Pedagogy behind cryptology CTF challenges and a way to improve them

Emanuel Nicolás Herrador

Facultad de Matemática, Astronomía, Física y Computación, Universidad Nacional de Córdoba, Argentina
emanuel.nicolas.herrador@unc.edu.ar

Abstract. In this poster work, the objective is to open a talk with conference participants about cryptology CTF challenges, its reality nowadays and a way to improve them. Since the scope of this challenges is limited to break particular implementations of systems or servers that use an specific set of protocols or tools with some error (to introduce a weakness to exploit it), it's a little hard to create new creative problems that aren't reduced only to a "paper-search" or looking an error with the implementation (some bits leaked, a nonce reused, a way to get an encrypt oracle for ciphers non CPA secures, or a decrypt oracle for non CCA secures, etc.).

The poster objective is to open a talk about the pedagogy behind this challenges and how to improve them to do them more interesting and, also, with a high educative value. Along with this, the poster will show an example of an actual CTF challenge for people that doesn't knows them or their structure, or people that wants to solve a challenge. This problem is *Samsara* of the International Cybersecurity Challenge 2024, and it's about the Frozen Heart Vulnerability for a non-interactive Girault's proof of knowledge protocol, with a non-sequential LCG to be able to recover the modulo and exploit it. Finally, the poster will contain a question about how to improve this specific challenge or how the participants will do challenges for their specific research field.

Introduction and Contributions

Capture the Flag (CTF) is a competition type for computer science field, more specific for cybersecurity field, where participants should solve problems finding hidden strings with an specific format that are called "flags". The flags are usually in specific points of a server, program or implementation to make sure that getting this secret string means that the problem is solved using the author's ideas and specific vulnerabilities included to exploit. I.e., usually a problemsetter for CTF challenges tries to include a flag forcing that solutions has to break a protocol, tool or system with a known way to do that (can be a general idea or maybe an specific attack found in a paper that describes it with a similar or same system configuration).

There're two main variations of CTFs that are Attack/Defense and Jeopardy. This poster will be focused principally in Jeopardy-style problems where flags are only stolen from the competition system and not from another teams (as is in Attack/Defense).

Categories for Jeopardy-style problems usually are Web Exploitation, Cryptography, Binary Exploitation, Reverse Engineering, Forensics, Miscellaneous, Hardware Hacking, OSINT (Open-Source Intelligence) or PPC (Profesional Programming Challenges). I'll focus in the Cryptography category, but sometimes problems of another categories contains a little of usually-known cryptography to solve as a middle step.

CTF is a type of competition and exists a lot of them as *DEF CON CTF*, *ICC* (International Cybersecurity Challenge), *ECSC* (European Cybersecurity Challenge), *Pwn2Own* or *GoogleCTF*. But also is a way to improve in cybersecurity field learning through a gamification way. CTF-style problems can be used for teachers, high schools or universities to teach about vulnerabilities in computer science fields, risks for bad implementations and cybersecurity skills to move securely in the network and using third party tools. Is a good and effective way to incorporate concepts into students by making them solve problems and study on their own how to solve them. Also, is a way to show how attacks in a textbook can be implemented in real life for non secure systems.

With this in mind, the poster will be focused in how CTF problems are useful to teach about specific cryptology fields and also making participants to think how they could create problems to show their specific field of study in a game form. The contribution is the idea of how each one could create a problem, being a teacher, researcher or student, and also how this way to learn can help us to improve our general knowledge about cryptography. Another contribution is a solution of a problem of the International Cybersecurity Challenge 2024, a competition in which all the world are participating representing their regions (Europe, USA, Canada, Latin America, Africa and Oceania).