INTL JOURNAL OF ELECTRONICS AND TELECOMMUNICATIONS, 2017, VOL. 63, NO. 2, PP. 217–222
Manuscript received January 19, 2017; revised April, 2017. DOI: 10.1515/eletel-2017-0029

Network Information Hiding and Science 2.0: Can it be a Match?

Steffen Wendzel, Luca Caviglione, Wojciech Mazurczyk, and Jean-Francois Lalande

***Abstract*—Science 2.0 aims at using the information sharing and collaborative features of the Internet to offer new features to the research community. Science 2.0 has been already applied to computer sciences, especially bioinformatics. For *network information hiding*, a field studying the possibility of concealing a communication in networks, the application of Science 2.0 is still a rather uncovered territory. To foster the discussion of potential benefits for network information hiding, we provide a disquisition for six different Science 2.0 aspects when applied to this domain.**

***Keywords*—Network Steganography, Information Hiding, Steganography, Science 2.0, Open Science, Covert Channels**

I. Introduction

SCIENCE 2.0 aims at fully exploiting the Internet to enable researchers to collaborate and share information (e.g., ideas, experiments, datasets and scientific papers) in order to increase both the volume and the quality of results, while mitigating costs. Science 2.0 is rooted within the "open" movement and emphasizes the collaborative flavor made feasible by the advent of Web technologies.

As today, one of the most successful examples of Science 2.0 is given by myExperiment [1], which is a social website enabling to share scholarly information and scientific workflows in the field of bioinformatics. Another popular attempt is Galaxy Zoo [2] using crowdsourcing to foster the collaboration among scientists for the morphological classification of galaxies. For the case of network security, there are no Science 2.0 initiatives comparable with the aforementioned ones. The only notable exception is given by arXiv [3], a database of preprints of scientific papers, which contains the cs.CR category for "Cryptography and Security". Even if it was intended as a place to store works from different research fields, e.g., mathematics, statistics and physics as shown in Table I, it is not uncommon to find results dealing with computer science or network security.

In this paper, we focus on *network information hiding*, a discipline of network security that tries to hide the exchange of information on the network and that also tries to detect such stealthy communications. For instance, network information hiding is becoming an increasingly popular technique for malware, which can remain stealthy for a long time by cloaking the flows of stolen information within licit network traffic.

S. Wendzel is with the Worms University of Applied Sciences, Worms, Germany (e-mail: wendzel@hs-worms.de).

L. Caviglione is with the Institute for Intelligent Systems for Automation (ISSIA), Genova, Italy (e-mail: luca.caviglione@ge.issia.cnr.it).

W. Mazurczyk is with the Warsaw University of Technology, Institute of Telecommunications, Warsaw, Poland (e-mail: wmazurczyk@tele.pw.edu.pl).

J.F. Lalande is with the INSA Centre Val de Loire - Inria, Bourges, France (e-mail: jean-francois.lalande@insa-cvl.fr).

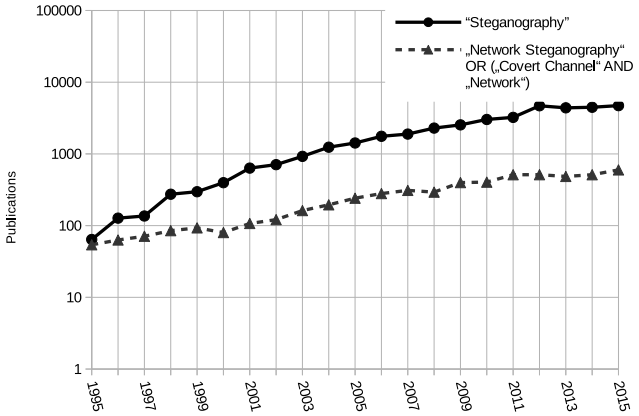

Fig. 1. Google Scholar hits for selected search terms (1995-2015).

When searching the 2015 arXiv pre-print's abstracts for information hiding-related keywords, only 8 papers contain the terms "network" and "steganography" (network steganography is a sub-discipline of network information hiding), 16 contain "steganography" (which is a term that includes network information hiding but also other terms of information hiding, such as hiding techniques for audio or video content), and 6 contain "covert" and "channel" (a term to describe a hidden communication channel).

On the other hand, Figure 1 shows the yearly publications per search term obtained from Google Scholar between 1996-2015. As the comparison of of both sources (arXiv and Google Scholar) indicates, the number of related publications per year that were indexed by Google Scholar (that also indexes non-open publications) is significantly higher, indicating that arXiv is not equally covering network information hiding publications.

TABLE I
Statitics for arXiv pre-prints for the year 2015

Category	cs	cs.CR	math	q-bio	q-fin	physics	stat
# papers	16179	828	28753	1558	689	8719	2541

With regard to security, information hiding definitely plays a role since it has been used to increase the stealthiness of many hazards, for instance Internet malware [4]. In essence, it aims at studying techniques (and countermeasures) to inject secret data within an innocent looking carrier. It aims at cloaking a

communication within network traffic to make any third part observers unaware of the undergoing data exchange. Moreover, even if important, it represents a small niche of network security. For this reason, the research community investigating network information hiding is small and conferences explicitly dealing with such results are rare.

In this perspective, Science 2.0 could be an important enabler to help the network information hiding community to reach a proper critical mass as well as to capture more attention from academics, vendors, and professionals working in the network security panorama. Therefore, the contributions of this paper are: *i*) to propagate a tailored discussion of Science 2.0 in the area of information hiding in communication networks, *ii*) to foster the analysis of a Science 2.0-driven collaboration, experiment design, handling of re-inventions, tracking of progress in the research domain and potential impacts on teaching of network information hiding, and *iii*) to enlighten possible matches among Science 2.0 and well-defined tasks that need to be undertaken by the research community dealing with network information hiding.

This paper is structured as follows. Section II presents related work on Science 2.0. We discuss Science 2.0 in information hiding by starting with a discussion on terminological issues and the handling of re-inventions in Section III, followed by covering Science 2.0-based experiments in Section IV, and the tracking and fostering of the research progress in Section V. Our discussion continues by highlighting the importance of Science 2.0 in the development of standards and countermeasures for network information hiding in Section VI, a Science 2.0-supported teaching of network information hiding at universities in Section VII, and the required effort to introduce Science 2.0 in the research domain in Section VIII. Section IX concludes.

II. Related Work

A large number of publications is available on scientific practice and Science 2.0 in the age of Web 2.0. For instance, Priem and Hemminger discuss scholarly impact metrics in the social Web, called "Scientometrics 2.0" in [5]. The authors emphasize three important uses of Scientometrics 2.0, which are the evaluation of scholars, the recommendation of articles, and the study of science. In addition, the authors mention several limitations of the paradigm, e.g., that Web 2.0 tools are replaced by other Web 2.0 tools in a frequent manner and can face spam. Various advantages and drawbacks as well as the motivation of interviewed scientists when using Science 2.0 are highlighted in [6]. Nattkemper discusses the use of Science 2.0 in applied (bio)informatics and medicine in [7]. He states that Science 2.0 is not used in its full capacity and solutions need to provide new data analysis methods for researchers to motivate a stronger value for them. Bücheler and Sieg study the applicability of Crowdsourcing and Open Innovation in the scientific context [8] while West *et al.* [9] review the contribution and evolution of Open Innovation from the history perspective. Franzoni and Sauermann [10] analyze an open collaborative fashion of scientific research which is often referred to as Crowd Science. The authors identify two characteristic features of such projects, namely open participation and open sharing of intermediate inputs, and then explore crowd science's potential knowledge-related and motivational benefits. Laursen and Salter [11] study a paradox of openness where firms (but also research teams) to innovate need to collaborate with many outside actors (research teams, organizations, institutions, etc.). Thus the creation of innovations requires openness, but on the other hand the commercialization of innovations requires protection. Similar issues are often considered for Science 2.0. Anderson discusses several potential advantages of Science 2.0 in the conference review process for computer science [12]. We will refer to selected aspects of his work in the context of network information hiding in Section V-3. In addition, Science 2.0 (and related topics, such as eScience or Open Science) is dealt with in own conferences.

III. Terminological Issues and Handling of Re-Inventions

A consistent terminology is essential for every domain to ensure the efficient progress of research work and the communication between scholars. In computer security and dependability, working groups such as the Fundamental Concepts and Terminology committee exist since decades to develop such a unified terminology [13].

So-called re-inventions have always been a component of science [14]. Especially due to the rapid development of different types of information hiding methods and terminological inconsistencies in this field, various ideas how to hide data were invented multiple times [15]. The largest divergence in the network information hiding terminology can be found in the valley between the terms 'network covert channels' and 'network steganography' as these overlapping areas developed various similar/identical aspects. Various approaches were made to unify the terminology and categorization of hiding methods. Two recent surveys are [15] and [16].

Currently, another problem is that many different information hiding techniques can be utilized on a single device simultaneously. This is a consequence of the trend of devices combining features previously covered by several separate ones. For instance, smartphones offering a high-resolution camera, different air interfaces (e.g., Bluetooth, 3G and IEEE 802.11), and GPS. In this scenario, known classifications are too method-specific, thus requiring a wider perspective. Especially, there is a need for a taxonomy allowing to grasp all the areas in which information hiding can take place, thus demanding for a 'cross-layer' scheme.

The need for the above-mentioned publications reflects the fact that terminological inconsistencies are present in the research domain. Science 2.0 tools can support a clean terminology and taxonomy. For instance, a collaborative Wiki can be used to discuss and merge terms. A similar approach, namely using a structured website with user comments for discussion of a research topic, is applied by the software

patterns[1] research community, in which patterns are discussed online [17]. Patterns can also be used to build terminological databases and taxonomies as they can form hiearchies. In network information hiding, [15] also shows that 109 information hiding methods developed between 1987 and 2013 can be reduced to only eleven similar methods by describing these methods using a pattern-based taxonomy. This will most likely lead to novel countermeasures which counter whole patterns of hiding methods instead of only one of the more than 100 hiding methods. The authors have proposed the setup of online platforms for pattern-based discussions in network information hiding. By applying these recent outcomes of research work, unintentional re-inventions of hiding methods will not be eliminated but reduced.

On the contrary, we need to consider if there are points which speak against the use of Science 2.0 for improving terminology and handling re-inventions. Firstly, it could have only a moderate effect on the taxonomy of the research domain as existing publications feature old terminology and not all new research will adapt the new terminology. Secondly, online discussions can lead to *forks*, i.e., novel terminological paths that may improve the existing terminology but lead to even more terms. Thirdly, existing terminology and taxonomy working groups are already capable to achieve a high-quality output (e.g., [13]) without using Science 2.0 methods.

IV. Experiments

Experiments in network information hiding can be represented by two cases. Firstly, those experiments that test and measure the quantitative and qualitative aspects of hiding methods. Secondly, experiments that test and measure the quantitative and qualitative aspects of countermeasures for hiding methods. As reported in [15], more than hundred techniques for network covert channels are known. Also, a plethora of countermeasures are known for these techniques. For only few of these techniques, researchers can directly access and modify proof of concept implementations, experimental data, and exact workflow descriptions.

1) Collaborative Experiments: Science 2.0 provides various online solutions, such as the mentioned *MyExperiment* [1] which allows the detailed description of particular scientific workflows. In network information hiding, such workflows need to include information about the configuration of proof of concept codes, network interfaces, virtual machines, data to process, and all other components of the experimental design. The community can help to review experimental setups and can thus help to improve these before research work is actually submitted.

Collaborative tools such as *Github* [18] allow the easy sharing of code and forking of software projects. Nevertheless, there is no effort for formalizing the set of inputs and to support the execution of experiments for a perfect reproducibility. New tools with less development functionalities but with better collaborative aspects for research appeared. For example, HubZero [19] allows to build a light virtual environment and to upload the software code of an experiment. Then, this environment acts as a module and can be called by other modules in order to benefit from the service. Each module, published under open source license, allows to produce new derivative experiments and obtain results using a physical back-end supporting the infrastructure. The platform reduces software and licensing costs for external researchers but (long-term) maintenance costs still remain for HubZero.

A variety of Science 2.0 tools to support experiments have been developed by physicists and biologists. These tools are barely used in information security, including network information hiding. The reasons for non-use are: *i*) the lack of a common format for scientific data, *ii*) the lack of software components which can be run to conduct related experiments, and *iii*) the lack of detailed workflow descriptions which can be integrated into platforms such as *MyExperiment*. The adoption of Science 2.0 tools into the network information hiding domain will be a clear advantage if these previous aspects can be improved by the research community.

In a further step, experimental setups could most easily be shared as virtual machines including pre-configured testbeds. Alternatively, research institutions with a strong focus on network information hiding could provide a publicly-accessible shared testbed for network information hiding techniques to which every institution could contribute own (virtualized) machines which feature testbed setups. Such a research infrastructure will require massive and long-term funding which could be a strong limitation. Possibly existing unused infrastructure could be utilized for such testbeds to reduce costs.

By releasing both covert channel tools and countermeasures tools under OSS licenses, e.g. as done in case of CCEAP [20], the research community could evaluate them in a comparable manner and experiments could easily be reproduced by third parties. Therefore Science 2.0 could form a common “battleground” to enable reliable comparative analysis of new and existing approaches for network hiding methods detection.

2) Competition and Overhead: However, we also identified several difficulties for Science 2.0-driven experiments, especially for young researchers with a restricted budget.

Science 2.0 tools, especially in open communities, require individual scientists to share their insights, experimental setup details and tools. Providing these information means to give away an advantage, which is important for especially younger scientists who need to establish a unique profile in the community in order to reach a permanent position in academia.

The overhead of work to make experiments usable by other researchers could be too high for convincing researchers to publish their experimental systems (code, workflow descriptions, etc.). Processed data may be confidential, especially if captures of real network traffic are used, which may contain hidden messages from real attackers.

In addition, as Science 2.0 lowers the barrier for interacting with other research projects, it could become increasingly tempting for individual researchers to join a large number of research projects simultaneously. As stated by Bertolotti *et al.*, multi-team memberships of R&D teams do not solely lead to advantages but also to challenges for these teams

[1]Software patterns are abstract descriptions of solutions to problems in a given context; they originate from the field of architecture. For instance, a pattern can describe a user-interface (solution) for a website (context) to achieve a suitable way to insert specific data (problem).

[21]. For instance, if one researcher allocates few time on one of his many projects but some particular project demands his contribution, the progress made by the project can be decreased.

V. Tracking and Fostering Research Progress

The network information hiding community is small in comparison to many other communities of information security. Its size may enable the manual tracking of the field's progress by a single researcher.

3) Tracking for Individuals: Manual tracking consumes a larger percentage of the researcher's time. The support of Science 2.0 tools enables the faster tracking of the domain's developments. Science 2.0 tools are already used by a larger number of information hiding researchers as the presence of online profiles reveals. However, as also reflected in [22] the popularity of various Science 2.0 platforms differs significantly. For instance, in the field 'science and engineering' more than 90% of the researchers who reported to *Nature* said they are at least aware of *Google Scholar* [23] (or visit regularly) while less than 20% of the scholars were aware of *Microsoft Academic Search* [22]. A stronger use of the available tools will benefit the research domain. In addition, the scientific progress can be accelerated while allowing its tracking when Science 2.0 is used for the review process.

4) Fostering Research Progress: Websites and apps such as Google Scholar, ResearchGate [24], Overleaf [25], Authorea [26], HubZero [19] and Mendeley [27] provide reference managers, tools to read and annotate publications, and various ways for scientific collaboration. These platforms allow to track either particular researchers of a domain or a whole domain itself, for instance, by subscribing to search terms. Joint online writing and tools to perform experiments can help especially narrow fields to become more mature due to collaboration. In addition, such online collaboration tools increase the chances of individual authors for finding international co-authors. This factor is important as papers with multi-national authors increase the likeliness of citations [28], while citations and related research indicators influence research policies and performance incentives such as funding allocation [29].

Another aspect of research progress tracking is the review process. Anderson suggests to improve the transparency of the review process in [12]. One of his suggestions is that all reviewed papers of a conference should be published online. Without Science 2.0, accepted papers appear in proceedings and journals while rejected paper will not appear although they can still contribute significantly to research. For this reason, Anderson states that the *research community is worse off* if rejected papers remain unpublished [12]. This argument is supported by Mogul's statement that computer science reviewing is becoming *increasingly "hypercritical"* [30]. Additional evidence and discussion on this problem is provided by Meyer in [31]. Anderson mentions the fact that with the current system, some authors tend to submit unfinished work in the hope to get it accepted nevertheless. In network information hiding, for instance, some submitted papers lack a strong evaluation or a proof of concept implementation. If even rejected submissions will be published online, authors may not want to see their names on their own publications as these are unfinished [12]. In this context, Science 2.0 can increase the quality of submissions by preventing intentionally low-qualified papers which are submitted only to receive review feedback. Instead of publishing unfinished work, ongoing work can be developed online together with other scientists before it will be submitted. Overall, such approaches, including the community review of web publications [12], [30], could speed up the progress in information hiding while also easing progress tracking.

5) Required Effort: As mentioned in Section V-3, Science 2.0 tools enable a faster tracking of the domain's progress. However, the field of network information hiding may be too small for the utilization of *multiple* Science 2.0 tracking tools to be profitable for the individual researcher. In addition, the researchers' time to maintain online scientific data on several webpages or tools could require more time than the manual tracking itself. For instance, maintaining online research profiles requires the researcher to list his publications in each platform and to correct errors of automatically detected articles. Participation via Science 2.0 means to read and publish online discussions, to review peer's articles in various other platforms, and to perform collaboration using different tools at the same time. The combination of all these tasks can lead to a large overhead.

VI. Standardization

In network information hiding there is a tight relation between the hiding method and carrier: the injection of hidden information primarily takes place by exploiting features of software implementations and protocol behavior with respect to the protocol's specification. In order to hide data within network traffic, precisely understanding how and where the needed information is stored within the related flow of packets is a mandatory step. At the same time, scientific literature already proved that there exists no general countermeasure to limit all forms of network information hiding. For this reason, each hiding method must be carefully studied.

6) From Standards to Countermeasures: By addressing information hiding early during the design phase (e.g., by using formal methods such as the *Shared Resource Matrix* (SRM) [32]) it should be possible to develop protocols more robust against data hiding. A tight interaction among researchers and developers could prevent issues, such as packets with unneeded fields or ambiguous meanings, which are a primary target for the injection of cloaked information. In this perspective, Science 2.0 would improve the pollination across academia and standardization bodies, which often neglect more theoretical and "what if" cases in favor of well-agreed implementations or practices. Thus, the collaborative nature of Science 2.0 could make the scientific pipeline (e.g., the process ranging from research planning to publication of results) more accessible. For instance, the standardization world can request and suggest ad-hoc tests, while the scientific world can perform state-of-the-art analysis on protocols albeit in an alpha phase.

For the case of Internet protocols, researchers and network/software engineers can collaborate through Science 2.0 tools in order to assess steganography risks early during the design stage. From the viewpoint of evaluating novel data hiding attacks, the access to the needed information is already possible by retrieving the proper *Request for Comments*, which are made publicly available by the *Internet Engineering Task Force* (IETF). One of IETF's founding rules is *rough consensus and running code*, what makes IETF a standardization body already compliant with the Science 2.0 paradigm. As consequence, this has two major implications: *i*) attackers and researchers have access to precise information about protocols and prototype implementations avoiding the need of performing reverse engineering or toy set-ups to test the effectiveness of their network steganography methods, and *ii*) the standardization process is open to all participants, thus enabling to early address steganographic threats during the development phase. In other words, when designing new protocols, addressing 'security' is mandatory for IETF.

In this perspective, the adoption of the Science 2.0 paradigm can boost the cooperation among the two worlds having positive impacts, such as: making the standardization community more aware of steganographic threats, establishing trial-and-error cooperation to mitigate the features that can be exploited for data hiding, and providing an unified and coherent knowledge to be used for the development on countermeasures. This is an important outcome as it can increase the chances of having countermeasures handled within the standardization pipeline and, eventually, increase their diffusion and adoption.

7) Efforts for the Standardization Process: Being able to actively participate in standardization activities, especially during the design phase of network protocols, requires both formal and technical knowledge. To this aim, Science 2.0 can improve the credibility of a (group of) scientist(s), but could fail to support claims to be pushed in the standardization pipeline. In fact, experimental set-ups are still only a starting point while standardization needs working prototypes and solutions rising a wide interest. Additionally, a standardization process requires the support of companies that have a strong interest to see the proposed standards adopted. These latter should have a major role in key sectors like telecommunications or the Internet of Things, where pushing countermeasures into new standards would have an impact. Using collaborative tools or open licenses may result in a conflict with these companies' policies and reduce the global effort in a standardization process where countermeasures would be seen as additional constraints for developing business.

VII. Teaching

Only few courses on network information hiding can be found at the undergraduate or graduate level (e.g., Master's level courses at the Warsaw University of Technology since 2012). Teaching is essential to keep the research domain alive and to allow its growth.

As mentioned in the introduction, recently a new attack trend has been discovered as network information hiding methods are increasingly utilized for improved stealthiness by various types of current malware [4]. This fact makes it important to incorporate lectures about information hiding techniques, the threat they pose and possible countermeasures as an essential part of information/network security courses.

8) Designing Network Information Hiding Lectures: Teaching of network information hiding should be included at different levels of education including specialized courses for security professionals. The sooner the knowledge about recent advances in network information hiding methods and countermeasures is disseminated among scientists, students and security professionals the higher the awareness and sensitivity for such threats. This is where Science 2.0 could play a significant role.

However, there are no unified methods to teach network information hiding, especially when laboratory experiments must be performed (e.g., determining the capacity of a covert channel). As mentioned before, experimental setups and code are often not available. Hence, teaching cannot profit from it.

9) Teaching and Science 2.0-based Learning: Social networks dedicated to self-learning tools like *Massive Open Online Courses* (MOOC) can be considered a core component of a Science 2.0-based learning. Using a creative common license to distribute courses supports the dissemination of materials and increases their visibility. Online courses could be created by cooperating groups that are specialized in network information hiding. This would enable a detailed coverage of the most important aspects of this field. For the setup of testbeds with the already mentioned Science 2.0 solutions, such as myExperiment and HubZero, or tailored open source tools such as CCEAP [20], experimental setups can easily be made accessible to students and used for teaching purposes.

Nevertheless, ensuring the quality of online lectures and the easy application of available experiments in local setups can be difficult. Scientific experiments are designed in a detail level that is often too difficult to be used on an undergraduate level. Implementing hidden channels requires to know precisely the target programming language of the hosts (Java under Android, C for a regular Linux process, etc.) and to have advanced knowledge of networks. The amount of required knowledge and the programming skills could make it difficult to obtain an online course which is understandable, especially for MOOCs.

VIII. Required Effort for the Research Community

Compared to other research topics (e.g., network security intended as a monolithic area), the volume of works dealing with network steganography is quite modest, as also demonstrated by terminological issues and recent surveys [15], [16]. Therefore, the knowledge in terms of papers and prototypes needing to be migrated over Science 2.0 platforms could be easily handled by the research community. Figure 1 already highlighted the yearly publications per search term obtained from Google Scholar. Due to this still rather low number of publications, the effort to port past papers and research results into a Science 2.0 area could be feasible and could help potentially emerging network information hiding into a Science 2.0-native discipline.

Nevertheless, groups performing research on network steganography appear as highly segmented. For instance, there are excellences studying the threat in smart buildings, mobile devices and in Voice over IP (VoIP) protocols. The migration of results towards a Science 2.0 approach requires cooperation and trust between the participating researchers.

These requirements could become a hurdle for achieving the cooperation of a larger number of research groups. A virtualized and segment-overlapping framework based on Science 2.0 would help research groups to have a greater critical mass, achieving a wider knowledge and develop more sophisticated methods and countermeasures. Moreover, papers may in future be authored by a larger number of researchers which are participating in the scientific process, resulting in lower career value for each author.

IX. Conclusion

We highlighted six Science 2.0-related aspects and discussed their potential influence on network information hiding. We see a clear benefit of Science 2.0 for this research domain although the mentioned hurdles exist and drawbacks must be considered. The size of the community, the inter-disciplinary nature of the field, the requirement of experimental setups and the links with standards and teaching facets result in a majority of the provided arguments. In particular, the bridge between reusable academic experiments and the effort in the standardization of countermeasures requires to have development and collaborative tools to structure the research community. For monitoring and disseminating the research results, Science 2.0 efforts are already ongoing. Nevertheless, the academic teaching of information hiding is still in its infancies but is expected to benefit from Science 2.0.

References

[1] D. D. Roure, C. Goble, and R. Stevens, "The design and realisation of the virtual research environment for social sharing of workflows," *Future Generation Computer Systems*, vol. 25, no. 5, pp. 561 – 567, 2009.
[2] Zooniverse, "Galaxy Zoo website," 2015, http://www.galaxyzoo.org.
[3] Cornell University, "ArXiv website," 2015, http://arxiv.org/.
[4] W. Mazurczyk and L. Caviglione, "Information hiding as a challenge for malware detection," *IEEE Security & Privacy*, vol. 13, no. 2, pp. 89–93, 2015.
[5] J. Priem and B. M. Hemminger, "Scientometrics 2.0: Toward new metrics of scholarly impact on the social web," *First Monday*, vol. 15, no. 7, July 2010.
[6] T. Lin, "Cracking open the scientific process," January 2012, http://www.nytimes.com/2012/01/17/science/open-science-challenges-journal-tradition-with-web-collaboration.html.
[7] T. W. Nattkemper, "Are we ready for science 2.0?" in *International Conference on Knowledge Management and Information Sharing*, K. Liu and J. Filipe, Eds., Barcelona, Spain, 2012, pp. 302–306.
[8] T. Bcheler and J. H. Sieg, "Understanding science 2.0: Crowdsourcing and open innovation in the scientific method," *Procedia Computer Science*, vol. 7, no. 0, pp. 327 – 329, 2011.
[9] J. West, A. Salter, W. Vanhaverbeke, and H. Chesbrough, "Open innovation: The next decade," *Research Policy*, vol. 43, no. 5, pp. 805 – 811, 2014, open Innovation: New Insights and Evidence.
[10] C. Franzoni and H. Sauermann, "Crowd science: The organization of scientific research in open collaborative projects," *Research Policy*, vol. 43, no. 1, pp. 1 – 20, 2014.
[11] K. Laursen and A. J. Salter, "The paradox of openness: Appropriability, external search and collaboration," *Research Policy*, vol. 43, no. 5, pp. 867 – 878, 2014, open Innovation: New Insights and Evidence.
[12] T. Anderson, "Conference reviewing considered harmful," *ACM SIGOPS Operating Systems Review*, vol. 43, no. 2, pp. 108–116, 2009.
[13] A. Avižienis, J.-C. Laprie, B. Randell, and C. Landwehr, "Basic concepts and taxonomy of depandable and secure computing," *IEEE Trans. Depandable and Secure Computing*, vol. 1, no. 1, pp. 11–33, 2004.
[14] D. K. Simonton, *Creativity in science: Chance, logic, genius, and zeitgeist*. Cambridge University Press, 2004.
[15] S. Wendzel, S. Zander, B. Fechner, and C. Herdin, "Pattern-based survey and categorization of network covert channel techniques," *ACM Computing Surveys (CSUR)*, vol. 47, no. 3, 2015.
[16] W. Mazurczyk and L. Caviglione, "Steganography in modern smartphones and mitigation techniques," *Communications Surveys Tutorials, IEEE*, vol. 17, no. 1, pp. 334–357, Firstquarter 2015.
[17] "User interface design patterns," 2015, http://ui-patterns.com/patterns.
[18] "Github website," 2015, https://github.com/.
[19] M. McLennan and R. Kennell, "Hubzero: A platform for dissemination and collaboration in computational science and engineering," *Computing in Science Engineering*, vol. 12, no. 2, pp. 48–53, March 2010.
[20] S. Wendzel and W. Mazurczyk, "Poster: An educational network protocol for covert channel analysis using patterns," in *Proc. 23rd ACM Conference on Computer and Communications Security (CCS)*. ACM, 2016, pp. 1739–1741.
[21] F. Bertolotti, E. Mattarelli, M. Vignoli, and D. M. Macr, "Exploring the relationship between multiple team membership and team performance: The role of social networks and collaborative technology," *Research Policy*, vol. 44, pp. 911–924, 2015.
[22] R. Van Noorden, "Online collaboration: Scientists and the social network," *Nature (News Feature)*, vol. 512, pp. 126–129, August 2014.
[23] Google Inc., "Google scholar website," 2015, http://scholar.google.de/.
[24] ResearchGate GmbH, "ResearchGate website," 2015, http://www.researchgate.net/.
[25] "Overleaf website," 2015, https://www.overleaf.com/.
[26] "Authorea website," 2015, https://www.authorea.com.
[27] Mendeley Ltd., "Mendeley website," 2015, https://www.mendeley.com.
[28] K. A. Khor and L.-G. Yu, "Influence of international co-authorship on the research citation impact of young unviersities," *Scientometrics*, vol. 107, pp. 1095–1110, 2016.
[29] J. Kosten, "A classification of the use of research indicators," *Scientometrics*, vol. 108, pp. 457–464, 2016.
[30] J. C. Mogul, "Towards more constructive reviewing of CS papers," *ACM SIGCOMM Computer Communication Review*, vol. 43, no. 3, pp. 90–94, Jul. 2013.
[31] B. Meyer, "The nastiness problem in computer science," *BLOG@CACM*, August 2011, http://cacm.acm.org/blogs/blog-cacm/123611-the-nastiness-problem-in-computer-science/fulltext.
[32] R. A. Kemmerer, "Shared resource matrix methodology: an approach to identifying storage and timing channels," *ACM Transactions on Computer Systems*, vol. 1, no. 3, pp. 256–277, 1983.