Shifts in the Cybersecurity Paradigm: Zero-Day Exploits, Discourse, and Emerging Institutions

Andreas Kuehn
School of Information Studies, Syracuse University
221 Hinds Hall
Syracuse, New York 13244
ankuhn@syr.edu

Milton Mueller
School of Information Studies, Syracuse University
307 Hinds Hall
Syracuse, New York 13244
mueller@syr.edu

ABSTRACT

This ongoing dissertation research examines the institutionalization of new cybersecurity norms and practices that are emerging from current controversies around markets for software vulnerabilities and exploits. A market has developed for the production and distribution of software exploits, with buyers sometimes paying over USD 100,000 for exploits and software vendors offering bounties for the underlying vulnerabilities. Labeled a 'digital arms race' by some, it is generating a transnational debate about control and regulation of cyber capabilities, the role of secrecy and disclosure in cybersecurity, and the ethics of exploit production and use. The research takes a qualitative approach to theorize the emerging cybersecurity institutions. It shall provide insights into the technical, economic and institutional shifts in cybersecurity norms and practices. Analyzing the bug bounty programs run by Microsoft and Facebook as examples, the paper discusses the role of institutions in facilitating software vulnerability markets. The paper summarizes preliminary findings presented at NSPW 2014.

Categories and Subject Descriptors

K.4.1 [**Computers and Society**]: Public Policy Issues—*regulation*; K.6.5 [**General**]: Security and Protection—*invasive software, unauthorized access*

General Terms

Management, Economics, Security

Keywords

Cybersecurity; software vulnerability; software exploit; discourse; institutions; Internet governance.

1. INTRODUCTION

Software vulnerabilities and exploits have attracted significant attention recently because of their implications for cybersecurity, cyber crime, and cyber war. In recent years, actors began to realize the economic and military value of retaining exclusive knowledge of vulnerabilities. A market has developed for the production and distribution of software vulnerabilities; buyers sometimes pay over USD 100,000 for software exploits. Major software companies now run bug bounty programs to acquire vulnerabilities in order to patch their products. Security firms, such as VUPEN, Endgame, Netragard, and TippingPoint's Zero Day Initiative bring together suppliers and buyers in this market. U.S. government intelligence services have become a de facto regulator by virtue of their ability to spend millions to develop or acquire software exploits.

A *software vulnerability*, also referred to as a *security bug*, is a flaw in computer code that can compromise the security of a computer system. Software and network protocols often contain security vulnerabilities that are unintended consequences of design choices or mathematical errors in models. An *exploit* makes use of such vulnerabilities to circumvent security mechanisms and allows unauthorized actors to intrude into, destroy, manipulate or steal data from an information system. A zero-day exploit (ZDE) is a special type of exploit. It makes use of an undisclosed vulnerability, whose existence is kept secret. Thus, established security procedures and technologies such as antivirus or intrusion detection systems cannot defend against them. Hence, ZDEs are a central component and provide effective means in cyber operations and attacks for offensive and defensive ends. Stuxnet, Flame, and Aurora are examples of cyber weapons that made use of ZDEs [12, 24].

1.1 Research Problem

The proliferation of exploits and ZDEs raises fundamental questions about the relationship between technology and society and heightens concerns about the unaccountable use of cyber attack capabilities. Labeled a 'digital arms race' by some, it is generating a transnational debate about control and regulation, the role of secrecy and disclosure, and the ethics of exploit production and use (e.g., [18, 4]). The controversy reflects underlying conflicting rationales: while intelligence and military circles are concerned about national security, industrial and civilian logics emphasize matters of trade, innovation and freedom. Recent revelations about NSA spying have amplified this debate, including reports that the NSA spent USD 25 million in 2013 to acquire exploits [6]. The U.S. President's Review Group made specific recommendations regarding software exploits [2].

NSPW'14, September 15–18, 2014, Victoria, BC, Canada.

ACM 978-1-4503-3062-6/14/09 ...$15.00.
http://dx.doi.org/10.1145/2683467.2683473.

Issues regarding secrecy and disclosure, knowledge and ignorance, and transparency and concealment are paramount in this debate [21, 22]. There is a longstanding debate in computer security about the role of disclosure in improving or undermining security (e.g., [20]). Since cybersecurity is one of the key problems facing our globally interconnected society, understanding how software vulnerabilities and exploits – and cyber weapons more generally – are used, defined, and controlled is of utmost importance for society as a whole and for policy-makers.

This ongoing dissertation research studies software vulnerabilities with respect to their exploitation and the debate over their production, sale and regulation. Drawing from the literature on Science and Technology Studies and Institutional Theory, this research takes a qualitative, empirical stance to examine the discourse and the emerging institutions in the controversy about software vulnerability and exploit markets and their regulation. Its broader goal is to make the public aware of the implications of vulnerabilities upon the security and reliability of the Internet.

2. THEORY

Discourse and institutions are the two theoretical pillars of this work, they are interrelated and mutually shape each other. Jasanoff termed this process as co-production [8]. Co-production explains how the mutual shaping of discourse and institutions produce social order. For instance, changes in a discourse over time might lead to modifications in institutions. If significant, such changes may lead to shifts in a paradigm central to a domain.

2.1 Discourse

Edwards defines 'discourse' as the "social interactions [...] through which reality is interpreted and constructed for us and by us" [5, p. 34]. His notion of discourse is not confined to language or speech acts but includes techniques, technology, and practices, which are constitutive elements of the discourse. Analyzing the discourse provides a revealing window into the complex factors shaping the controversy among competing actors, their values, interests, and ideologies. Of particular interest is how actors attempt to frame the discourse in order to achieve an institutional outcome that supports their interests. A number of closely related discourses on current cybersecurity policies of nation-states; on states' understanding of defensive and offensive cyber capabilities; on disclosure and information sharing practices; and on software vendors' patching practices construct this domain.

2.2 Institutions

North describes institutions as "the rules of the game in a society" [19, p. 3]; they govern social behavior and human interactions, and order markets and society. These institutions, formal (e.g., constitutions, laws, regulations, property rights) or informal (e.g., customs, traditions, norms, taboos, codes of conduct) in their nature [3, 25], can reduce uncertainty by enforcing rules or constraining behavior, and thus facilitate mutually beneficial exchanges that would not occur otherwise. As such, institutions are a starting point to ponder how the software vulnerability trade can be governed.

Developing institutions that affect and influence the trade of software vulnerabilities and exploits fall into two broad categories: (1) the *formation of new markets*, such as vulnerability markets or bug bounty programs; and (2) the *expansion of existing control regimes*, such as the Wassenaar Arrangement, a multilateral export control regime for dual-use technologies, which was amended in 2013 to include cybersecurity and surveillance technologies [9].

Linking back to the broader concern of discourse, institutional economic theory is based on human behavior; the decisions and actions in human interaction which are formed upon subjective perceptions and imperfect information. According to North [19, p. 111] "ideas and ideologies shape the subjective mental constructs that individuals use to interpret the world around them and make choices." North enables us to connect institutional economic theory to discourse theory by opening up the former and addressing ideas and ideologies. The ideas, ideologies and beliefs that are incorporated into human decision-making are expressed in the wider discourse and become part of the explanation of how ideas, concepts, ideologies, and beliefs shape institutions.

3. VULNERABILITY MARKETS AS INSTITUTIONS

This section reports briefly on a preliminary analysis of bug bounty programs – a type of a vulnerability market – as institutions. In addition, it wonders whether these changes in norms and practices are a potential source for significant shifts in the cybersecurity paradigm. For an extended account, see [11].

3.1 Bug Bounty Programs

Acquiring software bugs and monetarily rewarding its discoverers through a formalized bug bounty program (BBP) is a rather new development. The commodification of software vulnerabilities – bugs for bucks – may lead to significant shifts in the cybersecurity paradigm. Major software companies have recently adapted their security practices by more openly incorporating externally acquired vulnerability information. Previously, individuals shared this information with the developers at no cost in order to build their reputations as experts in information security. Now, independent security researchers are selling security vulnerabilities to increase their income.

In recent years, numerous Internet companies and software developers started to run or experiment with some forms of BBPs to harness external security expertise. Mozilla, for instance offers a USD 3,000 reward for security critical and high severity bugs in Firefox and Thunderbird [17]. Google pays out between USD 100 and USD 20,000 for discovered vulnerabilities in Google.com, Youtube.com. In addition, the search giant seeks security patches for selected open source projects, offering awards between USD 500 to USD 10,000 (Google, 2013). Started in 2012 and 2013, respectively, HackerOne [7] and Bugcrowd [1] run platforms to manage BBPs for various software applications and Internet services.

3.2 Two Empirical Cases

3.2.1 Microsoft

Microsoft launched its Bounty Programs in June 2013, offering monetary compensation for reporting security vulnerabilities and novel exploitation techniques. Prior, Microsoft rejected the idea of a BBP in favor of its bug competition,

the BlueHat Prize [10]. Microsoft considered this development as decisive shift, as an investment in the research community to engage with "clever hackers" to strengthen its defenses [15]. Notably, Microsoft attempts to target the black market with its BBP. The company stated that it was "cutting down the time that exploits and vulnerabilities purchased on the black market remain useful, especially for targeted attacks that rely on stealthy exploitation without discovery" [14]. Starting with three different programs, Microsoft offered bounties up to USD 11,000 for flaws in the Internet Explorer 11 beta, up to USD 100,000 for novel exploitation techniques, and up to USD 50,000 for defensive approaches against these techniques. By July 2014, Microsoft paid out USD 253,000 to seven different security researchers [13].

3.2.2 Facebook

Even before Facebook formalized its bug bounty program in July 2011, the social networking company embraced external security researchers under its White Hat initiative to support its internal security team. A year after its start, Facebook extended the program from security bugs on its social networking platform to include its internal infrastructure to the bug hunting grounds, including corporate networks, and the production infrastructure [23]. In 2013, Facebook awarded USD 1.5 million to 330 researchers. Forty-one bugs were categorized as high severity. The largest Facebook bounty by then amounted to USD 33,500.

3.3 Institutional Analysis

Using documents (e.g., media reports, blog posts, and websites), the preliminary analysis examined institutional elements in Facebook's and Microsoft's BBP. As key players in the Internet and software world, their BBPs received considerable attention in expert circles and attracted a large number of contributors, particularly in the case of Facebook. While smaller BBPs for other software existed previously, the decision made by large technology companies to build up a BBP sent a strong signal to emerging vulnerability markets.

The analysis identified four institutional elements: (1) explicit *procedures* allow for straightforward, standardized forms of interactions and ensure, for instance that external knowledge about vulnerabilities is collected and made available to the internal security team; (2) *technical specifications* describe technical and formal requirements, such as the type of bugs (e.g., remote code execution, cross-site scripting) that are eligible under a BBP; (3) *terms and conditions* govern a BBP with regard to its structure and scope, they determine the types and sizes of bounties and stipulate rules for concurrent submission of the same bug; and (4) *acknowledgment and reputation* are important motivational elements, such as a 'Hall of Fame' of contributors, to engage talented security researchers.

3.4 Theoretical Considerations

The properties of software vulnerabilities are difficult to assess. Thus, seller and buyers of these information goods are confronted with a high degree of uncertainty and risk of defection (i.e., transactions are conducted anonymously; vulnerabilities are not exploitable as promised; vulnerabilities are offered and sold on multiple markets), which leads to high transaction costs that may prevent the exchange taking place. Miller referred to this as "inherent obstacles" that precluded the formation of legitimate vulnerability markets [16]. Despite these barriers, how was it possible that these bug bounty programs emerged and continue to spread?

Institutional economics provide a theoretical explanation. Central to North's [19] argument is that (1) institutions exist due to the uncertainties in human interaction, and (2) institutions are constraints that structure the interaction between humans. While transactions are rather costly in the case of software vulnerabilities, BBPs as institutions can remediate those issues and facilitate a market for security bugs. The four elements outlined in this preliminary analysis provide means to overcome obstacles in the vulnerability market; they lower transaction costs and uncertainty. In short, institutions matter for vulnerability markets.

3.5 A Shift in the Cybersecurity Paradigm?

Exploring emerging BBPs and software vulnerability markets more broadly, one can observe that multiple technical, economic, organizational, and institutional changes are under way. Comparing to early accounts of vulnerability markets (e.g., [16]), the advancing institutionalization of BBPs allows to observe those changes over time. The examples of Facebook and Microsoft illustrated that BBPs led to novel approaches in acquiring and integrating external vulnerability information. Disrupting established norms and practices, one may ask how these changes affect cybersecurity and if they lead to paradigmatic shifts.

Table 1 outlines a set of then-now changes, construed as working hypotheses for further discussion about what direction this development may take and how it may affect cybersecurity. These working hypotheses suggest a set of dimensions against which changes can be measured in order to determine a shift in the paradigm.

4. CONCLUSION

This paper summarized the ongoing research presented at NSPW 2014. It introduced the notions of 'discourse' and 'institutions' to study controversial issues around software vulnerabilities and exploits, particularly with regard to questions about their control and regulation. Applying institutional economic theory to BBPs, the paper suggested that markets for vulnerability information yield to lower transaction costs and uncertainty between transacting parties.

Using Microsoft's and Facebook's BBP as examples, the paper briefly described and analyzed these software vulnerability markets as institutions. While not addressed in this paper, the discursive elements will receive more attention in future research. The two examples demonstrated that – even if not perfect – uncertainty can be and has been reduced, resulting in new forms of exchanges. Operators of BBPs need to send clear signals to security researchers that they will not defect from their promise to pay for security bugs. The institutional analysis provided preliminary insights into the changing norms and practices in cybersecurity.

5. ACKNOWLEDGMENTS

I would like to thank my advisor Milton Mueller for his valuable advice and support in the course of this research. This NSPHD paper received helpful feedback and generous guidance from three anonymous NSPW reviewers, Rainer Böhme, and the workshop participants.

Table 1: Working Hypotheses: Changes towards a New Paradigm

Then	Now
Markets. No legitimate markets for software vulnerabilities exist.	BBPs emerge; number of BBPs is increasing.
Disclosure. Security researchers report software bugs for free / for reputation; software companies do not pay for discovered vulnerabilities in their software.	Security researchers are compensated for discovered security bugs; software companies offer rewards for bugs in their software and in some cases even for bugs in third-party software.
Testing. Security testing conducted by internal, corporate employees within organizational boundaries; hiring information security personnel through traditional human resource channels.	Crowd sourcing of security and penetration testing to independent security researchers across organizational boundaries to support internal security efforts; hiring security researchers who successfully contributed to BBPs.
Value of Vulnerabilities. Security vulnerability information does not represent a monetary value.	Commodification of software vulnerability, representing an economic and/or intelligence/military value.
Actors. Exploiting unknown software vulnerabilities (e.g., zero-day exploits) for sophisticated cyber attacks confined to state actors (e.g., military and intelligence services)	Increasing number of cyber attacks in which criminals deploy sophisticated software exploits (e.g., ZDEs).
Expertise and Skills. Technical security expertise required to identify security bugs.	Tools for automated security testing and bug discovery become more readily available.
Bug Types. Focus on easy-to-find, shallow bugs.	Focus on more sophisticated bugs and security circumvention techniques; fewer easy-to-find bugs left in software.
Income. Difficulty to generate legitimate income as a bug hunter.	Additional, legitimate income for independent security researchers; occasionally hired into internal security team because of participation in BBPs.

6. REFERENCES

[1] Bugcrowd. Crowdsource Your Cybersecurity. https://bugcrowd.com.

[2] R. A. Clarke, M. J. Morell, G. R. Stone, C. R. Sunstein, and P. Swire. Liberty and Security in a Changing World: Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies. Technical report, President's Review Group on Intelligence and Communications Technologies, Washington, DC, 2013.

[3] P. DiMaggio and W. W. Powell. Introduction. In P. DiMaggio and W. W. Powell, editors, *The New Institutionalism in Organizational Analysis*, pages 1–38. University of Chicago Press, Chicago, IL, 1991.

[4] Economist. The digital arms trade. *The Economist*, 2013.

[5] P. Edwards. *The Closed World: Computers and the Politics of Discourse in Cold War America.* MIT Press, 1996.

[6] B. Fung. The NSA hacks other countries by buying millions of dollars' worth of computer vulnerabilities. http://www.washingtonpost.com/blogs/the-switch/wp/2013/08/31/the-nsa-hacks-other-countries-by-buying-millions-of-dollars-worth-of-computer-vulnerabilities, Aug. 2013.

[7] HackerOne. Effective vulnerability disclosure programs. https://hackerone.com.

[8] S. Jasanoff, editor. *States of Knowledge.* Taylor & Francis, Abingdon, UK, 2004.

[9] S. Jones. Cyber war technology to be controlled in same way as arms. http://www.ft.com/cms/s/0/2903d504-5c18-11e3-931e-00144feabdc0.html, Dec. 2013.

[10] G. Keizer. Microsoft kicks off $250,000 security contest. http://www.computerworld.com/s/article/9218845/Microsoft_kicks_off_250_000_security_contest, 2011.

[11] A. Kuehn and M. Mueller. Analyzing Bug Bounty Programs: An Institutional Perspective on the Economics of Software Vulnerabilities. In *The 42nd Research Conference on Communication, Information and Internet Policy (TPRC 42)*, Washington DC, 2014.

[12] R. Lemos. Private market growing for zero-day exploits and vulnerabilities. *Information Security Magazine*, 14(10), 2012.

[13] Microsoft. Bounty Hunters: The honor roll. http://technet.microsoft.com/en-us/security/dn469163.

[14] Microsoft. Bounty Evolution: $100,000 for New Mitigation Bypass Techniques Wanted Dead or Alive. http://blogs.technet.com/b/bluehat/archive/2013/11/01/bounty-evolution-100-000-for-new-mitigation-bypass-techniques-wanted-dead-or-alive.aspx, 2013.

[15] Microsoft. Heart of Blue Gold – Announcing New Bounty Programs. http://blogs.technet.com/b/bluehat/archive/2013/06/19/heart-of-blue-gold-announcing-new-bounty-programs.aspx, 2013.

[16] C. Miller. The legitimate vulnerability market: the secretive world of 0-day exploit sales. In *6th Workshop on the Economics of Information Security (WEIS 2007)*, 2007.

[17] Mozilla. Bug Bounty Program. http://www.mozilla.org/security/bug-bounty.html.

[18] M. Mueller. Regulating the Market for Zero-day Exploits : Look to the demand side, 2013.

[19] D. C. North. *Institutions, Institutional Change and Economic Performance*. Cambridge University Press, 1990.

[20] S. Ransbotham and S. Mitra. The Impact of Immediate Disclosure on Attack Diffusion and Volume. In *10th Workshop on Economics of Information Security (WEIS 2011)*, Fairfax, VA, June 14–15, 2011.

[21] B. Rappert. *How to Look Good in a War - Justifying and Challenging State Violence*. Pluto Press, London, UK, 2012.

[22] J. Reppy, editor. *Secrecy and Knowledge Production*. Cornell University, Peace Study Program, Ithaca, NY, occasional edition, 1999.

[23] J. Robertson. Facebook Widens 'Bug Bounty' Program to Combat Internal Breaches. `http://www.bloomberg.com/news/2012-07-26/facebook-widens-bug-bounty-program-to-combat-internal-breaches.html`, 2012.

[24] B. Schneier. The Story Behind The Stuxnet Virus. `http://www.forbes.com/2010/10/06/iran-nuclear-computer-technology-security-stuxnet-worm.html`, July 2010.

[25] W. R. Scott. *Institutions and Organizations*. SAGE Publications, Thousand Oaks, CA, 2001.