Justin Leonard

CSF 430

Report

Cybersecurity as Realpolitik

Cybersecurity is one of the most important fields in today's technological world. The safety and security of all systems, networks, and data for both individual users and large organizations is imperative. In 2014, Dr. Dan Geer made a keynote speech entitled "Cybersecurity as Realpolitik" at the Black Hat conference. This speech covered a variety of topics relating to cybersecurity and how it is important and ever changing today. My overall thoughts on this speech are very positive. I thought it was an informative, comprehensive, and humble look on cybersecurity. There is a lot of talk of the importance of acknowledging that you are wrong in order to properly address the problems in security, as well as taking the issue of security seriously. Though there is a lot of grey area related to any individual's proposed security concepts or solutions, I did find a lot of what he said to be compelling and informative. Dr. Geer goes through his own proposals, concepts, and thoughts about security throughout his speech to address problems that we have to face. He begins talking about how specialization in specific areas of security is very important because of how admittedly impossible it has become to know all information and everything that is going on in all aspects of security. This shows just how expansive security has become and how it is no longer attached to an individual. It's not about knowing everything or controlling power, but about trying your absolute best to create as many secure policies as possible as security becomes integrated into all aspects of our lives. Another general point he gets into is security as it relates to governments and the balance between freedom and safety as policy for nations gets more vital and powerful to protect the interests of both executives and citizens alike.

There were numerous proposals that Dr. Geer went over in his speech. These include mandatory reporting, net neutrality, source code and liability, strike back, resilience, vulnerability finding, right to be forgotten, internet voting, abandonment, and convergence. I thought that the proposals were predominantly varied, in depth, and well researched. I believe that the proposals mentioned here provide some viable solutions to a lot of high priority and important security problems that still exist today. There were some solutions that were either not developed enough or did not solve the problem effectively, but for the most part I believe there were a myriad of good points made in this speech. I will be going over two proposals Dr. Geer mentioned that I agree with, which will be mandatory reporting and source code and liability, and one that I disagree with which is abandonment.

To begin, I agree with Dr. Geer's proposal on mandatory reporting. As stated in the speech, there are other fields where mandatory reporting is already set in place. An example would be the medical field with reporting the spread of viruses. This is especially important today with the coronavirus pandemic. There are already some implemented reporting requirements for certain events such a data breaches in most states, but they are not as comprehensive nor followed correctly at times. It was found that nearly 70% - 80% of data breaches at this time were reported by third parties unrelated to the event, not by the victims. Reporting these events is crucial to finding the source and stopping attacks, detecting vulnerabilities, fixing exploits, and gaining as much data as possible from the nature of these attacks to prevent them in the future. There is so much information that needs to be documented from an attempted or successful attack. This can include the nature of the fault, the vulnerabilities exploited, damages done and scope of the attack. The data that can be found from the severe cybersecurity failures and attacks should be mandatory to be reported. There needs to be laws implemented for failure to report these events. Companies and some individuals should have an ethical and legal responsibility to report these security events. I agree that there should, to some extent, exist a system used to document and enforce the mandatory reporting of these cyber events. I believe this would be best implemented in the industry by having a global standard for mandatory reporting, a location for individuals to document the security events, and laws and policies in place to enforce this. The standard would be used to determine what kinds of events need to be reported, and the method in which to categorize these events. Using Dr. Geer's statement, there should be a severity threshold defined that determines if a security event should be reported. If the cybersecurity failure is above this threshold, then it should be mandatory to be reported. If the cybersecurity failure is below the threshold, then it can be voluntarily reported at the victim's discretion. The definition of this threshold will be negotiated and could be a combination of the type of failure or attack, the severity of the damages, etc. The method to categorize these events in the standard would be based on characteristics of the failure such as type of failure, nature of attack, victim name, attacker name if determined, date and time occurred, severity of failure, and detailed data related to the exact events that happened. The location for individuals to document the security events could be a centralized database that will use the rules set by the standard mentioned above to document and categorize reported security events. The laws and policies will be put in place by governments to ensure that this new standard for mandatory reporting of cybersecurity failures is enforced.

Furthermore, I agree with Dr. Geer's proposal on source code and liability. When companies and individuals acquire and use a software product, there is some implicit trust that the code for the application was made by professionals and is secure. The problem comes when the software fails and causes damages to the user. At the time, software products are not covered by product liability unlike other products. The liability is on the user of the software if damages should occur, not the creator. The mentality is that users should protect themselves and any failure that should happen is on the fault of the user. I agree with Dr. Geer that this is a very bad mentality to have. Companies should be held accountable for having unsecure or poorly written source code that could potentially cause security and product damage to users. Companies need to make quality products that are backed with liability to ensure the security of their customers. This liability should account for poorly written source code, bad documentation, and insufficient testing of the product. I believe this would be best implemented in the industry by having more updated standards set in place to write, document, and test secure source code, to introduce laws and policies for inspecting potentially unsecure source code, and for software distributors to be held liable for damages caused by faulty software products. Having standards in place to ensure all software distributors create secure source code to begin with will help stop these security faults from happening in the first place. Having legislation in place to hold companies liable for damages that their software product create will both act as motivation for other companies to create more secure products and ensure that user's will be covered if a fault occurs.

Finally, I disagree with Dr. Geer's proposal on abandonment. Software creators are constantly upgrading and creating new products that have more optimized and secure features. As time goes on, there will be an eventual decline in support and security updates to these older products. Eventually, they will be completely abandoned as support for the most current products will be the highest priority. As technology and hardware advances, the software must be upgraded as well. This is seen to happen with numerous products across many different categories. A good example would be Microsoft stopping support and security updates for their past operating systems. Windows XP and Windows 7 have already lost support. Now with the release of Windows 11, Microsoft has stated that they will stop support for Windows 10 in five years time. I disagree with the proposal Dr. Geer made in his speech that states if a company abandons a codebase or software product, that it must be made open source. I do not believe that companies should be forced to release the source code for their product just because they stop supporting it. In my opinion, it is natural and justified that older products will eventually lose support. It makes no sense to continue wasting time and resources supporting a product that is decades old and only a small amount of people use. Never-ending support should not be forced, nor the release of the product to the public. Technology and security are changing so rapidly that newer software products should be preferred by users to stay up to date and protected. Voluntarily using very old and outdated products is a vulnerability itself. It would not work to force companies to release their products to the public because this could unveil even more security vulnerabilities to threat actors as well as private company assets. Abandonment of products could still be a problem, especially if it is done at a rapid pace. It could have damaging consequences to the security and data of users. If you acquire a software product, you expect it to be supported within a reasonable timeframe. I think a solution to this would be instead of making the product open source to try to reverse the affects of abandonment, it is better to mitigate the consequences of abandonment. This can be done by creating policies for companies to follow if they create a product and want to stop support. There should be a minimum amount of time that a product should be supported for, so user's have the peace of mind that the product they are purchasing has some enforced long term support for the time being. There should also be a predefined amount of time after a company states that they will stop support for a product in which the product will still be supported so the users have ample time to migrate to a more secure and supported product. There should be some exceptions for if a company goes bankrupt or can no longer immediately support a product for extreme reasons. These cases should be taken and examined individually in order to find the most secure and reasonable solution.