OECD Working Party on Digital Security (WPDS) Meeting | Paris, Nov 2024

Markets for digital security vulnerabilities

& case for a nation-wide bug bounty program

Dr. Stefan Frei

frei@techzoom.net | Web https://techzoom.net | BlueSky stefanfrei.bsky.social

Context

Since 2020, the OECD has prioritized digital security vulnerabilities, identifying them as key risks. Inadequate legal frameworks create uncertainty and risks for “white hat” researchers, despite their contributions to cybersecurity [1,2]. This led to a Council Recommendation to improve policies, support vulnerability research, and establish legal protections for researchers [3].

Questions for discussion by experts and delegates:

- What are the key characteristics of markets for vulnerabilities? Is there a market failure and if so, why?
- What are the incentives for researchers to sell vulnerabilities on the grey or black rather than white markets?
- How do the grey and black markets influence the white market?
- Given that vulnerabilities are inevitable, and that grey and black markets exist, how can vulnerability owners maximize profits?
- What policy measures could encourage transactions on the white market and/or discourage transactions on the black and grey markets?

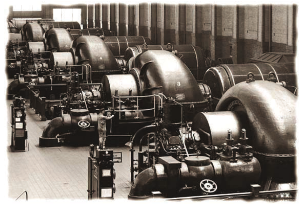
[1] Encouraging vulnerability treatment
https://techzoom.net/articles/oecd-encouraging-vulnerability-treatment
[2] Understanding the digital security of products
https://techzoom.net/articles/oecd-digital-security-of-products
[3] Recommendation of the Council on the Treatment of Digital Security Vulnerabilities
https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0482

Introducing security

A bit of history of technology

Cyber is not the first disruptive technology

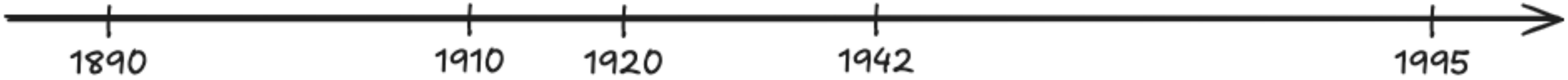
electricity generation



commercial airlines

Internet

Yahoo! - NCSA Mosaic
File Edit History Manager View Navigate Tools Hotlists Help
Other Doc
http://www.yahoo.com
YAHOO!
What's New
Check Email
Personalize
Help
Yahoo! Auctions
Pokemon, Rolex, 'N Sync
free_email@yahoo.com
Win Free Flowers
FTD.COM
Search
advanced search
Shopping - Auctions - Yellow Pages - People Search - Maps - Travel - Classifieds - Personals
Games - Chat - Clubs
Mail - Calendar - Messenger - Companion - My Yahoo! - News - Sports - Weather - TV -
Tue 06/06/00 9:33:04

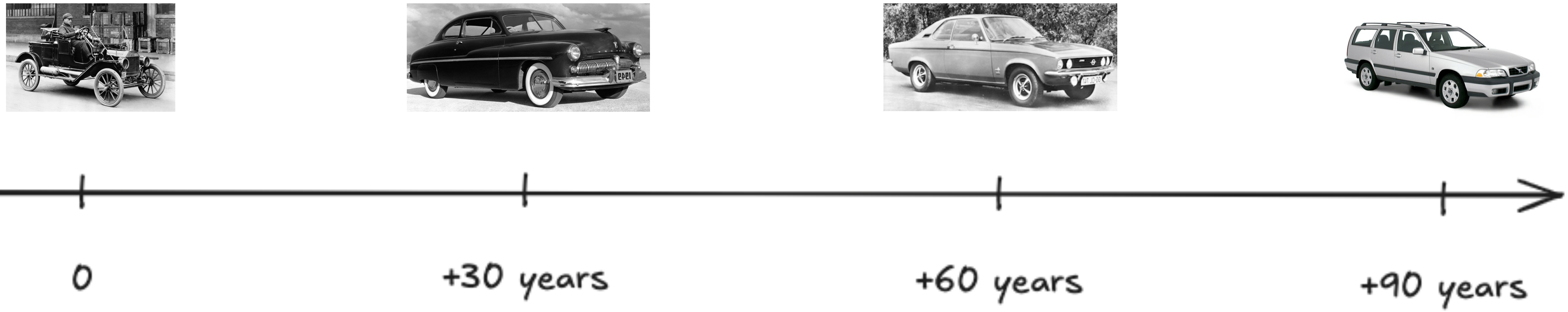


automobile mass-affordable

antibiotics mass production

”When was the **National Highway Traffic Safety Administration** (NHTSA) established”

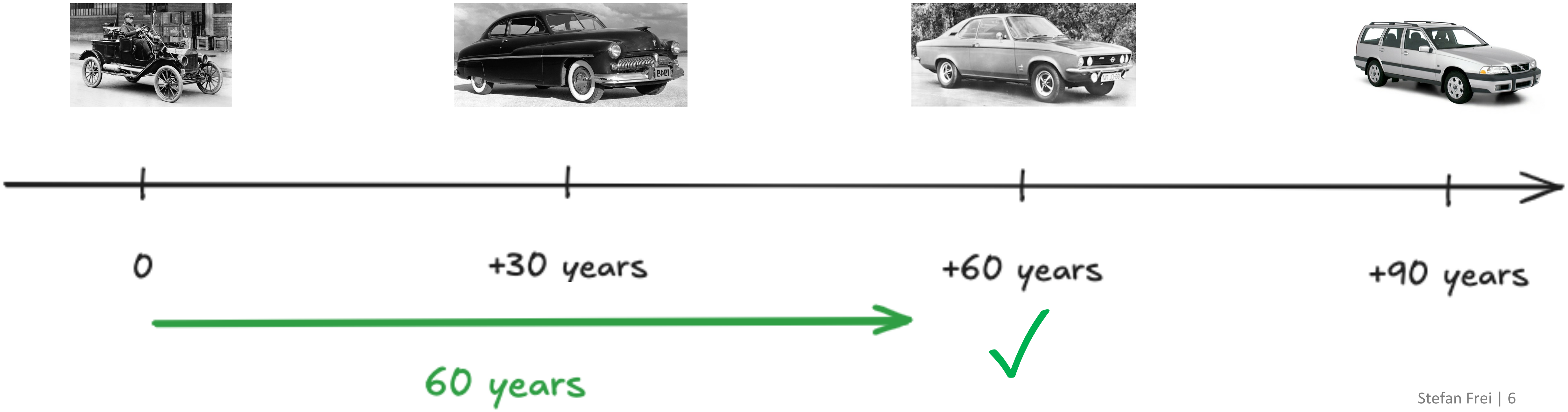
?



It takes time ..

The **National Highway Traffic Safety Administration (NHTSA)** was **founded in 1970**. Established under the **Highway Safety Act of 1970,** part of the U.S. Department of Transportation.

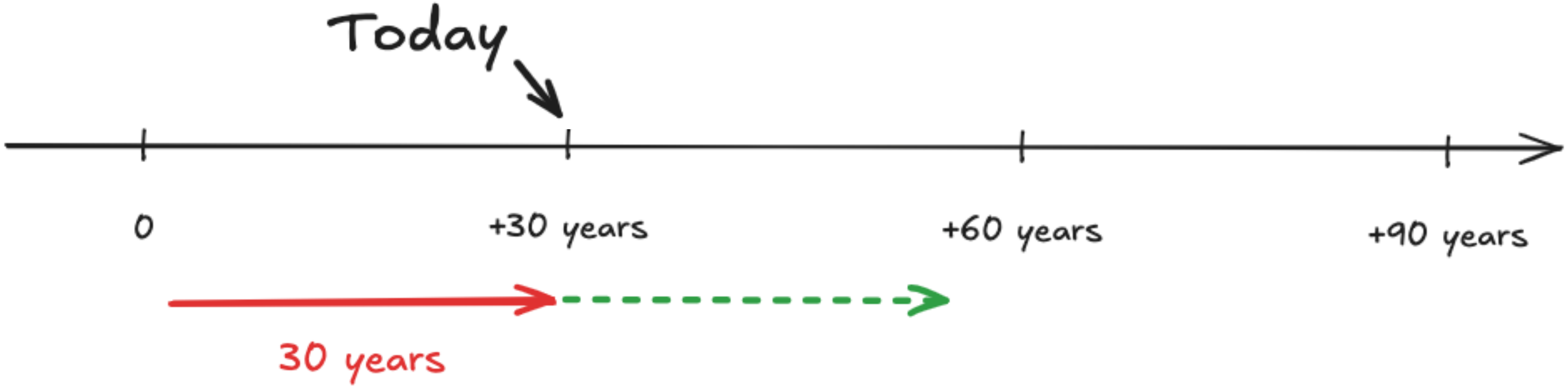
Mission: **improve road safety, set and enforce vehicle performance standards**, conduct **vehicle safety research**, and promote **public awareness about road safety**.



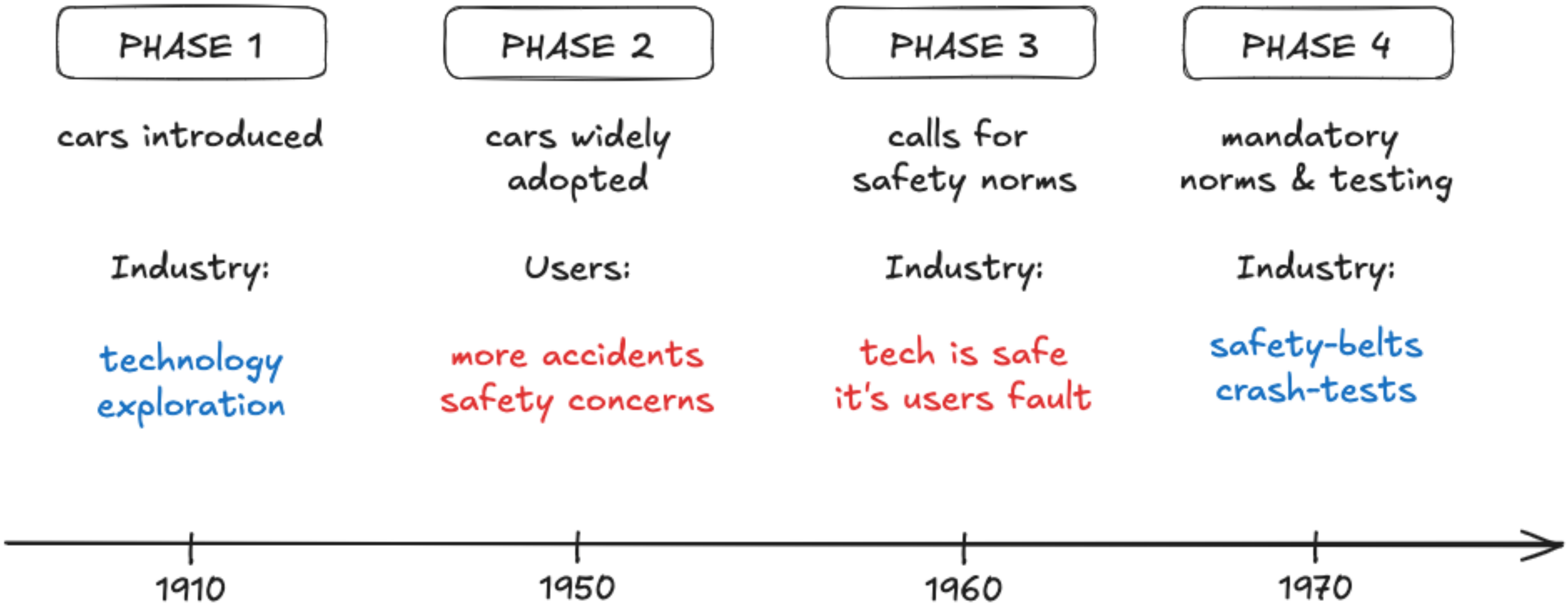
Cyber is still a young industry

Society eventually introduced enforceable safety norms for all critical technologies like aviation or automotive ..

Cyber



A repeating pattern ..



PHASE 1	PHASE 2	PHASE 3	PHASE 4
cars introduced	cars widely adopted	calls for safety norms	mandatory norms & testing
Industry:	Users:	Industry:	Industry:
technology exploration	more accidents safety concerns	tech is safe it's users fault	safety-belts crash-tests
1910	1950	1960	1970

New technology – new types of solutions

Automotive

- Passive security through crunch zones

Aviation

- Safety culture, speak up
- Human performance and limitations

Cyber

- Compensating vulnerability discoverers for ethical reporting

We need to familiarize decision makers with novel approaches

Vulnerability Markets

The illusion of secure software

Vulnerabilities in software have increased, in spite of massive security investment

- There is no real penalty for the producer for releasing insecure software
- Software producers prioritize features and time-to-market over security
- Users pay the price

- Software is everywhere, including critical functions

Situation

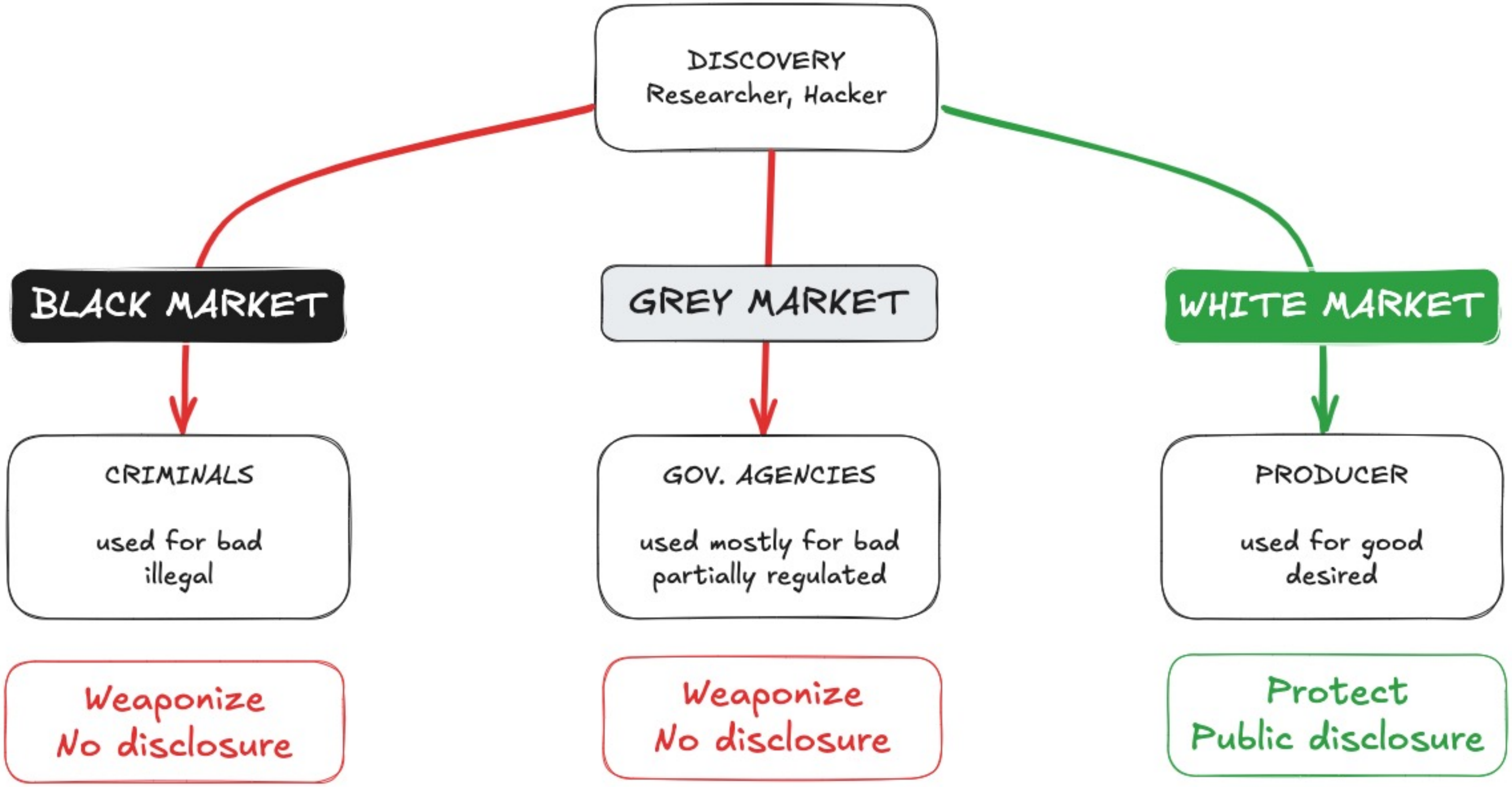
What we cannot prevent

- Ongoing discovery of new vulnerabilities
- **Criminals** or **gov. agencies** finding, buying, and stockpiling vulnerabilities

- Software **producers** disclaiming liability for poor quality

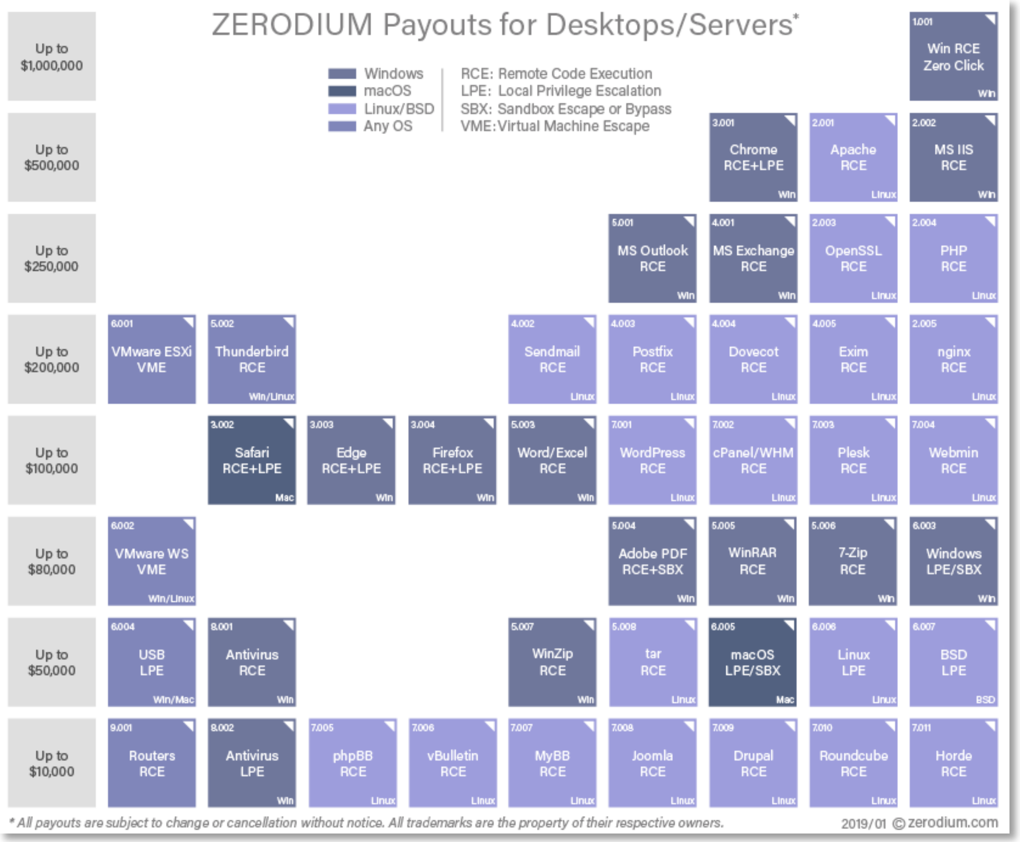
[1] US cybersecurity chief: Software makers shouldn't lawyer their way out of security responsibilities
https://www.theregister.com/2023/02/28/cisa_easterly_secure_software

Vulnerability markets



Grey market offerings

Desktop / Server
up to $1.0 million



ZERODIUM Payouts for Desktops/Servers*

- ■ Windows
- ■ macOS
- ■ Linux/BSD
- ■ Any OS

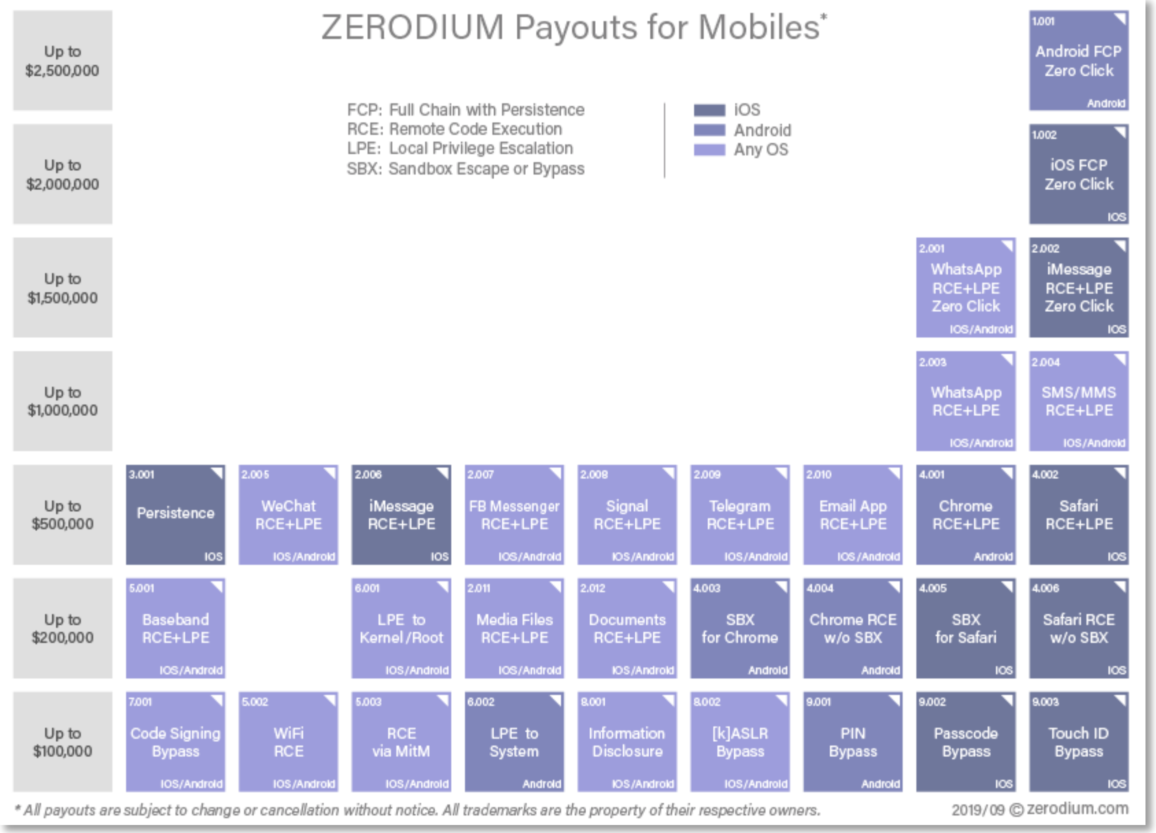
RCE: Remote Code Execution
LPE: Local Privilege Escalation
SBX: Sandbox Escape or Bypass
VME: Virtual Machine Escape

Up to $1,000,000									1.001 Win RCE Zero Click Win
Up to $500,000							3.001 Chrome RCE+LPE Win	2.001 Apache RCE Linux	2.002 MS IIS RCE Win
Up to $250,000						5.001 MS Outlook RCE Win	4.001 MS Exchange RCE Win	2.003 OpenSSL RCE Linux	2.004 PHP RCE Linux
Up to $200,000	6.001 VMware ESXi VME	5.002 Thunderbird RCE Win/Linux			4.002 Sendmail RCE Linux	4.003 Postfix RCE Linux	4.004 Dovecot RCE Linux	4.005 Exim RCE Linux	2.005 nginx RCE Linux
Up to $100,000		3.002 Safari RCE+LPE Mac	3.003 Edge RCE+LPE Win	3.004 Firefox RCE+LPE Win	5.003 Word/Excel RCE Win	7.001 WordPress RCE Linux	7.002 cPanel/WHM RCE Linux	7.003 Plesk RCE Linux	7.004 Webmin RCE Linux
Up to $80,000	6.002 VMware WS VME Win/Linux					5.004 Adobe PDF RCE+SBX Win	5.005 WinRAR RCE Win	5.006 7-Zip RCE Win	6.003 Windows LPE/SBX Win
Up to $50,000	6.004 USB LPE Win/Mac	8.001 Antivirus RCE Win			5.007 WinZip RCE Win	5.008 tar RCE Linux	6.005 macOS LPE/SBX Mac	6.006 Linux LPE Linux	6.007 BSD LPE BSD
Up to $10,000	9.001 Routers RCE	8.002 Antivirus LPE Win	7.005 phpBB RCE Linux	7.006 vBulletin RCE Linux	7.007 MyBB RCE Linux	7.008 Joomla RCE Linux	7.009 Drupal RCE Linux	7.010 Roundcube RCE Linux	7.011 Horde RCE Linux

* All payouts are subject to change or cancellation without notice. All trademarks are the property of their respective owners.

2019/01 © zerodium.com

Mobile
up to $2.5 million



ZERODIUM Payouts for Mobiles*

FCP: Full Chain with Persistence
RCE: Remote Code Execution
LPE: Local Privilege Escalation
SBX: Sandbox Escape or Bypass

- ■ iOS
- ■ Android
- ■ Any OS

Up to $2,500,000									1.001 Android FCP Zero Click Android
Up to $2,000,000									1.002 iOS FCP Zero Click iOS
Up to $1,500,000								2.001 WhatsApp RCE+LPE Zero Click iOS/Android	2.002 iMessage RCE+LPE Zero Click iOS
Up to $1,000,000								2.003 WhatsApp RCE+LPE iOS/Android	2.004 SMS/MMS RCE+LPE iOS/Android
Up to $500,000	3.001 Persistence iOS	2.005 WeChat RCE+LPE iOS/Android	2.006 iMessage RCE+LPE iOS	2.007 FB Messenger RCE+LPE iOS/Android	2.008 Signal RCE+LPE iOS/Android	2.009 Telegram RCE+LPE iOS/Android	2.010 Email App RCE+LPE iOS/Android	4.001 Chrome RCE+LPE Android	4.002 Safari RCE+LPE iOS
Up to $200,000	5.001 Baseband RCE+LPE iOS/Android		6.001 LPE to Kernel/Root iOS/Android	2.011 Media Files RCE+LPE iOS/Android	2.012 Documents RCE+LPE iOS/Android	4.003 SBX for Chrome Android	4.004 Chrome RCE w/o SBX Android	4.005 SBX for Safari iOS	4.006 Safari RCE w/o SBX iOS
Up to $100,000	7.001 Code Signing Bypass iOS/Android	5.002 WiFi RCE iOS/Android	5.003 RCE via MitM iOS/Android	6.002 LPE to System Android	8.001 Information Disclosure iOS/Android	8.002 [k]ASLR Bypass iOS/Android	9.001 PIN Bypass Android	9.002 Passcode Bypass iOS	9.003 Touch ID Bypass iOS

* All payouts are subject to change or cancellation without notice. All trademarks are the property of their respective owners.

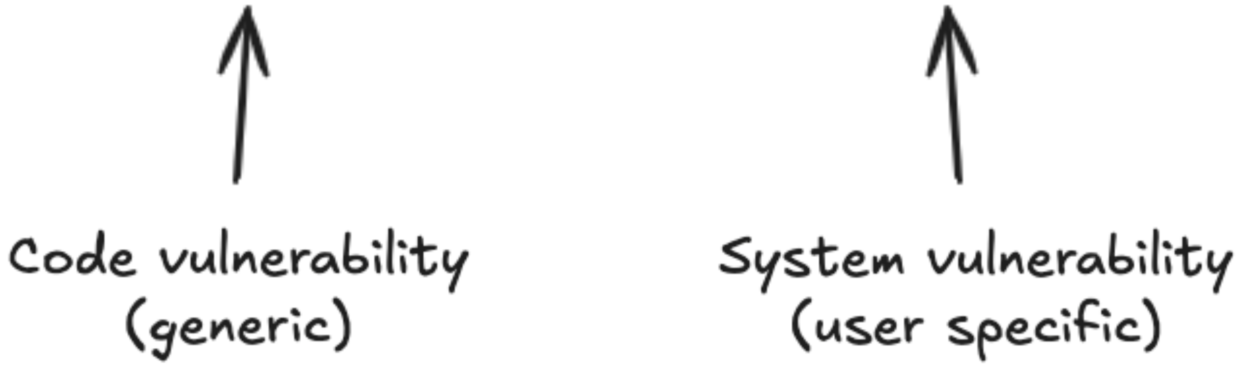
2019/09 © zerodium.com

Source: https://zerodium.com (Nov 2024)

Objectives

What we want

- Have a fix before vulnerability is publicly known (> Discoverer, Producer)
- Increase software quality, less vulnerabilities (> Producer)
- Users deploy security updates and secure configurations (> User)



Code vulnerability
(generic)

System vulnerability
(user specific)

Instruments

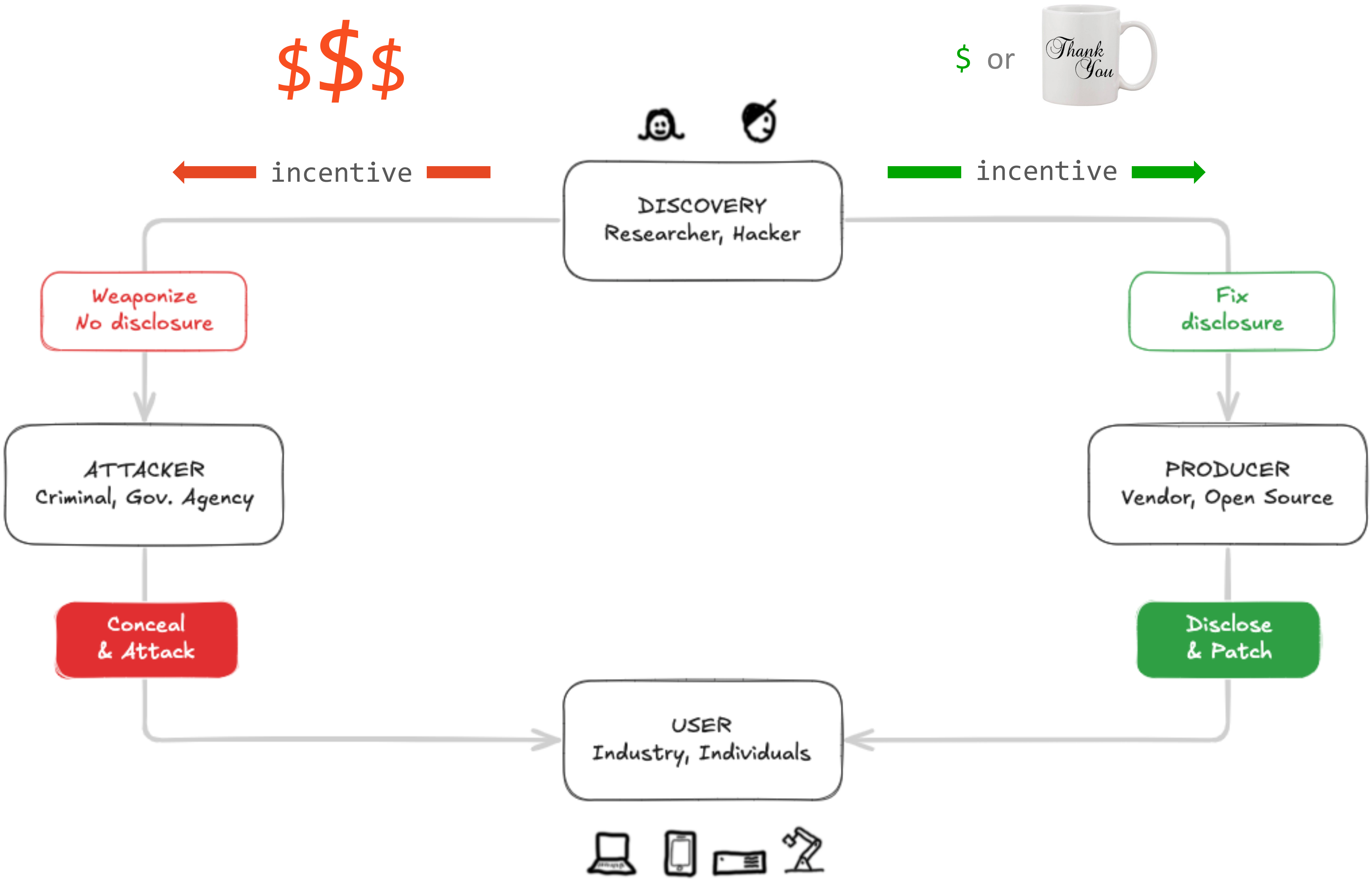
What we need

- Incentives for secure products (> Producer)
- Incentives to report vulnerabilities to producer (> Discoverer)
- Incentives to implement best practice and known security (> User)
- Depleting vulnerability stockpiles of criminals & gov. agencies (> Discoverer)

Tools

- Information
- Regulation

Market Failure ?!



$$$

$ or

incentive

incentive

DISCOVERY
Researcher, Hacker

Weaponize
No disclosure

ATTACKER
Criminal, Gov. Agency

Conceal
& Attack

Fix
disclosure

PRODUCER
Vendor, Open Source

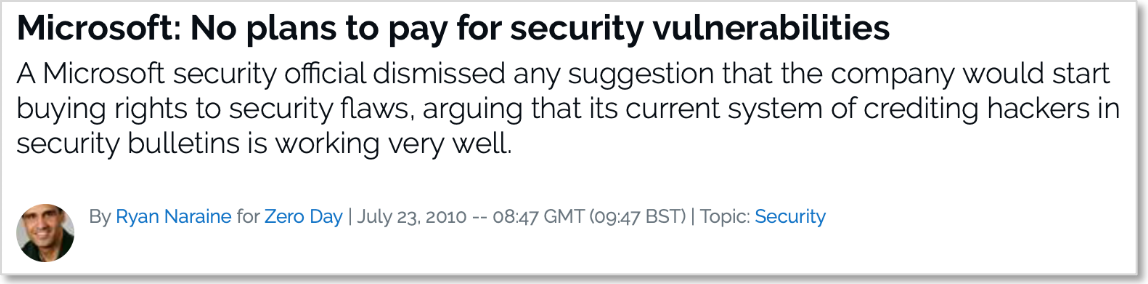
Disclose
& Patch

USER
Industry, Individuals

Bug bounties - Getting to yes

Microsoft 2010

Paying for vulnerabilities?
Forget about it!



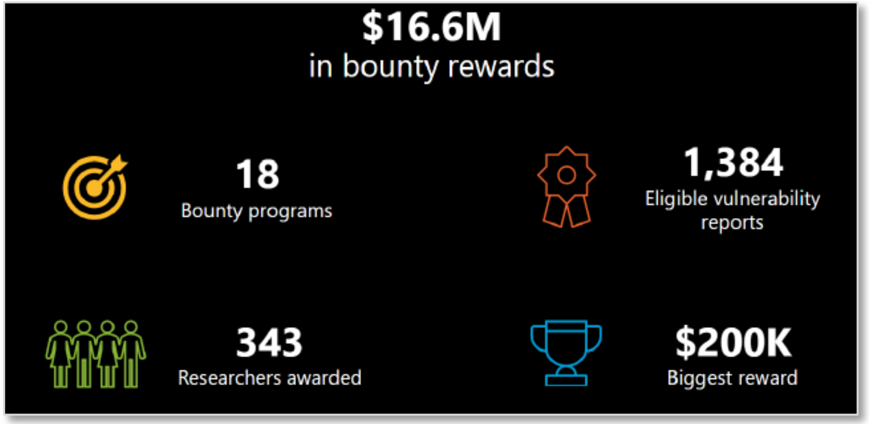
Microsoft: No plans to pay for security vulnerabilities

A Microsoft security official dismissed any suggestion that the company would start buying rights to security flaws, arguing that its current system of crediting hackers in security bulletins is working very well.

By Ryan Naraine for Zero Day | July 23, 2010 -- 08:47 GMT (09:47 BST) | Topic: Security

Microsoft 2024

Hey, we paid **$16.6 million** in bug bounties!



$16.6M
in bounty rewards

18
Bounty programs

1,384
Eligible vulnerability reports

343
Researchers awarded

$200K
Biggest reward

Celebrating 10 Years of Microsoft's Bug Bounties - The Beginning (Nov 2013)
https://www.lutasecurity.com/post/celebrating-10-years-of-microsoft-s-bug-bounties-the-beginning

Market failure?

Microsoft 2024

We paid **$16.6 million** in bug bounties!

per year

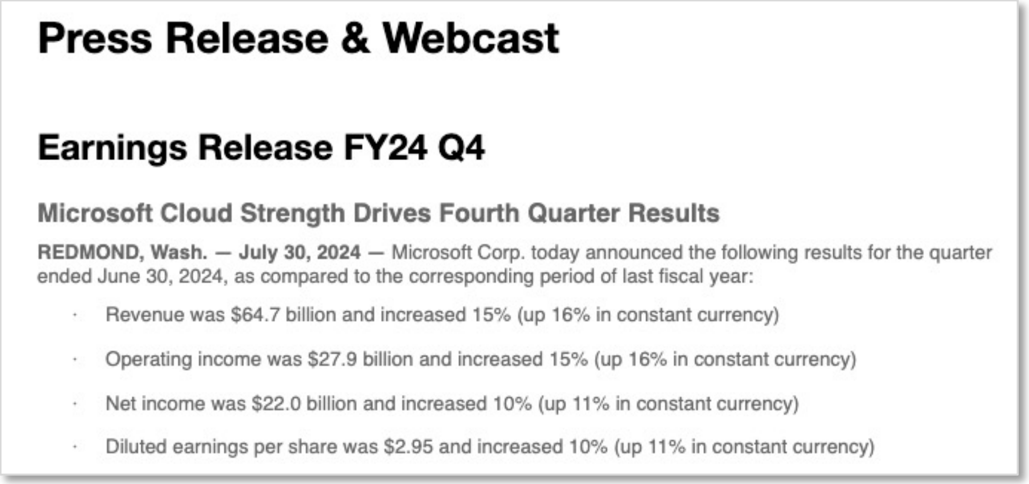
0.0064%

of revenue

also Microsoft 2024

Revenue $64.7 billion (+15%)

per quarter



Press Release & Webcast

Earnings Release FY24 Q4

Microsoft Cloud Strength Drives Fourth Quarter Results

REDMOND, Wash. — July 30, 2024 — Microsoft Corp. today announced the following results for the quarter ended June 30, 2024, as compared to the corresponding period of last fiscal year:

- Revenue was $64.7 billion and increased 15% (up 16% in constant currency)
- Operating income was $27.9 billion and increased 15% (up 16% in constant currency)
- Net income was $22.0 billion and increased 10% (up 11% in constant currency)
- Diluted earnings per share was $2.95 and increased 10% (up 11% in constant currency)

(Inter)national bug bounty program (BB)

Program scope

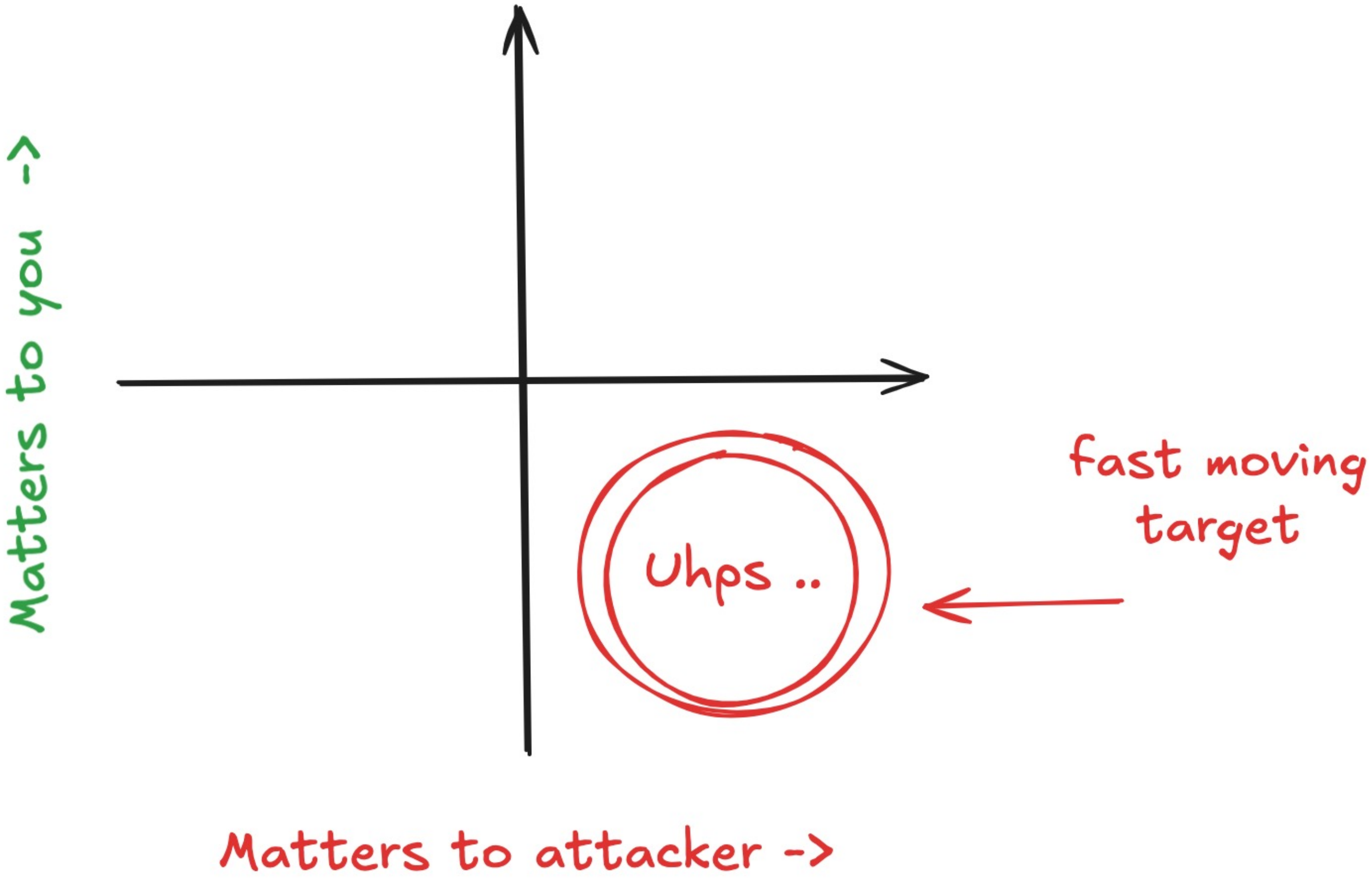
- Critical industries of a nation or economic region (e.g. EU)
- Organizations in critical industries (energy, transport, ..) > User of software
- Products used in critical industries > Producer of software

Benefits of a nation wide program

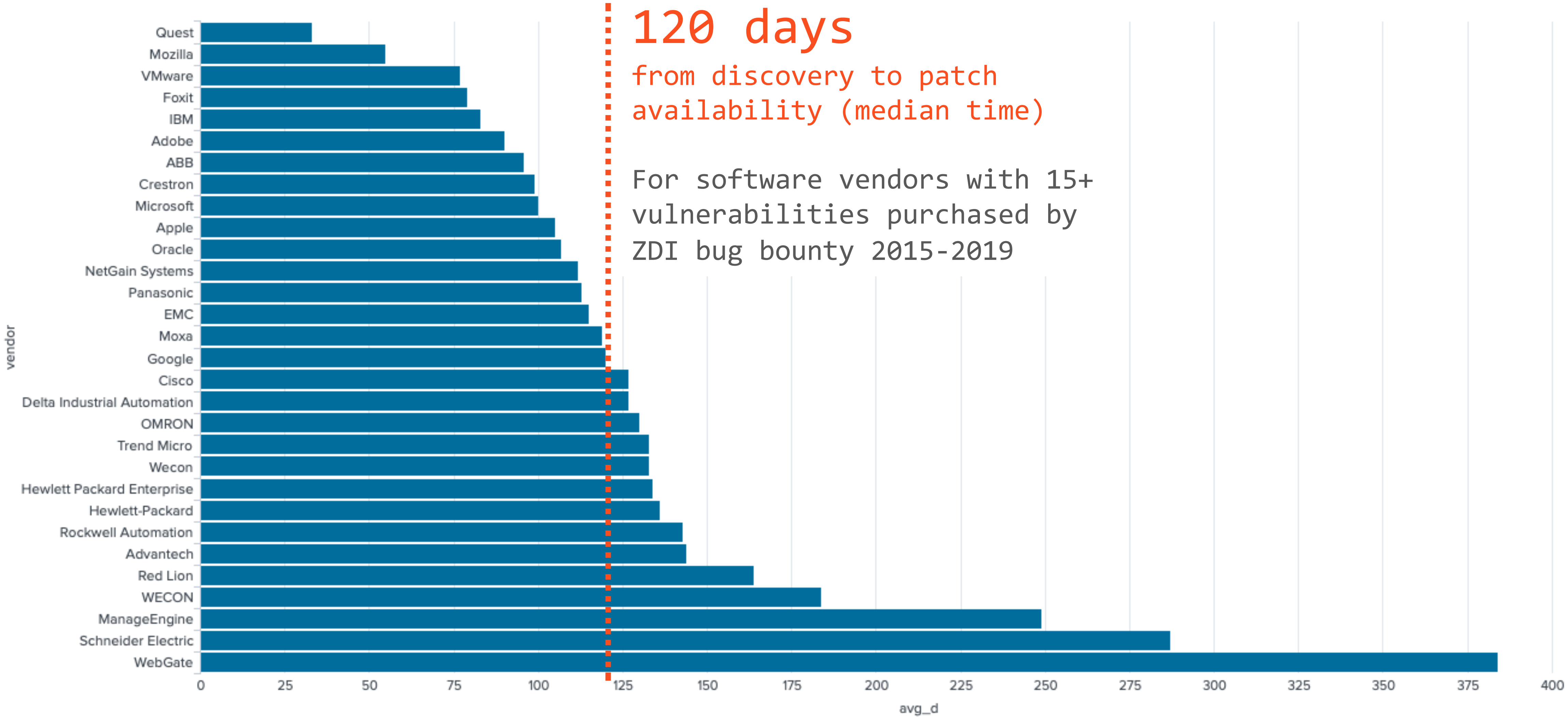
- Scales better and ensures complete coverage of critical industries
- Requires less coordination effort than incentivizing individual organizations
- Economic and effective (no waste of re-testing same products used industry wide)
- Nation-wide telemetry on the exposure of critical industries
- Transparency on the security of producers

It is not your perspective that matters what gets attacked ..

what matters is
the attacker's
perspective



Example: Time to fix from bug bounty data



120 days

from discovery to patch availability (median time)

For software vendors with 15+ vulnerabilities purchased by ZDI bug bounty 2015-2019

[1] The Known Unknowns in Cyber Security https://techzoom.net/papers/the-known-unknowns-in-cyber-security/

[2] Zero Day Initiative (ZDI) https://www.zerodayinitiative.com

Conclusion

Vulnerability markets

Incentives for discoverer, software producer, and users

- Set incentives towards better security

Nation-wide bug bounty program (BB)

- Bug bounties are an established, economic, and scalable security control
- Provide nation-wide coverage and transparency on the security of critical industries
- The economics of nation scale bug bounties is already validated [1]

Representative data is essential for effective security management and setting incentives

[1] Bug Bounty Program of Last Resort
https://techzoom.net/papers/bug-bounty-reloaded

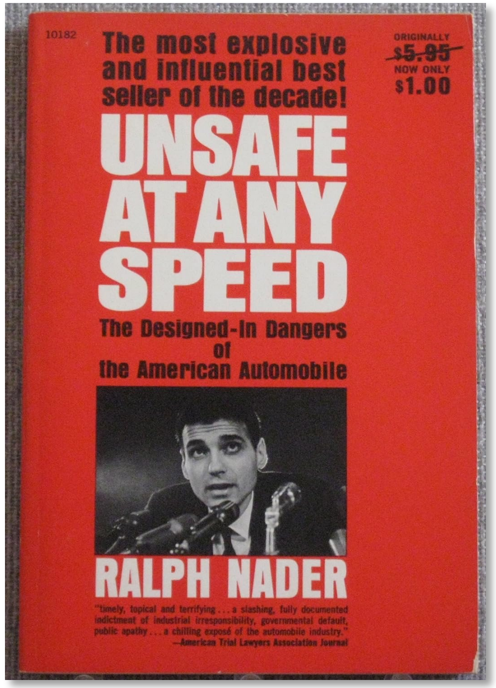
Q & A

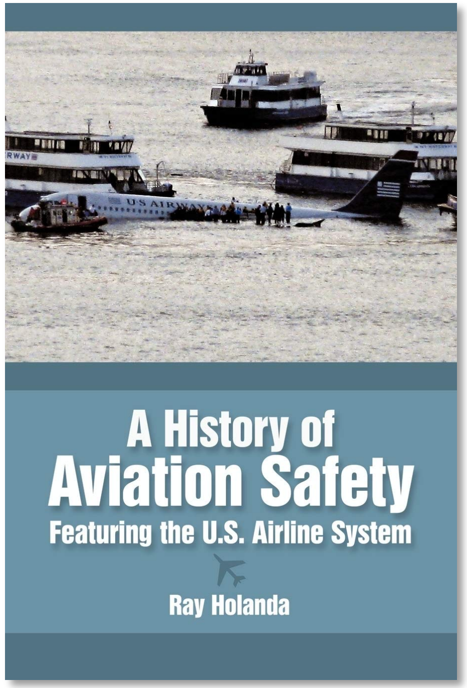
References

References

- Microsoft: No money for bugs (Jul 2010)
  https://www.computerworld.com/article/1510124/microsoft-no-money-for-bugs-2.html
- Celebrating 10 Years of Microsoft's Bug Bounties - The Beginning (Nov 2013)
  https://www.lutasecurity.com/post/celebrating-10-years-of-microsoft-s-bug-bounties-the-beginning
- US cybersecurity chief: Software makers shouldn't lawyer their way out of security responsibilities (Feb 2023)
  https://www.theregister.com/2023/02/28/cisa_easterly_secure_software/
- Digital security of products (Feb 2021)
  https://techzoom.net/tags/oecd-digital-security/

Examples: Aviation & Automotive


10182
The most explosive and influential best seller of the decade!
ORIGINALLY ~~$5.95~~
NOW ONLY $1.00
UNSAFE AT ANY SPEED
The Designed-in Dangers of the American Automobile
RALPH NADER
"timely, topical and terrifying . . . a slashing, fully documented indictment of industrial irresponsibility, governmental default, public apathy . . . a chilling exposé of the automobile industry."
—American Trial Lawyers Association Journal



"Unsafe at Any Speed" played a crucial role in the establishment of the National Highway Traffic Safety Administration (NHTSA) and the development of stronger vehicle safety standards.

https://www.amazon.com/Unsafe-Any-Speed-Ralph-Nader/dp/1561290505

A common theme appears throughout this history: a technological solution is typically available for over a decade to solve a safety problem before it is implemented into the safety system.

https://www.amazon.com/History-Aviation-Safety-Featuring-Airline/dp/144900797X

Key Terms 1

Bug Bounty Program

Bug bounty program (BB) are crowdsourcing initiatives that reward individuals for discovering and reporting vulnerabilities to vulnerability owners.

Vulnerability

A vulnerability is a flaw or weakness in software. It's similar to having a defect in a door lock mechanism, which can potentially be abused or exploited.

Exploit

An exploit is the actual method or tool used to leverage a vulnerability. It's akin to using a specific tool or technique to exploit the defect in the door lock.

Key Terms 2

White-market

Connect vulnerability owners and researchers, with or without a reward mechanism. E.g. bug bounties, coordinated disclosure

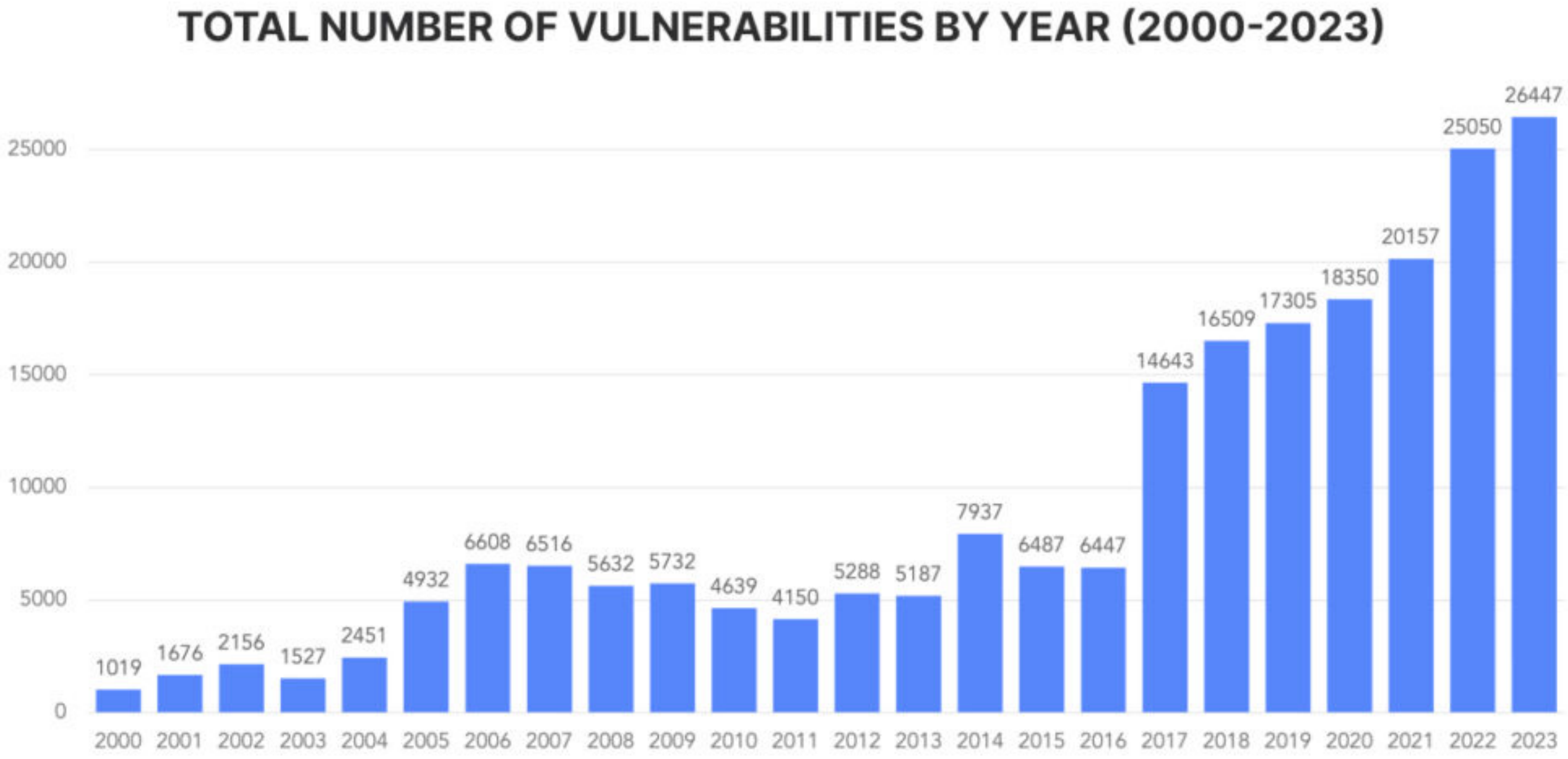
Grey-market

Vulnerability brokers connect sellers with buyers who whose objective is not to fix the vulnerability. Customers are: government intelligence agencies, companies developing and selling exploits used by law enforcement or intelligence

Black-market

Buyers and sellers trade vulnerabilities for offensive use, generally on underground platforms in the dark web, through online chat rooms, or specialized marketplaces

Published vulnerabilities 2000-2023


TOTAL NUMBER OF VULNERABILITIES BY YEAR (2000-2023)