Cyber Security Training

A Survey of Serious Games in Cyber Security

Jin-Ning Tioh, Dr. Mani Mina, Dr. Douglas W. Jacobson
Department of Electrical and Computer Engineering
Iowa State University
Ames, IA, USA
jinning@iastate.edu, mmina@iastate.edu, dougj@iastate.edu

***Abstract*—Within the field of computer and information security, there has been a relatively recent surge of interest on a multitude of topics, ranging from secure programming practices, protocols and algorithm design to cryptography and ethics. However, this body of research typically focuses on the implementation or theory of security controls and mechanisms at the application, operating system, network, and physical layers. The user layer, long recognized as the weakest link in the security chain, has had little to no attention paid to it by comparison, especially from a sociotechnical perspective which is comparatively new to engineering. Thus steps have to be taken then to instill safe cyber security practices in the general computer user, overcoming their propensity to act without forethought for the consequence of their actions, including ignoring warning messages, visiting unsafe websites, and communicating with unauthenticated entities. While there are significant studies that show the importance of game-based learning for the process of cognitive development and learning concepts of students, there have been relatively few papers or attempts at presenting forms of assessing the potential of these resources. Here then, we will endeavor to present a brief overview of the necessary background as well as a concise view of the current state of serious games dealing specifically with the topic of cyber security.**

Keywords—serious game; game-based learning; cyber security; computer security literacy.

I. INTRODUCTION

The past decade has seen a phenomenal increase in the number of cybercrimes, including financial fraud, identity theft and denial of service attacks just to name a few. In fact, one could correctly assert that it has become a fact of life for anyone who spends any amount of time on the internet each day to fend off spam and phishing attempts on a daily basis, with these attempts only growing in sophistication as time passes. And of course, cybercrime isn't simply limited to the home front. In 2013, 7% of US organizations lost $1 million or more due to the commission of cybercrimes. The US Director of National Intelligence has even gone so far as to rank cybercrime as the top national security threat, with the FBI notifying 3,000 US companies in 2013 - ranging from small banks, leading retailers, and major defense contractors - that they had been victims of cyber intrusion [1].

Given this growing threat, there has naturally been a surge of interest within the field of computer and information security over recent years, covering a wide range of topics including secure programming practices, protocols and algorithm design to cryptography and ethics. However, this body of research typically focuses on the implementation or theory of security controls and mechanisms at the application, operating system, network, and physical layers. The user layer, long recognized as the weakest link in the security chain, has had little to no attention paid to it by comparison, especially from a sociotechnical perspective which is fairly new to engineering [2]. Steps have to be taken then to instill safe cyber security practices in the general computer user, overcoming their propensity to act without forethought for the consequence of their actions, including ignoring warning messages, visiting unsafe websites, and communicating with unauthenticated entities.

This paper is structured as follows. We will first further clarify and elaborate on the problem of computer security literacy as well as our stated goals in section 2. We will briefly explore the definition of a serious game in section 3 before delving into the motivation behind utilizing game-based learning over more traditional methods in section 4. We then explain our survey method, and present the results of both our paper and product survey in that order in the following sections. Finally, we will present our conclusions on the current state of serious games dealing with the subject of cyber security.

II. PROBLEM STATEMENT

Before proceeding further, it behooves us to ground our field of inquiry so as to avoid wandering too far off topic. As noted earlier, besides the use of a computer in the commissioning of a cybercrime, each of these crimes shares another common thread - the hackers often take advantage of the user layer. The vast majority of these users more likely than not lack awareness of basic information assurance concepts, including confidentiality, authentication, integrity, and availability, thus leading to a sketchy decision making process, and leaving them more susceptible to attacks such as phishing, computer virus hoaxes, and so on. The obvious goal then, is to raise awareness on such attacks and bestow knowledge on sound security practices. Computer security professionals most

978-1-5090-5920-1/17/$31.00 ©2017 IEEE

commonly accomplish this through awareness campaigns and the creation of websites that contain security tips and advice [2]. In addition, conventions and competitions such as DEFCON, and the National Collegiate Cyber Defense Competition are held annually.

Unfortunately, such measures don't do enough to overcome the common perception that computer security is a topic of concern only for the technological elite. Several researchers and developers have caught on to this perception, and have developed a number of serious games focused on the topic cyber security. This paper then will focus on exploring the current state of cyber security training games, providing the necessary background before investigating the effectiveness of existing products and academic studies in the area.

III. Serious Games

As this is a term which appears with some regularity in the field, we thought it important to cover it at least briefly. Defined originally in 1970 by Clark Abt [3], but updated by Mike Zyda in 2005, a serious game is "a mental contest, played with a computer in accordance with specific rules that uses entertainment to further government or corporate training, education, health, public policy, and strategic communication objectives [4]." They are usually simulations of real-world processes designed for solving a problem. This doesn't necessarily preclude entertainment; solving problems is simply an additional purpose of the game [5].

It is also worthwhile to take note of the fact that while serious games didn't originally refer to video games alone, for the purposes of this paper we will treat it as such.

IV. Game-Based Learning

As any educator will attest to, one of the key ingredients of successful learning is motivation - a motivated learner will tend to find a way to overcome any obstacles or difficulties over their less-motivated kin. Unfortunately, traditional pedagogical strategies tend to come across as 'dry' and 'technical' to current students, which leads to a natural erosion in their motivation to learn more about a subject. Several authors such as Presnky [4] explain this phenomenon by arguing that current students are what are termed as 'digital natives', people used to interacting on a daily basis with rich interactive digital media devices such as computers, mobile devices and video game consoles [4, 5].

Perhaps more so than any other, a single industry specializes in motivation - the computer and video games industry. Game designers have long been experts in the art of player engagement - the ability to keep people in their seats hour after hour, day after day, at rapt attention, actively trying to reach new goals, elated by each success and determined to overcome each failure, constantly coming back for more. Since its inception in 1974 with Pong, there is now an estimated 170 million people who play games at least casually in the US as of a study done in 2009 [6], which constitutes more than half of the US population. In addition, the growing popularity of major digital distribution platforms such as Steam and GOG.com makes it easier than ever to reach them, compared to traditional retail distribution methods with cumbersome CD and DVD boxes. As of February 2015, Steam alone has 125 million active users, boasting as many as 9 million concurrent users as of March 2015 [7].

To quote another old adage then, one might as well fight fire with fire. Instead of competing against the video games industry, it makes a great deal of sense to attempt merging the content of learning with the motivation of games [5]. Educational games have the potential to enhance the learning process in several respects. One of the most discussed and pointed out of course involves player engagement. The ability to capture and hold a person's attention while keeping them engaged and immersed is a quality which can be easily exploited to motivated a student to keep at a particular subject matter for hours continuously - a trying task at the best of times [8, 9]. Another interesting trait is the ability to provide deep, immersive in-game worlds which students can freely explore at their leisure, promoting self-directed learning [10]. Additionally, games oftentimes have a short feedback cycle - an almost immediate and steady stream of rewards and punishments for each action taken by a student, which in turn gives them the perception of relatively rapid progress [11]. Last but not least, in comparison to traditional training methods, game-based learning allows students to make mistakes and learn from them in a risk-free environment [12]. The following table shows a comparison between traditional training methods which include lectures and online tutorials, hands-on training methods such as apprenticeship programs, and game-based learning.

TABLE I. Comparison of Traditional Training, Hands-On and Game-Based Learning [12]

	Traditional Training	Hands-On Training	Game-Based Learning
Cost-effective	X		X
Low physical risk / liability	X		X
Standardized assessments allowing student-to-student comparisons	X		X
Highly engaging		X	X
Learning pace tailored to individual student		X	X
Immediate feedback in response to student mistakes		X	X
Student can easily transfer learning to real-world environment		X	X
Learner is actively engaged		X	X

TABLE II. RESULTS OF PAPER SURVEY

Paper(s)	Game Name	Game Type	Topic	Methodology	Results
[14] – [18]	Anti-Phishing Phil	Web-Based 2D Point-and-Click	Staying Safe Online	Think Aloud, Pre-Test and Post-Test Survey, SUS Usability Questionnaire	Positive impact on phishing susceptibility.
[19] – [25]	CyberCIEGE	Stand-Alone 3D Simulation	Corporate Cyber Security	Self-Assessment	Generally positive.
[26]	Internet Hero	Web-Based 2D Point-and-Click	Staying Safe Online	Informal Survey	Children liked the game.
[27]	PicoCTF	Web-Based 2D Point-and-Click	Cyber Security	Survey	Positive feedback from students and instructors.
[28]	SecurityEmpire	Web-Based 2D Point-and-Click	Cyber Security	Informal Survey	High school students liked the game.
[29]	Security Games	Web-Based 2D Point-and-Click	Network Security	Comparing on-task performance	Significant improvement in test group.
[30] – [31]	*Untitled*	Web-Based 2D Point-and-Click	Staying Safe Online	Pre-Test and Post-Test Survey	No significant improvement in awareness.

The effectiveness of hands-on training approaches such as apprenticeship programs can't be disputed - it has a rich history which traces all the way from ancient times to the present day. However, well-designed game-based learning could potentially retain the advantages of both traditional training and hands-on training, being both relatively cost-effective and low-risk (safety training utilizing a virtual representation of machinery as compared to using live machinery). In addition, as we noted earlier, learners are free to re-enact a precise set of circumstances multiple times, exploring the consequences of different actions which could have disastrous consequences in real life. For example, learners could deliberately cause a virtual explosion to understand why gas line disasters happen, which would not be a viable nor desirable option during hands-on training. Finally, with virtual reality head-mounted displays such as the Oculus Rift making virtual reality relatively affordable for consumers, game-based learning could potentially become even closer to the real thing, engaging learners even further.

V. SURVEY METHOD

With the increasingly burgeoning amount of research being conducted in the field, as well as the potential applications and ramifications in a commercial setting, we felt it necessary to conduct a search of both current scientific studies as well as current commercial products.

The literature search was conducted in April 2016 and includes both conference and journal publications. It was conducted utilizing the academic search engine Google Scholar, as it was and still is one of the best and easiest methods to source relevant literature. The search was carried out using a combination of the following keywords - serious games, cyber security, game-based learning and gamification. It is worth noting that the search results returned utilizing the keywords listed above included a great number of hits which covered topics related to security, game theory, as well as other topics beyond the purview of this survey. We limited ourselves to the first 40 results for each keyword, sorted for relevance by the search engine, proceeding then to inspect each of these for relevance, picking only those academic papers which described a cyber security game of some kind. We further pared these down by limiting ourselves to those papers which described an empirical study including some kind of effect measurement, arriving at the final 18 papers listed in Table 2, grouped by the games they describe.

The product survey was carried out in April 2016, utilizing a combination of the web search engine Google, as well as Serious Game Classification [13], a dedicated database of serious games. The same combination of keywords used in the literature search was also applied here. Using the same criteria as in the paper survey, only games which directly addressed cyber security were selected, and we did not include any games with broken links (which happened frequently with former research projects) or insufficient information to classify them. We arrived at a final selection of 13 products currently on the market.

VI. PAPER SURVEY

Shown above in table 2 is a quick summation of the results of our literature review. As we noted before, only academic papers which described a serious game related to cyber security and included some form of evaluation was focused upon. The selected papers were then classified and summarized by the authors. As the majority of the games found and included would fall under the traditional game genre of casual games, we tried to further break it down in our summation. Almost all the results however turned out to be of the web-based variety. Most of them focus on the topic of general cyber security awareness. While almost all studies focus on efforts to train or raise awareness within the general public, several such as Anti-Phishing Phil have been adapted towards training corporate employees as well.

Taking the pre and post test results for Anti-Phishing Phil (depicted in figure 1) as an example, in which three separate groups of 14 students were asked to read existing training material on phishing, go through a tutorial on phishing the authors had created, and finally play the game for 15 minutes, the group of students who played the game showed the greatest

TABLE III. RESULTS OF THE PRODUCT SURVEY

Game Name	Game Type	Topic	Target Audience
Agent Surefire [32]	Stand-Alone 3D Adventure	Corporate Cyber Security	Corporate Employees
Anti-Phishing Phil [33]	Web-Based 2D Point-and-Click	Staying Safe Online	Corporate Employees
Budd:e [34]	Web-Based 2D Point-and-Click	Staying Safe Online	Children / Teenagers
Carnegie Cadets [35]	Web-Based 2D Point-and-Click	Staying Safe Online	Children
CyberCIEGE [36]	Stand-Alone 3D Simulation	Corporate Cyber Security	Students (18+)
CyberProtect [37]	Web-Based 2D Simulation	Fundamentals of Cyber Security	Students (18+)
CyberSecure Contingency Planning [38]	Web-Based 2D Point-and-Click	Preventing Data Breaches at Health Practices	Health Practice Decision Makers
Cyphinx [39]	Virtual World Games Portal	Varied	Teenagers / Students (18+)
FBI Kids Games [40]	Web-Based Games Portal	Staying Safe Online	Children / Teenagers
Game of Threats [41]	Multiplayer	Cyber Breach Response	Corporate Employees
NSteens [42]	Web-Based Games Portal	Staying Safe Online	Teenagers
OnGuardOnline [43]	Web-Based Games Portal	Staying Safe Online	Children / Teenagers
PBS Cybersecurity Lab [44]	Web-Based 2D Puzzle	Varied	Teenagers

improvement with regards to identifying phishing websites. These results help show that game-based learning could be applied to the topic of cyber security to great effect. However, it is worth stressing again that a great number of papers which described similar cyber security training games were excluded due to a lack of evaluation of any kind. Even then, of those that we did include, most only included informal feedback from their test subjects as to the effectiveness of their games. Only Anti-Phishing Phil and Security Games showed a measurable impact on the learning outcomes of their subjects, and even then the samples were relatively small. Thus while the overall outcomes have been positive thus far (with the exception of the untitled game, which showed no significant improvement), this serves to highlight the immaturity of the field, and the need for more rigorous evaluation.

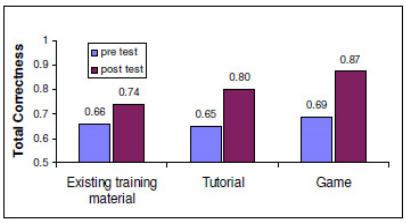

Fig. 1. Results of the Anti-Phishing Phil game [16].

VII. PRODUCT SURVEY

In table 3, we provide a summation of the serious games currently available on the market which specifically target the field of cyber security. We attempt to classify each game by their type, topic and target audience. The majority of them are free to play casual web games which target children, teenagers and students, with only one or two specifically designed with the goal of training corporate employees. As virtually little to no empirical information exists regarding the effectiveness of each product (with the notable exception of former research projects such as CyberCIEGE and Anti-Phishing Phil), we were unable to determine their possible impact.

VIII. CONCLUSIONS

In this paper, we laid out the background and then explored the current state of both academic studies and existing products dealing with cyber security. While a number of games have been developed and corresponding academic studies have been conducted, most of these have only include an informal survey or a relatively small sample size. And though the results from these studies have been generally positive, it is clear that a more rigorous evaluation is required. And while there are an increasing number of products that relate to this growing field, a study of their effectiveness would be beneficial as well. With CyberCIEGE and Anti-Phishing Phil being the only notable exceptions to appear in both academic studies and the product survey as well though, questions could be raised about the sustainability of games developed for academic studies.

In the end, despite some generally positive early indications, the question as to the effectiveness of serious games dealing with the training of cyber security is a difficult one to answer conclusively at this point.

REFERENCES

[1] K. Mickleberg, L. Schive, and N. Pollard, "US cybercrime: Rising risks, reduced readiness," 2014. [Online]. Available: http://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/2014-us-state-of-cybercrime.pdf. Accessed: Apr. 15, 2016.

[2] D. Jacobson and J. Idziorek, Computer security literacy: Staying safe in a digital world. United States: CRC Press, 2012.

[3] C. C. Abt, Serious games, 4th ed. New York: Penguin (Non-Classics), 1971.

[4] M. Zyda, "From visual simulation to virtual reality to games," Computer, vol. 38, no. 9, pp. 25-32, Sep. 2005.

[5] E. Adams, "The designer's notebook: Sorting out the genre muddle," in Gamasutra, 2009. [Online]. Available: http://www.gamasutra.com/view/feature/4074/the_designers_notebook_sorting_.php?page=2. Accessed: Apr. 15, 2016.

[6] M. Prensky, "Digital natives, digital immigrants part 1," On the Horizon, vol. 9, no. 5, pp. 1-6, Sep. 2001.

[7] M. Prensky, Digital game-based learning. New York: McGraw-Hill Education, 2001.

[8] T. Thorsen, "US gamer population: 170 million - NPD," in GameSpot, 2010. [Online]. Available: http://www.gamespot.com/articles/us-gamer-population-170-million-npd/1100-6214598/. Accessed: Apr. 15, 2016.

[9] R. Smith, "Valve to showcase SteamVR hardware, steam machines, & more at GDC 2015," in AnandTech, https://www.facebook.com/AnandTech, 2015. [Online]. Available: http://www.anandtech.com/show/9003/valve-to-showcase-steamvr-hardware-steam-machines-more-at-gdc-2015/. Accessed: Apr. 15, 2016.

[10] J. P. Gee, "What video games have to teach us about learning and literacy," Computers in Entertainment, vol. 1, no. 1, p. 20, Oct. 2003.

[11] T. W. Malone, "Toward a theory of intrinsically motivating Instruction," Cognitive Science, vol. 5, no. 4, pp. 333-369, Oct. 1981.

[12] K. Squire, "Video games in education," International Journal of Intelligent Games & Simulation, vol. 2, no. 1, Jun. 2012. [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.543.5729&rep=rep1&type=pdf. Accessed: Apr. 15, 2016.

[13] "Serious game classification: The online classification of serious games,". [Online]. Available: http://serious.gameclassification.com/. Accessed: Apr. 15, 2016.

[14] N. A. G. Arachchilage, N. Asanka, S. Love, and M. Perry, "Security awareness of computer users: A game based learning approach," Brunel University, School of Information Systems, Computing and Mathematics, 2012. [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.425.7856&rep=rep1&type=pdf. Accessed: Apr. 15, 2016.

[15] N. A. G. Arachchilage and S. Love, "A game design framework for avoiding phishing attacks," Computers in Human Behavior, vol. 29, no. 3, pp. 706-714, May 2013. [Online]. Available: http://dx.doi.org/10.1016/j.chb.2012.12.018. Accessed: Apr. 15, 2016.

[16] S. Sheng et al., "Anti-Phishing Phil: the design and evaluation of a game that teaches people not to fall for phish," Proceedings of the 3rd symposium on Usable privacy and security, pp. 88-99, Jul 2007. [Online]. Available: http://dx.doi.org/10.1145/1280680.1280692. Accessed: Apr. 15, 2016.

[17] P. G. Nyeste and C. B. Mayhorn, "Training users to counteract Phishing," Proceedings of the Human Factors and Ergonomics Society Annual Meeting, vol. 54, no. 23, pp. 1956-1960, Sep. 2010. [Online]. Available: http://dx.doi.org/10.1177/154193121005402311. Accessed: Apr. 15, 2016.

[18] N. A. G. Arachchilage and S. Love, "Security awareness of computer users: A phishing threat avoidance perspective," Computers in Human Behavior, vol. 38, pp. 304-312, 2014. [Online]. http://dx.doi.org/10.1016/j.chb.2014.05.046. Accessed: Apr. 15, 2016.

[19] B. D. Cone, C. E. Irvine, M. F. Thompson, and T. D. Nguyen, "A video game for cyber security training and awareness," Computers & Security, vol. 26, no. 1, pp. 63-72, Feb. 2007.

[20] B. D. Cone, M. F. Thompson, C. E. Irvine, and T. D. Nguyen, "Cyber security training and awareness through game play," in IFIP International Federation for Information Processing. Springer Science + Business Media, pp. 431-436.

[21] C. C. Fung, V. Khera, A. Depickere, P. Tantatsanawong, and P. Boonbrahm, "Raising information security awareness in digital ecosystem with games - a pilot study in Thailand," 2008 2nd IEEE International Conference on Digital Ecosystems and Technologies, Feb. 2008.

[22] F. L. Greitzer, O. A. Kuchar, and K. Huston, "Cognitive science implications for enhancing training effectiveness in a serious gaming context," Journal on Educational Resources in Computing, vol. 7, no. 3, pp. 2-es, Nov. 2007.

[23] C. E. Irvine, M. F. Thompson, and K. Allen, "CyberCIEGE: Gaming for information assurance," IEEE Security and Privacy Magazine, vol. 3, no. 3, pp. 61-64, May 2005.

[24] C. E. Irvine and M. F. Thompson, "Simulation of PKI-enabled communication for identity management using CyberCIEGE," 2010 - MILCOM 2010 MILITARY COMMUNICATIONS CONFERENCE, Oct. 2010.

[25] M. Thompson and C. Irvine, "Active learning with the CyberCIEGE video game," USENIX Association, 2011, p. 10. [Online]. Available: http://dl.acm.org/citation.cfm?id=2028009. Accessed: Apr. 15, 2016.

[26] F. Kayali et al., "A case study of a learning game about the Internet," 2014. [Online]. Available: https://eprints.cs.univie.ac.at/4122/. Accessed: Apr. 15, 2016.

[27] P. Chapman, J. Burket and D. Brumley, "PicoCTF: A Game-Based Computer Security Competition for High School Students," 2014 USENIX Summit Gaming Games Gamification Secur. Educ. 3GSE 14, 2014.

[28] M. Olano, A. Sherman, L. Oliva, R. Cox, D. Firestone, O. Kubik, M. Patil, J. Seymour, I. Sohn, and D. Thomas, 2014, August. "SecurityEmpire: Development and Evaluation of a Digital Game to Promote Cybersecurity Education," 3GSE, 2014.

[29] S. Ariyapperuma and A. Minhas, "Internet security games as a pedagogic tool for teaching network security," Frontiers in Education, 2005. FIE'05. Proceedings 35th Annual Conference, p. S2D-1, 2005. [Online]. Available: http://dx.doi.org/10.1109/FIE.2005.1612218. Accessed: Apr. 15, 2016.

[30] W. A. Labuschagne, N. Veerasamy, I. Burke, and M. Eloff, "Design of cyber security awareness game utilizing a social media framework," Information Security South Africa (ISSA), 2011, pp. 1-9, 2011.

[31] W. A. Labuschagne, M. Eloff, "The Effectiveness of Online Gaming as Part of a Security Awareness Program," 13th European Conference on Cyber Warfare and Security ECCWS-2014 The University of Piraeus Piraeus, Greece, p. 125, 2014.

[32] MAVI Interactive LLC, "Agent Surefire." [Online]. Available: http://www.maviinteractive.com/default.asp. Accessed: Apr. 15, 2016.

[33] "Anti-Phishing Phil." [Online]. Available: http://www.ucl.ac.uk/cert/antiphishing/. Accessed: Apr. 15, 2016.

[34] Australian Department of Broadband Communications and the Digital Economy, "Budd;e Cybersecurity Education." [Online]. Available: https://budd-e.cybersmart.gov.au/. Accessed: Apr. 15, 2016.

[35] Carenegie Mellon, "The Carnegie Cyber Academy." [Online]. Available: http://www.carnegiecyberacademy.com/. Accessed: Apr. 15, 2016.

[36] "Cyber Ciege Educational Video Game." [Online]. Available: http://cisr.nps.edu/cyberciege/. Accessed: Apr. 15, 2016.

[37] Information Assurane Support Environment, "CyberProtect." [Online]. Available: http://iase.disa.mil/eta/Lists/IA%20Simulations/AllItems.aspx. Accessed: Apr. 15, 2016.

[38] "Cybersecure Contingency Planning." [Online]. Available: http://www.healthit.gov/sites/default/files/CyberSecure_103_FINAL/index.html. Accessed: Apr. 15, 2016.

[39] Cyber Security Challenge UK, "Cyphinx." [Online]. Available: https://cybersecuritychallenge.org.uk/cyphinx/. Accessed: Apr. 15, 2016.

[40] The Federal Bureau of Investigations, "Kids Games." [Online]. Available: https://www.fbi.gov/fun-games/kids. Accessed: Apr. 15, 2016.

[41] PwC, "Game of Threats - Cybersecurity Risk Simulation," PwC. [Online]. Available: http://www.pwc.com/us/en/financial-services/cybersecurity-privacy/game-of-threats.html. Accessed: Apr. 15, 2016.

[42] "NSteens." [Online]. Available: http://www.nsteens.org/Games. Accessed: Apr. 15, 2016.

[43] "OnGuardOnline." [Online]. Available: http://www.onguardonline.gov/media. Accessed: Apr. 15, 2016.

[44] "Cybersecurity Lab | NOVA Labs | PBS." [Online]. Available: http://www.pbs.org/wgbh/nova/labs/lab/cyber/. Accessed: Apr. 15, 2016.