Seeking Balance in Cyber Education

Commander Michael Bilzor, USN, PhD, U.S. Naval Academy

Abstract. The future cyber warriors of the U.S. and the Department of Defense are being groomed at our nation's universities right now. As they are imbued with the fundamentals of computer network attack and defense, the war rages on in cyberspace. Few questions are more critical to the future of DoD and the nation than how we can most effectively prepare these men and women for their mission. There are pitfalls in gravitating to extremes as we in academia chart their course. In the paragraphs that follow, we advocate for a balanced approach that maximizes educational value, in order to prepare those future cyber warriors for the battles that lay ahead of them.

Theory vs. Application

"A man must know how to choose the mean and avoid the extremes on either side, as far as possible" attributed to Socrates

An important aspect of any educational program is the balance between teaching theory and application. Some refer to this as "training vs. education." If students receive all theory and no application, they will be challenged to apply the theory to contemporary computer systems and networks. If students are only taught specific applications, they will be able to use today's systems, but will have difficulty adapting to new situations, tools, and technologies.

This tension is felt in traditional computer science, as it is in many engineering and scientific disciplines. In the field of cyber security, however, the inherent complexity of systems makes the divergence between theory and application more profound compared to traditional academic disciplines, and it is therefore more challenging to strike a proper educational balance between the two.

To illustrate the contrast, first consider a traditional discipline like material science. Mechanical engineers learn how materials fail by studying and measuring stress and strain, hardness and ductility, etc. They reinforce their theoretical understanding by breaking materials in the lab. When a bridge support or an aircraft bulkhead fails, they can appeal directly to the theory observed in the lab for confirmation.

Now let us consider the security failure of a cyber system. Many of the theoretical underpinnings of secure computer systems were established as early as the 1970s. Take a stroll down memory lane:

- The Bell-LaPadula (BLP) model for multi-level security, first outlined in 1973 [1]. In this model, subjects access objects; both subjects and objects have associated security labels. To preserve confidentiality, access is determined according to three rules: a subject may not read data at a higher security level (no read up, or "simple security"), a subject may not write data to a lower security level (no write down, or the "•-property"), and a subject that can both read and write must do so only at the same security level (the "strong •-property").

Fig 1: Illustration of BLP Formal Security Model

- The Biba model, published in 1975, did for integrity what BLP did for confidentiality [2]. The Biba model associates subjects and objects with integrity labels, with similar rules: a subject cannot write data to an object at a higher integrity level ("no write up"), a subject may not read data from an object at a lower integrity label ("no read down"), and a subject may not request a service from a subject of higher integrity.
- First introduced in 1983, the Kemmerer Shared Resource Matrix Methodology demonstrated the requirements for covert channels to exist in a computer system, and developed code-analysis techniques for identifying them [3].
- The Clark-Wilson model, introduced in 1987, outlined an approach where data integrity is preserved through a well-defined series of transactions [4].

What do these important theoretical security models have in common with the modern, commercially-available operating systems most widely used by DoD? Unfortunately, nothing. Of the vulnerabilities reported on the national vulnerability database for this year, how many refer to incorrect application of one of the formal security models listed above? None [5]. Why not? Because modern, general-purpose, commercially-available operating systems and applications used by DoD, even on classified systems, have not been implemented based on formal security models. The commercial market does not require formal security models, and the modern commercial code base is too complex and too rapidly evolving for this to be practical today.

It is true that some computer systems have been developed with provable security in mind. For example, seL4 is a microkernel whose security properties have been formally verified, but its complexity (8,700 lines of C code and 600 lines of assembler) pales in comparison to that of a full-blown commercial operating system, at tens of millions of lines of code [6]. Even a browser application can run into the millions of lines of code [7], and the overall complexity of a computer system is cumulative in the complexity of its components (software and hardware).

Returning to our example, a security failure of a computer system does not generally reflect a failure in the security theory, or an incorrect application of the security theory. Rather, a security failure of a computer system most often results from human error regarding implementation of a technology specific to that system. Understanding most modern computer security failures requires

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
FEB 2015		**00-00-2015 to 00-00-2015**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Seeking Balance in Cyber Education	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **U.S. Naval Academy,Computer Science Dept,572M Holloway Rd,Annapolis,MD,21401-5002**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The future cyber warriors of the U.S. and the Department of Defense are being groomed at our nation?s universities right now. As they are imbued with the fundamentals of computer network attack and defense, the war rages on in cyberspace. Few questions are more critical to the future of DoD and the nation than how we can most effectively prepare these men and women for their mission. There are pitfalls in gravitating to extremes as we in academia chart their course. In the paragraphs that follow, we advocate for a balanced approach that maximizes educational value, in order to prepare those future cyber warriors for the battles that lay ahead of them.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**5**	

not an understanding of traditional theoretical security models, but an understanding of the implementation details particular to a system, whether it is an operating system, a software application, or a piece of hardware. Unlike the mechanical engineer in our earlier example, the computer security engineer is more likely not relying on the basic theory to find the failure in the implementation.

Security theories outlined in BLP, Biba, and other models are covered by most university programs, and in some general certification programs like CISSP, as important background. Many undergraduate and graduate programs in Computer Science (CS), Information Technology (IT), and Information Systems (IS) do treat both the theoretical and applied aspects of security, but they often do so independently, without strongly connecting the two. This occurs in part because, compared to traditional science and engineering fields, theoretical models of computer security diverge further from their actual implementations, in real-world systems. Security is addressed in CS, IT, and IS curricula, but often in a way that leaves theory and application divorced. This leads to the challenge, in academia, of how best to effectively bridge the resulting gap.

Principles and Pillars vs. Applications and Tools

"Fly the Middle Course" – Daedalus to Icarus, in Cretan mythology

If the talented software engineers developing Windows, Linux, and OS X are not deriving their code directly from theoretical security models and applying formal proofs of correctness, at what level of abstraction can cyber security be applied to such systems?

Many experts in the field have enumerated principles -- understandable general statements about properties that can be applied to computer systems, networks, and software. For example, in our Introduction to Cyber Security Course, given to all U.S. Naval Academy midshipmen fourth class (freshmen), we outline three commonly-used principles of cyber defense: the Principle of Least Privilege, Defense in Depth, and Vigilance, and ask the students to implement them in a variety of ways during hands-on labs. [8]

Many organizations frame Cyber Security or Information Assurance in terms of pillars, fundamental properties that must be preserved by a computer network. Three of the most often used are confidentiality, integrity, and availability. Some institutions use only these three pillars. In our course, we add the pillars of authentication and non-repudiation. Others include additional pillars, as well [8,9]. Here again, the educational challenge is the gap between the principles or pillars and the tools and techniques needed to implement them. Without specific instructions explaining how a particular pillar or principal is applied to a specific network, host, or application, students do not find the application intuitively obvious, in our experience.

Alternatively, some organizations define their approach to cyber security at a more granular level, as in the following two examples.

NSA's Information Assurance Division outlines its Top 10 Mitigation Strategies [10]:

- Application Whitelisting
- Control Administrative Privileges
- Limiting Workstation-to-Workstation Communication
- Antivirus File Reputation Services
- Anti-Exploitation
- Host Intrusion Prevention Systems
- Secure Baseline Configuration
- Web Domain Name System Reputation
- Take Advantage of Software Improvements
- Segregate Networks and Functions

The SANS Institute enumerates its 20 Critical Controls as a guide to securing a computer network [11]:

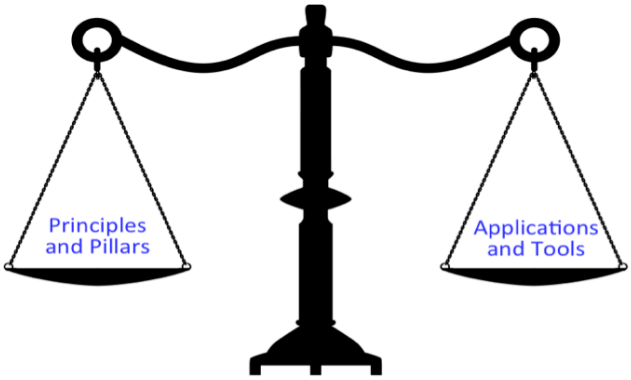
- Inventory of Authorized and Unauthorized Devices
- Inventory of Authorized and Unauthorized Software
- Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
- Continuous Vulnerability Assessment and Remediation
- Malware Defenses
- Application Software Security
- Wireless Access Control
- Data Recovery Capability
- Security Skills Assessment and Appropriate Training to Fill Gaps
- Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
- Limitation and Control of Network Ports, Protocols, and Services
- Controlled Use of Administrative Privileges
- Boundary Defense
- Maintenance, Monitoring, and Analysis of Audit Logs
- Controlled Access Based on the Need to Know
- Account Monitoring and Control
- Data Protection
- Incident Response and Management
- Secure Network Engineering
- Penetration Tests and Red Team Exercises

Teaching cyber security based only on enumerated lists like these requires teaching technology-specific, application-specific, and even tool-specific content. For example, tools like Microsoft's Active Directory and Group Policy, EMET, and Applocker can be used to support the controls above, but they might not be the principal tools of the trade in 10 or 20 years.

Principles are enduring, but applications and tools tend to change over time. In order to ensure that a cyber security education is not perishable, it should not focus too heavily on the applications and tools. There is a natural aversion in academia

to "teaching the tools", since students may learn the tool but not understand the theory. The solution is not to avoid tools altogether, but to employ them as facilitators of understanding, and connect them to the great principles.

To ensure that an academic program is contemporary and relevant, educators should not omit entirely the cutting-edge tools and technologies of the day. Here again, a balanced approach, containing appropriate quantities of each, may be the most suitable way. In a way, too, enumerated principles and pillars, even if not formally defined themselves (like BLP, Biba, or Clark-Wilson), can act as an informal bridge between enduring security theory and the security tools and practices of the day.



Computer Science vs. Cyber Operations

"I have always sought for the middle ground."
—James Madison

Another important schism in the education of our future cyber warriors is in the relationship between cyber security and the disciplines of computer science and information technology. Some commonality is generally acknowledged, but the degree and nature of the overlap is often debated.

Let's Get Interdisciplinary

A key difference, for many, is the assertion that cyber security is more of an interdisciplinary field of study, compared to traditional computer science or information technology. The Department of Defense, in particular, has acknowledged the impact of cyber-physical systems (CPS) on the future of warfare, which necessarily reaches beyond the traditional computing fields.

There are of course many legal, social, and ethical aspects of cyber security not traditionally covered by computer science degree programs. For example, DoD cyber operators should be familiar with the constructs of Title 10, the section of the U.S. code that clarifies military roles and authorities, and Title 50, which outlines intelligence roles and authorities, since these frequently overlap in the conduct of real-world cyber operations [12]. As another example, it is important to discuss in an educational setting the social, ethical, and legal aspects of insider leaks like the Manning and Snowden incidents, as well as the societal perception of government cyber programs, like those covered in media reports surrounding the Snowden affair [13,14]. In addition, an educational program in cyber operations would be remiss to omit topics like social engineering and activist hacking [15], or "hacktivism."

Let's Get (Cyber) Physical

The classic example of exploiting a cyber vulnerability to conduct a physical attack is of course Stuxnet [16], but there are other examples of how the effects of cyber attacks can be felt in the physical domain:

- In 2000, a disgruntled contractor, after being turned down for a job with the local government, gained control of the Maroochy Water Services system in Queensland, Australia [17]. Using only a laptop and a radio transmitter, the attacker was able to control 142 pumping stations for three months, "releasing over one million liters of untreated sewage into a stormwater drain that flowed into local waterways."
- The "Aurora Test," conducted by Idaho National Labs, despite some artificialities, illustrated how a large electrical generator could be destroyed, via a network connection, simply using cleverly-timed inputs from its SCADA controller [18].
- Although there are no published instances to date of a cyber attack causing a widespread critical infrastructure outage, academic research has illustrated the feasibility of such an attack. In research published in 2004, Albert et al. used a graph-based model of the North American power grid to show how successful attacks against a small number of distribution or generation nodes could have cascading effects on the rest of the grid [19]. A 2009 paper by Jian-Wei Wang and Li-Li Rong, examining the western U.S. power grid, also illustrated ways that critical infrastructure topologies can be vulnerable to attack [20].

Cyber attacks can also target information about military hardware, information that could be used to compromise those systems later on the battlefield:

- According to the U.S. government, " the owner of a Chinese aviation technology company with an office in Canada, conspired with two unidentified individuals in China to break into the computer networks of U.S. companies to get information related to military projects." The man's co-conspirators allegedly "claimed to have stolen 65 gigabytes of data from Boeing related to the C-17 military cargo plane" and "sought data related to other aircraft, including Lockheed Martin Corp.'s F-22 and F-35 fighter jets." [21]
- 2014 Media reports indicated a breach of three different Israeli defense companies, apparently resulting in the exfiltration of proprietary information about Arrow III missiles and Israeli UAVs [22].

However, it is important to note that, in general, as illustrated in the examples above, when a cyber attack involves a CPS, the vulnerability and the compromise take place in the computer system, while the effects are transmitted to the physical system through a PLC or a similar mechanism. An understanding of the interconnect and the physical system is important, but the fundamental security breakdown generally does not occur in the physical system, but in the cyber portion; the physical system's actions are usually just a manifestation of the compromise to the cyber portion.

While important, real-world compromises of CPS have been the exception, rather than the norm. For DoD, the most significant impact of real-world cyber warfare to date has been the compromise of important information, rather than the manifestation of a cyber attack on a physical system.

Foundational Skills

Therefore, a cyber security education, while interdisciplinary in scope, should also include a great deal of the fundamentals traditionally taught in computer science and information technology programs, such as networks, programming and scripting, and operating systems.

When we analyze the skills commonly thought of as supporting cyber security, many rely on a strong foundation in computer science. For example, we can examine NSA's syllabus components for its latest certification criteria as a Center of Academic Excellence in Cyber Operations [23], along with the topics' relationship to fundamental instructional areas in computer science, as well as closely related engineering fields. In Table 1, the first column lists the Cyber Operations content -- first required topics, then optional, of which 60% must be included in the academic program. The next columns indicate, respectively, whether the content referenced is traditionally taught in curricula for computer science and information technology (CS/IT), electrical and computer engineering or systems engineering (CE/SE), or some other department, respectively.

The NSA CAE criteria for Cyber Operations supplies just one example definition of the educational topics supporting cyber security, and others may differ slightly. However, we can conclude that, although the field encompasses topics from multiple disciplines, the preponderance of those derive from traditional areas of computer science and information technology. Overemphasizing the interdisciplinary aspects, therefore, risks giving short shrift to some of the core computing fundamentals.

Mandatory Content	CS / IT	CE / SE	Other
Low-level Programming Languages	X		
Software Reverse Engineering	X		
Operating System Theory	X		
Networking	X	X	
Cellular and Mobile Communications	X	X	
Discrete Math	X		
Overview of Cyber Defense	X		
Security Fundamental Principles	X		
Vulnerabilities	X		
Legal			X

Optional Content (60% minimum)	CS / IT	CE / SE	Other
Programmable Logic Languages		X	
FPGA Design		X	
Wireless Security	X	X	
Virtualization	X		
Large-scale Distributed Systems	X		
Risk Management of Information Systems	X		
Computer Architecture	X	X	
Microcontroller Design		X	
Software Security Analysis	X		
Secure Software Development	X		
Embedded Systems	X	X	
Forensics	X	X	
Systems Programming	X		
Applied Cryptography	X		
SCADA Systems		X	
HCI / Usable Security	X		
Offensive Cyber Operations	X		
Hardware Reverse Engineering		X	

Table 1: Topics required for certification as an NSA Center of Academic Excellence in Cyber Operations, and where those topics are most commonly covered in traditional university curricula.

Summary and Conclusions

In any discussion of an academic curriculum, the theory must be the foundation. However, in the modern field of cyber security, never has there been such a divergence between the traditional theories and the hands-on application. We bridge the gap to some degree with principles and pillars, which express concepts in an understandable way, but still require software tools and application-specific knowledge to implement. As a result, the maximally effective cyber education should be exclusive of neither, but seek a middle ground. Similarly, in the drive to include interdisciplinary studies in the realm of cyber operations, due to their real-world effects and connection to physical systems, we should not do so to the detriment of computer science and information technology, which form the foundation on which cyber attack and defense are built. Our future cyber warriors will be best prepared if we seek balance and find the middle way.

ABOUT THE AUTHOR

Commander Michael Bilzor, USN, PhD, is a Permanent Military Professor at the U.S. Naval Academy. As a Naval Flight Officer, he accrued more than 2,000 flight hours in the F-14 Tomcat and F/A-18F Super Hornet and flew combat missions in Iraq. At the Naval Academy, he served as course coordinator from 2013-2014 for the school's Introduction to Cyber Security class, taken by all midshipmen in their first year. Commander Bilzor has coached the midshipmen cyber competition team the last two years. His research interests are focused in cyber security, and he is currently associate chair of the Computer Science department.

572M Holloway Rd., Michelson 346
Stop 9F, Computer Science Dept.
U.S. Naval Academy
Annapolis, MD 21401-5002
Phone: 410-293-6802
Fax: 410-293-2686
E-mail: bilzor@usna.edu
Web: http://www.usna.edu/Users/cs/bilzor/

REFERENCES

1. Bell, D. Elliott, and Leonard J. LaPadula. Secure computer systems: Mathematical foundations. No. MTR-2547-VOL-1. MITRE CORP BEDFORD MA, 1973.
2. Biba, Kenneth J. Integrity considerations for secure computer systems. No. MTR-3153-REV-1. MITRE CORP BEDFORD MA, 1977.
3. Kemmerer, Richard A. "Shared resource matrix methodology: An approach to identifying storage and timing channels." ACM Transactions on Computer Systems (TOCS) 1.3 (1983): 256-277.
4. Clark, David D., and David R. Wilson. "A comparison of commercial and military computer security policies." 2012 IEEE Symposium on Security and Privacy. IEEE Computer Society, 1987.
5. "NVD - Home." NVD - Home. NIST, n.d. Web. 08 Aug. 2014. <http://nvd.nist.gov/home.cfm>.
6. Klein, Gerwin, et al. "seL4: Formal verification of an OS kernel." Proceedings of the ACM SIGOPS 22nd symposium on Operating systems principles. ACM, 2009.
7. R., Maxwell. "Lines of Code: How Our Favorite Apps Stack up against the Rest of Tech." Phone Arena. PhoneArena.com, 12 Nov. 2013. Web. 08 Aug. 2014.
8. Various. "SI110: Introduction to Cyber Security, Technical Foundations." SI110: Introduction to Cyber Security, Technical Foundations. U.S. Naval Academy, n.d. Web. 08 Aug. 2014. <http://www.usna.edu/CS/si110/index.html>.
9. Various. "Information Assurance." Wikipedia. Wikimedia Foundation, 22 July 2014. Web. 10 Aug. 2014.
10. Various. "IA Guidance" Information Assurance Guidance. NSA, 15 Jan. 2009. Web. 08 Aug. 2014. <http://www.nsa.gov/ia/mitigation_guidance/>.
11. Various. "Critical Security Controls." SANS Institute -. SANS Institute, n.d. Web. 08 Aug. 2014. <https://www.sans.org/critical-security-controls/>.
12. Wall, Andru E. "Demystifying the title 10 - title 50 debate: Distinguishing military operations, intelligence activities & covert action." (2011).
13. Gellman, Barton. "Edward Snowden, after Months of NSA Revelations, Says His Mission's Accomplished." Washington Post. The Washington Post, 23 Dec. 2013. Web. 10 Aug. 2014.
14. Fishman, Steve. "Bradley Manning's Army of One." NYMag.com. New York Magazine, 3 July 2011. Web. 10 Aug. 2014.
15. Times, High. "Anonymous Unmasked." The Huffington Post. TheHuffingtonPost.com, 01 Apr. 2014. Web. 10 Aug. 2014.
16. Mittal, Pawan. "How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History | Threat Level | WIRED." Wired.com. Conde Nast Digital, 09 July 0011. Web. 10 Aug. 2014.
17. Slay, Jill, and Michael Miller. Lessons learned from the maroochy water breach. Springer US, 2007.
18. Zeller, Mark. "Myth or reality–Does the Aurora vulnerability pose a risk to my generator?." Protective Relay Engineers, 2011 64th Annual Conference for. IEEE, 2011.
19. Albert, Réka, István Albert, and Gary L. Nakarado. "Structural vulnerability of the North American power grid." Physical review E 69.2 (2004): 025103.
20. Wei, Dong, et al. "An integrated security system of protecting smart grid against cyber attacks." Innovative Smart Grid Technologies (ISGT), 2010. IEEE, 2010.
21. Pettersson, Edvard. "Chinese Man Charged in Plot to Steal U.S. Military Data." Bloomberg.com. Bloomberg, 12 July 2014. Web. 08 Aug. 2014.
22. Krebs, Brian V. "Krebs on Security." Krebs on Security RSS. Krebs on Security, 14 July 2014. Web. 08 Aug. 2014.
23. Various. "NSA CAE CO" Academic Requirements for Designation as a Center of Academic Excellence in Cyber Operations. NSA, 12 Jan. 2012. Web. 08 Aug. 2014. <http://www.nsa.gov/academia/nat_cae_cyber_ops/nat_cae_co_requirements.shtml>.