HTTPS WITH FORWARD SECRECY AT SCALE
How do we add HTTPS to established sites?
ESTABLISHED PROPERTIES
NEW FROM SCRATCH
MILLIONS OF USERS
GOAL:
“How do I add HTTPS to my sites?”
DIFFERENT CONCERNS
SAME FUNDAMENTALS
How does AOL add HTTPS to its sites?
QUICK ANSWER:
CRYPTO ACCELERATOR
HOW WE KNOW
Y.M.M.V.
Step 1. RESEARCH
MODERN CRYPTOGRAPHY
I DON'T WANT TO ASSUME
Step 2.

TEST
TOOLS & TECHNIQUES
Step 3.
IMPLEMENT
DECISION MAKING
Step 4.

REFINE
a.k.a
WAR STORIES
I WILL GET TECHNICAL
BECAUSE I DO ASSUME
LET’S BEGIN...
IT ALL BEGINS WITH RESEARCH
SSL / TLS
SSL IS DEAD
IT GOT EATEN BY A FLUFFY DOG
“SSL” IS STILL IN THE COMMON VERNACULAR
BUT IT’S STILL DEAD
SO I’LL SAY TLS
PLEASE DO CORRECT ME
IT’S IMPORTANT
THE DEVIL IS IN
THE DETAILS
75 – 95 %
TO ERR IS HUMAN
MISUNDERSTANDING
UNDERSTANDING TLS
TLS HAS TWO LAYERS
HANDSHAKE
RECORD
TLS begins with a handshake
LET'S DO CRYPTO! HERE'S A LIST OF THE MATHS I KNOW
I LIKE OPTION XYZ. HERE'S MY CERT AND SOME RANDOM DATA
(Does math...) Here's some info you can use to create the same key
(DOES MATH...)  
SEND ENCRYPTED MESSAGE>
TWO THINGS
AGREEING ON CAPABILITIES
AGREE ON THE MATH
CIPHER SUITE
1. ASYMMETRIC
2. SYMMETRIC
3. IDENTITY VALIDATION
4. MESSAGE AUTHENTICATION CODE
CIPHER SUITES ARE STANDARDIZED
NAMES AND ID NUMBERS ARE REGISTERED
PLATFORMS USE THEIR OWN NAMES...
MASTER SECRET

→

RECORD LAYER
RECORD LAYER
RECORD LAYER EXCHANGES ARE EASY
RECORD LAYER EXCHANGES ARE EASIER
CREATING THE MASTER SECRET IS HARD
ASYMMETRIC ENCRYPTION IS HARD
DIFFICULT TO GET RIGHT
DIFFICULT TO DO
BECAUSE: MATH
WHAT?
WAIT A SECOND...
WE KNOW TLS ISN’T PERFECT
Here's my certificate so you know it's really me.

(Pretends to check)

Yup, looks good.
KEY MANAGEMENT
COMPUTERS ARE GOOD AT MATH
IT DEPENDS ON THE MATH...
HOLD THAT
THOUGHT
WHAT KIND OF CRYPTO DO YOU WANT?
GRADE
THIS IS A PROBLEM
“NO REASON NOT TO”
ESTABLISHED PROPERTIES
MILLIONS OF USERS
PERFORMANCE
COMPATIBILITY
FOCUS ON THEM
SOMETIMES THE INTERNET KNOWS
THERE ARE NO UNIVERSAL RULES
## SSL Report: gmail.com

**Assessed on:** Thu, 07 May 2015 11:51:34 UTC | [Clear cache](#)

<table>
<thead>
<tr>
<th>Server</th>
<th>Domain(s)</th>
<th>Test time</th>
<th>Grade</th>
</tr>
</thead>
<tbody>
<tr>
<td>1: 74.125.239.117</td>
<td>gmail.com <a href="http://www.gmail.com">www.gmail.com</a></td>
<td>Thu, 07 May 2015 11:49:03 UTC, Duration: 75.786 sec</td>
<td>B</td>
</tr>
<tr>
<td>2: 74.125.239.118</td>
<td>gmail.com <a href="http://www.gmail.com">www.gmail.com</a></td>
<td>Thu, 07 May 2015 11:50:19 UTC, Duration: 75.832 sec</td>
<td>B</td>
</tr>
</tbody>
</table>

SSL Report v1.16.14
THERE IS NO RIGHT OR WRONG
THERE ARE MANY VALID REASONS NOT TO SCORE A+
IMPORTANT QUESTIONS
CAN I CUT PEOPLE OFF?
CAN I CUT A REVENUE SOURCE OFF?
WHAT'S THE HARM IN NOT GETTING THE HIGHEST GRADE?
INSERT PICTURE OF SNOWDEN HERE
SOMEONE MIGHT DECRYPT YOUR TRAFFIC
MITIGATES KEY COMPROMISE
MITIGATES DECRYPTION RISK
WHICH ASYMMETRIC ALGORITHM
MATH
MATURE
MODULAR ARITHMETIC
EASY TO ACCELERATE IN HARDWARE
EASY TO BUILD INTO SILICON
NO FORWARD SECRECY
ECDHE IS DIFFERENT BUT THE SAME
EPHEMERAL KEYS
DHE DOES FORWARD SECRECY
DISCRETE LOGARITHM
HARD TO ACCELERATE IN HARDWARE
RSA WAS GOOD ENOUGH
DHE ACCELERATION IS LESS MATURE
YOU PAY FOR FORWARD SECRECY
SPEED
$4x - 10x$

SLOWER
PROCESSING
ORDER OF MAGNITUDE
BASED ON THE EXACT SOLUTION
TESTING
HOW MUCH SLOWER?
HOW MUCH OVERHEAD?
CONVENTIONAL WISDOM DOES NOT APPLY
WE NEED REAL NUMBERS
SITUATIONS
DIFFER
YOUR MILAGE WILL VARY
A TEST PLAN
APPLES TO APPLES
HOW DOES AOL TEST?
WE DDOS THINGS
WE DDOS THINGS

(IN OUR LAB)
THC-SSL-DOS
SSLSQUEEZE
BUT WE WANTED RESPONSE TIMES
SO WE WROTE OUR OWN TOOL SUITE
BEYOND BREAKAGE
THE SLA
MORE REALISTIC
DETERMINE THE BROWSER RATIO
DETERMINE THE CIPHER SUITE RATIO
SPEED

TPS

CPU
CONTROLLED
CAPACITY
COMPATIBILITY
<table>
<thead>
<tr>
<th>Technology</th>
<th>Icon</th>
<th>Status</th>
<th>Status</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Explorer</td>
<td>![IE Icon]</td>
<td>![Warning Icon]</td>
<td>![否 Icon]</td>
<td>![否 Icon]</td>
</tr>
<tr>
<td>Netscape Navigator</td>
<td>![Netscape Icon]</td>
<td>![X Icon]</td>
<td>![√ Icon]</td>
<td>![?]</td>
</tr>
<tr>
<td>America Online</td>
<td>![AOL Icon]</td>
<td>![√ Icon]</td>
<td>![√ Icon]</td>
<td>![否 Icon]</td>
</tr>
</tbody>
</table>
REAL BROWSER TESTING
BECAUSE: BUGS
IMPLEMENTATION
SPECIFIC
$ curl --q https://test.aol.com/n/0 | python -m json.tool
{
  "cipher_id": "0x00,0x35",
  "tls_version": "0x03,0x01",
  "client": "10.100.1.2"
}
$ curl -q https://test.aol.com/n/0 | python -m json.tool
{
    "cipher_id": "0x00,0x35",
    "tls_version": "0x03,0x01",
    "client": "10.100.1.2"
}
curl-7.30 on OSX 10.10:

Asymmetric: RSA
Symmetric: AES256 CBC Mode
Identity: RSA
MAC: SHA-1

Using: TLSv1.0
WHO SURFS WITH CURL?
STRUCTED DATA FROM REAL BROWSERS
SELENIUM
In [1]: from selenium import webdriver

In [2]: import json

In [3]: driver = webdriver.Remote(
    command_executor='http://selenium.aol.com:1234/wd/hub',
    desired_capabilities={
        'browserName': 'chrome', 'platform': 'MAC'
    }
)

In [4]: driver.get("https://test.aol.com/n/0")

In [5]: res = json.loads(driver.find_element_by_tag_name('pre').text)

In [6]: res
Out[6]:
{'cipher_id': '0xC0,0x13',
'tls_version': '0x03,0x01',
'client': '10.200.2.3'}

In [7]: driver.quit()
CONTINUOUS TESTING
IMPLEMENTATION
HONEST CONVERSATION
EVERYONE IS GETTING MORE SOPHISTICATED
REAL PRODUCT NEEDS
DOES IT NEED FORWARD SECRECY?
DOES IT NEED TO SUPPORT OLDER BROWSERS?
WHAT LETTER?
PKI & CONFIDENTIAL DATA
How do we add HTTPS to established sites?
Step 1.

RESEARCH
TECHNOLOGY

PRODUCT

BUSINESS NEEDS
Step 2.
TESTING
NO ASSUMPTIONS
ACCORDING TO A PLAN
Step 3.

IMPLEMENT
"THE NICE THING ABOUT STANDARDS..."
YES, WE HAVE THESE

• Browser matrices
• CVE mitigation policies
• RFC adherence policies
• Security standards
BUT IT REALLY IS ALL ABOUT THE USER
DOING THE
RIGHT THING
YOU KNOW WHAT
THAT IS BY NOW
Step 4.

REFINE
WAR STORIES
YOU SAID
SSL IS DEAD!
"SSL IS BROKEN!"
"SO TURN IT OFF"
BUT WAIT!
INTERNAL SITES?
Morale:

NO ASSUMPTIONS
IN VENDORS WE TRUST
MICROCODE UPDATE
THOROUGHLY VETTED
NOT THOROUGHLY VETTED ENOUGH
OLD BROWSERS?
SAFARI 6
Morale:

DO THE REAL BROWSER TESTING
JUST REDIRECT IT ALL
ADC OFFLOAD
APP GATING
HTTP ⇔ HTTPS
ON THE ADC
http://site.co.uk => https://site.com/en-uk
http://site.co.uk => https://site.co.uk
Morale: COMMUNICATION
THANK YOU
REFERENCES

1. Intel, Windows, Apple, Android, Safari, Firefox, Chrome and SCO logos shamelessly plundered from the ‘Net, but copyright the original owners.


3. Some icons are from the CC-SA licensed RRZE Icon Set: https://github.com/RRZE-PP/rrze-icon-set