BEAST TITLE TO-FILL

Yang Shichu
School of Cyber Science and Engineering
Huazhong University of Science and Technology
sigeryeung@gmail.com

Shu Yi
TO-FILL
TO-FILL
TO-FILL

Su Haochen
TO-FILL
TO-FILL
TO-FILL

Li Yucong
TO-FILL
TO-FILL
TO-FILL

Liao Haicheng
TO-FILL
TO-FILL
TO-FILL

ABSTRACT

Transport Layer Security (TLS) is an protocol that provides communication security over networks. However, there is a flaw in TLS 1.0 where the initial vectors for block ciphers are predictable. The BEAST attack, with some prerequisites and efforts, allows attackers in the middle to decrypt those encrypted messages. This paper will demonstrate the procedures of the BEAST attack, and propose methods in simulation and vulnerability detection.

General Terms

BEAST attack, TLS flaws, CBC exploits, vulnerability detection

Keywords

ACM proceedings, LaTeX, text tagging

1. INTRODUCTION

Transport Layer Security (TLS) has several versions. The specification for TLS 1.0 is RFC 2246[1].

2. BACKGROUND

2.1 A glance at TLS

2.2 CBC in block ciphers

CBC is one of the modes of operation used in block ciphers.

Supposing that $P_1, P_2, \cdots P_n$ are the plaintext blocks, with a initial vector IV, we have:

$$C_1 = E_k(P_1 \oplus IV)$$
$$C_i = E_k(P_i \oplus C_{i-1})(i \geq 2)$$

to obtain ciphertext blocks $C_1, C_2, \cdots, C_n$.

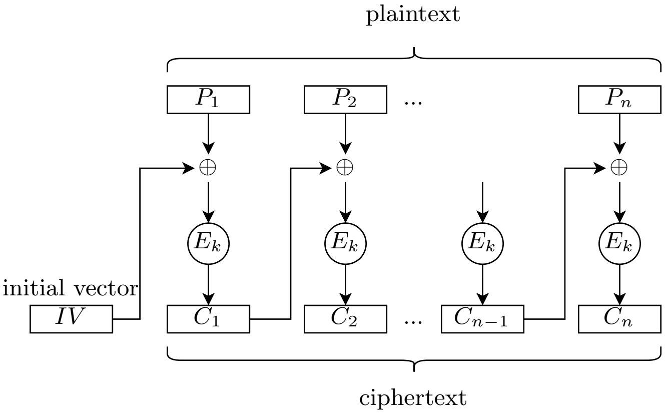

Figure 1: CBC encryptor

3. THREAT MODEL

4. DEMONSTRATION

5. PRACTICALITY AND DEFENSE

5.1 Praticality

While BEAST attacks are theoretically feasible, but through

6. REFERENCES

[1] C. Allen and T. Dierks. The TLS Protocol Version 1.0. RFC 2246, Jan. 1999.

APPENDIX

A. HEADINGS IN APPENDICES