Can we afford to ignore web security in the 21st century?

Rahat Khan - Expedia Inc
Natalia Oskina - Zuhlke UK

What data can we find on the web?

- Credit Cards
- Medical Records
- Financial Records
- Addresses
- Phone Numbers
- Birthdays
- Social Media

What if it was YOUR data?

- **Your** medical information
- **Your** credit cards
- **Your** personal account information

Some breaches in the last 12 months

- *Yahoo Sept 16* **500 million** accounts compromised
- *Weebly Oct 16* **43 million** users affected
- *National Payment Corporation of India* Oct 16
- *Cisco* Nov 16
- *AdultFriendFinder.com* Nov 16
- *San Francisco Municipal Transportation Agency* Nov 16
- Yahoo ~~Dec 16~~ ~~**1 Billion**~~ **3 Billion** **As of this month**
- *E-Sports Entertainment Association* Jan 17 **1.5 Million**
- *InterContinental Hotels Group* Feb 17
- *Arby's Feb 17*
- *River City Media March 17*

...

- *Verifone* Mar 17
- *Saks Fifth Avenue* Mar 17
- *UNC Health Care* Mar 17
- *America's JobLink* Mar 17
- *FAFSA: IRS Data Retrieval Tool* Apr 17
- *Chipotle* Apr 17
- *Sabre Hospitality Solutions* May 17
- *Gmail* May 17
- *Bronx Lebanon Hospital Center* May 17
- *Brooks Brothers* May 17
- *DocuSign* May 17

...

- *OneLogin* May 17
- *Kmart* May 17
- *University of Oklahoma* Jun 17
- *Washington State University* Jun 17
- *Deep Root Analytics* Jun 17
- *Blue Cross Blue Shield* Jun 17
- *California Association of Realtors* Jul 17
- *Verizon* Jul 17
- *TalentPen and TigerSwan* Sept 17
- *Equifax* Sept 17
- *Deloitte* Sept 17

Headlines this week

Equifax Says 15.2 Million UK Records Exposed - Reuters

Equifax Breach Included 10 Million US Driving Licenses - Engadget

Russian Agents Used Google to Interfere in Election - Gizmodo

North Korea Reportedly Hacked US-South Korean War Plans, Including How to Take Down Kim Jong-un - Gizmodo

Data Breach Exposed Medical Records, Including Blood Tests Results, of Over 100 Thousand Patients - Gizmodo

That’s a lot of breaches…

… But how much are we talking about?

http://breachlevelindex.com/

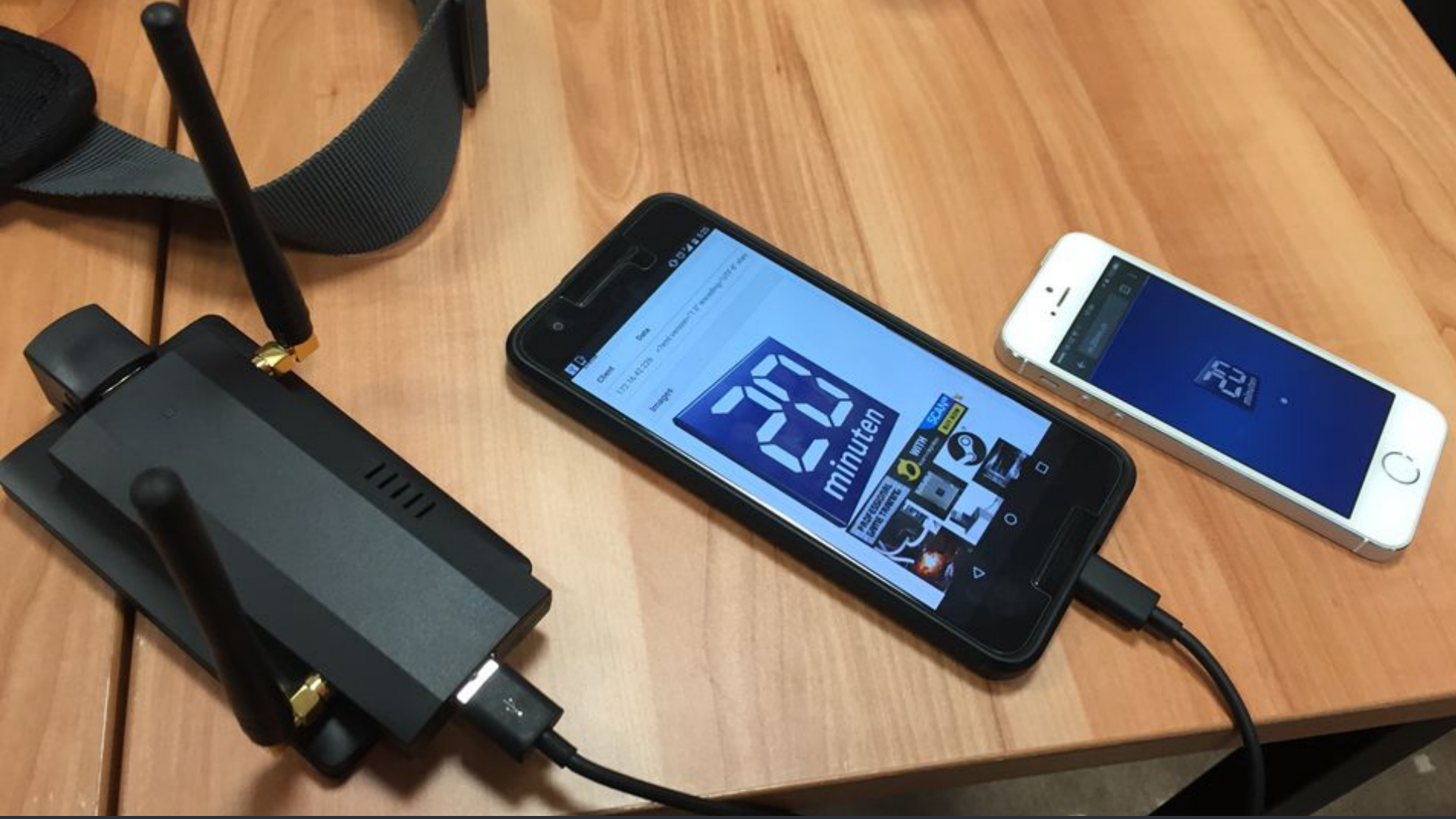
60 records per second!

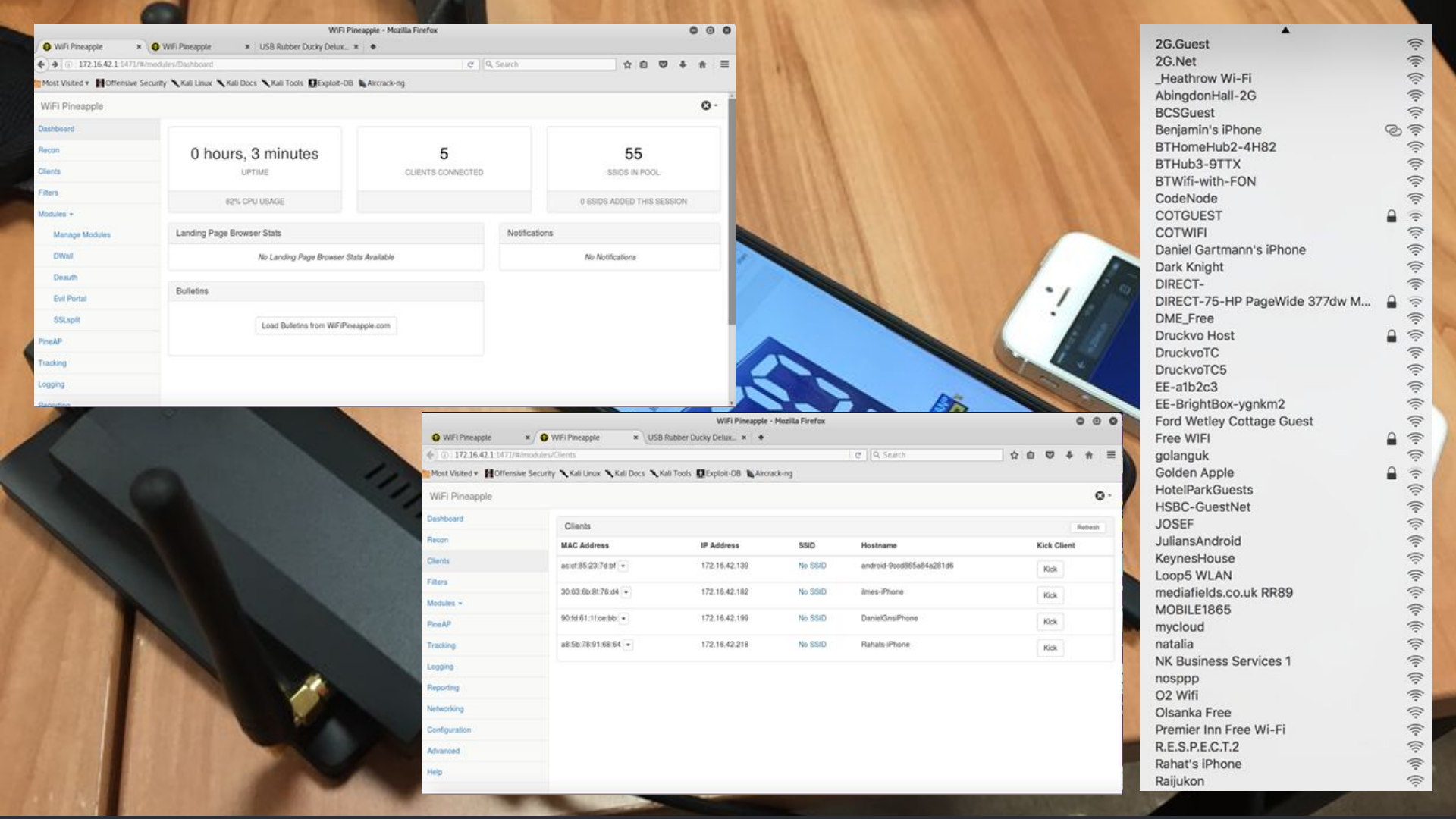
- *UK population: ~66 Million*
- *UK records stolen: ~136 Million*
- ***And… look at the USA!***

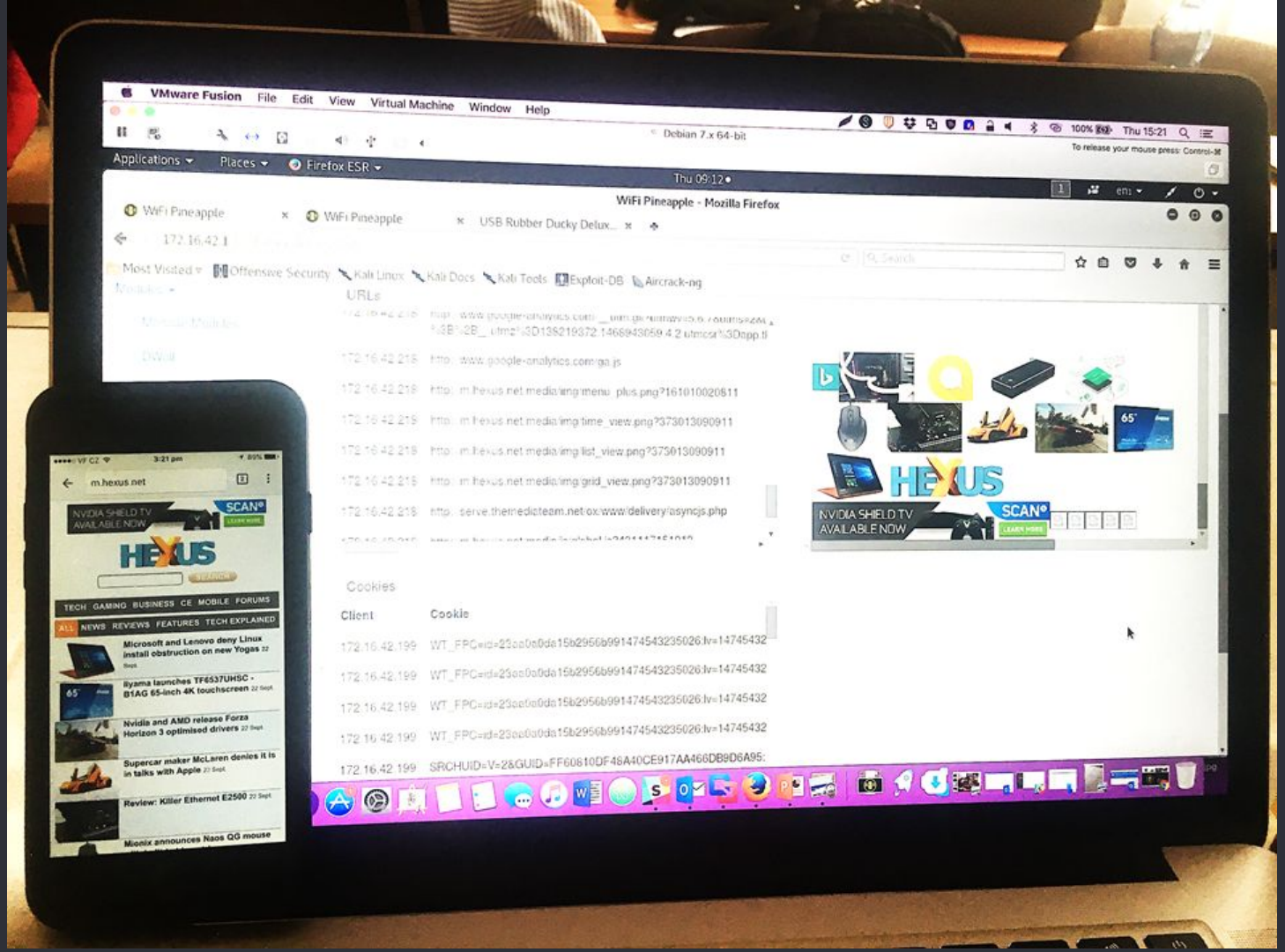
So how should we protect ourselves...

... if even the largest companies get hacked?

- We're not aiming for 100% security
- The cost of compromising your system should be greater than the value of the information that would be lost
- Start with simple security practises
- Start with HTTPS ... and here is why


minuten


WiFi Pineapple - Mozilla Firefox
WiFi Pineapple
0 hours, 3 minutes
UPTIME
5
CLIENTS CONNECTED
55
SSIDS IN POOL
82% CPU USAGE
0 SSIDS ADDED THIS SESSION
Landing Page Browser Stats
No Landing Page Browser Stats Available
Notifications
No Notifications
Bulletins
Load Bulletins from WiFiPineapple.com
WiFi Pineapple - Mozilla Firefox
WiFi Pineapple
Clients
MAC Address
IP Address
SSID
Hostname
Kick Client
ac:cf:85:23:7d:bf
172.16.42.139
No SSID
android-9ccd865a84a281d6
30:63:6b:8f:76:d4
172.16.42.182
No SSID
ilmes-iPhone
90:fd:61:1f:ce:bb
172.16.42.199
No SSID
DanielGinsiPhone
a8:5b:78:91:68:64
172.16.42.218
No SSID
Rahats-iPhone
2G.Guest
2G.Net
_Heathrow Wi-Fi
AbingdonHall-2G
BCSGuest
Benjamin's iPhone
BTHomeHub2-4H82
BTHub3-9TTX
BTWifi-with-FON
CodeNode
COTGUEST
COTWIFI
Daniel Gartmann's iPhone
Dark Knight
DIRECT-
DIRECT-75-HP PageWide 377dw M...
DME_Free
Druckvo Host
DruckvoTC
DruckvoTC5
EE-a1b2c3
EE-BrightBox-ygnkm2
Ford Wetley Cottage Guest
Free WIFI
golanguk
Golden Apple
HotelParkGuests
HSBC-GuestNet
JOSEF
JuliansAndroid
KeynesHouse
Loop5 WLAN
mediafields.co.uk RR89
MOBILE1865
mycloud
natalia
NK Business Services 1
nosppp
O2 Wifi
Olsanka Free
Premier Inn Free Wi-Fi
R.E.S.P.E.C.T.2
Rahat's iPhone
Raijukon


VMware Fusion File Edit View Virtual Machine Window Help
Debian 7.x 64-bit
Applications Places Firefox ESR
Thu 09:12
WiFi Pineapple - Mozilla Firefox
WiFi Pineapple
WiFi Pineapple
USB Rubber Ducky Delux...
172.16.42.1
Most Visited Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng
URLs
http://www.google-analytics.com/ga.js
http://m.hexus.net/media/img/menu_plus.png?1610100206111
http://m.hexus.net/media/img/time_view.png?373013090911
http://m.hexus.net/media/img/list_view.png?373013090911
http://m.hexus.net/media/img/grid_view.png?373013090911
http://serve.themediateam.net:ox:www/delivery/asyncjs.php
Cookies
Client
Cookie
172.16.42.199 WT_FPC=id=23aa0a0da15b2956b9914745432350261v=1474543243
172.16.42.199 WT_FPC=id=23aa0a0da15b2956b9914745432350261v=1474543243
172.16.42.199 WT_FPC=id=23aa0a0da15b2956b9914745432350261v=1474543243
172.16.42.199 WT_FPC=id=23aa0a0da15b2956b9914745432350261v=1474543243
172.16.42.199 SRCHUID=V=2&GUID=FF60810DF48A40CE917AA466DB9D6A95:
NVIDIA SHIELD TV AVAILABLE NOW
SCAN
HEXUS
m.hexus.net
TECH GAMING BUSINESS CE MOBILE FORUMS
ALL NEWS REVIEWS FEATURES TECH EXPLAINED
Microsoft and Lenovo deny Linux install obstruction on new Yogas
Iiyama launches TF6537UHSC - 81AG 65-inch 4K touchscreen
Nvidia and AMD release Forza Horizon 3 optimised drivers
Supercar maker McLaren denies it is in talks with Apple
Review: Killer Ethernet E2500
Monix announces Naos QG mouse

We should use HTTPS!

- As of early 2017 ~50% of the web is encrypted, up from 13% in early 2014
- Is HTTPS slower?
- https://www.httpvshttps.com/
- Using HTTPS lets us start using HTTP/2

Securing your sites

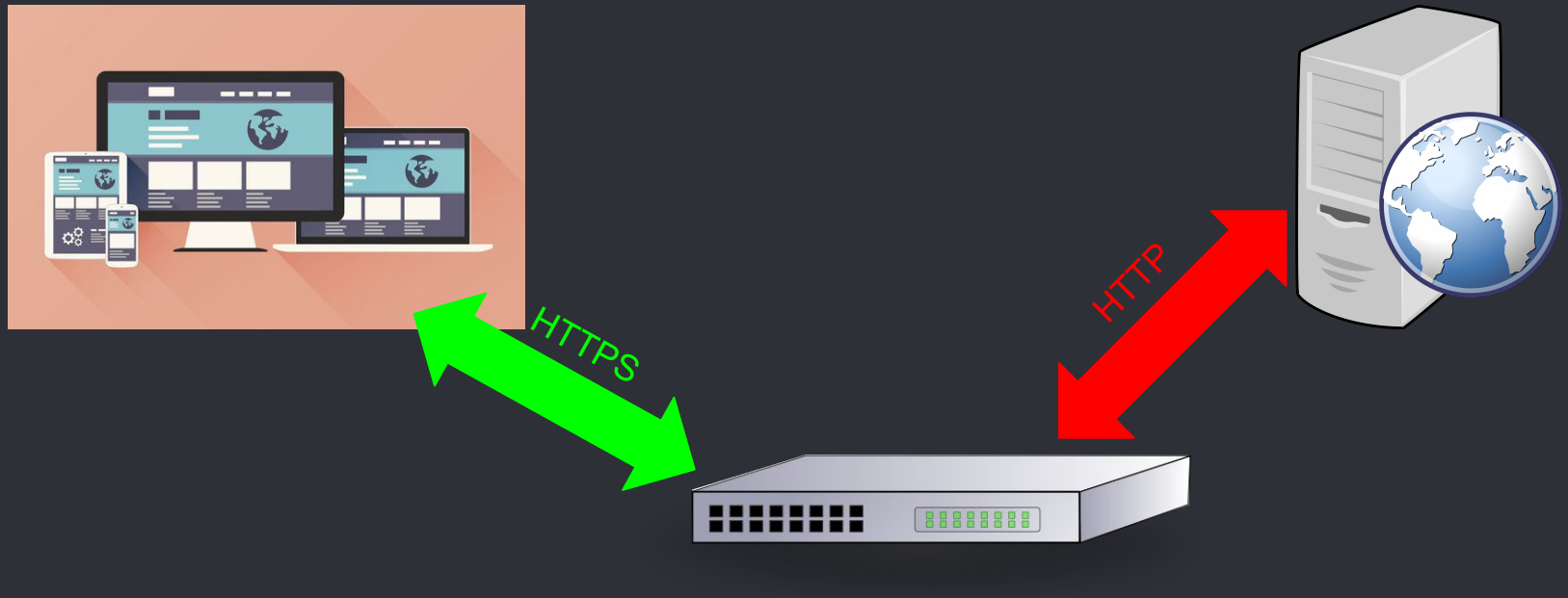
- Set the right Content Security Policy
  - Define a whitelist of trusted content sources
- Set-cookie: httponly
- X-XSS-Protection: 1; mode=block
  - Tells the browser not to try sanitize inputs when xss is detected
- X-Content-Type-Options: nosniff
  - Forces browsers to use the MIME type declared by the server
  - Reduces drive by downloads and user uploaded content where an executable might be pretended to be something else
- X-Frame-Options: DENY / SAMEORIGIN / ALLOW_FROM [uri]
  - Controls which domains can embed your page as an iframe
- HTTPS Strict Transport Security (HSTS)

It’s not easy to get SSL Certificates…
…wait a second, is it?

- Let’s Encrypt!
  - https://letsencrypt.org/
  - Free SSL certificates issued
  - Sponsored, supported and trusted by major players
- How do we test our ssl implementation?
  - https://www.ssllabs.com/ssltest/

Let’s Encrypt

HTTPS


HTTPS
HTTP


TP

Solution

- Use a public/private RSA key pair
- Server would produce at build time
- Clients would receive public key and use this to encrypt user credentials
  - We would send this along with IP information to the set
- Server would decrypt credentials and authenticate
  - Create a JWT with a session limit
  - Embed the original IP address that was authenticated into the JWT
- Client would send JWT with all subsequent requests
- Server checks the token is being used by the IP the token was initially authenticated with

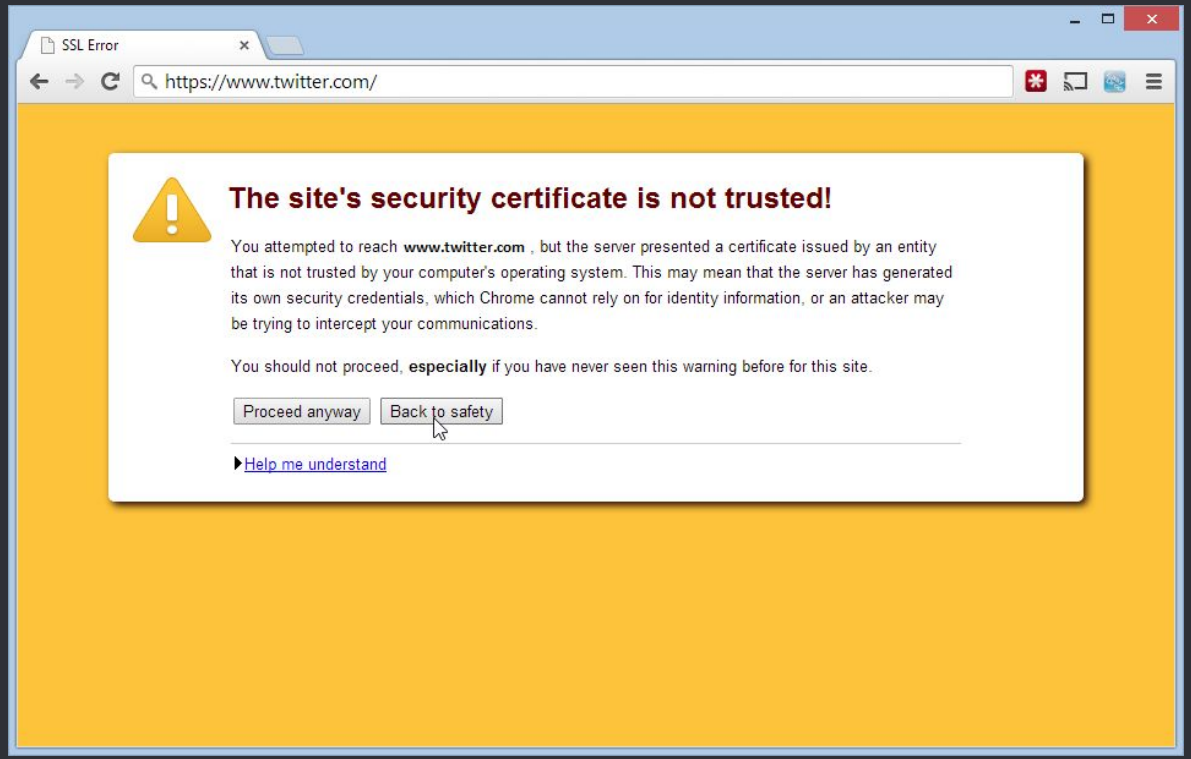
Solution

- Use a public/priva
- Server would pr
- Clients would r ser credentials
  - We would et
- Server would
  - Create a J
  - Embed the ted into the JWT
- Client would send J
- Server checks the toke he token was initially authenticated with

What did we learn?

- Its best to assume everything outside of your immediate control is compromised
- We shouldn’t rely on the firewall to protect us
- Security should be thought of on an app by app basis
- All it takes is one disgruntled employee!

Social Engineering?



Bash Bunny

Bash Bunny

- Pretends to be a keyboard
- Runs Linux
- Quad Core CPU
- Desktop Class SSD
- Payload delivered in 7 seconds
  - Like a self signed root certificate

Self Signed Root Certificate

- Top-most certificate in a certificate chain
- Not signed by a trusted certificate authority
- Enables yet another man in the middle attack
- Not just usb sticks you should be worried about!


lenovo
Superfish
Search Visually

Fishing for user data...

- Self signed root certificate installed on all notebooks
- So they could supply ads on secure sites
- Same private key on all notebooks
- UH OH...!!!

Security is everyone's responsibility

- Engineers should write secure code
- Engineers should ensure they have secure infrastructure
- QA should keep security in mind when testing
- PMs should incorporate security considerations into the development cycle
- Product Owners should accept the cost of implementing security features
  - Or the potential cost of NOT doing them!
- Teams should collaborate
- Share ideas
- Don't always reinvent the wheel

Don’t leave it till the end

- Think secure thoughts from the get go!
- Make it a part of the development cycle
- Pen test frequently, not just at the end
- Leaving it to the end is more tech debt

Start small

- Start with the easy and obvious
- It’s a marathon not a sprint to the finish line
- Increase the barriers to entry, one iteration at a time
- OWASP top 10
  - https://www.owasp.org/index.php/Top_10_2017-Top_10

OWASP Top 10

Top 10 2013	Top 10 2017
A1 – Injection	A1 – Injection
A2 – Broken Authentication and Session Management	A2 – Broken Authentication and Session Management
A3 – Cross-Site Scripting (XSS)	A3 – Cross-Site Scripting
A4 – Insecure Direct Object References	A4 – Broken Access Control
A5 – Security Misconfiguration	A5 – Security Misconfiguration
A6 – Sensitive Data Exposure	A6 – Sensitive Data Exposure
A7 – Missing Function Level Access Control	A7 – Insufficient Attack Protection
A8 – Cross-site Request Forgery (CSRF)	A8 - Cross-site Request Forgery (CSRF)
A9 – Using Components with Known Vulnerabilities	A9 – Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	A10 – Unprotected APIs

Secure System...

A system can be considered secure when the cost of stealing its data is higher than the value of the data itself.


You are in
Bear Country
Please store all
waste and pet
food inside

Remember these steps for securing your system

- Use HTTPS
- Secure with headers
- Don’t assume everything is secure
- Don’t accept false certificates *personal security*
- Involve everyone
- Make it a habit
- Start with security in mind
- OWASP Top 10
- The biggest security risk isn’t technical, it’s people!

DATA BREACH STATISTICS

DATA RECORDS LOST OR STOLEN SINCE 2013

9,053,156,308

ONLY **4%** of breaches were "Secure Breaches" where encryption was used and the stolen data was rendered useless.

DATA RECORDS ARE LOST OR STOLEN AT THE FOLLOWING FREQUENCY

EVERY DAY	EVERY HOUR	EVERY MINUTE	EVERY SECOND
5,188,055	216,169	3,603	60
Records	Records	Records	Records

Natalia Oskina @Curl_N natalia.oskina@zuhlke.com
Rahat Khan @rahatkhan1992 rakhan@expedia.com