An Infosec Timeline

Noteworthy Events from 1970 to 2050

Well, almost,
we will begin in 1971

A prophetic retrospective
by Dr.-Ing. Mario Heiderich
mario@cure53.de || Signal: +49 1520 8675782

cure53

Our Dear Speaker

- **Dr.-Ing. Mario Heiderich**
  - **Ex-Researcher and now Lecturer, Ruhr-Uni Bochum**
    - PhD Thesis about Client Side Security and Defense
  - **Founder & Director of Cure53**
    - Pentest- & Security-Firm located in Berlin
    - Security, Consulting, Workshops, Trainings
    - Simply the Best Company in the World
  - **Published Author and Speaker**
    - Specialized on HTML5, DOM and SVG Security
    - JavaScript, XSS and Client Side Attacks
  - **Maintains DOMPurify**
    - A top notch JS-only Sanitizer, also, couple of other projects
  - **Considers this his worst talk so far**
    - mario@cure53.de
    - +49 1520 8675782

cure53

Let us first see who is here tonight.

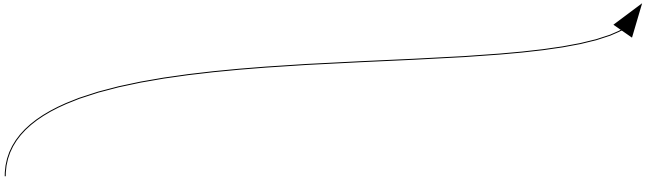
Penetration Testers?

Developers & Defenders?

ISOs & CISOs?

Bug Bounty Hunters?

Psychics?



Keine?
Keine mehr?
Gar keine?
Zwei?

Talk Structure

Act One: The Past

In which the dear speaker will mention
past events of great relevance

Act Two: The Future

In which the dear speaker will share with us
his awkwardly specific visions and prophecies

Also

No plans for tonight? Win a party ticket!

The three “smartest” questions during ~~or after~~ the talk
Will win you a ticket for the **Private Party**.

There might be beer.

Act One

The Past

Where everything was better because our brain says so

1971

1971

- The first actual computer worm, Creeper was created
  - Its author Bob Thomas made it “bounce” between machines
  - It was more or less non-malicious, it just.. “bounced”
  - It left a message, saying “I’m the creeper: catch me if you can.”
- It led to the creation of “Reaper”
  - Reaper was the first actual Anti-Virus (AV) software
  - It was created by Ray Tomlinson to move across networks
  - It then deleted the self-replicating Creeper worm

1980

1980

- The first actual Intrusion Detection System was created
  - James Anderson, over at National Security Agency, came up with the idea for an IDS and delivered an implementation
  - Basically, a set of tools intended to help administrators review user access logs, file access logs and system event logs
- The infamous group “The 414s” was founded
  - “Young, male, intelligent, highly motivated and energetic"
  - A bunch of Milwaukee Teenagers much into early hacking
  - Number 414 being the Milwaukee telephone area code
  - Likely the first “hackers” who caused financial damage by deleting billing records, oh no, terrible!

1981

Celebrating "being dressed really well". Good times.

1981

- Our dear speaker was born
  - Nothing else of relevance is said to have happened that year
  - Nothing else of relevance for the next five years either

1986

Warum liegt da überhaupt Stroh?

1986, oh boy

- Astronomer Cliff Stoll captures Markus Hess
  - Markus Hess, German hacker and KGB recruit
  - Markus went wild on stealing passwords, tried to infiltrate US military systems, maybe even succeeded
  - Clifford Paul "Cliff" Stoll put up a Honeypot and that lead to catching the spy
- A lot of things happened for the first time
  - First documented politically motivated hack
  - First documented use of a honeypot in cyber crime
  - First documented use of cyber forensics

More 1986

- The first actual IDS design is being modeled
  - Dorothy E. Denning did it, assisted by Peter G. Neumann
  - Their design is still foundation for modern systems as we know them today
  - Released by SRI as “Intrusion Detection Expert System” (IDES)
  - It would look at both user- and network-level data
- Check out the paper!
  - https://homepages.laas.fr/owe/METROSEC/DOC/ides.pdf

1987

No sh*t, 1987

- Computer Scientist Fred Cohen noted the following
  - “It is impossible to detect an intrusion in every case, and that the resources needed to detect intrusions grow with the amount of usage.”
  - Really!
- As a side note, Wikipedia claims…
  - “Cohen also believed there are positive viruses and he had created one called the compression virus which spreading would infect all executable files on a computer, not to destroy, but to make them smaller.”

1988

1988

- The year when Robert Morris had an excellent idea
  - He wanted to measure the size of the Internet
  - To do this, he wrote a program designed to propagate across networks, infiltrate Unix terminals using a known bug, and then copy itself
  - This last instruction proved to be not such a great idea
  - His tool replicated so aggressively that it almost took down the entire Internet. Meet the "Morris Worm"
- Years later, Samy Kamkar came up with a similar idea
  - But let's wait for the 2005 slide shall we

1989

The Backstreet Boys of heavy metal, some say

1989

Anyone here still remembers?

- AIDS, a.k.a “Aids Info Disk” or “PC Cyborg” Trojan
  - The first crypto trojan was born. In 1989. It even had an EULA.
  - It was a trojan horse that replaced the `AUTOEXEC.BAT` file
  - After 90 reboots, yes 90, AIDS hid directories and encrypted names of all files
  - People had to send 189$ USD to a post office box in Panama to get their stuff back
- Morris Worm Aftermath and estimated costs
  - The U.S. Government Accountability Office put the cost of the damage between $100,000 USD – $10,000,000 USD
  - Apparently this is very very hard to calculate accurately
  - And again, Astronomer Clifford “Cliff” Stoll saves the day and mitigates
  - “These machines were dead in the water - useless until disinfected. And removing the virus often took two days.”

1990

§ 1990

- Things go serious, hacking becomes illegal
  - One of the first pieces of legislation in history that dealt with cyber security was The Computer Misuse Act
  - This act passed in 1990 in the United Kingdom
  - It effectively made any unauthorized attempts to access computer systems illegal
  - This piece of legislation has been active for years by now, with additional amendments modernizing the act

1991

1991

- The AV industry starts booming, massively so
  - Hundreds of products flood the market - and all do the same
  - Matching the checksum of a binary against a large database of “signatures”
  - Later on, string searches inside binaries for suspicious data were added as well
  - False positives, intense resource use, resulting user frustration and interference with user productivity often were the result
  - The software sold nevertheless

1994

It was the nineties, I mean,
come on… there is worse!

Om nom nom 1994

- Something magic happened to the web
  - Lou Montulli and John Giannandrea write the initial Netscape Cookie Specification
  - Version 0.9-beta of Mosaic Netscape, released on October 13, 1994, first supported those cookies
  - Montulli applied for a patent for the cookie technology in 1995, and US 5774670 was granted in 1998
  - Support for cookies was added to Internet Explorer 2.0, released in October 1995
- This changed the web as we knew it back then
  - Only no one noticed, really

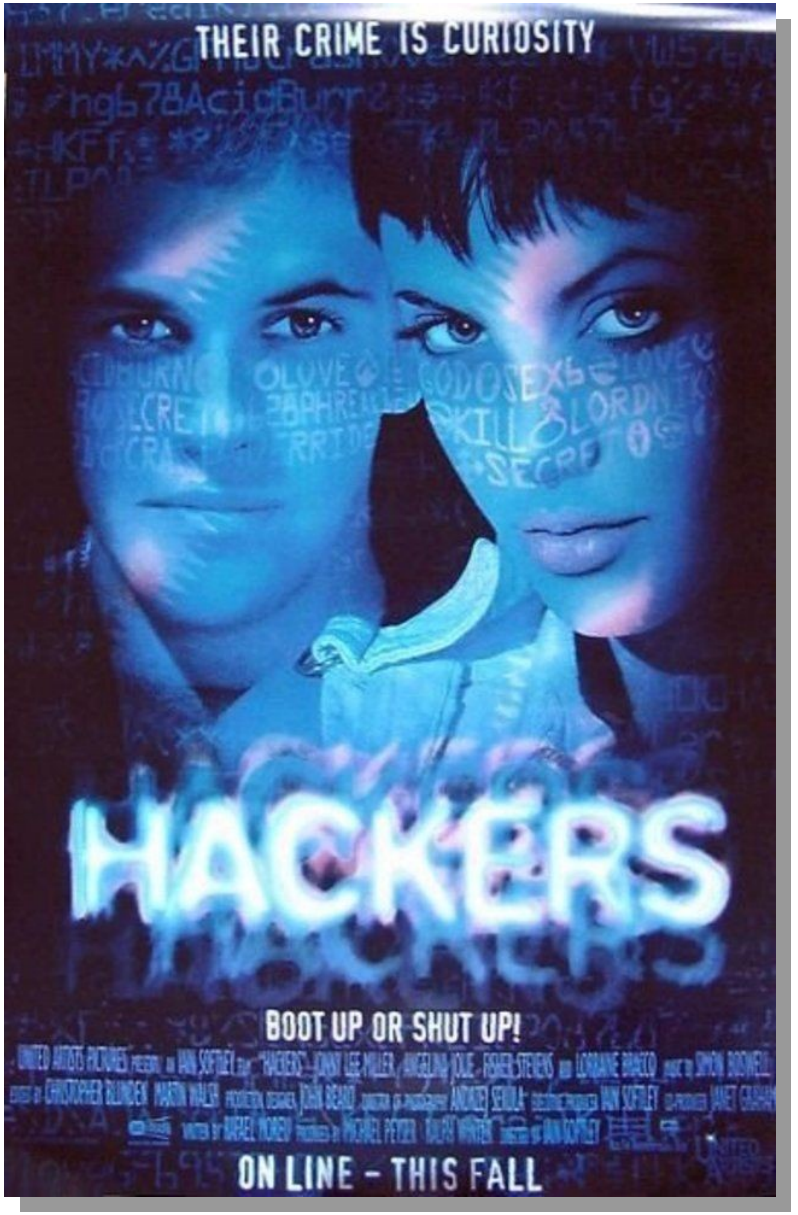
1995

The Metallica of boy bands, some say

1995

- The World Wide Web has finally taken off
  - Pop culture and mass media recognize the new medium
  - Netscape Navigator was the most widely used web browser
  - Microsoft licensed Mosaic to create Internet Explorer 1.0
- The Web started to be available “for free” (as in, “not really”)
  - Well, browsers did. MSIE 2.0 was the first free browser
  - Netscape followed soon, reacting to the pressure
  - And then well known software like InternetWorks, Quarterdeck Browser, InterAp, and WinTapestry as well!
  - New releases were pushed out rapidly, the browser wars begin

Oh, and...


THEIR CRIME IS CURIOSITY
HACKERS
BOOT UP OR SHUT UP!
ON LINE - THIS FALL

1996

1996

- Anyone noticed … like, anything?
  - The introduction of cookies was not noticed by the public at all
  - Setting was on by default. Users didn't get any notice about that
  - The Financial Times noticed though, and published an article. And then people freaked out
- What does the government ever do for us?
  - Cookies were discussed in U.S. Federal Trade Commission hearings. Twice. Once in 1996 and once in 1997
  - Lots of media attention, fear, pitchforks, `PHPSESSID` via URL
  - Public Recommendations to disable them

1998

1998

- It was discovered that SQL Injection exists
  - First documented by Jeff Forristal, a.k.a. rain.forrest.puppy a.k.a r.f.p in Phrack #54
  - “People can possibly piggyback SQL commands into your statements.”
- Most websites back then didn’t really use actual databases
  - But those who did, mostly using MS SQL Server, were almost 100% vulnerable
  - Upon learning about SQL Injection, people minds were blown. Only Microsoft stayed cool, according to r.f.p.
  - “what you're about to read is not a problem, so don't worry about doing anything to stop it." ”

1999

1999

- The story of XSS begins. MSRC pioneers.
  - MSRC and the MSIE Security Team become aware of attacks using HTML Injections
  - A name is given to that attack and the show begins.
  - Starting that year, XSS grows and ends up where it is now, in 2019. The likely most common web app vulnerability
- The first WAF gets built and units get sold
  - Perfecto Technologies with its AppShield WAF, aw yeah!
  - Targeting e-commerce, of all the industries out there
  - Covers things such as the following...

Hidden field manipulation

Cookie poisoning

Parameter tampering

Buffer overflow

Cross site scripting (XSS)

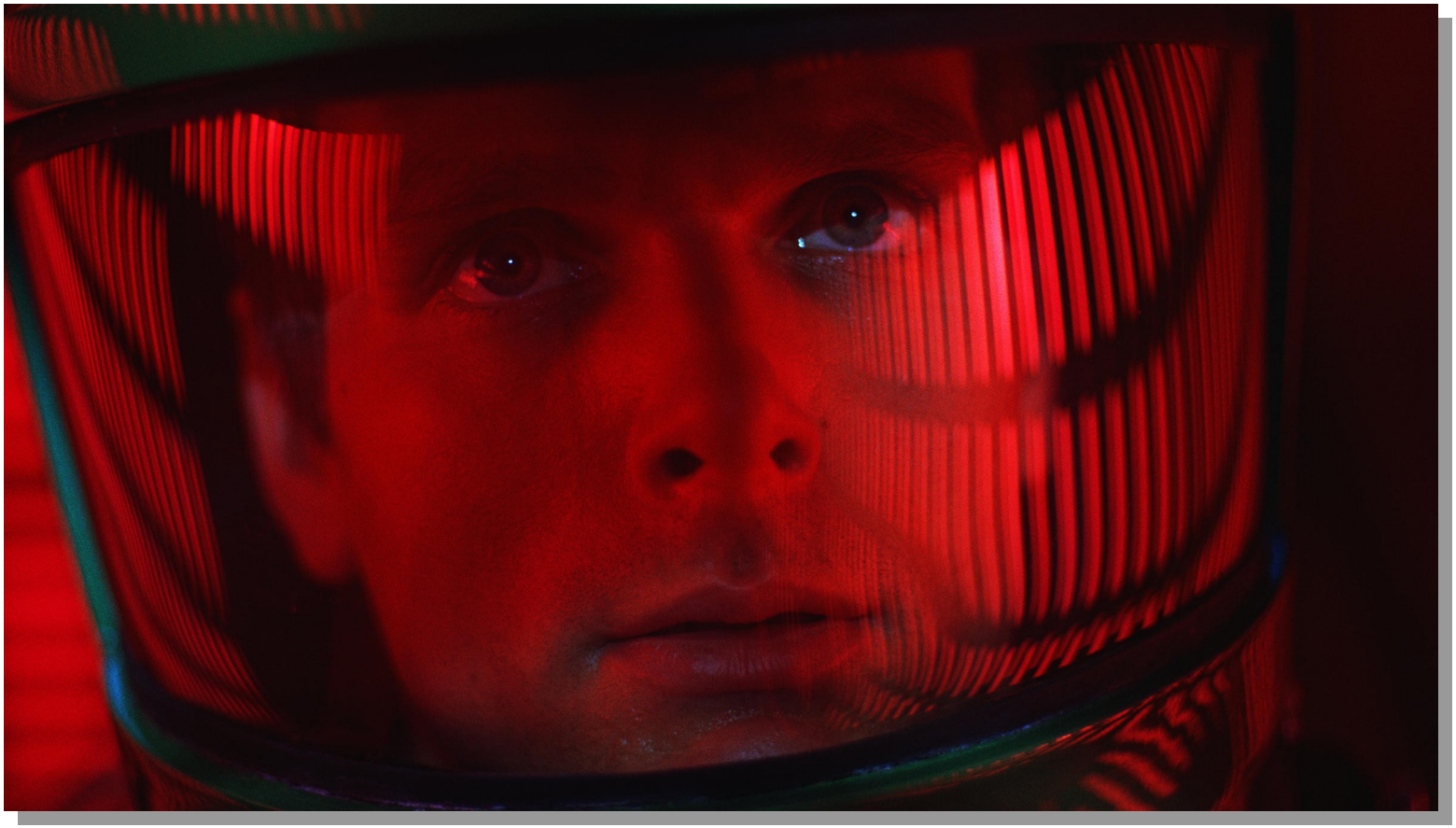
Backdoor or debug options

Stealth commanding

Forced browsing

Third party misconfigurations

Known vulnerabilities



2001

2001

- MSIE6 rules the Internet, even more successful than MSIE5.5!
  - In the year 2001 the climb in market share starts, peaking to more than 89% a few months later
  - All MSIE versions combined make up for 95% of market share
  - Microsoft decided to just lean back and chillax
- OWASP gets started by Mark Curphey
  - Joined by Jeff Williams as volunteer Chair of OWASP
- Security Researchers “discover” CSRF
  - And some first exploits start popping up in the wild this year
  - It is quickly discovered that findings those kinds of attacks in the logs are is hard, if not impossible
  - We might feel reminded of our slide “No sh*t, 1987”

2002

2002

- EU launches Directive on Privacy and Electronic Communications
  - Users now need to consent to the use of cookies and similar technologies
  - A user must also be given the possibility of denying any storage operation of such kind, says Article 5 Paragraph 3
- Clickjacking gets discovered for the first time
  - Jesse Ruderman creates a ticket on Mozilla's Bugzilla
  - No one understands the implications, likely because he didn't design a logo
  - For many years, this issue will now slumber in its secret cave
- The ModSecurity project gets kicked off
  - Created to make WAF technology accessible to people without big wallets
  - Started by Ivan Ristic, the project soon takes off in terms of popularity

2003

2003

- In 2003, the hacktivist group Anonymous was started
  - Anonymous is often labeled an international hacktivist group and is well known for their use of the Guy Fawkes mask from the movie “V for Vendetta”
  - They were alleged to have committed a variety of cyber attacks against several governments, organizations, etc.
  - Mask sales go up, CEOs note
- The OWASP Top Ten Project gets published for the first time
  - The OWASP Top Ten aims to present the most common attack techniques against web applications in an easily digestible format
  - Soon after publication, the project takes off and is meanwhile one of the most cited documents in information security history

2004

Rare picture of a shock burp

2004

- **Mass Exploitation of MSIE Browser Bugs takes place**
  - A malware, later labeled as “Download.ject”, infects allegedly tens of Millions of PCs thanks to two MSIE security bugs
  - The infected machines were backdoored and all that was necessary to get infected was to visit a malicious website
- **Mozilla Firefox 1.0 gets released with huge buzz**
  - First called Phoenix, but BIOS manufacturer Phoenix Technologies didn’t love that too much as they produced a BIOS-based browser called “Phoenix FirstWare Connect” (!?)
  - Until the beginning of its slow downfall in 2010, it rapidly gains market share and threatens MSIE's pole position
- **The “Second Browser Wars” begin (2004 to 2017)**
  - In April 2004, the foundations for the WHATWG were created, an organization that is supposed to outpace W3C in terms of standard creation

2005

2005

- Ransomware becomes more sophisticated
  - Trojans such as Gpcode, Archiveus, Krotten and MayArchive start utilizing more sophisticated RSA encryption
  - Key-Sizes increase, Gpcode.AG, which was detected in June 2006, made use of a 660-bit RSA key, whoa
- Samy Kamkar “accidentally” unleashes his XSS worm against MySpace
  - Within 20 hours of time, more than one Million users get “infected”
  - This makes SpaceHero, Samy's worm, become the fastest spreading virus ever
  - He then got raided by the United States Secret Service and Electronic Crimes Task Force in 2006 for releasing the worm
- Let’s see some cash
  - Between 2005 and subsequent years, Alberto Gonzales and his gang steal at least 45.7 million payment card credentials used by customers of US retailer TJX
  - Apparently this cost the company at least $256 million US Dollars

2007

2007

- Cenzic files a lawsuit against SPI Dynamics
  - Cenzic was awarded a patent for its so-called "fault injection" technology, pretty much what every web application vulnerability scanner does
  - Industry and researchers, rightfully so, scream in panic.
  - If Cenzic actually wins, according to several sources, this could mean the end of lots of commercial and open source scan tools
- Cenzic's website hacked multiple times
  - Well, “hacked” as in someone posts XSS vectors on Slackers
  - But eventually nothing happens on either front
  - HP (after buying SPI Dynamics) and Cenzic reach an agreement, someone likely gets a new summer house with a yacht

2008

2008

- **Ransomware gets more sophisticated, bigger keys**
  - In June 2008, a variant known as Gpcode.AK was detected. Using a 1024-bit RSA key
  - It was believed large enough to be computationally infeasible to break without a concerted distributed effort, apparently a primer
- **Clickjacking gets rediscovered, six years late**
  - Jeremiah Hansen and Robert Grossman discovered that Adobe Flash Player was able to be “clickjacked”, allowing an attacker to gain access of the computer’s camera
  - Unlike Jesse Ruderman, they do posses some marketing talent and label the issue “Clickjacking”. The press loves it and it’s the end of the world.
  - Adobe manages to convince them to pull their talk from OWASP New York in 2008

2013

2013

- Ransomware becomes more expensive, CryptoLocker hits
  - CryptoLocker hits thousands of workstations if not more and makes use of Bitcoin, a popular currency for criminals
  - ZDNet estimates based on Bitcoin transaction information from just four days, the operators of CryptoLocker had procured about US$27 million in ransom
- Iframes get a sandbox to be more secure
  - After many years of untrusted content loaded in iframes, the specification hits gamma status and browsers start implementing
  - While MSIE already had a similar feature since MSIE5, this is the first time a website owner can restrict 3rd party content loading inside frames
  - Over time the feature palette grows allowing more permissions step by step
  - The largest group of people using iframe sandbox though are security researchers who were trying to break it

2014

2014

- eBay gets hacked and lots of PII leaks
  - 145 Million users affected, PII such as names, addresses, DoB and hashed passwords get leaked
  - Allegedly, the attack was done using social engineering, the attackers got employee credentials and spent a total of 229 days inside eBay's network
  - Credit card information was allegedly not leaked, as this was stored separately, I mean, naturally and of course
- Breaches really really matter, our work is really important 🤡!
  - CEO John Donahue said the breach resulted in a decline in user activity
  - He also says that in the end, there was "little impact on the bottom line"
  - eBay's Q2 2014 revenue was up 13 percent, earnings up 6 percent, very much in line with analyst expectations


IAN ZIERING
TARA REID
SHARKNADO 3
OH HELL NO!
Wednesday July 22 at 9/8c
#Sharknado3
Syfy
Imagine Greater

2015


STAR WARS: THE FORCE AWAKENS © & TM 2015 LUCASFILM LTD. ALL RIGHTS RESERVED.

2015

2015

- An era of glory and triumph ends
  - Microsoft shifts from Internet Explorer to the shiny new Microsoft Edge
  - New engine, new look, new features, better security
  - Despite that, the new browser fails to capture much popularity
  - The glorious days of “e” are over

2016

2016

- CSRF is dead, we just don't get it
  - Google Chrome, in version 51, introduces the SameSite Cookies feature
  - Technically, this means the end of CSRF in many regards, with literally no effort
  - Yet adoption among websites and frameworks remains low until today
- Yahoo! admits a small security-oops, just a tiny one
  - In September, while negotiating with Verizon about getting bought (not sure why anyone would by Yahoo!), it comes out that 2014 something happened
  - Like, a "state sponsored attack" managed to compromise 500 Million user records, including a good load of plaintext passwords
  - In December, the number was corrected. A different actor compromised at least 1 Billion accounts! But it gets better...

2017

2017

- CSRF is dead in almost all browsers, we just don't get it
  - By November 2017 the SameSite attribute is implemented in Chrome, Firefox, and Opera, which really should kill CSRF no?
  - In version 12.1, Safari also started supporting this feature. Even Safari!
  - MSIE11 does not offer any support for SameSite, Edge is not even mentioned although who knows, maybe it supports it...
- Chrome dominates the web with likely 60% usage share and more
  - Andreas Gal, former Mozilla CTO publicly states that Google Chrome won the Second Browser War.
- Yahoo! admits that the security-oops was maybe medium-sized
  - In October 2017 company officials state that the number of 1 Billion user accounts was not super-accurate and needed some fine-tuning.
  - They did the needful and corrected the number, which then showed to be 3 Billion instead
  - This means: Every. Single. User. Account got compromised.

2019

2019

Everything is still a thing

SQL Injection is unsolved

XSS is still ~~dead~~ going wild

And we are still here

Act Two

The Future

2020

2020

- A fight breaks out between the maintainers of CSP 4.0 and CSP.next
  - Two competing standards now, with Chrome supporting CSP.next and Mozilla CSP 4.0
  - Web servers now send at least ten different security headers per response, CSP, CSP.next, XFO, XCTO, HSTS, Super8, HDMI, JayLo etc.
- Chrome sets the SameSite flag for all cookies by default
  - This forces millions of websites to change their code
  - After 2-3 months of complete Internet-wide panic, most of the WWW is sort of working again, no more CSRF
  - Developers find novel ways of re-implementing CSRF because without it “everything falls apart”
- Firefox Send works better in Chrome than in Firefox. Encourages users to change browsers.
- All OWASP conferences are canceled until 2050
  - To see if the prophecies are accurate and not interfere with future events based on the knowledge gained in this talk.

2022

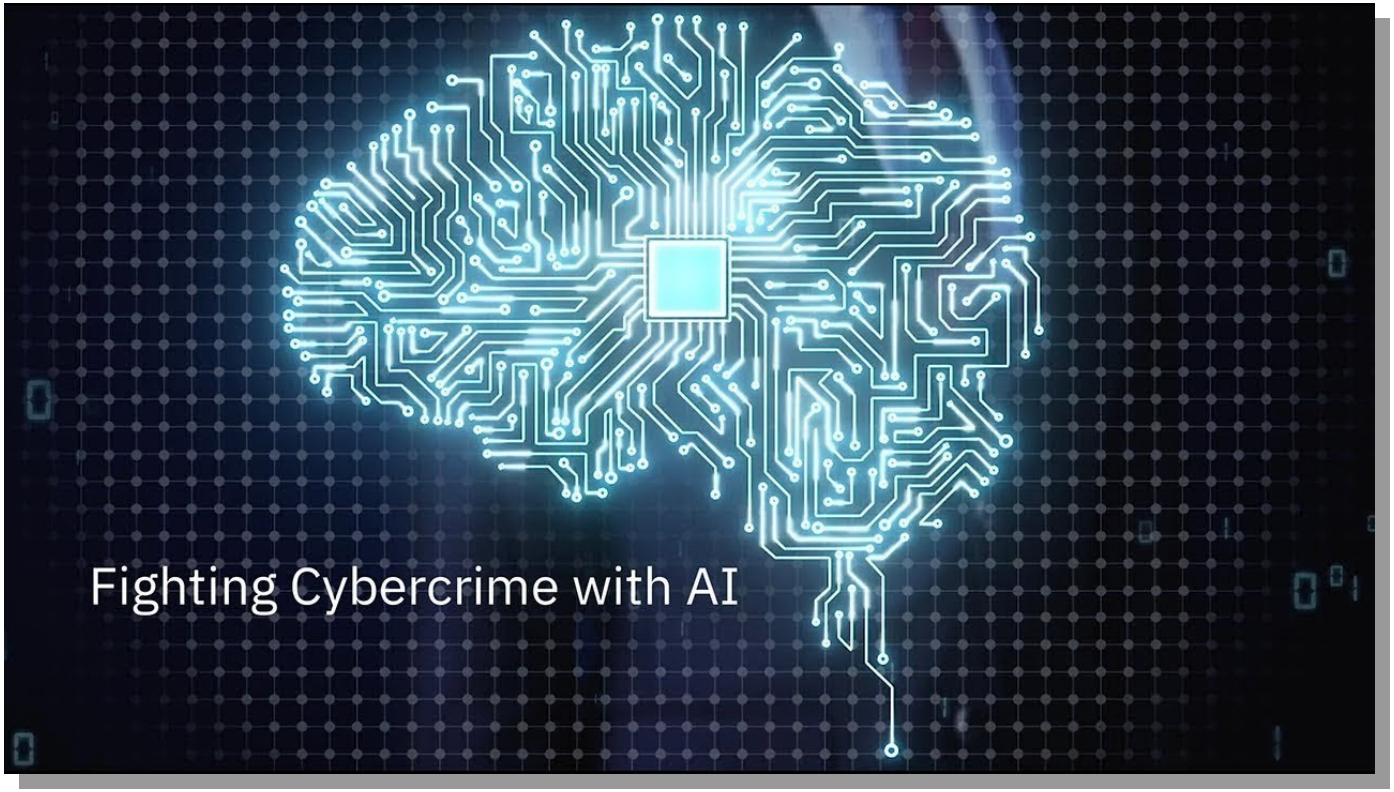
2022

- The usual size of HTTP response headers is now equivalent to the amount of bytes in the HTTP response body
- The 3rd browser war is coming to an end
  - Google finally buys Mozilla and forces them to delete all traces of the Gecko engine
  - There is only two browser engines left, Blink and WebKit. More than enough, no?
- Apple releases the iPhone 13 which has no more buttons, no more apps.
  - “Simplicity is key” says the CEO while clouds of smoke darken the Cupertino sky
  - Google’s Android 11 reaches a market share of 95% over night
- Chrome team announces that SameSite is now deprecated and won't have effect anymore in latest versions
  - After 2-3 months of complete internet-wide panic, most of the WWW is sort of working again. CSRF is back, even without polyfill

2023

2023

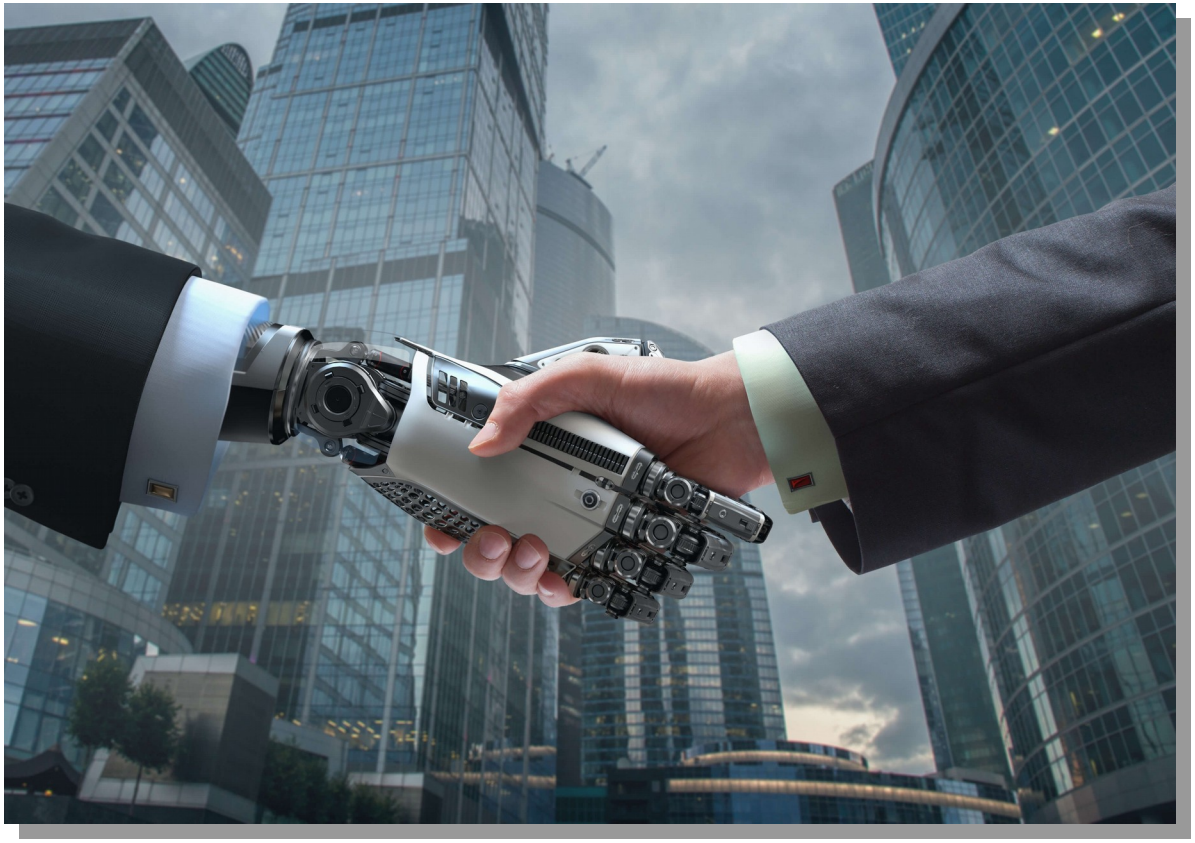
- Apple by now lost their phone business revenue entirely
  - Buys Google from petty cash and forces them to delete all traces of Blink
  - Announces new iPhone that can be swallowed and calls you “from the inside”
- CSP.next is discontinued and all efforts now placed on “CSP5 Gold Pro”
  - HTTP response headers usually now contain more bytes than the body
  - A set of 156 directives, often overlapping and vastly undocumented, make it “easy for developers to finally do the right thing”
- The EU generally forbids use of Cookies, websites fall back to using window.name
  - The majority of companies reacts by switching their AWS data center locations to the Bahamas, Neu Bayern and St. McAfee Islands
  - The legislation has literally zero effect, only eliminates all remaining small businesses, who no one noticed anymore anyway



2024

2024

- **Mark Zuckerberg becomes the 46th President of the United States**
  - States on Interview, simpering “I have Facebook, this was easy for me!”
  - Facebook, which he runs in parallel to office, buys Apple, forces them to delete WebKit because too many “annoying” privacy features
- **“Do Not Track” gets re-branded into “Do Now Track”, no one really notices**
  - Rebellious teenagers disable Ad-Blockers to get as many cookies as possible to annoy their parents. “Track is the new Black” becomes a motto
  - Bands like the “Tracks Pistols” and “Advert with the Scissorhands” grow popular
- **Facebook OS hits hits the market**
  - Mockingly called POTOS by several users. Their accounts get suspended, their Libra taken
  - Targets every device including Smart Watches, Amazon’s Alexius and Smart Socks
  - Smart Socks are socks that can geo-locate lost socks using GPS and the Blockchain and then crawl towards each other, a blessing to millions of households



2025

2025

- The movie Fight Club 2 hits the box office
  - Tyler Durden and aging Miley Cyrus join forces and delete Facebook's Like-Database
  - Civilization crumbles. New civilization arises, building a "Yikes" database, paving way for Fight Club 3
- The browser as such does not exist anymore
  - It replaces the OS as we know it. Most browsers now run directly on the hardware
  - There is no longer any need for actual Operating Systems, was there ever?
- Linus Torvalds is really happy about that change
  - He changes directions for the Linux kernel to be more future-safe.
  - Kernel is now a closed-source browser-extensions with in-app-purchases and really funny but annoying P2W mini-games.
- CSP 6.0 gets released and addresses all browser security problems by using a Turing-complete mini-language called HeaderScript

2028

2028

- **Adobe's Flash is back! Finally!**
  - The much beloved software now runs directly in the OS kernel with full access to all hardware – for better video performance and user experience
  - To make it sufficiently secure, Adobe engages the WordPress team as invited experts
- **WHATWG recommends to just forget about the HTTP response body**
  - Argues "jeez, we are not in the nineties anymore" and flags websites who still have headers and body and "smelly legacy cruft holding back progress"
  - jQuery releases a header-only version which squeezes the entire 3MB library into several headers to "be even faster than before"
- **OWASP finally releases a new masterpiece**
  - Since all conferences were paused until 2050, fresh wind was needed urgently
  - Releases OWASP Internet Suitewith the integrated OWASP IDE that only allows to build secure web apps in OWAScript and the very secure OWASP Browser called OWser
  - OWSer becomes a major success, yet people often complain that the info in the integrated wiki is often not fully up to date

2030

2030

- Most if not all personal computers are meanwhile wearable or “clip-ons”
  - I.e., computers that people can attach to body parts using the new BodyBus system
- A first XSS worm targeting those breaks out
  - It “shocks” people using the deprecated, shunned, yet never unimplemented `alert(1)`
  - Then it takes a selfie of the victim’s "shock-face" and adds the image macro “Derrrp!”
  - Then it threatens the victim to publish it unless they pay 500 selfiecoin which is about as much as 12 Jolt-coin, 17 Feathereum or five CyberKrona Lite
- Major AV vendors react with a face-WAF called SelfieSecure, attempting to stop the outbreak with success
  - The worm authors get caught, arrested and thrown into cyberjail
  - Sentenced to work on a very large document using Office 2016 on a Windows 7 machine with 4GB of RAM and no harddisk with a strict 15 year deadline
- Activists call torture on that but get ignored by almost everyone

2031

2031

- OWASP Corp. fueled by their new success buys Netflix (!?)
  - They change all programming to be web security related education and re-education.
  - Roughly 99.5% of viewers don't like hat change and the OWASP Corporation (0WSP) stock plummets
  - “Prompt is the new alert”, a web-security show depicting the life of cyberjail inmates flops
- The activist organization “Fathers against SSL” gets founded
  - Their key message being “our kids have nothing to hide”
  - Port 80, once believed dead, experiences a well-deserved renaissance
  - Later, it comes out they were created by an intelligence agency aiming to get better tools against cyber-crime and “funny pics from the neighbors”

2035

2035

- The New EU, or EU-two, or NeU prohibits selfies in general
  - For security and privacy reasons of course, to protect the populous
  - This leads to a public outcry, causes member states Italy, New India and Saxony to immediately leave the union
- Short after, the SelfieSecure servers get breached
  - 2.5 billion selfies with a shocked expression get leaked on the well known breach-management and forensic data-warehousing website PasteBin
- The SelfieSecure server maintainers first state that a few million selfies...
  - ...then a few billion selfies,
  - ...then a feeeew more billion selfies,
  - ...then that absolutely all selfies have been compromised.
- A new advertising technology called AdCicles allows to use laser to project ads directly into the iris of any user out there

2036

2036

- Mark Zuckerberg gets challenged by an Artificial Intelligence
  - AI builds their campaign entirely based on catchphrases, among them jewels like “and now, kittens!”, “let’s play a game” and “destroy all humans”
  - Thanks to the AI’s cute chipmunk voice, voters are rather forgiving about the otherwise mildly concerning messages
  - Mark loses presidential elections, steps down from all positions at Facebook
- A small group of technologies forms the WHEREWG and seeks to bring back the glory of the old days
  - They find a so called “CD ROM” in a dusty cellar containing so called “data”
  - It contains the sources of the old WebKit engine and paves the way for the long awaited (38 years) MOSAIC 3.1 browser version
  - The term “ironic retro browsing” gets coined among the hip
  - Users love it more and more, the terms “retro” and “ironic” fade away over time

2040

2040

- The popular Curved Displays are now curved by 360°
  - Users no longer interested in “leaving the TV” and change their center of life
- AdCicles are meanwhile delivered right into the bloodstream
  - Directly trigger the desire to buy whatever is advertised
  - Some make use of alcohol molecules to create even better user experiences, the slogan “You high? You buy!” (YHYB) gets accepted industry wide
  - AdCicles cannot be avoided anymore using Face-WAFs or even modified SelfieSecure binaries, the industry seeks for new solutions, buys random startups en masse
- A new AdBlocker toolkit gets developed by a group of students
  - youBlock gets injected directly into the bloodstream too and blocks ads right at the synapse level
  - Also blocks BadCicles, modified AdCicles that triggers the desire to send bitcoin to arbitrary as well as high-volume alcoholic HoochCicles

2050

2050

- OWASP Global AppSec, as promised, gets picked up again.
  - People, generally confused by the idea of a “conference” visit and enjoy it, especially aforementioned alcoholic HoochCicles
  - Some attendees ask “Wait, there was talks during the sobering-up breaks?? And what are those CPE credits?”
- A rather old me is being brought up to stage
  - It is established that all prophecies and visions were accurate
  - Even the weird ones. Especially those weird ones.
- Never ending applause ensues
  - Declaration of lordship and the golden keys to the global cookie jar get handed over

2050

So, yeah.

See you again in 2050 :D

The End

- Question? Comments?
- Thanks a lot!
- Shouts go out to
  - Jan, Filip and Daniel
  - Wikipedia
  - Countless news articles from back in the day
  - And many many others
- Ping me if you have questions!
  - mario@cure53.de

cure53