Quantitative Cyber-Security

Colorado State University

Yashwant K Malaiya

CS559

Quick Research Presentations Th a

CSU Cybersecurity Center
Computer Science Dept

Thursday

- Everyone must participate
  - Share questions/comments
  - Take notes
- Presenters: limit yourself to 5 minutes, 1 minute for q/c
  - Upload your slides and be ready to present
- Ujwal will run videos/presentations by some distance students
- The Peer Review Form (Canvas Assignments) due on Sat. Novelty/ Interest, Technical/ Research, Presentation

Presentations Today

T11 **Quant. examination of phishing**
Shree Harini Ravichandran

10 **Examination of the time a vulnerability remains undiscovered**
Luis Rodriguez
Luis Pineiro Rivera
Austen Weaver

9 **Quant modeling of the time to vulnerability discovery**
Alexandre Dubois

8 **Quant modelling of Vulnerability markets**
Wei Chen
Waylon Jepsen

7 **Annual security breach costs incurred to society/government/nations**
Zijuan Liu
Ya-Hsin Cheng
Sarah Houlton

3 **Quant. Examination of schemes for discovering previously unknown vulnerabilities**
Don Neumann

5 **Assessing probability of security breaches**
Siddhi Kotian
Dhruv Padalia

Time a vulnerability goes undiscovered, viewed along Zero-Day discoveries

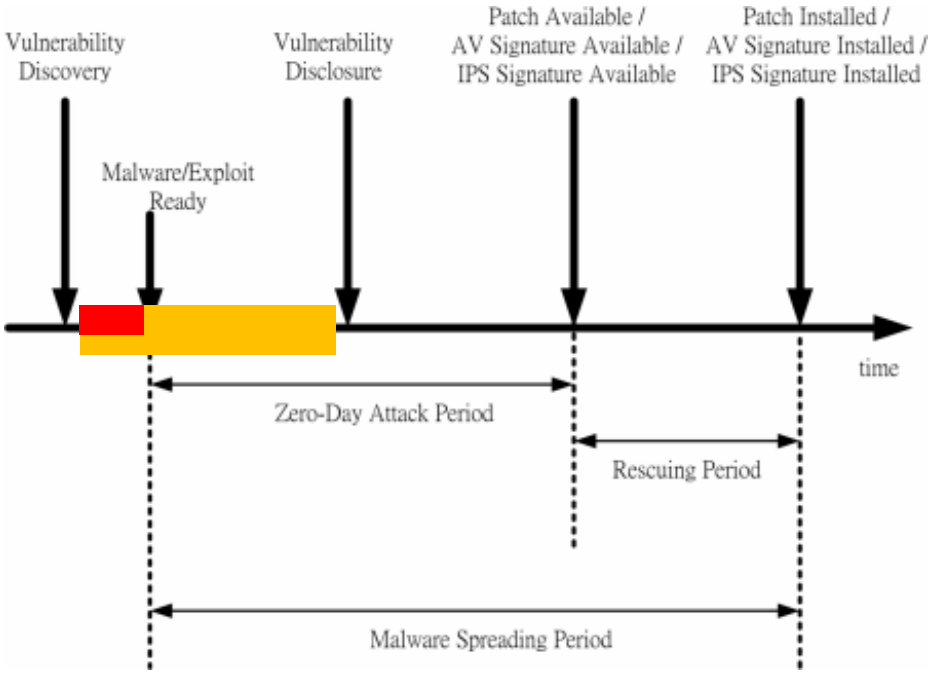
Luis Rodriguez

Research Scope

- Most vulnerabilities that stay hidden for a long time are Zero-Day
  - Newly discovered software hole
  - No time to patch up in time of attack
- What effect can a zero-day vulnerability have if it stayed stealthy?

Discovery/Zero Day Timeline

- Life cycle of a zero-day vulnerability
- Time for exploitation
- Time window for developers to discover bug
  - Incredibly valuable for both attackers and defenders [1]



Colorado State University

Vulnerability Window

- Vulnerabilities that are inactive for such a long period of time take a similar amount of time to be comprehended [2]
- These attacks are becoming more prevalent and dangerous throughout different industries
  - E.g. Stuxnet within industrial control systems
- During this *window of vulnerability*, victims do not have time to retaliate

Dormancy and Market value

- Dormancy of a vulnerability can be heavily correlated to underground market activity [3]
- Increased effort to find zero-days
  - From both attackers and defenders
- Higher incentive to keep potentially valuable exploits hidden for longer

References

- Chia-Nan Kao *et al*., "A predictive zero-day network defense using long-term port-scan recording," *2015 IEEE Conference on Communications and Network Security (CNS)*, Florence, 2015, pp. 695-696, doi: 10.1109/CNS.2015.7346890.
  - https://ieeexplore.ieee.org/document/7346890
- H. Al-Rushdan, M. Shurman, S. H. Alnabelsi and Q. Althebyan, "Zero-Day Attack Detection and Prevention in Software-Defined Networks," 2019 International Arab Conference on Information Technology (ACIT), Al Ain, United Arab Emirates, 2019, pp. 278-282, doi: 10.1109/ACIT47987.2019.8991124.
  - https://ieeexplore.ieee.org/document/8991124
- Allodi, Luca. 2017. “Economic Factors of Vulnerability Trade and Exploitation,” *2017 ACM SIGSAC Conference on Computer and Communications Security (CCS '17)*. Association for Computing Machinery, New York, NY, USA, 1483–1499. DOI:https://doi.org/10.1145/3133956.3133960
  - https://dl.acm.org/doi/10.1145/3133956.3133960

Examination of the Time a Vulnerability Remains Undiscovered

By Luis E Pineiro Rivera

Overview

Introduction

Weaponized Zero-Day Vulnerabilities

Commercial Products

Introduction

- What are zero-day vulnerabilities?
- Why are they hard to find?
- What's the Impact?
  - Economic
  - Military

Weaponized Zero-Day Vulnerabilities

1. STUXNET
    1. Iran Centrifuge Nuclear Program
    2. Targeted SCADA Systems
    3. No Signature
2. Georgia
    1. Russia disrupts Government and Industry entities
    2. Defaced Georgian President
    3. Redirected Traffic to fake websites
    4. 2008 and 2019
        1. 2008 – First known simultaneous Cyber attack and shooting war

Commercial Vulnerability Products

- IronNet
  - Founded by Gen (Ret.)Keith Alexander, Former Director of NSA and 1st USCYBERCOM Commander
  - Collective Cybersecurity Defense
- K2 Cybersecurity
  - Application API Function Call verification
- MixMode.ai
  - Unsupervised Machine Learning to learn user and network behaviors
- Kaspersky
  - Cybersecurity firm with tons of experience
- SANDIA National Labs
  - Government and Industry Cyber Research Center
- Google Project ZERO
  - Group of Cybersecurity experts finding zero-day exploits

Summary

- Introduction
- Weaponized Zero-Day Vulnerability Attacks
- Commercial Vulnerability Products

Questions?

Examination of the Time a Vulnerability Remains Undiscovered

By: Austen Weaver

CS559 – Quantitative Security

Online Masters of Computer Science

Colorado State University

Time to Discovery

- Time to Discovery is an unknown
- Some vulnerabilities are discovered before release
- Others, not for decades after
- Does anything effect time to Discovery?

Possible Correlations?

Device Count

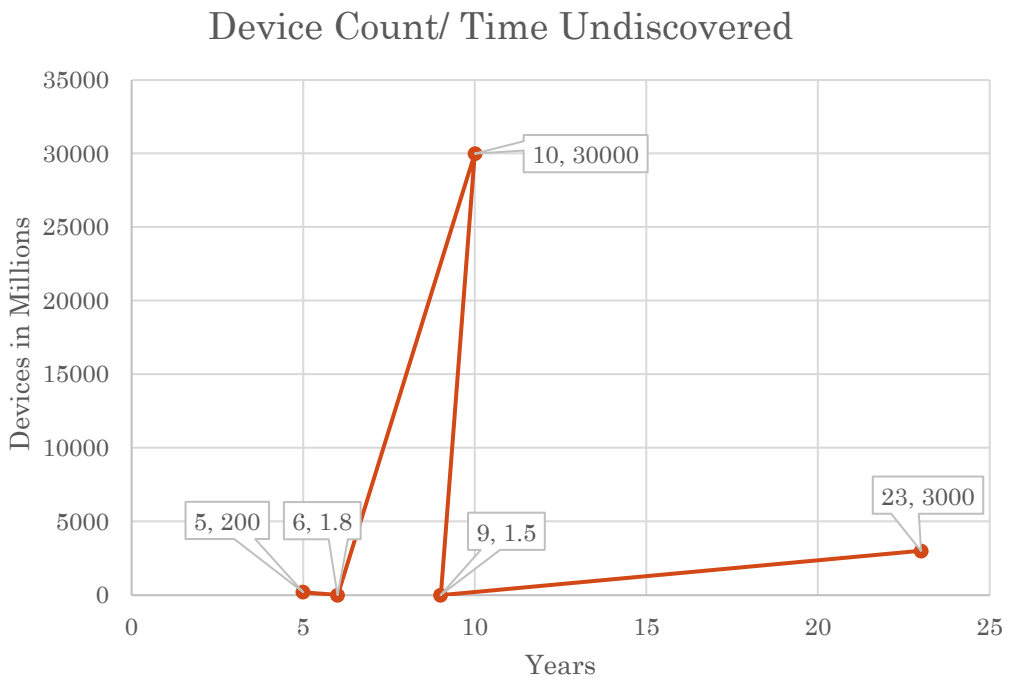
Type of Product:

- Military
- Industrial
- Commercial
- Personal Device

Difficulty of Accessing Vulnerability

Data device has access to:

- Personally Identifiable Information
- Financial
- Raw Data



Are Published Vulnerabilities the True time of Discovery?

- Spectre / Meltdown
  - Discovered by 4 teams at approximately the same time
- Governments / Nation-States
  - NSA
- Unknown Bad Actors
  - Black-Hat
  - Nation-States

Conclusion

- No strong correlations between vulnerability discovery time to predict a time to discovery.
- It is unknown if the first time a vulnerability is published it is its true initial discovery.

References

- [1] A. Hashim, "latesthackingnews.com," 8 September 2020. [Online]. Available: https://latesthackingnews.com/2020/09/08/critical-vulnerability-found-in-cisco-jabber-for-windows/. [Accessed 9 September 2020].
- [2] R. Z. Y. S. Dikla Barda, "Amazons Alexa Hacked," 13 August 2020. [Online]. Available: https://research.checkpoint.com/2020/amazons-alexa-hacked/. [Accessed 9 September 2020].
- [3] R. Jennings, "TPM-Fail: Intel and STMicro 'Fix' 26-Year-Old Vulnerability," 14 November 2019. [Online]. Available: https://securityboulevard.com/2019/11/tpm-fail-intel-and-stmicro-fix-26-year-old-vulnerability/. [Accessed 9 September 2020].
- [4] A. Laurie, "New Vulnerability Could Put IoT Devices at Risk," 19 August 2020. [Online]. Available: https://securityintelligence.com/posts/new-vulnerability-could-put-iot-devices-at-risk/. [Accessed 9 September 2020].
- [5] J. Fingas, "AMD CPUs for the past 9 years are vulnerable to data leak attacks," 8 March 2020. [Online]. Available: https://www.engadget.com/2020-03-08-amd-cpu-take-a-way-data-leak-security-flaw.html. [Accessed 9 September 2020].
- [6] A. Greenberg, "Triple Meltdown: How So Many Researchers Found a 20-Year-Old Chip Flaw at the Same Time," 7 January 2018. [Online]. Available: https://www.wired.com/story/meltdown-spectre-bug-collision-intel-chip-flaw-discovery/. [Accessed 9 September 2020].
- [7] T. Herr, B. Schneier and C. Morris, "Taking Stock: Estimating Vulnerability Rediscovery," July 2017. [Online]. Available: https://www.belfercenter.org/publication/taking-stock-estimating-vulnerability-rediscovery. [Accessed 9 September 2020].

Quantitative modeling of the time to vulnerability discovery

Alexandre Dubois
CS559 - Quantitative Security - Assignment 1

Summary

Context

A vulnerability is defined as:

"a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source" [1].

Context

Data source on vulnerabilities:

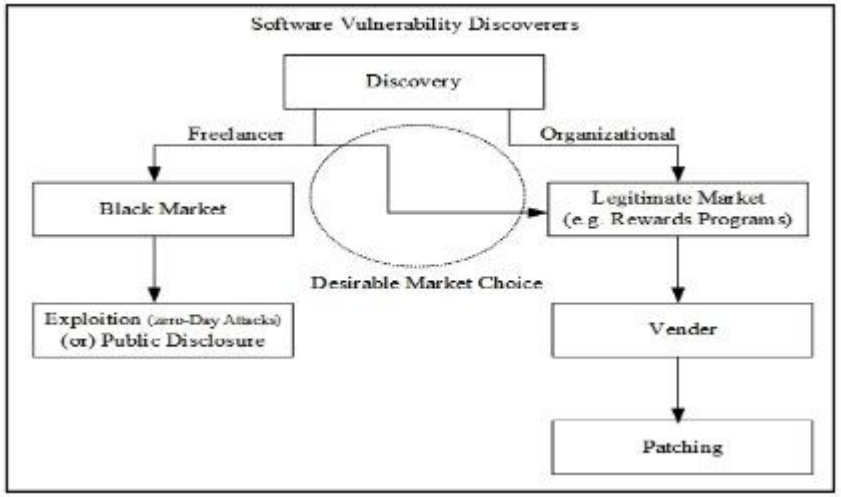
- National Vulnerability Database: https://nvd.nist.gov/
- SecurityFocus Vulnerability Database: https://www.securityfocus.com/vulnerabilities

Influential organizations:

- US government and agencies
- Universities: KTH, CSU, ...
- Critical industries: nuclear, aeronautics, defense, pharmaceutical, banking, ...

Recent developments

- New policy for vulnerability discovery disclosure of US government agencies
- New modeling of time to vulnerability discovery: Time Between each Vulnerability Discovery (TBVD)[2]
- Study of vulnerability discoverers motivations [5]



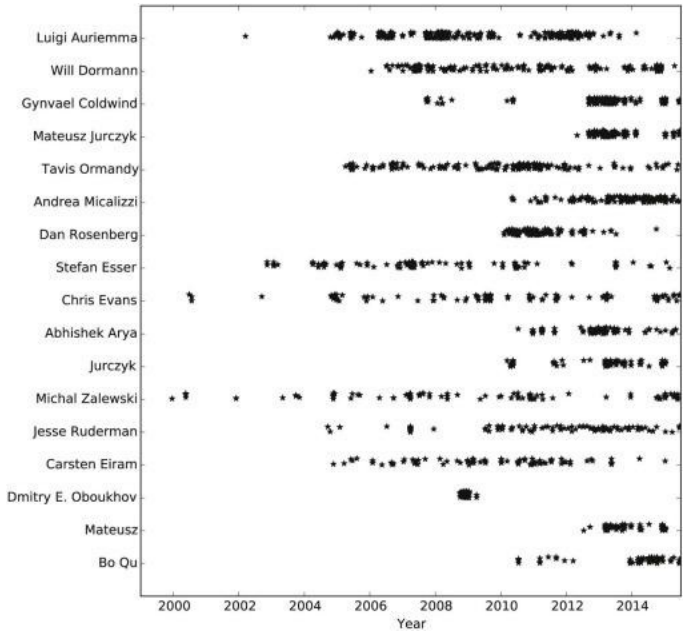
The events in the vulnerability life cycle [5]

Recent developments

Table 1 – Top 15 vulnerability analysts.

Analyst	Title	Company	No vulns	Mean TBVD
Luigi Auriemma	Independent Researcher	ReVuln	313	14 days
Mateusz Jurczyk	Security Researcher	Google	288	7 days
Will Dormann	Vulnerability Analyst	CERT/CC	260	13 days
Gynvael Coldwind	IT Security Engineer	Google	202	14 days
Tavis Ormandy	Information Security Engineer	Google	178	21 days
Andrea Micalizzi	Security Researcher	Self-employed	160	12 days
Dan Rosenberg	Senior Security Researcher	Azimuth Security	128	13 days
Stefan Esser	Head of R&D	SektionEins GmbH	120	37 days
Chris Evans	Chrome Security	Google	112	48 days
Abhishek Arya	Information Security Engineer	Google	105	16 days
Michal Zalewski	Information Security Televangelist	Google	94	60 days
Jesse Ruderman	Security Bug Hunter	Mozilla	91	43 days
Carsten Eiram	Chief Research Officer	Risk Based Security	85	44 days
Dmitry E. Oboukhov	Security & Firmware Consultant	Data Security Laboratory	82	2 days
Bo Qu	Architect, Security Engineer	Palo Alto Networks	81	23 days
Mean			**153**	**20 days**

Top 15 vulnerability analysts [2].



Vulnerability disclosure dates for the top 15 most productivevulnerability analysts [2]

References

1 R. Shirey, “Rfc2828: Internet security glossary,” USA, 2000.

2P. Johnson, D. Gorton, R. Lagerstr¨om, and M. Ekstedt, “Time between vulnerability disclosures: A measure of software product vulnerability,”Computers & Security, vol. 62, pp. 278 – 295, 2016. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167404816300955

3(September 3rd 2020) Administration moving forward with vulnerability disclosure policies. [Online]. Available: https://gcn.com/articles/2020/09/03/omb-cisa-vdp.aspx

4(September 2nd2020) Binding operational directive 20-01: Develop and publish a vulnerability disclosure policy. [Online]. Available: https://cyber.dhs.gov/bod/20-01/

5A. M. Algarni and Y. K. Malaiya, “Most successful vulnerability discoverers: Motivation and methods,” inProceedings of the International Conference on Security and Management (SAM).The Steering Committee of The World Congress in Computer Science, Computer, 2013,p. 1.

Economic modeling of vulnerability markets

--Progress Report

Reported by: WEI CHEN

Reporting Time: 04/25/2020

CONTENT

Part 01

The reasons for forming the software vulnerability market

The reasons for forming the software vulnerability market

Background and significance

Computer crime and online infringement in various fields are becoming more and more serious.

the security problem of network information systems is not only a technical problem, but also a problem of economy, management, and operation.

Part 02

Analyze the structure of the software vulnerability market

Analyze the structure of the software vulnerability market

First, in terms of software vulnerabilities, software manufacturers and security researchers have vigorously debated whether they need to actively find and publicly disclose vulnerabilities.

Second, for the defender, the software vulnerability information can indicate to the defender where to fix the product.

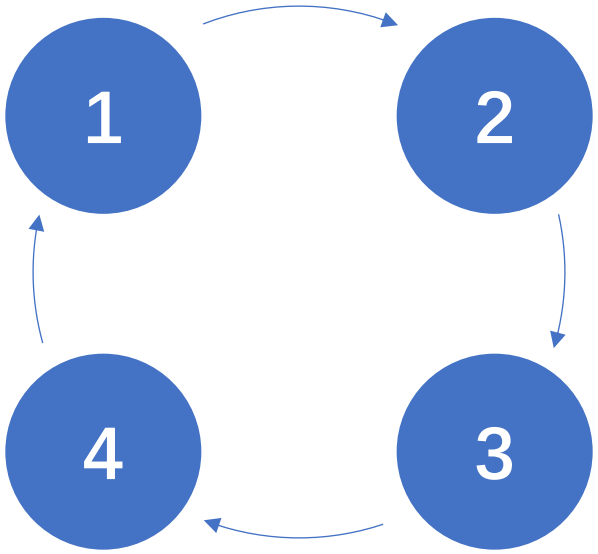
Third, product vulnerability information affects consumers' expectations of software products

Part 03

Preliminary model structure

1.Utility function for software consumers

$$U = \theta[V - k(\delta)B(t)]t - p$$



$$U = \theta[V - k(\delta)B(t)]t - p \geq 0$$

So the consumers satisfied the θ⩾θi choose to buy software

$$\theta \geq \frac{p}{[V - k(\delta)B(t)]t} = \theta_i$$

2. Profit function of software manufacturers

1

$$\pi(t,\delta) = D(p,t,\delta)p - FB(t)\delta$$

2

$$D(p,t,\delta) = N(\int_{\theta_i}^{1} d\theta) = N(1 - \frac{p}{\left[V - k(\delta)B(t)\right]t})$$

3

$$\pi(t,\delta) = D(p,t,\delta)p - FB(t)\delta$$
$$= N(1 - \frac{p}{\left[V - k(\delta)B(t)\right]t})p - FB(t)\delta$$

4

$$\frac{\partial \pi}{\partial p} = N\left(1 - \frac{2p}{\left[V - k(\delta)B(t)\right]t}\right) = 0$$

5

$$p = \frac{1}{2}\left[V - k(\delta)B(t)\right]t$$

$$\begin{aligned}\pi(t,\delta) &= D(p,t,\delta)p - FB(t)\delta \\ &= \frac{1}{4}N\left[V - k(\delta)B(t)\right]t - FB(t)\delta \\ &= \frac{1}{4}N\left[V - e^{-\lambda\delta}t^2\right]t - Ft^2\delta\end{aligned}$$

6

7

$$t = \frac{\pm\sqrt{3k(\delta)VN^2 + 16F^2\delta^2} - 4F\delta}{3kN}$$

$$\begin{aligned}\frac{\partial\pi}{\partial\delta} &= \frac{1}{4}N\lambda e^{-\lambda\delta}t^3 - Ft^2 \\ &= 0\end{aligned}$$

8

$$\delta = -\frac{1}{\lambda}\ln\frac{4F}{N\lambda t}$$

we can draw:

1. The higher the average cost of repair, the shorter the product life cycle t is, the slower the product goes to market

2. The increase in the cost of thousands of patches does indeed reduce the number of surge holes

3. The earlier the software product is released, the greater the number of software burrows in the product


Thanks for
listening

QUANTITATIVE ANALYSIS OF VULNERABILITY MARKETS

By Waylon Jepsen

CURRENT STATUS

- Bug bounty programs
- White Market
- Black Market
- Grey Market
- Third Party managed programs (TPMs)
- Internally managed programs (IMPs)

CURRENT STATE OF THE ART

Bug Bounty	Amount Paid YTD
Google (IMP)	$15 M
Facebook (IMP)	$7.5 M
HackerOne (TMP)	$100 M

Program	Funding	Founding Date
HackerOne	$110.4 M	2012
Bug Crowd	$48.7 M	2012
Cobalt	$8 M	2013

OPERATIONAL CONCERNS

- Black Market provides higher incentives
- Software development delays
- Development resistance for low potential bugs
- Increased awareness of vulnerabilities

RECENT DEVELOPMENTS

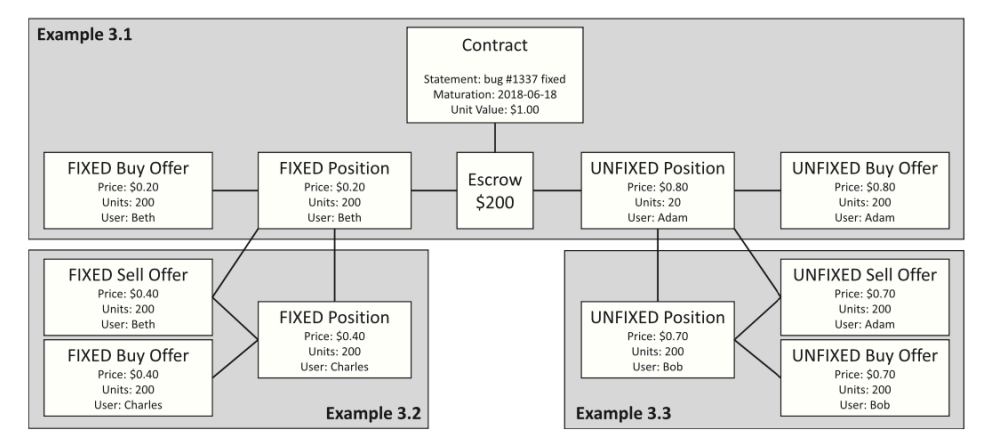
- In a paper by Malvika Rao and a variety of other authors published in 2019 in the journal of Cybersecurity a futures market for funders and quality-oriented developers was proposed.
- In a paper by Zhen li, and Qi Liao published in 2018 a model is introduced involving economic incentive solutions to motivate governments,

GOVERNMENT INCENTIVES

- Context of E-Government and Smart Cities
- Recommendations for Governments
- Cost of damage is the only limit of buying power

FUTURES CONTRACTS

- BugMart
- Advantages in open source software libraries
- Can be used for development
- Can be used for security
- In Open development
- Built on Distributed Ledger Technology



REFERENCES

- [n.d.]. #1 Crowdsourced Cybersecurity Platform. https://www.bugcrowd.com/ [n.d.]. Cobalt Application Security Platform. https://cobalt.io/ [n.d.].Hacker-PoweredSecurityTesting&BugBounty. https://www.hackerone.com/ Abdullah Algarni and Yashwant Malaiya. 2014. Software Vulnerability Markets: Dis-
- coverers and Buyers. International Journal of Computer, Information Science and
- Engineering 8 (01 2014), 71–81.
  Alex Hoffman and Hal Berghel. 2019. Moral Hazards in Cyber Vulnerability Markets.
- Computer52,12(2019),83–88. https://doi.org/10.1109/mc.2019.2936635
- Zhen Li and Qi Liao. 2018. Economic solutions to improve cybersecurity of govern- ments and smart cities via vulnerability markets. Government Information Quarterly 35,1(2018),151–160. https://doi.org/10.1016/j.giq.2017.10.006
- Lily Hay Newman. 2018. Facebook Bug Bounty Program Makes Biggest Reward Payout Yet. https://www.wired.com/story/facebook-bug-bounty-biggest-payout/#:~:text=Thebugbountyhaspaid, oneofitstopcontributors.
- S. Pfleeger and R. Cunningham. 2010. Why Measuring Security Is Hard. IEEE Security Privacy 8, 4 (2010), 46–54.
- Emil Protalinski. 2019. Google has paid security researchers over 15 million for
  bug bounties, 3.4 million in 2018 alone. https://venturebeat.com/2019/02/08/
  google- has- paid- security- researchers- over- 15- million- for- bug- bounties- 3- 4- million- in- 2018- alone/
- Malvika Rao, Georg J P Link, Don Marti, Andy Leak, and Rich Bodo. 2019. A market for trading software issues. Journal of Cybersecurity 5, 1 (10 2019). https://doi.org/10.1093/cybsec/tyz011 arXiv:https://academic.oup.com/cybersecurity/article- pdf/5/1/tyz011/33536116/tyz011.pdf tyz011.