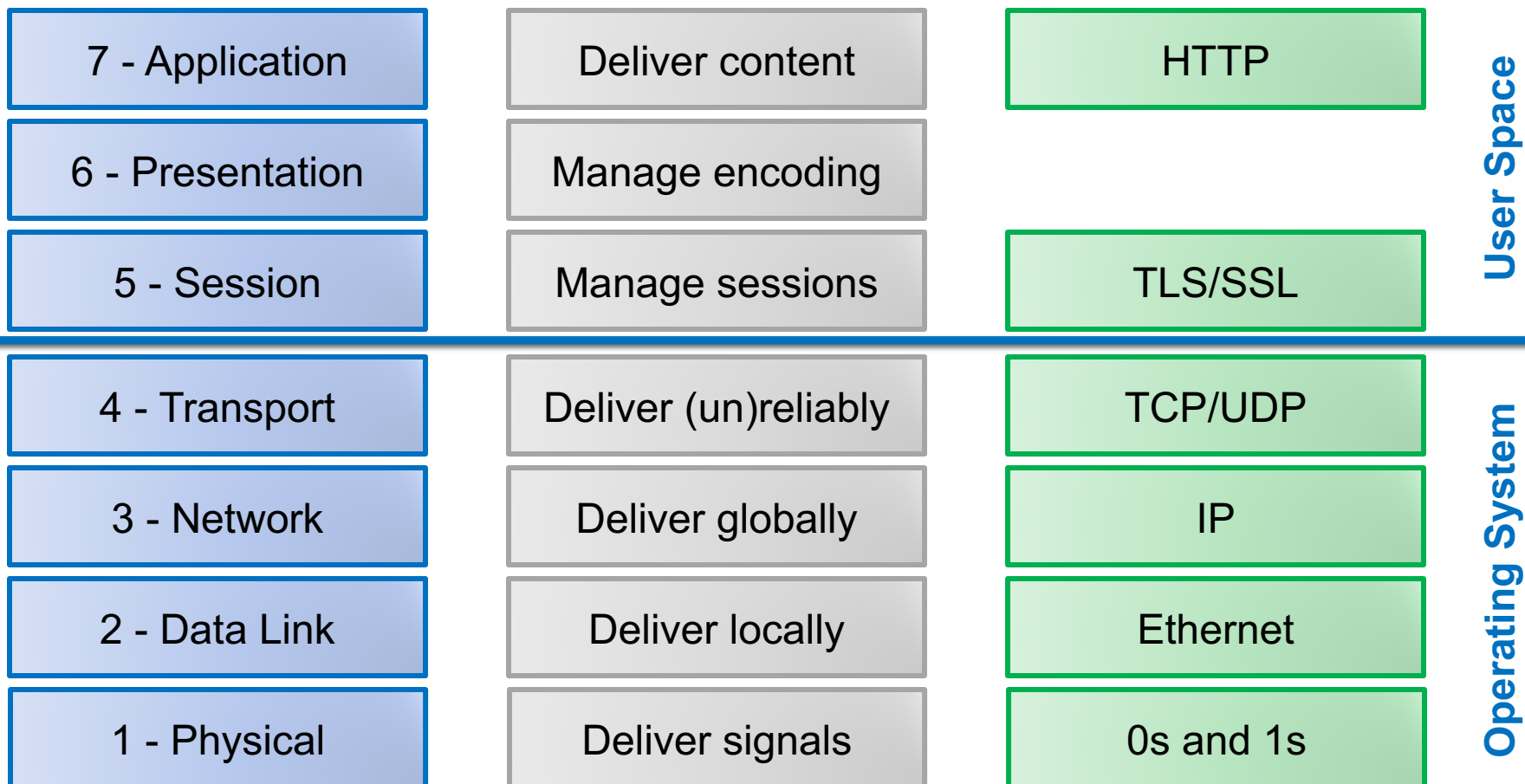


Lecture 23: Web Security

CS 181S

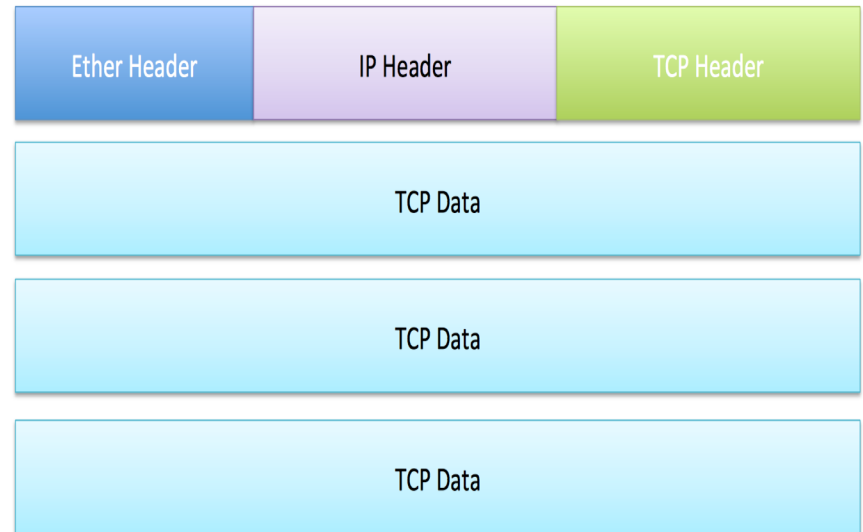
December 5, 2018

Networking Stack



OS Layers

- Layer 1: Physical
- Layer 2: Data Link
- Layer 3: Network
- Layer 4: Transport



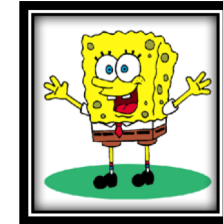
SSL/TLS Handshake



Version, cipher suites, rClient

Enc_pks(ms_p)

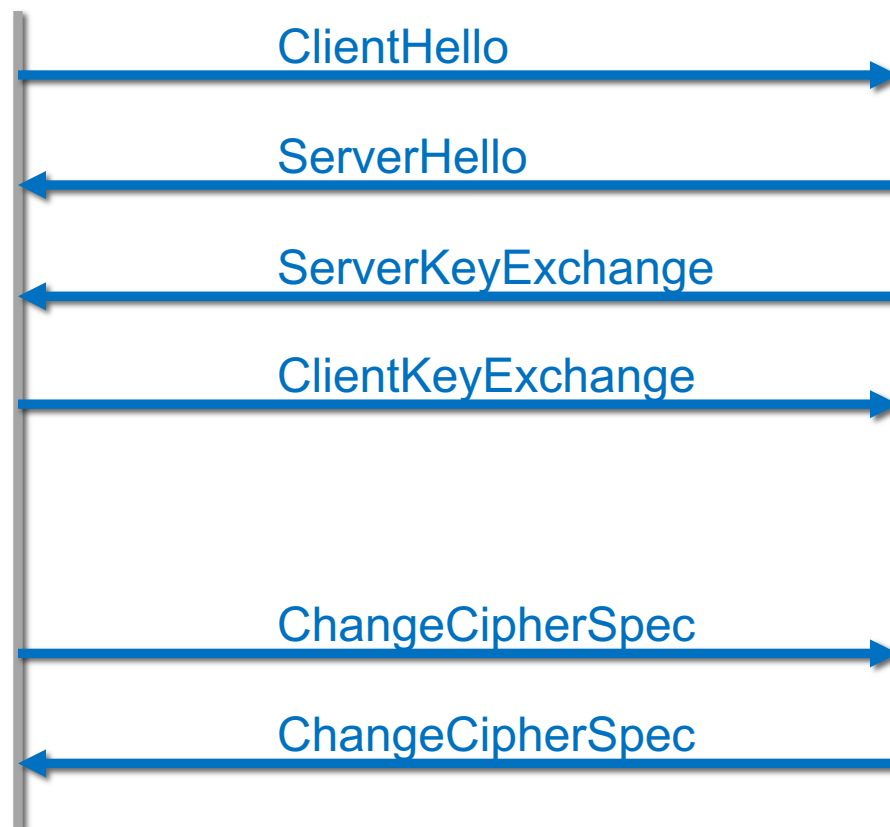
Compute master secret



Version, cipher suite, rServer, certificate

(optional)

Compute master secret



TLS record

+	Byte +0	Byte +1	Byte +2	Byte +3
Byte 0	Content type			
Bytes 1..4	Version		Length	
	<i>(Major)</i>	<i>(Minor)</i>	<i>(bits 15..8)</i>	<i>(bits 7..0)</i>
Bytes 5..(<i>m</i> -1)	Protocol message(s)			
Bytes <i>m</i> ..(<i>p</i> -1)	MAC (optional)			
Bytes <i>p</i> ..(<i>q</i> -1)	Padding (block ciphers only)			

Hex	Dec	Type
0x14	20	ChangeCipherSpec
0x15	21	Alert
0x16	22	Handshake
0x17	23	Application
0x18	24	Heartbeat

Application Layer: HTTP

- Hypertext Transfer Protocol (HTTP) is an application protocol for distributed information systems
- Stateless request-response protocol
- Requests resources identified by Uniform Resource Locators (URLs)

Request	Response
GET	Retrieve resource (no side effects)
HEAD	Retrieve header for GET request (no body)
POST	Requests that server accept new object (e.g., results of form or new database item) and store it as subordinate of resource identified by URI
PUT	Requests that server store new object under supplied URI
DELETE	Delete specified resource

Example Request

- HTTP Request: Request Method Path Protocol Version

```
1 | GET / HTTP/1.1
2 | Host: developer.mozilla.org
3 | Accept-Language: fr
```

Headers

- HTTP Response:

```
1 | HTTP/1.1 200 OK
2 | Date: Sat, 09 Oct 2010 14:28:02 GMT
3 | Server: Apache
4 | Last-Modified: Tue, 01 Dec 2009 20:18:22 GMT
5 | ETag: "51142bc1-7449-479b075b2891b"
6 | Accept-Ranges: bytes
7 | Content-Length: 29769
8 | Content-Type: text/html
9 |
10 | <!DOCTYPE html... (here comes the 29769 bytes of the request
```

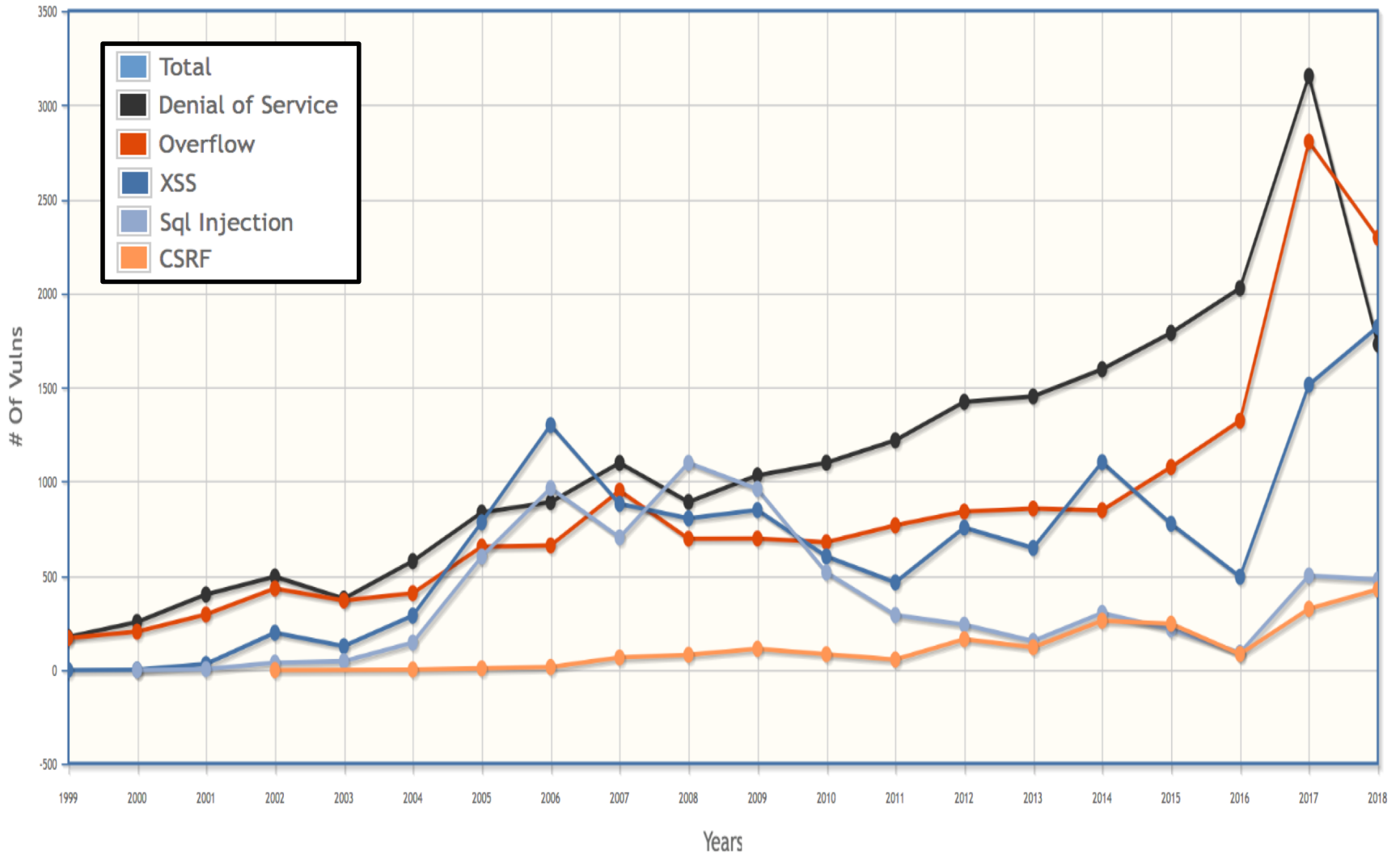
Header

Body

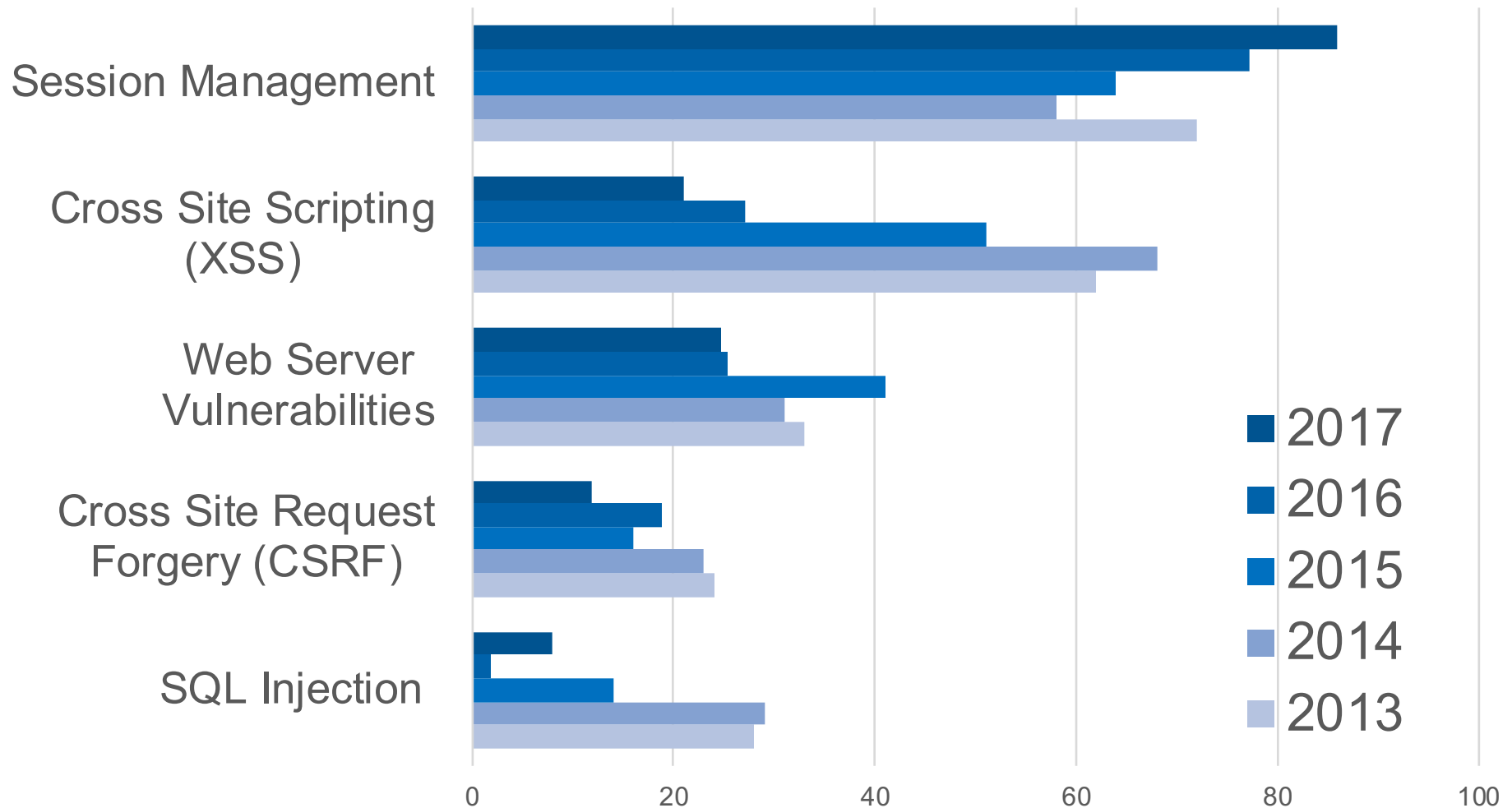
HTTP Response Codes

Code	Message
200	OK
201	Created
302	Found
401	Unauthorized
403	Forbidden
404	Not Found
409	Conflict
500	Internal Server Error
502	Bad Gateway

Vulnerabilities by Year



Vulnerability Occurrence in Applications



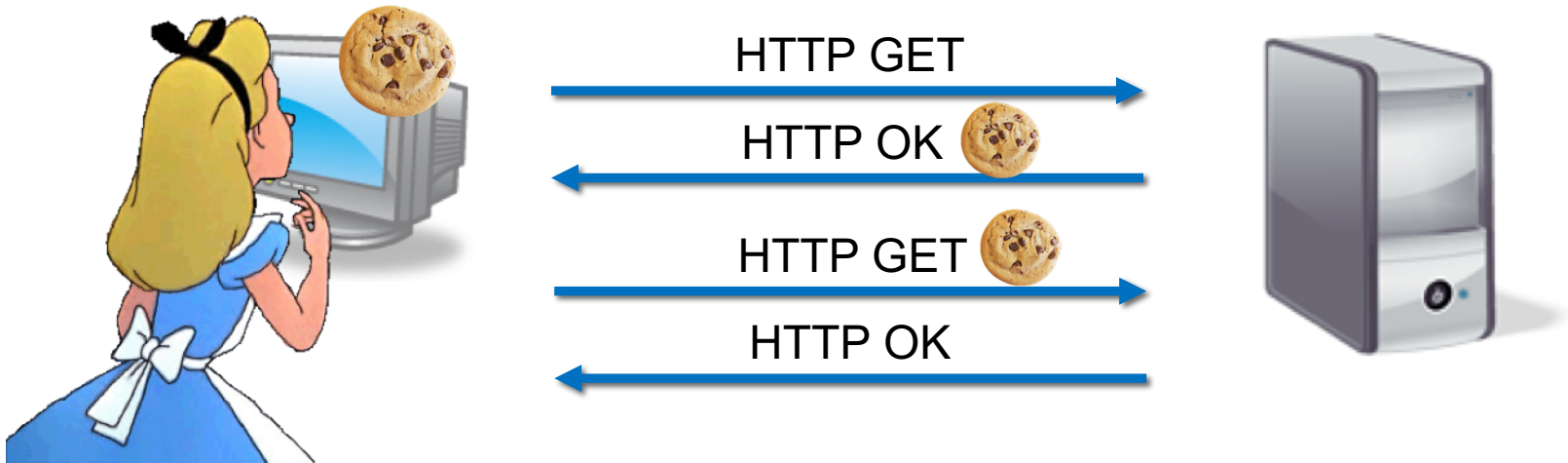
HTTP is stateless

```
GET /index.html HTTP/1.1  
Host: www.example.com
```



```
<head><title>An Example Page</title>  
</head>  
<body>  
  Hello World!  
</body>  
</html>
```

Session Management



Cookies

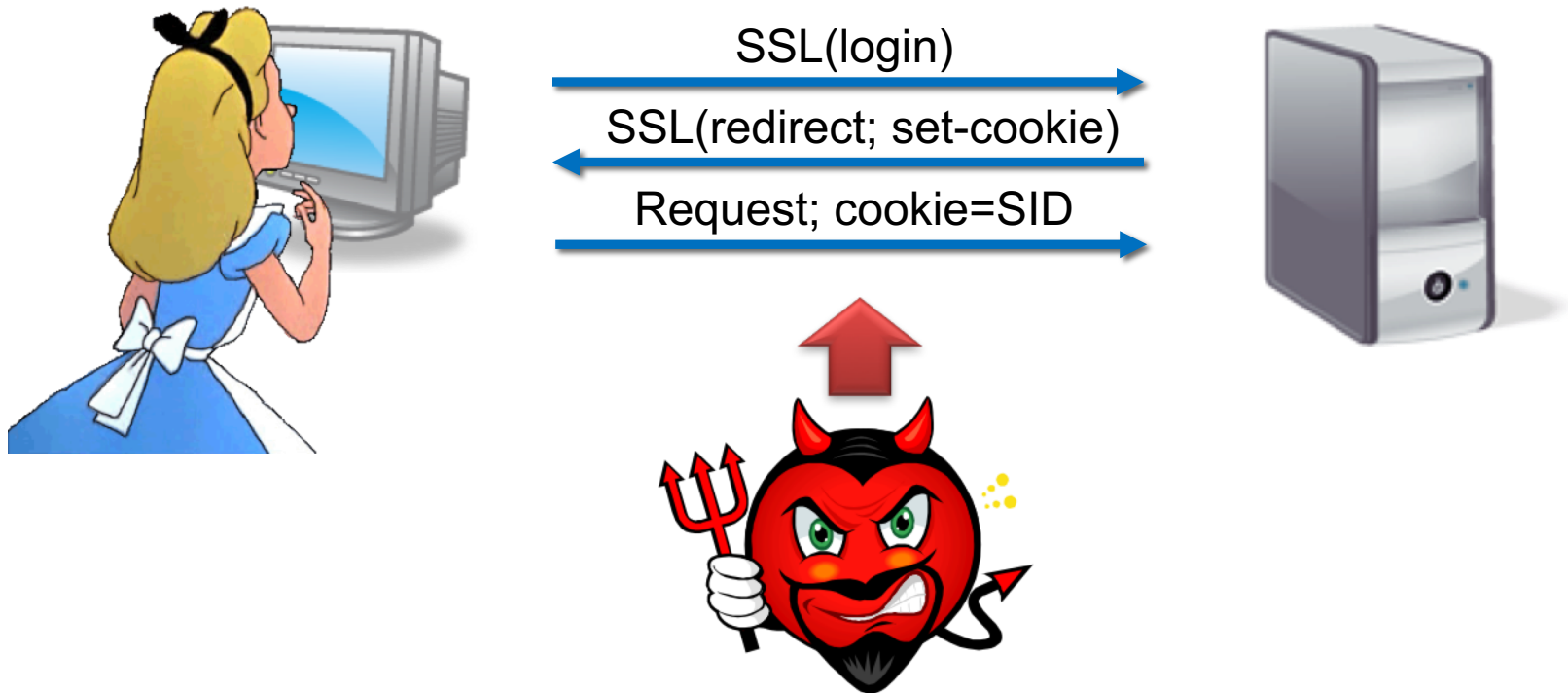
```
GET /index.html HTTP/1.1  
Host: www.example.org  
...
```

```
HTTP/1.0 200 OK  
Content-type: text/html  
Set-Cookie: theme=light  
Set-Cookie: sessionId=abc123; Expires=Wed, 09 Jun 2021 10:18:14 GMT  
...
```

Optional: path, domain

```
GET /spec.html HTTP/1.1  
Host: www.example.org  
Cookie: theme=light; sessionId=abc123  
...
```

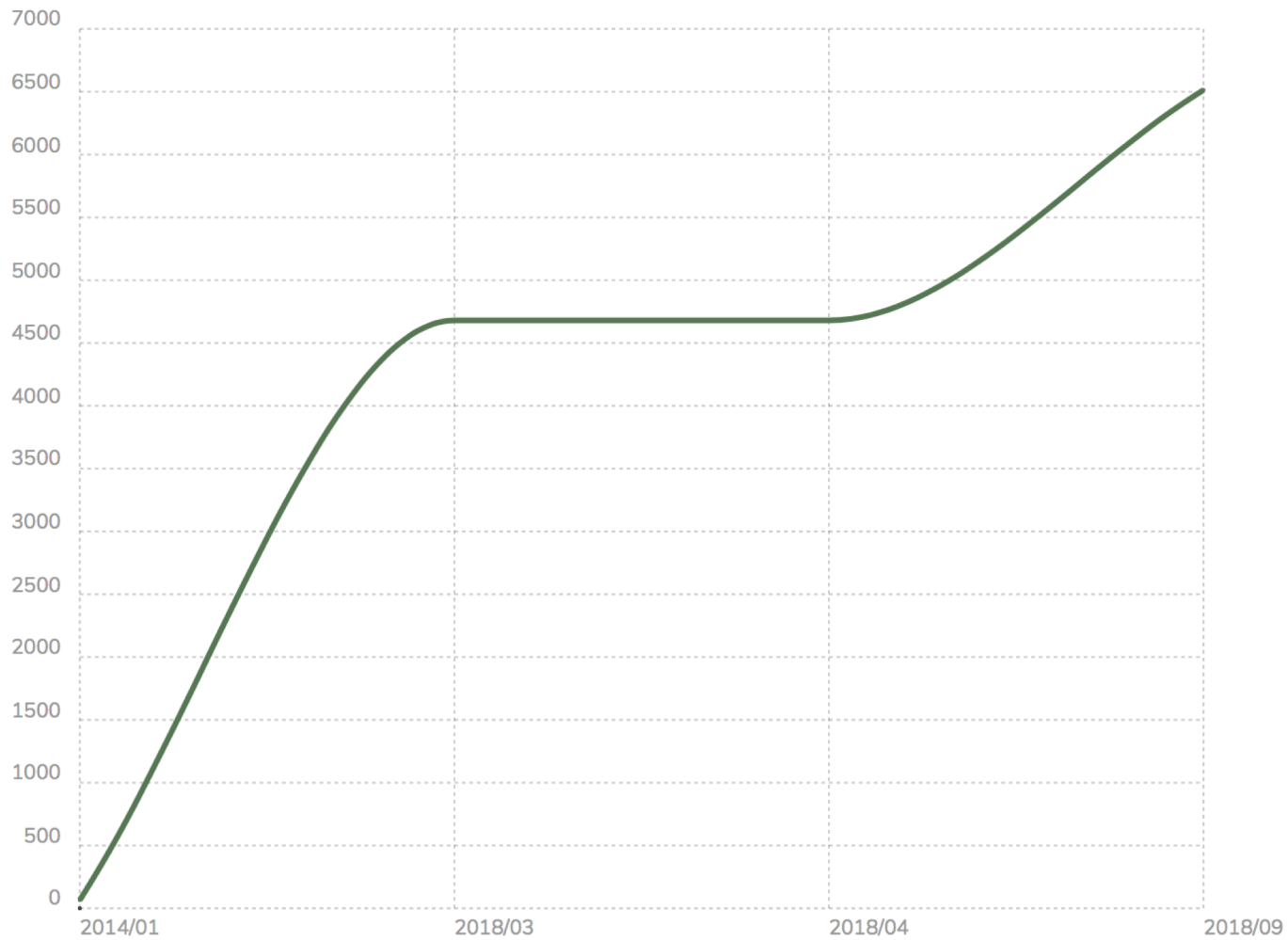
Cookie Side-jacking



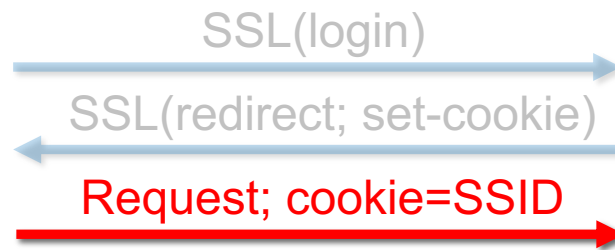
FireSheep (October 2010)



SSL by Default (top 10k)



Cookie Forgery



Cookie Forgery

YAHOO!


Cookie Theft

- Malware sometimes targets local browser state



facebook

Give us all your details we won't get hacked we promise

 Share photos and updates with hackers using View As

A screenshot of a web browser window. The address bar shows 'aol.net'. The page title is 'Relieve Stress Paint Tool'. The main content area features the 'RSP Relieve stress Paint' logo, a 'Download' button, and a large image of a child with colorful paint on their face and hands. Below the image is a green 'Download IT'S FREE' button.

Chrome Encrypted Cookies

- salt is 'saltysalt'
- key length is 16
- iv is 16 bytes of space b' ' * 16
- on Mac OSX:
 - password is in keychain: `security find-generic-password -w -s "Chrome Safe Storage"`
 - 1003 iterations
- on Chrome OS:
 - password is in keychain: `"security find-generic-password -wga Chrome"`
 - 1003 iterations
- on Linux:
 - password is peanuts
 - 1 iteration
- On Windows:
 - password is current user password
 - CryptProtectData uses 4000 iterations