THE GEORGE WASHINGTON UNIVERSITY
CYBER SECURITY POLICY
AND RESEARCH INSTITUTE
Thoughtful Analysis of Cyber Security Issues

Cyber Security: The Mess We're In
And Why It's Going to Get Worse

Julie J.C.H. Ryan, D.Sc.
The George Washington University

Report GW-CSPRI-2011-4

April 11, 2011

Abstract

We've dug ourselves into a hole with the decisions we have made in the last 30 years in Cybersecurity. Now we are faced with a system that is not only highly complex and tightly coupled but also riddled with holes and critically dependent on knowledge. The landscape of attacks and vulnerabilities has continued to evolve as well, making the existing situation extremely dicey. And it's only going to get worse unless we make radical changes in the way we approach the problem space.

Work supported by the Office of the Vice President for Academic Affairs and the School of Engineering and Applied Science of The George Washington University

The Mess We're In
And Why It's Going to Get Worse

Julie J.C.H. Ryan, D.Sc.
The George Washington University

Introduction

We, collectively, have dug ourselves into a hole with the decisions we have made in the last 30 years in Cybersecurity. Systematically, humans have adopted information technology at a dizzying pace, paying essentially no attention at all to security in the process. Despite the repeated efforts of scientists, policy makers, and engineers to both draw attention to the problem and to provide solutions, the market forces of adoption have overwhelmed the development processes. Time to market has been the driving force in innovation, rather than a measured and systematic development of well-engineered technologies.

Now we are faced with a system that is not only highly complex and tightly coupled but also riddled with holes and critically dependent on knowledge. The lack of systematic engineering to reduce the impact of exploited vulnerabilities is but one problem. An additional complicating factor is that so many so-called security engineers have little appreciation for either understanding or calculating the systemic effects of security choices in architectures. A disturbing number of certified security experts are woefully ignorant on many important issues in computer security. These symptoms of a kludged system in general have led to a reality where large corporations have to retrain newly hired computer scientists on how to develop relatively bug-free software, users of products routinely are forced to accept licenses that declaim any performance issues, and where information security officers play the functional equivalent of "whack-a-mole" with enterprise systems in order to thwart the bad guys.

To make things worse, the landscape of attacks and vulnerabilities has continued to evolve as well, making the existing situation extremely dicey. This is to be expected, since attackers have nothing but motivation to get better at their craft. But meanwhile, the products that continue to flood the market continue to have significant vulnerabilities that are just waiting to be discovered by the attackers. Even more disturbingly, the users of information technology seem to have thrown up their collective hands in the functional equivalent of "it's not my job." The result is a situation where attacks are effective, mistakes are prevalent, and critical processes are at extreme risk. (Really, it's fairly amazing that this whole kludged system works at all, much less as well as it does.) And it's only going to get worse unless we make radical changes in the way we approach the problem space.

The State of Affairs: A Brief Summary

Forty-one years after the publication of the landmark Defense Science Board report on Security Controls for Computer Systems (Ware 1970), we find ourselves in a computer ecosystem that is proliferated, entrenched, and poorly engineered. On top of this, attackers are moving beyond crude blast-type weapons and developing more sophisticated attacks. In fact, what could be referred to as 'Precision Weapons' are emerging. The use of the nomenclature 'precision weapons' is not without controversy (what is?), but the weapons being seen in the attack space are much more precise than the launch-and-see-where-it-goes weapons of only a few years back. Stuxnet, for example, seems to have been aimed very deliberately at a specific set of SCADA systems used by the Iranians in their nuclear program, limiting damage in other locales (Matrosov et al 2011). Targeted Malicious Email (TME), also known more colloquially as spear-phishing, is an extremely sophisticated combination of social engineering and targeted attack (Amin 2011). Software is not the only vector being exploited: supply chains are at risk as more evidence of counterfeit hardware is discovered (ICE 2010, Hsu 2010), leading some to wonder what modifications (if any) have been made to hardware elements manufactured in unsupervised facilities.

To complicate things, cybersecurity is increasingly seen as an elite task, the purview of those with specialized training, rather than everyone's job. This leads to systemic weaknesses in enterprises which then are easily exploitable. This also leads to systems being built with little or no consideration for security engineering. Unfortunately, security is and always has been a pay now or pay later proposition and it seems like the pay later option is now coming home to roost. Besides the costs associated with patching the gaping holes in systems that leave enterprises vulnerable, a non-trivial expense, it is with some relief to the security community that the lawyers have (finally) arrived, both in the international policy arena and in the product liability arena (CCDCOE 2009, 2010; Meyer 2008).

There is a common element to this challenging set of circumstances. That is the element of knowledge. Knowledge is gained and used by attackers in order to develop and execute their actions. Knowledge is increasingly accessed in complex ways for good purposes, where "good" can be operationally defined as including such various legitimate purposes as developing market awareness, advertising, law enforcement, and intellectual property protection. The knowledge needed to safely and securely use information technology is ignored by vast numbers of users, some because they do not have the fundamental skills needed to use such knowledge, others because they are overwhelmed by the complexity of the situation. Finally, the knowledge of how to secure systems is implemented in isolated and sometimes stupid ways by 'security professionals.'

So we have in a very real sense a knowledge war underway, which is currently being lost by the good guys. An anecdote to describe how bad the situation is: at a conference of security professionals, an executive from a security services company was asked to define his top priorities. He said, "Cryptography, Education, and Security." This is illustrative, in that most true security professionals consider cryptography to be an enabling technology for security, not something entirely separate. Unfortunately, this situation is not unique. The growth of the security certification market has led to an increase in those that are considered to be qualified to perform security services for the enterprise. Without naming names, it has been my distinctly unpleasant experience to discover, through classroom interactions, a disturbingly large number of students holding those certifications who do not understand some extremely fundamental concepts in cybersecurity. And yet these are the individuals we as a society trust to have the requisite knowledge needed to ensure a modicum of security in our systems.

What is All This Stuff?

It's complicated. Really, it is. Here is a brief review of all the material mentioned in the brief summary above for those readers who are not already intimately familiar with the referenced elements.

Stuxnet. First of all, it's a "worm." A worm is a category of malicious software (malware) that is self-replicating and mobile. In other words, it is capable of both reproducing itself and spreading the infection to other platforms. Next, researchers who have studied it carefully say that it appears to be specifically designed to go after software manufactured by Siemen's Corporation for use in their industrial control systems, specifically the supervisory control and data acquisition (SCADA) systems. The worm takes advantage of poor practices, as might be expected. After all, if someone leaves the front door open, why should a burglar bother to break in a window? In particular, the worm looked for default passwords in SCADA systems, used USB flashdrives to spread itself, and exploited some Microsoft Windows vulnerabilities. Researchers estimated that the development of this worm must have required a sophisticated team of developers working several years with access to very specific testing environments. Many excellent analyses of the Stuxnet worm have been published. Two that are recommended to those who would like to research further are Matrosov et al 2011 and Schneirer 2010.

Targeted Malicious Email (TME). Also known as spear-phishing, TME targets high value people specifically and believably in order to get the targets to take some sort of action, typically opening an infected attachment to an email. TME hijacks trusted relationships in order to effectively achieve the objectives of the attack. It is both very high impact and very difficult to detect, simply because of the nature of the attack. To illustrate the problem, consider the reaction of a senior executive for product development for a major software company when she receives an email from the head of marketing for that same organization. Looking at the "From" line, the first reaction is that the email is legitimate. Now consider if the email "Subject" line contains the title of an on-going discussion between the two parties. This further emphasizes the legitimacy of the email. That is what TME looks like: a fully legitimate email that matches the current operational patterns extremely well. Then when the recipient opens the attachment to the email, surreptitiously added malware is executed on the targeted system. The purposes for TME can vary, but typical motivations are data exfiltration (stealing information) and sometimes data infiltration (opening backdoors into the greater network). In other words, espionage tends to be a prime motivation for TME.

Counterfeit Hardware. In the last five years, an increasing number of cases of counterfeit hardware have been discovered. One of the biggest cases was that of Cisco routers and network cards, which had been manufactured in China and provided to customers such as "U.S. Marine Corps, U.S. Air Force, FBI, BOP, Federal Aviation Administration, Department of Energy, as well as defense contractors, universities, school districts and financial institutions." (ICE 2010) What actual activities were going on in those systems, besides the legitimate activities, is anyone's guess: it is notoriously hard to detect activities that are surreptitious. Another case was that of counterfeit chips sold for use in missile systems: "…more than 59,000 counterfeit computer microchips from China to the U.S. Navy and other clients for military use aboard American warships, fighter planes, missile and antimissile systems." (Hsu 2010) It doesn't take much of an imagination to think of scenarios where being able to control the actions of an adversary's missile might be advantageous.

Cybersecurity Elitism

In history, information security has long been held to be the responsibility of everyone. Rose Mary Sheldon, in her excellent book "Intelligence Activities in Ancient Rome," tells us of a Carthaginian ship captain who "deliberately drove his ship off course and into a shoal" in order to protect the secret of commercial interests of the state and was duly rewarded in return. (Sheldon 2005 pg 41) In World War II, citizens were admonished regularly that "loose lips sink ships," with the idea of reminding everyone that keeping secrets was everyone's job. (AdCouncil 2011)

The attitude that security is everyone's job is gone. This is partly because actually doing security well is time-consuming, boring, and detail oriented. The "Grandma problem" has long been a recognized challenge in security research, as has the "accidental help desk" phenomenon. The "Grandma problem" refers to the recognized challenges associated with elderly people not completely understanding new technologies. The "accidental help desk" phenomenon is reflected in the over-reliance in some workplaces on the one person who understands the technology. In the first case, Grandma suffers from diminished memory and needs to use easy to remember passwords, which are easy to crack, and never remembers to update her anti-virus software definitions. In the second case, the poor sap who is continually bugged by his colleagues to come fix their computers is rarely adequately trained but usually keeps the productivity at an acceptable level such that more professional help is avoidable, thus encouraging poor computing environments to flourish. In both cases, the situation opens the door to the rampant spread of malware. Because of the increasing interconnectedness of systems, these weak links endanger even the best protected systems, for example when the Grandson of Grandma brings an infected USB drive into work after visiting Grandma.

But beyond these two well-understood challenges, there is a more deeply seated attitude that information security is something that someone else does. It is not part of everyone's job description and increasingly employees expect that security is a service that is provided. As a result, poor security practices flourish. Employees looking to get their jobs done quickly find work-arounds for security controls, usually clueless as to how they are subverting their workplaces. Some real examples are described in the following paragraphs.

Example 1: I was invited to speak to a governmental advisory group. As part of the preparation, I was asked to send my personal information, including my social security number and other identifying information, to the staff who was coordinating the event. Despite the fact that the form on which I was to record this information clearly stated "do not transmit this form through unsecured email," the staff asked that I send them the form via email. When I protested, they informed me that because their email address was on a dot mil branch of the internet, it was secure. It took several go rounds with the staff before I got them to realize that unless encryption was used, there was absolutely no security in the transmission.

Example 2: A civilian employee of the US Department of Defense was ordered to travel to Kuwait. The US Army staff in Kuwait requested that he send an extraordinary amount of personally identifying information to them prior to his arrival. Why they needed or wanted this information is a mystery that has not yet been solved. Why they were willing to accept custodial responsibility for this information is an additional mystery. But they wanted it and they wanted it emailed to them. When the employee protested, the Army staff in Kuwait assured him that it was perfectly secure, since the information would be stored in pdf file format. It is not clear whether or not they ever got the message that sending information in plain text was not a great security solution. Luckily for the employee, the trip was cancelled and his information was not subjected to this incredible situation.

Example 3: An employee of a small company providing services to the US Department of Energy was required to use hardware encryption products in his network in order to establish secure communications with the DOE lab he was supporting. Despite the fact that the crypto card was in a folder that was marked in big red letters "Do Not Send Through Inter Office Mail," the card was sent to the contractor through inter-office mail, subject to who knows whose inspection and perhaps modification.

These situations seem incredible, but they are all true. The pervasive lack of personal responsibility for even the most mundane security elements of a job subverts all other security efforts. This must change if the security situation is ever to be made better. Somehow, security needs to be everyone's job, not just the job of the geek down the hall.

Systems Development

To exacerbate this situation, systems are being built with no security engineering whatsoever. Nancy R. Mead from Carnegie Mellon University, who has been following this problem for many years, succinctly writes:

> When security requirements are considered, they are often developed independently of other requirements engineering activities. As a result, specific security requirements are often neglected, and functional requirements are specified in blissful ignorance of security aspects. In reviewing requirements documents, we typically find that security requirements, when they exist, are in a section by themselves and have been copied from a generic list of security features. The requirements elicitation and analysis that are needed to get a better set of security requirements seldom take place.
>
> (Mead 2010)

When systems are developed without taking security requirements into account, they by definition are vulnerable to mischief. Too often I hear from students and colleagues of security requirements, as poorly defined as they might be, being pushed from the development phase to the operations and maintenance phase, thereby almost guaranteeing they will never be funded or met. I also hear of security compliance monitors who view security as a box to be checked rather than a function to be tested, resulting in paper security rather than real security. Efforts to force more structure on the security community, such as Sarbannes-Oxley and FISMA, have resulted in the growth of entire industries helping clients achieve compliance with the letter of the law. Has security improved as a result? Possibly for some enterprises but not for the cyberspace ecosystem as a whole, particularly when one considers the interaction of systems subject to compliance regulation and those that are not subject..

The Lawyers Have Arrived

That the legal community is beginning to be engaged is perceived as good news in a large portion of the security community. There are two ways that lawyers are starting to become engaged, and both are productive. First, in the realm of cyberwarfare, and, second, in the area of software utility.

In the realm of cyberwarfare, the lawyers are starting to understand and debate the geopolitical implications of multi-jurisdictional issues, such as attacks in cyberspace. The attacks on Estonia in 2007 got the attention of the legal community in a serious way, which the subsequent attacks on Georgia in 2008 solidified. There are active discussions and conferences being held to consider the laws of armed conflict and neutrality with regards to cyberwarfare and many, many lawyers are paying attention.

In the area of software utility, some legal scholars are starting to develop theories of negligence in information technology, something that the industry has fought long and hard to avoid. Dan Ryan in his paper "Product Liability for Security Software" (2003) discusses the fact that developers use contract disclaimers to protect themselves from liabilities associated with flawed software. It is no secret that software licenses typically contain declaimers that state that any problems with the software are not the fault of the developers and that the software is not warranted to actually work correctly. To the uninitiated, this is an amazing concept. To the security community, it is an infuriating concept. Typical language in a license agreement, chosen at random, is the following, including the capitalization:

> WARRANTY DISCLAIMER. WE DO NOT WARRANT THAT THIS SOFTWARE WILL MEET YOUR REQUIREMENTS OR THAT ITS OPERATION WILL BE UNINTERRUPTED OR ERROR-FREE. TO THE EXTENT ALLOWED BY LAW, WE EXPRESSLY DISCLAIM ALL EXPRESS WARRANTIES NOT STATED HERE AND ALL IMPLIED WARRANTIES, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.
>
> (Software Pursuits, 2010)

Product liability lawyers are paying attention and at least one case exists where a class action suit was successful against a software developer:

> "April 2008: Court Approves Final Nationwide Settlement Against Sage Software
> Meyer & Associates is pleased to announce the final approval of a nationwide settlement against Sage Software. Originally filed in 2005, the nationwide class action lawsuit claimed that the Defendant designed, manufactured, distributed and supplied defective ACT! 2005 software." (Meyer 2008)

This is a hopeful sign that perhaps pressure will be brought to bear on systems developers that they have a duty to design and build systems that are carefully constructed and tested, rather than developed at the speed of light using whatever talent happens to be at hand and be affordable.

The 600 pound gorilla in the room is the fact that information technology is increasingly embedded everywhere. It is in cars, from the ignition system to the brakes. It is in buildings, from the elevators to the locks. It is in airplanes, from fly-by-wire systems to navigation. It is in traffic systems, from lights to law enforcement. It is in power grids, from transmission to "smart" usage systems. What could possibly go wrong? Besides everything, that is. The systems are increasingly complex and increasingly tightly coupled. A problem in one area can quickly affect other areas. Should we not expect that our dependence on these systems be founded on some sort of assurance that adequate security is considered and included? In 1994, Peter G. Neumann brought attention to this very issue in his book, "Computer Related Risks." Charles Ashbacher captured the problem succinctly in his review, stating:

> Published in 1995 [sic], it was certainly an eye opener to the dangers of being lax in the use of computers. It was a bit scary when I read it, although at the time, I was optimistic that the danger could be managed.
> However, my position since then has changed in the negative sense. In rereading this book, it is clear that the dangers are the same and are greater in both breadth and depth. This book was written before the explosive growth of the Internet has turned nearly every computer into a potential node in an evil botnet. Also, the use of computers in the management of the modern world has dramatically expanded, increasing the possible ways in which danger can make an appearance.
> In looking through the risks, there is not a single one that has disappeared rather than increased in the level of the danger. Some examples are e-mail spoofs, insider misuse of data, denial of service attacks, threats to privacy, viruses and other malware, security vulnerabilities, computer errors in election results and financial fraud. And so it goes. If you are interested in looking back and seeing how little has changed in terms of the risks inherent with computer use, then read this book. It was and remains the original "canary in the coal" mine concerning the dangers that universal use of computers will generate.
> (Ashbacher 2008)

It is a fairly depressing situation to consider. And Ashbacher is absolutely correct to be depressed about the future. It's only going to get worse, particularly when you consider where we are going and the rate at which we are traveling.

Inside the Brain

News torn from the headlines: " Mind-reading Systems Could Change Air Security" (Tarm 2010).

> "The system … projects images onto airport screens, such as symbols associated with a certain terrorist group … The logic is that people can't help reacting, even if only subtly, to familiar images that suddenly appear in unfamiliar places. If you strolled through an airport and saw a picture of your mother, Givon explained, you couldn't help but respond."

Another headline: "'Mind-Reading' Technology Showcased in NYC: Intel Software Uses Brain Scans to Determine What Items People are Thinking About" (AP 2010). The title of the story is tantalizing enough, but deeper in the story was something even more intriguing (emphases added):

> "Other innovations on display … : Cell phone technology that would use motion, GPS and audio data gathered through users' cell phones to track what they're doing and who they're with. The technology can distinguish activities such as walking, giving a business presentation and driving. It also compares audio readings from different cell phones to determine who is in the same room. This would allow users to share their activity information with their close friends and watch avatar versions of their friends throughout the day. It would also let users track and analyze data about how they spend their time." (AP 2010)

These types of technologies may appear to be benign to the casual user, fun even, but when thrown into a system riddled with poorly designed and insecure components, the potential for disaster looms large. And that's even without a despotic government wishing to use these technologies to squash revolts or calls for reform.

Conclusions

What used to be considered to be secure, soon will not be. The way we think about computer security needs to change. It is critical that the security community embrace the non-technical aspects as part of the whole problem space if there is to be any hope whatsoever of successfully attacking the problem space. A focus on enterprise security goals rather than security technologies would be a good start -- when security is an architectural goal, there is less temptation to try to bolt on exotic solutions focusing on tiny slivers of the technological challenge. Instead, holistic and synergistic solutions must be developed. It is increasingly important that we architect solutions that incorporate human brains, taking into account intellectual property and human inadvertent activity.

Cybersecurity needs to be everyone's job, not just the elite geeks (although they are very important!). System developers must be held to a reasonable standard of conduct that accounts for security. Systems operators and service providers must be held equally responsible. Until these things occur, no real progress will be made. Cybersecurity requirements must be included in all system development efforts, even the small ones given the weak link theory. This needs to be real security engineering, not just bandaids or menu driven options.

This is a 'systems' issue, not simply a computer science or technology issue and as such must be approached as such, taking into account all elements, including people, processes, including mental, inputs, outputs, and interfaces using 'Systems of Systems' approaches. Until such overarching approaches are taken, no real solutions will be found.

References

[AdCouncil 2011] AdCouncil. Security of War Information - Loose Lips Sink Ships (1942-1945). Online Archives of the Advertising Council. ://www.adcouncil.org/default.aspx?id=127

[Amin 2011] Rohan Amin, Detecting Targeted Malicious Email Campaigns Through Supervised Classification of Persistent Threat and Recipient Oriented Features. PhD Dissertation, 2011: The George Washington University.

[AP 2010] AP News. "'Mind-Reading' Technology Showcased in NYC: Intel Software Uses Brain Scans to Determine What Items People are Thinking About" AP News, NEW YORK, April 8, 2010 http://www.cbsnews.com/stories/2010/04/08/tech/main6374956.shtml

[Ashbacher 2008] Charles Ashbacher. Review of "Computer Related Risks". Amazon.com reviews, June 12, 2008. ://www.amazon.com/Computer-Related-Risks-Peter-G-Neumann/dp/020155805X/ref=sr_1_1?ie=UTF8&qid=1302375174&sr=8-1

[CCDCOE 2009] NATO Cooperative Cyber Defense Center of Excellence, Cyber Conflict Legal and Policy Conference 2009. September 9-11, 2009, Tallinn, Estonia. http://www.ccdcoe.org/legalconference/

[CCDCOE 2010] NATO Cooperative Cyber Defense Center of Excellence, Conference on Cyber Conflict. June 15-18, 2010, Tallinn, Estonia. ://www.ccdcoe.org/conference2010/

[Hsu 2010] Spencer S. Hsu Case targets microchips sold to Navy. Washington Post: September 15, 2010. ://www.washingtonpost.com/wp-dyn/content/article/2010/09/14/AR2010091406962.html

[ICE 2010] US Immigration and Customs Enforcement, News Release Sept 7, 2010: Texas man sentenced for selling counterfeit "Cisco" routers. Available online at ://www.ice.gov/news/releases/1009/100907houston.htm

[Matrosov et al 2011] Aleksandr Matrosov, Eugene Rodionov, David Harley, and Juraj Malcho, Stuxnet Under the Microscope. ESET Corporation White Papers, January 2011. ://www.eset.com/resources/white-papers/Stuxnet_Under_the_Microscope.pdf

[Mead 2010] Nancy R. Mead. Security Requirements Engineering. Software Engineering Institute, Carnegie Mellon University. 2006-08-10; Updated 2010-07-14. Available from ://buildsecurityin.us-cert.gov/bsi/articles/best-practices/requirements/243-BSI.html?layoutType=plain

[Meyer 2008] Meyer & Associates, News Release April 2008: Court Approves Final Nationwide Settlement Against Sage Software. http://www.dmlaws.com/ConsumerClassAction/ClientSuccesses.aspx#sage

[Neumann 1994] Peter G. Neumann. Computer Related Risks. Addison-Wesley, 1994.

[Ryan 2003] Daniel J. Ryan. Product Liability for Security Software. IEEE Security & Privacy, v. 1 n. 1, January 2003.

[Schneirer 2010] Bruce Schneirer, Stuxnet. ://www.schneier.com/blog/archives/2010/10/stuxnet.html

[Sheldon 2005] Rose Mary Sheldon. Intelligence Activities in Ancient Rome: Trust in the Gods, but Verify. New York, 2005: Routledge Publishing Group.

[Software Pursuits 2010] Software Pursuits. Software License Agreement, Revised: 2010-03-02. http://www.softwarepursuits.com/license.asp

[Tarm 2010] Michael Tarm "Mind-reading Systems Could Change Air Security", The Aurora Sentinel, Jan 8, 2010, ://www.aurorasentinel.com/news/national/article_c618daa2-06df-5391-8702-472af15e8b3e.html

[Ware 1970] Willis Ware, Security Controls for Computer Systems (U): Report of Defense Science Board Task Force on Computer Security; Rand Report R609-1, The RAND Corporation, Santa Monica, CA (Feb. 1970)

Ryan References of General Interest

Ryan, Julie J.C.H. and Daniel J. Ryan, "Performance Metrics for Information Security Risk Management," IEEE Security and Privacy, vol. 6 no. 5, Sep/Oct 2008, pp. 38-44.

Ryan, Julie J.C.H. and Daniel J. Ryan. "Expected Benefits of Information Security Investments," Computers and Security, Vol. 25, Issue 8. Amsterdam: Elsevier. Pages 579-588. (November 2006). (http://www.sciencedirect.com/science/article/B6V8G-4KXDR1G-1/2/f3dbf2660eab68ae4bf87dde49b7f687)

Ryan, Julie J.C.H. "Use of Information Sharing Between Government and Industry as a Weapon," Journal of Information Warfare 5 no 2 (2006): 1 – 10.

Ryan, Julie J.C.H. and Daniel J. Ryan. "Proportional Hazards in Information Security," Risk Analysis 25 no. 1 (February 2005): 141.

Ryan, Julie J.C.H. and Corey D. Schou. "On Security Education, Training and Certifications," Information Systems Control Journal 6 (2004): 27.

Ryan, Julie J.C.H. "Information Security Tools and Practices: What Works?" IEEE Transactions on Computers 53 no. 8 (August 2004): 1060.

Ryan, Julie J.C.H. "Architecting Information Assurance," Proceedings of the 23rd IEEE International Performance Computing and Communications Conference, Phoenix, Arizona. 2004. pg. 669.

Ryan, Julie J.C.H. "Teaching Information Security to Engineering Managers," Proceedings of the 33rd ASEE/IEEE Frontiers in Education Conference, Boulder, Colorado. November 2003.

Jefferson, Theresa I. and Julie J.C.H. Ryan. "A Comparative Analysis of Privacy Policies of Popular E-Businesses," Proceedings of the 2003 ASEM National Conference, St. Louis, MO.

Ryan, Julie J.C.H. and Theresa I. Jefferson. "The Use, Misuse and Abuse of Statistics in Information Security Research," Proceedings of the 2003 ASEM National Conference, St. Louis, MO.

Ryan, Julie J.C.H. "The Effect of Public Budgetary and Policy Decisions on Development of Trusted Systems," Proceedings of the 2002 ASEM National Conference, Tampa, Florida. pp. 130 – 134.

Ryan, Daniel J. and Julie J.C.H. Ryan. "Institutional and Professional Liability in Information Assurance Education," Proceedings of the 2002 IEEE Workshop on Information Assurance at the United States Military Academy, West Point, NY June 2002.

Julie J.C.H. Ryan, D.Sc.
Associate Professor and Chair
Engineering Management and Systems Engineering
George Washington University
1776 G. St. NW Suite 101
Washington, DC, 20052
jjchryan@gwu.edu

Julie J. C. H. Ryan is Associate Professor and Chair of Engineering Management and Systems Engineering at George Washington University. She holds a B.S. degree from the U.S. Air Force Academy, M.L.S. in Technology from Eastern Michigan University, and D.Sc. in Engineering Management from the George Washington University. Dr. Ryan began her career as an Intelligence Officer, serving the U.S. Air Force and the U.S. Defense Intelligence Agency, focusing on communications and computer issues. She followed that service with a period of activity in industry, working for companies such as TRW and Booz•Allen & Hamilton. She has been in academia since 2001. Her areas of research interest are in information security and information warfare research. She was a member of the US National Research Council's Naval Studies Board from 1995-1998 and currently sits on the Standing Committee for Technology Insight-Gauge, Evaluate & Review (TIGER). She is co-author of the book "Defending Your Digital Assets Against Hackers, Crackers, Spies, and Thieves" (McGraw Hill 2000).