RSAConference2018

San Francisco | April 16 – 20 | Moscone Center

NOW MATTERS

SESSION ID: SP02-R14

ALICE IN POST-QUANTUM WONDERLAND; BOB THROUGH THE DIGITAL LOOKING-GLASS

Jon Geater

Chief Technology Officer
Thales eSecurity
@jongeater

Hold onto your hats!

- This is a very fast-paced presentation
- The idea is not to teach you everything in-depth, but to give you the right questions you can look up later
- Jumping-off points and resources will be posted to my Thales eSecurity blog and twitter after the talk – follow me @jongeater!
- Here we go…

Hold onto your hats!

- Constantly hit with new stories claiming to change the world
- Much of it is just sensationalist
  - Or simply uninformed

In other words….

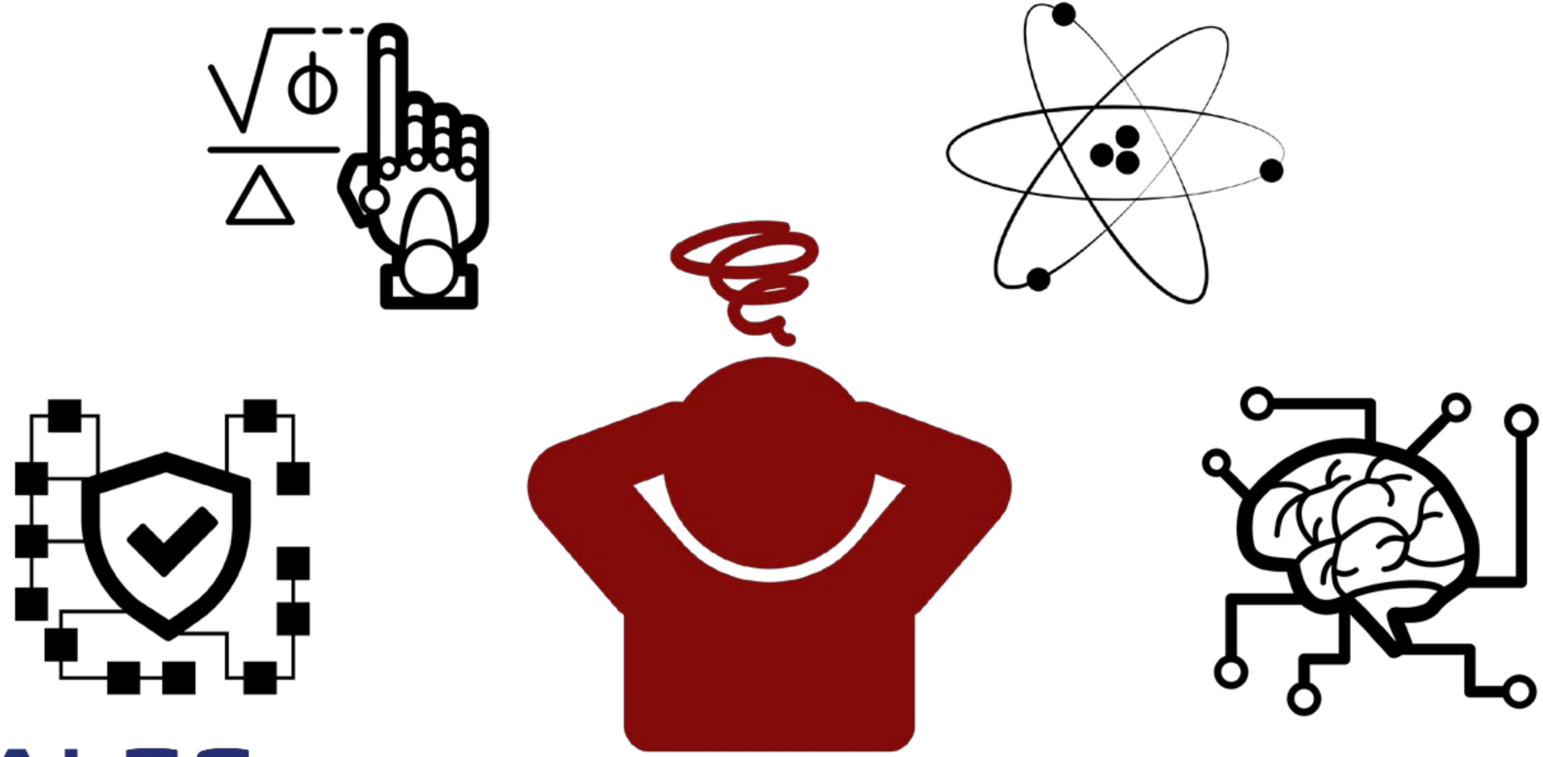
BEWARE

FAKE NEWS

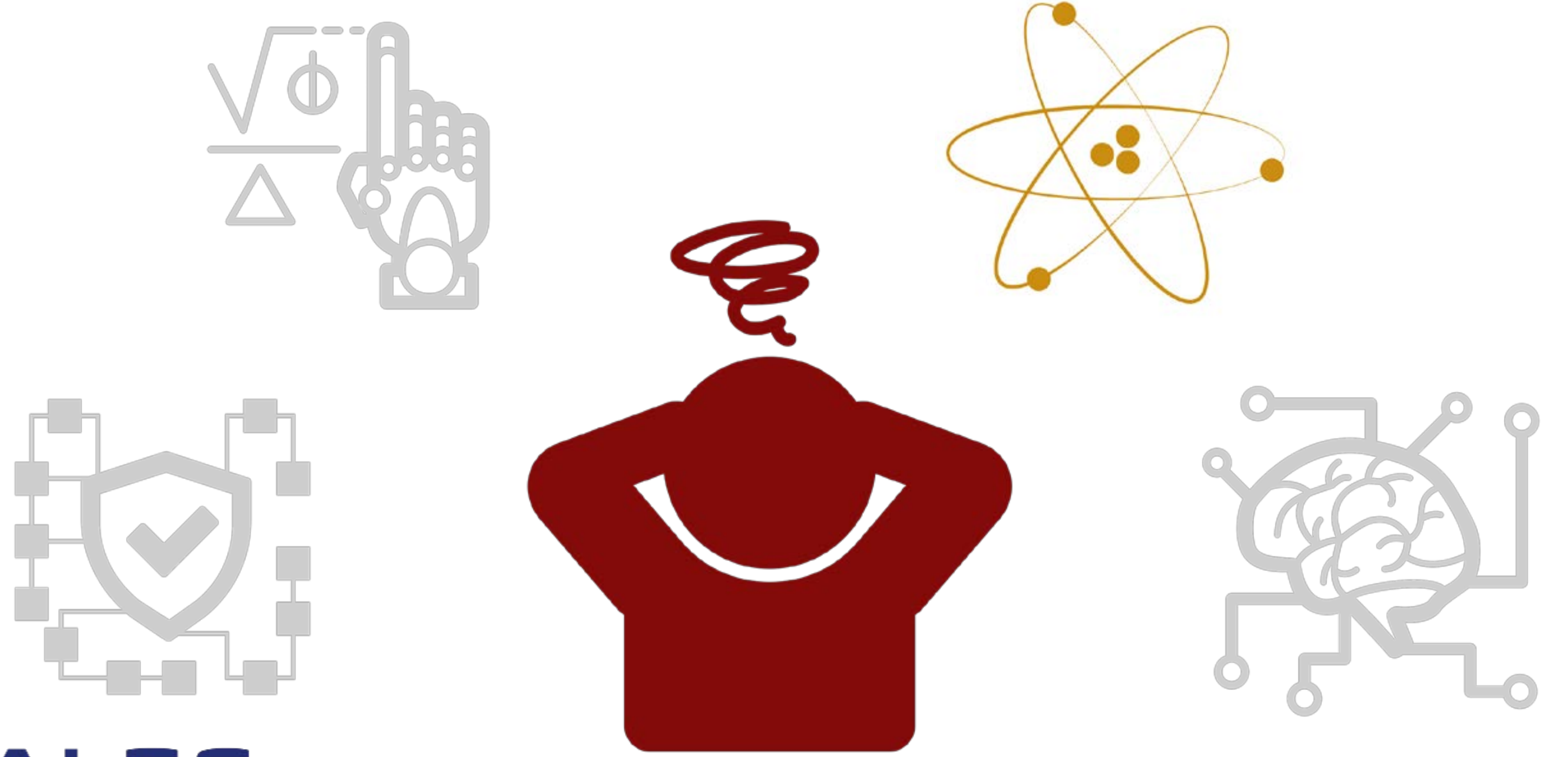
Hold onto your hats!

- Constantly hit with new stories claiming to change the world
- Much of it is just sensationalist
  - Or simply uninformed
- Nonetheless there are kernels of truth worth grabbing hold of

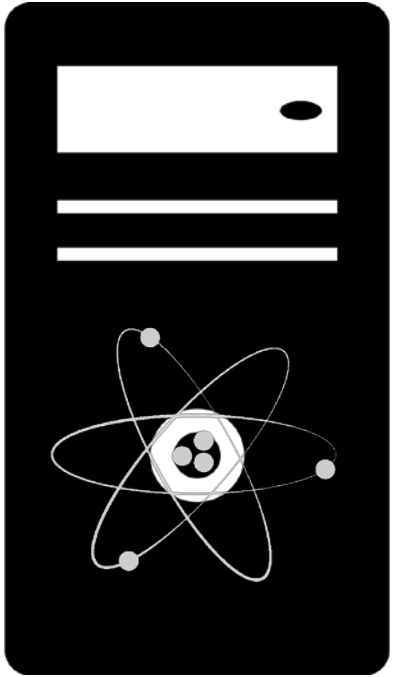
Lions, Tigers and Bears. Oh my!



First: Quantum…



Quantum Computing



Quantum Computing

- To run quantum algorithms you need a quantum computer
- It’s often suggested that quantum computers are on a path to directly replace existing computer systems, but this is not (necessarily) true.
  - Different types of quantum computing
    - — Annealing vs Universal
    - — Think valve machine vs semiconductors
  - Different machines are better specialised to different tasks
  - Don’t forget the practical aspects
- There has been some notable progress
  - IBM’s Quantum Experience
  - D-Wave

Quantum Cryptogrpahy

Quantum Cryptography

- Quantum Cryptography is effectively “doing cryptography with quantum computers”
- There are several potential techniques
- One thing that is well established is Quantum Key Distribution
  - This has almost nothing to do with Quantum Computing!
  - Transmit keys from one place to another as quantum state in photons
  - Relies on the quantum mechanical phenomenon that you cannot observe a photon without disturbing its state
  - Theoretically extremely secure, but suffers practical issues
- Famously recently used by China in satellites

Quantum Cryptanalysis

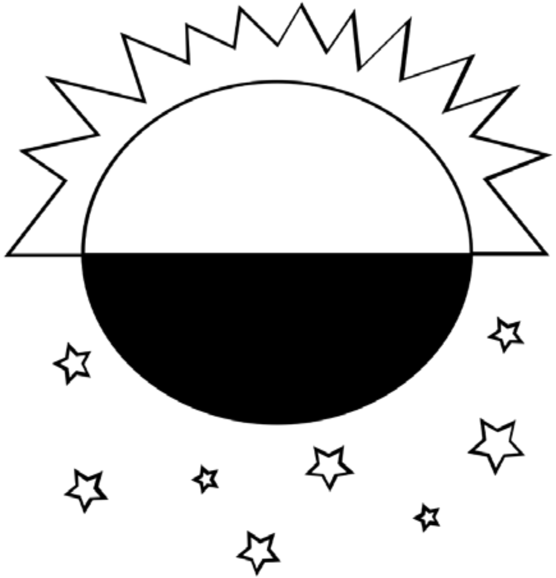
Quantum Cryptanalysis

- Quantum Cryptanalysis is effectively “breaking cryptography with quantum computers”
- Grover’s algorithm
  - Given a functioning Universal Quantum Computer, Grover’s algorithm weakens the currently assumed strength of symmetric algorithms like AES
- Shor’s algorithm
  - Given a functioning Universal Quantum Computer, Shor’s algorithm weakens the currently assumed strength of asymmetric algorithms like RSA, ECC
- This is the big threat
  - If our cryptography is broken, then everything breaks!

Quantum Cryptanalysis

- Quantum Cryptanalysis is effectively “breaking cryptography with quantum computers”
- Grover’s algorithm
  - Given a functioning Universal Quantum Computer, Grover’s algorithm weakens the currently assumed strength of symmetric algorithms like AES
- Shor’s algorithm
  - Given a functioning Universal Quantum Computer, Shor’s algorithm weakens the currently assumed strength of asymmetric algorithms like RSA, ECC
- This is the big threat
  - If our cryptography is broken, then everything breaks!

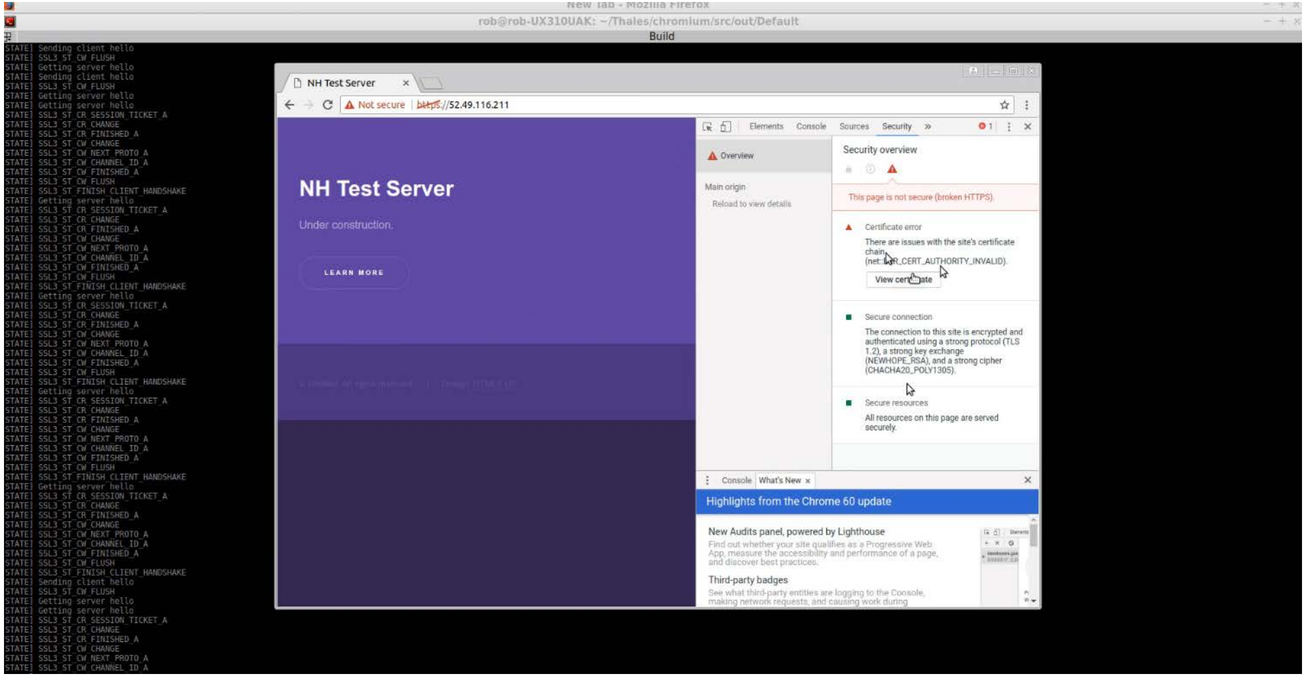
Quantum Cryptanalysis



Don’t let the Sun go down on me…

- This essentially puts a ‘sunset’ on current popular algorithms
- But this is business as usual!
  - Remember SHA-1? Single DES? DSA?
  - Remember what happened in 2010?
- But don’t jump too soon
  - Work out what your exposure is
  - Work out how long it will take for you to move
  - Balance this risk against the possibility that the new algorithms might have classical weaknesses!
  - NIST ‘competition’ going on right now

Here’s one we made earlier!



New Tab - Mozilla Firefox
rob@rob-UX310UAK: ~/Thales/chromium/src/out/Default
Build

```
STATE] Sending client hello
STATE] SSL3_ST_CW_FLUSH
STATE] Getting server hello
STATE] Sending client hello
STATE] SSL3_ST_CW_FLUSH
STATE] Getting server hello
STATE] Getting server hello
STATE] SSL3_ST_CR_SESSION_TICKET_A
STATE] SSL3_ST_CR_CHANGE
STATE] SSL3_ST_CR_FINISHED_A
STATE] SSL3_ST_CW_CHANGE
STATE] SSL3_ST_CW_NEXT_PROTO_A
STATE] SSL3_ST_CW_CHANNEL_ID_A
STATE] SSL3_ST_CW_FINISHED_A
STATE] SSL3_ST_CW_FLUSH
STATE] SSL3_ST_FINISH_CLIENT_HANDSHAKE
STATE] Getting server hello
STATE] SSL3_ST_CR_SESSION_TICKET_A
STATE] SSL3_ST_CR_CHANGE
STATE] SSL3_ST_CR_FINISHED_A
STATE] SSL3_ST_CW_CHANGE
STATE] SSL3_ST_CW_NEXT_PROTO_A
STATE] SSL3_ST_CW_CHANNEL_ID_A
STATE] SSL3_ST_CW_FINISHED_A
STATE] SSL3_ST_CW_FLUSH
STATE] SSL3_ST_FINISH_CLIENT_HANDSHAKE
STATE] Getting server hello
STATE] SSL3_ST_CR_SESSION_TICKET_A
STATE] SSL3_ST_CR_CHANGE
STATE] SSL3_ST_CR_FINISHED_A
STATE] SSL3_ST_CW_CHANGE
STATE] SSL3_ST_CW_NEXT_PROTO_A
STATE] SSL3_ST_CW_CHANNEL_ID_A
STATE] SSL3_ST_CW_FINISHED_A
STATE] SSL3_ST_CW_FLUSH
STATE] SSL3_ST_FINISH_CLIENT_HANDSHAKE
STATE] Getting server hello
STATE] SSL3_ST_CR_SESSION_TICKET_A
STATE] SSL3_ST_CR_CHANGE
STATE] SSL3_ST_CR_FINISHED_A
STATE] SSL3_ST_CW_CHANGE
STATE] SSL3_ST_CW_NEXT_PROTO_A
STATE] SSL3_ST_CW_CHANNEL_ID_A
STATE] SSL3_ST_CW_FINISHED_A
STATE] SSL3_ST_CW_FLUSH
STATE] SSL3_ST_FINISH_CLIENT_HANDSHAKE
STATE] Getting server hello
STATE] SSL3_ST_CR_SESSION_TICKET_A
STATE] SSL3_ST_CR_CHANGE
STATE] SSL3_ST_CR_FINISHED_A
STATE] SSL3_ST_CW_CHANGE
STATE] SSL3_ST_CW_NEXT_PROTO_A
STATE] SSL3_ST_CW_CHANNEL_ID_A
STATE] SSL3_ST_CW_FINISHED_A
STATE] SSL3_ST_CW_FLUSH
STATE] SSL3_ST_FINISH_CLIENT_HANDSHAKE
STATE] Sending client hello
STATE] SSL3_ST_CW_FLUSH
STATE] Getting server hello
STATE] Getting server hello
STATE] SSL3_ST_CR_SESSION_TICKET_A
STATE] SSL3_ST_CR_CHANGE
STATE] SSL3_ST_CR_FINISHED_A
STATE] SSL3_ST_CW_CHANGE
STATE] SSL3_ST_CW_NEXT_PROTO_A
STATE] SSL3_ST_CW_CHANNEL_ID_A
```

NH Test Server

Under construction.

Security overview

This page is not secure (broken HTTPS).

▲ Certificate error

There are issues with the site's certificate chain (net::ERR_CERT_AUTHORITY_INVALID).

■ Secure connection

The connection to this site is encrypted and authenticated using a strong protocol (TLS 1.2), a strong key exchange (NEWHOPE_RSA), and a strong cipher (CHACHA20_POLY1305).

■ Secure resources

All resources on this page are served securely.

Highlights from the Chrome 60 update

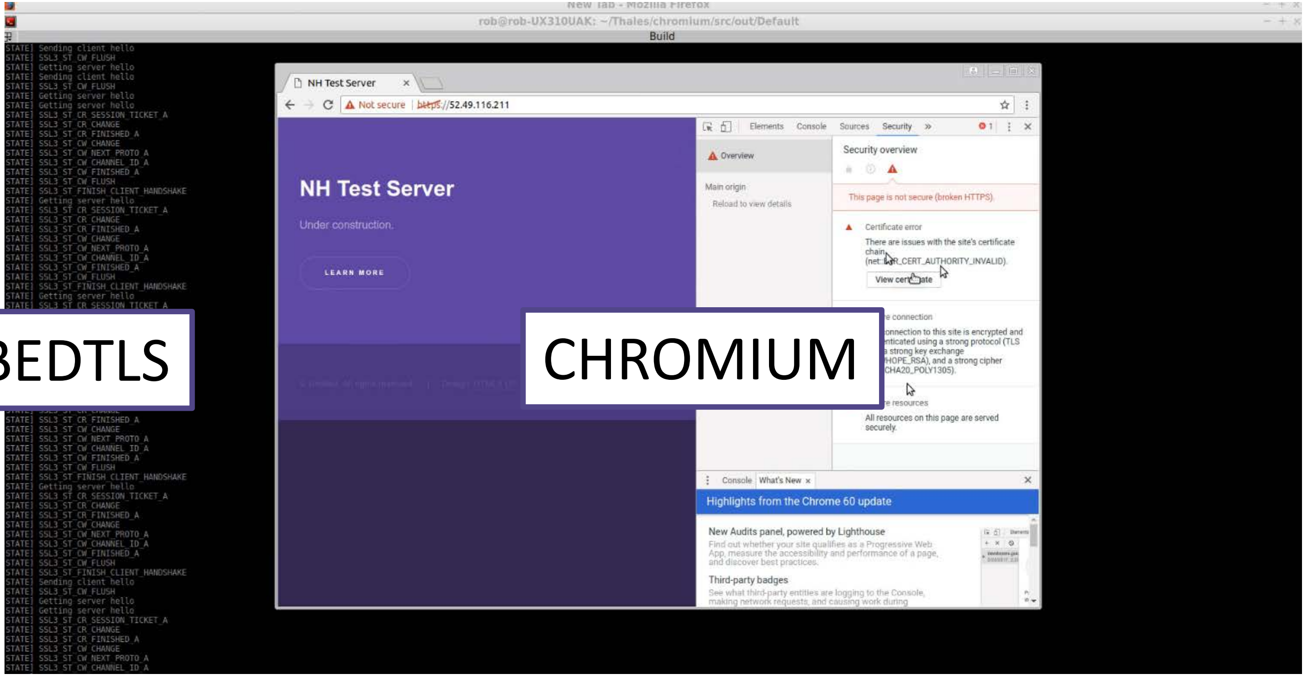
New Audits panel, powered by Lighthouse

Find out whether your site qualifies as a Progressive Web App, measure the accessibility and performance of a page, and discover best practices.

Third-party badges

See what third-party entities are logging to the Console, making network requests, and causing work during

Here’s one we made earlier!



```
STATE] Sending client hello
STATE] SSL3_ST_CW_FLUSH
STATE] Getting server hello
STATE] Sending client hello
STATE] SSL3_ST_CW_FLUSH
STATE] Getting server hello
STATE] Getting server hello
STATE] SSL3_ST_CR_SESSION_TICKET_A
STATE] SSL3_ST_CR_CHANGE
STATE] SSL3_ST_CR_FINISHED_A
STATE] SSL3_ST_CW_CHANGE
STATE] SSL3_ST_CW_NEXT_PROTO_A
STATE] SSL3_ST_CW_CHANNEL_ID_A
STATE] SSL3_ST_CW_FINISHED_A
STATE] SSL3_ST_CW_FLUSH
STATE] SSL3_ST_FINISH_CLIENT_HANDSHAKE
STATE] Getting server hello
STATE] SSL3_ST_CR_SESSION_TICKET_A
STATE] SSL3_ST_CR_CHANGE
STATE] SSL3_ST_CR_FINISHED_A
STATE] SSL3_ST_CW_CHANGE
STATE] SSL3_ST_CW_NEXT_PROTO_A
STATE] SSL3_ST_CW_CHANNEL_ID_A
STATE] SSL3_ST_CW_FINISHED_A
STATE] SSL3_ST_CW_FLUSH
STATE] SSL3_ST_FINISH_CLIENT_HANDSHAKE
STATE] Getting server hello
STATE] SSL3_ST_CR_SESSION_TICKET_A
```

```
STATE] SSL3_ST_CR_FINISHED_A
STATE] SSL3_ST_CW_CHANGE
STATE] SSL3_ST_CW_NEXT_PROTO_A
STATE] SSL3_ST_CW_CHANNEL_ID_A
STATE] SSL3_ST_CW_FINISHED_A
STATE] SSL3_ST_CW_FLUSH
STATE] SSL3_ST_FINISH_CLIENT_HANDSHAKE
STATE] Getting server hello
STATE] SSL3_ST_CR_SESSION_TICKET_A
STATE] SSL3_ST_CR_CHANGE
STATE] SSL3_ST_CR_FINISHED_A
STATE] SSL3_ST_CW_CHANGE
STATE] SSL3_ST_CW_NEXT_PROTO_A
STATE] SSL3_ST_CW_CHANNEL_ID_A
STATE] SSL3_ST_CW_FINISHED_A
STATE] SSL3_ST_CW_FLUSH
STATE] SSL3_ST_FINISH_CLIENT_HANDSHAKE
STATE] Sending client hello
STATE] SSL3_ST_CW_FLUSH
STATE] Getting server hello
STATE] Getting server hello
STATE] SSL3_ST_CR_SESSION_TICKET_A
STATE] SSL3_ST_CR_CHANGE
STATE] SSL3_ST_CR_FINISHED_A
STATE] SSL3_ST_CW_CHANGE
STATE] SSL3_ST_CW_NEXT_PROTO_A
STATE] SSL3_ST_CW_CHANNEL_ID_A
```

NH Test Server

Under construction.

This page is not secure (broken HTTPS).

Certificate error

There are issues with the site's certificate chain (net::ERR_CERT_AUTHORITY_INVALID).

e connection

onnection to this site is encrypted and enticated using a strong protocol (TLS a strong key exchange HOPE_RSA), and a strong cipher CHA20_POLY1305).

e resources

All resources on this page are served securely.

Highlights from the Chrome 60 update

New Audits panel, powered by Lighthouse

Find out whether your site qualifies as a Progressive Web App, measure the accessibility and performance of a page, and discover best practices.

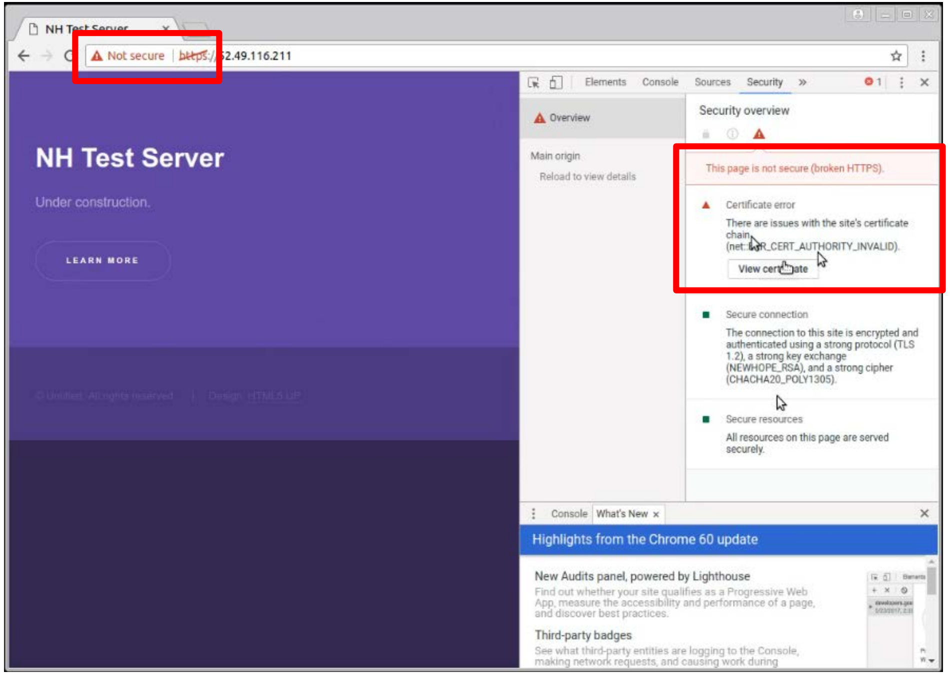
Third-party badges

See what third-party entities are logging to the Console, making network requests, and causing work during

MBEDTLS

CHROMIUM

Here’s one we made earlier!



NH Test Server

Under construction.

© Untitled. All rights reserved. | Design: HTML5 UP

Security overview

This page is not secure (broken HTTPS).

Certificate error

There are issues with the site's certificate chain (net::ERR_CERT_AUTHORITY_INVALID).

View certificate

Secure connection

The connection to this site is encrypted and authenticated using a strong protocol (TLS 1.2), a strong key exchange (NEWHOPE_RSA), and a strong cipher (CHACHA20_POLY1305).

Secure resources

All resources on this page are served securely.

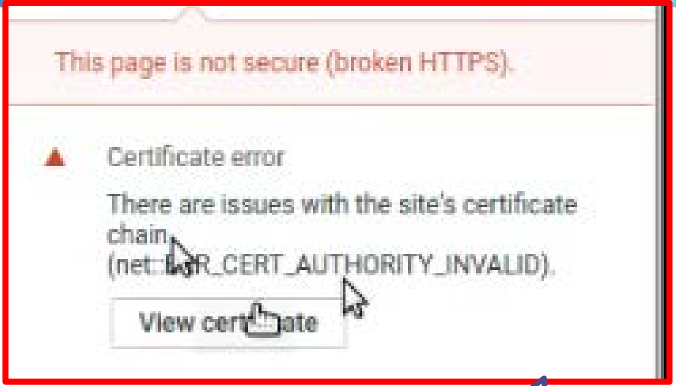
Highlights from the Chrome 60 update

New Audits panel, powered by Lighthouse

Find out whether your site qualifies as a Progressive Web App, measure the accessibility and performance of a page, and discover best practices.

Third-party badges

See what third-party entities are logging to the Console, making network requests, and causing work during



This page is not secure (broken HTTPS).

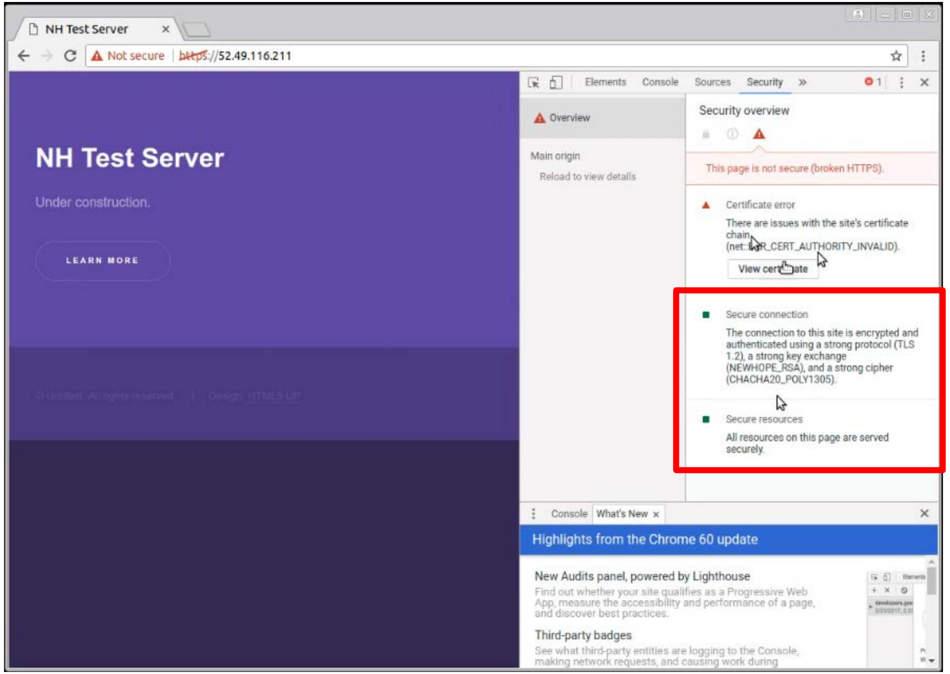
Certificate error

There are issues with the site's certificate chain. (net::ERR_CERT_AUTHORITY_INVALID).

View certificate

Don’t worry about this: it’s just a lack of root issuer certificate…part of the transition pain.

Here’s one we made earlier!



NH Test Server

Under construction.

© Untitled. All rights reserved. | Design: HTML5 UP

Security overview

This page is not secure (broken HTTPS).

Main origin

Reload to view details

Certificate error

There are issues with the site's certificate chain (net::ERR_CERT_AUTHORITY_INVALID).

Secure connection

The connection to this site is encrypted and authenticated using a strong protocol (TLS 1.2), a strong key exchange (NEWHOPE_RSA), and a strong cipher (CHACHA20_POLY1305).

Secure resources

All resources on this page are served securely.

Highlights from the Chrome 60 update

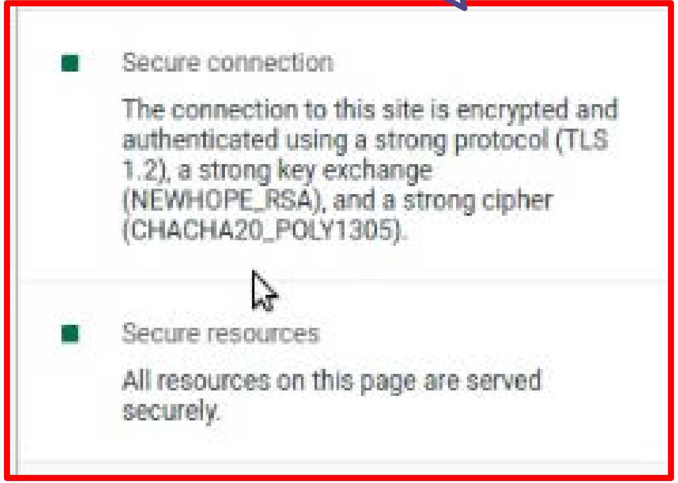
New Audits panel, powered by Lighthouse

Find out whether your site qualifies as a Progressive Web App, measure the accessibility and performance of a page, and discover best practices.

Third-party badges

See what third-party entities are logging to the Console, making network requests, and causing work during

This is the important part: All resources served securely with NEWHOPE and CHACHA



Secure connection

The connection to this site is encrypted and authenticated using a strong protocol (TLS 1.2), a strong key exchange (NEWHOPE_RSA), and a strong cipher (CHACHA20_POLY1305).

Secure resources

All resources on this page are served securely.

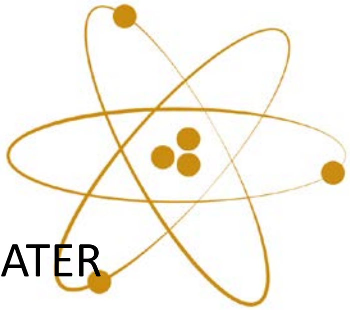
Quantum Computing and Security

The fundamentals

- Several different quantum-related technologies are often reported together. They are NOT the same!
- RSA and ECC are the place to concentrate on replacements
- Chances of needing PQC by 2031 rated as high a 50%

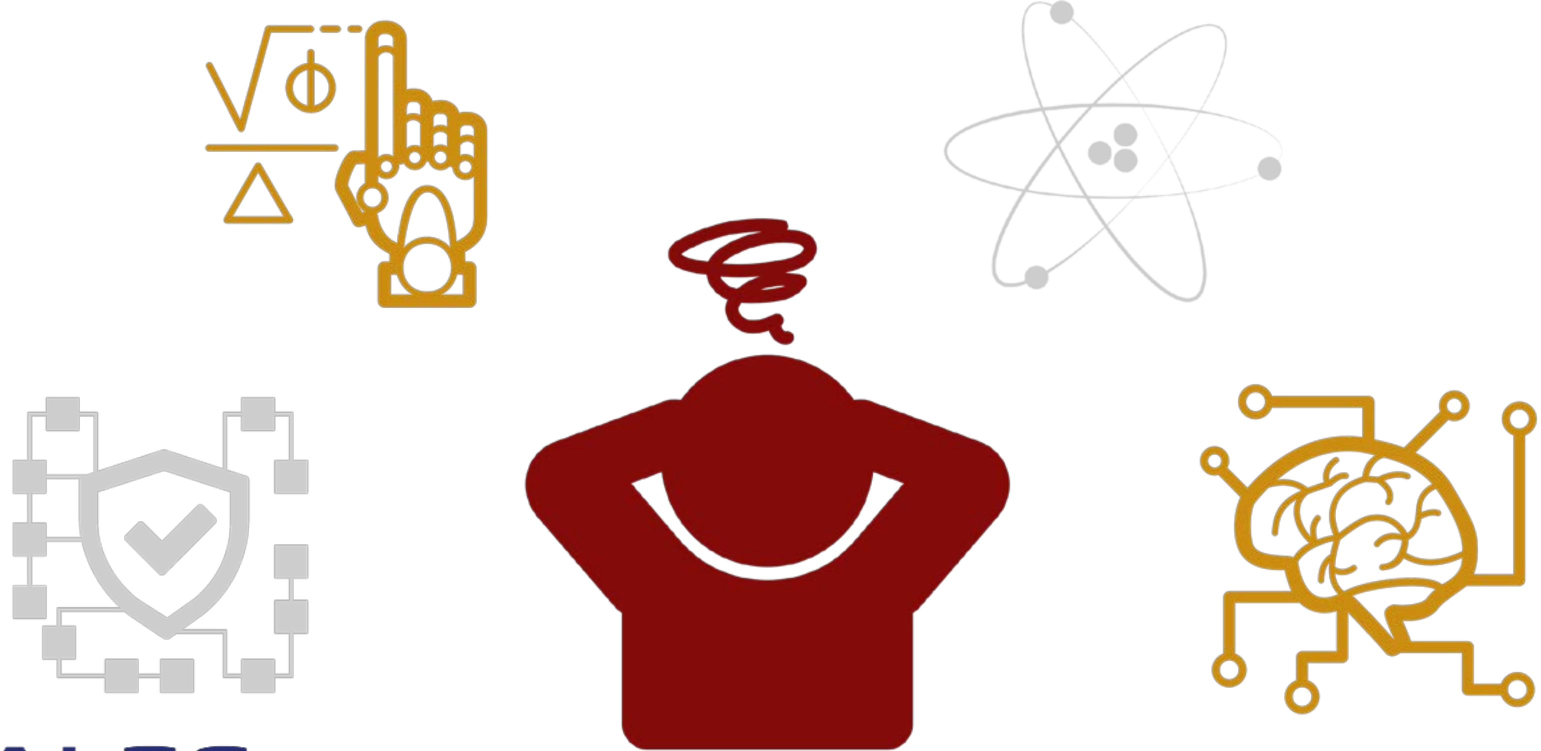
Why it matters to security

- Some of the technology is security-enhancing, some very much not
- I hope this is obvious!
- Data security lifetime is important! Remember adversaries can collect traffic NOW and break LATER



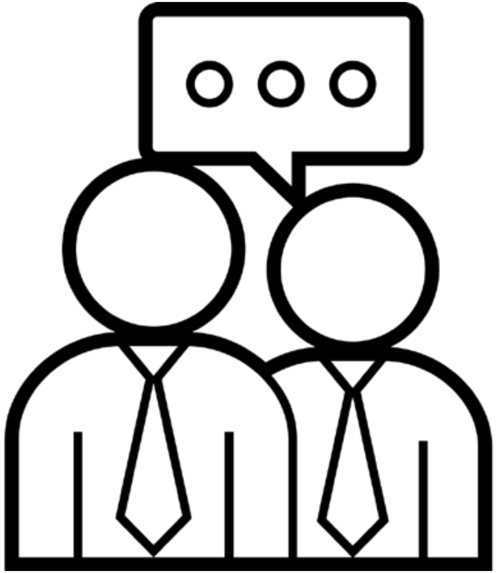
NEXT UP…

Next: Machine Learning, AI, …



Relationship with Big Data

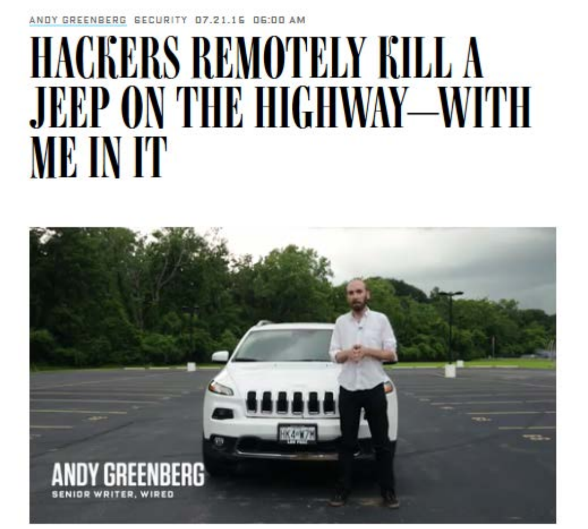
All things to all men



A favourite example: Connected Car

A favourite example: Connected Car

https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/



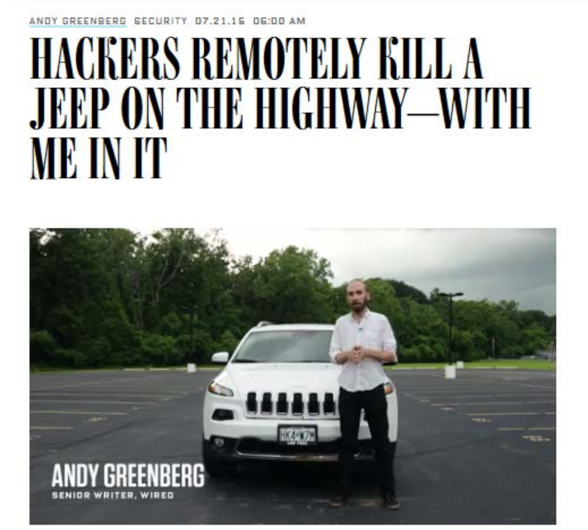
ANDY GREENBERG SECURITY 07.21.15 06:00 AM

HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT

ANDY GREENBERG
SENIOR WRITER, WIRED

A favourite example: Connected Car

https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/



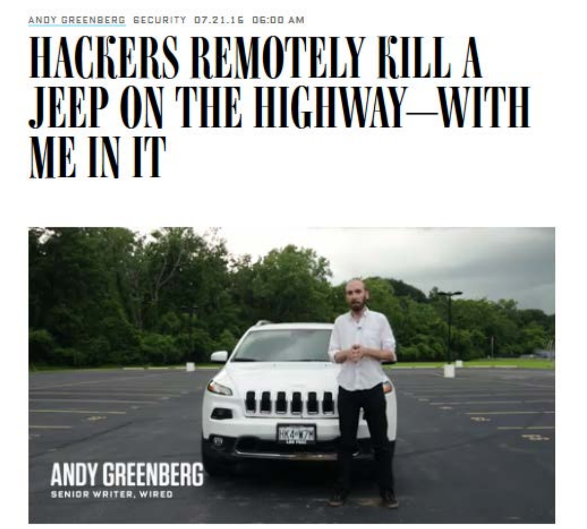
ANDY GREENBERG SECURITY 07.21.15 06:00 AM

HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT

ANDY GREENBERG
SENIOR WRITER, WIRED

A favourite example: Connected Car

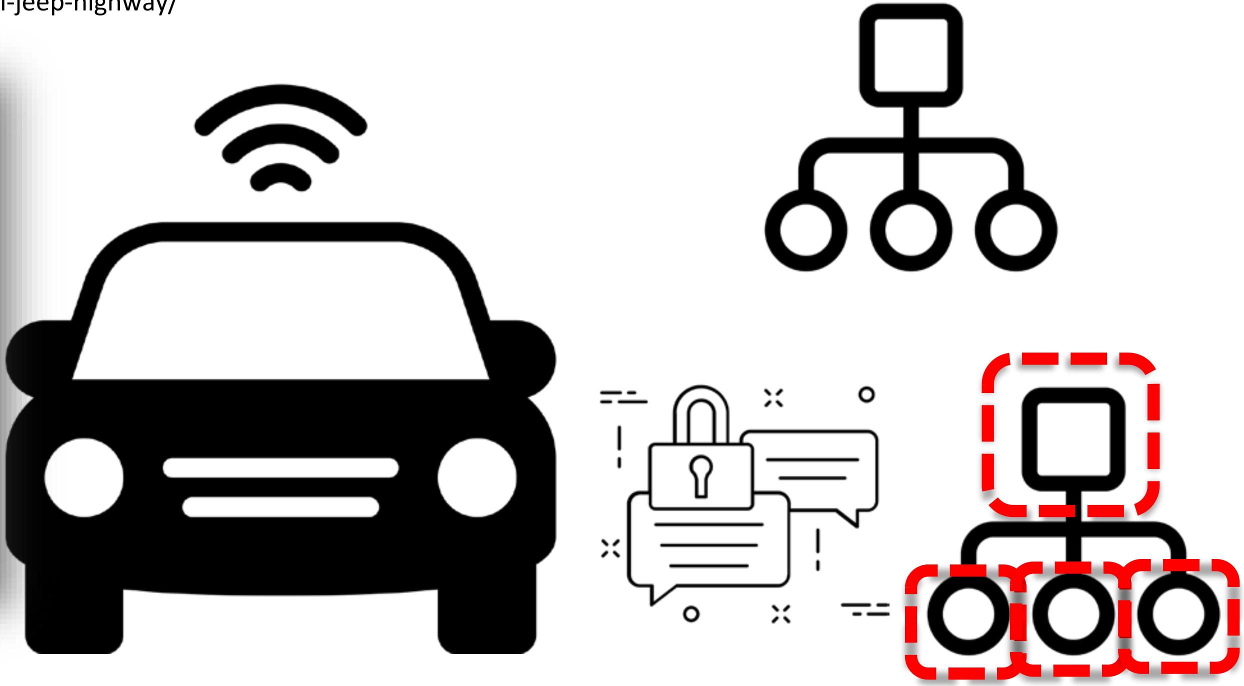
https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/



ANDY GREENBERG SECURITY 07.21.15 06:00 AM

HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT

ANDY GREENBERG
SENIOR WRITER, WIRED



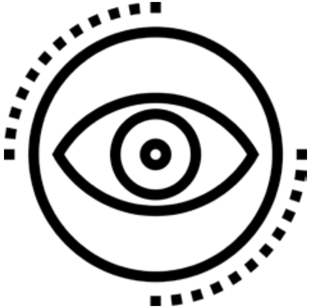
A favourite example: Connected car

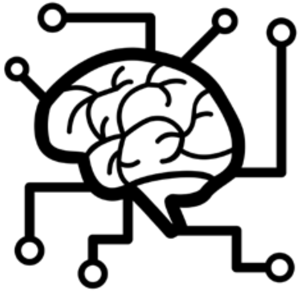
A favourite example: Connected car

UKAutodrive

A favourite example: Connected car

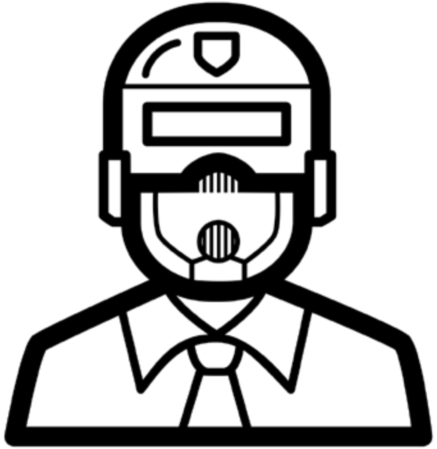
UKAutodrive

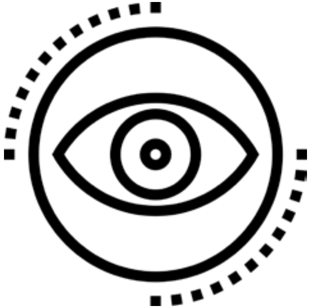


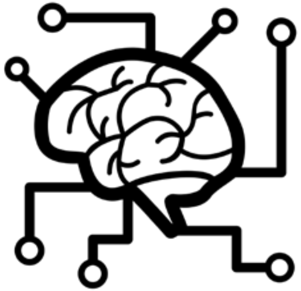


A favourite example: Connected car

UKAutodrive







Artificial Intelligence and Security

The fundamentals

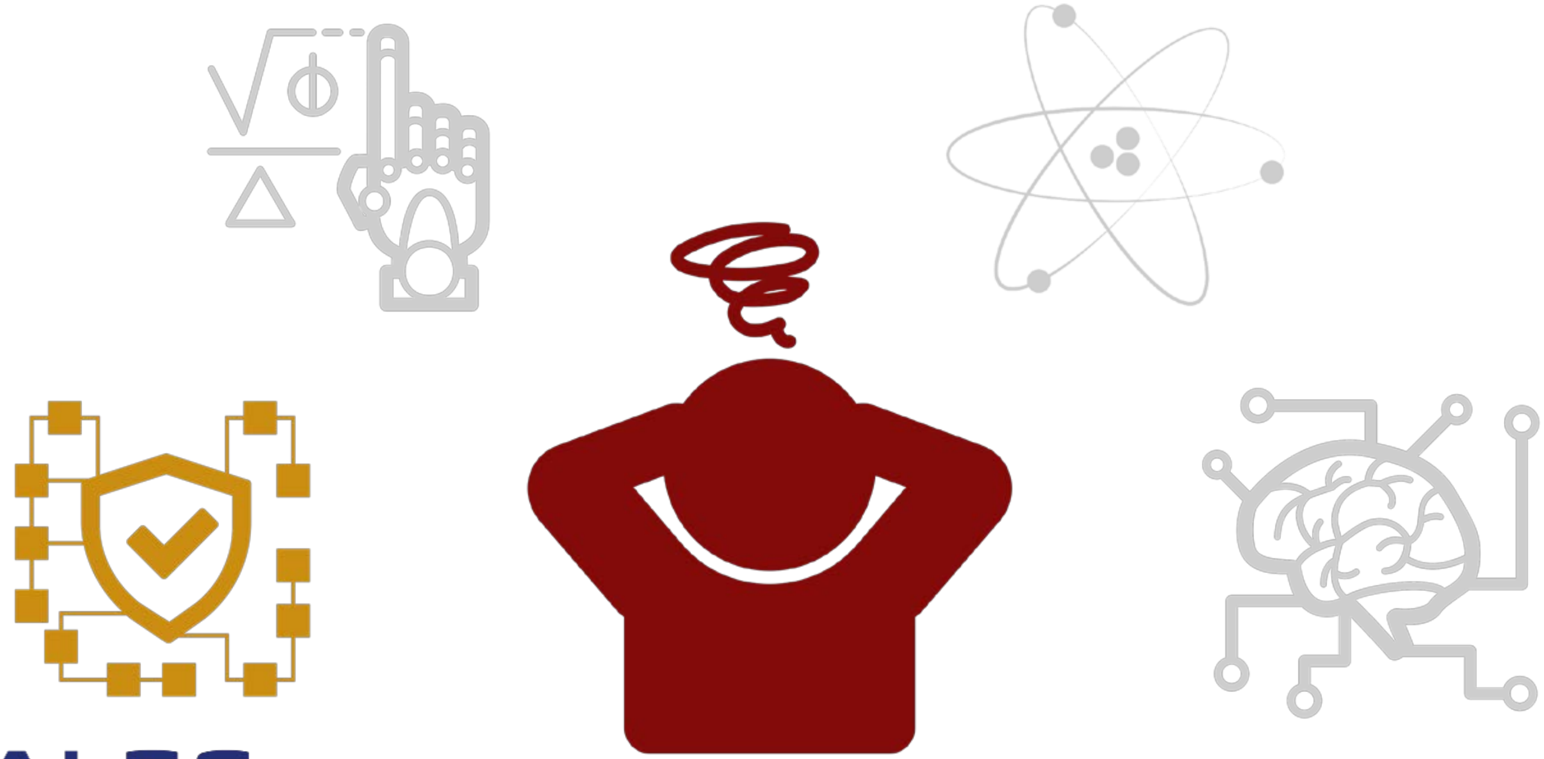
- This is another area where multiple very different technologies are often conflated
- Input and Training Data become more important than the program
- Overlaying with traditional systems is most effective for now

Why it matters to security

- Risk of conferring benefits of all on one: systems will fail
- We don't know how to apply certification to this type of system
- Don't substitute out existing best practice just yet!

NEXT UP…

Last but not least: Blockchain…



One of the biggest problems with blockchain

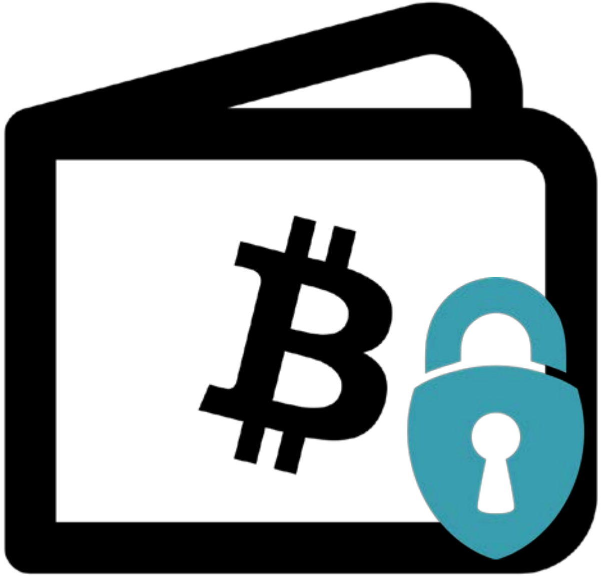
One of the biggest problems with blockchain

FOMO

Bitcoin

Not Bitcoin

Bitcoin hacks

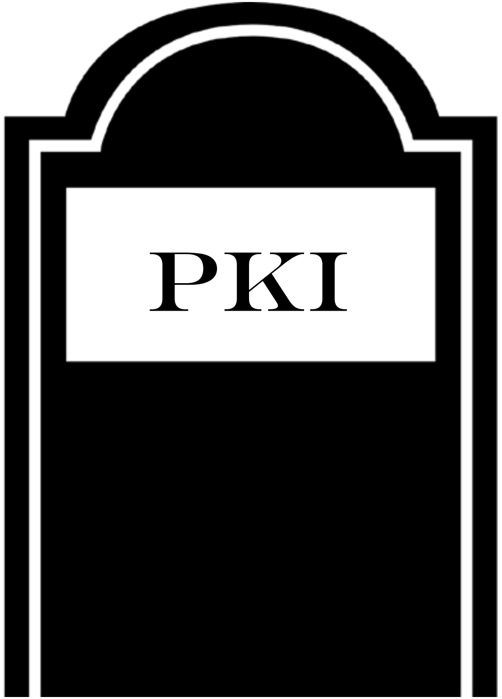


Bitcoin hacks

Bitcoin hacks

https://magoo.github.io/Blockchain-Graveyard/

The end of PKI?



Blockchain security addressed

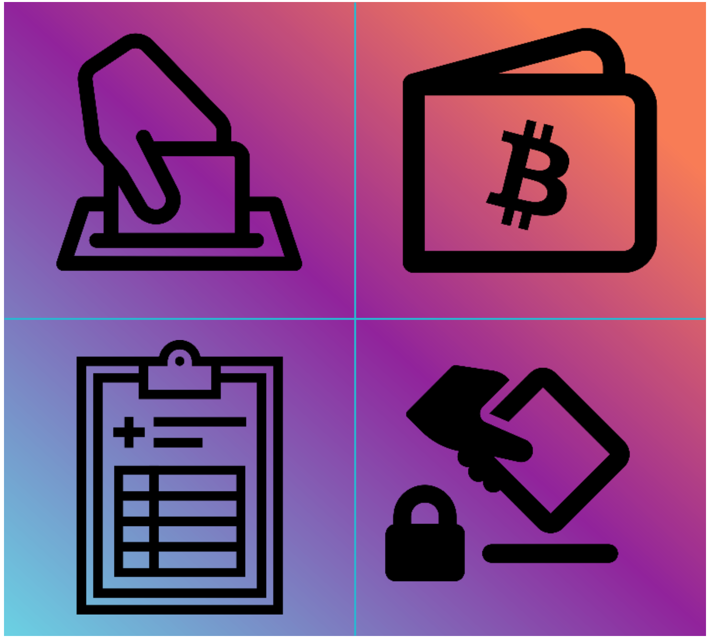
Enterprise use

	PERMISSIONED	PERMISSIONLESS
PUBLIC	ALL CAN VIEW WRITE RESTRICTED	ALL CAN VIEW ALL CAN WRITE
PRIVATE	VIEW RESTRICTED WRITE RESTRICTED	VIEW RESTRICTED ALL CAN WRITE

Enterprise use

PUBLIC

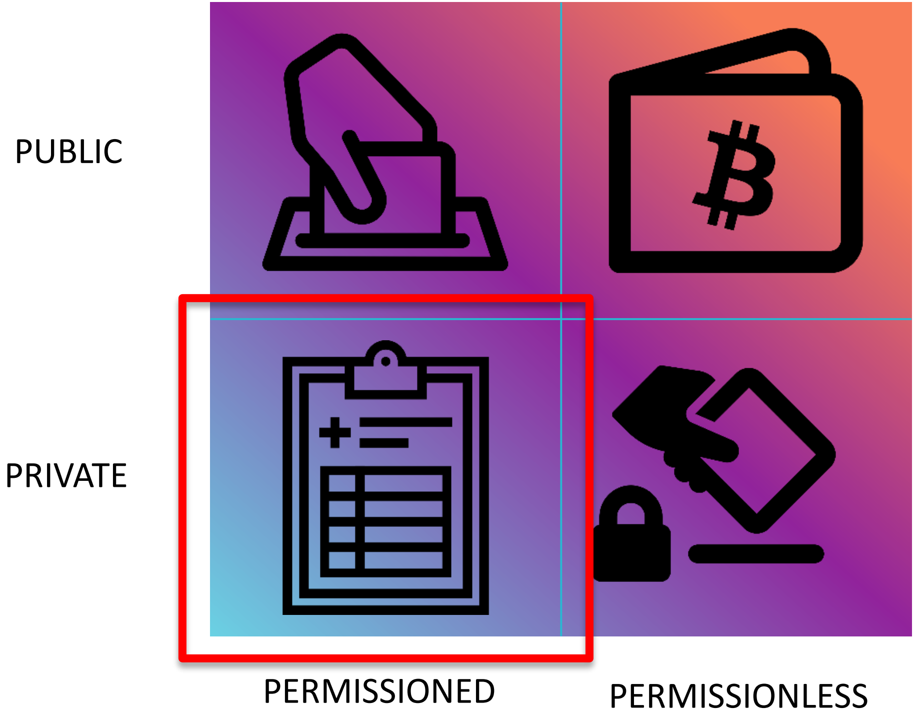
PRIVATE



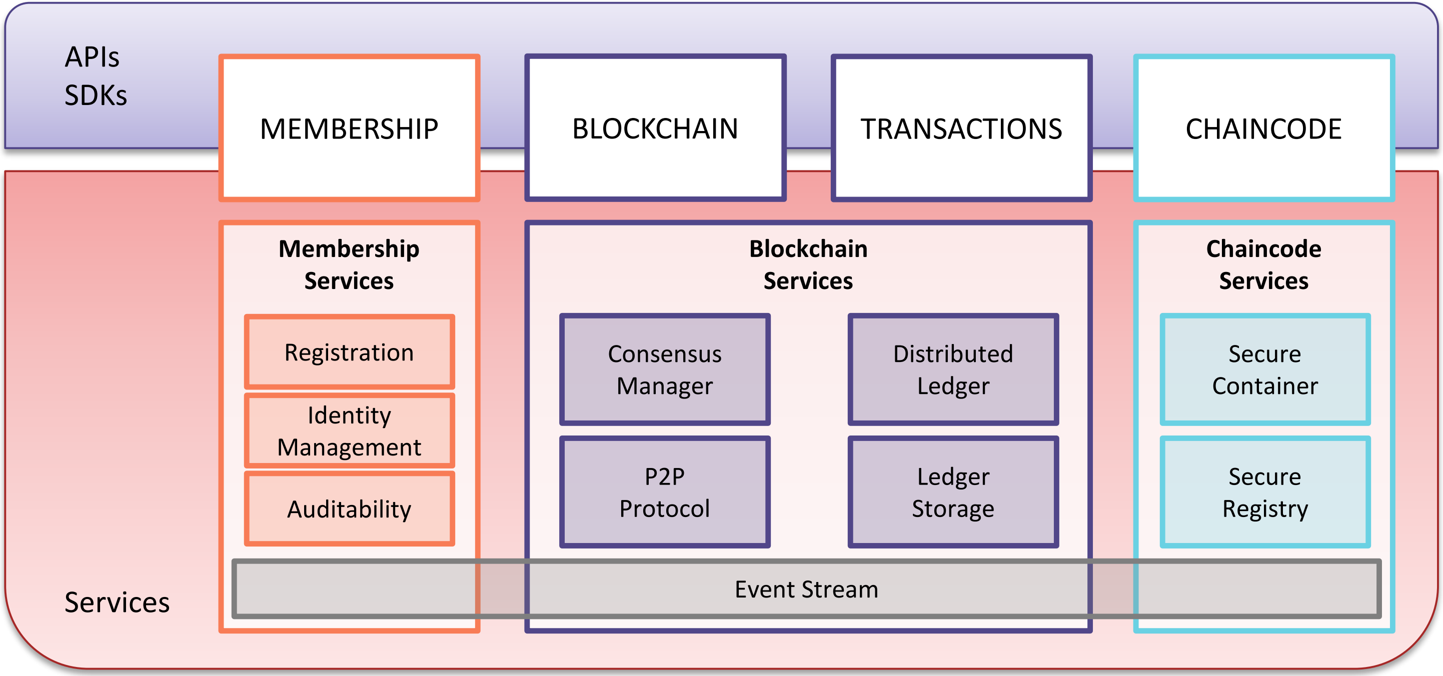
PERMISSIONED

PERMISSIONLESS

Enterprise use



Example: Hyperledger Fabric Architecture



Blockchain and security

The fundamentals

- Blockchain is not bitcoin
- Blockchain is not magic
- Just because it’s on the ledger, doesn’t make it true
- Crypto protection is *vital*

Why it matters to security

- Focus on private/permissioned
- We still have to build system security just the same as we did before
- Data security is still vital: maybe more so than before because of non-repudiation. Blockchain does A, not CI
- As ever

TAKE-AWAYS

Key take-aways

HOW WE BUILD SYSTEMS IS FUNDAMENTALLY CHANGING

Key take-aways

EVERYTHING YOU KNOW IS WRONG

Key take-aways

EVERYTHING YOU KNOW IS NOT WRONG

Key take-aways

- Quantum Crypto:
  - Remember the difference between the different technologies
  - Don’t panic, but do plan! Take this as a nudge to do standard good transition planning
  - Existing best practice still applies. Remember PQC only brings you back up to 256-bit (ish)
- Machine learning & AI
  - This absolutely will change the world of safety and security…but there’s a way to go yet
  - Whole system approach – including humans and classic apps – is essential
  - Attack focus shifts from the application to the data and/or training set
- Blockchain
  - Don’t feel compelled to use it!
  - The difference between public and private ledgers is *huge*. Don’t think about Bitcoin.
  - Crypto key protection is *even more sensitive* than it was before

Apply What You Have Learned Today

- Don’t forget the fundamentals
  - Identify your business problems before looking for solutions
  - Don’t panic
- Look to deploy these techniques over the next few years
  - As part of larger systems. None of them is a Silver Bullet
- Always concentrate on the cryptographic data security
  - Whether training sets or big data for AI, or a shadow data store for a blockchain, the need for strong crypto is growing!
  - Invest in flexible and strong cryptographic key management systems

THANK YOU!

Questions? Comments?