MITRE EMBEDDED CAPTURE THE FLAG COMPETITION

MITRE's Embedded Capture-the-Flag (eCTF) is an embedded security competition that gives teams the opportunity to experience of creating a secure system and learning from their mistakes. This competition helps develop practical skills that can be applied to securing critical embedded systems, such as UAVs, smart grids, and IoT devices. Participation can pave the way to a lifelong career in the embedded security space.

COMPETITION FORMAT

Over each Spring semester, hundreds of students across the globe compete in MITRE's eCTF competition.

MITRE's eCTF is unique from other CTF competitions. First, the focus of the eCTF is on embedded systems, and competitors work on physical hardware. This presents a new set of challenges and security implications. Second, MITRE's eCTF balances offense and defense by testing and awarding both sets of skills.

The competition is split into two six-week phases: "Design" and "Attack". In the design phase, students develop a secure embedded system that meets a set of requirements. In the attack phase, students compete to break the security of other teams' designs.

Design Phase

Teams design and implement systems that meet security and functionality requirements

Handoff

Organizers test each design for functionality

Attack Phase

Teams analyze and attack each other's designs for points

Join Us in Developing Tomorrow's Cyber Workforce:

Don't miss out on the chance to be a part of this extraordinary journey. Together, let's shape the landscape of cybersecurity and unveil a world where innovation and secure embedded systems thrive!

eCTF10
10 YEARS OF THE EMBEDDED CAPTURE THE FLAG

MITRE EMBEDDED CAPTURE THE FLAG COMPETITION

What Students Get Out of the eCTF

Throughout the competition, students have the opportunity to learn hard and soft skills not often taught in the classroom.

During the design phase, students design and build a realistic system and meeting complex security requirements without sacrificing functionality. This open-ended task promotes problem-solving and offers what are many students' first experiences in project management, cybersecurity, and embedded systems. Students also gain an understanding of cryptography through the design and implementation of their secure protocols.

During the attack phase, students learn hands-on, real-world attacks in an unparalleled experience. Since the designs being attacked are created by other teams, students search for and encounter real, unintended vulnerabilities, rather than pre-canned challenges that are often used in other CTFs.

During the attack phase, students learn hands-on, real-world attacks in an unparalleled experience. Since the designs being attacked are created by other teams, students search for and encounter real, unintended vulnerabilities, rather than pre-canned challenges that are often used in other CTFs.

The eCTF as a Course

Many schools offer the eCTF as a for-credit course, often as a special topics course or an independent study. We strongly recommend this route as it helps students to commit time for the competition and recognizes and awards students for their efforts.

Example syllabi are available upon request.

The eCTF challenge defines several deliverables that universities can use as course assignments. These include design documents, offensive and defensive writeups, and the system implementation itself.

Faculty may also choose to augment the competition with additional lectures or readings.

Next Steps

If you are interested in the eCTF, please go to https://ectf.mitre.org to join our email list for updates about the competition. You may also want to begin the process of creating a for-credit course for your team next semester.

When team registration opens in September at https://ectf.mitre.org, you will be able to register your intent to form a team, even if you don't yet know the exact students that will participate.

100%

Learned more about embedded system security through the eCTF

3X

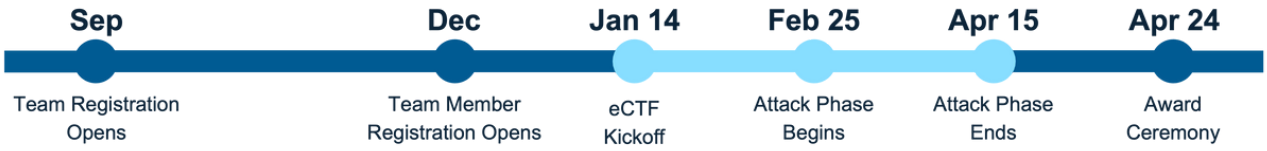
Likelihood for a team that was offered college credit to make it to the attack phase

30%

Higher self-reported learning outcomes by students who were offered college credit

eCTF 10
10 YEARS OF THE EMBEDDED CAPTURE THE FLAG

MITRE EMBEDDED CAPTURE THE FLAG COMPETITION



Frequently Asked Questions

Does the eCTF cost anything?
Participation in the eCTF is entirely free! MITRE will provide the resources to complete the competition including hardware, however teams may choose to purchase additional resources to aid with development or attacking.

Who can participate?
Anyone! Students at all academic levels are welcome to participate. Basic programming experience is required and any experience with C and Python will greatly help teams. Sponsorship of a faculty member, teacher, or adult mentor to act as a team advisor is required.

How big should a team be?
Team sizes are unlimited. We have seen successful teams of anywhere from one to 40 students, however we generally recommend new teams aim for 4-10 students. Fewer than four and students can become overwhelming if the team isn't prepared for the commitment

What is provided by MITRE to help?
MITRE provides teams with a reference implementation, embedded hardware, and technical guidance throughout the competition.

How can I prepare my team?
You can view pasts competitions on our rules website at https://rules.ectf.mitre.org, which should get your team up to speed on what is expected. The competitions run on affordable, commercially-available microcontrollers, so you can purchase additional ones to practice development and attacks at any time.

What is this year's challenge?
TIn the 2026 eCTF, teams will design and implement a secure storage solution for a chip foundry. The system must allow users with various roles to access the proper data without leaking sensitive chip designs to unauthorized parties.

FOR MORE INFORMATION ABOUT MITRE'S ECTF, CONTACT ectf@mitre.org OR VISIT US AT https://ectf.mitre.org

eCTF10
10 YEARS OF THE EMBEDDED CAPTURE THE FLAG