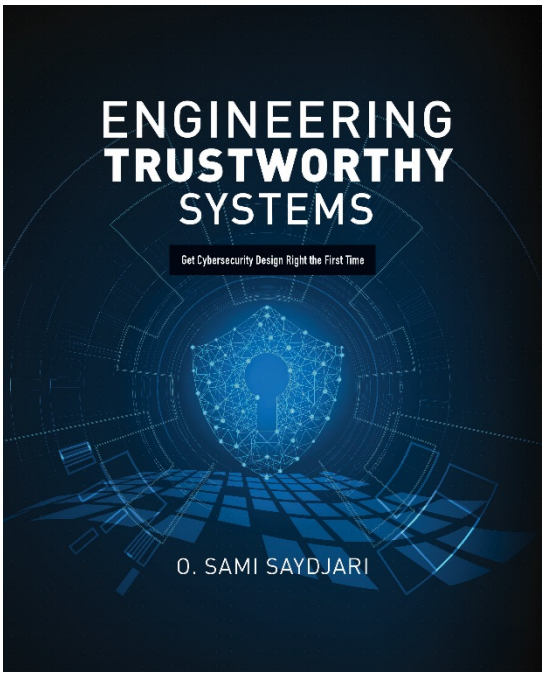
New Cybersecurity Bible by NSA Insider Teaches Next-Generation IT Strategies and Defenses



"This is the "bible" for cybersecurity, which needs to be consulted as we struggle to solve this enormous threat to our national security."

--John M. Poindexter, PhD, VADM, USN(ret), Former National Security Advisor to President Ronald Reagan

Cybersecurity poses the leading threat to global commerce, the military, government agencies, individual privacy, and data integrity for leading institutions. Tens of billions of dollars are spent annually to build, upgrade, and fix computer networks to withstand terrorism, hackers, spies, criminals, and corporate espionage. The next generation of cybersecurity professionals needs to be armed with a comprehensive defense. internationally recognized cybersecurity expert O. Sami Saydjari has written the authoritative bible for crafting cutting-edge cybersecurity solutions to defend against even the most sophisticated attacks, ***Engineering Trustworthy Systems; Get Cybersecurity Design Right the First Time*** (McGraw-Hill, July 2018, 672 pages; Trade Paper, $60, ISBN: 978-1-260-11817-9).

This professional guide shows, step-by-step, how to design and deploy highly secure systems on time and within budget. It offers a comprehensive set of objectives and best practices and shows how to build and maintain powerful, cost-effective cybersecurity systems. Whether you are a cyber-emergency responder, manager of information technology, or a red teamer, tester, accreditor, evaluator or systems designer, you will learn to think strategically, identify the highest priority risk, and apply advanced countermeasures that address the entire attack space.

"Much of the information in this book can be found nowhere else and represents the distilled experiences of over three decades of work as a cybersecurity researcher, architect, and engineer," says Saydjari. "The book carefully builds from the most foundational elements of cybersecurity to the most complex and nuanced topics that can make your performance in cybersecurity more effective, efficient, and stronger." Saydjari has been a visionary and thought-leader in cybersecurity for thirty-five years, working for elite organizations and government powers such as NSA, DARPA, the DoD, and NASA. He has published more than a dozen papers in the field, consulted to national leaders on cybersecurity policy and has been featured in interviews with major media, including *Time, CNN, The Washington Post, PBS, Wall Street Journal, ABC*, and *The Financial Times*. He is the founder and president of Cyber Defense Agency, a leading cybersecurity consulting firm.

He is available to discuss the following:

- What IT professionals and professors need to know about new cybersecurity threats.
- How an organization, business, or government agency should assess its cybersecurity risks.
- What's not being done to architect a cybersecurity-sound system.
- How we can understand the attacker's mindset in order to prevent such attacks.
- How to protect against the failures to guard data such as those were experienced by Equifax, Yahoo, Adult Friend Finder, eBay, JP Morgan Chase, and Target.

Engineering Trustworthy Systems covers the following five major areas:

Part I: What Do You Want? Defines the cybersecurity problem and all of its aspects in order to determine next steps.

Part II: What Could Go Wrong? Reveals why cybersecurity engineers must deeply understand the nature of attacks to properly design defenses against them.

Part III: What Are The Building Blocks Of Mitigating Risk? Explores the solution space for the problems defined in the first two parts.

Part IV: How Do You Orchestrate Cybersecurity? Addresses the attack space holistically and lays out the principles of cybersecurity architecture, including dependability and intrusion tolerance.

Part V: Move Cybersecurity Forward. Shows how to plan for the future.

Cybersecurity professionals, computer scientists, computer engineers, and systems engineers will benefit from a deeper understanding of the principles of architecting a trustworthy system. Saydjari's breakthrough, up-to-date, comprehensive book confers essential knowledge to the next generation so it can solve important and emerging problems. It not only meets the urgent needs of today's IT professional and IT student, it lends insight on the future of cybersecurity.

It also covers these pressing topics:

- Defining a cybersecurity mission.
- Understanding potential adversaries and evaluating harm.
- How to take countermeasures and put into place security controls.
- Which strategy should be invested in.
- Deterrence and adversarial risk.
- Detection foundation systems and strategies.
- Cryptography, authenticating, and authorization.

Dozens of figures and charts fill the book, shown alongside helpful chapter overviews and summaries and insightful questions that enhance the reader's critical thinking skills. An extensive glossary with all key words specially marked throughout the book is provided to facilitate the grasping of important terminology.

Engineering Trustworthy Systems is unique in its breadth, depth, and scope of topics covered. Written in an accessible style, it offers readers a strategic perspective about cybersecurity. It also underscores the need for national investment in cybersecurity.

"This book is for those vulnerable to cyberattacks, the very people who are dependent on information technology – businesses, government, legal, medical, and academic sectors," says Saydjiari.

"This book is about how to engineer trustworthy systems using timeless principles. It is about how trust can be earned through sound system-design principles. It fills gaping holes in the literature and is structured to allow readers to grasp this complex discipline in digestible chunks that build on each other."

"I can think of no person better qualified to write this sorely-needed tome. Sami is one of the leading conceptual innovators in the cybersecurity field with over three decades of experience in all aspects of cybersecurity engineering. He is internationally recognized and trusted as a talented cybersecurity architect. His understanding of this complex topic is both expansively wide and impressively deep in many areas. Despite that, or perhaps because of it, he has a unique ability to communicate the most complex and subtle content in terms that are clear and easily understood. He is part of the world's brain trust on the topic and cares deeply about passing on the collection of wisdom and deep insights to help make cyberspace a safer place.

"This book will be the go-to reference book in cybersecurity engineering for decades to come.'

--Brian Snow, former National Security Agency, Technical Director of three different key components, Research and Engineering, Information Assurance, and the National Cryptologic School

Contact: MEDIA CONNECT
Brian Feinblum 212-583-2718 brian.feinblum@finnpartners.com
Spencer Bement 212-583-2729 spencer.bement@finnpartners.com
Stephen Matteo 212-583-2776 Stephen.Matteo@finnpartners.com

O. Sami Saydjari
Biography

O. Sami Saydjari is the founder and president of Cyber Defense Agency, a premier professional services firm specializing in cybersecurity, computer network defense, and information security. Formed over fifteen years ago, the firm's clients include major banks, power companies, and security product vendors, as well as the Navy, Air Force, Department of Defense, NASA, U.S. Department of Homeland Security, Office of the Secretary of Defense, members of the United States intelligence community, and Defense Advanced Research Projects Agency (DARPA), where he created one of the most significant investments in information assurance in the nation's history.

Under his leadership and guidance, Mr. Saydjari has attracted twenty of the nation's top security experts to create a uniquely superb national asset to help defend the country's most important information systems. He provides vision and expertise for building a research and consulting organization that creates effective systematic defenses for high-value systems against aggressive cyberattack.

Among his circle of contacts, he associates with Richard Clarke, former special assistant to the president for cybersecurity; John Poindexter, former National Security Advisor; Brian Snow, former technical director of cybersecurity at NSA; Mike McConnell, former director of NSA; Steve Lukasik, former director of, DARPA; early founders of the cybersecurity field Earl Boebert and Peter Neumann; and the founder of Bell-Lapadula Model, David Bell.

With thirty-five years of experience in the field, he's been quoted by or featured in major news media outlets, including: *The New York Times, Washington Post, Financial Times, Wall Street Journal, Fox News, CNN, PBS Frontline, ABC, CBS* and *Al Jazeera America.* He is the author of ***Engineering Trustworthy Systems: Get Cybersecurity Design Right the First Time*** (McGraw-Hill, July 2018).

Before founding the Cyber Defense Agency, Mr. Saydjari was a senior staff scientist in SRI International Computer Science Laboratory, where he was the program leader of the Cyber Defense Research Center (CDRC). Prior to SRI, Mr. Saydjari was the Information Assurance Program Manager for DARPA's Information Systems Office.

Mr. Saydjari earned his M.S. in Computer Science from Purdue University. The Director of NSA named him an NSA Fellow in 1993 and 1994. He has published more than a dozen technical papers in the field of information security in publications such as the *National Cryptographic Quarterly*, and has presented the results of his research at major cybersecurity venues such as the National Computer Security Conference, the Annual Computer Security Applications Conference, the IEEE Security and Privacy Conference, and the ACM New Security Paradigms Workshop.

For more information, please consult: www.SamiSaydjari.com and www.EngineeringTrustworthySystems.com He resides in Clarksville, Maryland.

O. Sami Saydjari
Q&A
Engineering Trustworthy Systems

1. What trends are you seeing today when it comes to the newest threats in cybersecurity? Cyberattacks are becoming more frequent, complex, sophisticated, purposeful and targeted. The sheer volume of attacks is increasing exponentially. It is only a matter of minutes between when a computer is first connected to the network and the first attack on that computer. Attacks are now more complex--they employ more steps, and those steps attack more fundamental layers, such as operating systems. They are more sophisticated--they leverage knowledge of flaws in systems design and of the defense systems themselves, steering around and underneath protections. They are more purposeful and targeted—when they attack, it is to gain some effect, such as ransomware to gain money, or Stuxnet to destroy centrifuges.

2. Sami, what inspired you to publish *Engineering Trustworthy Systems*? Cyberattacks pose an existential threat to our entire society; addressing this problem has been a lifelong passion of mine. My career has spanned a good portion of the cybersecurity field. Much of the field grew and evolved as I was learning and applying it. There are many good books on particular aspects of cybersecurity, but there are none that really address the problem holistically, practically, and in an organized manner that starts with a foundational understanding of the problem. I feel it is important and urgent to confer this essential knowledge to the next generation so they can use timeless principles, developed over three decades, to solve important, emerging, and future problems.

3. What can you do to ensure that those who engineer, maintain, or grow an electronic data and information system don't come back to sabotage, blackmail, extort, steal, or destroy these bits and bytes? This is known generally as the insider threat problem. One addresses this problem through a three-layer architecture that is robust against any single security failure. The first is prevention, which creates bulkheads so that insiders cannot access all of the system if they have access to one part of the system. The second layer is detection, which detects anomalous activities, such as accessing parts of the system that a person does not normally access. This indicates an intrusion or abnormal behavior suggesting insider activity. The third layer is tolerance, in which the system reconfigures itself to continue operation if the insider damages a portion of the system.

4. What gaping holes in cybersecurity literature are filled by your book? The first gap is in the union between cybersecurity theory and practice. Although there are good books on theory and on practice, there are none on applying theory in practical situations. The second gap is in the systematic and holistic way of addressing the architecture of cybersecurity. Cybersecurity must be thought of as orchestration and integration of many different moving parts to effectively defend against the entire spectrum of attacks. The third gap is taking an attacker's perspective. It's important for people designing cybersecurity systems to understand fundamentally how attackers can succeed. The designer's job is to make the attacker's life miserable. If the attacker can easily get around a defense, the defense is useless.

5. What could global-scale cyberwarfare look like in a decade? Imagine a world without electrical power, telecommunications, money, and oil and gas to run essential machinery. That is what global-scale cyberwarfare looks like. Our society depends heavily on computers to run these critical infrastructures.

Cyberwarfare is capable of not only short-term disabling of these infrastructures, but actually physically damaging infrastructure such as electrical generators and transformers, for which there are no easy replacements. The effect is the reduction of humanity back to a pre-modern world. We must do everything possible to create a safer and more secure cyberspace to reduce the probability of an all-out global cyberwar because these consequences are as serious and significant as nuclear warfare.

6. What are some of the bigger mistakes one makes when engineering a cybersecurity system? The first is to consider cybersecurity too narrowly. Most cybersecurity engineers specialize in firewalls or intrusion detection. A more holistic approach, stressing how attacks and defenses interplay, is one of the hardest parts of the discipline and also the least well-understood by cybersecurity engineers today. Another big mistake is underestimating the attacker's breadth and depth, finding ways around or underneath defenses. The breadth and depth of defenders must match that of the attackers. Many people make the mistake of spending their budgets on one mechanism that someone claims is the next best thing, instead of considering a range of mechanisms and how much each reduces risk compared to cost.

7. Why do some tend to think of cybersecurity as purely a technological problem? Why is that bad? If you have a hammer, everything looks like a nail. Cybersecurity was invented by technology research engineers, so solutions have naturally been technology focused. We understand that the solutions involve a great variety of disciplines and ideas, including sociology, psychology, and decision theory. For example, phishing attacks use social engineering, which uses psychology to get an authorized user to unwittingly facilitate an attack. The psychology of users and the sociology of user communities working within systems is highly relevant. There is some research in this direction, but it does not receive adequate attention today. The book addresses user behavior and how people really operate in cyberspace.

8. How do cyberattacks pose an existential threat to our entire society? Many people think cyberspace is an optional space of convenience, enabling email or online shopping. In reality, every major infrastructure now depends critically on cyberspace, making it essential to modern life. If a city such as New York loses access to rail deliveries because of a cyberattack, it could not survive beyond three days, thus requiring complete evacuation. Because cyberattacks can destroy physical things, the consequence is not a matter of inconvenience for a day, but rather regional devastation lasting years. If the Unites States or any like nation were to lose power for six months, its very sovereignty would be at stake. That is the level of threat we are now experiencing in this world, and it is untenable.

9. Based on your successful career experiences, your book provides wisdom from those who worked at NASA, Department of Defense, IBM, Honeywell, Cornell University, Columbia University, National Science Foundation, DARPA, Naval Research Lab, Carnegie Mellon University, Orincon, and dozens of other leading institutions, corporations, and government agencies. Does it surprise you that everyone knows pieces of cybersecurity but few, if any, truly command complete knowledge of it? It is no surprise at all. Research in the community developed in a fragmented way. There were intrusion-detection researchers, firewall, and cryptographic researchers. Thus, each discipline grew and developed their own sub-disciplines, their own sub-lingos and their own sub-communities. Often, these sub-communities did not communicate with one another and, in fact, often disrespected the other's contribution. At DARPA, I focused on bringing together these disciplines, including outside disciplines such as reliability and dependability, to address the problem systematically. We continue to need the deep expertise in areas such as firewall design, but we also need the generalists who understand the strengths and weaknesses of a broad set of mechanisms and how they can be woven together for effective defense.

10. What does the cybersecurity solution landscape look like? We are used to thinking in only three dimensions. Cyberspace is hyper-dimensional, with hundreds of dimensions. The cybersecurity solution landscape is thus equally complicated. An attacker can get from one side of the world to the other in

minutes, and a cyber weapon that costs a few dollars to create can cause millions of dollars of damage. If an attacker has a zero-day attack (i.e., one that has never been seen before) in the operating system, the attacker comes from underneath, as if reaching out from underground and grabbing your feet. If we do not foresee such attacks, it's hard to defend against them. This book helps cybersecurity professionals to appreciate required solution space against the complex attack space.

11. How can confidentiality and secrecy backfire when engineering a cybersecurity system? Benjamin Franklin once said that three people can keep a secret only if two are dead. Secrecy is fleeting. Missions that depend on secrecy to achieve their goal are in jeopardy. Furthermore, secrecy breeds secrecy because things connect and because people develop hegemony by keeping secrets. In addition, it costs resources and time to keep secrets secret. Finally, labeling data or whole systems as secret tends to paint a big red target on a system or data to somebody who's interested in acquiring those secrets and a road map to exactly where to attack to get those secrets. So, we must engineer organizations, not just systems, to tolerate the loss of secrets while protecting those secrets as long as possible.

12. What type of cyberspace exercises should one's cybersecurity system undergo? Organizations should periodically red team their systems to gauge an organization's vulnerability to cyberattack. Red teams are good-guy cyberattackers who have skills commensurate with adversaries who might attack the system. Other exercises should be run on an organization's users, including benign phishing attacks to identify vulnerable people and target training accordingly. Finally, organizations need to understand how they will continue to operate without portions of their information technology infrastructure because they could lose it. Backups or alternative IT sites often fail when activated because there have not been adequate exercises to ensure that these plans work under stress, in the moment when they're needed, when attacks succeed against the primary system.

13. Can cryptography really work well enough to protect Bitcoin and alternate forms of currency? Cryptography is a power tool. It is effective and robust against a variety of attacks if it is designed well and operated well by people who understand what they are doing. At the same time, cryptography can be attacked in many ways. For example, quantum computing, when it comes, will be sufficiently fast to break most cryptography done today. There are ways of improving cryptography to be able to resist these attacks, but those are still on the drawing board and not deployed widely today. Bitcoin--and any technology that depends on cryptography—is vulnerable to mechanisms that fail. If such failure results in a catastrophic failure of the entire system, then the design is poor.

14. Do today's business leaders and entrepreneurs have a proper foundation of understanding what needs to be done to protect their company's transactions, data, and consumer privacy? Given the number of recent major breaches in supposedly well-defended systems, the answer is clearly no. Business leaders today are ill-equipped to understand threats to cybersecurity, the gravity of the consequences, or to distinguish good solutions crafted by experts from snake oil talismans sold by charlatans. In the same way that they must manage risk for their company's funds, stock values, and vulnerability to competition, today's leaders must broadly understand cybersecurity risk to make intelligent decisions to protect their companies. This book is written in such a way that company leadership can easily understand the broad concepts, while professional cybersecurity engineers can grasp the depths of how to design effective systems.

15. What happens when detection and deterrence of an attack do not work? Consider cybersecurity defense as a series of layers represented as discs, with holes in them that represent defense weaknesses. The disc placement order is: deterrents, prevention detection, and then tolerance. If deterrents fail, prevention should stop the attacks, particularly where deterrents are weak. Where prevention fails, detection must be engaged to sense and identify an entire gamut of attacks. One must deploy sensors for attacks in a variety of places to ensure that the attacks are detected despite potential weaknesses or even

failures of certain detection mechanisms. Finally, we must assume that attacks will succeed, and we must detect resulting system degradation, and must be able to recover by such actions as rebooting the entire system from golden copies.

16. How does one properly assess risk mitigation in their security system? Assessing risk starts with understanding an organization's mission and how it depends on information technology. Leadership then identifies what bad headlines keep them up at night—for example, what bad IT outcomes would cause a major mission disruption? Once identified, security engineers develop "attack trees," which elucidate the manner, sequencing, and likelihood of attack steps to accomplish the bad outcomes. Then, from that analysis, mitigation steps, including the application of cybersecurity mechanisms, procedures, and architectures can be applied. Each of the possible mitigations can then be re-assessed against the attack scenarios, and the overall risk can be calculated to determine risk-effectiveness. One iterates that process until the organization reaches an acceptable risk level given their budget constraints.

17. There's an ever-increasing dependency and fragility between the Internet of Things. What strategic policy is needed to ensure cybersecurity in the virtual world? The Internet of Things (IoT) poses an interesting cybersecurity challenge because IoT devices are small, low-power, cheap, and ubiquitous—with hundreds or thousands of devices per household. Today these devices are being deployed with little security. Because they connect with the Internet, they create an avenue of attack to other critical Internet-connected systems. Device cybersecurity needs to be built-in from the outset. Device manufacturers must be held accountable for any breaches that result from failure to integrate reasonable cybersecurity. With proper assignment of risk, manufacturers will be incentivized to secure their devices. If not, the equivalent of seat-belt laws or building codes may need to be established for these devices, for the good of the entire community.

18. You were mentored by Brian Snow, the former National Security Agency Technical Director of National Cryptologic School. Who mentors those seeking to crack the cybersecurity of corporations, governments, or individuals? There are two cyberattacker worlds: informal hackers, who hack for fun and mischief, and professional (including military) attackers who attack for high stakes. The hacker community has a hierarchy in which position is established by the coolness and difficulty of various attacks demonstrated to their colleagues. The best of the best, the so-called "uber hackers," become mentors for the hackers who then create tools for what we call the "script kiddies"—those who attack using pre-made scripts, which they tailor without understanding what they're doing. Professional attackers, on the other hand, have a normal organizational infrastructure in which experts rise up to the become mentors. Those cyberattackers are dangerous and capable of major destruction of cyberspace.

19. Does the publishing of your book give insight and ammunition to the very thieves you seek to help others defend against? Certainly. Any good book on cybersecurity defense is also a book that informs offense. Cybersecurity is inherently a double-edged sword. It is the same in the physical world for defense and strategy books as well. On the other hand, cyberspace currently is highly vulnerable and unsafe, without my book being published. Any increased threat from knowledge in my book will be overwhelmingly offset by people designing, operating, and building better systems that make it more difficult for cyberattackers to succeed. So, overall, cyberspace will become more secure as a result of my book, even though some attackers may gain some insights they did not have before.

20. What should an organization do once it discovers its systems have been compromised? The first priority is to stop further compromise. This involves a diagnostic process to discern the source, the nature of the attack, and close the avenues of those attacks before further damage occurs. Then a damage assessment—what was lost, what was damaged, what was compromised—and how to recover from that damage. The organization must then analyze how the attack succeeded so that it can improve its system to ensure that such attacks don't succeed in the future. That requires an open-minded view of these attacks,

and not one that closes down, shuts off, and covers up the fact that the attack occurred. That sort of culture needs to be the norm.

21. What advice do you have for aspiring cybersecurity professionals about the industry they are about to enter? The first thing is to develop an understanding of the nature, mechanisms, and methods of cyberattack. One cannot successfully defend a system without a mindset of how systems are attacked. Second, cyberspace defenders must understand the nature of the technology that they are defending. No matter how narrow their interest area, they must understand the basics of how applications, operating systems, device drivers, and hardware work. They need to understand the nature of novel and complex attacks, because attacks will constantly evolve. Lastly, they need to understand and adapt the principles behind cybersecurity, not just the facts and the mechanisms.

22. Is mastering cybersecurity like a chess game? How does one continually stay on top of the latest virus, hacking technique, or techno-threat? The rules are complex; pieces can move in large leaps not apparent to untrained defenders. One needs vision to understand the broader game. The game is multidimensional, with multiple players playing against a defender representing multiple adversary types. Because cyberspace is malleable and ever-changing, the chessboard can change during the course of play. That very complex game must be understood to properly defend cyberspace. Most attacks simply re-use old attacks against systems for which vulnerability patches exist, but for which the system owners have failed to patch. Occasionally, attack types do emerge. It is only through principles of design, operations, and strategy that we will successfully navigate the complicated chess game of cybersecurity.

23. How does human psychology stand in the way of resisting changes to cybersecurity? Organizations, including nations, are like people. We tend to think better of ourselves than the harsh reality of who we really are. Organizations develop blind spots and an unwillingness to consider significant vulnerabilities such as the possibility that it could die—overnight—as a result of a misstep. If one has not seen a bad event recently, then it's not real; for example, healthy people sometimes choose not to buy health insurance because they've been healthy during the last ten years. Organizations act this way with respect to cyberspace threats. We resist change because it is hard. Organizations sometimes cannot hear cybersecurity experts when they say an organization is vulnerable and action is required.

24. Cybersecurity is not just a matter of good design; it is also a matter of good operations. When a system comes under attack, what important questions does it raise that are important to both operations and the design of systems? First, the time to consider one's options is *not* during the attack. Designers must prepare for these attacks, and they must prepare the operations people by providing the tools to identify, diagnose, and stop those attacks. Both designers and operators must consider how to identify and react to attack scenarios in advance of the attacks, creating "cyberwar playbooks." After a successful attack, an organization needs a lessons-learned-knowledge feedback loop to improve both operations and design. As with aviation accidents, cyberattacks require a deep causal analysis of all contributing factors in all systems involved. The book discusses methodologies to mine cyberattacks for maximum information and how to create that critical design feedback loop.

25. What have you learned from some of the biggest security breaches in just the past decade from Equifax, Yahoo, and Adult Friend Finder, to a ransomware worm exploiting a known vulnerability in Windows? Very few of the major cybersecurity breaches offer new insights into the proper defense of systems. Many leave vulnerabilities wide open that could have been closed with good patching and operations practices. So, the first step is to immediately apply best cybersecurity practices—often cutting risk in half for little cost. Second, systematic defense is critical. Often these organizations have good firewalls but few internal controls, or good intrusion detection systems but no skilled operators to monitor them. This lack of systematic defenses drives home the focus of my book: systematically applying

cybersecurity principles against cyber-attacks—weaving together defenses to make it difficult for cyber attackers to succeed—is essential to protect organizations at any level.

Cybersecurity Insights: Now & The Future
Excerpted: *Engineering Trustworthy Systems*

- Cyberattack scenarios are plausible and therefore worthy of urgent attention. The nations of the world are unprepared to properly defend themselves and recover from a strategic cyberattack. To recognize the plausibility and consequences of such attacks without undertaking any governmental action would be unconscionable. The only rational approach to address a problem of this magnitude and scale is a concerted, high-priority government program on the order of the Manhattan Project. Failure to embark on such a program will have disastrous consequences for this generation and the next.

- Cyber conflict can use cyberspace to affect strategic damages very quickly in the physical world, which could, as a result, escalate the situation to physical warfare and potential nuclear warfare. The risk is serious and it is real.

- In the information age, information and information processing are primary resources over which countries will compete. Further, and more importantly, cyberspace controls critical infrastructure in the physical world, including: electrical power, telecommunications and banking. The information technology supporting the critical infrastructure is called the critical information infrastructure, and it is highly vulnerable to attack.

- Secrecy and privacy are almost surely going to erode at an increasing pace as automated inference capabilities increase.

- Cyberspace is full of ordinary criminal risks and extraordinary cyber warfare risks. Ordinary risk is the responsibility of the information infrastructure owners, but extraordinary risk is squarely the responsibility of governments.

- A major assault on cyber infrastructure? Surely, it's coming, and it's undoubtedly already in its planning stages.

- We are in a space race–cyberspace. Cyberspace represents an equally powerful and equally dangerous space for strategic control. Cyberspace affords a similar ability to launch devastating strategic attacks against one's opponents from anywhere in the world with little warning. In some sense, cyberspace is a fabric that lies underneath all systems today. One can view it as the ultimate "low ground" from which a cyber soldier can pop up and grab the legs of their adversaries, and pull them to their metaphorical deaths in a zombie apocalyptic fashion.

- There is a quiet space race going on in cybersecurity. Nations are rushing to exploit the vast vulnerabilities of the current generation of information technology, while attempting to patch their own vulnerabilities against such attacks. This creates a highly destabilized situation.

- Every time before a major change occurs in technology, engineers need to think about the end-game and the evolutionary pressures being created. A bit of forethought now, on ways that engineers can design systems to decrease the probability of a negative outcome for humanity, the better off we will be. The details on how best to do that should be the subject of collaboration of some of the world's best scientists, engineers, and ethicists. The effort should start now, before the rate of progress gets beyond the point of exercising effective control.

- Artificial intelligence represents a black swan event in cybersecurity. Artificial intelligence techniques can be valuable in responding to machine-speed attacks. At the same time, artificial intelligence poses significant risks to mankind that should be deeply considered now, before it becomes too difficult to affect the course of the evolution of increasingly intelligence systems.

- Infosphere pollution will become a critical problem of the future.

- The virtual economy inside the gaming industry and virtual currencies are emerging as a significant part of the real economy and need to be taken more seriously from a cybersecurity perspective.

45 Things IT Professionals Need To Know About Cybersecurity

1. Trustworthiness of a system is a fundamental property of a system that must be designed into the system from the outset.

2. The quest for trustworthy systems raises many questions relating to cybersecurity and other attributes, including operational questions relating to dealing with attacks.

3. Cybersecurity engineering involves many delicate trade-offs with one's mission. Cybersecurity requires a trade-off of mission performance and functionality.

4. To understand cybersecurity, one must understand how systems are attacked.

5. Risk is particularly high at interfaces between systems because of bad assumptions.

6. Organizations weigh the needs for confidentiality, integrity, and availability of data.

7. Take the attacker's perspective and seek to minimize the value an attacker will derive.

8. Avoid concentrating valuable data in one place to avoid creating a high-value target.

9. Avoid outsourcing critical functionality and data to potentially untrustworthy entities.

10. Partition data into tiers of criticality based on the degree to which mission depends on it.

11. Examine cross-product of the mission and the critical data elements to find strategic harm.

12. Systems are too complex to understand without modeling in some way.

13. Abstraction helps focus attention and foster better cybersecurity design and operation.

14. Models can be inaccurate, incomplete, or obsolete, causing design and operations errors.

15. Attacker models have the asymmetric advantage of the element of surprise.

16. Defender and adversary models are themselves valuable targets.

17. Assume an adversary deeply knows the target system's design and implementation.

18. More strongly, assume that adversaries are inside the system in the form of malicious code.

19. Discretionary access control is useful, but does not prevent the leakage of sensitive data.

20. Mandatory access control determines access based on rules about user and data attributes, but may need finer-grained controls as well.

21. Identity-based access control provides fine-grained control, but can be unmanageable.

22. Key generation must be truly randomly chosen from within the key space – it's hard.

23. Keys must be securely distributed to intended recipients of encrypted data.

24. Cryptographic algorithm design is a complex art that should not be done by amateurs.

25. If you cannot trust the hardware, then the work required to trust the software is futile.

26. Hardware has some software driving its operation, posing a little-known cybersecurity risk.

27. Countermeasure design-to-purpose maps countermeasures to attack space.

28. Broadly cover all important attack classes with some mechanism or architectural feature.

29. Defense in breadth is brittle without defense in depth; depth is useless without breadth.

30. Multilevel security research had a profound influence on trustworthiness research.

31. Integrity policy and control are the foundation of all cybersecurity.

32. Cybersecurity measures are ineffective if they are not usable.

33. Cost, in a variety of forms, is a key factor in cybersecurity engineering trade-offs.

34. Failures can predict attack – with significantly higher damage.

35. Attack tree forests need to be representative of the attacker goal space.

36. Include critical suppliers, and distributors, and service providers in system analysis.

37. Adversaries do not play fair and violate unrealistic or poorly understood assumptions.

38. Attackers will begin targeting cyber-physical systems and underware.

39. Cyber exercises are essential in both guiding design and operational preparedness.

40. The six authentication phases are: entity identification, identify certification, identity resolution, identity assertion, identity proving, and identity decertification.

41. Entity identification use three schemas: something you know (e.g. passwords), something – you-have (e.g. an authentication token), and something you are (e.g. biometrics).

42. Identity decertification when a person leaves an organization, must be quick and thorough.

43. Detection complements prevention focusing on attacks that cannot be easily prevented.

44. Detection starts with good feature selection and proceeds up a hierarchy of seven layers.

45. Subtle attacks require correlating multiple events; one event rarely gives definitive proof.

Endorsements

"A technical tour-de-force! This is the book I have wanted for over a decade."
—Eugene 'Spaf' Spafford, Professor of Computer Science and leader of the CERIAS Project, Purdue University

"[A] definitive text [that] delivers insightful philosophy, deep understanding, practical guidance, and detailed instruction for building future systems that mitigate cybersecurity threats."
—Marv Langston, Former Navy CIO

"One of the great experts in our field [...] has produced one of the finest [...] works in our field."
—Dr. Edward G. Amoroso, CEO of TAG Cyber, and former CSO, AT&T.

"Distills the lessons of a lifetime. [...] Both comprehensive and easy to read [and] notable for its emphasis on looking at a system as a whole, not just an aggregation of components, and for helping readers understand how to value information and [...] deal with risk."
—Carl Landwehr, IEEE Fellow and member of the National Cybersecurity Hall of Fame

"An authoritative, timeless, and practical guide to cybersecurity [...] underscores that our opponents' reach, speed, and understanding of our vulnerabilities currently outmatch our defenses, which is why [...] our future depends on it."
—Melissa Hathaway, former cyber advisor to presidents George W. Bush and Barack H. Obama

"Perfectly captures the asymmetrical nature of cyber-warfare [and] will help level the playing field and put the adversary on their heels."
—Jim Carnes, former Chief of Security Testing Center at the Department of Defense

"Reflects decades of experience in designing and building secure computer systems."
—Steven B. Lipner, Member of the National Cybersecurity Hall of Fame

"Brings together [...] for the first time [...] the myriad cybersecurity perspectives, the types and impact of failure, and the latest thinking in mitigation strategy."
—Tom Longstaff, Chair, Computer Science, Cybersecurity, and Information Systems Engineering Programs, The Johns Hopkins University Engineering for Professionals

"Cybersecurity practitioners, designers, and researchers will all find that the lessons in this book add inestimable, tangible value to their missions; the depth and breadth of this book is truly impressive."
—Roy Maxion, PhD, Research Professor, Computer Science Dept, Carnegie Mellon University

Goes "straight to the heart of very real operational problems that undermine current defensive capabilities and strategies."
—Kymie Tan, Systems Engineer, Jet Propulsion Laboratory, NASA

“A comprehensive and straightforward approach that draws on examples from other fields such as biology and astronomy to enhance clarity and purpose.”
—Teri Shors, Dept. of Biology, University of Wisconsin Oshkosh; author of *Understanding Viruses*

“Provides a refreshing look at cybersecurity by acknowledging the need for systems engineering.”
—Joe Weiss PE, CISM, CRISC, ISA Fellow, IEEE Senior Member, Managing Director ISA99 (Industrial Automation and Control Systems Security)