MysteryTwister C3

THE CRYPTO CHALLENGE CONTEST

Heartbleed – Part 2

Author: Arno Wacker

August 2014 (Update: December 2019)

Introduction

This 3-part-challenge is based on the Heartbleed bug in OpenSSL discovered in April 2014. The group for Privacy and Compliance with the Research Institute Cyber Defence (CODE) at Bundeswehr University Munich provides a server for this challenge, which is specifically prepared to be vulnerable to the Heartbleed bug:

`https://heartbleed.datcom-unibw.de/`

On the above website, there is also further information about this challenge. To access the second part you have to solve stage 1 at first. The description for stage 3 will become available after you solve the respective preceding stage. All three stages can be solved by exploiting the Heartbleed bug. When solved correctly, you will find a codeword for each part.

Note

It is explicitly allowed to attack this server by exploiting the Heartbleed bug. This is safe since the server is isolated from the group's productive infrastructure. As long as you are accessing `https://heartbleed.datcom-unibw.de/` you are on the isolated bastion server. Additionally, there is no real information stored on it. The used self-signed certificate is considered compromised. All usernames and passwords used are fake and do not provide any real login to any of the group's systems.

Instructions

Please visit the website

`https://heartbleed.datcom-unibw.de/`

and solve the second part of this challenge. The found codeword is required for MTC3. In order to get access to the next stage of this challenge additional information might be required.

Even though this challenge cannot be solved with pen & paper, it is considered level 1 as there are tools available, which can get you to the solution. However, it is slightly more complicated than stage 1.

Remark

We added this challenge to MTC3 as an example for the fact, that in reality most of the times it is not the cryptography itself, which is attacked, but it's implementation.