HTTPS WITH FORWARD SECRECY AT SCALE

Aol.

How do we add HTTPS to established sites?

Aol.

ESTABLISHED PROPERTIES

~~NEW FROM SCRATCH~~

MILLIONS OF USERS

GOAL:

“How do I add HTTPS to my sites?”

Aol.

DIFFERENT CONCERNS

SAME FUNDAMENTALS

How does AOL add HTTPS to its sites?

Aol.

QUICK ANSWER:

CRYPTO ACCELERATOR

Aol.

HOW WE KNOW

Y.M.M.V.

Step 1.

RESEARCH

MODERN CRYPTOGRAPHY

Aol.

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

Aol.

LET’S BEGIN…

IT ALL BEGINS WITH RESEARCH

SSL / TLS

SSL IS DEAD

Aol.

IT GOT EATEN BY A FLUFFY DOG

“SSL” IS STILL IN THE COMMON VERNACULAR

Aol.

BUT IT'S STILL DEAD

Aol.

SO I'll SAY TLS

PLEASE
DO
CORRECT ME

Aol.

IT’S IMPORTANT

THE DEVIL IS IN THE DETAILS

75 – 95 %

Aol.

TO ERR IS HUMAN

Aol.

MISUNDERSTANDING

UNDERSTANDING TLS

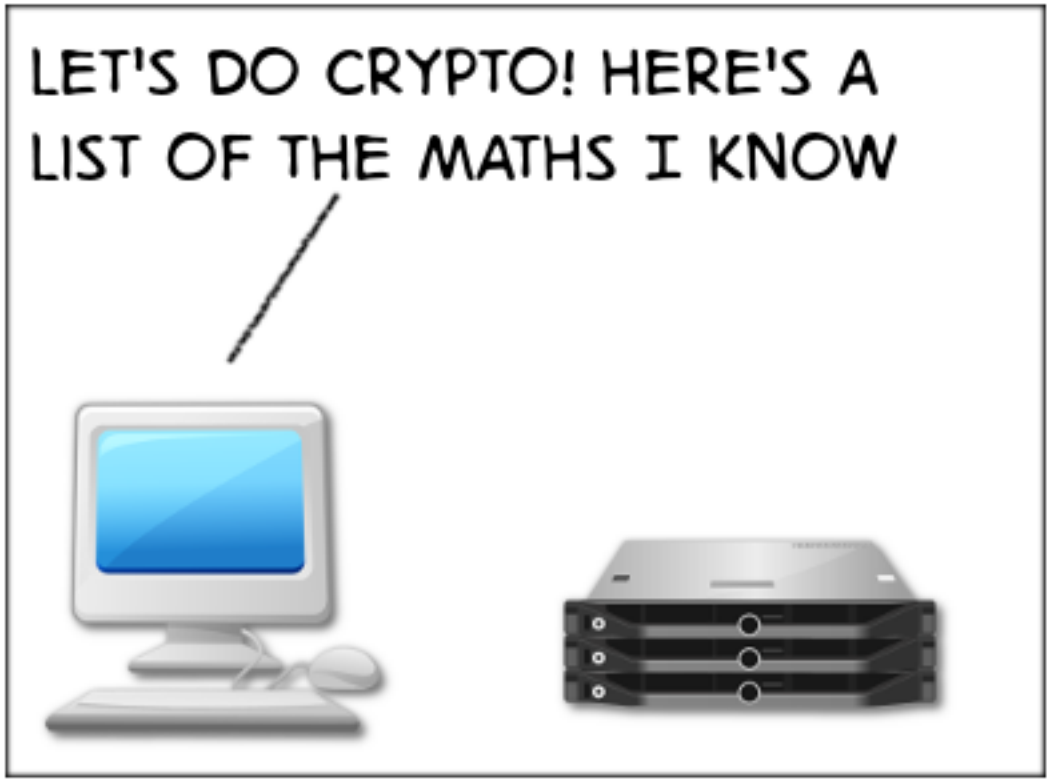
Aol.

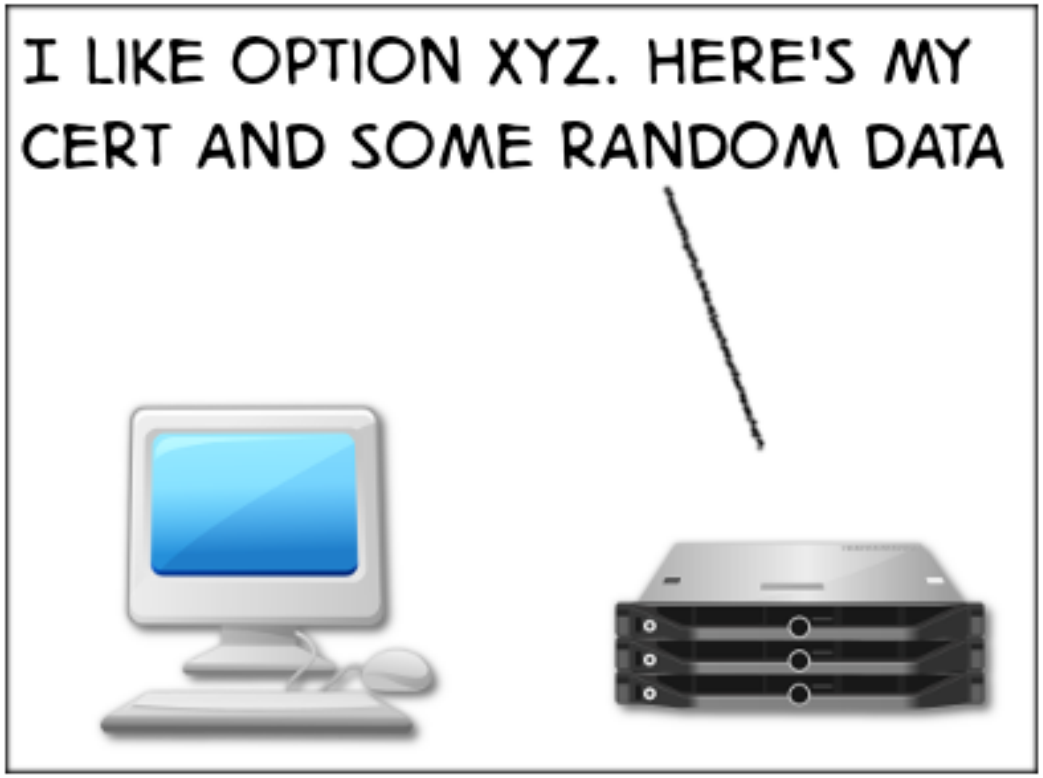
TLS HAS TWO LAYERS

HANDSHAKE RECORD

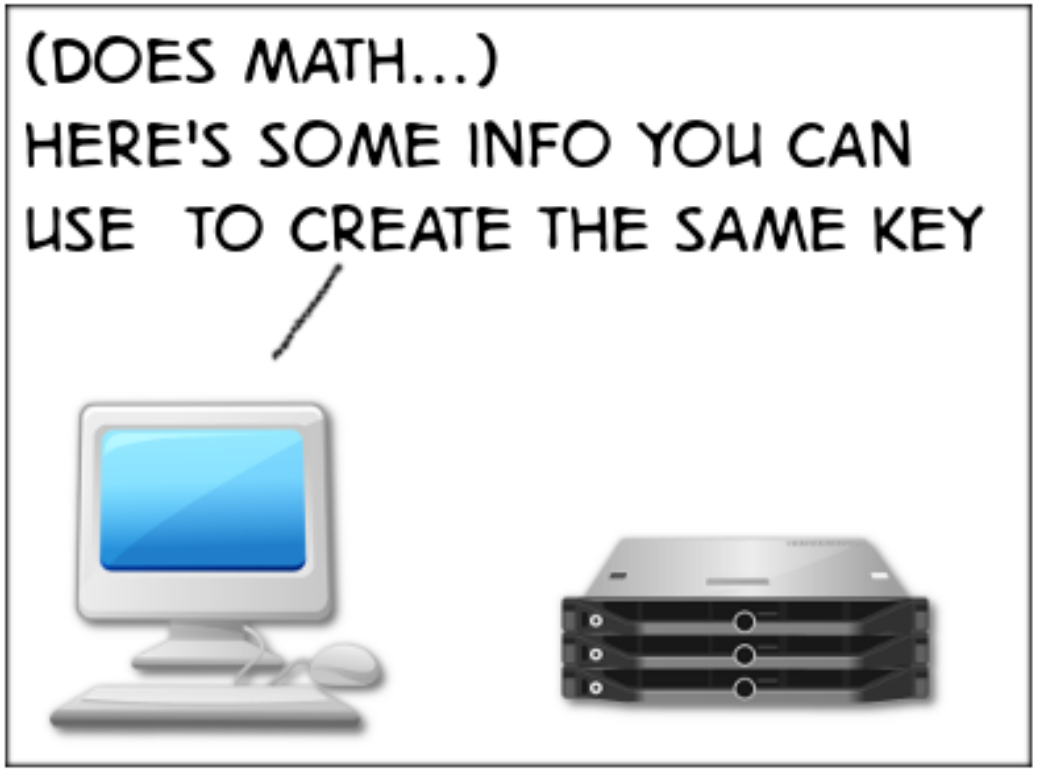
TLS BEGINS WITH A HANDSHAKE

Aol.

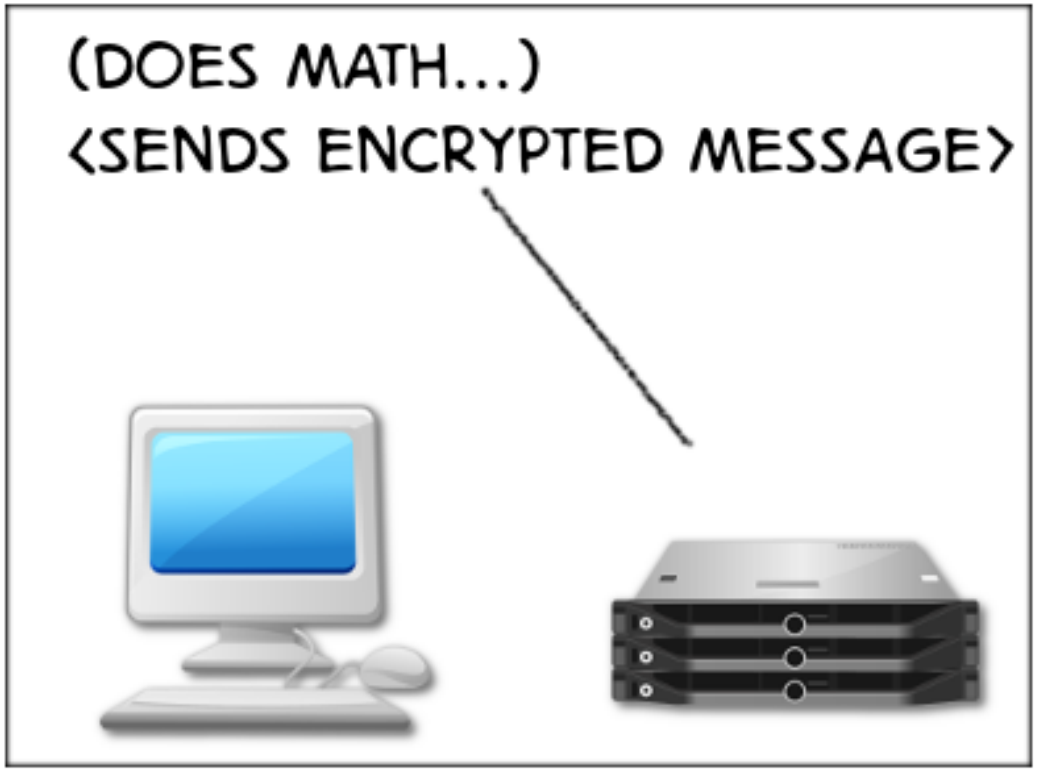




Aol.



Aol.



Aol.

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

Aol.

NAMES AND ID NUMBERS ARE REGISTERED

PLATFORMS USE THEIR OWN NAMES…

HANDSHAKE

↓

MASTER SECRET

MASTER SECRET

RECORD LAYER

RECORD LAYER

RECORD LAYER EXCHANGES ARE EASY

RECORD LAYER EXCHANGES ARE EASIER

Aol.

CREATING THE MASTER SECRET IS HARD

ASYMMETRIC ENCRYPTION IS HARD

Aol.

DIFFICULT TO GET RIGHT

DIFFICULT TO DO

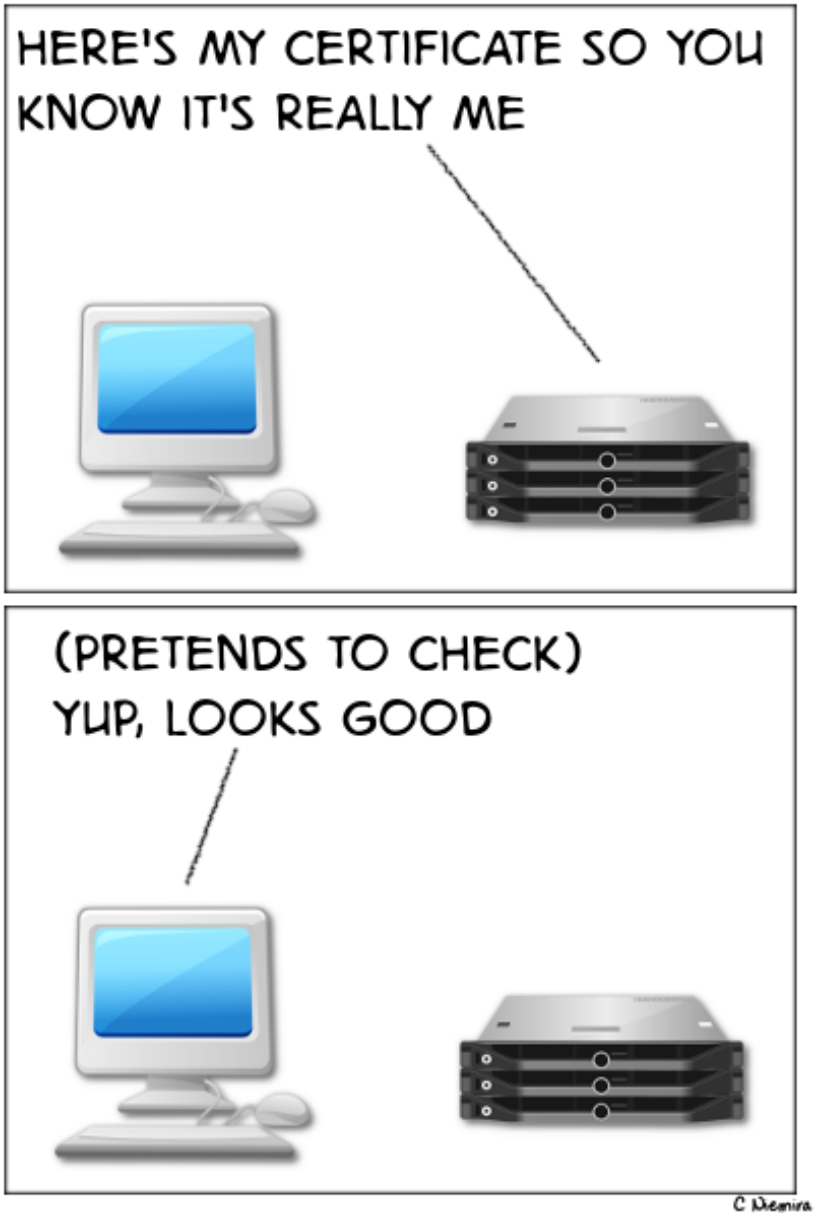
BECAUSE: MATH

WHAT?

WAIT A SECOND...

WE KNOW TLS ISN’T PERFECT

Aol.


HERE'S MY CERTIFICATE SO YOU KNOW IT'S REALLY ME
(PRETENDS TO CHECK) YUP, LOOKS GOOD
C Meanira

Aol.

CVE

KEY MANAGEMENT

???

COMPUTERS ARE GOOD AT MATH

Aol.

IT DEPENDS ON THE MATH…

HOLD THAT THOUGHT

Aol.

WHAT KIND OF CRYPTO DO YOU WANT?

GRADE

A+

THIS IS A PROBLEM

"NO REASON NOT TO"

Aol.

ESTABLISHED PROPERTIES

MILLIONS OF USERS

PERFORMANCE

COMPATIBILITY

FOCUS ON THEM

SOMETIMES THE INTERNET KNOWS

Aol.

THERE ARE NO UNIVERSAL RULES

Aol.

QUALYS® SSL LABS

Home Projects Qualys.com Contact

You are here: Home > Projects > SSL Server Test > gmail.com

SSL Report: gmail.com

Assessed on: Thu, 07 May 2015 11:51:34 UTC | Clear cache

Scan Another >>

	Server	Domain(s)	Test time	Grade
1	74.125.239.117 nuq05s01-in-f21.1e100.net Ready	gmail.com www.gmail.com	Thu, 07 May 2015 11:49:03 UTC **Duration:** 75.786 sec	B
2	74.125.239.118 nuq05s01-in-f22.1e100.net Ready	gmail.com www.gmail.com	Thu, 07 May 2015 11:50:19 UTC **Duration:** 75.832 sec	B

SSL Report v1.16.14

Aol.

THERE IS NO RIGHT OR WRONG

Aol.

THERE ARE MANY VALID REASONS NOT TO SCORE A+

Aol.

IMPORTANT QUESTIONS

CAN I CUT PEOPLE OFF?

Aol.

CAN I CUT A REVENUE SOURCE OFF?

Aol.

WHAT'S THE HARM IN NOT GETTING THE HIGHEST GRADE?

Aol.

INSERT PICTURE OF
SNOWDEN HERE

SOMEONE MIGHT DECRYPT YOUR TRAFFIC

Aol.

PERFECT FORWARD SECRECY

Aol.

FORWARD SECRECY

MITIGATES KEY COMPROMISE

MITIGATES DECRYPTION RISK

Aol.

WHICH ASYMMETRIC ALGORITHM

Aol.

MATH

RSA

MATURE

MODULAR ARITHMETIC

EASY TO ACCELERATE IN HARDWARE

EASY TO BUILD INTO SILICON

NO FORWARD SECRECY

DHE

DH

ECDHE

ECDHE IS DIFFERENT BUT THE SAME

EPHEMERAL KEYS

DHE DOES FORWARD SECRECY

Aol.

DISCRETE LOGARITHM

HARD TO ACCELERATE IN HARDWARE

Aol.

RSA WAS GOOD ENOUGH

Aol.

DHE ACCELERATION IS LESS MATURE

Aol.

YOU PAY FOR FORWARD SECRECY

SPEED

4× – 10×
SLOWER

Aol.

PROCESSING

ORDER OF MAGNITUDE

BASED ON THE EXACT SOLUTION

Aol.

TESTING

HOW MUCH SLOWER?

HOW MUCH OVERHEAD?

CONVENTIONAL WISDOM DOES NOT APPLY

Aol.

WE NEED REAL NUMBERS

SITUATIONS DIFFER

Aol.

SOLUTIONS DIFFER

Aol.

YOUR MILAGE WILL VARY

Aol.

A TEST PLAN

APPLES TO APPLES

HOW DOES AOL TEST?

Aol.

WE DDOS THINGS

Aol.

WE DDOS THINGS

(IN OUR LAB)

Aol.

THC-SSL-DOS

SSLSQUEEZE

BUT WE WANTED RESPONSE TIMES

SO WE WROTE OUR OWN TOOL SUITE

BEYOND BREAKAGE

Aol.

THE SLA

MORE REALISTIC

DETERMINE THE BROWSER RATIO

DETERMINE THE CIPHER SUITE RATIO

SPEED

TPS

CPU

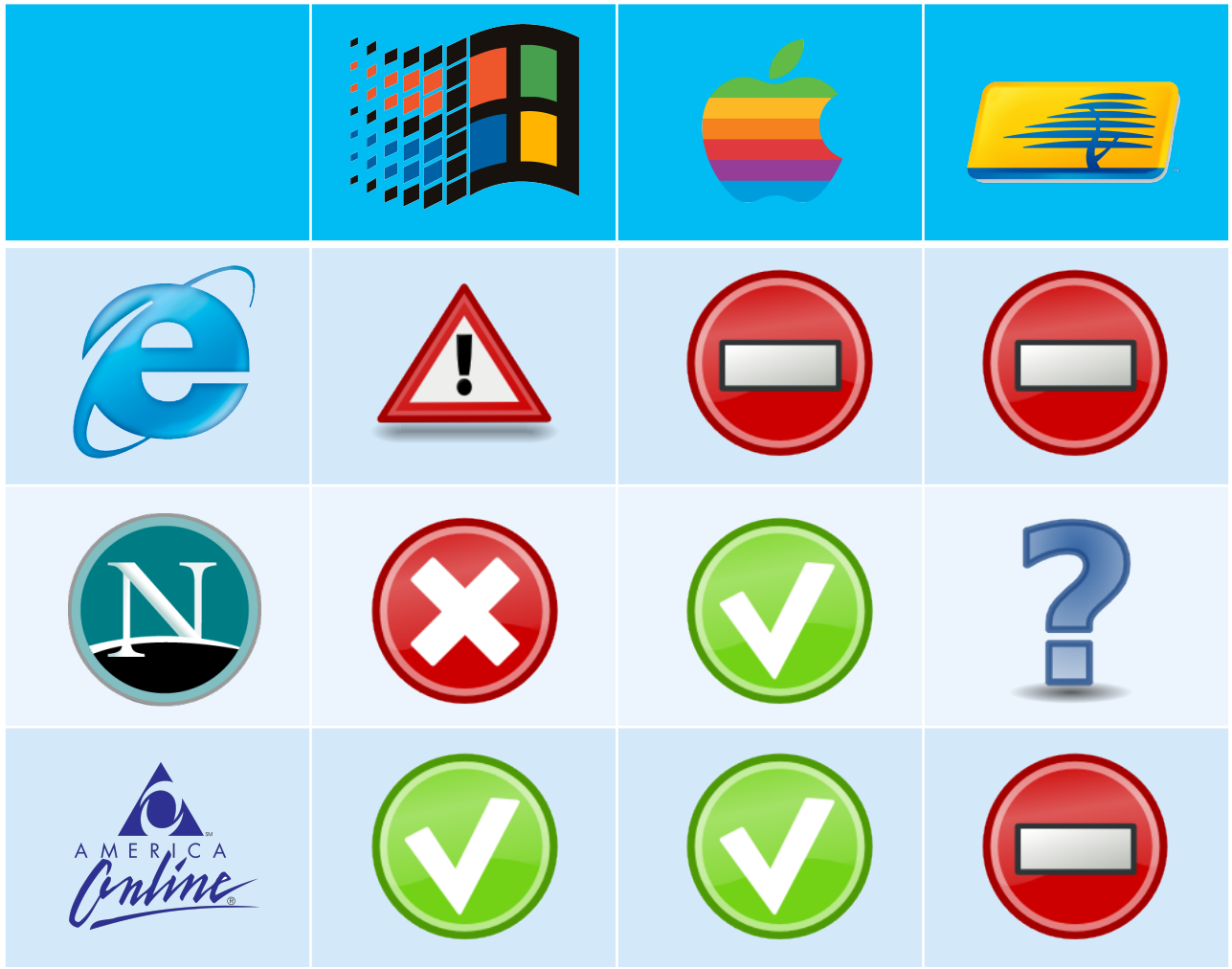
CONTROLLED

CAPACITY

COMPATIBILITY

	✓	✓	✓
	✓	✓	✓
	✓	✓	⊖

Aol.



Aol.

REAL BROWSER TESTING

BECAUSE: BUGS

IMPLEMENTTION 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"
}
```

Aol.

```
$ 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"
}
```

Aol.

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?

Aol.

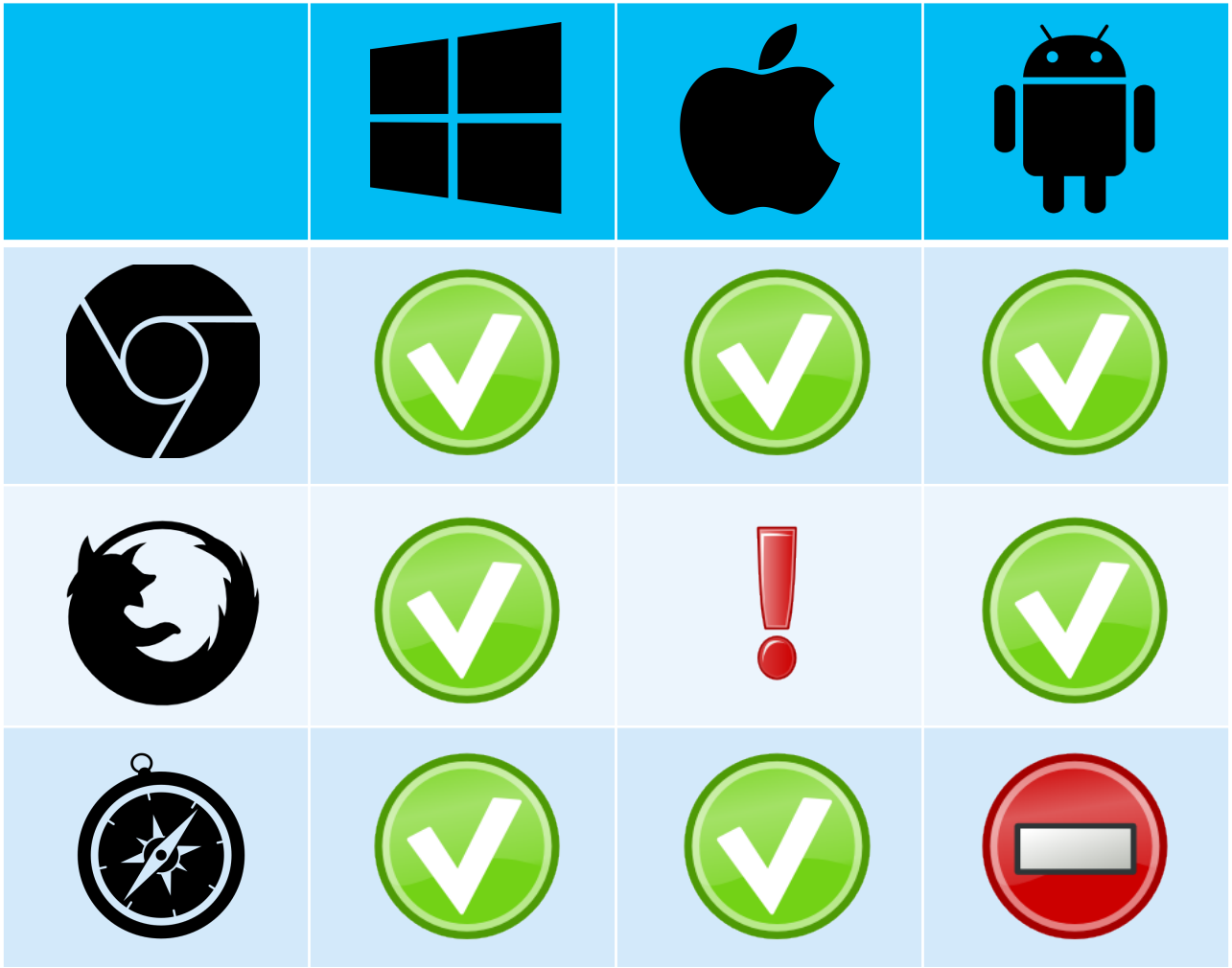
STRUCTED DATA FROM REAL BROWSERS

Aol.

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()
```

Aol.



Aol.

TEST PRODUCTION

CONTINUOUS TESTING

IMPLEMENTATION

HONEST CONVERSATION

Aol.

EVERYONE IS GETTING MORE SOPHISTICATED

Aol.

REAL PRODUCT NEEDS

DOES IT NEED FORWARD SECRECY?

Aol.

DOES IT NEED TO SUPPORT OLDER BROWSERS?

Aol.

WHAT LETTER?

PKI & CONFIDENTIAL DATA

Aol.

How do we add HTTPS to established sites?

Aol.

Step 1.

RESEARCH

TECHNOLOGY

PRODUCT

BUSINESS NEEDS

Step 2.

TESTING

NO ASSUMPTIONS

ACCORDING TO A PLAN

Aol.

Step 3.

IMPLEMENT

“THE NICE THING ABOUT STANDARDS…”

Aol.

YES, WE HAVE THESE

- Browser matrices
- CVE mitigation policies
- RFC adherence policies
- Security standards

BUT IT REALLY IS ALL ABOUT THE USER

Aol.

DOING THE RIGHT THING

Aol.

YOU KNOW WHAT THAT IS BY NOW

Step 4.

REFINE

WAR STORIES

Aol.

YOU SAID SSL IS DEAD!

Aol.

"SSL IS BROKEN!"

"SO TURN IT OFF"

BUT WAIT!

INTERNAL SITES?

Morale:

NO ASSUMPTIONS

IN VENDORS WE TRUST

Aol.

MICROCODE UPDATE

THOROUGHLY VETTED

NOT THOROUGHLY VETTED ENOUGH

Aol.

OLD BROWSERS?

SAFARI 6

Morale:

DO THE REAL BROWSER TESTING

Aol.

JUST REDIRECT IT ALL

Aol.

ADC OFFLOAD

APP GATING

HTTP => HTTPS ON THE ADC

Aol.

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.

2. Katz, Jonathan, and Yehuda Lindell. *Introduction to Modern Cryptography*. Boca Raton: Chapman & Hall/CRC, 2008. Print.

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