Situation Awareness-Oriented Cybersecurity Education

Jun Dai
Computer Science, California State University, Sacramento
jun.dai@csus.edu

Abstract—This Research to Practice Full Paper presents a new methodology in cybersecurity education. In the context of the cybersecurity profession, the 'isolation problem' refers to the observed isolation of different knowledge units, as well as the isolation of technical and business perspectives. Due to limitations in existing cybersecurity education, professionals entering the field are often trapped in microscopic perspectives, and struggle to extend their findings to grasp the big picture in a target network scenario. Guided by a previous developed and published framework named "cross-layer situation knowledge reference model" (SKRM), which delivers comprehensive level big picture situation awareness, our new methodology targets at developing suites of teaching modules to address the above issues. The modules, featuring interactive *hands-on labs* that emulate *real-world multiple-step attacks*, will help students form a knowledge network instead of isolated conceptual knowledge units. Students will not just be required to leverage various techniques/tools to analyze breakpoints and complete individual modules; they will be required to connect logically the outputs of these techniques/tools to infer the ground truth and gain big picture awareness of the cyber situation. The modules will be able to be used separately or as a whole in a typical network security course.

Keywords—cybersecurity education, situation awareness, multiple-step attack, mission-driven analytics

I. INTRODUCTION

A. Problem

Cybersecurity has by necessity become a robust and thriving field, producing an immense variety of solutions to control or mitigate cyber threats. However, researcher have identified an 'isolation problem' [9] in the field, in terms of the inherent gap between different 'abstraction levels of the computer and information system semantics', and accordingly, between the security solutions on these levels. Specifically, for an intrusion, "damage can be identified at the business process level, application/service level, operating system object (file or process) level or instruction level (memory unit, instruction, register and disk sector). System experts exactly know which file is stolen or modified, but they hardly know how this can impact the business level. On the other hand, business managers can rapidly notice a suspicious financial loss, but they won't relate it to an un-allowed system call parameter inside the operating system" [9]. Pioneering work has been done in [9] and in follow-up work [4-8] to demonstrate that big-picture cyber awareness cannot be achieved unless this isolation is broken.

As a foundation for workforce development, cybersecurity curricula continue to expand to incorporate emerging topics and necessary critical knowledge units. The 'isolation problem,' in the context of current cybersecurity curricula, refers to the topic-by-topic coverage of security knowledge units which results in isolation between knowledge units, as well as between perspectives/views. The consequences are twofold: 1) students can be trapped in microscopic perspectives (usually bound to what a security tool shows, like the intrusion detection system), and unable to extend the findings to reveal more, failing to gain big picture awareness of the situation in a target attack scenario; 2) students can be biased to technical perspectives and unable to communicate well with others who hold different perspectives, such as business managers or clients.

Our observations were strongly underscored at a February 6, 2015 on-campus cybersecurity symposium, by an Federal Bureau of Investigation (FBI) agent who was supervising a new cybersecurity graduate and said of cybersecurity graduates in general, "They are confined [with]in techniques." The agent explained that students with computer science or computer engineer backgrounds are mostly trained to be good at technical investigation, but lack the awareness and capabilities to correlate their investigation outcomes to the mission impact analysis. According to the agent, students may be good at digging into individual intrusion symptoms or evidence, but they cannot write their findings into a comprehensive report or communicate well with their supervisors or clients. We have noted that the agent's perspective seems to be shared by other experts and even by students themselves. For example, after a regular computer forensics training, one student observed, "I now know well the steps to use the techniques and tools, but I still could not imagine how they can help with the real-world incident investigations." In response to such observations and concerns, this paper offers a solution to the 'isolation problem' in cybersecurity curriculum.

B. Objectives and Benifits

This paper aims to solve the 'isolation problem' in cybersecurity curriculum. Specifically, we propose the new philosophy to deliver suites of teaching modules that can be

978-1-5386-1174-6/18/$31.00 ©2018 IEEE

used separately or as a whole in a typical network security course. These units will help students form knowledge networks instead of isolated conceptual knowledge units, learn how to leverage knowledge to gain cyber situation awareness (e.g., mission impact and damage assessment) based on intrusion symptoms, and move beyond the microscopic points of view rendered by some existing security tools. This paper fits well into the spirit of NICE (National Initiative for Cybersecurity Education) Cybersecurity Workforce Framework (NCWF) [11] for developing materials for the following areas: 1) cyber threats and vulnerabilities; 2) network security methods; 3) cybersecurity principles.

In contrast to traditional cybersecurity teaching strategies, we aim to design the proposed curriculum with the following four unique features: 1) the modules are drawn based on **emulation of real-world security incidents**; 2) the methodology is designed to **break isolation** between different knowledge units; 3) the approach promotes the practicing of **communication/presentation skills** based on the inter-connection between different (i.e., business versus technical) perspectives; 4) the outcomes include **visualizations** to help students build their conceptual mental models.

The main benefit of these curricular improvements will be **better cybersecurity workforce development, specifically the production of graduates who are more career-ready, due to being more skilled with logical inference and cross-perspective communication**. These skills will be especially beneficial for those graduates who will enter government positions with organizations such as the National Security Agency (NSA) and FBI, including those enrolled in the NSF SFS (National Science Foundation Scholarship for Service) program.

C. Overview

This paper offers a new style of cybersecurity education labeled 'situation awareness-oriented' education, in response to the overly 'technique-oriented' nature of the traditional approach. By 'technique-oriented' we refer to the observed teaching philosophy in cybersecurity education that focuses primarily on training students to grasp specific, isolated techniques via various security labs. Within this paradigm, students do not get a chance to practice how the different techniques may be combined to analyze a real security incident, and what they gain remains at the level of isolated knowledge units. In contrast, the proposed 'situation awareness-oriented' curriculum will allow students to learn key cybersecurity techniques and also apply them in combination to analyze a real or emulated security incident. The proposed curriculum will also train students to effectively connect technical with business perspectives and communicate effectively with those coming from business perspectives, further responding to limitations of traditional cybersecurity curricula.

The curriculum developed using the proposed new philosophy will draw attack scenarios, business workflows, vulnerability exploitations, etc. from various incidents, and incorporate them into suites of modules, with each suite corresponding to one incident. The learning artifacts presented to students will not be individual labs, but rather, chained modules (including interactive hands-on labs) that together reveal the attack motivations, cyber contexts and intrusion symptoms of a security incident. Students will not be merely required to leverage various techniques and tools to complete individual modules, but will be further required to connect them logically to infer the ground truth and gain big picture awareness of the cyber situation. As a result of these advances as well as improvements in communication instruction, graduates trained on the proposed curriculum will be much more career-ready than those in traditional programs. Our proof-of-concept data and results show that the proposed idea is highly feasible.

II. Related Work

A. Cybersecurity Curriculum Developments

A representative of the relevant work of this paper is the recent cybersecurity curriculum development program initiated by National Security Agency (NSA) [15][19], which is a set of fifty-four cybersecurity curriculum development projects with merits in different aspects. For example, SEED labs provide a *virtual attack environment*, covering "some of the most common vulnerabilities in general software", and make the environment portable based on virtual machine image and open to the community for practical usage in cybersecurity education [16]. Labtainer provides a docker-based "*framework* to simplify creation, deployment, and assessment of stand-alone cyber security lab exercises, intended for use on individual student computers" [17]. ctf.0xEvilC0de.com develops a jeopardy style no-cost Catch the Flag (CTF) *platform* [18]. Others mainly expand the cybersecurity curriculum *materials* to cover more topics or areas, such as SCADA, IoT, blockchain, reverse engineering, digital forensics, malware, vulnerabilities, cloud, cellular and wireless/mobile network, privacy, crypto, risk, cyber security principles, secure software or design, secure programming, game theory, competency, HCI, etc. [19]

The NSA cybersecurity curriculum development initiative is not the only effort in the frontiers of cybersecurity education. There are a number of platforms developed to emulate the multi-step real-world incidents/attacks, such as the various cyber ranges which are built as virtual environment for cyber warfare training or technology development. Particular examples include the Class Capture-the-Flag Exercises of the DETER project [21], EDURange by Evergreen State Colleague [22] or Virginia Cyber Range [23], etc.

Different from all the above efforts for curriculum development or platform building, this paper is promoting a new *philosophy* for cybersecurity curriculum development and education practice. That is, based on the observations and outcomes (such as the SKRM model) of research papers [4-6][8-9], cybersecurity analysts are usually bound to what their security tool, e.g., intrusion detection system, shows, and need to learn how to leverage knowledge to gain cyber situation awareness (e.g., mission impact and damage assessment) based on intrusion symptoms. Based on real-world incidents that will provide background and context, the modules

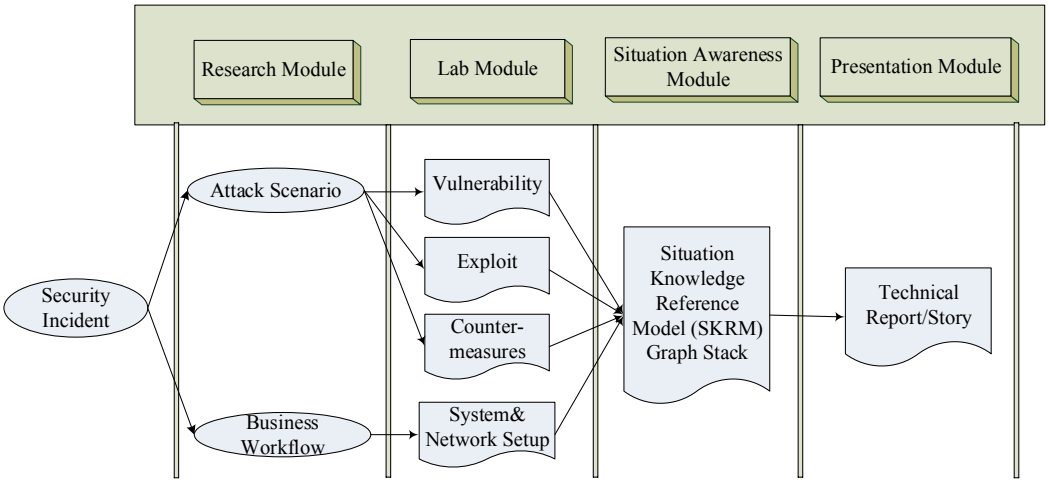

Fig. 1. General organization of a module suite

developed under the situation awareness-oriented paradigm will enable students to assess the attacks' motivations, cyber contexts and intrusion symptoms.

The methodology of this paper can be a support to implement and evaluate ISO/IEC 27001:2013 (ISO 27001) in work environment, which is "the international standard that describes best practice for an ISMS (information security management system)" [20].

B. Situation Knowledge Reference Model (SKRM)

As pointed out above, a core engine is needed to enable the interconnection and visualization of different perspectives, so we adopt a new cross-layer model called a "Situation Knowledge Reference Model" (SKRM) proposed in [9]. This paper calls for efforts from cybersecurity researchers across diverse backgrounds and expertise, to further apply this insight and redesign cybersecurity education to be friendlier to career-ready workforce development.

Illustrating the levels of situation knowledge and the perspectives required to analyze and profile an enterprise-level network, an SKRM is a cross-layer model integrating, from top to bottom, a *Workflow Layer*, *App/Service Layer*, *Attack Graph Layer*, *Operating System Layer* and *Instruction Layer*. See Table I for node, edge and perspective details and Fig. 2 for a sample SKRM-enabled graph stack [9]. Each layer represents a situation perspective (see Table I). The main features of the SKRM model [9] are duplicated below, and detailed definitions of layers, nodes and edges are elaborated in [9].

- "Each layer generates a directed graph, and each graph covers the entire enterprise network.
- Cross-layer relationships are captured. The individual graphs are interconnected to become a graph stack.
- The graph stack enables both intra-layer diagnosis and cross-layer analysis.
- Each layer is a view of the same network from a different perspective and thus at a different granularity.
- Isolated perception that is gained at different layers/granularities is integrated into a more comprehensive, scalable system to support higher levels of Situation Awareness.
- Higher levels of situation awareness lead to comprehension, projection and resolution." [9]

III. APPROACH

The proposed new approach of cybersecurity curriculum development will carefully pick notorious real-world security incidents and leverage their anatomy profiles (vulnerability, exploits and violated cybersecurity principles) as basic materials, integrating interactive labs, visualizations and presentations. This way, concepts are introduced with applied contexts and scenarios, and labs and concepts will have concrete examples as backgrounds. Students are familiar with such real-world security incidents through news and research, and this familiarity will help them to connect to the material and understand how technical and business elements are correlated, specifically how an intrusion incident changes business workflow and incurs business damage and loss. Students will also find such entry points accessible and intriguing. Recent cybersecurity incidents provide numerous appealing candidates for inclusion, such as the 2013 Target financial data leakage, 2014 OpenSSL Heartbleed attack, 2015 iOS App XcodeGhost infection, 2016 dirty COW attack, 2017 WannaCry ransomware attack, etc.

Fig. 1 illustrates the general organization for a module suite, which our approach suggests to develop for each real-world security incident to be emulated. Each suite will include a Research Module, Lab Module, Situation Awareness Module (with a Situation Knowledge Reference Model (SKRM) graph stack as its visualization outcome), and Presentation Module. The SKRM graph stack bridges different perspectives by mapping between multiple fine-grained layers, and helps students extend their findings to other parts of the business workflow, ultimately allowing them to approach big picture situation awareness far beyond individual and isolated security breakpoints.

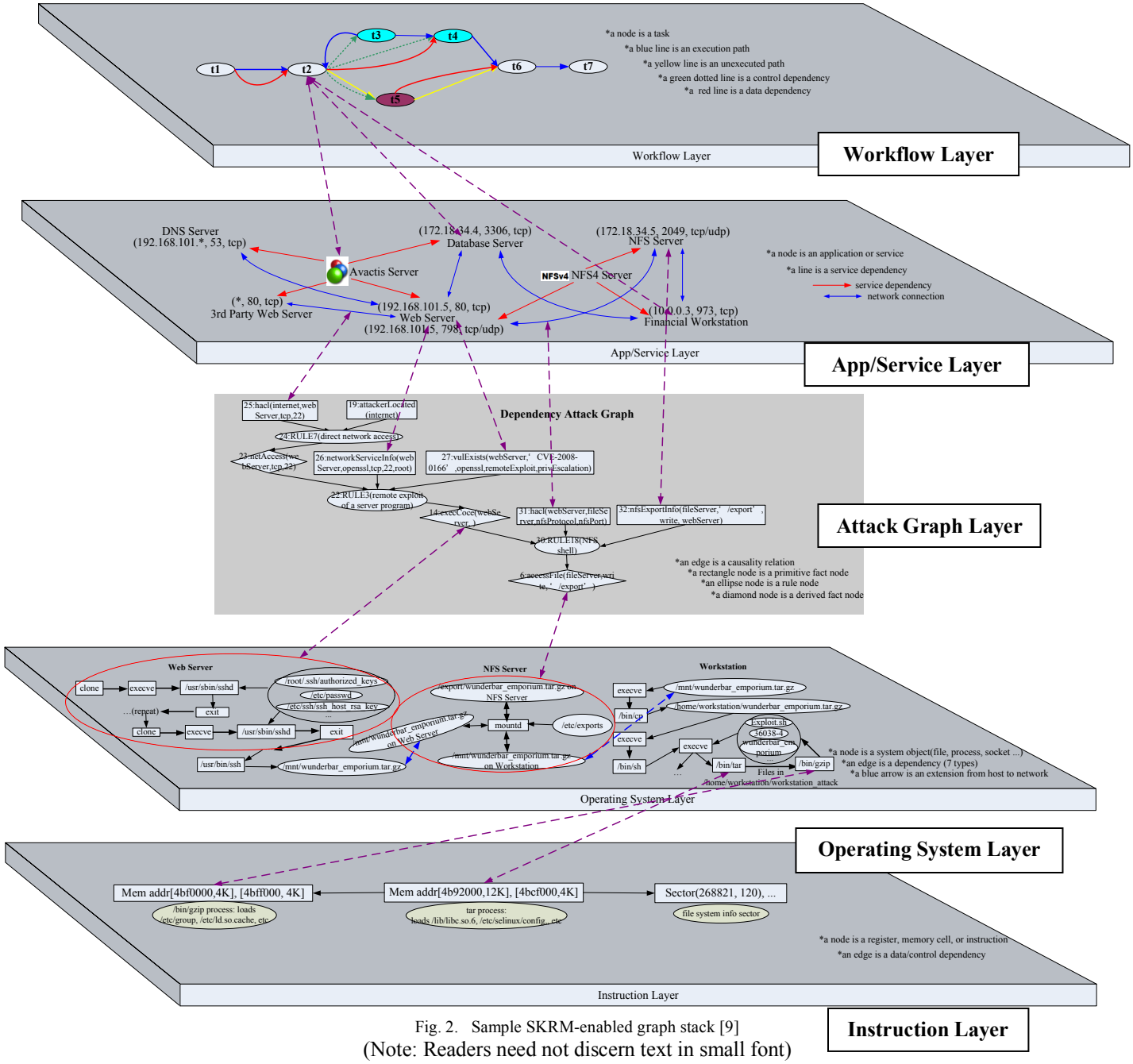

Fig. 2. Sample SKRM-enabled graph stack [9]
(Note: Readers need not discern text in small font)

Also in contrast to traditional cybersecurity education, the SKRM-enabled interconnection and visualization proposed here will give students excellent practice in research and communication/presentation skills. This will not only promote deep conceptual understanding, but also better prepare students to apply their knowledge quickly when investigating real-world incidents.

The developed materials will be of great use to the cybersecurity education community because any existing network security course could incorporate them without modification, as they will be modular and the instructor could flexibly choose to add one or more suites of modules to satisfy their own needs.

To elaborate on the core approach of this paper illustrated in Fig. 1, the Research Module mainly has students working with supporting materials that can be obtained through search engines or academic queries. During class time, the instructor can guide students to search for the supporting materials by themselves before directly disseminating the instructor-prepared ones. This will help students investigate incidents independently in the future. The Research Module includes at least an attack scenario and business workflow.

TABLE I. DETAILS OF SKRM LAYERS

SKRM Layer	Node	Edge	Perspective
Workflow Layer	Task	Data/Control Dependency	Business
App/Service Layer	Application/Service	Service Dependency/ Network Connection	Service
Attack Graph Layer	Network Reachability/ Host Configuration/ Vulnerability Existence	Causality Relations	Analysis
Operating System Layer	System Object (Process/File/Socket)	Data/Control Dependency	System
Instruction Layer	Instruction/Register/ Memory Cell	Data/Control Dependency	Instruction

TABLE II. SAMPLE SUITE OF MODULES CORRESPONDING TO FIG. 2'S SKRM

Research Module	Fig. 3
Lab Module	Lab: OpenSSL brute force key guessing attack (vulnerability: CVE-2008-0166)
	Lab: NFS mount misconfiguration
	Lab: NULL pointer dereference attack via bypassing *mmap_min_addr* (vulnerability: CVE-2009-2692) hours)
	Lab: symbolic race condition attack (vulnerability: CVE-2011-4089)
	Lab: network and system setup of a testbed for web-shop
Situation Awareness Module	Fig. 2
Presentation Module	Story: how a non-member gets member service through hacking

TABLE III. MODULE DELIVERABLES AND ESTIMATED INSTRUCTION TIME

Module	Deliverable	Estimated instruction time
Research Module	Business and Attack Scenario (of the chosen intrusion incident)	Micro-module (1-4 hours)
Lab Module	Lab Instructions (scripts/commands to configure vulnerability, perform exploit and do counter-measure analysis)	Nano-module (up to 1 hour) or Micro-module (1-4 hours)
Situation Awareness Module	A Stack of Graphs (from different technique/tools/perspectives)	Module (4-10 hours)
Presentation Module	Oral Presentation and Writing Instructions	Micro-module (1-4 hours)

The Lab Module focuses on **interactive** and **hands-on** labs on intrusion penetration, especially leveraging malware to exploit corresponding vulnerability to gain unwelcomed access and perform privilege escalation. These labs are the best hands-on time to introduce students to system and network configurations, vulnerability, malware exploits and possible countermeasures. Depending on the real-world security incident emulated, buffer overflow, cross-site scripting, SQL injection, race condition, session hijacking, etc. may be appropriately covered. In class time, the instructor can choose to do demos or provide stepwise guidance to students to perform some labs on their own. The proposed approach supports to both adopt or develop security labs in an open source way, and take advantage of various tools like MulVAL [10], Patrol [8] and ZePro [5] to gain visual display and analysis within the labs.

The Situation Awareness Module leverages a Situation Knowledge Reference Model (SKRM), described in detail in Section III.B., as the engine to cover, interconnect and visualize all the relevant knowledge units. The SKRM model is proposed in [9] and semi-automated in follow-up work [4-8]. The Situation Awareness Module will take the outcomes (mainly in the form of graphs, such as a network topology graph and attack graph [10]) of the Lab Module as inputs, and integrate them into a graph stack. The wide technical community has already contributed various open-source tools to generate system object dependency graphs [5][8], and SKRM as a reference model guides to identify tools and methodologies that generate graphs to best visually represent different respective (business or technical) views, and instructors can do most of work needed to prepare solutions that interconnect those graphs/perspectives ahead of class time. In class, the students will spend most of their time during this module mapping elements between different SKRM layer graphs, with the individual layer graphs prepared for them. Completing this task by focusing on obtaining visual graphs, after having already completed the hands-on labs, will help students gain a better conceptual understanding than provided by traditional cybersecurity training.

The Presentation Module develops students' ability to describe, using an oral presentation and/or written report, the situation knowledge that they gained around a given incident based on integration of technical findings and business scenarios/workflows. During class time, the instructor can interact with students, offering them options for describing the situations or pointing out ways to improve their descriptions. The SKRM-enabled interconnection and visualization helps presenters organize clear, concise, complete and logical plain-language descriptions of the incidents, incorporating the necessary and professional terminologies. The SKRM graph stack's cognition-friendly nature also facilitates audience comprehension of the oral or written presentations.

IV. Proof of Concept

The sample SKRM graph stack in Fig. 2 is based on proof-of-concept data collected from an emulated intrusion incident shown in [8-9] towards a web shop hosted in a test-bed, i.e., a 3-step attack to get member service from the web shop as a non-member. Fig. 3 gives the attack scenario corresponding to Fig. 2 [8]. Although the experiment and data are preliminary, they show the feasibility of generating a suite of modules depicted in Fig. 1 and validate the idea of this paper.

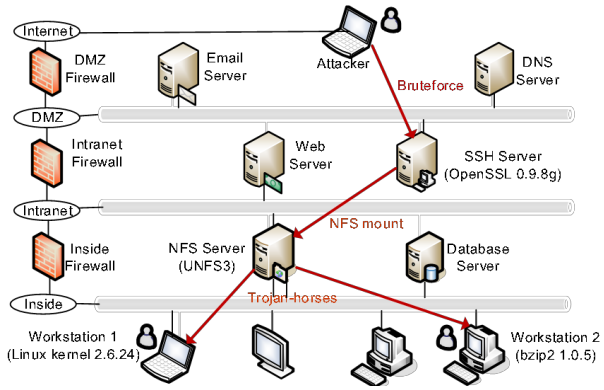

Fig. 3. Sample attack scenario corresponding to Fig. 2's SKRM [8]

Table II specifies the suite of modules that we generated for the specific situation illustrated in Fig. 2 and 3. Five labs were created based on either the cyber-attacks involved (made up of the corresponding vulnerability, exploits and potential counter-measures) or the system/network setups (made up of the various user-land or kernel service configurations). Such labs are hands-on examples of studying the CAE core or optional knowledge units, such as Information Assurance Fundamentals and Network Security Administration. Furthermore, these labs are not presented as isolated units for understanding and practicing individual concepts. Rather, they are put in an integrated way to tell the whole attack story with enriched cyber contexts, which greatly enhances student understanding of the intrusion motivations, step-wise penetration steps and potential intrusion symptoms. All such elements are important sources of experience in becoming a well-trained cybersecurity analyst, but they are not seen in existing cybersecurity lab design. The process used to generate these test modules is expected to apply easily to other real-world security incidents as well.

A. *Multiple-Step Attack: Chained Lab Modules*

The lab modules listed in Table II are actually corresponding to the **various steps of a multiple-phase attack**, which is depicted in Fig. 3, an attack scenario borrowed from [8].

It is very changing and almost unlikely that an attacker can directly break into the final target. Instead, the attacker has to jump over several stepping stones one by one before (s)he reaches the final target machine. The multiple steps of the attack form a so-called attack path, and the exploits along the attack path contributed to the **chained** lab modules.

Specifically, in our proof of concept, the first exploit converted into a lab is a *brute-force key guessing attack* (CVE-2008-0166) towards an SSH Server located in DMZ, via which the attack could gain root-privilege access control over the SSH Server, by taking advantage the pseudo-random number generation vulnerability within the OpenSSL 0.9.8c-1 up to versions before 0.9.8g-9 on Debian-based operating systems [12]. The second exploit is an *NFS mount misconfiguration* due to the wrong permission setting on an intranet-public directory, i.e. /exports, which allows follow-up trojan-horse file uploads [10][8]. The third exploit is a *NULL pointer dereference* (CVE-2009-2692) which bypasses mmap_min_addr to get the code placed on page zero executed, to create an unknown account on victim machine for the attacker [13]. The fourth exploit is a *symbolic race condition* (CVE-2011-4089), which misleads the victim machine to run malicious code for privilege escalation. The fifth lab is network and system setup working as a production environment, meanwhile enabling all the above vulnerabilities. For each of these labs, students will get to learn why the victim system is vulnerable, how the vulnerability could be exploited, what impact the exploitation may generate, and what countermeasures can be leveraged to defend. Moreover, students get to learn the **chain effect** of all the attacks put together.

B. *Stacked SKRM Graphs*

To help students digest the involved security concepts and extend their understanding, the spirit of the SKRM engine is to **visualize** the network and system entities in a stack of graphs. For example, Fig. 4, the outcome of [8] using a system called Patrol to monitor the victim systems under attack, visualizes the chained attacks described above at the Operating System Level, during which each file is an ellipse node, each process is a rectangle node, each socket is a diamond node, and each edge denotes a dependency relationship. Fig. 4 is a part of Fig. 2, i.e. the Operating System Layer. It is supposed to map to other adjacent layers, as guided by the SKRM-enabled cross-layer diagnostics [9], helping students to gain bigger-picture awareness of the attack's workflow-level impact, service-level damage and instruction-level taint. Such **wholistic** view also help students complete writing and presenting the incident, to audience from various backgrounds, such as business, service, system, network, hardware, security, etc.

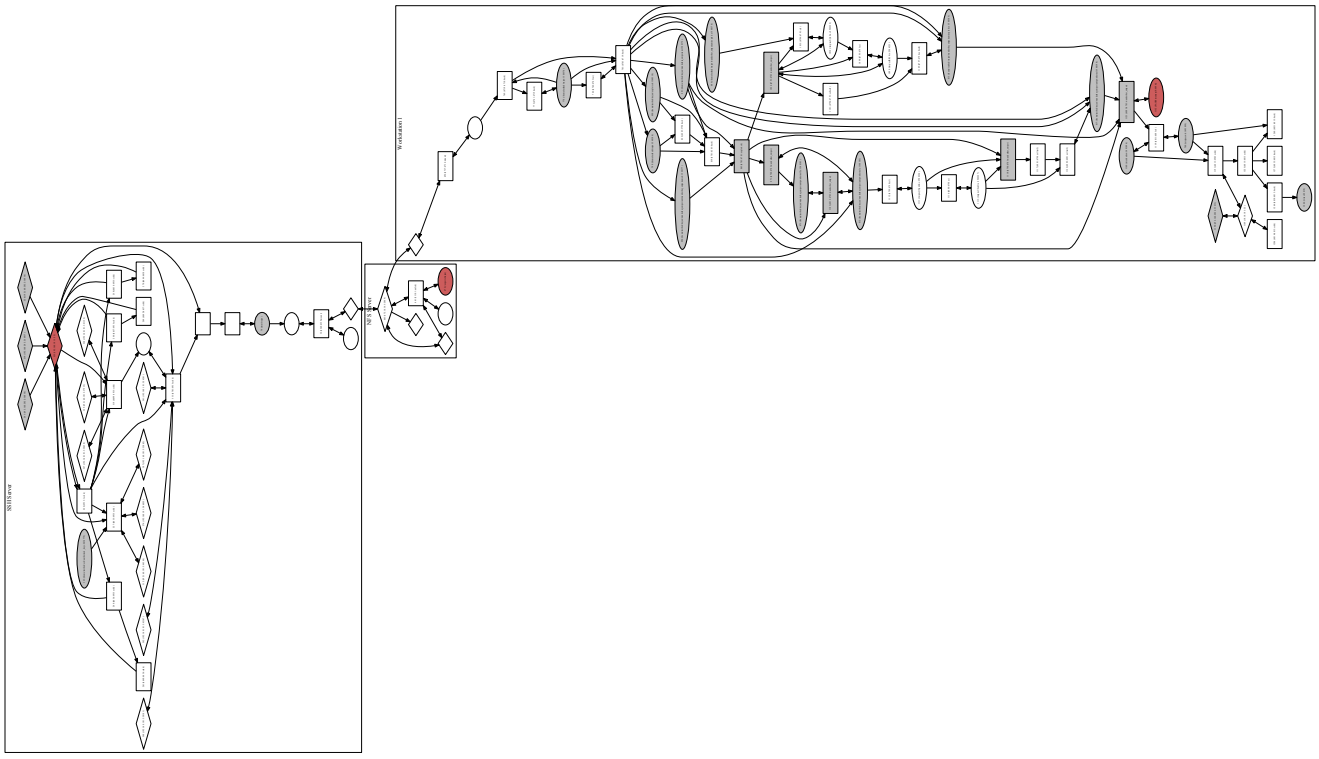

Fig. 4. Sample SKRM Graph to visualize chained attacks at Operating System Level [8]

(Note: Readers need not discern text in small font)

C. Deliverables

Table III shows the deliverables of the developed curriculum items under the situation awareness-oriented philosophy. As you can see, there are different types of deliverables which vary by time: *modules* (4-10 hours), *micro-modules* (1-4 hours), and *nano-module* (up to 1 hours). This design is in alignment with the requirement of the NSA Cybersecurity Curriculum Development Project 2017 [15]. The modules can be adopted separately or as a whole in any typical network security course.

V. Conclusion

This paper presents a new methodology in cybersecurity education: situation awareness-oriented curriculum development and practice. Different from traditional methodologies, this one targets to break the isolation of different knowledge units and lab practices. It adopts an outcome in cybersecurity situation awareness research, i.e. the Situation Knowledge Reference Model (SKRM), as engine to guide the development of chained hands-on cybersecurity modules based on real world multiple-step attacks. This helps students to gain big picture comprehension and build a knowledge network instead of isolated conceptual knowledge units. It also enables better cybersecurity workforce development, specifically the production of graduates who are more career-ready, due to being more skilled with logical inference and cross-field communication.

References

[1] M. Bishop, J. Dai, M. Dark, I. Ngambeki, P. Nico and M. Zhu. "Evaluating Secure Programming Knowledge." WISE 10, 2017.

[2] C. Li, B. White, J. Dai, C. Zhang. "Enhancing Secure Coding Assistant with Error Correction and Contract Programming." National Cyber Summit 2017.

[3] B. White, J. Dai, C. Zhang. "Secure Coding Assistant: Enforcing Secure Coding Practices Using the Eclipse Development Environment." National Cyber Summit 2016.

[4] X. Sun, J. Dai, P. Liu, A. Singhal, J. Yen. "Using Bayesian Networks to Fuse Intrusion Evidences and Detect Zero-day Attack Paths." Book chapter in Springer LNCS volume "Network Security Metrics and Applications", 2017.

[5] X. Sun, J. Dai, P. Liu, A. Singhal, J. Yen. "Towards Probabilistic Identification of Zero-day Attack Paths." IEEE CNS 2016.

[6] X. Sun, J. Dai, A. Singhal, P. Liu. "Enterprise-level Cyber Situation Awareness." Book chapter in Springer LNCS volume "Recent Advances in Cyber Situation Awareness", 2015.

[7] X. Sun, J. Dai, A. Singhal, P. Liu. "Inferring the Stealthy Bridges between Enterprise Network Islands in Cloud Using Cross-Layer Bayesian Networks." SecureComm 2014.

[8] J. Dai, X. Sun, P. Liu. "Patrol: Revealing Zero-day Attack Paths through Network-wide System Object Dependencies." ESORICS 2013.

[9] J. Dai, X. Sun, P. Liu, N. Giacobe, "Gaining Big Picture Awareness through an Interconnected Cross-layer Situation Knowledge Reference Model." ASE/IEEE Cyber Security 2012.

[10] X. Ou, S. Govindavajhala, A. W. Appel, "MulVAL: A logic-based network security analyzer," USENIX Security, 2005.

[11] NICE Cybersecurity Workforce Development: https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework.

[12] CVE-2008-0166. http://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2008-0166.

[13] CVE-2009-2692. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2692.

[14] CVE-2011-4089. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-4089.

[15] NSA Cybersecurity Curriculum Development Project 2017: https://niccs.us-cert.gov/featured-stories/call-cybersecurity-curriculum-development-grant-proposal.

[16] SEED Labs: http://www.cis.syr.edu/~wedu/seed/labs.html.

[17] Lab Irvine, C.E., Thompson, M. F., and Khosalim, J., "Labtainers: A Framework for Parameterized Cybersecurity Labs Using Containers", National Security Summit, 2017.

[18] J. Stroschein. Development of a custom CTF Framework. https://ctf.0xevilc0de.com/.

[19] Curriculum on Display. Cyber Ed Workshop 2018. http://cis1.towson.edu/~cyber4all/index.php/cybered-2018/.

[20] ISO/IEC 27001:2013 (ISO 27001), the international information security standard. https://www.itgovernance.co.uk/iso27001.

[21] J Mirkovic and P. Peterson, "Class Capture-the-Flag Exercises-The Deter Project", in 3GSE, 2014.

[22] Edurange: A Cybersecurity Competition Platform to Enhance Undergraduate Security Analysis Skills. https://sites.evergreen.edu/edurange/.

[23] Virginia Cyber Range. https://virginiacyberrange.org/.