Introduction

Researchers Karthikeyan Bhargavan and Gaëtan Leurent from INRIA (Institute for Research in Computer Science and Automation) in France had identified a new vulnerability that has been recognized by the CVE (Common Vulnerabilities and Exposures) as CVE-2016-2183. During this attack, known block cipher vulnerabilities are used against 64-bit block ciphers such as 3DES and Blowfish. These block ciphers can be found in software like OpenVPN, OpenSSL, Apache Server etc. While tackling, the attacker needs to detect a collision of an encrypted block of CBC (Cipher Block Chaining) data flow to be able to decrypt the traffic between the victim and the server. The researchers also came up with a BWAIN (Bug With An Impressive Name) Sweet32 as well as a logo:

![Sweet32 logo](image)

**Picture 1. Sweet32 Birthday attack logo.**

### Attack overview

There are two particular parts that the attackers use. One of them is the JavaScript program and another part is the attacker whose responsibility is to process the cipher text and recover the 16-byte secret data.

```javascript
var url = "https://10.0.0.1/index.html";
var xhr = new XMLHttpRequest;

// Expand URL to ~4kB using a query string
// Alternatively, force a large cookie
url += '?';
var x = 10000000;
for (var i=0; i<=500; i++) {
    url += x++;
}
while(true) {
    xhr.open(\"HEAD\", url, false);
    xhr.withCredentials = true;
    xhr.send();
    xhr.abort();
}
```

**Code 1. JavaScript file worker.js.**

```html
<html>
<body>
<script>
var W = new Array;
for (var i=0; i<8; i++) {
    var x = new Worker("worker.js");
    W.push(x);
}
</script>
</body>
</html>
```

**Code 2. HTML file attack.html.**

---

4. [https://sweet32.info](https://sweet32.info)
The 3DES is the only cipher that is used in the SSL/TLS (Secure Sockets Layer/Transport Layer Security) protocol with a block in size of 64 bits. The attack is executed by MITM (Man-in-the-middle) tracing a large amount of communication between the server and the victim. Attackers usually use JavaScript based files that are used to exploit Sweet32. For the attack to be successfully ran on 64-bit block ciphers, at least 32GB of data needs to be collected. Since during every new session an original symmetric key is generated, the data should be acquired from a single SSL/TLS session.\(^5\)

This is one of the techniques attackers can use to utilize Sweet32. The technique is part of BEAST attack. BEAST (Browser Exploit Against SSL/TLS) is a utility that is used to exploit a weakness in SSL/TLS protocol.\(^6\)

Another way of using the BEAST utility is to force the victim to visit a malicious website of the attacker’s choice, which will then deploy a JavaScript on a victim’s browser. The script will then decrypt the HTTPS-protected session cookies assigned from the website running TLS version 1.0. After decrypting the cookies, the script can send gathered data to any website selected by the attacker.\(^7\)

The HTML code above uses the JavaScript code to issue `XMLHttpRequests` using the `withCredentials` property to make sure that cookies are sent in the cross-origin request.\(^4\)

When these attacks become successful, the attackers can get ahold of information such as passwords, credit card numbers, personal details etc., which may be later leveraged against them. To ensure his safety, the victim should scan his network to see if it is vulnerable to BEAST attacks at: https://www.ssllabs.com/index.html.\(^7\)

### Solution

There are multiple ways to avoid the attack, however the most significant step to take is to configure web servers and VPNs to use AES (Advanced Encryption Standard) with 128-bit blocks instead of the 64-bit block ciphers and server. Servers that are using OpenSSL with AES-128 and AES-268 cipher suites, should not disable them.\(^5\)

Overall, web servers that support AES but prefer to use 3DES, should use 3DES as a fallback-only cipher to avoid any further problems. Since the attackers need to collect lots of data during one session, the TLS libraries and applications should limit the length of a 64-bit cipher TLS sessions. This could be easily done by just closing the connection and starting a new one.\(^4\)

---

\(^5\) https://access.redhat.com/articles/2548661
\(^6\) https://blogs.akamai.com/2012/05/what-you-need-to-know-about-beast.html
\(^7\) http://resources.infosecinstitute.com/beast-vs-crime-attack/#gref
Attacks that use BEAST utility have a workaround. First of all, the user should open The Local Group Policy Editor, which can be done by entering “gpedit.msc” into command line. A window, shown in picture 2, should appear after that. The user should then open “Computer Configuration” → “Administrative Templates” → “Network” and then click on the “SSL Configuration Settings” as shown below.

After opening the editor, under SSL Configuration Settings, choose “SSL Cipher Suite Order” and click on it. A window should pop up as shown below in picture 3.
The cipher suites named: TLS_RSA_WITH_RC4_128_SHA and TLS_WITH_RC4_MD5 must be set to be first in line. By doing that, SSL will use these cipher suites in the specific order.\textsuperscript{7}

In conclusion, I am of the opinion that the methods mentioned above are very efficient in avoiding the attack. Short block ciphers are well-known to be vulnerable to birthday attacks, even if the attacks are not against the block cipher itself. Sweet32 attack took less than two days to generate traffic. The researchers that found the vulnerability will try to raise the awareness of the short block ciphers and the safest way to use them.
Sources

4. https://sweet32.info
5. https://access.redhat.com/articles/2548661