

Padding Oracle in ASP.NET

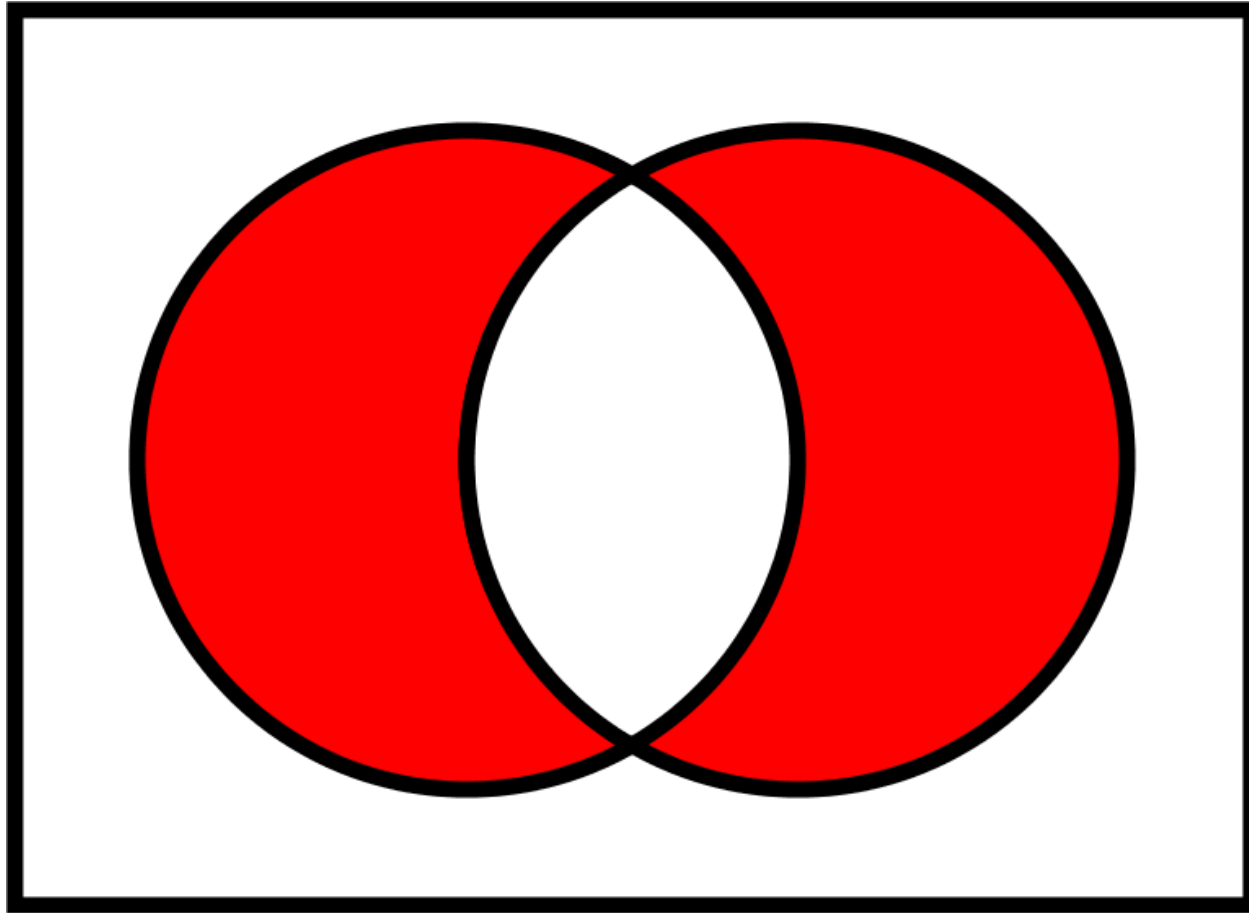
Caveat Emptor

- Exploit code is unreleased
- Observations based on Mono 2.8
 - Open source .NET implementation
 - Close to 100% .NET 2.0 compatible
- Not a professional cryptographer

Things to cover

- Refresher
 - XOR
 - Cipher block chaining
 - Padding
- New Information
 - Oracles in crypto
 - How ASP.NET uses crypto
 - Web.config
- Attack
 - Demo Video
 - Explanation
- Mitigation
 - Prevention
 - Microsoft's recommendations
 - Patch

XOR



XOR

$$A \oplus 0 = A$$

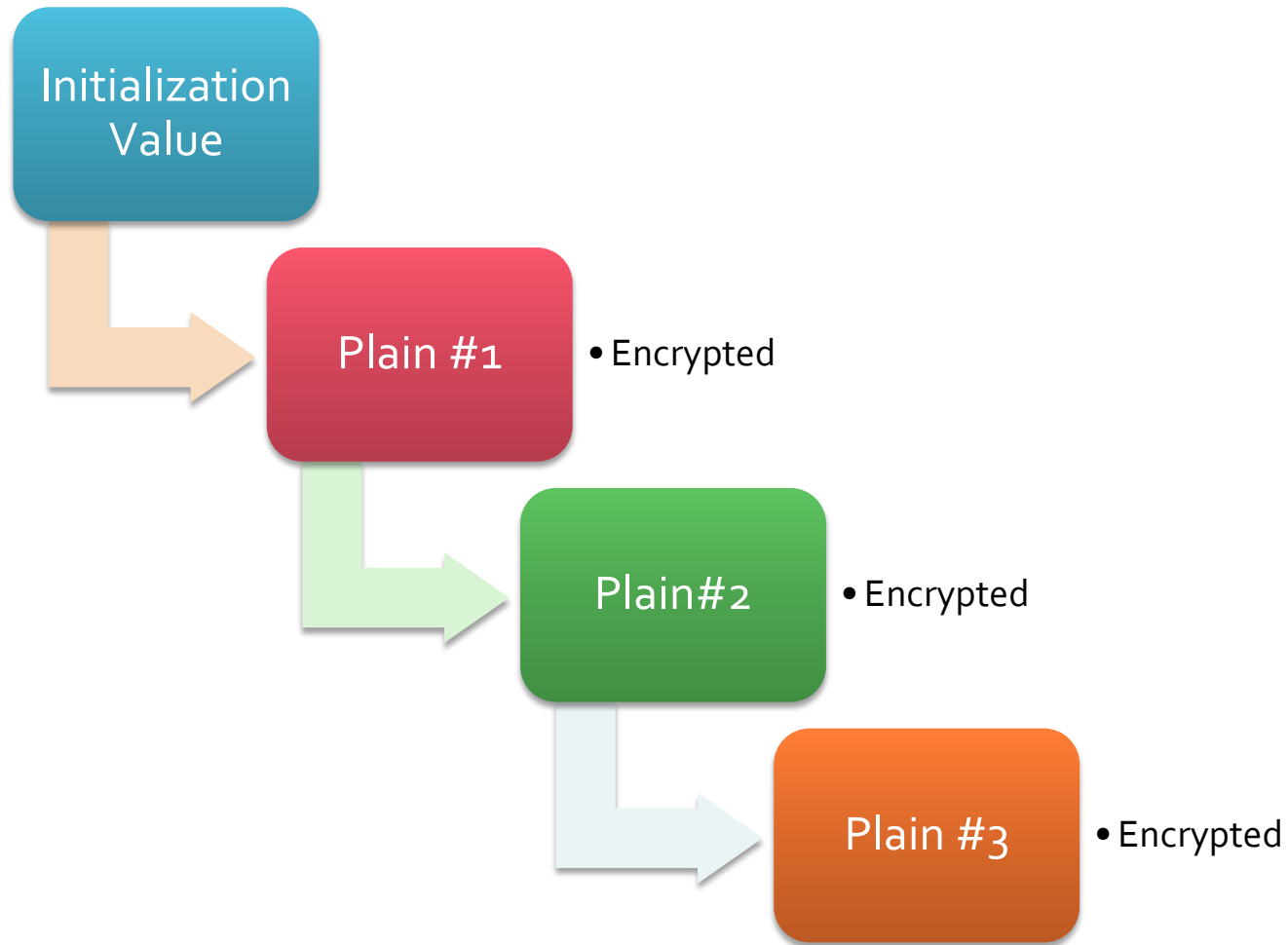
$$A \oplus A = 0$$

$$A \oplus B = C$$

$$C \oplus B = A$$

$$C \oplus A = B$$

Cipher Block Chaining

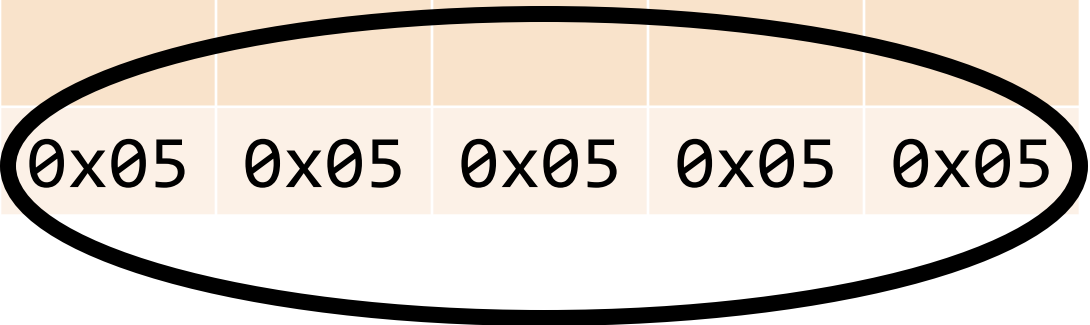


Padding

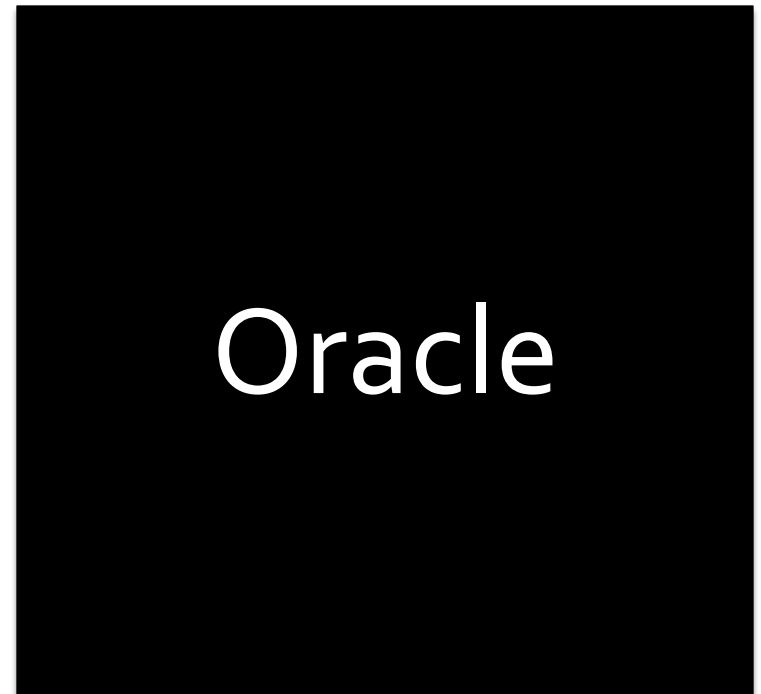
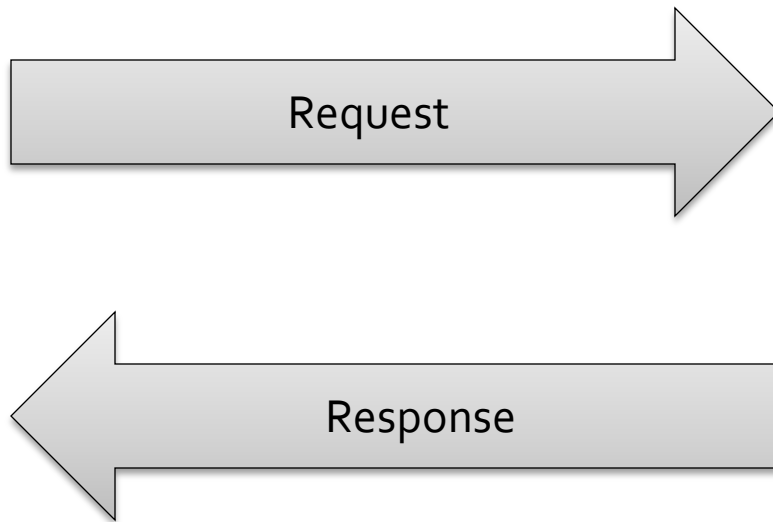
H	e	l	l	o		W	o
0x48	0x65	0x6C	0x6C	0x6F	0x20	0x57	0x6F
r	l	d					
0x72	0x6C	0x64	0x05	0x05	0x05	0x05	0x05

Padding

H	e	l	l	o		W	o
0x48	0x65	0x6C	0x6C	0x6F	0x20	0x57	0x6F
r	l	d					
0x72	0x6C	0x64	0x05	0x05	0x05	0x05	0x05



Oracles in crypto



Padding Oracle



Oracle

Padding Oracle



Oracle

How ASP.NET uses crypto

- ViewState
 - Not encrypted by default
 - Optionally encrypted and signed
- Authentication Cookies
 - Encrypted and signed by default
- WebResource
 - Encryption only no signing
 - Serves embedded resources
- ScriptResource
 - Encryption only no signing
 - Serves combined JavaScript files off the filesystem

Web.config

- XML configuration file
- Sits in root of application
- Contains:
 - Database connection strings
 - Encryption keys
 - Validation keys
- IIS blocks *.config from being served

Demo

- http://www.youtube.com/watch?v=yghiC_U2RaM

Padding

H	e	l	l	o		W	o
0x48	0x65	0x6C	0x6C	0x6F	0x20	0x57	0x6F
r	l	d					
0x72	0x6C	0x64	0x05	0x05	0x05	0x05	0x05

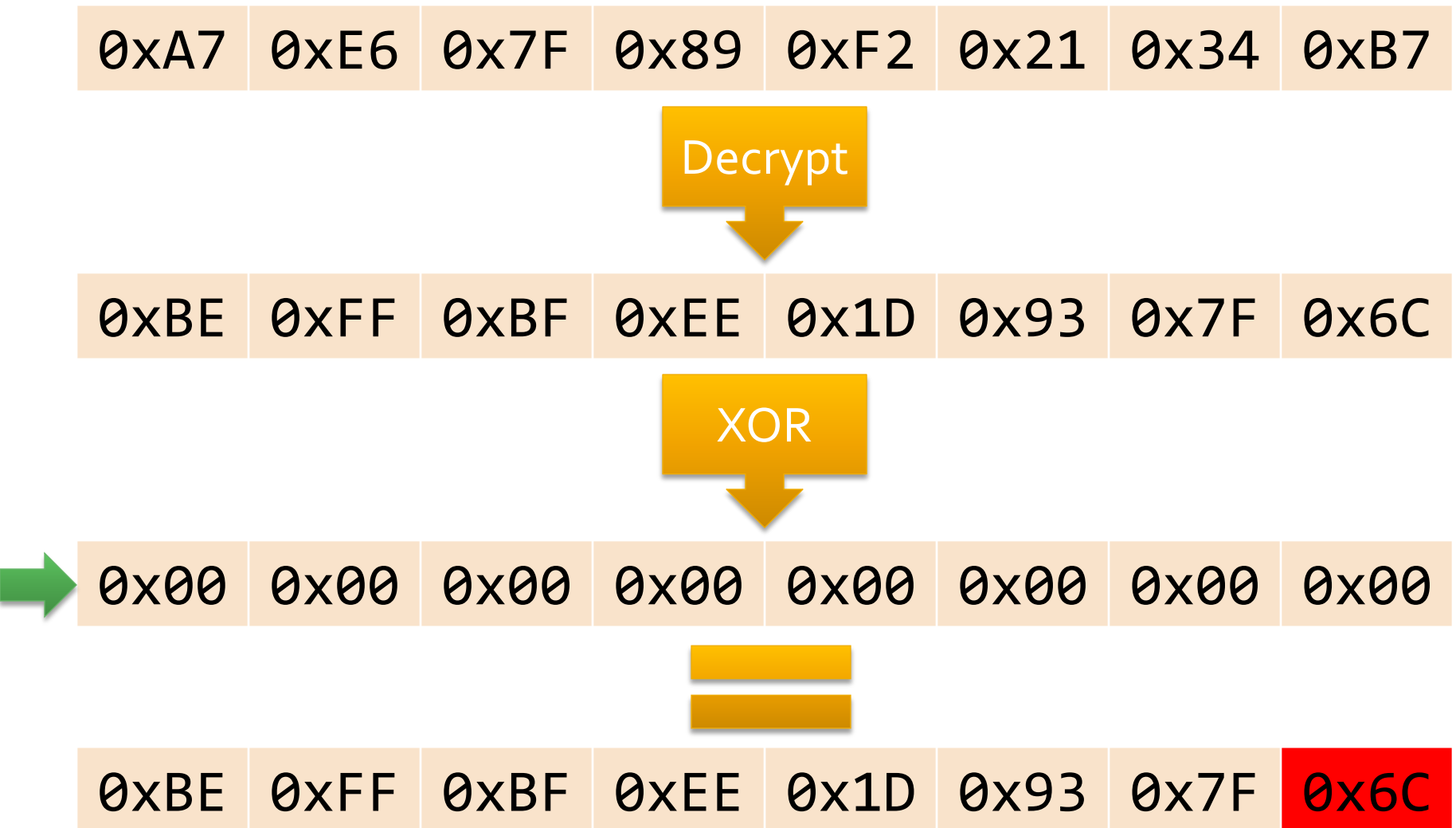
Intercepted

0x80	0x11	0x48	0x08	0x8B	0xEE	0x4E	0xF8
0xCC	0x93	0xDB	0xEB	0x18	0x96	0x7A	0x69
0xA7	0xE6	0x7F	0x89	0xF2	0x21	0x34	0xB7

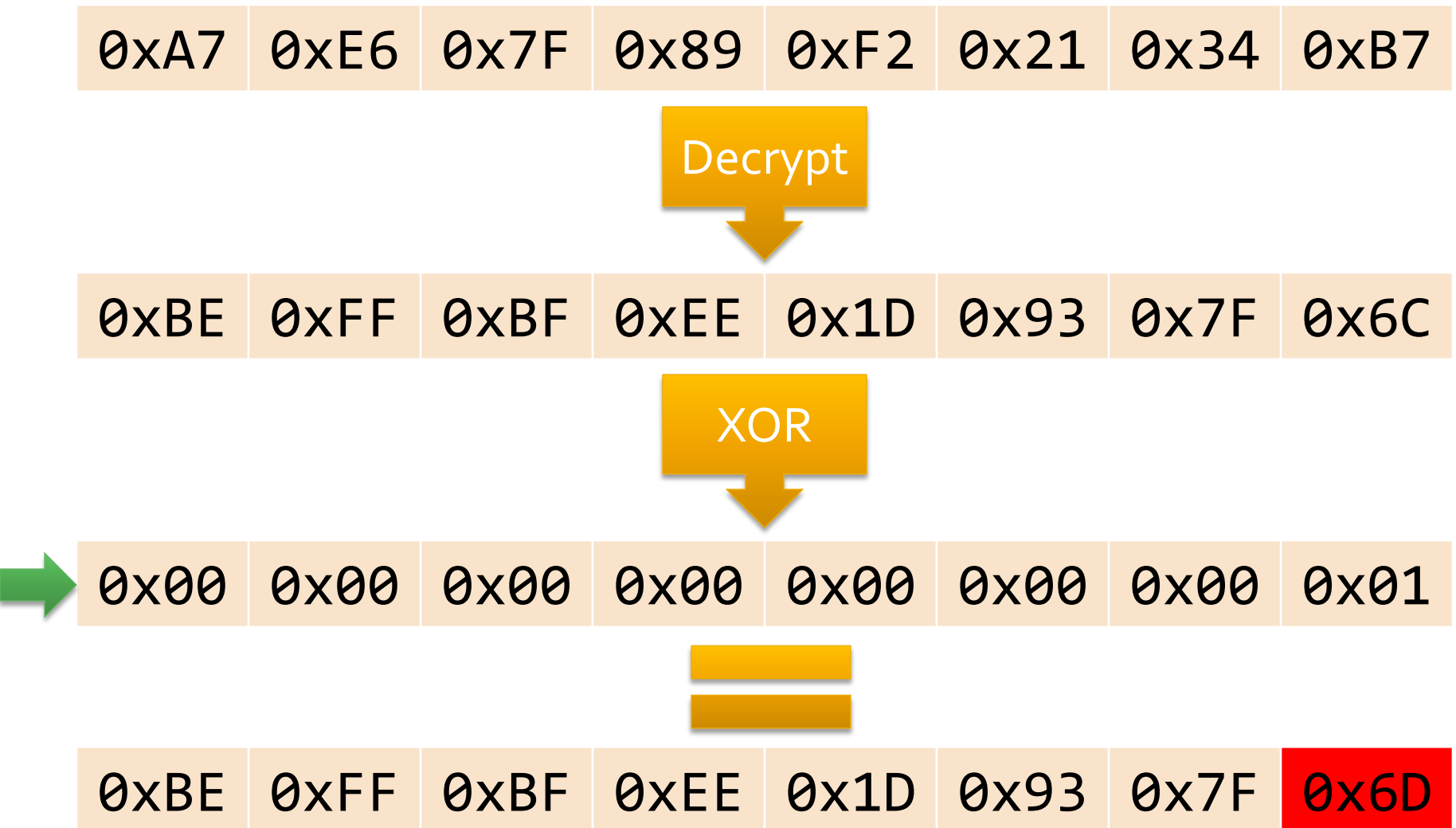
Request

0x80	0x11	0x48	0x08	0x8B	0xEE	0x4E	0xF8
0x00	0x00	0x00	0x00	0x00	0x00	0x00	0x00
0xA7	0xE6	0x7F	0x89	0xF2	0x21	0x34	0xB7

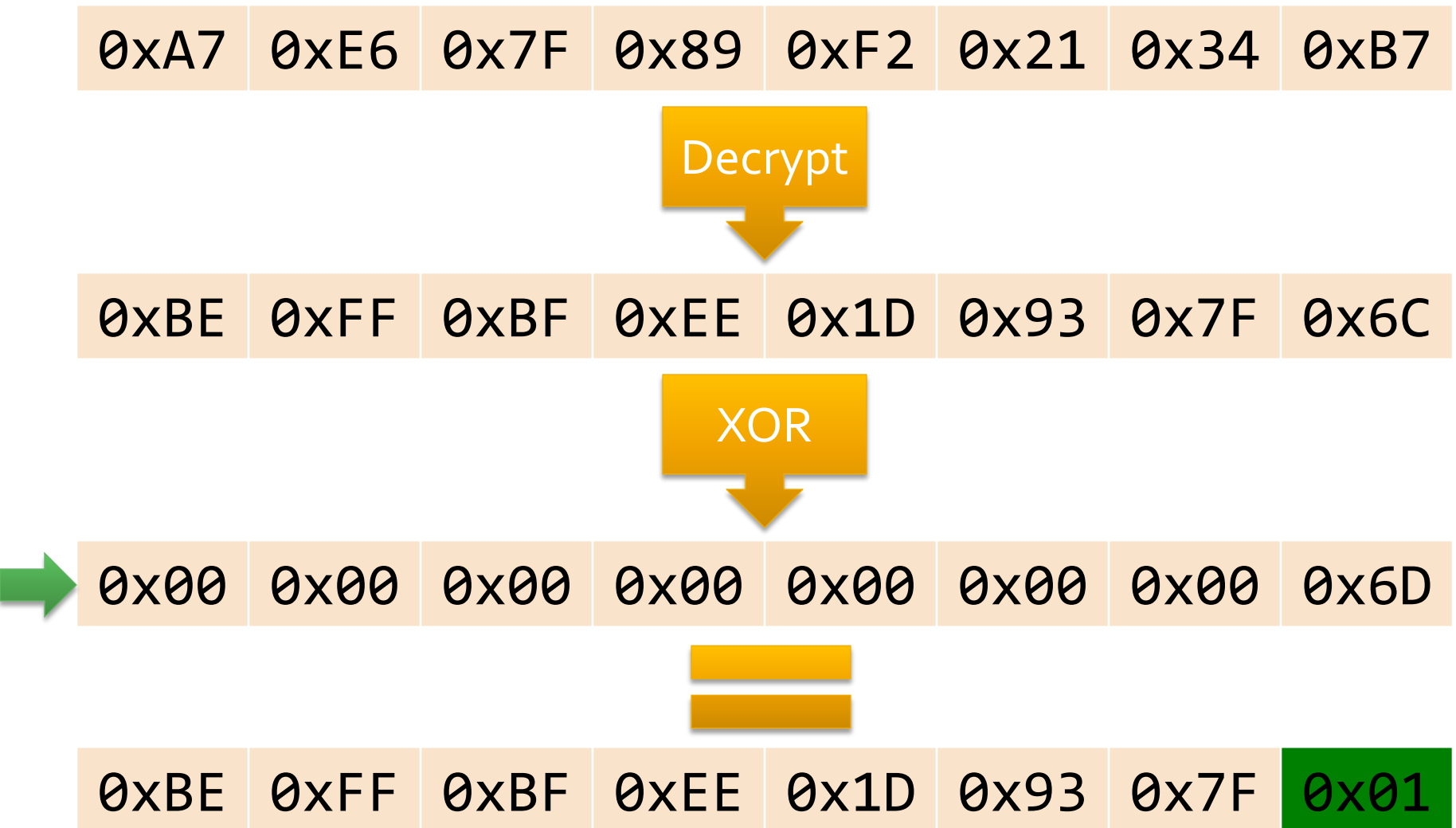
Padding Oracle



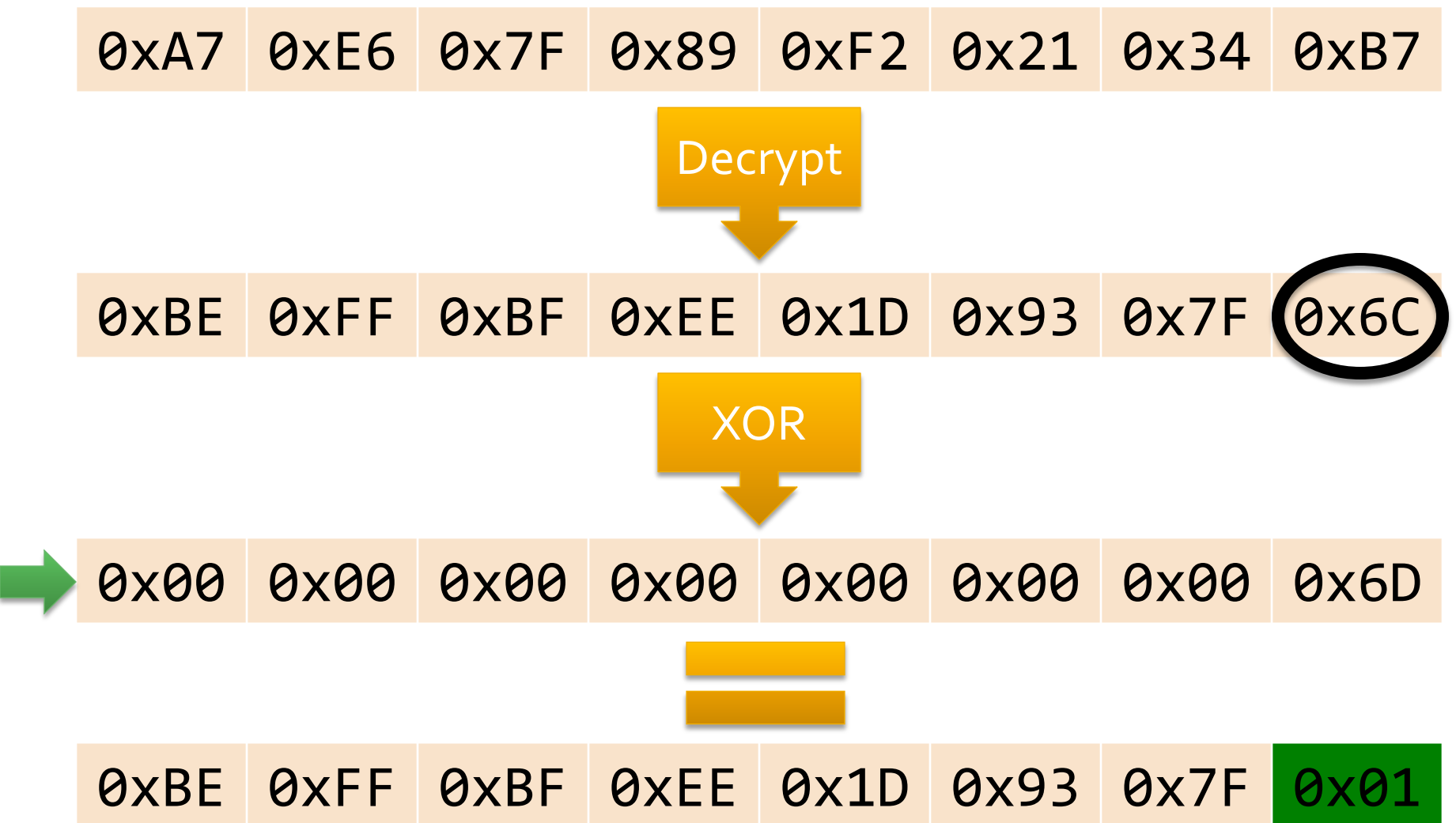
Padding Oracle



Padding Oracle



Padding Oracle



Padding Oracle

$$0x6D \oplus 0x01 = 0x6C$$

Padding Oracle

0x80	0x11	0x48	0x08	0x8B	0xEE	0x4E	0xF8
0xCC	0x93	0xDB	0xEB	0x18	0x96	0x7A	0x69
0xA7	0xE6	0x7F	0x89	0xF2	0x21	0x34	0xB7

Padding Oracle

$$0x6C \oplus 0x69 = 0x05$$

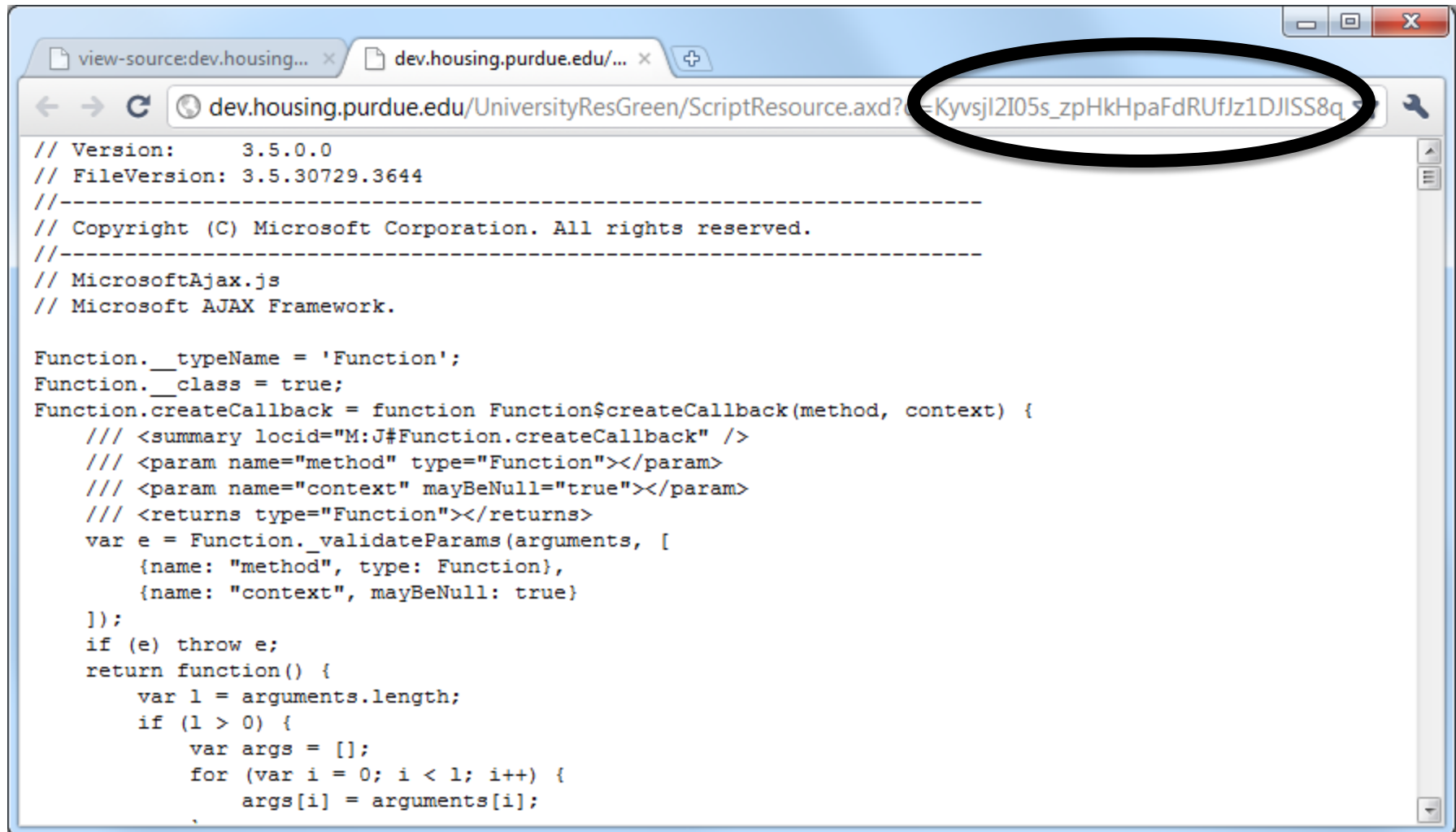
Matches Plaintext

H	e	l	l	o		W	o
0x48	0x65	0x6C	0x6C	0x6F	0x20	0x57	0x6F
r	l	d					
0x72	0x6C	0x64	0x05	0x05	0x05	0x05	0x05

How ASP.NET uses crypto

- ViewState
 - Not encrypted by default
 - Optionally encrypted and signed
- Authentication Cookies
 - Encrypted and signed by default
- WebResource
 - **Encryption only no signing**
 - Serves embedded resources
- ScriptResource
 - **Encryption only no signing**
 - **Serves combined JavaScript files off the filesystem**

ScriptResource.axd



```
// Version:      3.5.0.0
// FileVersion:  3.5.30729.3644
//-----
// Copyright (C) Microsoft Corporation. All rights reserved.
//-----
// MicrosoftAjax.js
// Microsoft AJAX Framework.

Function.__typeName = 'Function';
Function.__class = true;
Function.createCallback = function Function$createCallback(method, context) {
    /// <summary locid="M:J#Function.createCallback" />
    /// <param name="method" type="Function"></param>
    /// <param name="context" mayBeNull="true"></param>
    /// <returns type="Function"></returns>
    var e = Function._validateParams(arguments, [
        {name: "method", type: Function},
        {name: "context", mayBeNull: true}
    ]);
    if (e) throw e;
    return function() {
        var l = arguments.length;
        if (l > 0) {
            var args = [];
            for (var i = 0; i < l; i++) {
                args[i] = arguments[i];
            }
        }
    };
}
```

ScriptResource.axd

Kyvsjl2lo5s_zpHkHpaFdRUf
Jz1DJlSS8qjN...

ScriptResource.axd

FileA.js;FileB.js;FileC.js

ScriptResource.axd

FileA.js;web.config;FileC.js

Encryption Oracle

- Newish technique called CBC-R
 - Turns a padding oracle into an encryption oracle
- Encrypt any plaintext
- Best case if you control IV
 - First block will be garbage otherwise
- ScriptResource has a fixed IV
 - Tactics to work around the issue

Keys to the kingdom

Cookie: User=Administrator

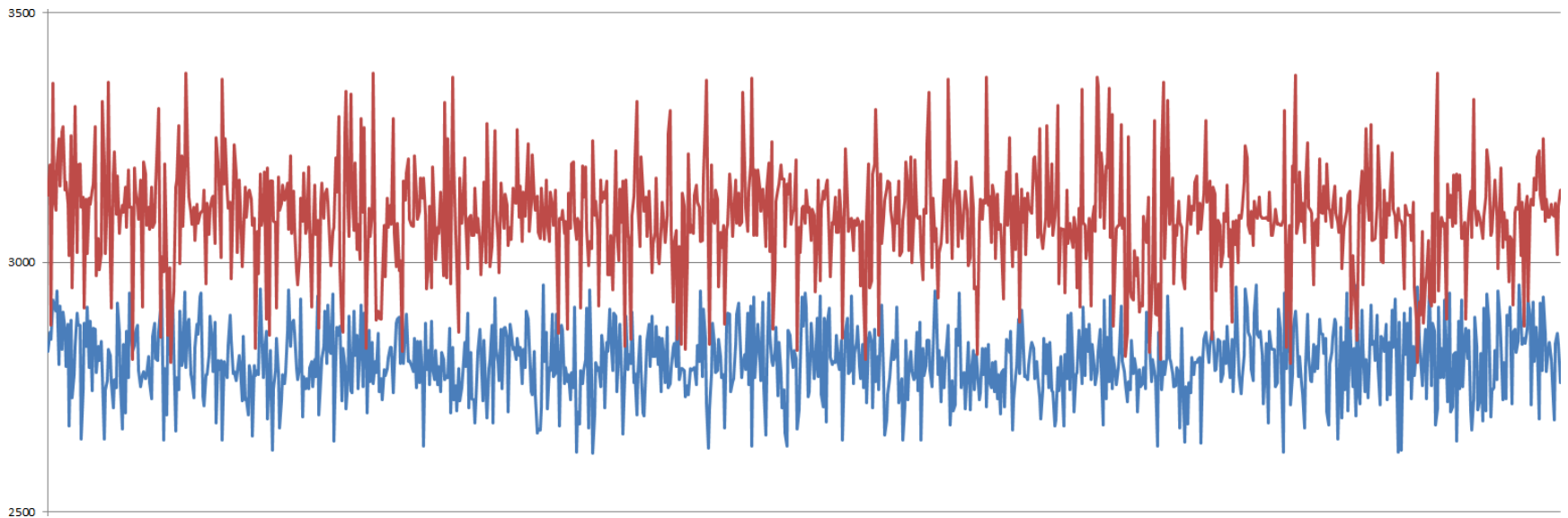
Prevention

- Authenticate before decryption
 - Prevents padding oracle
 - Microsoft did authenticate in some case
 - Only after decryption though
 - Can't create an encryption oracle

Microsoft's recommendations

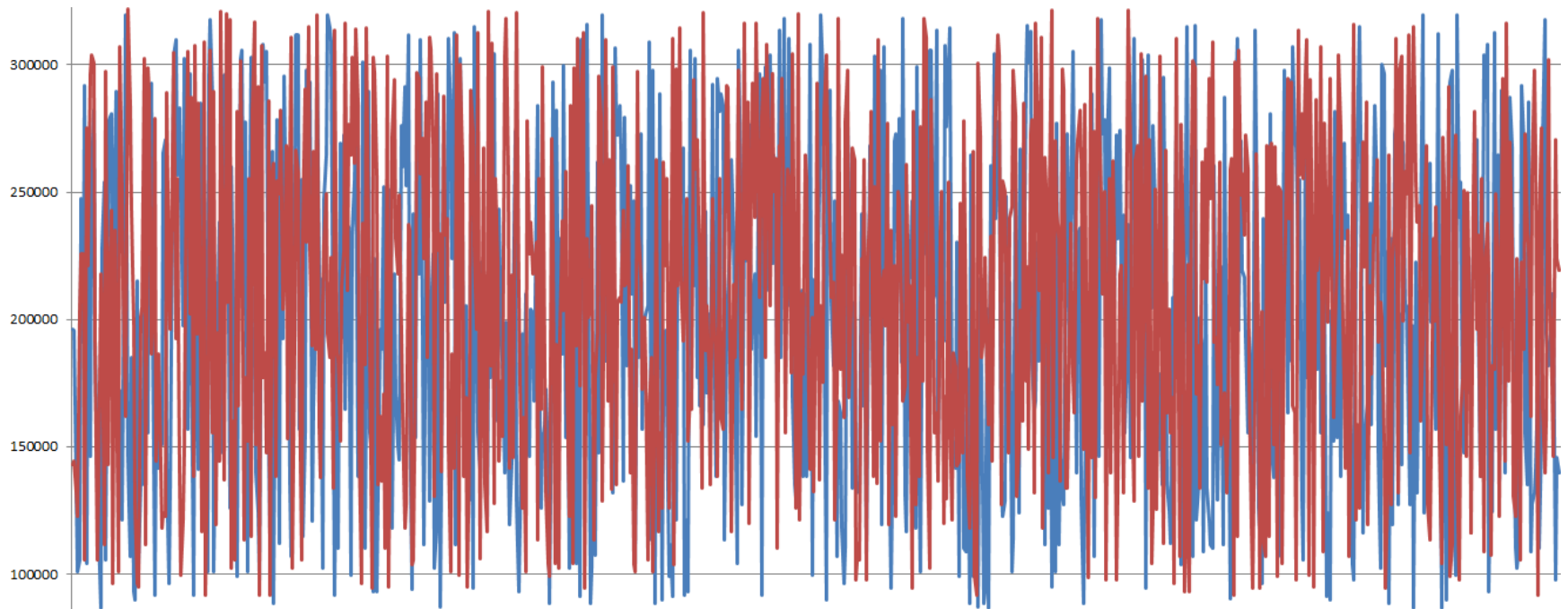
- Forced rewrite on error
 - Ever response becomes 200 OK
 - Remove custom 500 and 404 responses
- Add random sleep to error page
 - 0-255 ms random sleep

Without Random Sleep



Source: <http://www.troyhunt.com/2010/09/why-sleep-is-good-for-your-apps-padding.html>

With Random Sleep



Source: <http://www.troyhunt.com/2010/09/why-sleep-is-good-for-your-apps-padding.html>

Patch!

Resources

- Patch
 - <http://www.microsoft.com/technet/security/bulletin/ms10-070.msp>
- Announcements
 - <http://weblogs.asp.net/scottgu/archive/2010/09/18/important-asp-net-security-vulnerability.aspx>
 - <http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3332>
- Slides
 - <http://netifera.com/research/poet/PaddingOraclesEverywhereEkoparty2010.pdf>
- Papers
 - https://media.blackhat.com/bh-eu-10/whitepapers/Duong_Rizzo/BlackHat-EU-2010-Duong-Rizzo-Padding-Oracle-wp.pdf
- Blog Posts
 - <http://www.troyhunt.com/2010/09/fear-uncertainty-and-and-padding-oracle.html>
 - <http://www.troyhunt.com/2010/09/why-sleep-is-good-for-your-apps-padding.html>
 - <http://www.gdssecurity.com/l/b/2010/09/14/automated-padding-oracle-attacks-with-padbuster/>
- Open Source .NET implementation
 - <http://mono-project.org>