rennes.fr

More details on our website:
cyberschool.univ-rennes.fr

Supported by:

CYBERSCHOOL
ÉCOLE UNIVERSITAIRE
DE RECHERCHE EN CYBERSÉCURITÉ

MASTER INFORMATIQUE
MAJEURE SÉCURITÉ MATÉRIELLE

DIPLÔME : Master informatique parcours cybersécurité

- **ECTS :** 120 ECTS
- **Durée :** 2 ans, temps plein
- **Délivré par :** Université de Rennes 1
- **Formation assurée par :** CyberSchool
- **Lieu :** Campus de Beaulieu, Rennes

OBJECTIF DE LA FORMATION

Cette majeure est axée sur la sécurisation des systèmes embarqués. Ces derniers sont des systèmes électroniques et informatiques autonomes contraints. Leur connectivité aux réseaux du monde extérieur et les données qu'ils renferment en font des cibles privilégiées aux yeux des attaquants potentiels.

Avec cette spécialisation, les étudiant.e.s sont formé.e.s aux audits logiciels et hardware et à la sécurité des systèmes embarqués. L'objectif est ainsi de former des auditeur.trice.s capables de vérifier la sécurité d'une plateforme IoT tant au niveau du matériel que du logiciel et de la cryptographie qui sont embarqués dessus.

ORGANISATION PÉDAGOGIQUE

Le master est divisé en 4 semestres, comprenant des cours magistraux, des travaux dirigés et des travaux pratiques. Les étudiant.e.s suivent des cours consacrés à la majeure Sécurité matérielle, ainsi que des cours mutualisés et partagés avec les étudiant.e.s des autres spécialisations de la CyberSchool.

L'enseignement est partiellement dispensé en anglais.

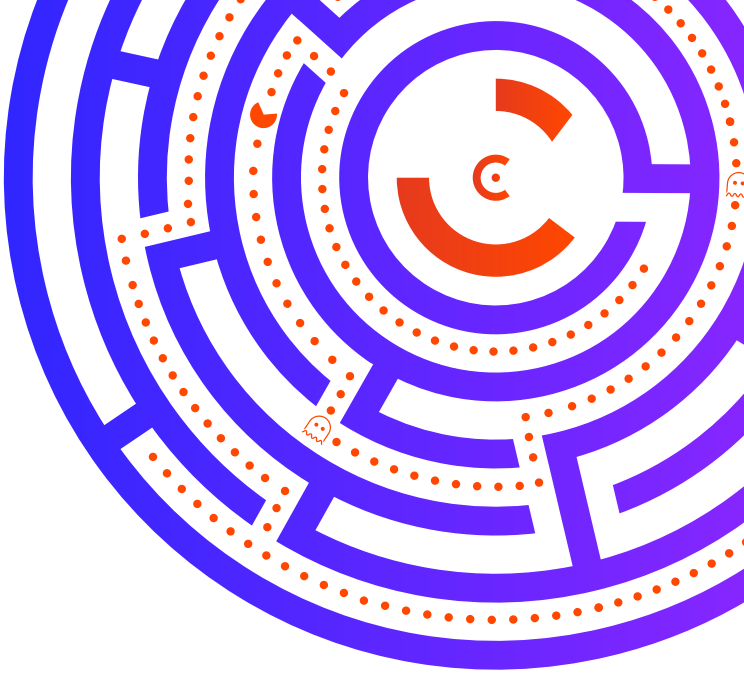
Tous nos enseignements sont assurés par des enseignant.e.s-chercheur.euse.s et des professionnel.le.s spécialisé.e.s dans le domaine de la cybersécurité.

- En première année, un stage de 2 à 3 mois en entreprise est prévu à partir du mois de mai (optionnel).
- En deuxième année, les étudiant.e.s réalisent un stage en entreprise ou laboratoire de recherche dès le mois de mars, et ce pour une durée de 4 à 6 mois. Le stage peut être effectué à l'étranger. Il donne lieu à un mémoire et une soutenance.

Plus d'infos sur notre site internet :
cyberschool.univ-rennes.fr

CYBERSCHOOL

ÉCOLE UNIVERSITAIRE DE RECHERCHE EN CYBERSÉCURITÉ



ALTERNANCE

Les étudiant.e.s qui choisissent la majeure Sécurité matérielle ont la possibilité de réaliser leur deuxième année de master en alternance par le biais d'un contrat d'apprentissage ou d'un contrat de professionnalisation.

COMPÉTENCES ACQUISES

- Audit et sécurité des plateformes matérielles embarquées.
- Rétroingénierie et objets connectés.
- Assistance à la sécurisation d'objets ou de plateformes matérielles.
- Analyse de sécurité de protocoles radiofréquences.
- Aide à la conception et au développement de plateformes matérielles sécurisées.

PRÉREQUIS

- **Licence en informatique ou génie électrique et électronique.**
- **Formation sélective avec admission sur candidature et étude de dossier.**

DÉBOUCHÉS

- Pentester.euse ou auditeur.trice de systèmes embarqués.
- Consultant.e en cybersécurité dans le domaine des IoT.
- Poursuite d'études vers un doctorat.

NOUS CONCTACTER

CYBERSCHOOL
Pôle Numérique Rennes Beaulieu
263 Av. du Général Leclerc - CS 74205 - 35042 Rennes cedex
E : cyberschool@univ-rennes.fr

Plus d'infos sur notre site internet :
cyberschool.univ-rennes.fr

Avec le soutien de :