OWASP London Chapter - 21st May 2009

HashCookies

A Simple Recipe

- Take a cookie
- Add some salt
- Add a sequence number

John Fitzpatrick

john.fitzpatrick@mwrinfosecurity.com

Full paper at http://labs.mwrinfosecurity.com

MWR InfoSecurity

Structure

- What are hashCookies
- Benefits
- How they work
- Outcomes

What are HashCookies

- They are cookies which are hashed with a random salt
- Prevent an intercepted session ID being useful to an attacker

What they are not

- They are not a means to secure data in transit. SSL does that.

Benefits

- Prevent an intercepted session ID being useful to an attacker
- Prevent session hijacking being feasible, whatever means are used to obtain the session.
- XSS, weak session IDs, session fixation, session IDs revealed through whatever means etc...

How they Work

They make use of 3 values

- Session ID
- Salt
- Sequence Number

How they Work

```
GET / HTTP/1.0
Host: www.mwrinfosecurity.com
User-Agent: Mozilla/7.0 (X11; U; Linux i986; en-GB; rv:1.9.0.3)
Accept: text/html,application/xml;q=0.9,*/*;q=0.8,hashCookie
Accept-Language: en-gb,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Proxy-Connection: keep-alive
```

How they Work

```
HTTP/1.1 200 OK
Date: Thu, 04 Dec 2008 17:37:29 GMT
Server: server
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0,
pre-check=0
Set-Cookie: SESSION=cb58609ecb4b8f5b4fd1235c7bd60aeb;
salt=ea043ecb41517205154ddf8c658b6d0961c17fe3; path=/;
Pragma: no-cache
Content-Length: 4347
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html
```

How they Work

HashCookie = sha1(currentSessionID-salt-sequenceNumber)

```
Set-Cookie: SESSION=cb58609ecb4b8f5b4fd1235c7bd60aeb;
salt=ea043ecb41517205154ddf8c658b6d0961c17fe3;
```

HashCookie = sha1(
cb58609ecb4b8f5b4fd1235c7bd60aeb-
ea043ecb41517205154ddf8c658b6d0961c17fe3-
1)

= a29befed094761ea3dfa9e9de164b5fdfbc7d6a9

How they Work

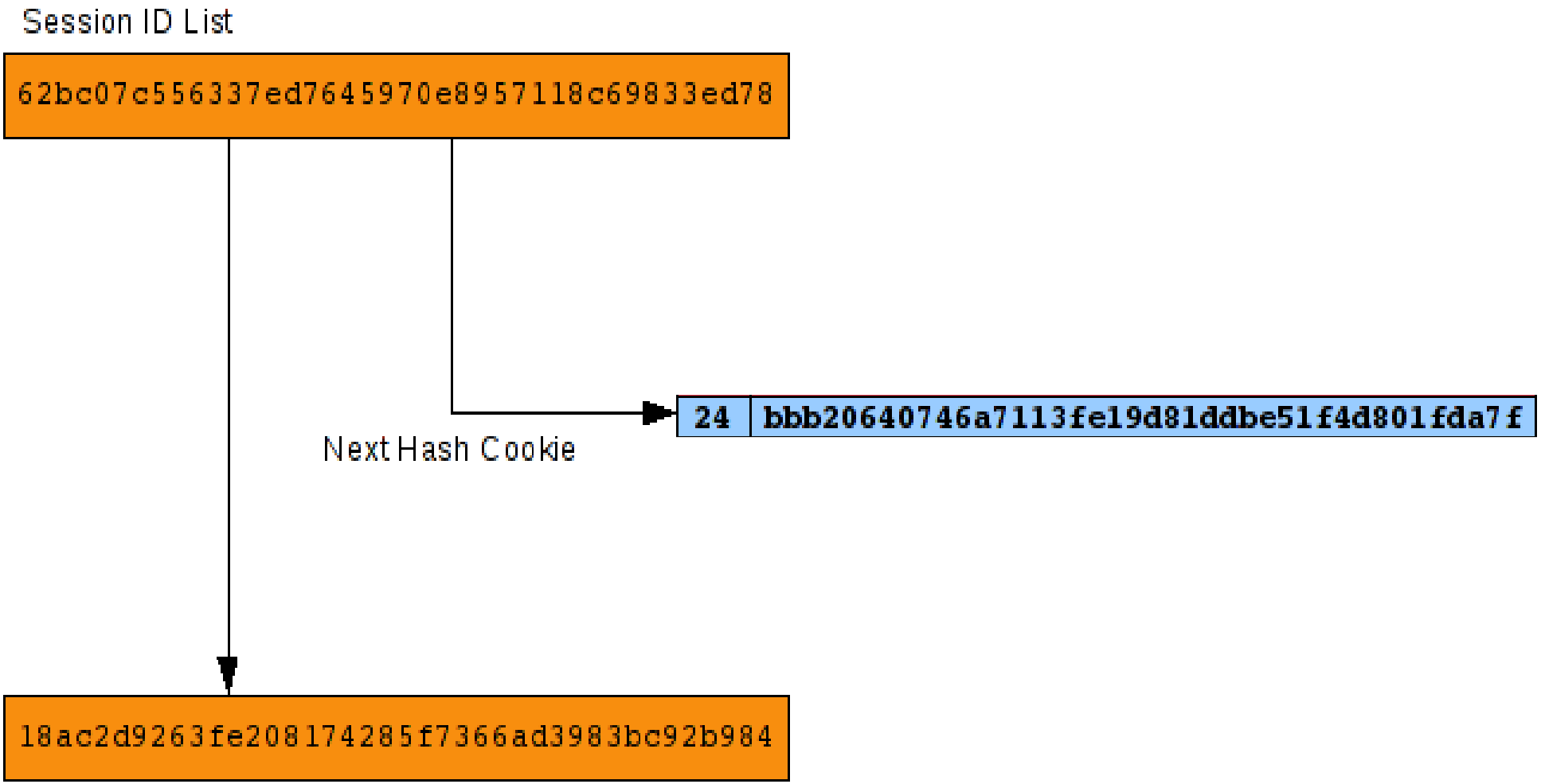
```
GET /nextPage.mwr HTTP/1.0
Host: www.mwrinfosecurity.com
User-Agent: Mozilla/7.0 (X11; U; Linux i986; en-GB; rv:1.9.0.3)
Accept: text/html,application/xml;q=0.9,*/*;q=0.8,hash-cookie
Accept-Language: en-gb,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Proxy-Connection: keep-alive
Cookie: SESSION=cb58609ecb4b8f5b4fd1235c7bd60aeb-
a29befed094761ea3dfa9e9de164b5fdfbc7d6a9-1
```

- Pass the session ID and sequence number up with request too – they form the cookie

How they Work

- Request to server
- Hash cookie valid?
- Y: Honour request
- N: Do not honour request

How they Work




```
HashCookie = sha1(currentSessionID-salt-sequenceNumber)

Cookie = SessionID-HashCookie-sequenceNumber
```

How they Work

- Out of order requests
- Multi Threading

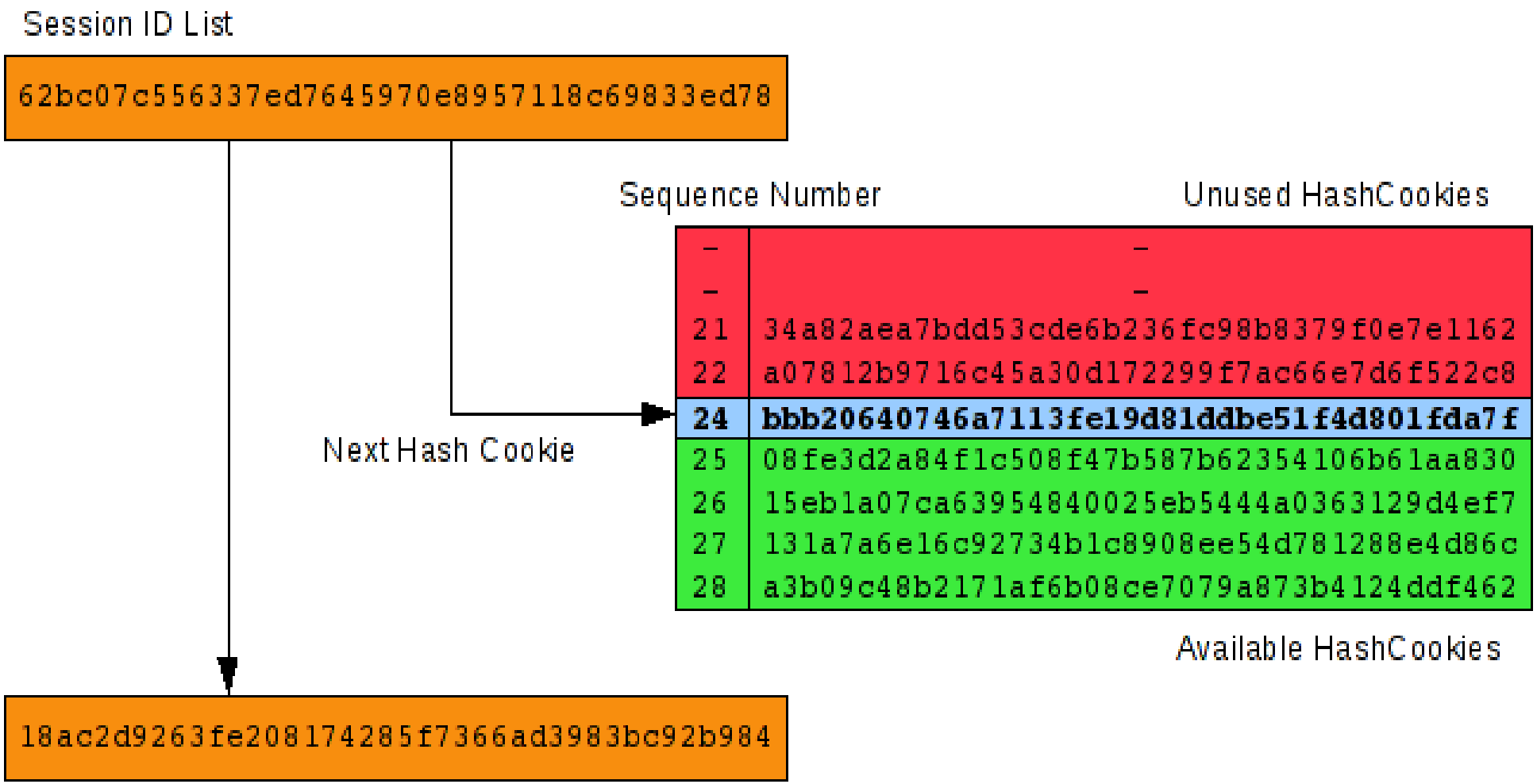
How they Work

- This is where the sequence number is important
- Valid window of cookies

How they Work

- So what if we have a hashCookie with sequence number greater than that of “next hashCookie” pointer but with a valid hashCookie?

How they Work



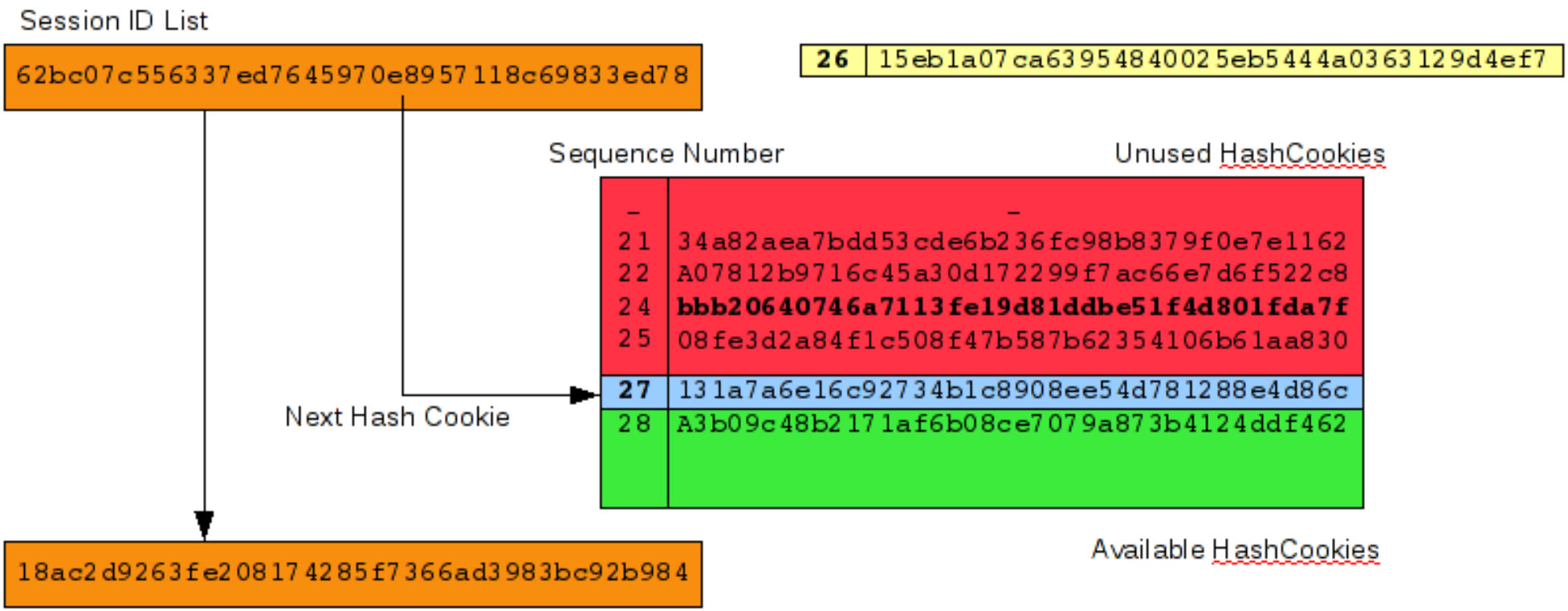
HashCookie = sha1(currentSessionID-salt-sequenceNumber)

Cookie = SessionID-HashCookie-sequenceNumber

How they Work

- Server receives request
- Sequence number not in window?
  - Reject
- Sequence number in available hashCookies window?
  - HashCookie is valid?
    - Remove hashCookie from window
    - Increment “Next hashCookie” pointer
    - Shift everything below it into Unused hashCookies window
    - Honour request

How they Work



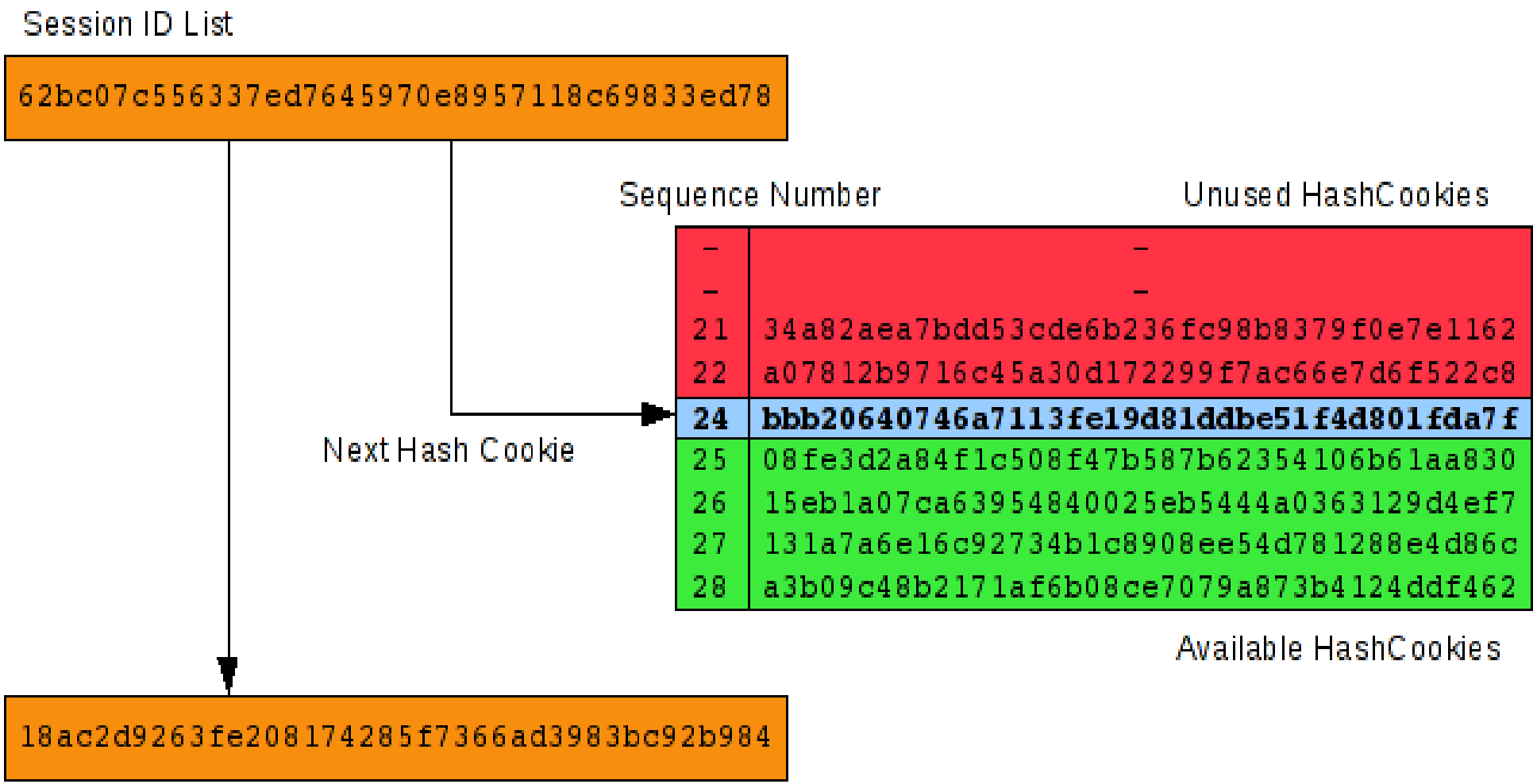
HashCookie = sha1(currentSessionID-salt-sequenceNumber)

Cookie = SessionID-HashCookie-sequenceNumber

How they Work

- So what if we have a cookie with sequence number less than that of “next hashCookie” pointer?

How they Work



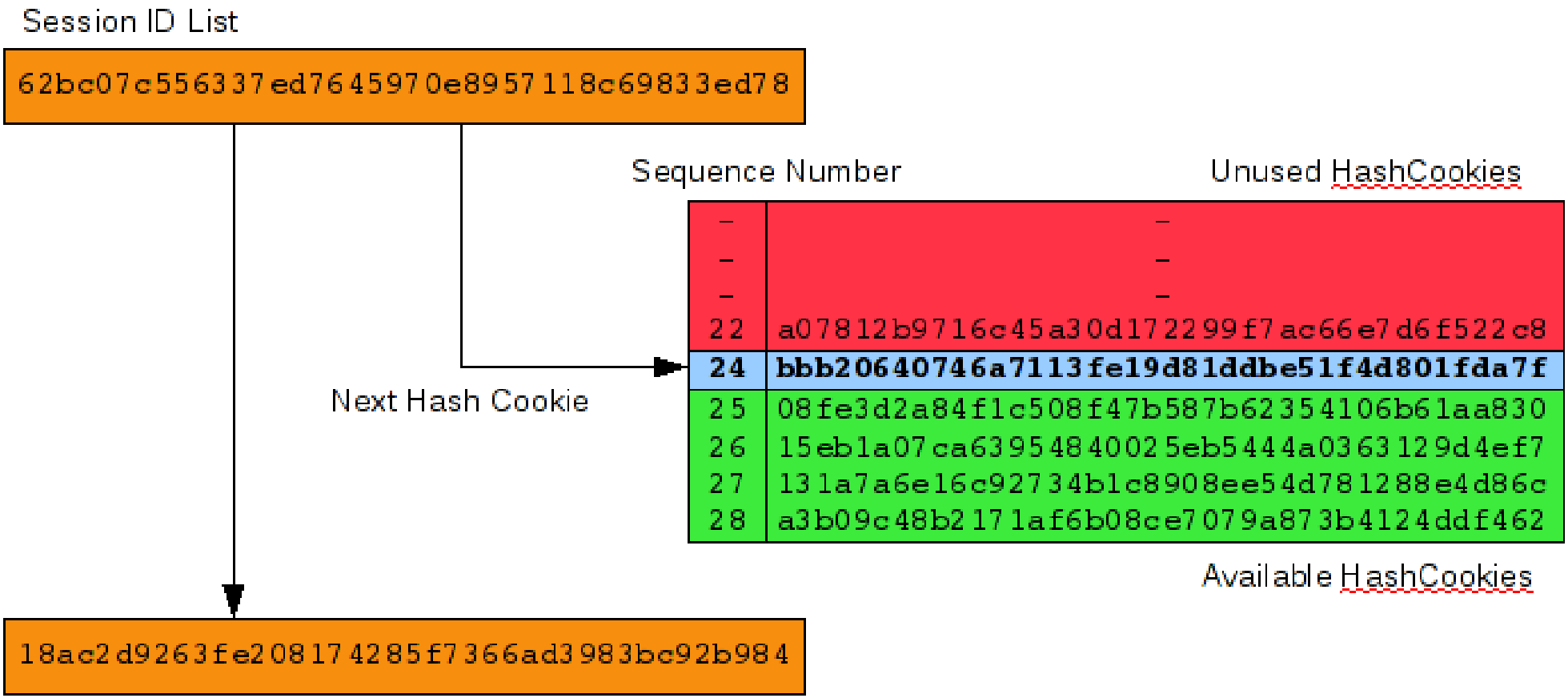
HashCookie = sha1(currentSessionID-salt-sequenceNumber)

Cookie = SessionID-HashCookie-sequenceNumber

How they Work

- Server receives request
- Sequence number not in window?
  - Reject
- Sequence number in unused hashCookies window?
  - HashCookie not outside of acceptable range?
    - Remove hashCookie from window
    - Honour request

How they Work



HashCookie = sha1(currentSessionID-salt-sequenceNumber)

Cookie = SessionID-HashCookie-sequenceNumber

Outcomes

- Questions?
- Anyone broken it yet?
- Should we be looking to push for this type of improvement in our browsers/web servers?
- Is this something that we can see working?
- http://labs.mwrinfosecurity.com