UNIVERSITÄT PADERBORN
Die Universität der Informationsgesellschaft

HTTP Desync Attacks: Smashing into the Cell Next Door

Shashank Kanakapura Srivatsa
University of Paderborn
Paderborn, Germany
srivatsa@mail.uni-paderborn.de

Seminar report – May 15, 2020.
System Security Group.

Supervisors: **Prof. Dr-Ing. Juraj Somorovsky**
University of Paderborn
Paderborn, Germany
juraj.somorovsky@upb.de

Abstract

Internet has become an integral part of the modern world and it is extremely difficult to imagine a world without internet. One of the most significant activity on the internet is exchange of data between computers, generally referred to as Clients and Servers. There are a huge number of formats in which the data can be transferred over internet and many new formats are being introduced. To organize and govern such data transfers, there are several protocols defined by reputed researchers and organisations. One such prominent protocol is Hyper Text Transfer Protocol(HTTP), where a Client submits a request to the Server over the internet and the Server responds to the Client with approriate data or message.
Like several other protocols, HTTP also contains some vulnerabilities which can be exploited by malicious attackers and thus it becomes extremely necessary to identify such vulnerabilities. Security experts or *White hat hackers* help to identify vulnerabilities present in protocols such as HTTP and notify the concerning organisations or individuals about the same. This helps to fix the vulnerabilities present and thus prevent information leakage. There are several vulnerabilities that have been identified in the past and many of these problems are already addressed. In this report, we talk about a relatively new technique known as 'HTTP Desync Attack' which is developed to exploit the vulnerability in HTTP protocol. In this technique, the attacker tricks the Server into believing that the malicious request is actually a part of a normal user‘s request and thus allows the attacker to gain control over the request. This report reviews HTTP Desync Attacks in detail and further evaluates it to understand the pros and cons of the technique.

0.1 Introduction

If an attacker is able to snoop in on the data being exchanged, it can be used for malicious purposes. It can contain personal information of a person or an organisation, confidential data of goverments and organisations, financial data and so on.

HTTP has been constantly improved and has become an important protocol to secure the data that is transmitted over the internet. However, as the growth of internet increases the need for securing these data transfers also increases with it.

0.2 Background

- HTTP [1] :
- HTTP 1.1 :
- HTTP Headers :

0.3 Problem Statement

0.4 Approach

0.5 Case Studies

0.6 Evaluation

0.7 Advantages and Disadvantages

0.8 Future Work

0.9 Conclusion

Bibliography

[1] https://tools.ietf.org/html/rfc7231