A Taxonomy and a Knowledge Portal for Cybersecurity

David Klaper
Carnegie Mellon University
5000 Forbes Avenue
Pittsburgh, PA, United States
dklaper@cs.cmu.edu

Eduard Hovy
Carnegie Mellon University
5000 Forbes Avenue
Pittsburgh, PA, United States
hovy@cmu.edu

ABSTRACT

Smart government is possible only if the security of sensitive data can be assured. The more knowledgeable government officials and citizens are about cybersecurity, the better are the chances that government data is not compromised or abused. In this paper, we present two systems under development that aim at improving cybersecurity education. First, we are creating a taxonomy of cybersecurity topics that provides links to relevant educational or research material. Second, we are building a portal that serves as platform for users to discuss the security of websites. These sources can be linked together. This helps to strengthen the knowledge of government officials and citizens with regard to cybersecurity issues. These issues are a central concern for open government initiatives.

Categories and Subject Descriptors

K.3.2 [**Computers and Education**]: Computer and Information Science Education

General Terms

Security, Human Factors

Keywords

Cybersecurity, Taxonomy, Systematization, Education

1. INTRODUCTION

Every day the news presents new revelations about a company being "hacked". *Cybersecurity* is the field of securing the cyberspace. It is about defending digital systems against abuse, intrusion, and other dangers. Often cybersecurity is seen as a purely technical discipline. However, humans take the decisions and humans usually have the power to overrule a system. Therefore, it is important that the people who administrate or even just use systems containing sensitive information know important safety principles and mechanisms. Otherwise, the easiest way to get the sensitive information is approaching the users or administrators and misleading them.

dg.o '14, June 18 - 21 2014, Aguascalientes, Mexico Copyright is held by the owner/author(s). Publication rights licensed to ACM. ACM 978-1-4503-2901-9/14/06 $15.00. http://dx.doi.org/10.1145/2612733.2612759

One task of open government initiatives is offering data and services to their citizens over the web. Unfortunately, the web is often an insecure place. A government cannot afford to lose the trust of its citizens. Thus, any compromised data equates a disaster. In explaining the cybersecurity lifecycle for open government, Microsoft claims that it is not possible to guarantee security [11]. In consequence, they advise planning for the security lifecycle. This means having specific detection and recovery plans. Of course, one goal of governments should be to reduce the number of times the recovery plan is needed. Educated personnel and citizens can help mitigate some of the common security holes. For example, a common belief that can be very dangerous is that it is always safe to visit sites that were previously safe. Cybersecurity education resources can aid in explaining why this is not true. This paper presents resources that help to provide an organization of cybersecurity topics.

The impact of cybersecurity is particularly critical for governments. In addition to sensitive data that could be exposed, any incident could shatter citizen support for open government initiatives or any other form of online participation of the government. The sheer number of government reports shows the relevance of the subject. Tehan [19] has compiled a list for the U.S. congress. Government reports advise on ways how to reduce the risks by using frameworks and following certain tips. For instance, the report by the Department of Treasury [4] states "*Although there are many cybersecurity standards, practices, and guidelines, they do not appear to be consistently or uniformly applied*". To mitigate this circumstance they recommend adopting the NIST cybersecurity framework [12] that has recently been released. The framework outlines specific actions, such as protection of data in transit, to improve cybersecurity. However, it does not say how this is to be achieved. Similarly, the Government Accountability Office report [7] concentrates on strategic issues. The report by the President's council of advisors on science and technology [16] explicitly points out that fast response is a critical factor in cybersecurity.

The reports are good at showing what needs to be done but they are largely silent on how to keep the necessary knowledge current. It is impossible to react timely if the responsible people do not have the vocabulary to communicate what kind of attack it is. A taxonomy of cybersecurity can mit-

igate this by providing a sound classification of concerns. Furthermore, an up-to-date taxonomy can serve as basis for building tailored training courses for staff. The courses can balance technical topics with background on the history, law, and motives behind cybercrime.

The outline of this paper is as follows. After this introduction, Section 2 starts with an overview of the taxonomy we are creating. Subsequently, the most important concepts of the taxonomy are explained. In Section 3, the *Personal Cybersecurity Assistant* (PCA) portal is introduced. This is a browser plugin and website for commenting on websites that can be used to discuss specific security concerns. Also, it provides links to relevant educational content. In Section 4, we outline some future work for this project. Finally, Section 5 briefly summarizes this paper.

2. TAXONOMY

Cybersecurity is a quite fragmented field. It is hard to find overviews that consider a broad spectrum of research directions. Teaching or understanding cybersecurity requires an organized overview. Ideally, this overview is complemented with educational material. Therefore, we have started to compile various resources and collect them in a taxonomy. The taxonomy[1] organizes the concepts hierarchically. Each concept includes a short description and relevant external links, for instance, links to relevant research papers. There are also relations between the different concepts; sometimes the taxonomy contains crosslinks (although we have not studied the types of relations between the different concepts systematically yet).

2.1 Different Taxonomies

We have created three taxonomies, each showing a different aspect. The main taxonomy is our focus and is explained in detail below. It has grown to a rather broad scope although it has started as a rather technical taxonomy. The main taxonomy is complemented by two much smaller taxonomies. First, an operational taxonomy copied from Cebula and Young [1], which is enriched with relevant links. Second, a taxonomy that focuses on different types of users and their specific cybersecurity knowledge needs. In the remaining subsections we present the most important concepts of the main taxonomy. Since its inception the scope has grown and it covers both technical and social aspects of cybersecurity. The two different views are separate concepts in the taxonomy. Together they can combine to form a better understanding of the whole field of cybersecurity.

2.2 Technical Aspects of Cybersecurity

The technical concepts in the taxonomy relate to specific attacks, subareas of the field, and defense mechanisms. The initial taxonomy had five concepts. The five concepts are 'data integrity verification', 'cryptography', 'intrusion detection and risk mitigation', 'authentication and authorization', and 'auto-analysis of legitimate usage patterns'. Later, we added 'computer forensics' as a concept. We explain each of these main concepts below and detail the corresponding subconcepts to give an indication of the multitude of topics that comprise cybersecurity and may have impact on open government initiatives.

Data integrity verification deals with asserting that data has not been tampered with or changed. This requires methods that can distinguish between the original content of a file and any changed versions of the file. The subconcepts of this topic are particular strategies to achieve this goal. For instance, 'quantum communication' uses photons that change their value when they are measured. Then, 'checksums and cyclic redundancy checks' calculate a number from the binary representation of a file. They only protect against hardware or communication failures but not against malicious modification. Also, 'tamper-evident logging' make it impossible to change the logs. If logs can be guaranteed not to be modified, it is easy to check these logs manually or with automatic scripts. Such an approach is described by Crosby and Wallach [3]. The final subconcept is 'hash-based integrity verification'. Such verification uses a mathematical function to calculate an almost unique number for any possible file. From the number (called hash value) it is impossible to learn about the content of the file. If the content changes, the hash value changes as well.

Cryptography is concerned with making messages unreadable for anyone except the intended recipient. It is a very large subfield of cybersecurity. The concepts regarding cryptography are 'quantum cryptography', 'ciphers', 'public-key cryptography', and 'hash functions'. 'Quantum cryptography' uses the same techniques with photons as the 'quantum communication' above. 'Ciphers' are encryption methods that make a text unreadable for anyone who does not know the password. 'Hash functions' are the concept used above for the integrity verification. As stated then, they are mathematical functions, for which it is very hard to find the input, given an output. Moreover, it is almost impossible to find a different input that yields the same result as a given input. Finally, 'public-key cryptography' is concerned with encrypting messages for someone without having a password. It uses asymmetric encryption that allows anyone to encrypt a message for the recipient with the public key, but only the recipient with the private key can decrypt it. Paar and Pelzl [14] have published a book that covers most of these topics. The subconcepts point to more specialized resources that are helpful for readers that want to know more details.

Intrusion detection and risk mitigation concerns all forms of cyber-attack, how to detect or prevent them, and how to mitigate their effects. It outlines the possible attacks and methods of intrusion. It points to resources about how to defend against such attacks. The subconcepts are 'malware', 'denial of service', and 'intrusion detection'. 'Malware' is concerned with the different kinds of malicious software and their way of intruding the system. For instance, a trojan creates a hidden path for information, while spyware is specifically collecting personal information. 'Denial of service' is overloading a server with requests, to make it inaccessible for other people. Lately, distributed denial of service attacks have become popular, using botnets of thousands of infected computers to overload a server with requests. Such approaches can undermine the usefulness of any open government initiative. 'Intrusion detection' is the task of monitoring the activity on a computer system in

[1]The taxonomy URL is `http://www.cs.cmu.edu/~dklaper/cybersecurity/website/`.

order to identify malicious activity. This is an area that is fairly well studied and there are taxonomies of cyber-attacks such as the malware taxonomy by Chapman et al. [2].

Authentication and authorization is relevant for recognizing who is trying to access the system and what that person is allowed to do. In the 'authentication' concept, different methods of establishing someone's identity are discussed. Authentication can be performed with a piece of knowledge, such as a password. Another way is to use a specific object, such as a smart card, to authenticate. Finally, an increasingly popular way is to use something related to the person's body, such as a biometric signal, for example a fingerprint or an iris scan. In contrast, 'authorization' is the task of deciding what an identified user is allowed to do. For example, in a bank a customer can see his or her account but he or she cannot transfer money from someone else's account, while a teller can do that (upon order by a client). This is so-called role-based access control. There are also more advanced techniques based on the same principle, such as provenance-based access control, which takes into account the reputation of a user [15]. Finally, there is the concept of 'message authentication'. The task is to make sure that the message is sent by whom he or she claims to be and that the message has not been modified. This partly overlaps with 'data integrity verification' in the sense that the integrity of the message must be verified, but additionally, the sender must also be authenticated through the message.

Auto-analysis of legitimate usage patterns aims at recognizing automatically when someone tries to remove, change or copy data for malicious reasons. In particular, this concerns insiders that have legal access to the data. Insider attacks are a growing problem and the subconcepts present methods for prevention, detection, and mitigation of insider attacks. Insiders have leverage, because of the knowledge they possess that might allow them to circumvent security procedures. An overview of research in this area is given by Salem et al. [17].

Finally, **Computer Forensics** is the science of reconstructing the traces of an intruder. The goal is to secure digital evidence that allows understanding what has happened in a cybercrime. This should also help to avoid the same mistakes in the future. Currently, we have no subconcepts yet, although it is clear that examining the remains of a defective hard disk requires quite different skills from tracing malicious network data. The *Computer Emergency Readiness Team* (CERT) report [20] gives a short overview of Computer Forensics, explains its importance, and provides useful pointers for more in depth information.

In conclusion, there is a broad range of technical topics in cybersecurity and virtually all of them can be relevant for open government data providers or even users. Our taxonomy is an attempt to organize the different topics in an application-oriented way. It is intended to be a central source of educational material about cybersecurity. The six main concepts of this technical part of the taxonomy are 'data integrity verification', 'cryptography', 'intrusion detection and risk mitigation', 'authentication and authorization', 'auto-analysis of legitimate usage patterns', and 'computer forensics'. While this part of the taxonomy is concerned with the technical aspects of cybersecurity, the next section focuses on impacts of cybercrime and cybersecurity in social and other areas.

2.3 Impacts of Cybercrime and Cybersecurity

A rather different side of cybersecurity is the impact that digital crimes have on other areas. In particular, governments create cybersecurity laws and policies, political activists use cyber threats, and businesses need to spend money on cyber defense software. Therefore, we recently started looking into the economic and policy impacts of cybersecurity. This is particularly important for open government initiatives, since the necessary costs and the right strategy to address the dangers are policy decisions that need to be made by the leaders.

This part of the taxonomy is still in development and does not yet have a deeper structure. The main concepts of this part are 'history', 'social activism', 'policy and law', 'education', 'economic impact', and 'awareness efforts: initiatives and tools'. These all highlight different issues. 'History' might seem to be a bit of an outlier at first, but in fact it helps understanding the basic motives behind cybercrime and how they evolved. Therefore, it is also related to the economic impact of cybersecurity.

The **history** of cybersecurity and cybercrime is not documented in a comprehensive way. There are different starting points but one of the first *modern* cyber-attacks was the creation of whistles to make free phone calls. The phone systems during the 1970s operated with acoustic control signals and so-called "phone phreaks" built devices to fake those signals. This was the first kind of cyber fraud. In the 1980s banks become targets of cybercrime by insiders and the first self-replicating programs ("worms") appear. In the second half of the 1990s the emergence of the internet leads to an exponential increase in cybercrime. Military services become targets of attacks and viruses literally "go viral". New types of malware appear, such as trojan horses that allow remote access. Also, tools start to be published that simplify the intrusion process and allow people without much knowledge to attack others. At the turn of the millennium, the first denial of service attacks against large websites are performed. In the middle of the 2000s the attacks become very diverse, ranging from keylogging passwords for identity theft to industrial and military espionage. The second half of the 2000s is shaped by the emergence of script injection and cross-site scripting to inject malicious content into legitimate websites. Furthermore, distributed denial of service attacks by huge botnets make large web services inaccessible. Finally, the 2010s started off with the emergence of the anonymization software Tor and the infamous "Silk Road" platform that offered all kinds of criminal services. This platform was recently shut down. Moreover, cyber-attacks became more popular as a mean of political propaganda. The Wavefront Consulting Group [21] provides a detailed selection of important cybersecurity events until 2008. The two most important trends in the recent past are the professionalization and the diverse motives (money, intellectual property, or political statement) of cybercrime.

Social activism is most often the reason for defacement attacks. In a defacement attack a website's content is replaced by a usually defamatory message of the hackers, which states

their point of view. Another tactic used by so-called *Hacktivists* is the dissemination of confidential information. Two cybercrime groups that claim to support their political cause through their cyber actions are Anonymous and the *Syrian Electric Army* (SEA). The SEA uses defacement tactics to spread their message to support the Syrian president Assad in his war against the rebels. They also break into social media accounts of major news organizations to promote their message. On the other hand, Anonymous is a loose movement with fewer common goals. They were in the news for several major distributed denial of service attacks and for obtaining and publishing confidential data. Their political goals are incoherent but often have anti-government tendencies. Held [8] explores the motives behind Anonymous and their dissemination of confidential data.

Policy and law is concerned with the political strategies and specific laws about cybersecurity. In the beginning of the digital era it was not clear how to apply the current law to cybercrime. With the advent of the internet the issues became even more complicated. In the internet national boundaries largely disappear and accountability is difficult to establish. On the 'policy' site, the United States are one of the few countries with an explicit, comprehensive cybersecurity policy. Luiijf et al. [9] compare different national cybersecurity strategies including the U.S. cybersecurity strategy. Since then, the focus on cybersecurity has been even more emphasized by the Obama administration, as shown for example, by the presidential policy directive [13] detailing the structure to secure critical infrastructure. A clearly articulated and well executed cybersecurity policy can help making an open government initiative stable, secure, and trustworthy. On the 'law' side, over the years numerous laws about cybersecurity have been established. Fisher [5] has compiled an overview of American cybersecurity laws for the members of congress. The main question regarding laws are whether they cover the emerging forms of cybercrime well enough to be applied in a sensible fashion and whether the laws allow balanced judgments by the judicial authorities. Without a cybersecurity policy and appropriate laws an open government initiative may lack the legal means to protect its data.

Education is about courses, curricula, and degrees for cybersecurity professionals, as well as the education of users in the general workforce to help them stay safe on the internet. One of the biggest initiatives in this regard is the *National Initiative for Cybersecurity Education* (NICE), which aims at improving the cyber behavior of all segments of the population[2]. It offers resources with cybersecurity tips for users, as well as a framework for classifying the different jobs concerned with cybersecurity. Another resource that guides cybersecurity education is the requirement catalogue for becoming a center of academic excellence[3]. These guidelines however are fairly broad and it is not very constrained in what order the subjects should be taught. The *Association for Computing Machinery* (ACM) is trying to explore what needs to be included in a cybersecurity curriculum and how to teach it [10]. In brief, cybersecurity education is still in its child shoes, partly because it is a fragmented field. Maybe this taxonomy can be a small help towards a more holistic view of cybersecurity.

The **economic impact** of cybersecurity is huge considering the amount of money involved. There are two sides of this impact. On the one hand, cybercriminals earn a lot of money with selling identities and cybercrime services on hidden online marketplaces. On the other hand, businesses spend large amounts of money for getting professional protection from the aforementioned cybercriminals. Although black markets are an old concept, they have been reloaded in the digital world. Goncharov [6] has examined the Russian underground market and shows the kind of services that are up for sale in some parts of the web. Additionally, he examines the prices to acquire cyber-attacks. For businesses, the question is how much money can they afford to spend for information security and what are the most efficient ways to secure their information. For more than a decade the *Workshop on the Economics of Information Security* (WEIS)[4] discusses this topic each year. The costs of a security breach can be huge, nevertheless it is impossible to completely eliminate that risk even with an infinite amount of money. Additionally, businesses are under pressure to yield gains, thus, the available money for cybersecurity, which does not produce any direct returns, is limited. The central question from a business perspective is how to estimate the necessary budget to keep their information reasonably safe.

Awareness efforts: initiatives and tools summarizes specific efforts for raising cybersecurity awareness among the population and tools that help users understand the cybersecurity risk, as well as improve cybersecurity infrastructure. The efforts are partitioned into three subconcepts based on their origin, government, commercial, or research. The United States government initiatives are the *Comprehensive National Cybersecurity Initiative* (CNCI)[5], which aims at improving cybersecurity on all levels, including cybersecurity education, and the Department of Homeland Security's *National Cybersecurity Communications Integration Center* (NCCIC)[6], which focuses on communicating with federal agencies, as well as other companies involved with critical infrastructure to ensure their cybersecurity. The commercial applications are websites that help users decide whether a given website is safe. In particular, these are Web of Trust (`http://www.mywot.com`), McAfee SiteAdvisor (`http://www.siteadvisor.com`) and Norton Safe Web (`http://safeweb.norton.com`). Finally, our cybersecurity portal called Personal Cybersecurity Assistant is a research tool improving cybersecurity awareness. This portal is explained in the next section.

To conclude, there is a wide spectrum of non-technical issues in cybersecurity. These are also important for open governments and can help making informed decisions about

[2] `http://csrc.nist.gov/nice/` last checked April 29, 2014.

[3] `http://www.nsa.gov/academia/nat_cae_cyber_ops/nat_cae_co_requirements.shtml` last checked April 29, 2014.

[4] `http://weis2014.econinfosec.org/` last checked April 29, 2014.

[5] `http://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative` last checked April 29, 2014.

[6] `http://www.dhs.gov/about-national-cybersecurity-communications-integration-center` last checked April 29, 2014.

cybersecurity. The main concepts in this part of the taxonomy are 'history', 'social activism', 'policy and law', 'education', 'economic impact', and 'awareness efforts: initiatives and tools'. These show an overview over the efforts, effects and decisions related to cybersecurity and cybercrime. The remainder of the paper is concerned with the second part of our research and future work. We are building a cybersecurity portal that may serve as a discussion platform and information source.

3. PERSONAL CYBERSECURITY ASSISTANT PORTAL

The *Personal Cybersecurity Assistant* (PCA) portal was originally developed by Sharifi et al. [18] as a website note-storing service called SmartNotes. We enhance the portal to provide better discussion options. Furthermore, we implemented automated links to relevant taxonomy entries based on the content of the discussion. The system consists of a browser plugin and a website that stores and provides the data on the corresponding website[7].

The browser plugin has multiple functionalities. First, it allows the user to write a comment or question about the website he or she is currently browsing, or block that website from being accessed again. Second, it displays previously saved notes, and blocks access to sites that have been previously blocked by the user. Third, it shows notifications: when notes by other people are available on the current website, or if someone has replied to one of the user's notes, the user will be informed by the plugin.

The website hosts the browser plugin download. In addition, it hosts user discussions. The main part of the website is accessible directly from the plugin. The discussions are conveniently structured, which means if you are accessing the website from the plugin it is possible to reply to any post by clicking a button next to it. It is also worth mentioning that notes by default apply to all pages of a website. When writing a note the user can choose to make the note apply to the entire site or only to the specific page the user is visiting. When searching discussions for a specific page, the notes that apply to the whole website are also displayed, but with a different background color.

3.1 Browser Plugin

The heart of the PCA is the browser plugin, which manages the login and lets the user write a note about the website he or she is viewing at any time. The user can also give the website a rating. Furthermore, the system notifies the users of relevant notes and replies by other people to his or her notes. From the plugin, the user can reach an overview of his or her notes. Also, the user can visit the website without logging in again, and additionally can set the action when visiting the website again. Either the note written about the website can be displayed, or the website can be blocked, i.e., hidden by a warning banner with the information that the user has chosen earlier not to visit this site. In addition, the user can share the note with an email address. Of course, the user can also delete notes. The interface of the browser plugin is shown in figure 1.

[7]The Personal Cybersecurity Assistant URL is `http://erie.lti.cs.cmu.edu`).

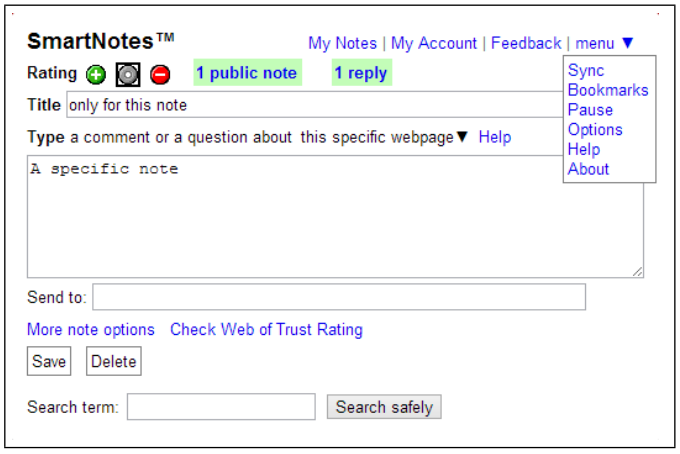

Figure 1: Screenshot of the browser plugin

Besides writing notes, the plugin offers the capability to view notifications about other notes concerning the current website, checking the rating of a website on a commercial site, and using a google safe search that is constrained to results by Wikipedia and big antivirus software manufacturers. The search is meant to allow quick lookup of information about cybersecurity on trustworthy websites. While this constrains the search space massively, it also makes sure that the user does not directly go to a dangerous website.

There are two types of users, registered users and anonymous users. Anonymous users have downloaded the plugin but never registered an account, i.e., they do not have a password. Registered users have multiple advantages. First, they can recover their notes on other computers with the browser plugin. Second, they have additional features. For instance, they can share their notes via e-mail and they can use the safe search mentioned above. Moreover, registered users have a username instead of just a number. When a user logs in the plugin automatically switches to the extended layout.

The plugin is constantly running in the background while the user is surfing. If the user does not want the plugin to display notes or send the website addresses visited to the PCA server, he or she can pause the plugin. The plugin can be configured to ask the user after 10 minutes whether it should reactivate. During deactivation, no user notes are displayed and the user will also not be blocked from visiting websites he or she has chosen to block. While this could be a risk, it is a technical necessity, since the plugin does not send any information to the server in paused mode.

In short, the plugin offers a variety of functionality, especially for registered users. The main functionality of the plugin is to enable writing notes, as well as displaying saved notes and blocking the user from revisiting websites again that were blocked. In addition, it provides a safe search field, notifications relevant to the user, and serves as the entrance to the website where users can engage in discussions and reply to notes as described in the next section.

3.2 Website

The website hosts the discussions and has the interfaces for managing the notes, as well as reading replies or even reading discussions about other websites. It has a help section for the plugin and hosts the plugin package. Furthermore, a user that is logged in can directly reply to any note there and provide a rating of the website in his or her reply. Also, the website links the notes to educational material to facilitate improvement of user knowledge.

The use of the website has some constraints. One important point is that the website should be accessed through the plugin. Otherwise the user may not be recognized and would not be able to respond to any discussions. Furthermore, the website can only be used for replying to an existing note and not to create a new discussion. The idea is that people are more encouraged to participate in a discussion and not just create new single notes.

The discussions on the website link to appropriate taxonomy entries. If a website has one or more discussions, there is a box containing links to related educational content. This should encourage learning about the background of the discussed matter. Currently, it links to entries in the taxonomy, but it is possible to add content from other sources. It is implemented as a web service that runs silently and performs the mapping from PCA discussions to educational resources. This feature aims at connecting the concrete use of the platform with educational background material to support cybersecurity education for the users of the platform. The platform could also be used by governments and other organizations as an internal tool. Then it could link to internal training materials or glossaries in addition to the taxonomy.

As a summary, the Personal Cybersecurity Assistant platform consists of a browser plugin for Chrome to store notes about websites and an associated website that hosts the discussions and allows replying to notes. Furthermore, users are notified of replies to their notes, as well as of notes by other people about the website they are currently viewing. Users have the possibility to search on google with returning results about cybersecurity from only a very small set of manually selected, trustworthy websites. Furthermore, when browsing websites with existing discussions, these are enriched by links to relevant educational material from the taxonomy. This encourages users to learn about cybersecurity. The PCA can provide guidance about specific websites, while helping users to understand cybersecurity methods and risks on the internet.

4. FUTURE WORK

The taxonomy and the portal are work in progress. Here we outline the potential future work. One important point is expanding the taxonomy concepts in more depth. In particular, the impact of cybersecurity portion of the taxonomy needs more depth. Moreover, the taxonomy resources need to be expanded with resources for less advanced users who cannot understand cybersecurity research papers, such as informational videos, presentations, and lay articles. Automatic techniques for content harvesting and classification could aid this extension.

Another goal is to build a more versatile platform that can be used for websites, as well as other digital objects. The platform should be accessible to users of all knowledge levels and provide trustworthy information. For instance, users could have a reputation and trustworthiness level. The platform should also allow incorporation of other cybersecurity services, for instance, email classification into the various kinds of malware, spam, etc. Moreover, it should be suited for use in organizations as an internal tool. One idea is to evolve the PCA platform to this platform. In any case, the experiences with the PCA will be helpful for designing this broader cybersecurity platform.

Finally, the platform should integrate educational information tighter. For this new algorithms should be devised that are capable of linking discussions robustly to relevant educational material and vice versa. A good matching algorithm could provide users with exactly the background that they need for understanding the technical discussion.

In brief, the taxonomy needs to be expanded to provide greater depth and resources for less advanced readers. Additionally, the scope of the Personal Cybersecurity Assistant platform needs to be expanded to be useful for more than just websites. Last, there should be a tight and concise coupling between educational material and concrete discussions about cybersecurity.

5. CONCLUSIONS

Cybersecurity is a central issue for open government initiatives. Only if politicians, officials, and users understand the dangers of the internet, can open government data be reasonably protected from malicious activity. In this paper, we present two resources to help people increase their knowledge about cybersecurity and discuss the security aspects of specific websites. The taxonomy serves as a collection and organization of existing knowledge about cybersecurity. It contains a technical view, as well as background information about the impact of cybercrime and cybersecurity. The Personal Cybersecurity Assistant consists of a browser plugin and a website. It offers the possibility to discuss the security of websites. Furthermore, it points to relevant educational resources based on the discussions of a specific website. Together, these resources form a more coherent and complete picture of cybersecurity.

6. ACKNOWLEDGMENTS

We'd like to thank Mehrbod Sharifi and Eugene Fink for letting us use their code for SmartNotes to create the PCA. In addition we'd like to thank Dr. Joe Kielman and Dr. Virgil Gligor for their suggestions regarding the taxonomy. Finally, we'd like to thank Navneet Rao for helping to collect resources for the taxonomies.

7. REFERENCES

[1] J. J. Cebula and L. R. Young. a taxonomy of operational cyber security risks. Technical report, Software Engineering Institute, CMU, 2010.

[2] I. M. Chapman, S. P. Leblanc, and A. Partington. Taxonomy of cyber attacks and simulation of their effects. In *Proceedings Military Modeling & Simulation MMS*, 2011.

[3] S. A. Crosby and D. S. Wallach. Efficient data structures for tamper-evident logging. In *Proceedings USENIX Security Symposium*, 2009.

[4] Department of the Treasury. Treasury department report to the President on cybersecurity incentives. `http://www.treasury.gov/press-center/Documents/Supporting%20Analysis%20Treasury%20Report%20to%20the%20President%20on%20Cybersecurity%20Incentives_FINAL.pdf` (last checked April 29, 2014), 2013.

[5] E. A. Fisher. Federal laws relating to cybersecurity: Overview and discussion of proposed revisions. `https://www.fas.org/sgp/crs/natsec/R42114.pdf` (last checked April 29, 2014), 2013. Congressional Research Service.

[6] M. Goncharov. Russian underground 101. Research Paper, 2012. Trend Micro Incorporated.

[7] Government Accountability Office. Cybersecurity: National strategy, roles, and responsibilities need to be better defined and more effectively implemented. `http://www.gao.gov/products/GAO-13-187` (last checked April 29, 2014), 2013.

[8] W. V. Held. Hacktivism: An analysis of the motive to disseminate confidential information. Master's thesis, Texas State University - San Marcos, 2012.

[9] H. A. M. Luiijf, K. Besseling, M. Spoelstra, and P. de Graaf. Ten national cyber security strategies: A comparison. In *Proceedings CRITIS*, 2011.

[10] A. McGettrick. Toward curricular guidelines for cybersecurity. `http://www.acm.org/education/TowardCurricularGuidelinesCybersec.pdf` (last checked April 29, 2014), 2013.

[11] Microsoft. Cybersecurity for open government: Security planning in the era of transparency. White Paper, 2010.

[12] National Institute of Standards and Technology. Framework for improving critical infrastructure cybersecurity. `http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf` (last checked April 29, 2014), 2014.

[13] B. Obama. Presidential policy directive – critical infrastructure security and resilience. `http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil` (last checked April 29, 2014), 2013.

[14] C. Paar and J. Pelzl. *Understanding Cryptography: A Textbook for Students and Practitioners*. Springer, 2010.

[15] J. Park, D. Nguyen, and R. Sandhu. A provenance-based access control model. In *Proceedings IEEE Privacy, Security and Trust (PST)*, 2012.

[16] President's Council of Advisors on Science and Technology. Report to the President: Immediate opportunities for strengthening the nation's cybersecurity. `http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_cybersecurity_nov-2013.pdf` (last checked April 29, 2014), 2013.

[17] M. B. Salem, S. Hershkop, and S. J. Stolfo. *Insider Attack and Cyber Security: Beyond the Hacker*, chapter A Survey of Insider Attack Detection Research, pages 69–90. Springer, 2008.

[18] M. Sharifi, E. Fink, and J. G. Carbonell. SmartNotes: Application of crowdsourcing to the detection of web threats. In *Proceedings Systems, Man, and Cybernetics (SMC)*, pages 1346–1350. IEEE, 2011.

[19] R. Tehan. Cybersecurity: Authoritative reports and resources, by topic. `http://www.fas.org/sgp/crs/misc/R42507.pdf` (last checked April 29, 2014), 2014. Congressional Research Service.

[20] US Computer Emergency Readiness Team (US-CERT). Computer forensics. `http://www.us-cert.gov/sites/default/files/publications/forensics.pdf` (last checked April 29, 2014), 2008.

[21] Wavefront Consulting Group. A brief history of cybercrime. `http://www.wavefrontcg.com/A_Brief_History_of_Cybercrime.html` (last checked April 29, 2014), 2008.