The Law and Economics of Bug Bounties

Amit Elazari, Berkeley Law, CLTC Grantee
@amitelazari #legalbugbounty

@d0tslash

Photo Credit DFSB DE

DJI launches bug bounty program for its software and drones

Posted Aug 28, 2017 by Matt Burns (@mjburnsy)

Crunchbase

DJI

FOUNDED

cyberscoop

SPORTATION | HEALTHCARE | TECHNOLOGY | FINANCIAL | WATCH | LISTEN

GOVERNMENT

How DJI fumbled its bug bounty program and created a PR nightmare

Here come the lawsuits

The ensuing argument between Finisterre and DJI at one point crossed into threats of a Computer Fraud and Abuse Act lawsuit launched by the Chinese company against Finisterre.

dji
THE FUTURE OF POSSIBLE

October 27, 2017

Legal Department
[redacted]
China

Mr. Kevin Finisterre
[redacted]

Re: DJI Bug Bounty Program

Dear Mr. Finisterre,

Thank you for your report to DJI regarding an information security issue. While we appreciate your support, DJI's legal department noticed that you had obtained DJI proprietary and confidential information by accessing DJI server without authorization on or about September 27, 2017, which caused damage to the integrity of the server and aforementioned information. Without waiving other rights under applicable laws, DJI hereby demands you to immediately delete and destroy any copies of information you obtained from such unauthorized access in a complete and irrevocable way.

Please note that your report to DJI and correspondence therefor do not constitute DJI's grant of authorization to you. This could be evidenced by the DJI Bug Bounty Program agreement that DJI has been discussing with you since receiving your report. In addition, in the email dated September 2, 2017 that is followed by your report email dated September 27, 2017, you acknowledged that people who wanted to participate in the DJI Bug Bounty Program do not have authority to access DJI servers: "[y]ou will note that elaborate bugs like this [cannot] be exposed if researchers are prevented from accessing the infrastructure…in theory more bounty worthy bugs could be disclosed IF researchers are allowed to continue."

Please be advised that DJI is in good faith willing to explore the possibility of reaching an amicable resolution regarding the aforementioned unauthorized access and transmission of information, including a release of liability agreed by both parties. In the interim, DJI reserves all rights under applicable laws, including but not limited to, its right of action under the Computer Fraud and Abuse Act.

Should you have any questions, please contact us at legal@dji.com.

Sincerely,

DJI Legal Department

Sources: https://www.cyberscoop.com/dji-bug-bounty-drone-technology-sean-melia-kevin-finisterre/ *but see* https://www.dji.com/newsroom/news/statement-about-dji-cyber-security-and-privacy-practices

KF
@d0tslash

Following

Welp... here it is. The @djiglobal @djienterprise AWS key leak writeup & why I walked away from $30,000 bounty loot. digitalmunition.com/WhyIWalkedFrom...

1:15 AM - 16 Nov 2017

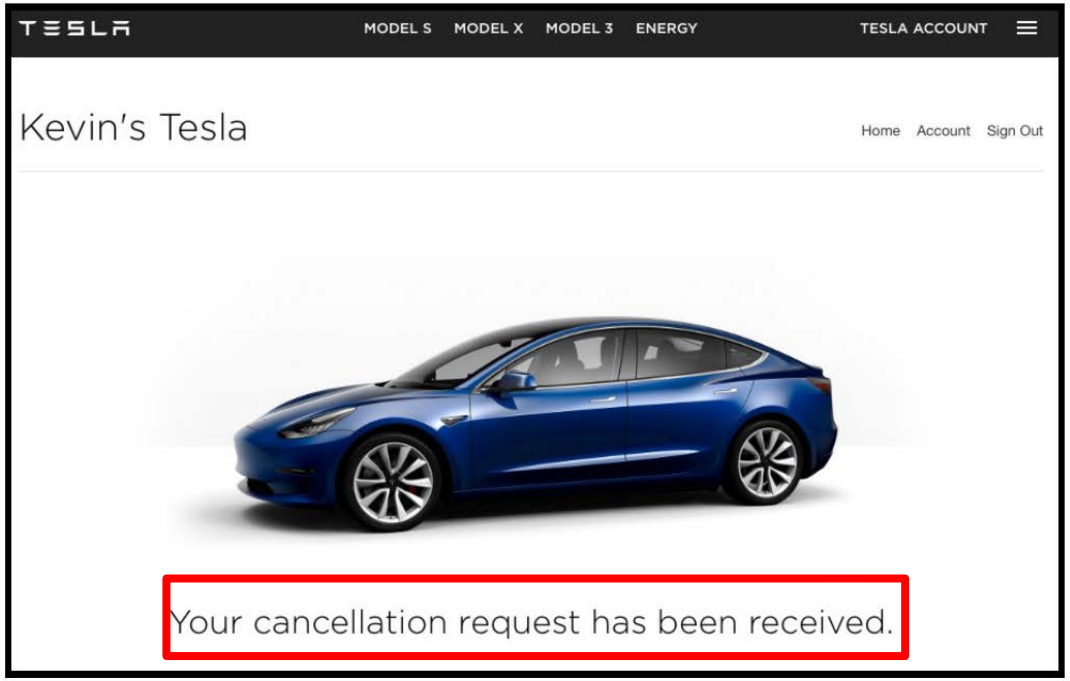
ars TECHNICA BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE FORUMS

DRONE WRECK —

Man gets threats—not bug bounty—after finding DJI customer data in public view

A bug bounty hunter shared evidence; DJI called him a hacker and threatened with CFAA.

SEAN GALLAGHER - 11/17/2017, 10:30 AM



Sources: https://arstechnica.com/information-technology/2017/11/dji-left-private-keys-for-ssl-cloud-storage-in-public-view-and-exposed-customers/ *but see* https://www.dji.com/newsroom/news/statement-about-dji-cyber-security-and-privacy-practices

The Law and Economics of Bug Bounties

Amit Elazari, Berkeley Law, CLTC Grantee
@amitelazari #legalbugbounty

ZDNet

VIDEOS SMART CITIES WINDOWS 10 CLOUD INNOVATION SECURITY TECH PRO MORE NEWSLETTERS ALL WRITERS

MUST READ WINDOWS 10 SPRING CREATORS UPDATE: ACT FAST TO DELAY THIS BIG UPGRADE

Lawsuits threaten infosec research — just when we need it most

Security researchers and reporters have something in common: both hold the powerful accountable. But doing so has painted a target on their backs — and looming threats of legal action and lawsuits have many concerned.

By Zack Whittaker for Zero Day | February 19, 2018 -- 13:00 GMT (05:00 PST) | Topic: Security

Zack Whittaker ✓

@zackwhittaker

Following

I spoke to 11 hackers and security researchers. Not one said they didn't have concerns from the threat of lawsuits or legal action. Some had painful stories to tell.
zd.net/2BDrO7F

http://www.zdnet.com/article/chilling-effect-lawsuits-threaten-security-research-need-it-most/

"Security researchers hesitate to report vulnerabilities and weaknesses to companies for fear of facing legal retribution; these chilling effects invite the release of anonymous, public zero-day research instead of coordinated disclosure. The undersigned urge support for security researchers and reporters in their work, and decry those who oppose research and discussion of privacy and security risks. Harming these efforts harms us all."

https://cdt.org/files/2018/04/2018-04-09-security-research-expert-statement-final.pdf

ACLU

AMERICAN CIVIL LIBERTIES UNION

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

CHRISTIAN W. SANDVIG
2117 Washtenaw Avenue
Ann Arbor, MI 48104,

KYRATSO KARAHALIOS
1109 S. Douglas Avenue
Urbana, IL 61801,

ALAN MISLOVE
5 Grayfield Avenue
West Roxbury, MA 02132,

CHRISTOPHER WILSON
46 Symmes Street, No. 3
Roslindale, MA 02131,

FIRST LOOK MEDIA WORKS, INC.
114 Fifth Avenue, 18th Floor
New York, NY 10011,

Plaintiffs,

-v.-

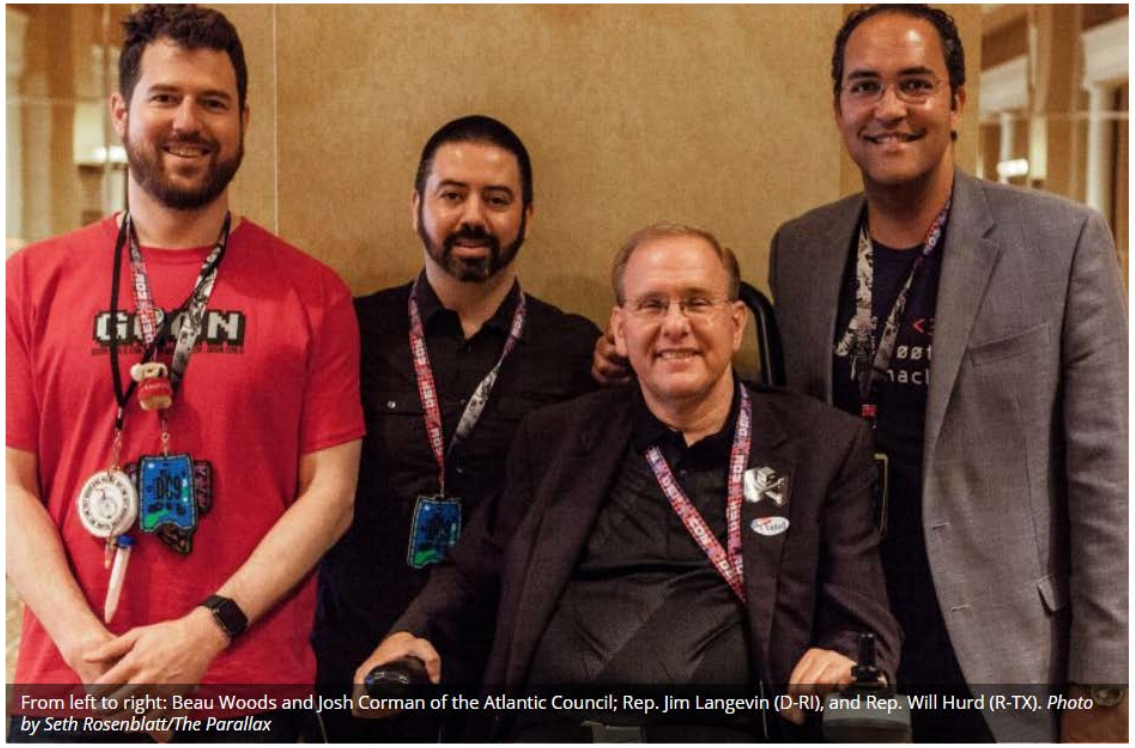
LORETTA LYNCH, in her official capacity as
Attorney General of the United States
950 Pennsylvania Avenue, NW
Washington, DC 20530,

Defendant.

Case No.

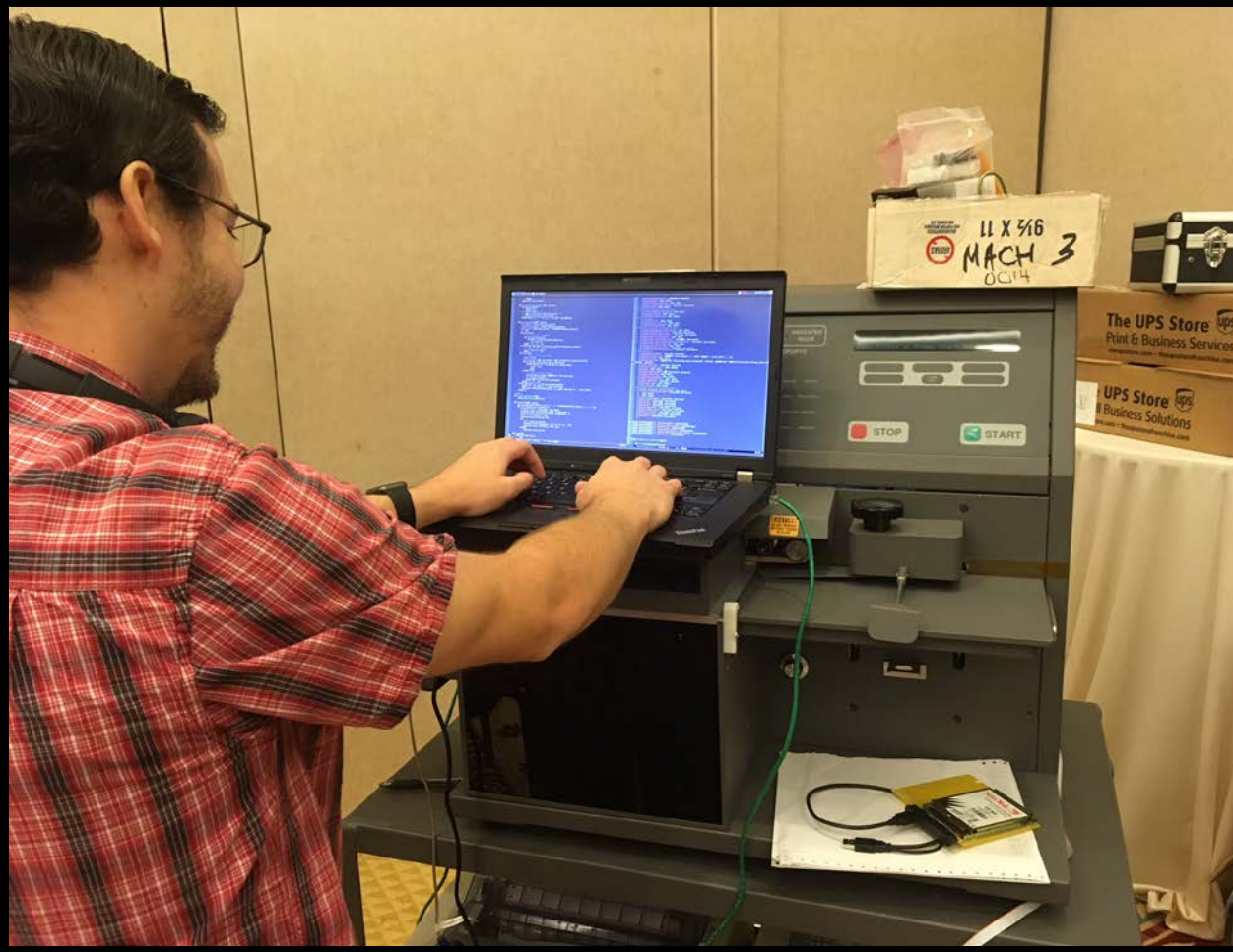
COMPLAINT FOR DECLARATORY AND INJUNCTIVE RELIEF

I Am The Cavalry



From left to right: Beau Woods and Josh Corman of the Atlantic Council; Rep. Jim Langevin (D-RI), and Rep. Will Hurd (R-TX). *Photo by Seth Rosenblatt/The Parallax*

Congressmen at DefCon: Please help us, hackers!



Source: https://www.the-parallax.com/2017/08/01/congress-defcon-help-hackers

Bug Bounty Programs

Google Application Security

Google Vulnerability Reward Program (VRP) Rules

We have long enjoyed a close relationship with the security research community. To honor all the cutting-edge external contributions that help us keep our users safe, we maintain a Vulnerability Reward Program for Google-owned web properties, running continuously since November 2010.

Services in scope

In principle, any Google-owned web service that handles reasonably sensitive user data is intended to be in scope. This includes virtually all the content in the following domains:

Legal notes:

Your submission of a bug constitutes acceptance of the AVG End User License Agreement (www.avg.com/eula) for the corresponding product, and all submissions will be considered user comments in accordance with the EULA.

Legal

In connection with your participation in this program you agree to comply with all applicable local and national laws.

Yahoo reserves the right to change or modify the terms of this program at any time.

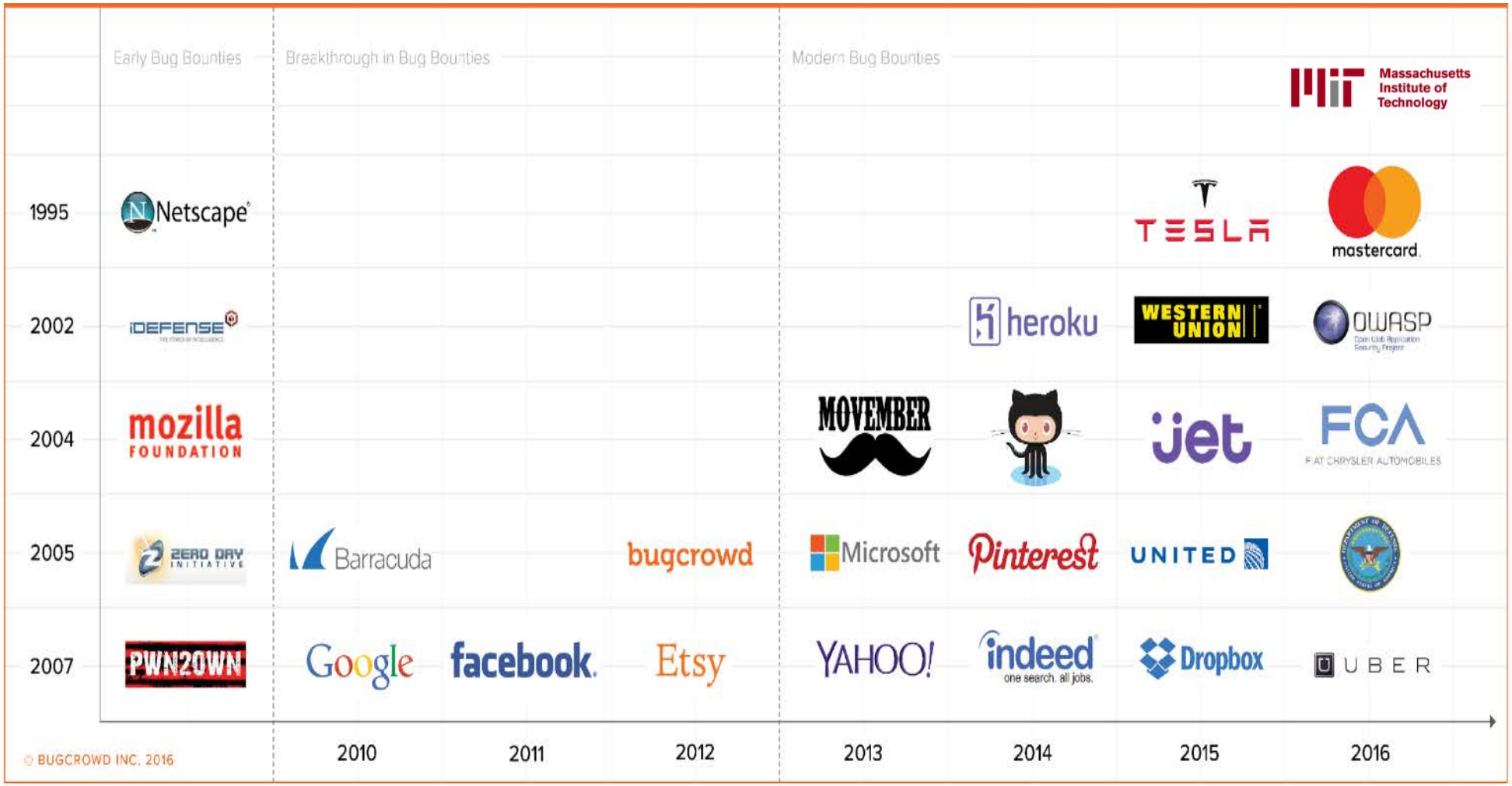
Terms and Conditions

1. ONLY technical vulnerabilities will be accepted and rated.
2. With regarding to security reasons, reporters agree to cooperate with ASRC exclusively on the vulnerability he/she submitted and not disclose any information of vulnerability to any third-parties.
3. In the case that more than one person report the same security vulnerability, the reward will be given to the first person who accomplish a Qualified Reporting.
4. NO LICENSE OR PERMISSION IS GIVEN TO ANY PENETRATION OR ATTACK AGAINST ANY OF ALIBABA SYSTEMS.


I ACCEPT

Disclaimer

2017



https://bugcrowd.com/resources/history-of-bug-bounties

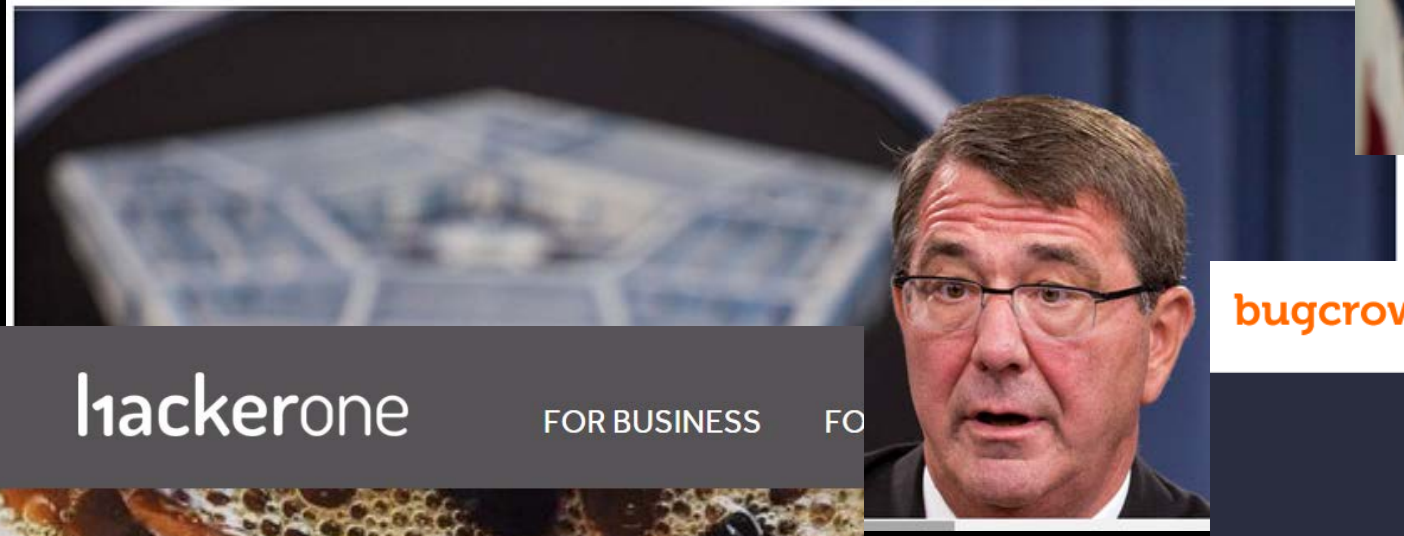
Talk to Me in Numbers...

- **Bugcrowd:**
  - **$6M+ total payouts**
  - **53K+ researchers**
  - **52K+ vulnerabilities**
  - **700+ programs**
- **HackerOne:**
  - **$30M+ total payouts**
  - **800+ programs**
  - **50K+ vulnerabilities (88 individual bounties over $10K)**
  - **70K+ researchers**
- **Google: $9M+ paid**
- **Facebook: $6M+ total payouts**
- **Mozilla & Firefox: ~$1M total payouts**
- **Microsoft: $3M+ total payouts**

Bugcrowd and Hackerone reports, Mozilla, Bug Bounty Program, https://www.mozilla.org/en-US/security/bug-bounty/.

By BRIAN MASTROIANNI / CBS NEWS / March 2, 2016, 1:43 PM

Defense Department invites you to "Hack the Pentagon"



hackerone FOR BUSINESS FO

Starbucks

Inspiring and nurturing the human

www.starbucks.com • @Starbucks •

Policy Hacktivity Thanks Updates (0)

bugcrowd How it Works Solu

Western Union

Moving money for better

$100 – $5,000 per vulnerability

Program Details Hall of Fame


TESLA
Information Security
TESLA
Information Security

UNITED | Proud to fly Team USA

Reservations Travel information Deals & offers MileagePlus®

Jordan Wiens
@psifertex

Home > Contact us > **Bug Bounty Program**

United Airlines bug bounty program

Wow! @united really paid out! Got a million miles for my bug bounty submissions! Very cool.

Most recent account activity

Date	Description	Activity
07/10/2015	United Bug Bounty	1
07/10/2015	United Bug Bounty	999,999

@jackhcable

“The advantages of these bug bounty programs are great because you get recognition from the companies, they pay you and you get to say you found a vulnerability rather than just having to hide it.”

Source: https://www.marketplace.org/2017/08/10/tech/17-year-old-hacked-air-force

Jack Cable
@jackhcable

Following

Can't wait to get started! Crazy how bug bounties can take you from no knowledge of security to a job at the Pentagon in a few years.

> **Defense Digital Svc** @DefenseDigital
> Excited to have @jackhcable come join the Rebel Alliance at DDS in just a couple weeks! Oh, and we are hiring for other talented hackers, engineers, designers, and product people chicagomag.com/city-life/June...

Value of Bug Bounties

- Depending on your security product maturity level, an economically effective way to discover vulnerabilities and prevent data breaches
- Insights on your ***security development life cycle*** (Uber's dash board) and your vendors security posture
- Engagement with the community and communication channel (depending on how prepare and responsive you are) → critical regulatory and legal value
- Hiring channel (security pipe line)
- Reputational value

But, if not planned right → Bug Bounties can go terribly wrong

1983: VRTX
Get a Bug (or $1,000) if You Find a Bug

Get a bug if you find a bug.

Show us a bug in our VRTX® real-time operating system and we'll return the favor. With a bug of your own to show off in your driveway.

There's a catch, though.

Since VRTX is the only microprocessor operating system completely sealed in silicon, finding a bug won't be easy.

Because along with task management and communication, memory management, and character I/O, VRTX contains over 100,000 man-hours of design and testing.

And since it's delivered in 4K bytes of ROM, VRTX will perform for you the way it's performing in hundreds of real-time applications from avionics to video games.

Bug free.

So, to save up to 12 months of development time, and maybe save a loveable little car from the junkyard, contact us. Call (415) 326-2950, or write Hunter & Ready, Inc., 445 Sherman Avenue, Palo Alto, California 94306.

Describe your application and the microprocessors you're using—Z8000, Z80, 68000, or 8086 family. We'll send you a VRTX evaluation package, including timings for system calls and interrupts. And when you order a VRTX system for your application, we'll include instructions for reporting errors.*

But don't feel bad if in a year from now there isn't a bug in your driveway.

There isn't one in your operating system either.

HUNTER & READY

VRTX

Operating Systems in Silicon.

*Call or write for details. But, considering our taste in cars, you might want to accept our offer of $1,000 cash instead. © 1983 Hunter & Ready, Inc.

2017:
Senate Bill to Enact Bug Bounty at DHS

115TH CONGRESS
1ST SESSION

S. 1281

To establish a bug bounty pilot program within the Department of Homeland Security, and for other purposes.

IN THE SENATE OF THE UNITED STATES

MAY 25, 2017

Ms. HASSAN (for herself, Mr. PORTMAN, Mrs. MCCASKILL, and Ms. HARRIS) introduced the following bill; which was read twice and referred to the Committee on Homeland Security and Governmental Affairs

---

A BILL

To establish a bug bounty pilot program within the Department of Homeland Security, and for other purposes.

https://techcrunch.com/2017/01/19/hacking-the-army/,
https://www.gpo.gov/fdsys/pkg/BILLS-115s1281is/pdf/BILLS-115s1281is.pdf

"Indeed, in many cases, the FTC has alleged, among other things, that ***the failure to maintain an adequate process for receiving and addressing security vulnerability reports from security researchers*** and academics is an unreasonable practice, in violation of Section 5 of the FTC Act"

STATE OF DELAWARE

DEPARTMENT OF TECHNOLOGY AND INFORMATION

801 Silver Lake Blvd.
Dover, Delaware 19904

Doc Ref Number:	SE-VUL-001	**Revision Number:** 0
Document Type:	Enterprise Policy	**Page:** 1 of 8
Policy Title:	Vulnerability Disclosure Policy	

Synopsis:	Guide collaboration between the public and DTI regarding reported vulnerabilities.

https://dti.delaware.gov/information/standards-policies.shtml

Keren Elazari:

Hackers: the Internet's immune system

TED2014 · 16:39 · **Filmed** Mar 2014

27 subtitle languages

View interactive transcript

Add to list

Like

Download

Rate

Share this idea

Facebook LinkedIn Twitter Link Email Embed

2,069,029 Total views

So why we are still attacking friendly hackers **instead of helping them to help us**?

Who dictates the rules of this bug bounty/VDP economy?

Who safeguards the legal interests of the individual hackers, the crowd, given this is a very risky legal business?

Companies often put hackers in “legal” harm’s way, shifting the risk for liability towards hackers instead of authorizing access and creating “safe harbors”

Legal

In connection with your participation in this program you agree to comply with all applicable local and national laws.

Legal points

We are unable to issue rewards to individuals who are on sanctions lists, or who are in countries (e.g. Cuba, Iran, North Korea, Sudan and Syria) on sanctions lists. You are responsible for any tax implications depending on your country of residency and citizenship. There may be additional restrictions on your ability to enter depending upon your local law.

This is not a competition, but rather an experimental and discretionary rewards program. You should understand that we can cancel the program at any time and the decision as to whether or not to pay a reward has to be entirely at our discretion.

Of course, your testing must not violate any law, or disrupt or compromise any data that is not your own.

“You agree to comply with all applicable local and national laws”

See for more examples the terms of Twitter, Yahoo, Avg, Google, NetGear

Hackers Might be Forced into Contractual Breach and Civil and Criminal Liability by the Terms

Legal notes:

Your submission of a bug constitutes acceptance of the AVG End User License Agreement (www.avg.com/eula) for the corresponding product, and all submissions will be considered user comments in accordance with the EULA.

AVG EULA: "**You may not**…(A) reverse engineer, disassemble, decompile, translate, reconstruct, transform or extract any Solution or any portion of the Solution (including without limitation any related malware signatures and malware detection routines), or …. **attempt to gain unauthorized access** to any Solution or to networks connected to it, or to content stored or delivered through it, by any means, including by **hacking, spoofing or seeking to circumvent** or defeat any firewalls or other technological or other protections or security measures".

Terms and Conditions

1. ONLY technical vulnerabilities will be accepted and rated.
2. With regarding to security reasons, reporters agree to cooperate with ASRC exclusively on the vulnerability he/she submitted and not disclose any information of vulnerability to any third-parties.
3. In the case that more than one person report the same security vulnerability, the reward will be given to the first person who accomplish a Qualified Reporting.
4. NO LICENSE OR PERMISSION IS GIVEN TO ANY PENETRATION OR ATTACK AGAINST ANY OF ALIBABA SYSTEMS.

Microsoft Cloud Bounty Program

Microsoft Cloud Bounty Program

PROGRAM DESCRIPTION

In September 2014, we launched the first phase of the Microsoft Online Services Bug Bounty program, and expanded the program in April 2015 and the August 2015 to include various Azure and additional Office 3
initiative, individuals across the globe have the opportunity to earn a bounty on vulnerability submissions for specific Online Services provided by Microsoft. The program is now referred to as the Microsoft Cloud B

Qualified submissions are eligible for a minimum payment of $500 USD up to a maximum of $15,000 USD. Bounties will be paid out at Microsoft's discretion based on the impact of the vulnerability.

As of July 17, 2018, identity related vulnerabilities have been removed from the Cloud Bounty Program and moved into the Microsoft Identity Bounty Program. Go here for more information on the new bounty pro
https://www.microsoft.com/msrc/bounty-microsoft-identity.

WHAT CONSTITUTES AN ELIGIBLE SUBMISSION FOR O365, MICROSOFT AZURE, AND MICROSOFT ACCOUNT?

Generally, bounties will be paid for significant web application vulnerabilities found in eligible online service domains. Additionally, in order for submissions to be processed as quickly as possible and to ensure the highest payment for the type of vulnerability being reported, submissions should include concise repro steps that are easily understood.

LEGAL NOTICE

To get additional information on the Microsoft legal guidelines please go here.

Microsoft Bounty Terms and Conditions

Last updated: February 1, 2018

CODE OF CONDUCT

By participating in the Program, you will follow these rules:

- Don't do anything illegal.
- Don't engage in any activity that exploits, harms, or threatens to harm children.
- Don't send spam. Spam is unwanted or unsolicited bulk email, postings, contact requests, SMS (text messages), or instant messages.
- Don't share inappropriate content or material (involving, for example, nudity, bestiality, pornography, graphic violence, or criminal activity).
- Don't engage in activity that is false or misleading.
- Don't engage in activity that is harmful to you, the Program, or others (e.g., transmitting viruses, stalking, posting terrorist content, communicating hate speech, or advocating violence against others).
- Don't infringe upon the rights of others (e.g., unauthorized sharing of copyrighted material) or engage in activity that violates the privacy of others.
- Don't help others break these rules.

If you violate these Terms, you may be prohibited from participating in the Program in the future and any Submissions you have provided may be deemed to be ineligible for Bounty payments.

NO WARRANTIES

MICROSOFT, AND OUR AFFILIATES, RESELLERS, DISTRIBUTORS, AND VENDORS, MAKE NO WARRANTIES, EXPRESS OR IMPLIED, GUARANTEES OR CONDITIONS WITH RESPECT TO THE PROGRAM. YOU UNDERSTAND THAT YOUR PARTICIPATION IN THE PROGRAM IS AT YOUR OWN RISK. TO THE EXTENT PERMITTED UNDER YOUR LOCAL LAW, WE EXCLUDE ANY IMPLIED WARRANTIES IN CONNECTION WITH THE PROGRAM. YOU MAY HAVE CERTAIN RIGHTS UNDER YOUR LOCAL LAW. NOTHING IN THESE TERMS IS INTENDED TO AFFECT THOSE RIGHTS, IF THEY ARE APPLICABLE.

LIMITATION OF LIABILITY & BINDING ARBITRATION

If you have any basis for recovering damages in connection with the Program (including breach of these Terms), you agree that your exclusive remedy is to recover, from Microsoft or any affiliates, resellers, distributors, third-party providers, and vendors, direct damages up to $100.00. You can't recover any other damages or losses, including direct, consequential, lost profits, special, indirect, incidental, or punitive. These limitations and exclusions apply even if this remedy doesn't fully compensate you for any losses or fails of its essential purpose or if we knew or should have known about the possibility of the damages. To the maximum extent permitted by law, these limitations and exclusions apply to anything or any claims related to these Terms and the Program.

Third-party bugs

If issues reported to our bug bounty program affect a third-party library, external project, or another vendor, Tesla reserves the right to forward details of the issue to that party without further discussion with the researcher. We will do our best to coordinate and communicate with researchers through this process.

After reading hundreds of terms, I found that

While programs usually clearly disclose the “technical scope” of authorization given to the researcher, the legal scope of “authorization” and “access” is often ignored, non-existing or lacking.

Safe harbor is the exception not the standard.

- 17 out of 77 analyzed policies on *Hackerone* platform (1/2016), had a clause stating they will not take legal action against Researchers (a *partial safe harbor*)

- The average level of the Flesch *ReadingEase* index of those policies is 39.6, meaning it required some college education (on average) to understand

Laszka, A., Zhao, M., Malbari, A. & Grossklags, J. “The Rules of Engagement for Bug Bounty Programs”. Proceedings of the Twenty-Second International Conference on Financial Cryptography and Data Security (FC)

Hackers care about their legal risk and legal incentives should matter

"The threat of legal action was cited by 60% of researchers as a reason they might not work with a vendor to disclose"

Researchers fear "they may be subject to legal proceedings *if they disclose their work*."

September 2015, the National Telecommunications and Information Administration (NTIA) a survey among 414 security researchers participating in coordinated disclosure

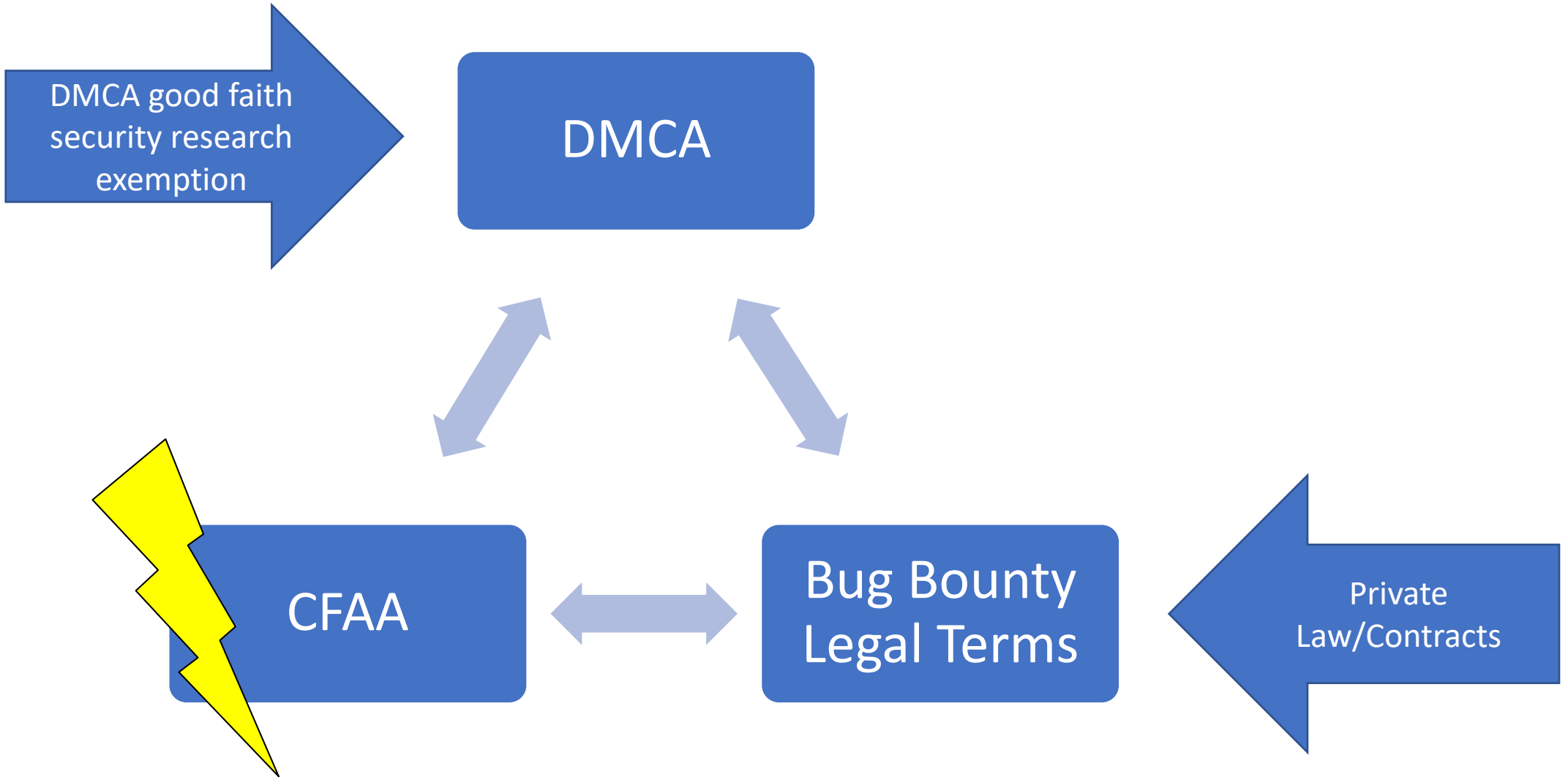
- "Nearly ***half of the researchers*** interviewed mentioned the DMCA specifically as a source of legal risk … In some cases, researchers avoided working with devices and systems protected by access controls to eliminate the legal risks stemming from the DMCA."
- "***Half of the interview subjects reported the CFAA as a primary source of risk***. Of those, more than half reported avoiding some or all types of research that might implicate the CFAA".

source: CDT, https://cdt.org/files/2018/04/2018-03-27-Risk-Basis-for-Security-Research-FNL.pdf, March 2018

Hackers care about Communication/Trust and the Policy Language Matters in this Respect

- "The vast majority of researchers (92%) generally engage in some form of coordinated vulnerability disclosure. When they have gone a different route (e.g., public disclosure) **it has generally been because of frustrated expectations, mostly around communication**." (NTIA Survey)
- "[T]he results indicate that **rules with more content** (e.g., more detailed list of included / excluded areas and issues) and explicit statements on duplication, disclosure, etc., **are associated with more bugs resolved**." (Laszka et al., 2018)

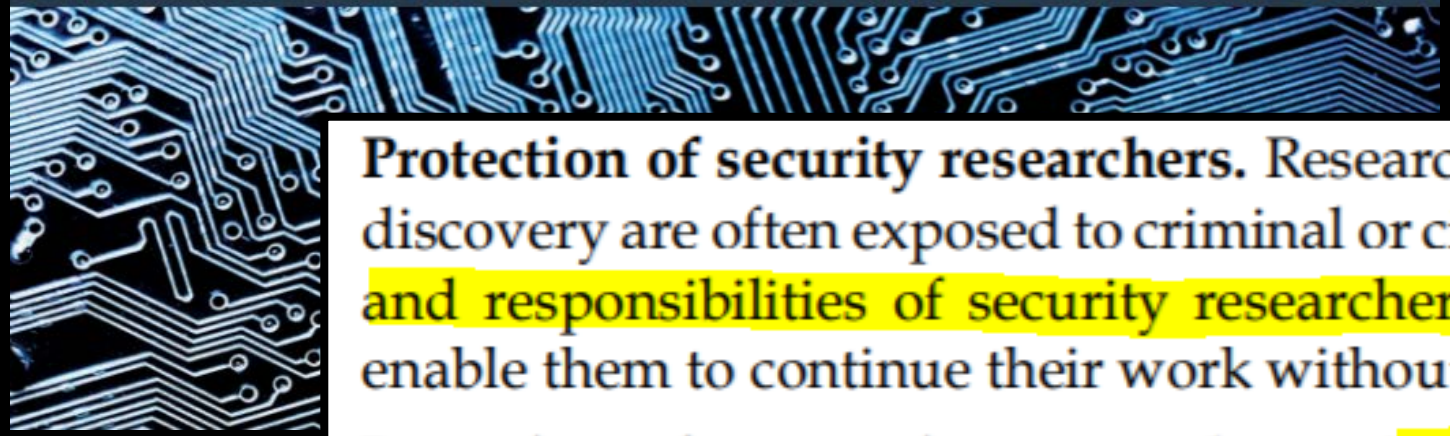
Why VDP/Bug Bounty Terms are so Important



Software Vulnerability Disclosure in Europe

Technology, Policies and Legal Challenges

Report of a CEPS Task Force



Protection of security researchers. Researchers involved in vulnerability discovery are often exposed to criminal or civil liability.[4] The legal liability and responsibilities of security researchers should be fully clarified to enable them to continue their work without fear of prosecution.

Incentives for security researchers. Appropriate policies should be adopted with the aim of encouraging 'white-hat hackers' to actively participate in coordinated vulnerability disclosure programmes.

General Data Protection Regulation

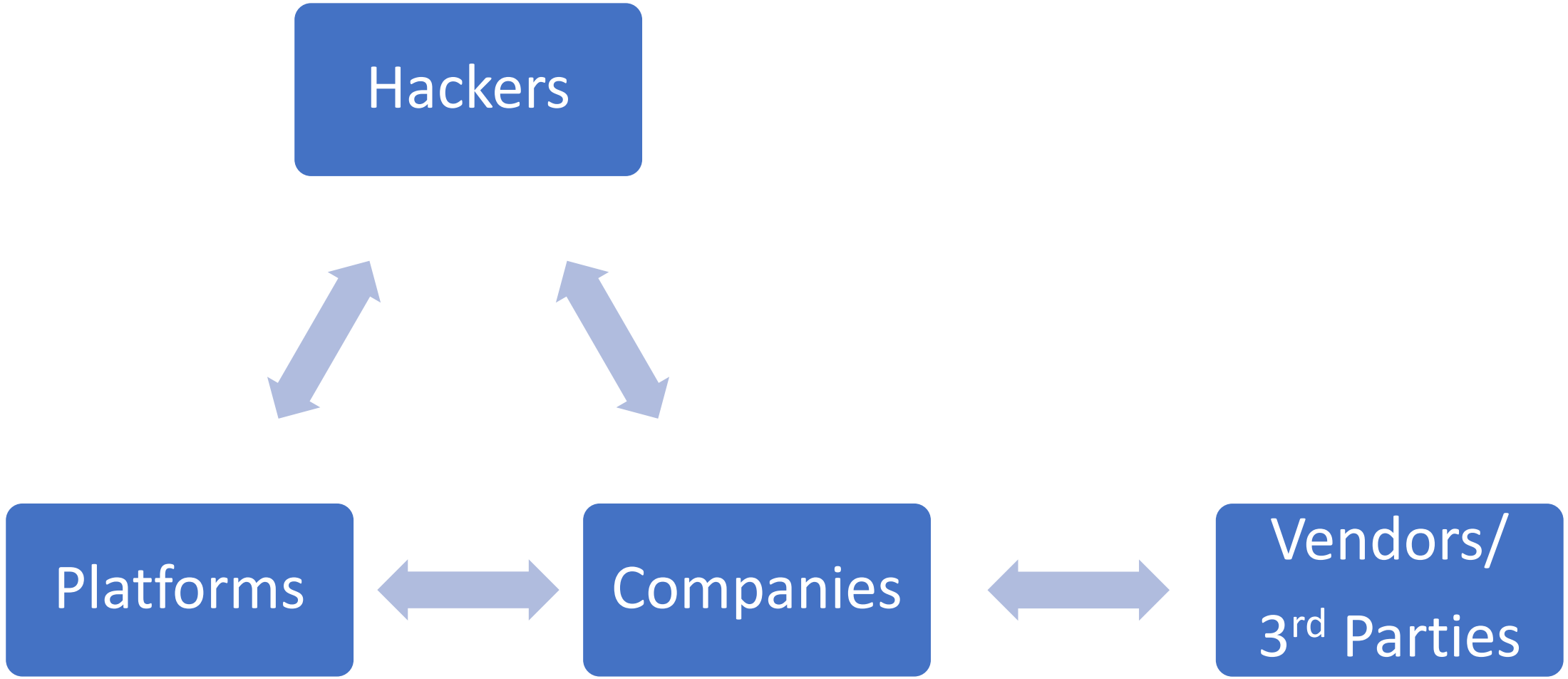
"a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed."

ARTICLE 29 DATA PROTECTION WORKING PARTY

18/EN

WP250rev.01

Potential Agency Problem – Different Legal/Economic Interests



What can we do?

Hackers want to play by the rules but the rules won't let them: therefore, clearly the rules should change.

Ethics goes both ways.

Cybersecurity Unit
Computer Crime & Intellectual Property Section
Criminal Division
U.S. Department of Justice

1301 New York Avenue, N.W., 6th Floor, Washington, D.C. 20530 - CYBERSECURITY.CCIPS@USDOJ.GOV - (202)514-1026

A Framework for a Vulnerability Disclosure Program for Online Systems[1]

Version 1.0 (July 2017)

DoJ “Framework for a Vulnerability Disclosure Program for Online Systems”

- Set guidelines: “Describe authorized and unauthorized conduct in **plain, easily understood terms**”
- Establish **Boundaries**: Prevent damage to system integrity and maintain users privacy, use test accounts, detail prohibited techniques
- **Be prepared**: “Crawl, Walk, Run”, VDP, staffing, patching, regulatory implications (notification)
- Engagement of with the crowd (tweaking the policy, CTF, “Treasure” maps)
- Safe Harbors

https://www.justice.gov/criminal-ccips/page/file/983996/download

DoJ “Framework for a Vulnerability Disclosure Program for Online Systems” – Legal Implications

- Careful and Clear Scoping: “Consider whether any of the network components or data within the scope of the vulnerability disclosure program **implicates third-party interests**”
- Setting expectations on PoCs: “Describe the form in which proof of a vulnerability should be submitted”: Provide examples and case studies of effective PoCs that maintain the integrity of the system and protect users privacy

https://www.justice.gov/criminal-ccips/page/file/983996/download

Lacking Terms Vs. Clear Safe Harbors

- ✘ The submission of a bug "constitutes acceptance of our *End User License Agreement." The EULA will usually prohibit testing, hacking or "spoofing"*
- ✘ *Stating the researcher should "comply with all laws" without authorizing access under the relevant laws*
- ✘ *Creating complex disclosures where contracts are hyperlinked and legal terms are buried in multiple links*
- ✘ *Failing to provide clear technical scopes and instructions with respect to allowed disclosures and techniques as well as prohibited usage*

- ✓ *Prioritize the legal part of your bug bounty policy*
- ✓ *Eliminate paradoxical terms: Researchers should be exempted from general EULA "anti-hacking" language*
- ✓ *Simplify disclosures and create legal educational resources for researchers*
- ✓ *Include a contractual commitment not to pursue legal action for in-scope testing*
- ✓ *Provide Specific authorization (with clear scope) for the purpose of the CFAA, DMCA and other relevant laws in light of DOJ framework*

Specific authorization (with clear scope) for the purpose of the CFAA and the DMCA in light of DOJ framework - Make the Exception the Standard

DOJ Framework suggest for example this language:

1. The organization *will not to pursue* civil action for accidental, good faith violations of its policy or initiate a complaint to law enforcement for unintentional violations.

2. The organization considers activities conducted consistent with the policy to *constitute "authorized" conduct* under the Computer Fraud and Abuse Act, [The DMCA and applicable anti-hacking laws such as Cal. Penal Code 502(c)][my addition – A.E.]".

3. If legal action is initiated by a third party against a party who complied with the vulnerability disclosure policy, the organization will take steps to make it known, either to the public or to the court, that the individual's actions were conducted in compliance with the policy.

https://www.justice.gov/criminal-ccips/page/file/983996/download

How many programs adopted an *Explicit Safe Harbor (clear authorization)* – ***1 Year*** after the publication of the DOJ framework?

#LEGALBUGBOUNTY HALL OF FAME

1. Dropbox
2. DJI*
3. Ed
4. LegalRobot
5. Keeper*
6. HackerOne
7. Upserve
8. Zomato
9. RightMesh
10. Bugcrowd

11. Block.one
12. liberapay
13. Tezos
14. Augur
15. Tron
16. OS.University
17. ChainRift
18. tendermint
19. Telenet
20. Shopify
21. Mozilla
22. Tesla

http://amitelazari.com/%23legalbugbounty-hof

Standardization of Legal language in VDP/BBP

- One language of safe harbor akin to Creative Commons/Open Source: see #legalbugbounty
- Create an industry standard that will serve as a benchmark and signal to hackers if companies don’t adopt it
- Reduce the informational burden and increase hackers’ awareness towards terms
- Reduce transaction and drafting costs, simplify the disclosures
- Create a reputation system for legal terms

EdOverflow / legal-bug-bounty

Watch 0 | Star 6 | Fork 0

Code | Issues 1 | Pull requests 0 | Projects 0 | Wiki | Insights

Branch: master ▾ legal-bug-bounty / templates / safe_harbor.md

Find file | Copy path

EdOverflow Fix "my". eaff338 16 days ago

1 contributor

32 lines (24 sloc) | 4.32 KB

Raw | Blame | History

The below safe harbor language is based on Amit Elazari's general academic research in this field, the DOJ guidelines on this issue (which you must read! - https://www.justice.gov/criminal-ccips/page/983996/download) and some leading policies like Dropbox.

Template 1: Explicit safe harbor with good faith violations

> To encourage responsible disclosures, we will not pursue civil action or initiate a complaint to law enforcement for accidental, good faith violations of this policy. We consider security research and vulnerability disclosure activities conducted consistent with this policy to constitute "authorized" conduct under the Computer Fraud and Abuse Act, the DMCA and applicable anti-hacking laws such as Cal. Penal Code 502(c). We waive any DMCA claim against you for circumventing the technological measures we have used to protect the applications in scope.
>
> If legal action is initiated by a third party against you and you have complied with this bug bounty policy, we will take steps to make it known that your actions were conducted in compliance with this policy.
>
> Please understand that if your security research involves the networks, systems, information, applications, products, or services of another party (which is not us), that third party may determine whether to pursue legal action. We cannot and do not authorize security research in the name of other entities.
>
> You are expected, as always, to comply with all applicable laws.
>
> Please submit a report to us before engaging in conduct that may be inconsistent with or unaddressed by this policy.

https://github.com/EdOverflow/legal-bug-bounty/blob/master/templates/safe_harbor.md

EULA Conflict

- The Bug Bounty Terms [use a term you previously defined] supplement the terms our [X] User Agreement [With Hyperlink], [Y] Agreement [With Hyperlink] with you [collectively the “Agreements”]. The terms of those Agreements will apply to your use and participation in our Bug Bounty Program. If any inconsistency exists between the terms of such Agreements and the Bug Bounty Terms, the Bug Bounty Terms will prevail with respect to your participation in the Bug Bounty Program.

https://github.com/EdOverflow/legal-bug-bounty/blob/master/templates/safe_harbor.md

Third Party/Vendor Authorization

"We will not share your report with a third-party without gaining their commitment they will not pursue legal action against you or refer you the public inquiry. Please note again that we can't authorize out-of-scope testing in the name of third parties and such testing is beyond the scope of the program."

- Establish a process to report a bug to a third party
- Commitment to the researcher + waiver
- Get contractual commitments and authorization
- Encourage vendors to adopt VDP process with a safe harbor

https://github.com/EdOverflow/legal-bug-bounty/blob/master/templates/safe_harbor.md

Proof of concepts

Issue type	When to report the issue
XSS	For XSS, a simple `alert(document.domain)` should suffice.
RCE	Please only execute harmless code. Simply printing something or evaluating an expression should be enough to demonstrate the issue.
SQLi	Report it as soon as you have a SQL error that indicates SQL injection or you are able to disclose the SQL server's version number.
Unvalidated redirect	Set the redirect endpoint to http://example.com if possible.
CSRF	Either attach a file to demonstrate the issue or paste the code in a code block in your report.
SSRF	Do not go playing around on any internal networks. Report as soon as you believe that you have a potential SSRF issue and we will look into it for you.
LFI	The same applies here — please do not go against the guideline listed in the *Disclosure policy* section. We investigate LFI reports in a dev environment to make sure it is valid.

Source: https://github.com/EdOverflow/legal-bug-bounty, credit @edoverflow

ars TECHNICA

BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE

RULES OF ENGAGEMENT —

New open source effort: Legal code to make reporting security bugs safer

The Disclose.io framework seeks to standardize "safe harbor" language for security researchers.

SEAN GALLAGHER - 8/2/2018, 6:00 AM

disclose.io is a collaborative and vendor-agnostic project to standardize best practices around safe harbour for good-faith security research.

Read the core terms

The project expands on the work done by Bugcrowd and CipherLaw's Open Source Vulnerability Disclosure Framework, Amit Elazari's #legalbugbounty, and Dropbox's call to protect security researchers.

Safe Harbor

When conducting vulnerability research according to this policy, we consider this research to be:

- Authorized in accordance with the Computer Fraud and Abuse Act (CFAA) (and/or similar state laws), and we will not initiate or support legal action against you for accidental, good faith violations of this policy;
- Exempt from the Digital Millennium Copyright Act (DMCA), and we will not bring a claim against you for circumvention of technology controls;
- Exempt from restrictions in our Terms & Conditions that would interfere with conducting security research, and we waive those restrictions on a limited basis for work done under this policy;
- Lawful, helpful to the overall security of the Internet, and conducted in good faith.

You are expected, as always, to comply with all applicable laws.

If at any time you have concerns or are uncertain whether your security research is consistent with this policy, please submit a report through one of our Official Channels before going any further.

@d0tslash

DJI Security Response Center Home Policy Report a Bug

“Waiver and Release

By participating in this program and abiding by these terms, DJI grants you limited “authorized access” to its systems under the Computer Fraud and Abuse Act in accordance with the terms of the program and will waive any claims under the Digital Millennium Copyright Act (DCMA) and other relevant laws. Furthermore, if you conduct your security research and vulnerability disclosure activities in accordance with the terms set forth in this policy, DJI will take steps to make known that your activities were conducted pursuant to and in compliance with this policy in the event of any law enforcement or civil action brought by anyone other than DJI.”

boingboing / CORY DOCTOROW / 8:28 AM THU DEC 21, 2017

Ars Technica's Dan Goodin is being sued by Keeper Security over an article about a defect in its password manager

Guidelines:

This Vulnerability Disclosure Policy sets out expectations when working with good-faith hackers, as well as what you can expect from us.

If security testing and reporting is done within the guidelines of this policy, we:

- Consider it to be authorized in accordance with Computer Fraud and Abuse Act,
- Consider it exempt from DMCA, and will not bring a claim against you for bypassing any security or technology controls,
- Consider it legal, and will not pursue or support any legal action related to this program against you,
- Will work with you to understand and resolve the issue quickly, and
- Will recognize your contributions publicly if you are the first to report the issue and we make a code or configuration change based on the issue.

https://bugcrowd.com/keepersecurity

Consequences of Complying with This Policy

We will not pursue civil action or initiate a complaint to law enforcement for accidental, good faith violations of this policy. We consider activities conducted consistent with this policy to constitute "authorized" conduct under the Computer Fraud and Abuse Act. To the extent your activities are inconsistent with certain restrictions in our Acceptable Use Policy, we waive those restrictions for the limited purpose of permitting s der this policy. We will not bring a DMCA claim against you for circumventing the techno used to protect the applications in scope.

If legal action is initiated by a third party against you and you have complied with Dropbox will take steps to make it known that your actions were conducted in comp

TECHNOLOGY

Dropbox revamps vulnerability disclosure policy, with hopes that other companies follow suit

Justin Gardner
@Rhynorater

Following

Props to Dropbox for adopting such a solid Safe Harbor policy! I'll be hacking on your program because of it. @AmitElazari @Dropbox #bugbounty

Amit Elazari @AmitElazari · Mar 8

#legalbugbounty I want to congratulate @Dropbox bug bounty for being a pioneer and following DOJ framework and adding an explicit safe harbor (CFAA authorization)!!! now how about DMCA and other relevant laws? @d0nutptr

> **Kumar Saurabh** @kumarsaurabh__
>
> Replying to @AmitElazari @d0nutptr
>
> Yeah! hackerone.com/dropbox

1 2 15

d0nut
@d0nutptr

Following

Replying to @AmitElazari @Dropbox

Thanks for the feedback, Amit! We added a DMCA clause, live now:
hackerone.com/dropbox/policy …

Mozilla Security
@MozillaSecurity

Following

We've added an explicit Safe Harbor provision to our Bug Bounty program! Many thanks to @AmitElazari for the inspiration and a shoutout to @dropbox @scarybeasts blog.mozilla.org/security/2018/ …

3:16 PM - 1 Aug 2018

24 Retweets **41** Likes

24 41

Private Ordering Shaping Cybersecurity Policy: The Case of Bug Bounties

Amit Elazari Bar On*

An edited version of this paper is forthcoming in Rewired: Cybersecurity Governance, Ryan Ellis and Vivek Mohan eds. Wiley, 2018

---

* Adv., LL.M. (Doctoral Law Candidate, J.S.D., UC Berkeley School of Law). The author would like to thank the Center for Long-Term Cybersecurity at the University of Berkeley, California for supporting this project and future related projects it entails, to professor Chris Jay Hoofnagle for his valuable advice and to Dropbox's security and legal teams, for being a pioneer in adopting safe harbors for security researchers in bug bounties. The author also thanks Keren Elazari for inspiration, support and advice. All errors remain my own. This is not legal advice. This project has a GitHub resource page available at https://github.com/EdOverflow/legal-bug-bounty. The majority of the terms-of-use discussed in this paper were accessed by May, 2017 or before.

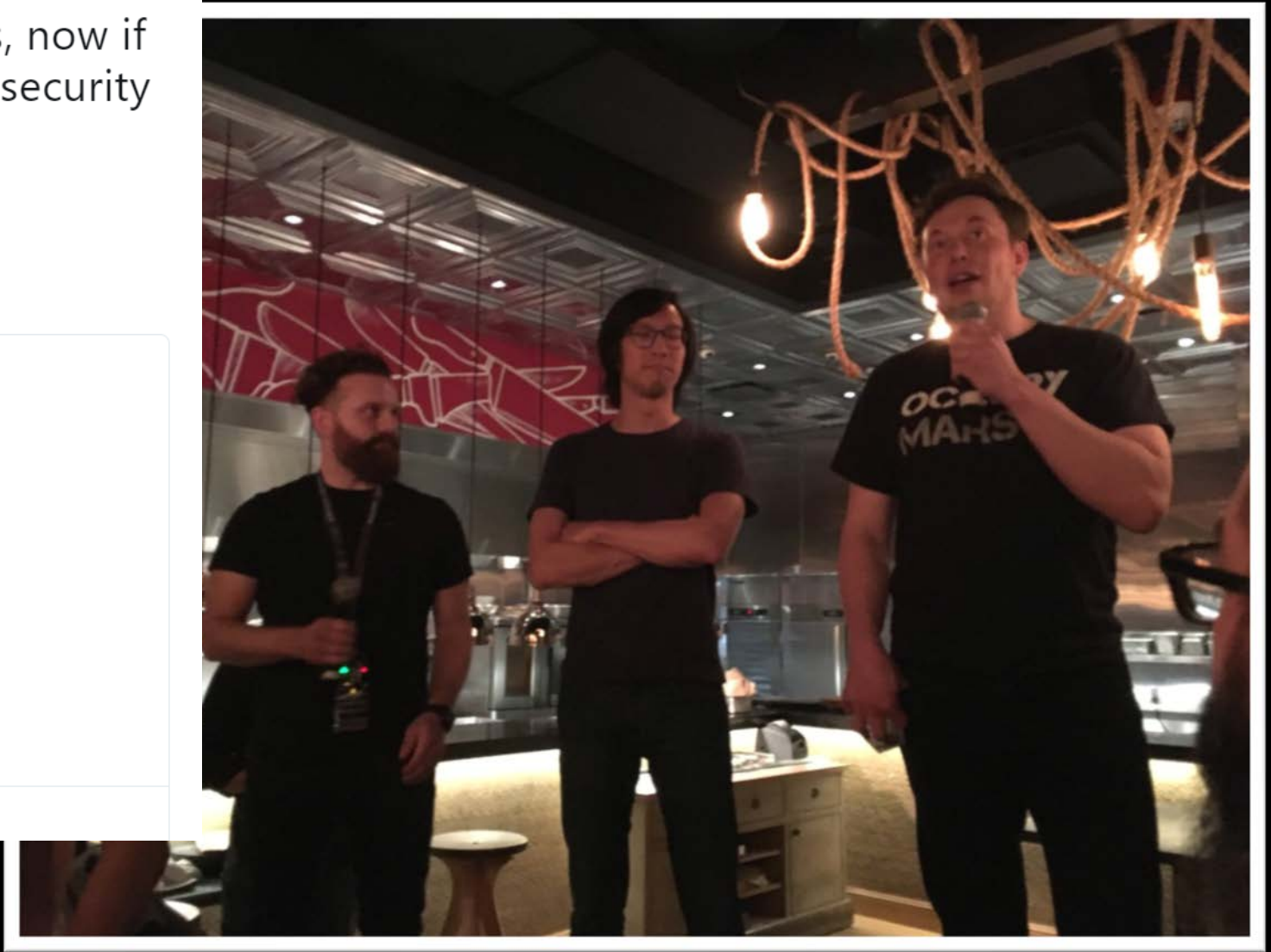
Bitquark ✨ @ Defcon
@Bitquark

Following

We've updated our bug bounty terms, now if you accidentally brick your car doing security research we'll help you fix it 🚗 🔧
tesla.com/about/security (cc @Tesla @Bugcrowd @defcon @elonmusk @AmitElazari @k3r3n)

TESLA

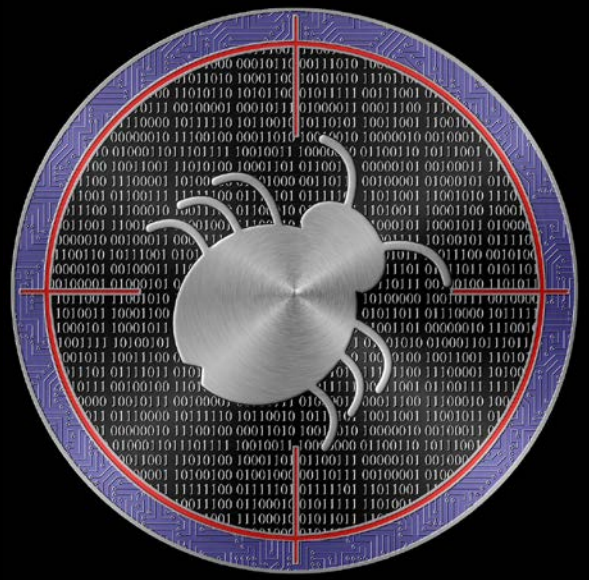
Product Security | Tesla



For the avoidance of doubt,

- If, through your good-faith security research, you (a pre-approved, good-faith security researcher) cause a software issue that requires your research-registered vehicle to be updated or "reflashed," as an act of goodwill, Tesla shall make reasonable efforts to update or "reflash" Tesla software on the research-registered vehicle by over-the-air update, offering assistance at a service center to restore the vehicle's software using our standard service tools, or other actions we deem appropriate. Tesla has complete discretion as to the software or other assistance that will be provided and it may be only for a limited number of times. Tesla's support does not extend to any out-of-pocket expenses (e.g. towing) incurred by you. Tesla reserves the right to limit the number of service requests per pre-approved, good-faith researcher and unregister a research-registered vehicle at any time.
- Tesla considers that a pre-approved, good-faith security researcher who complies with this policy to access a computer on a research-registered vehicle has not accessed a computer without authorization or exceeded authorized access under the Computer Fraud and Abuse Act ("CFAA").
- Tesla will not bring a copyright infringement claim under the Digital Millennium Copyright Act ("DMCA") against a pre-approved, good-faith security researcher who circumvents security mechanism, so long as the researcher does not access any other code or binaries.
- Tesla will not consider software changes, as a result of good-faith security research performed by a good-faith security researcher, to a security-registered vehicle to void the vehicle warranty of the security-registered vehicle, notwithstanding that any damage to the car resulting from any software modifications will not be covered by Tesla under the vehicle warranty.

This community has the power to change this reality, and this can start right now



Amit Elazari, Doctoral Candidate, UC Berkeley School of Law, CLTC Grantee
@amitelazari, www.amitelazari.com
#legalbugbounty