MAY 2016 // VOLUME 112 // NUMBER 2

THE BRIDGE

The Magazine of IEEE-Eta Kappa Nu

CYBERSECURITY

Cyber-Physical Security Assessment (CyPSA) for Electric Power Systems

Security Analytics: Essential Data Analytics Knowledge for Cybersecurity Professionals and Students

A Brief Review of Security in Emerging Programming Networks

IEEE-HKN AWARD NOMINATIONS

As the Honor Society of IEEE, IEEE-Eta Kappa Nu provides opportunities to promote and encourage outstanding students, educators and members.

Visit www.hkn.org/awards to view the awards programs, awards committees, list of past winners, nomination criteria and deadlines.

Outstanding Young Professional Award
Presented annually to an exceptional young professional who has demonstrated significant contributions early in his or her professional career. (Deadline: Monday after April 30)

Vladimir Karapetoff Outstanding Technical Achievement Award
Recognizes an individual who has distinguished themselves through an invention, development, or discovery in the field of electrical or computer technology. (Deadline: Monday after April 30)

Alton B. Zerby and Carl T. Koerner Outstanding Student Award
Presented annually to a senior who has proven outstanding scholastic excellence, high moral character, and exemplary service to classmates, university, community and country. (Deadline: 30 June)

Outstanding Chapter Award
Singles out chapters that have shown excellence in their activities and service at the department, university and community levels. Winners are determined by their required Annual Chapter Reports for the preceding academic year. (Deadline: 30 September)

C. Holmes MacDonald Outstanding Teaching Award
Presented annually to a dedicated young professor who has proven exceptional dedication to education, and has found the balance between pressure for research and publications, classroom enthusiasm and creativity. (Deadline: Monday after 30 April)

Distinguished Service Award
Presented annually to recognize those members who have devoted years of service to the society, resulting in significant benefits to all of the Society's members. (Deadline: Monday after 30 April)

IEEE-Eta Kappa Nu (IEEE-HKN) was founded by Maurice L. Carr at the University of Illinois at Urbana-Champaign on 28 October 1904, to encourage excellence in education for the benefit of the public. IEEE-HKN fosters excellence by recognizing those students and professionals who have conferred honor upon engineering education through distinguished scholarship, activities, leadership, and exemplary character as students in electrical or computer engineering, or by their professional attainments. THE BRIDGE is the official publication of IEEE-HKN. Ideas and opinions expressed in THE BRIDGE are those of the individuals and do not necessarily represent the views of IEEE-HKN, the Board of Governors, or the magazine staff.

THE BRIDGE

The Magazine of IEEE-Eta Kappa Nu

2016 Cybersecurity

FEATURES

DEPARTMENTS

IEEE-HKN INTERNATIONAL HEADQUARTERS

Editorial inquiries: IEEE- Eta Kappa Nu, 445 Hoes Lane, Piscataway, NJ 08854, USA

US Toll Free: +1 800 406 2590 | Outside US: +1 732 465 5846 | Email: info@hkn.org | www.hkn.org

Subscription address and email changes: IEEE Contact Center US Toll Free: +1 800 678 4333 | Outside US: +1 732 981 0060

Fax: +1 732 562 6380 | Email: contactcenter@ieee.org

Our Cover

See page **5** for details about cover image

S.K. Ramesh

Lambda Beta Chapter

Phone: +1 818 677 4501
s.ramesh@ieee.org

Greetings,

Welcome to the May 2016 issue of THE BRIDGE! This year's IEEE-HKN Student Leadership Conference was hosted by the Beta Epsilon Chapter from the University of Michigan at Ann Arbor. At the annual meeting of the national ECE Department Heads Association (ECEDHA), we celebrated the 22 Outstanding Chapters from the past year with a special reception and awards ceremony. It is inspiring to note the individual accomplishments of these chapters that exemplify the best of IEEE-HKN and all that we stand for. Collectively, these Chapters reported 53,740 hours of service, which is a remarkable figure in itself, and gives you an idea of the impact that IEEE-HKN and these Chapters have had in their respective universities and communities.

Also at ECEDHA 2016, we recognized one of our illustrious Past Presidents – Thomas Rothwell (Upsilon Chapter '53, the University of Southern California) with a special recognition plaque from the Board of Governors for Tom's singular contributions in advancing IEEE-HKN. The plaque was received, on behalf of Tom, by his longtime friend and President of the Los Angeles Alumni Chapter, Mr. John DeGraw. It was fitting that President Max Nikias from USC was in the audience at the awards reception to witness the presentation. President Nikias himself was recognized later in the evening with ECEDHA's diversity award for his leadership and contributions in supporting and increasing the number of women and underrepresented minorities across USC. And last but not the least, it was a pleasure to meet and present the 2015 Alton B. Zerby and Carl T. Koerner Outstanding Student Award to Sarah Kouropis (Xi Chapter, 2015) for her very impressive contributions and academic excellence at Auburn University. It was great to meet Sarah's parents and learn that Sarah's mother is herself an IEEE-HKN member from the Beta Mu Chapter (Georgia Tech)! ECEDHA 2016 featured several interesting plenaries on the challenges with diversity in ECE education and the actions that are necessary to increase diversity going forward. Given our history, it is clear that IEEE-HKN can and will play an important role in this conversation as we look to the future.

What is the envisioned future? Our ongoing priorities are: 1) realize sustained membership growth; 2) establish financial security; 3) expand signature activities; 4) grow alumni participation; 5) integrate IEEE-HKN fully into IEEE; and 6) establish corporate partnerships. These priorities are embedded in our strategic plan, which the Board has been actively working to refine. Priorities and strategies are being reviewed and ranked. President-Elect Tim Kurzweg and I plan to have a couple of focus group breakouts during the SLC (one with students and another with faculty advisors) to gather their perspectives on our future. Ultimately, we are aiming to fully develop an "actionable" strategic plan for both the near term (3 years), and the longer term (5 years and beyond), as well as define and monitor relevant metrics for success. I am confident that IEEE-HKN has a bright future ahead thanks to all of you, and we look forward to serving you and the Society in the year ahead. Until next time,

Best wishes,

S. K. Ramesh

2016 IEEE-HKN President

Dr. Steve E. Watkins

Gamma Theta Chapter

Phone: +1 573 341 6321
E-mail: steve.e.watkins@ieee.org

Dear Eta Kappa Nu Members and Friends,

This issue of THE BRIDGE magazine has a theme of "Cybersecurity." Our guest editor, Dr. Egemen K. Çetinkaya, has provided an insightful introduction to the field with papers on security in cyber-physical systems, data analytics, and programmable networks.

An important layer of electronic security is passwords. While I understand the effort required to maintain strong, unique passwords for multiple devices, and to revise them on a regular schedule, the process is essential for protecting your systems and information from unauthorized access. However, the use of bad passwords is common, according to annual reports, and the lists of these passwords illustrate typical password mistakes. Common mistakes are passwords made from dictionary words (forward or backward), foreign words, simple keyboard sequences, and words with predictable character substitutions such as retupmoc, elektrotechnik, 1qaz2wsx, and en9in33r$, respectively. Our cover, below, shows such passwords. Is yours on the list?

A topic at our recent Student Leadership Conference was the service aspect of our organization. Our initiation ritual notes that an aspect of "character," as in HKN's membership requirements of scholarship, character, and attitude, is the willingness for service to society. Chapters that are winners of the Outstanding Chapter Activities Award frequently document a variety of service activities in their reports. Examples of these winning chapter reports are shown on the IEEE-HKN website:

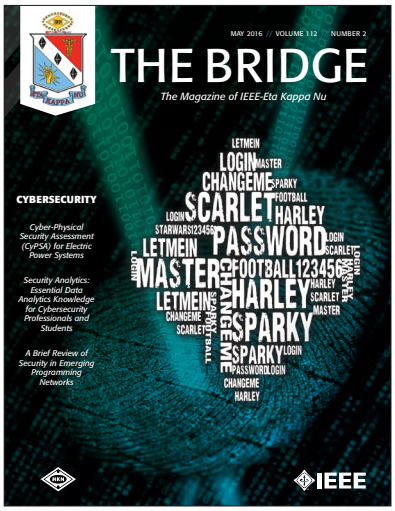
http://www.ieee.org/education_careers/education/ieee_hkn/awards/ieee_hkn_winning_chapter_reports.html

If your chapter has a notable service activity, please contact us. We would like to highlight some of these activities in future issues of THE BRIDGE.

Let us know what you think of our new format. Also, we welcome your content suggestions.

Regards,

Steve E. Watkins



▲ Poor Passwords

Nancy M. Ostin

Gamma Theta Chapter

Phone: +1 732 465 6611
Email: n.ostin@ieee.org

Dear Reader:

Thank you for opening this issue of THE BRIDGE, and for your interest in IEEE-HKN and this publication. IEEE-HKN is a unique and wonderful organization; I am proud to serve in the capacity as Director, and work with our Board of Governors, volunteers, student leaders, faculty advisors, members, and those wishing to learn more about us.

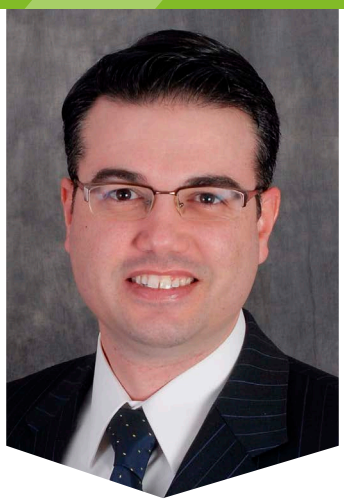
In this issue, we highlight a Chapter who ran the outreach program "Wall of Love" to benefit a local charity. This effort and the many programs run by our chapters each year, have an important impact on ALL students…IEEE-HKN, IEEE, IEEE student branches at their universities; faculty; and the community. I applaud their commitment and the number of hours spent in service to others. When we presented the Outstanding Chapter Awards for 2015, the number of service hours by our chapters was nearly 55,000 (or 2,291 days) spent on helping others. What an amazing impact IEEE-HKN students and chapters have today on the communities they serve, and on their own professional and personal development…Talk about impact!

Please join me in celebrating all that IEEE-HKN represents: Scholarship, Attitude, Character, and the unique difference our program brings to our members for the development of our future leaders, service to others, and the great history and traditions of IEEE-HKN. I personally support IEEE-HKN in both the Student Leadership Conference Fund, and our Annual Fund, because I believe in what we do and who we serve. I hope that you will consider making a gift via the IEEE Foundation.

Thank you for your support!

Sincerely,

Director, IEEE-HKN



Egemen K. Çetinkaya

Gamma Theta Chapter

Email: cetinkayae@mst.edu

Recent Advances in Cybersecurity

From the early days of simple ciphers used in hieroglyphs to the recent information leak revealed by the Snowden case, securing communication has kept many people busy. It is interesting to see how a security ecosystem involves such a variety of competing players aiming for different objectives. The recent Cybersecurity National Action Plan, which was released on February 2016, is the latest news presenting how serious the US government takes the cybersecurity environment[1]. However, despite numerous efforts, we still lack tools and a deep understanding on how to secure our communication[2].

This special issue on cybersecurity contains three invited papers. In the first paper, titled "Cyber-Physical Security Assessment (CyPSA) for Electric Power Systems," Katherine R. Davis et al. present a novel framework that evaluates the security of interdependent cyber-physical systems. The second paper, "Security Analytics: Essential Data Analytics Knowledge for Cybersecurity Professionals and Students," by Rakesh Verma et al., describes important skills and knowledge base necessary for those who work in the field of data analytics security. This paper is a reprint and was originally published in IEEE Security & Privacy Magazine, Volume 13, Issue 6, pp. 60 – 65, 2015. The last paper, "A Brief Review of Security in Emerging Programmable Computer Networking Technologies," by Egemen K. Çetinkaya, presents a brief survey of security in emerging programmable networks, including cloud computing, fog computing, software-defined networks, and network function virtualization environments.

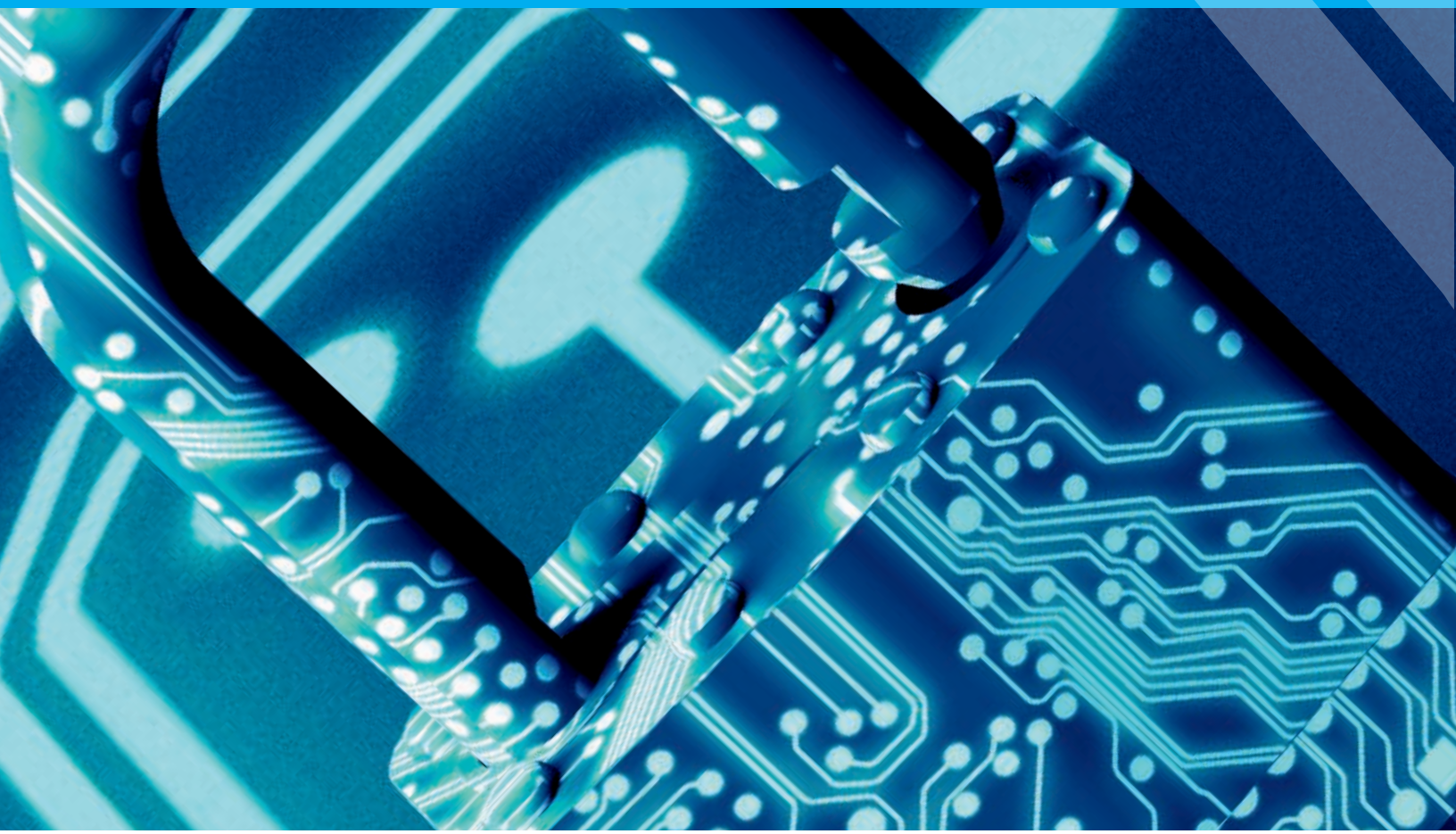
I hope that the readers will find this issue interesting and exciting. I would like to thank the reviewers for timely delivery of insightful reviews. Moreover, I express special thanks to Prof. Steve E. Watkins, Editor-in-Chief of IEEE-HKN's THE BRIDGE Magazine for his support in preparing this special issue on cybersecurity.

Sincerely,

Egemen K. Çetinkaya

[1] https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan

[2] http://web.cs.ucdavis.edu/~rogaway/papers/moral.html



Cyber-Physical Security Assessment (CyPSA) for Electric Power Systems

Katherine R. Davis, *Member, IEEE,* Robin Berthier, Saman A. Zonouz, *Member, IEEE,* Gabe Weaver, Rakesh B. Bobba, Edmond Rogers, Peter W. Sauer, *Life Fellow, IEEE,* David M. Nicol, *Fellow, IEEE*

Abstract

The electric power grid's day-to-day operations and functionality rely on a vast network of computers or cyber infrastructure. The cyber infrastructure is an unseen backbone of power system operations. Measurements and commands are relayed over a communication network connecting computers in the control room to a vast number of devices in the field. This article introduces the Cyber-Physical Security Assessment (CyPSA) framework and toolset: a security-oriented analogy to real-time contingency analysis that will identify the most critical cyber assets and attack paths with the potential for severe physical impact.

Index Terms—Cyber-physical systems, cyber security, contingency analysis, operational reliability, attack trees, cyber-physical topology.

I. INTRODUCTION

THE integration of cyber communications and control systems into power grid infrastructures is widespread and can have a profound impact on the operation, reliability, and efficiency of the grid. While cyber technologies allow for efficient management of the power system, they may contain vulnerabilities that need to be managed. One important possible consequence is the introduction of cyber-induced or cyber-enabled disruptions of physical components. Presently, the cyber infrastructure and the impact of any failures or compromises in the cyber system are hidden from the power system operators and planners.

This article introduces the Cyber-Physical Security Assessment (CyPSA) framework, a security-oriented analogy to real-time contingency analysis that will identify the most critical cyber assets and attack paths with the potential for severe physical impact. CyPSA, an evolution of the CPMA framework [1], is an online framework that allows stakeholders to assess the operational reliability impacts due to threats to the cyber infrastructure of power systems. This framework is an important step towards addressing the critical challenge of understanding and analyzing complex cyber-physical systems at scale. We build upon [1] to describe the current working characteristics of the CyPSA framework and toolset.

Utilities already assess the state of the power system to plan against events. This is the traditional contingency analysis; we extend that concept to cyber. What if an organization could predict, not only what the operational reliability impact would be of a cyber outage, but also what the most critical components are that need to be protected? A critical part of cyber-physical contingency analysis is understanding how the electrical network and its communication networks are connected and being able to model those interactions. A cyber-physical power grid model comprises the full-topology physical power system and the cyber systems connected with its operation. Our model maps the points of interconnection between the cyber and physical systems, allowing CyPSA to determine what physical actions are possible from any given host in the cyber network. Using power system models, cyber system models, threat models, real-time alert information, and our ranking algorithm, the CyPSA framework implementation provides a way to manage the input data, preform the security-driven operational reliability analysis, and present the results in a meaningful way.

CyPSA manages the data to inform system operators of outages that may be more likely, due to cyber connectivity. This information also informs system managers of what the most vulnerable portions of their systems are and what components and paths are most critical to protect. Our analysis adds the ability to use information such as access control policies, device type, and a database of known vulnerabilities to identify contingencies that are more closely coupled than might otherwise be assumed.

II. Operational Reliability For Cyber

The concept of operational reliability (formerly called system security) and operating states were introduced decades ago to indicate the condition of a power system [2]. CyPSA extends those concepts of operational reliability to include cyber aspects. The primary goal of CyPSA is to answer the question: ***How can we preventatively operate the system such that if a cyber compromise occurs, there is no degradation of the power system operating state?*** Operational reliability assessment for cyber demands a security-oriented, physical-impact-oriented analysis framework. CyPSA emphasizes scenarios involving the organization's communications and control network, and its ability to cause physical impact.

Power system operating states. The operating states are illustrated in Figure 1. The *normal state* is often

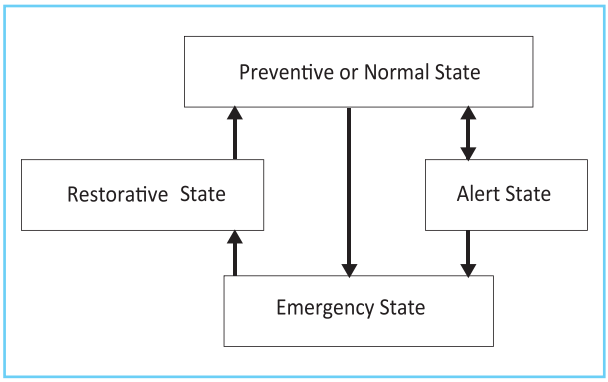


Figure 1. Power system operating states [2] [4]

This work was supported in part by the Advanced Research Projects Agency-Energy (ARPA-E), U.S. Department of Energy, under award number DE-AR0000342.
K. Davis, R. Berthier, G. Weaver, E. Rogers, P. Sauer, and D. Nicol are with the University of Illinois at Urbana-Champaign (emails: krogers6@illinois.edu, rgb@illinois.edu, gweaver@illinois.edu, ejrogers@illinois.edu, psauer@illinois.edu, dmnicol@illinois.edu). R. Bobba is with Oregon State University and S. Zonouz is with Rutgers University (emails: rakesh.bobba@oregonstate.edu, saman.zonouz@rutgers.edu).

described as a condition where all equality constraints are met, i.e., all equipment and loads are in service, and all inequality constraints are met, i.e., all equipment are within limits. The *alert state* is the condition when one or more inequality or equality constraint would be violated under the occurrence of a credible contingency, such as the loss of a line, transformer, or generator [3]. This alert state is considered "insecure" in an operational reliability sense. The operator is usually required to make dispatch or network changes to eliminate this potential violation. The *emergency state* is the condition when one or more equality or inequality constraints are violated in real time. This is an insecure state from which emergency action must be promptly taken to move the system into the restorative state and then the normal state. The *restorative state* is a time of transition to having all constraints satisfied.

III. The Use Case For CyPSA

CyPSA improves an organization's operational reliability and security posture by enabling stakeholders to evaluate and rank their system's most critical cyberphysical threats. The following two use applications of CyPSA illustrate its major use cases to extend operational reliability to include cyber.

Prioritizing N-x Contingency Analysis. Contingency elements previously considered to be independent may in reality be coupled through the cyber network and/or commonalities in software and devices. CyPSA can rank contingencies taking into account both the impact of the contingency and the cyber-exposure of the transmission line and can be used to prioritize multiple-contingency cases. For example, for an N-2 contingency criterion, double contingencies involving the most cyber-exposed line with each of the other lines could be considered first. Prioritizing the multiple-contingency cases that require attention can provide significant cost savings and help balance reliability and economical operation considerations.

Cyber-Physical Asset Ranking. CyPSA can rank both physical and cyber assets based on both their exposure to cyber attack and potential impact of their compromise on the physical system. Cyber security personnel at a utility have to prioritize their efforts due to limited resources and time constraints. While security prioritization is already practiced to an extent, it is not often informed by the significance of the asset to the physical system in any formal way. The impact of an asset that is exposed because of a new vulnerability might be low when considered individually, but if many similar assets (e.g., relays from the same manufacturer) are present in the infrastructure, the combined impact of compromising all or a subset of them is likely to be significant.

IV. CyPSA Overview

The current toolset of CyPSA can be divided into several functional blocks, as illustrated in Figure 2. Each block is responsible for a combination of specialized data handling capabilities, algorithms, and interfaces which together establish the core functionality.

In our primary CyPSA pipeline, the NP-View [5] module first analyzes the cyber network and provides connectivity information. It then works with the CyPSA Engine to analyze cyber vulnerabilities and compute potential attack paths. Then, the CyPSA Engine interacts with PowerWorld [6] to calculate performance indices for all critical assets and generates a list of cyber-physical attack paths (Section VI), ranked by a security index (Section VII). Finally, CyPSA sends the new cyber-physical attack graph results to be displayed. During online operation, the analysis is run periodically to update the results as information changes. An overview of CyPSA inputs and modules is presented next.

Cyber Topology. The cyber system model in CyPSA describes the connectivity and interactions among cyber nodes, as well as existing security mechanisms that can restrict communication between connected hosts. The control network, to the extent that it affects the operational reliability of the grid, is CyPSA's focus. This network is geographically distributed and encompasses both control center networks and substation networks.

Routers and firewalls determine which hosts on a network are able to communicate, and the model must

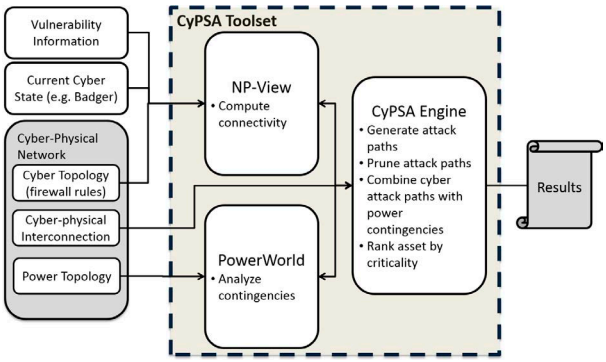
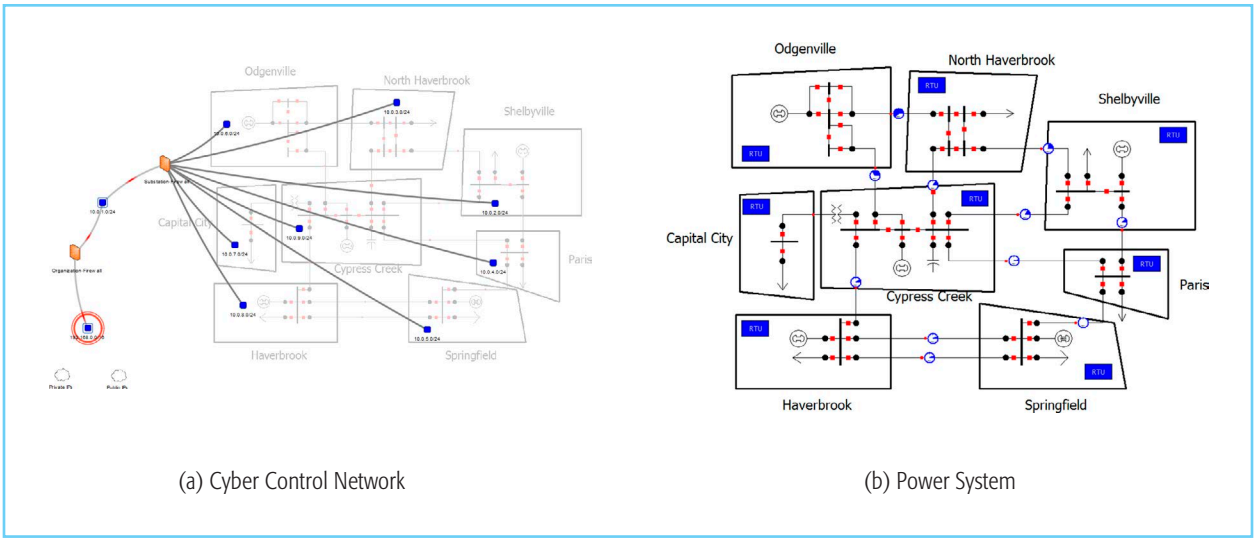


Figure 2. Overview of CyPSA



(a) Cyber Control Network

(b) Power System

Figure 3. Side-by-side views of a sample cyber-physical model as seen in NP-View and in PowerWorld Simulator

capture this logical communication paths. Building and managing cyber network models is a challenging process for an organization. CyPSA makes use of Network Perception's NP-View software [5] to automatically generate a topology map and connectivity among the cyber components of the communication network from firewall and router configurations. Tools like NP-View simplify the task of visualizing and understanding network connections as well as help organizations perform security audits.

Figure 3 shows side-by-side views of a sample cyber-physical model in both NP-View [5] (left) and PowerWorld Simulator (right) [6]. The cyber topology captures the connections to the substation RTUs allowed by the firewall rules.

Power Topology. Meaningful cyber-physical analysis requires working with the full topology representation of the system. Figure 4 shows a full breaker-level topology diagram of three substations and their connecting transmission lines, as would be used in a state estimator [7] and by CyPSA. Even in a simple model like the one

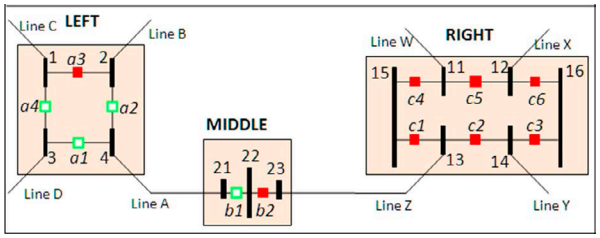


Figure 4. Line status determination from breaker status

shown in Figure 3, multiple breakers may be involved in isolating a line from the rest of the system. For example, since breaker a1, a2, and b1 are open, Line A is open. Most Energy Management Systems (EMS) have a feature to export the full topology model data in a text file format.

Cyber-Physical Interconnections Model. Measurements and controls from the SCADA system and control network map to modeled devices such as circuit breakers in the full topology model. These dependencies between the cyber system and the power system need to be represented in an interconnections model. The Cyber-Physical Topology Language (CPTL), detailed in Section V, is CyPSA's preferred approach for describing and communicating the cyber-physical interconnections data and other cyber-physical data using an open and common data model. CPTL explicitly captures the cyber model information and its connections with the power model.

These cyber-physical interconnections are critical to the analysis. As our work matures in CyPSA, we feed back into the development of CPTL with the intent that it will grow into a universal language for our industry, supported by common data formats such as JSON.

Threat Model and Vulnerability Information. In order to design and develop cyber-physical analysis tools, it is critical to understand and capture the relevant cyber-physical threats. A cyber vulnerability can compound an electrical system weakness. Cyber induced circuit breaker actions, particularly line outages, are our main

focus. Attack trees [8] can enumerate potential paths which may lead to a line outage [1], [9]. Nmap [10] scans can retrieve ports and services on devices from which CyPSA can retrieve and interpret vulnerability information and adversary cost (see Section VI).

Attack Graph Analysis. An attack graph, an extension of the attack tree concept [8], is calculated based on the possible connectivity paths among cyber components and their potential vulnerabilities. The attack graph is automatically updated when the system changes or new threat information is received (see Section VI).

Cyber Security State. Detection is an indivisible component of situational awareness. CyPSA is designed to incorporate cyber security state estimates, if such information is available. Hosts deemed compromised by the provided security state estimates are treated as an entry point for the attacker while performing cyber-physical security analysis.

Power System Analysis. Power system topology and the available power system state are used to compute the impact of contingencies such as line outages induced through cyber-attacks. CyPSA communicates with PowerWorld in real-time to obtain the operational reliability impact of critical asset outages.

Cyber Contingency Analysis. CyPSA uses information about the current security state of the cyber system, the threat model, the cyber topology, and the interdependencies between the cyber and the physical systems to assess and rank contingencies potentially induced by a cyber adversary. Cyber contingency analysis is originally proposed in [11] and has since been modified as described in Section VI of this article.

CyPSA Control Panel. CyPSA is driven through a graphical user interface (GUI) which has been designed in a web-page format and allows users such as security administrators, managers, and power engineers to interact with and visualize information from CyPSA and its components. The control panel showing asset ranking results for a fictitious 8-substation model is shown in Figure 5. The left panel is a table of the assets in the system, with properties listed for each node. On the right are three clickable tabs which show the cyber network, the power network, and the prioritized list of paths through the asset selected on the left.

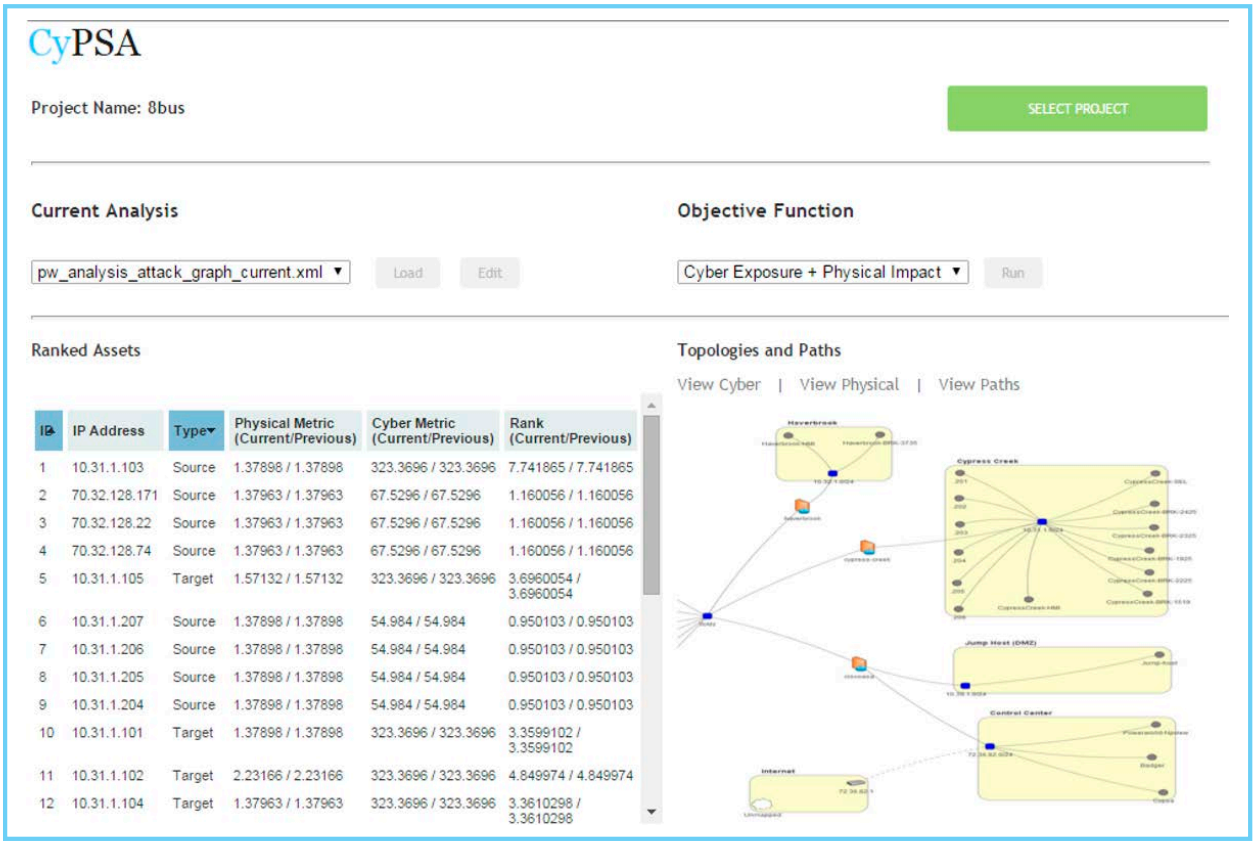


Figure 5. Control panel for asset ranking analysis

Compromise and Patching Analysis. CyPSA is powerful as a planning tool that operates on system snapshots. When used in the planning mode, a user is able to construct input scenarios and study the effect of potential changes in the network, while CyPSA updates the results and provides the ability to compare results from different analysis runs. Network changes studied may include configuration changes, vulnerability patch status changes, component security or compromised state changes to name a few.

Real-time Analysis. As the system evolves, CyPSA is designed to take into account alerts from monitoring systems and to update the cyber topology, connectivity, and power model. Asset prioritization results are updated during real-time operations to take prevailing conditions into account.

Modular Design and Interoperability. The interfaces have been designed such that each block can be developed and interacted with independently. CyPSA facilitates the integration and interchangeability of specialized software packages from different domains by using well-defined and consistent interfaces. CyPSA is designed for real-time use with existing security, operations, and asset management systems at electric utilities.

V. Inventory Management

Through interactions with utilities while developing CyPSA, we have learned that managing the asset-related information used by CyPSA is in itself an enormous challenge. The inventory management problem is compounded by the vast quantity of communications network assets at a utility. Some of these network assets interface directly with the power grid, as is the case with some protective relays. The systems are so complex and unique right now for each utility in the industry, that any improvement towards formally organizing this information will be a significant help.

Electrical power utilities have a large amount of heterogeneous types of data that includes but is not limited to node-breaker models, substation networks, and logs generated by devices. The CyPSA framework, in order to perform cyber-physical asset ranking, must be able to incorporate a wide variety of such data. The objective of the Cyber Physical Topology Language (CPTL) is to provide practitioners with a human-readable, machine-actionable language to integrate diverse data sources and to communicate such data in an open format. The long-term goal of CPTL is to enable a broad range of new research on realistic cyber-physical architectures by giving utilities, auditors, managers, and researchers a common language with which to communicate and analyze those architectures [12].

CyPSA uses CPTL to integrate information from a wide variety of data sources and subsequently present the output of analytics using a CPTL model browser, as shown in Figure 6.

A CPTL model consists of (1) a graph that captures connectivity information among assets, (2) a set of ontologies that specify the types of those assets and associated graph attributes, and (3) a mapping from concepts and roles in those ontologies to the graph [13]. CPTL implements these abstractions as (1) a JavaScript Object Notation (JSON) [14] node-link graph whose vertices correspond to assets and edges to links among those assets, and (2) a set of W3C Web Ontology Language (OWL) [15] ontologies that document a controlled vocabulary for vertex and edge attributes, including vertex and edge types. The mapping from ontology concepts and roles to the graph (component 3 of a CPTL model) is implicit in the properties associated with vertices and edges in the JSON graph.

CyPSA uses CPTL to represent connectivity information for assets within a utility's control center, substation networks, and substation yards. More information about CPTL, including open-source code and schema to represent CPTL models may be found at the CPTL repository [16].

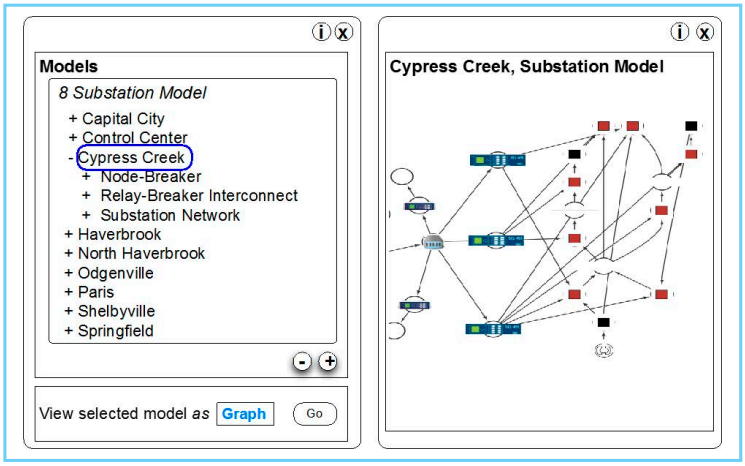


Figure 6. CPTL model viewer in CyPSA

VI. Cyber Control Network Analysis

An important contribution of CyPSA is analysis of the cyber control network and its effect on the power network in a similar manner to the look-ahead contingency studies that are done with only the power transmission network. Cyber-physical network contingency planning requires knowledge of the cyber control network connectivity and its interconnection with the physical network. In order to understand how cyber components are connected to each other, CyPSA leverages the NP-View software [5]. The software creates a logical model of the network based on the physical traffic routes and access control rules. This representation is then used to compute the connectivity among cyber components.

The connectivity is a list of possible communication paths among the different end points connected to the network. For example, a data historian that periodically receives measurement information from a SCADA controller would require a communication path. This path would be one entry in the connectivity list produced by NP-View.

A software module in CyPSA Engine called *attack graph analyzer* (AGA) combines the connectivity paths and end point vulnerability information in order to generate an attack graph. This graph combines individual paths chaining system vulnerabilities in order to produce a list of potential attack paths. For instance, an attacker compromising a VPN controller could get access to a data historian (represented as the first segment in the attack path) and then exploit a vulnerability in the data historian to gain local control and connect to a SCADA controller (represented as the second segment in the attack path).

The set of vulnerabilities depends on the versions and configurations of network assets and software. For real-time consideration of the software vulnerabilities, our solution dynamically connects to the National Vulnerability Database (NVD) portal [17] to fetch specific vulnerability information about installed software on the control network computers. This step can be performed offline when deemed necessary or at regular intervals. A cost metric associated with realizing a particular attack path is scored using the Common Vulnerability Scoring System (CVSS). A script is used to extract the exploitability sub-score using the access complexity (AC) and authentication (AU) scores from the National Vulnerability Database, as in Figure 7. The formatted CVE number identifies the vulnerability in the Common

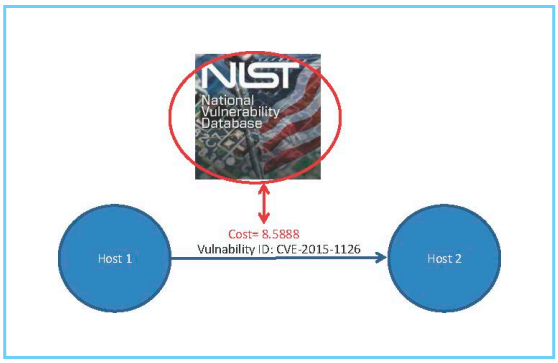


Figure 7. Vulnerability score computed through connection to the National Vulnerability Database (NVD) portal [17]

Vulnerabilities and Exposures (CVE) dictionary of publicly known information security vulnerabilities and exposures [18]. Paths between nodes that are reported in the analysis connectivity map for which we have vulnerability information are assigned with the corresponding cost. When given the complete topology and vulnerability information, AGA ensures that the generated attack graph includes *all* possible adversarial attack paths, i.e., the sequence of subsequent vulnerability exploitations.

Our solution also provides power system operators with security-oriented and proactive control network risk and impact analysis. In particular, CyPSA speculatively investigates and quantifies the impact of a particular software vulnerability exploitation (e.g., a host system compromise) or patching such that the corresponding vulnerability cannot be exploited in the future. The operators can select the list of vulnerabilities that they intend to patch, and the engine updates the previously generated attack graph accordingly (Figures 8 and 9). In particular, AGA refines the graph by pruning the nodes that are feasible only through the exploitation of to-be-patched vulnerabilities. The pruned attack graph is then used to recompute the cyber contingency analysis results.

The operators can also select a list of specific vulnerabilities or host systems to study potential exploitations. CyPSA updates the generated AGA's attack graph accordingly. It considers the compromised set of corresponding host systems as the attacker's initial point in its analyses. In the implementation, CyPSA creates a single dummy initial attack node in the AGA's graph and builds a first ε transition edge to the AGA's initial node as well as the nodes that are assumed to be compromised. The ε edge can be taken by the attacker successfully without taking any action, i.e., a no-operation action. The creation of

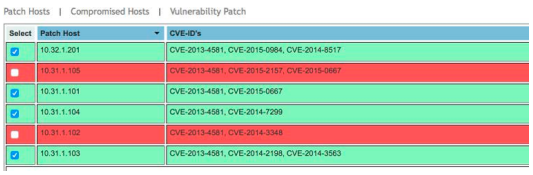


Figure 8. Selection of hosts and vulnerabilities for patching analysis

the dummy node simplifies our implementations significantly.

Consequently, CyPSA analyzes the pruned graph exploring the feasible attack paths and quantifying the negative impact on the overall system if a potential attack path is taken successfully by the adversaries. Every attack path's impact is measured as a function of how difficult the path's individual vulnerabilities are to exploit and how severe the impact of the attack would be on the underlying power system if it is carried out successfully. Specifically, CyPSA adds up the difficulty of the individual vulnerability exploitations on the attack path, and multiplies it by the power system impact measure. CyPSA applies the quantified measures to rank individual paths for the cyber-physical contingency analysis purpose (see below). The metrics can also be applied to individual assets by aggregating the costs of the paths through that asset.

VII. Physical System Impact

In CyPSA, the physical system under study has always been an electrical power system of a utility. While the transmission networks of power systems have been our focus, it is important to note that other types of cyber-physical systems (i.e., water, pipelines, etc.) at other levels of detail can also be studied in the same way. The information needed about *any* physical system under study is a mathematical model of the physical system's behavior, a method of connecting points of impact (actuators) in the physical network to the cyber network, and a common scheme for describing, sharing, and handling the information, particularly about topology and impact.

CyPSA quantifies the impact of the outage(s) on the physical system using a metric called *performance index (PI)*. The *PI* used in our studies is computed with the following equation, which measures the severity of the transmission line outages, due to an adversary following path *p(i)*, based on the subsequent line overload(s):

$$PI\left(p(i)\right)=\sum_{l\in L}\left[max\left\{\frac{f_s(l)}{f^{MAX}(l)}-1,0\right\}^2\right] \quad (1)$$

Here, L is the set of all lines, $f_s(l)$ denotes flow on line l in state s induced by adversarial actions, and $f^{MAX}(l)$ denotes the maximum flow allowed on line l. In the case of a power flow that does not solve (i.e., a blackout), a large near-infinite number is used. It is important to note that while the *PI* used here is very similar to that used in traditional contingency analysis, in principle it could be any agreed-upon metric of physical impact severity.

The attack paths are ultimately ranked based on a calculated *security index* (*SI*). AGA provides the estimated *cyber cost* (*CC*) to the adversary by summing the vulnerability scores over the assets a for each cyber path *p(i)* that leads to a critical asset (i.e., a relay that operates a circuit breaker). Multiple vulnerabilities in a

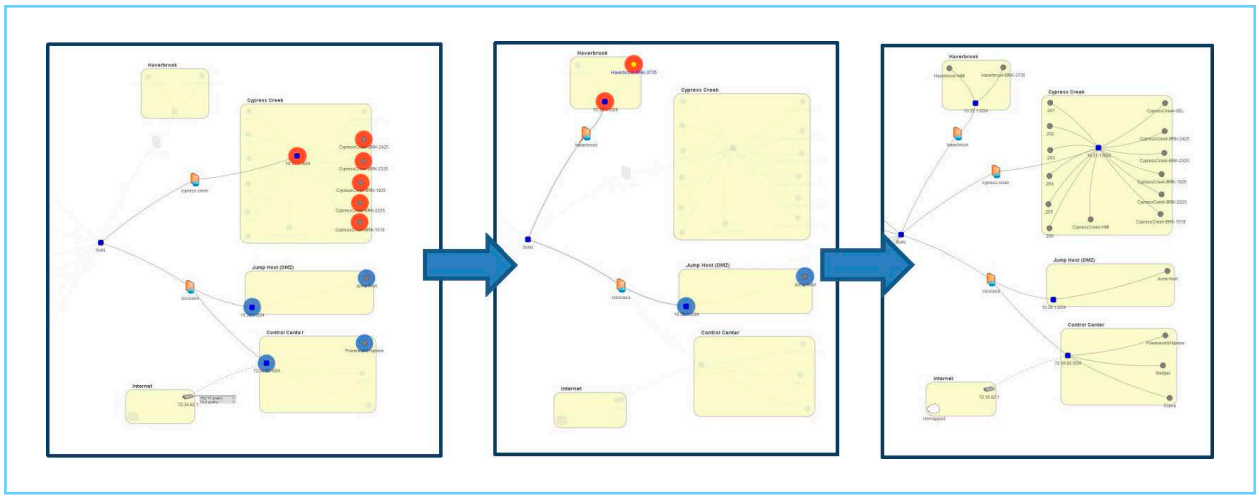


Figure 9. Visualization of patching analysis steps

device may exist, as illustrated in Figure 10. The cost computation uses only the lowest cost vulnerability to reach a particular asset, although the attack graph retains all vulnerability IDs.

$$CC\left(p(i)\right) = \sum_{l \in L} min\{V(a)\} \quad (2)$$

CyPSA obtains vulnerability scores *V(a)* from the National Vulnerability Database (NVD), as discussed in Section VI. In the *SI* calculation, the inverse cost *CC* is multiplied by the attack impact, as obtained by the *PI*:

$$SI\left(p(i)\right) = \frac{PI\left(p(i)\right)}{CC\left(p(i)\right)} \quad (3)$$

CyPSA thus prioritizes low cost, high-impact attacks. The prioritization scheme can be adjusted to use other metrics.

VIII. Cyber-Physical Testbed

The Information Trust Institute at the University of Illinois, where the CyPSA project is housed, is home to the extensive Trustworthy Cyber Infrastructure for the Power Grid (TCIPG) cyber-physical testbed. The testbed provides a scalable and flexible framework that can operate at varying fidelities to facilitate emerging research [19]. The TCIPG testbed contains many real power system devices, including firewalls, substation computers, and IP-addressable microprocessor-based relays, that can be networked together (Figure 12). For CyPSA, we configure the testbed to emulate substations that we are studying, as shown in Figure 11. The configuration is then used to develop and implement tests for validating our toolset and our models in a realistic environment before deploying it in a utility. The lab environment also allows us to configure and verify particular attack vectors that could affect utilities but cannot be evaluated in an operational network.

IX. Related Work

Over the last few years, design and analysis of cyber-physical systems have received considerable attention in the research community. In [20], Lee discussed cyber-physical system design challenges and argued that existing abstractions and modeling techniques are inadequate, while Derler *et al.*, [21] named specific factors presenting these challenges. More specific to energy, Ilic *et al.*, [22] proposed cyber-physical

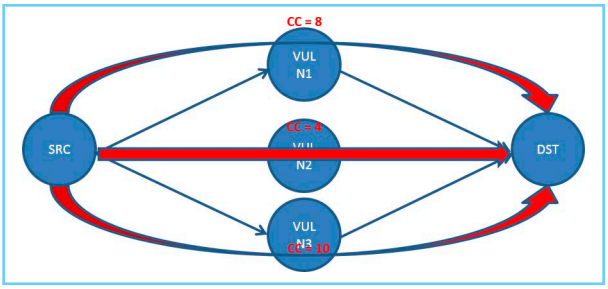


Figure 10. Vulnerabilities with exploitation costs CC from source to destination node

models of generation and load components and their interconnection through the electrical network. Palensky *et al.*, [23] discussed the challenges associated with continuous-time and discrete time cyber-physical models of energy systems and compared the scalability of these two approaches.

Security and reliability of the cyber-physical energy infrastructures has also received considerable attention (e.g., [24], [25], [26], [27], [11]). A switched systems view of the power grid is used by both [25], [26]. Challenges facing secure control and survivability of cyber-physical systems were discussed in [24]. They suggest as missing an ability to estimate the state of the cyber network along with the state of the physical system and an ability to use that information in improving the physical system's performance. In [27], Zonouz *et al.*, proposed a framework that leverages estimates of security state of the cyber infrastructure to improve electrical system state estimation. In [28], [29], security-oriented techniques for effective steady

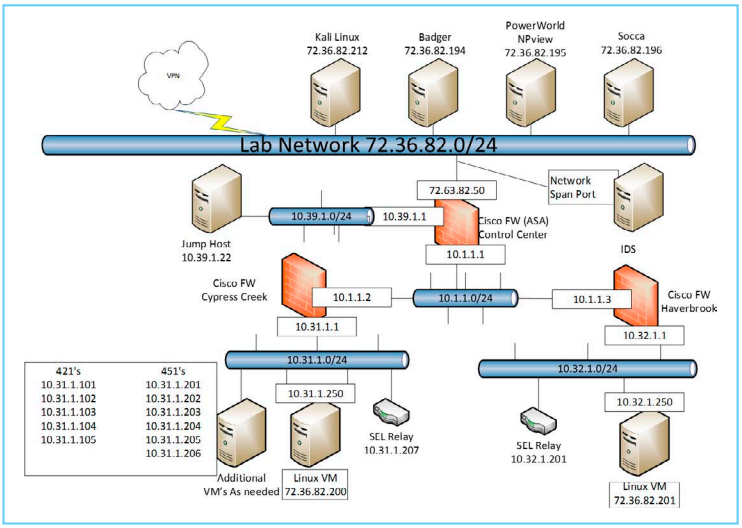


Figure 11. TCIPG testbed configured to represent two substations with actual devices and IP addresses for CyPSA

Figure 12. Equipment in TCIPG testbed

state cyber-physical abstraction using stochastic control algorithms are introduced. They also discussed how such models could be used for automated decision-making for optimal response actions against adversaries who target safety-critical infrastructures. Chen *et al.*, [30], proposed a workflow based security assessment framework and demonstrated its use using the case of Advanced Metering Infrastructure.

X. Conclusion

Contingency analysis in power systems is a study of *"what if"* scenarios, where engineers evaluate and prepare for events such as if a line or a generator goes out of service. CyPSA, presented in this article, extends this ccapability to the cyber side of the power system infrastructure by allowing users to study the impact of cyber assets going out of service or being under an attacker's control. CyPSA is at a prototype stage, and we are seeking partners to further test and demonstrate our software in real-word settings.

XI. Acknowledgements

The authors acknowledge contributions to this work from other CyPSA team members Charles Davis, Luis Garcia, Olivier Soubigou, Mouna Bamba, and Panini Patapanchala. The information, data, or work presented herein was funded in part by the Advanced Research Projects Agency-Energy (ARPA-E), U.S. Department of Energy, under award number DE-AR0000342.

References

[1] K. Davis, C. Davis, S. Zonouz, R. Bobba, R. Berthier, L. Garcia, and P. Sauer, "A cyber-physical modeling and assessment framework for power grid infrastructures," *IEEE Transactions on Smart Grid*, vol. 6, no. 5, pp. 2464–2475, Sept 2015.

[2] T. Liacco, "The adaptive reliability control system," *IEEE Transactions on Power Apparatus and Systems*, vol. PAS-86, no. 5, pp. 517–531, May 1967.

[3] North American Electric Reliability Corporation's Transmission Operations Standard top-004-1. [Online]. Available: http://www. nerc.com/files/TOP-004-1.pdf

[4] L. Fink and K. Carlsen, "Power/energy: Operating under stress and strain: This, part two of the blackout series, defines control objectives for various levels and types of emergencies," *IEEE Spectrum*, vol. 15, no. 3, pp. 48–53, March 1978.

[5] Network Perception, Inc. (2015) NP-View: Network security audit for critical infrastructures. [Online]. Available: http://www.network-perception.com

[6] PowerWorld Corp. (2005) PowerWorld Simulator. [Online]. Available: www.powerworld.com

[7] A. Monticelli, State Estimation in Electric Power Systems: A Generalized Approach. Kluwer Academic Publishers, 1999.

[8] B. Schneier, "Attack trees: Modeling security threats," Dr. Dobb's Journal, 1999.

[9] C.-W. Ten, C.-C. Liu, and M. Govindarasu, "Vulnerability assessment of cybersecurity for scada systems using attack trees," in *Power Engineering Society General Meeting*, 2007. IEEE, June 2007, pp. 1–8.

[10] G. F. Lyon, Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning. USA: Insecure, 2009.

[11] S. Zonouz, C. Davis, K. Davis, R. Berthier, R. Bobba, and W. Sanders, "SOCCA: A security-oriented cyber-physical contingency analysis in power infrastructures," *IEEE Transactions on Smart Grid*, vol. 5, no. 1, pp. 3–13, 2014.

[12] G. A. Weaver, C. Cheh, E. J. Rogers, W. H. Sanders, and D. Gammel, "Toward a cyber-physical topology language: Applications to NERC CIP audit," in *Proceedings of the First ACM Workshop on Smart Energy Grid Security (SEGS '13)*. New York, NY, USA: ACM, 2013, pp. 93–104.

[13] C. Cheh, G. A. Weaver, and W. H. Sanders, "Cyber-physical topology language: Definition, operations, and application," in *Proceedings of the 21st IEEE Pacific Rim International Symposium on Dependable Computing (PRDC 2015)*. IEEE, 2015.

[14] X. Barbosa. (2014) JSON Reference. [Online]. Available: http://json-spec.readthedocs.org/en/latest/reference.html

[15] OWL Working Group. (2012) Web ontology language (owl). [Online]. Available: http://www.w3.org/2001/sw/wiki/OWL

[16] G. Weaver, ITI/CPTL Power Repository. [Online]. Available: https://github.com/ITI/cptl-power

[17] National Vulnerability Database. [Online]. Available: http://nvd.nist.gov/

[18] The MITRE Corporation. (2015) Common vulnerabilities and exposures. [Online]. Available: https://cve.mitre.org/

[19] TCIPG. (2014) Testbed cross-cutting research. [Online]. Available: http://www.tcipg.org/research/testbed-cross-cutting-research

[20] E. A. Lee, "Cyber physical systems: Design challenges," in *11th IEEE International Symposium on Object Oriented Real-Time Distributed Computing (ISORC)*. IEEE, 2008, pp. 363–369.

[21] P. Derler, E. A. Lee, and A. S. Vincentelli, "Modeling cyber–physical systems," *Proceedings of the IEEE*, vol. 100, no. 1, pp. 13–28, 2012.

[22] M. Ilic, L. Xie, U. Khan, and J. Moura, "Modeling future cyber-physical energy systems," in *Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century*, 2008 IEEE, July 2008, pp. 1–9.

[23] P. Palensky, E. Widl, and A. Elsheikh, "Simulating cyber-physical energy systems: Challenges, tools and methods," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 44, no. 3, pp. 318–326, March 2014.

[24] A. Cardenas, S. Amin, and S. Sastry, "Secure control: Towards survivable cyber-physical systems," in *28th International Conference on Distributed Computing Systems Workshops, 2008. ICDCS '08.*, June 2008, pp. 495–500.

[25] S. Liu, X. Feng, D. Kundur, T. Zourntos, and K. Butler-Purry, "Switched system models for coordinated cyber-physical attack construction and simulation," in *IEEE First International Workshop on Smart Grid Modeling and Simulation*, 2011, pp. 49–54.

[26] A. Dominguez-Garcia, "Reliability modeling of cyber-physical electric power systems: A system-theoretic framework," in *Power and Energy Society General Meeting, 2012 IEEE*, July 2012, pp. 1–5.

[27] S. Zonouz, K. Rogers, R. Berthier, R. Bobba, W. Sanders, and T. Overbye, "SCPSE: Security-oriented cyber-physical state estimation for power grid critical infrastructures," *IEEE Transactions on Smart Grid*, vol. 3, no. 4, pp. 1790–1799, 2012.

[28] S. A. Zonouz, H. Khurana, W. H. Sanders, and T. M. Yardley, "RRE: A game-theoretic intrusion response and recovery engine," in *IEEE/IFIP International Conference on Dependable Systems & Networks*, 2009. DSN'09., 2009, pp. 439–448.

[29] Zonouz, A. Houmansadr, and P. Haghani, "EliMet: Security metric elicitation in power grid critical infrastructures by observing system administrators' responsive behavior," in *IEEE/IFIP International Conference on Dependable Systems and Networks*, DSN '12, 2012, pp. 1–12.

[30] Chen, Z. Kalbarczyk, D. M. Nicol, W. H. Sanders, R. Tan, W. G. Temple, N. O. Tippenhauer, A. H. Vu, and D. K. Yau, "Go with the flow: Toward workflow-oriented security assessment," in *Proceedings of the 2013 Workshop on New Security Paradigms Workshop (NSPW '13)*. New York, NY, USA: ACM, 2013, pp. 65–76.

Biographies

Katherine R. Davis (S 05, M 12) is a Research Scientist for the Information Trust Institute (ITI) and an Adjunct Assistant Professor in Electrical and Computer Engineering at the University of Illinois at Urbana-Champaign. She received B.S. degree in Electrical Engineering from the University of Texas at Austin in 2007, and M.S. and Ph.D. degrees in Electrical Engineering from the University of Illinois Urbana Champaign in 2009 and 2011. Before joining ITI, she worked for PowerWorld Corporation as a Software Engineer and Senior Consultant. Her research interests include data enhanced power system modeling and analysis and power grid security.

Robin Berthier is a Research Scientist at the Information Trust Institute, University of Illinois at Urbana-Champaign. Robin graduated from the Reliability Engineering Department at the University of Maryland in 2009. His doctoral dissertation with Prof. Michel Cukier focused on the issue of honeypot sensors deployed on large networks. He introduced a new architecture to increase the scalability of high-interaction honeypots, and combined network datasets of different granularities to offer unique attack forensics capabilities. His current research interests include advanced intrusion detection systems and the security of critical infrastructures.

Saman Zonouz (S 06, M 11) is an Assistant Professor in the Electrical and Computer Engineering Department at Rutgers University. He received his Ph.D. in Computer Science from the University of Illinois at Urbana-Champaign in 2011. He has worked on intrusion response and recovery, information flow-based security metrics for power-grid critical infrastructures, online digital forensics analysis and monitorless recoverable applications. His research interests include: computer security and survivable systems, control/game theory, intrusion response and recovery systems, automated intrusion forensics analysis, and information flow analysis-based security metrics.

Gabriel A. Weaver is a Research Scientist at the University of Illinois at Urbana-Champaign (UIUC). His current research interests involve the citation and analysis of evolving entities across heterogeneous data sources. Weaver's research builds upon previous work in the Classics for Harvard's Center for Hellenic Studies and the Archimedes Palimpsest Project. He received his Ph.D in 2012 from Dartmouth College for XUTools. XUTools extends Unix text-processing tools (grep, diff, wc) to a broader class of languages found in security policies. His postdoctoral research at UIUC focused on developing the Cyber-Physical Topology Language (CPTL) to represent and analyze critical infrastructures. Both XUTools and CPTL enable the retrieval and analysis of multiversioned entities using high-level language constructs.

Rakesh B. Bobba (M 06) is an Assistant Professor in the School of Electrical Engineering and Computer Science (EECS) at Oregon State University (OSU). His research interests are in the design of secure and trustworthy networked and distributed computer systems, with a current focus on cyber-physical critical infrastructures, shared computing infrastructures and real-time systems. He obtained his Ph.D. and M.S. in Electrical and Computer Engineering from the University of Maryland at College Park. Prior to joining OSU, Dr. Bobba was a Research Assistant Professor at the Information Trust Institute, University of Illinois, Urbana-Champaign.

Edmond Rogers is a Smart Grid Security Engineer with the Information Trust Institute at the University of Illinois at Urbana Champaign. Before joining ITI, Edmond Rogers (CISSP) was actively involved as an industry participant in many research activities in ITI's TCIPG Center, including work on NetAPT (the Network Access Policy Tool) and LZFuzz (Proprietary Protocol Fuzzing). Prior to joining ITI, Rogers was a security analyst for Ameren Services, a Fortune 500 investor-owned utility, where his responsibilities included cyber security and compliance aspects of Ameren's SCADA network. Before joining Ameren, he was a security manager and network architect for Boston Financial Data Systems (BFDS), a transfer agent for 43% of all mutual funds. He began his career by founding Bluegrass.Net, one of the first Internet service providers in Kentucky. Rogers leverages his wealth of experience to assist ITI researchers in creating laboratory conditions that closely reflect real-world configurations.

Peter W. Sauer (S 73, M 77, SM 82, F 93, LF 12) obtained his Bachelor of Science degree in Electrical Engineering from the University of Missouri at Rolla in 1969, the Master of Science and Ph.D. degrees in Electrical Engineering from Purdue University in 1974 and 1977 respectively. From 1969 to 1973, he was the electrical engineer on a design assistance team for the Tactical Air Command at Langley Air Force Base, Virginia. From August 1991 to August 1992 he served as the Program Director for Power Systems in the Electrical and Communication Systems Division of the National Science Foundation in Washington D.C. He is currently the Grainger Chair Professor of Electrical Engineering at Illinois.

David M. Nicol (M, F 04) obtained his Bachelor of Arts degree in mathematics from Carleton College in 1979, the Master of Science and Ph.D. degrees in computer science from University of Virginia in 1983 and 1985 respectively. From 1985 to 1987, he was a staff scientist at the Institute for Computer Applications in Science and Engineering. He then joined the faculty at the College of William and Mary in the computer science department, and in 1996 joined the faculty of Dartmouth College, also in computer science. He joined the faculty of the University of Illinois in 2003, where he is currently the Franklin W. Woeltge Professor of Electrical and Computer Engineering, and the Director of the Information Trust Institute.

This article was previously published in Security & Privacy, IEEE, vol.13, no.6, pp.60-65, Nov.-Dec. 2015
Editors: Melissa Dark, dark@purdue.edu | Jelena Mirkovic, mirkovic@isi.edu

Security Analytics: Essential Data Analytics Knowledge for Cybersecurity Professionals and Students

Rakesh Verma | University of Houston
Murat Kantarcioglu | University of Texas at Dallas
David Marchette | Naval Surface Warfare Center
Ernst Leiss and Thamar Solorio | University of Houston

Abstract
Abstract: At the 2015 Workshop on Security and Privacy Analytics, there was a well-attended and vigorous debate on educating and training professionals and students in security analytics. This article extends this debate by laying out essential security analytics concepts for professionals and students, sharing educational experiences, and identifying gaps in the field.

Key words: education, security, cybersecurity, data analysis, security analytics

We live in an exciting period of technological progress. The 20th century was the age of electricity and electronics, integrated circuits, computing, and the Internet. We expect the present century to herald *data analytics*—data and discovery through data analysis. Data analytics' ultimate goal is to achieve insight or cognitive computing by extracting interesting and meaningful patterns, or knowledge, from all types of data—record, transaction, graphical, ordered, and text. Thus, in our view, data analytics includes statistics, data mining, machine learning, and natural language processing (NLP).

Why should cybersecurity professionals and students understand data analytics? First, security challenges such as intrusion detection, insider threats, malware detection, and phishing detection lack exact algorithmic solutions. The boundary between normal and anomalous behavior isn't clear cut, especially because attackers are continuously improving their evasive techniques and strategies. Second, much software was designed and developed before the Internet and before software developers became aware of the many cybersecurity challenges. Third, text data in emails and social media outlets tends to be noisy, and computer understanding of natural language for even clean document text is extremely challenging (and not just for computers!). Finally, the large amount of data generated by, for example, automatic logs and sensors necessitates efficient and automated data analytics techniques. Recognition of these challenges has led to the explosion of data analytics applications in cybersecurity.

We believe that security analytics provides the skills needed to address today's challenges. The question then becomes, what topics must be covered when training and educating students and professionals in security analytics? This article serves as an exposition of the essential concepts for comment and debate in the field. We also share our teaching experiences, invite additional research by exposing open security issues, and touch on connections to a cybersecurity education initiative.

Cybersecurity's Unique Challenges

Cybersecurity imposes some unique challenges to data analytics techniques, which we describe briefly.

Dataset Availability

Some security challenges, such as inside attacks, lack datasets or ground truth because of competition or privacy concerns. In such cases, it's very hard to make progress.

Imbalanced Datasets and Diverse Data in Each Class

In security challenges such as intrusion detection, much legitimate data is available, but not enough attack traces. For challenges such as phishing, access to a diverse set of legitimate emails is lacking, but attacks can be found on the Internet. Legitimate emails are sometimes available but have been sanitized for privacy reasons (for example, the email headers in the Enron dataset). In some cases, data is very diverse in each class, which requires techniques that can deal with imbalance and diversity.

Asymmetrical Costs of Misclassification

For sophisticated email users, the potential harm is less if a phishing email is misclassified as legitimate. However, the potential harm increases if a legitimate email is misclassified as phishing. Also, in network packet-based intrusion detection, the vast number of nonattack packets means that even a small fraction of false positives can overload an intrusion detection system, rendering it unusable. Hence, the false positives (we consider the attacks "positive" in both examples) should be minimized for such an application. False negatives can be very harmful in the case of malicious software. Thus, data techniques that can take a cost matrix for misclassification as input are needed.

Active Adversary

One of the most important differences between applying data analytics techniques to cybersecurity versus other applications is the existence of malicious adversaries who continually adapt their behavior to hide their actions (so data distributions are nonstationary) and make static data mining models useless. Unfortunately, traditional data-mining techniques are insufficient to handle such adversarial problems directly. The adversaries adapt to the data miner's reactions, and data-mining algorithms constructed based on a training dataset degrade quickly, a problem usually referred to as *adversarial learning*.[1–5]

In many respects, the adversarial learning problem resembles game theory's two-player games. Recent research often models the problem as a game between a classifier and an adversary that modifies the data distributions.[2,3]

For many cybersecurity applications, the assumption that the adversary doesn't know the data miner's strategy is invalid; the adversary might obtain this information by probing the data miner's strategy models. For example, different spam emails could be generated to probe and understand the spam filter internals. Therefore, for many cybersecurity applications, the adversarial learning problem is more appropriately modeled as a sequential game between two players. The first player must commit to a strategy before the second player responds. Thus, the responding player has partial or complete information on the first, which allows him or her to play an optimal strategy. This research area is active.

Potential Dataset Poisoning

Datasets are available on the Internet, so they could be deliberately contaminated with malicious intent. This could be considered one of the dangers of having an active adversary and be treated holistically. Note also that attackers might poison the data in various ways (for example, by controlling spam generation).

Base-Rate Fallacy

Because an attack's incidence varies with the anticipated prize, when a classifier that's 95 percent accurate predicts an attack, the probability of it being an attack isn't actually 95 percent. For instance, when the attack probability is low, say 10 percent, and the classifier for attack is 90 percent accurate, then using Bayes' rule, a positive decision from the classifier implies that the attack's probability rises to only 50 percent. Thus, the evaluation scenario for reporting results needs to be realistic.

Attack Time Scale

A computer attacks' time scale can be extremely small, such that an attack can compromise a system and damage or steal data within a fraction of a second of mounting the attack. This means that the defender must make critical decisions about the appropriate reaction very quickly. Reacting to false alarms can cause the system to effectively "attack itself." Attackers sometimes flood an intrusion detection system with items known to trigger false alarms to cause the system to be ignored or to hide the real attack in a flood of noise. We need methods that can deal with time scale issues.

Data Analytics for Cybersecurity: Essential Concepts and Knowledge

We've organized the essential data analytics knowledge into four main themes: *preprocessing data and visualization*, *statistics*, *data mining and machine learning*, and *NLP*. This knowledge's basic prerequisites are mathematics and computer programming through data structures and algorithms, which are already typically included in a computer science degree.

Preprocessing Data and Visualization

Visualization can be an effective way to put data patterns in context and to formulate hypotheses. However, data might be noisy, have missing or corrupted values, or have attributes of widely varying type and scale. The first case might require a cleaning procedure, and the second, decisions on handling missing or corrupted values. For visualization of text data, there are two specific concerns: tokenization and normalization. Finally, elegant visualization techniques might aid understanding of the attributes of very different aspects.

Beyond a solid understanding of the types of data and attributes (categorical, discrete, and continuous) and their permissible operations,[6] cybersecurity professionals and students must know how to preprocess the data and attributes and how to conduct discretization of continuous attributes and normalization of the attributes that vary widely in scale as appropriate for the specific data-analytic method. Finally, a working knowledge of data querying tools would be useful.

Statistics

A basic applied statistics course covering parameter estimation, confidence intervals, hypothesis tests (parametric and nonparametric), and Bayesian techniques is essential. Linear and logistic regression are important tools for undergraduate and graduate students and advanced practitioners, and are essential for understanding many of the machine-learning techniques required for computer security data analysis. Principal component analysis and multidimensional scaling techniques are important for multivariate data analysis.

Goodness-of-fit tests, model selection and validation, and experimental design are important for proper application and assessment of statistical methods. Although we don't expect practitioners or students to

become statisticians, they should understand the basic ideas behind these topics.

Various types of statistical graphics are also important for understanding data and guiding the selection of appropriate analysis tools. These include scatter plots and pairs plots (also called scatter plot matrices), bar plots, histograms and density plots, parallel coordinates plots, and mosaic plots (for categorical data). A statistical data visualization course can be a valuable addition to a curriculum that covers statistical pattern recognition and machine learning.

Knowledge of a statistical software package such as R is desirable. We strongly recommend a hands-on, applied statistics course that uses such a software package rather than a purely theoretical one, particularly for practitioners. Advanced practitioners should be familiar with basic time-series analysis, including the concepts of correlation, stationarity, and nonstationarity. They should also have a working knowledge of basic models such as moving average and autoregressive models. Again, this knowledge should be obtained in a hands-on course using extensive real-world data.

Data Mining and Machine Learning for Security

Somewhat arbitrarily, we distinguish between unsupervised and supervised learning methods—*data mining* and *machine learning*, respectively. Briefly, unsupervised means that the data item's class attribute is either not present or ignored, whereas supervised means that the data item's class attribute is both present and used in a nontrivial way.

Students of data-mining and machine-learning techniques need thorough knowledge of data structures and algorithms at the junior level and knowledge of databases (new noSQL systems such as Hadoop and Spark are desirable).

We believe that the following data-mining techniques are essential: association rule mining, clustering, anomaly detection, experimental design issues including cross validation and overfitting, and applications of these concepts to cybersecurity. In addition, students should get hands-on exposure to at least one tool, such as Weka or R. In association rule mining, students should learn the technique's assumptions, support and confidence, how frequently item sets are generated, how association rules are generated, and techniques for evaluating the rules' quality. For graduate students and professionals, we would also include compact representation of frequent item sets and selected advanced topics in association analysis. In clustering, students should learn about clustering methods assumptions, K-means and K-medoids, agglomerative hierarchical clustering techniques, model-based clustering, and cluster evaluation. Again, hands-on exposure is essential. Among data mining's cybersecurity applications, we recommend intrusion detection (such as anomaly detection methods and malware analysis for clustering techniques[7,8]). Association analysis for security challenges isn't as well explored as other data-mining techniques.[9]

As the earlier discussion on active adversaries suggests, basic game theory should be taught as part of either a specific data mining for cybersecurity class or a regular game theory class. (For example, game theoretical knowledge might be covered in the first two weeks of a graduate-level data mining for cybersecurity course; www.utdallas.edu/muratk/courses/dbmsec-15s.html.)

In machine learning, we strongly recommend the following topics: nearest neighbor, decision trees, Bayesian classifiers, neural networks, support vector machines (SVMs), and their cybersecurity applications. For the serious cybersecurity student, we also recommend semisupervised learning, time-series prediction basics, and nonstationarity. Dealing with nonstationarity requires incremental classification methods.

There are incremental versions of decision trees,[10] Bayesian classifiers, neural networks, and SVMs.[11] Various oversampling or undersampling methods are available for unbalanced data. However, we believe that better success lies in designing generalizations of machine learning classification techniques, such as the so-called soft-margin SVM.[12] For graduate students and professionals, we also recommend online learning and ensemble algorithms, such as random forests and boosting.[12] Applications of these classifiers include filtering spam email (nearest neighbor and Bayesian)[13] and intrusion detection (neural networks and SVMs).[14]

NLP for Security

Prerequisites for NLP security applications include basic knowledge of information retrieval techniques such as retrieval models, Web search including PageRank and the hubs and authorities algorithm, and information retrieval metrics such as recall, precision, and F-score.

We recommend teaching the following NLP concepts and topics: N-grams, language models, Markov models including hidden Markov models (HMMs), topic

segmentation, part-of-speech tagging, word-sense disambiguation, knowledge bases like WordNet, and the security applications of these concepts. N-grams have been used in spam detection, authorship detection, and malware detection.[15–17] Language models are also useful in authorship detection. Markov models, including HMMs, have been applied to various security challenges. The classic HMM reference is Lawrence Rabiner's "A Tutorial on Hidden Markov Models and Selected Applications in Speech Recognition."[18] HMMs have been used in intrusion detection[19] and traffic analysis,[20] among other applications. Students and professional might learn about incremental machine learning algorithms[21] and an incremental Baum-Welch algorithm (here "incremental" refers to streaming data or time-series analysis),[22] as well as nonstationary HMMs.[23] Part-of-speech tagging, word-sense disambiguation, and knowledge bases such as WordNet have been used in phishing email detection.[24,25] NLP techniques have also been applied to phishing websites and URL detection.[26]

Most of these NLP techniques are suitable for cybersecurity students from diverse backgrounds: information technology, management information, computer engineering, and computer science. Perhaps the only exception is HMM, which might be more appropriate for engineering and science students.

Teaching Security Analytics

Various formats are possible for teaching the essential concepts to undergraduate and graduate students. In spring 2015, Rakesh Verma taught the University of Houston's first security analytics course to advanced undergraduate and graduate students. He used a modular format, with each module lasting three to four weeks. Each module began with a 30-minute pretest, continued to lectures on the module's topics, and ended with a 30-minute posttest and a 45-minute quiz. Modules included homework, reading, and viewing assignments in addition to the in-class material presented on the board or in slides. This course's four modules reflected the data analytics fields discussed in the previous section: basics of security, data mining for security, machine learning for security, and NLP for security. Topics included in the basics of security module were security goals (confidentiality, integrity, authentication, availability, accountability, authorization, and nonrepudiation), introduction to cryptography, message integrity, malware analysis, intrusion detection, denial-of-service attacks, and brief reviews of software security and secure systems design. The data mining for security and NLP for security modules covered all the topics discussed previously. The machine learning for security module also included the topics described in the previous section, with the exception of online learning, learning for stream data, and learning for nonstationarity. (More details are available at http://capex.cs.uh.edu.)

One lesson from this offering is that many cybersecurity examples should be used to motivate all discussions of data analytics. Another lesson (from a course taught by author Murat Kantarcioglu) is that it's critical to combine understanding of cybersecurity background with data analytics knowledge.

A word of caution: although we believe that some knowledge of data analytics and techniques is essential for cybersecurity professionals and students, it's difficult to ensure their expertise in these topics. Hence, we anticipate that security professionals will still need to work with data analytics experts, and having basic knowledge in the area will help ensure a successful collaboration. Data analytics experts will also benefit, for example, by being able to better prioritize the problems they work on.

Toward a Science of Security Analytics

There are three major gaps in the nascent field of security analytics. The first, which multiple participants of this year's Workshop on Security and Privacy Analytics mentioned, is the lack of good, publicly available datasets. Such datasets provide normative standards against which all competing techniques must be compared and are very common in other fields (such as pattern recognition and visualization). These datasets' availability would allow more rapid advances in the security analytics field. The second gap is that many classification methods don't provide an intuitive, human-understandable explanation for their classification decisions. Finally, in many cybersecurity scenarios, an active adversary is trying to defeat the classification algorithms.

Connections to the National Initiative for Cybersecurity Education

Version 1.0 of the National Initiative for Cybersecurity Education (NICE) Framework comprises 31 specialty areas organized into seven categories (for the complete list, see http://csrc.nist.gov/nice/framework). For obvious reasons, we believe that four of these categories directly consume data-analytic concepts and techniques:

securely provision, protect and defend, investigate, and analyze.

We explored the evolving field of security analytics, describing essential knowledge for serious cybersecurity professionals and students and identifying the field's current challenges and gaps. Readers interested in learning more about these topics are referred to the "Further Reading" sidebar.

Yogi Berra is famously quoted as having said, "It's hard to make predictions, especially about the future." Yet, we attempt a forecast. Demand for data science and data analytics graduates has seen a significant uptick in the past five years, with companies like Mu Sigma and Two Sigma achieving success as a generalist and a financial firm, respectively. Under its platforms, Mu Sigma lists data sciences. We predict that demand for graduates in security analytics will increase for the foreseeable future (for example, see a report claiming that big data will revolutionize cybersecurity in the next two years; http://cloudtimes.org/2014/02/12/gartner-report-big-data-will-revolutionize-the-cybersecurity-in-next-two-year).

Acknowledgments

Rakesh Verma was supported in part by National Science Foundation grants DUE 1241772, CNS 1319212, and DGE 1433817. Murat Kantargcioglu was supported in part by Army Research Office grant W911NF-12-1-0558. The authors thank George Cybenko and Bhavani Thuraisingham, who contributed to the panel and shaped our thoughts. Many thanks also go to Melissa Dark for her guidance and support throughout the review process.

References

1. M. Barreno et al., "Can Machine Learning Be Secure?," *Proc. ACM Symp. Information, Computer and Communications Security* (ASIACCS 06), 2006, pp. 16–25.
2. M. Brückner and T. Scheffer, "Stackelberg Games for Adversarial Prediction Problems," *Proc. 17th ACM SIGKDD Int'l Conf. Knowledge Discovery and Data Mining* (KDD 11), 2011, pp. 547–555.
3. N. Dalvi et al., "Adversarial Classification," *Proc. 10th ACM SIGKDD Int'l Conf. Knowledge Discovery and Data Mining* (KDD 04), 2004, pp. 99–108.
4. Y. Zhou and M. Kantarcioglu, "Adversarial Learning with Bayesian Hierarchical Mixtures of Experts," *Proc. SIAM Int'l Conf. Data Mining* (SDM 14), 2014, pp. 929–937.
5. Y. Zhou et al., "Adversarial Support Vector Machine Learning," *Proc. 18th ACM SIGKDD Int'l Conf. Knowledge Discovery and Data Mining* (KDD 12), 2012, pp. 1059–1067.
6. P.-N. Tan, M. Steinbach, and V. Kumar, *Introduction to Data Mining*, Pearson Education, 2006.
7. W. Lee and S.J. Stolfo, "Data Mining Approaches for Intrusion Detection," *Proc. 7th Conf. USENIX Security Symp.* (SSYM 98), 1998, p. 6.
8. U. Bayer et al., "Scalable, Behavior-Based Malware Clustering," *Proc. Network and Distributed System Security Symp.* (NDSS 2009), 2009; www.isoc.org/isoc/conferences/ndss/09/pdf/11.pdf.
9. H.-W. Hsiao, H.-M. Sun, and W.-C. Fan, "Detecting Stepping-Stone Intrusion Using Association Rule Mining," *Security and Communication Networks*, vol. 6, no. 10, 2013, pp. 1225–1235.
10. S.L. Crawford, "Extensions to the CART Algorithm," *Int'l J. Man-Machine Studies*, vol. 31, no. 2, 1989, pp. 197–217.
11. G. Cauwenberghs and T. Poggio, "Incremental and Decremental Support Vector Machine Learning," *Proc. Advances in Neural Information Processing Systems 13* (NIPS 2000) 2000, pp. 409–415; http://papers.nips.cc/paper/1814-incremental-and-decremental-support-vector-machine-learning.
12. T. Hastie, R. Tibshirani, and J.H. Friedman, *The Elements of Statistical Learning: Data Mining, Inference, and Prediction*, Springer, 2001.
13. I. Androutsopoulos et al., "Learning to Filter Spam E-Mail: A Comparison of a Naive Bayesian and a Memory-Based Approach," *Proc. 4th European Conf. Principles and Practice of Knowledge Discovery in Databases* (PKDD 2000), 2000; http://arxiv.org/pdf/cs/0009009.pdf.
14. A.H. Sung and S. Mukkamala, "Identifying Important Features for Intrusion Detection Using Support Vector Machines and Neural Networks," *Proc. Symp. Applications and the Internet* (SAINT 2003), 2003, pp. 209–217.
15. V. Keselj et al., "DalTREC 2005 Spam Track: Spam Filtering Using N-Gram-Based Techniques," *Proc. 14th Text REtrieval Conf.* (TREC 2005), 2005; http://trec.nist.gov/pubs/trec14/papers/dalhousieu.spam.pdf.
16. H.J. Escalante, T. Solorio, and M. Montes-y-Gómez, "Local Histograms of Character N-Grams for Authorship Attribution," *Proc. 49th Ann. Meeting of Assoc. Computational Linguistics: Human Language Technologies* (ACL 2011), 2011, pp. 288–298; www.aclweb.org/anthology/P11-1030.
17. J.Z. Kolter and M.A. Maloof, "Learning to Detect and Classify Malicious Executables in the Wild," *J. Machine Learning Research*, vol. 6, 2006, pp. 2721–2744.
18. L.R. Rabiner, "A Tutorial on Hidden Markov Models and Selected Applications in Speech Recognition," *Proc. IEEE*, vol. 77, no. 2. 1989, pp. 257–286.
19. L. Huang and M. Stamp, "Masquerade Detection Using Profile Hidden Markov Models," *Computers and Security*, vol. 30, no. 8, 2011, pp. 732–747.

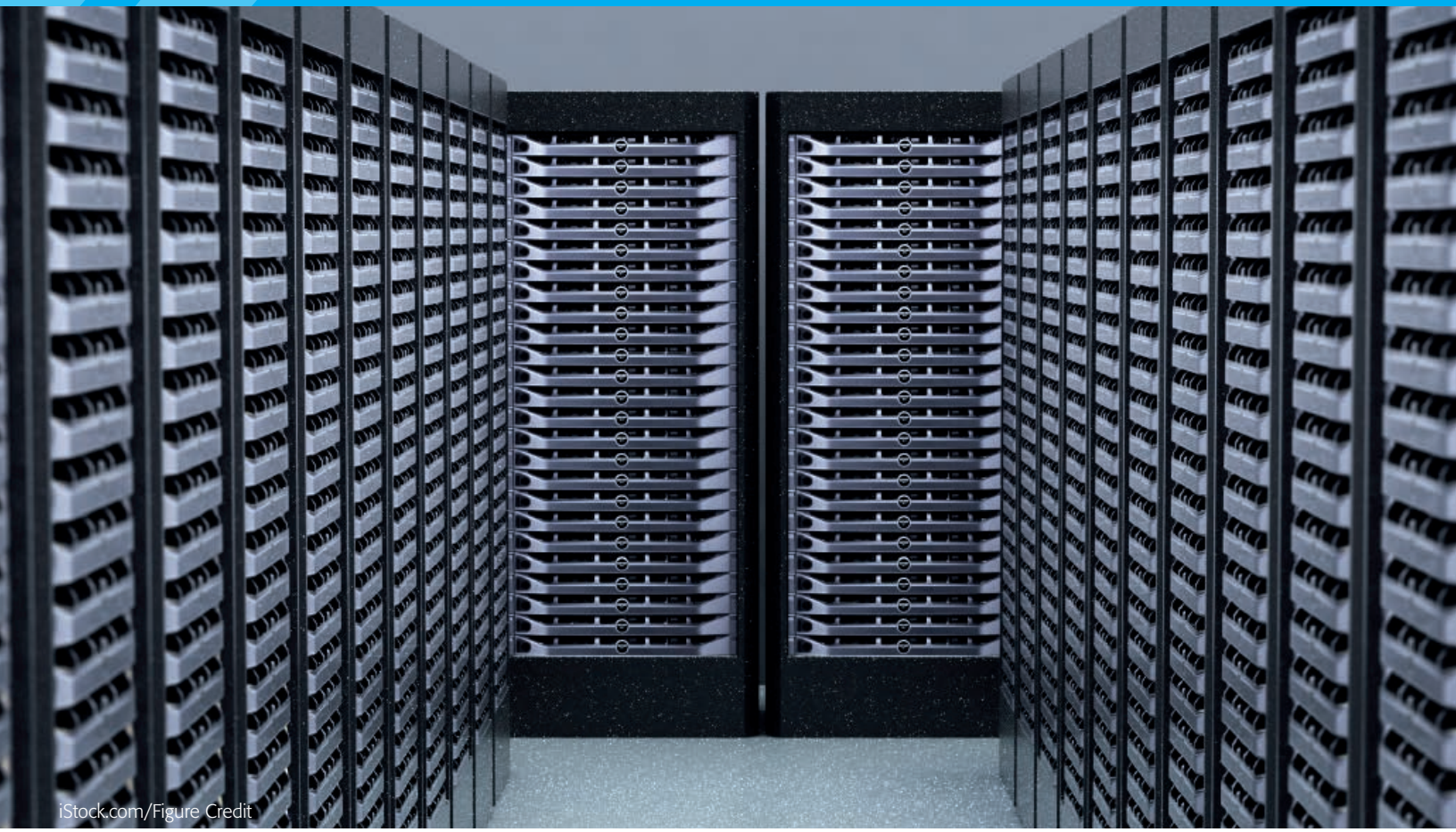
20. S. Zhioua, "Tor Traffic Analysis Using Hidden Markov Models," *Security and Communication Networks*, vol. 6, no. 9, 2013, pp. 1075–1086.
21. P.R. Cavalin et al., "Evaluation of Incremental Learning Algorithms for HMM in the Recognition of Alphanumeric Characters," *Pattern Recognition*, vol. 42, no. 12, 2009, pp. 3241–3253.
22. B. Stenger et al., "Topology Free Hidden Markov Models: Application to Background Modeling," *Proc. 8th IEEE Int'l Conf. Computer Vision* (ICCV 01), 2001, pp. 294–301.
23. A.J. Serralheiro, Y. Ephraim, and L.R. Rabiner, "On Nonstationary Hidden Markov Modeling of Speech Signals," *Proc. 1st European Conf. Speech Communication and Technology* (EUROSPEECH 89), 1989, pp. 1159–1162.
24. R. Verma, N. Shashidhar, and N. Hossain, "Phishing Email Detection the Natural Language Way," *Proc. 17th European Symp. Research in Computer Security* (ESORICS 12), 2012, pp. 824–841.
25. R. Verma and N. Hossain, "Semantic Feature Selection for Text with Application to Phishing Email Detection," *Proc. 16th Int'l Conf. Information Security and Cryptology* (ICISC 13), 2013, pp. 455–468.
26. T. Thakur and R. Verma, "Catching Classical and Hijack-Based Phishing Attacks," *Proc. 10th Int'l Conf. Information Systems Security* (ICISS 14), 2014, pp. 318–337.

Further Reading

Numerous resources are available for readers interested in learning more about this article's topics.[1–8] For statistical learning specifically, we refer readers to *An Introduction to Statistical Learning with Applications in R* for undergraduate students,[2] and *The Elements of Statistical Learning: Data Mining, Inference, and Prediction* for graduate students and professionals.[9]

References

27. [1] D. Heckerman, *A Tutorial on Learning with Bayesian Networks*, tech. report MSR-TR-95-06, Advanced Technology Division, Microsoft Research, 1996.
28. [2] G. James et al., *An Introduction to Statistical Learning with Applications in R*, Springer, 2014.
29. [3] M. Kantarcioglu, B. Xi, and C. Clifton, "Classifier Evaluation and Attribute Selection against Active Adversaries," *Data Mining and Knowledge Discovery*, vol. 22, 2011, pp. 291–335.
30. [4] W.S. Sarle, "AI-FAQ/neural Nets Index, Part 2," 11 Oct. 2002; ftp://ftp.sas.com/pub/neural/FAQ2.html#A styles batch vs inc.
31. [5] B. Gyawali et al., "Evaluating a Semisupervised Approach to Phishing URL Identification in a Realistic Scenario," *Proc. 8th Ann. Collaboration, Electronic Messaging, Anti-abuse and Spam Conf.* (CEAS 11), 2011, pp. 176–183.
32. [6] T. Basar and G.J. Olsder, *Dynamic Noncooperative Game Theory*, Society for Industrial and Applied Mathematics, 1999.
33. [7] R. Verma and K. Dyer, "On the Character of Phishing URLs: Accurate and Robust Statistical Learning Classifiers," *Proc. 5th ACM Conf. on Data and Application Security and Privacy* (CODASPY 15), 2015, pp. 111–122.
34. [8] G. Xiang et al., "A Hierarchical Adaptive Probabilistic Approach for Zero Hour Phish Detection," *Proc. 15th European Symp. Research in Computer Security* (ESORICS 10), 2010, pp. 268–285.
35. [9] T. Hastie, R. Tibshirani, and J.H. Friedman, *The Elements of Statistical Learning: Data Mining, Inference, and Prediction*, Springer, 2001.



iStock.com/Figure Credit

A Brief Review of Security in Emerging Programmable Computer Networking Technologies

Egemen K. Çetinkaya
IEEE Senior Member

Abstract
Recent programmable networking paradigms, such as cloud computing, fog computing, software-defined networks, and network function virtualization gain significant traction in industry and academia. While these newly developed networking technologies open a pathway to new architectures and enable a faster innovation cycle, there exist many problems in this area. In this article, we provide a review of these programmable networking architectures for comparison. Second, we provide a survey of security attacks and defense mechanisms in these emerging programmable networking technologies.

Keywords—Cloud Computing, Fog Computing, Software-Defined Network, SDN, Network Function Virtualization, NFV, Virtualization, Security, Resilience

I. Introduction and Motivation

Communication networks in general, and the Internet in particular, have become an essential part of society. The evolution of networks continues as the technologies progress; on the other hand, the complexity of operations, protocols, and interdependencies makes our understanding of networks formidable. While the open nature of the Internet enables its growth and innovation, this openness also has become an obstacle for its flexibility and management. In the past two decades, research efforts have aimed to design and develop *programmable networks* to overcome this *ossification* in network management. Programmable networks allow customization of networks thus leading to faster service creation and granular network management.

In recent years, we have seen an explosion in network technology (however, we note that the fundamentals of these technological progresses can be rooted back to 1960s [1]–[3]). Notable networking technology progress has been in Cloud Computing (CC), Fog Computing (FC), Software-Defined Networks (SDNs), and Network Function Virtualization (NFV). These emerging network paradigms are becoming more widespread. For example, cloud-based applications such as Google Docs, Apple iCloud, Amazon Cloud Drive, Microsoft OneDrive, and Dropbox are becoming pervasive in our daily lives. Moreover, among the many emerging paradigms that use these new networking technologies are: Internet of Things (IoT) [4], big data analytics [5], connected vehicles [6], and intelligent environments such as smart city [7] and smart grid [8]. Additionally, these emerging networking concepts (in particular OpenFlow-enabled SDNs) are widely accepted by major service providers, data center networks, and network equipment vendors [1], [9]–[11]. It is noted that in 2016, the SDN market will worth $3.7 billion and will reach $15.6 billion in 2018 [10]. The North American SDN market is projected to increase with a Compound Annual Growth Rate of 25% between 2014 and 2019 [12].

As communication networks became a critical infrastructure and ubiquitous utility offering a variety of services and applications, communication networks also become an obvious target for intelligent adversaries with economical, political, or recreational objectives. Resilience, which is defined as providing an acceptable level of service in the face of attacks and challenges [13], has become an important objective to achieve for all players including: end users, equipment providers, service providers, governments, and researchers. The two main resilience disciplines include *trustworthiness,* which specifies measurable properties of network resilience and *challenge tolerance,* which addresses varying classes of challenges to the network [13]. Security is also a resilience discipline, and it is an important attribute of the emerging programmable networking technologies such as CC, FC, SDN, and NFV.

In this brief survey paper we have two modest objectives: i) to provide a brief overview of the emerging programmable networking architectures; ii) to briefly survey of security attacks and defense mechanisms in cloud computing, fog computing, SDN, and NFV. We note that there are extensive surveys of cloud security [14], [15] and SDN security [9], [11]. We did not find comprehensive surveys relating to fog computing and NFV security since they are relatively recent topics being investigated. We also keep our presentation to the work published within the last five years and include related industry - organization publications in addition to the academic papers in our survey.

II. Overview of Emerging Technologies

Virtualization is the core of the emerging programmable network technologies, which aims for efficient utilization of shared physical resources. The history of virtualization goes back to early 1960s with the IBM time-sharing machines (i.e., virtual operating systems). While the virtual memory concept was developed in the 1970s, VLAN (Virtual Local Area Network) development was in the 1980s. While these new programmable network paradigms, CC, FC, SDN, NFV, relate to each other, they do not depend on each other but rather complement one another [1], [2]. These emerging technologies are summarized in Table I and explained in the rest of this section.

A. Cloud Computing Architecture

Cloud computing has a service-oriented architecture, as shown in Figure 1. In this architecture, the resources (i.e., processing, storage, bandwidth, infrastructure) are controlled to offer different services to customers [2], [16]–[18]. The services can be IaaS (Infrastructure-as-a-Service), PaaS (Platform-as-a-Service), SaaS (Software-as-a-Service), DaaS (Data-as-a-Service), SecaaS (Security-as-a-Service), XaaS (Anything-as-a-Service), etc. The control functions include cloud operating system, orchestration, and optimization.

TABLE I. Summary of Emerging Technologies

Technology	Acronym	Important feature
Cloud Computing	CC	Service-oriented architecture at the core
Fog Computing	FC	Computing at the edge
Software-Defined Networking	SDN	Separates data and control planes
Network Function Virtualization	NFV	Utilizes COTS hardware to implement network functions

B. Fog Computing Architecture

Fog computing (named to mean that resources are closer to end users (ground)), is a virtualized platform and an extension of cloud computing for applications such as IoT, data analytics, Smart X, connected vehicles [19]. Some of the main characteristics of location-aware fog platforms are low latency and mobility support for applications and services. The new fog computing paradigm has an hierarchical architecture (shown in Figure 2) in which at the bottom are end users, at the edge are the fog devices, and at the core is the cloud [20], [21]. This hierarchical model is similar to the Internet's hierarchical model in which at the top is the core layer, in the middle is the distribution layer, and at the bottom is the access layer.

C. SDN Architecture

The concept of programmable networks is not new, but recent efforts have focused on Software-Defined Networks (SDNs), a concept that evolved from early ideas of programmable networks [1], [3]. The simplified architecture of the SDN (Software-Defined Network) is shown in Figure 3. The two main ideas of SDNs are: 1) to decouple the control and data planes, 2) to consolidate the control plane (i.e., logically) such that it controls multiple data-plane elements. Decoupling of control and data planes can be accomplished via an API (Application Programming Interface) such as OpenFlow [1]. A northbound API such as OpenDaylight provides the interface between control and application planes. An example of a joint SDN and cloud network operation is

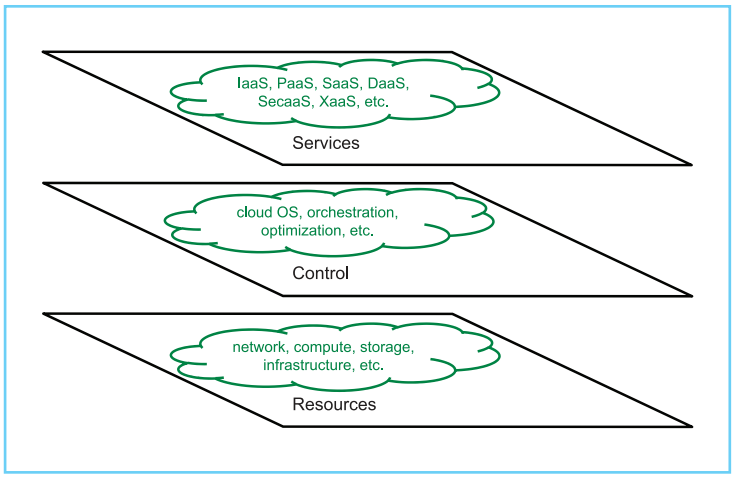


Fig. 1. Cloud computing architecture

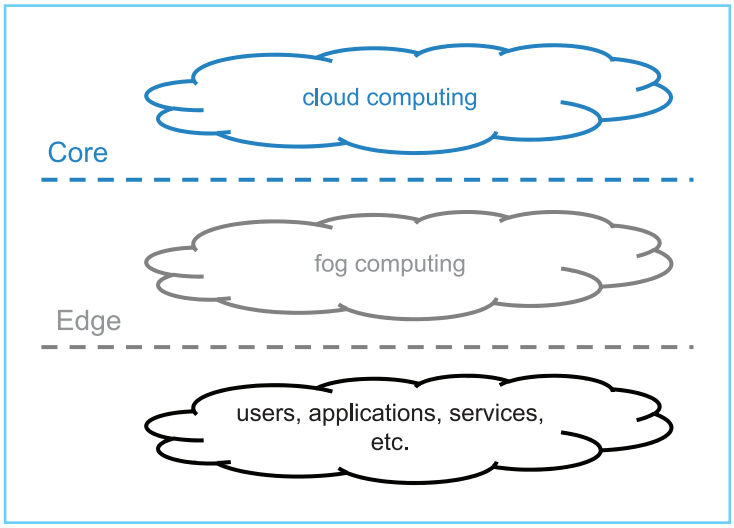


Fig. 2. Fog computing architecture

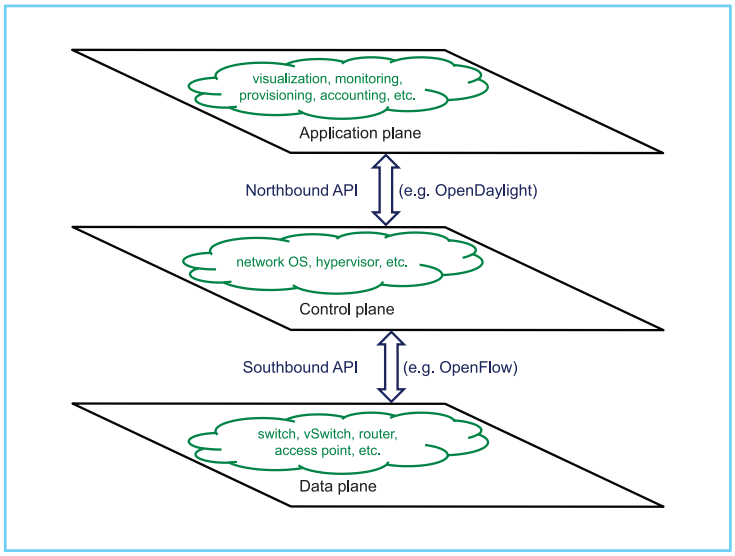


Fig. 3. SDN architecture

using SDN to traffic engineer an application hosted on the cloud network [18].

D. NFV Architecture

NFV (Network Function Virtualization) aims to virtualize network functions necessary for serving customers using shared physical resources that are implemented on COTS (commercial off-the-shelf) hardware. With the current trends, i.e., reduced ARPU (Average Revenue Per User), increased CAPEX (Capital Expenditures), and OPEX (Operational Expenditures), service providers cannot keep up with a silo of network infrastructure that does not provide new service to their customer. Instead, a better alternative would be to provide new (or existing) services using COTS (commercial off-the-shelf) hardware. Moreover, by off-loading functions of ASICs and FPGA hardware to software, this opens a path for development of new business models to the market in a fast and cost-efficient fashion. Consequently, NFV aims to virtualize network functions necessary for serving customers using shared physical resources that are implemented on COTS hardware.

ETSI (European Telecommunications Standards Institute) Network Functions Virtualisation Industry Specification Group (NFV ISG) leads the development and architecting the NFV - related technologies [22]. It is foreseen that NFV will reduce the cost of operating networks as the infrastructure transitions from custom-built hardware to using commercial hardware for compute, storage, and network resources [23]. Moreover, the passage of network functions from hardware to software will open the pathway to new business models and innovation. However, there are some realistic risks to be considered:

1. There are potential risks associated with increased OPEX [23].
2. The performance of shared virtualized network functions will not be same as the dedicated physical resources [24].
3. The value added by transitioning functions from hardware implementations to softwarization in certain application domains (e.g. home network vs. access network) will not be as high [24].

The architectural framework (shown in Figure 4) and design philosophy of virtualized network functions is described by ETSI [25]. In this architecture, the NFV infrastructure layer consists of physical and virtual resources, as well as a virtualization layer that provides partitioning of hardware resources and providing virtual

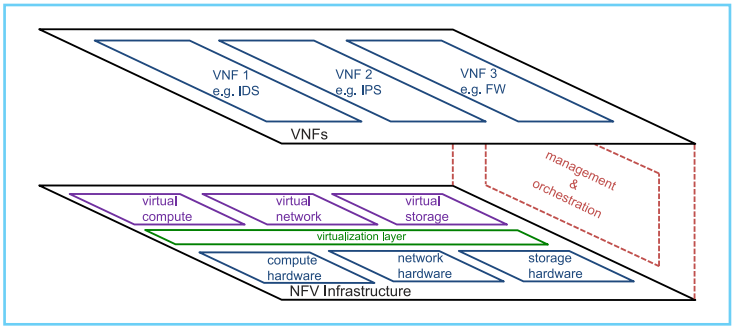


Fig. 4. NFV architecture

resources to the VNF (Virtual Network Function) layer. The virtualization layer function is similar to a hypervisor or a virtual machine (VM). Example VNFs include network functionalities such as IDS (Intrusion Detection System), IPS (Intrusion Prevention System), FW (Firewall), and load balancer. Orthogonal to the NFV Infrastructure and VNF layers, the management and orchestration layer provides the control and monitoring of the overall VNF lifecycle.

III. Network Security

We present security issues and solutions in the cloud computing, fog computing, SDN, and NFV in this section. Virtualization is a fundamental technology that enables existence of these emergent networking technologies. We will not present virtualization security here, but we point the reader to extensive literature surveys [26]–[28].

A. Cloud Computing Security

The Cloud Security Alliance (CSA) guidance document summarizes the best practices for secure cloud operation and governance [29]. It recommends evaluation of the assets (i.e., data or application/function/process) on the different cloud deployment models (i.e., public, private, community, hybrid) under different hosting scenarios (i.e., internal, external, combined). Aside from industry recommendation, there have been extensive surveys of the cloud security in the literature [14], [15], [30]–[32].

Security issues related to three cloud service delivery models (SaaS, PaaS, IaaS) are discussed [30]. Cloud threats, vulnerabilities, and attacks are extensively categorized according to cloud deployment and service delivery models [14], [15]. User-level threats at physical, virtualization, and application layers are detailed alongside security requirements for cloud computing [31]. Authors argue that a combination of PKI (Public Key Infrastructure), SSO (Single Sign-On), and LDAP

(Lightweight Directory Access Protocol) mechanisms can address horizontal security requirements in the cloud computing [31]. Software patching, data isolation across logical resources sharing same physical substrates, SSO for authentication across multiple clouds are additional considerations to secure the cloud computing infrastructure [32]. Furthermore, infrastructure- and process-level diversity is promoted as defensive mechanisms against the attacks due to monoculture (e.g., hardware monoculture, software monoculture) [33].

B. Fog Computing Security

A man-in-the-middle (MiM) attack on a gateway fog device is performed and shown that the MiM attack can be stealthy based on CPU utilization and memory consumption. Further, an authentication scheme is proposed to overcome such MiM attacks, in particular when the connection between fog and cloud is not stable [20]. Several security and privacy issues such as intrusion detection, access control, secure data storage and computation are discussed within the context of fog computing [21].

C. SDN Security

There have been extensive surveys of SDN security published in the recent past [9]–[11], [34], [35]. It is a consensus that there are two ideas in regards to SDN security: 1) there are those who conduct research aiming to secure the programmable network and 2) those who conduct research aiming to provide security as a service [9], [10]. Moreover, an extensive survey of resilience research (i.e., survivability, dependability, disruption tolerance, performability, traffic tolerance, security) in SDNs is presented [34]. Authors conclude based on their survey that security is built in SDNs via (i) as an addition or (ii) as an embedded property in the architecture [34]. Regardless of the school of thought, next, we summarize SDN security research.

In extensive surveys of the SDN security [11], [35], authors present a review of the literature on the past SDN security efforts. Security challenges and solutions in each of the application, control, and data planes of the SDNs are presented in detail. Some of the attacks in each layer include: application plane attacks (e.g., access control for third party applications), control plane attacks (e.g., fraudulent flow rules insertion, DoS attacks, and unauthorized access to the controller), and data plane attacks such as flooding the SDN switch and router components. Authors argue that while SDNs ease the global visibility of network states against challenges and attacks, the logically centralized control plane has also become an attractive target for the attackers [11], [35]. Other surveys review SDN security from a STRIDE (Spoofing, Tampering, Repudiation, Information disclosure, Denial of Service, and Elevation of Privilege) perspective [9], [36]. Additionally, a brief survey of wireless SDN and SDN experimentation literature is presented [36]. Recently, we conducted security experiments on the GENI testbed performing DDoS attacks (ICMP echo flood and TCP SYN flood) [37].

Some of the secure mechanisms against attacks in the SDN domain can be listed as: access control providing authorization and authentication, attack detection and filtering, flow aggregation to prevent information disclosure, and rate limiting at the control plane to thwart DDoS attacks [9]. It was noted that most of these defense mechanisms are not implemented. In addition to the defense mechanisms [9], federation of heterogeneous network applications (e.g. IoT, SmartX, connected vehicles) and defining security policies across different domains using SDN will be a future research direction [10].

D. NFV Security

ETSI Network Functions Virtualisation Industry Specification Group (ISG) has published several specifications in regards to NFV security [38]–[42]. Potential threats and players in the security domain are explained in the ETSI Security Problem Statement specification [38]. NFV poses threats due to network protocol vulnerabilities (e.g., flooding attack, routing insecurity), which are not related with virtualization, and due to virtualization (e.g., memory leaks and interrupt isolation) [38]. Furthermore, virtualization can, while mitigating some, incur new security threats [38]. Other specifications discuss OpenStack security [39], trust and its domains [40], lawful intercept points [41], and host application and platform security [42] as they relate to NFV.

In addition to the ETSI ISG specifications, other papers are available in the literature that we summarize next. A DDoS attack mitigation strategy using NFV technology is discussed [43]. In another paper, authors propose an architecture for trust monitoring in SDN and NFV [44]. In this architecture, an out-of-band SDN verifier component is added to SDN architecture to attest the network configuration, hardware identity check, and software trust measurement. They also investigate potential

architectures to build the attestation mechanism in virtual hosts executing critical network functions [44]. An extended SDN architecture to prevent intrusions via addition of virtualized packet inspection function is presented [45]. The simulation result of such a virtualized DPI function can improve the network performance (e.g., throughput, overhead) significantly compared to stand-alone OpenFlow-based SDN architecture [45]. An anti-virus (AV) solution was proposed and tested as a virtual network function [46]. It was shown that this AV-NFV solution did not require a proxy compared to the traditional AV solutions and its performance and memory usage was better. A virtual firewall leveraging both SDN and NFV techniques is presented that adapts to changing virtual network characteristics [47]. Intrusion detection is experimented on a testbed as a virtualized network function [48] and further the intrusion detection function is incorporated into service chaining [49]. Some security-related use cases for the NFV environments is presented [50]. In addition to the security aspects of the NFV, placement of network security functions (e.g., packet inspection, firewalls) in the topology is also an active area of research [47], [51].

IV. Conclusions

We are in an exciting era in new networking technology progression. Programmable networks, which provide greater control and management functionality, as well as enabling the pathway to greater innovation lifecycle, are being developed and deployed. Of these recently networking technologies, we observe cloud computing, fog computing, software-defined networks, and network function virtualization are becoming more pervasive for applications. We described the architecture of these different network technologies. We observe that different network architectures show similarities. At the bottom layer is some infrastructure (physical and/or virtual), in the middle is control and management of these infrastructures, and on the top is the delivery of some services/functions/applications. Another common important feature of these networking technologies is that they rely heavily on *virtualization*. Next, we present a survey of the security issues in CC, FC, SDN, and NFV. We observe that while cloud and SDN security literature is becoming rich, fog computing and NFV security is in its infancy. We believe that, regardless of the technologies, all these different emergent programmable networks pave the road to the Future Internet Architectures.

Acknowledgment

We would like to acknowledge members of the CoNetS group for discussions on this work. We thank anonymous reviewers for feedback on an early draft of this paper.

References

[1] N. Feamster, J. Rexford, and E. Zegura, "The Road to SDN: An Intellectual History of Programmable Networks," *ACM SIGCOMM Computer Communication Review*, vol. 44, no. 2, pp. 87–98, 2014.

[2] R. Jain and S. Paul, "Network Virtualization and Software Defined Networking for Cloud Computing: A Survey," *IEEE Communications Magazine*, vol. 51, pp. 24–31, November 2013.

[3] D. Medhi, B. Ramamurthy, C. Scoglio, J. P. Rohrer, E. K. Çetinkaya, R. Cherukuri, X. Liu, P. Angu, A. Bavier, C. Buffington, and J. P. Sterbenz, "The GpENI Testbed: Network Infrastructure, Implementation Experience, and Experimentation," *Computer Networks*, vol. 61, pp. 51–74, March 2014.

[4] S. Sicari, A. Rizzardi, L. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," *Computer Networks*, vol. 76, pp. 146–164, January 2015.

[5] I. A. T. Hashem, I. Yaqoob, N. B. Anuar, S. Mokhtar, A. Gani, and S. U. Khan, "The rise of 'big data' on cloud computing: Review and open research issues," *Information Systems*, vol. 47, pp. 98–115, January 2015.

[6] M. Whaiduzzaman, M. Sookhak, A. Gani, and R. Buyya, "A survey on vehicular cloud computing," *Journal of Network and Computer Applications*, vol. 40, pp. 325–344, April 2014.

[7] H. Schaffers, N. Komninos, M. Pallot, B. Trousse, M. Nilsson, and A. Oliveira, "Smart Cities and the Future Internet: Towards Cooperation Frameworks for Open Innovation," in *The Future Internet*, vol. 6656 of *Lecture Notes in Computer Science*, pp. 431–446, Springer Berlin Heidelberg, 2011.

[8] S. Bera, S. Misra, and J. J. Rodrigues, "Cloud Computing Applications for Smart Grid: A Survey," *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, no. 5, pp. 1477–1494, 2015.

[9] D. Kreutz, F. M. V. Ramos, P. E. Verissimo, C. E. Rothenberg, S. Azodolmolky, and S. Uhlig, "Software-Defined Networking: A Comprehensive Survey," *Proceedings of the IEEE*, vol. 103, no. 1, pp. 14–76, 2015.

[10] S. T. Ali, V. Sivaraman, A. Radford, and S. Jha, "A Survey of Securing Networks Using Software Defined Networking," *IEEE Transactions on Reliability*, vol. 64, no. 3, pp. 1086–1097, 2015.

[11] S. Scott-Hayward, S. Natarajan, and S. Sezer, "A Survey of Security in Software Defined Networks," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 1, pp. 623–654, 2016.

[12] "North America Software Defined Networking Market, by Solution (SDN Switching, SDN Controllers, Virtual Cloud Application), by End User (Enterprise, Telecommunication Service Providers, Cloud Service Providers), by Geography - Analysis & Forecast to 2019." http://www.micromarketmonitor.com/market/north-america-software-defined-network-sdn-9065162554.html, July 2015.

[13] J. P. G. Sterbenz, D. Hutchison, E. K. Çetinkaya, A. Jabbar, J. P. Rohrer, M. Schöller, and P. Smith, "Resilience and survivability in com- munication networks: Strategies, principles, and survey of disciplines," *Computer Networks*, vol. 54, no. 8, pp. 1245–1265, 2010.

[14] D. A. B. Fernandes, L. F. B. Soares, J. V. Gomes, M. M. Freire, and P. R. M. Inácio, "Security issues in cloud environments: a survey," *International Journal of Information Security*, vol. 13, no. 2, pp. 113– 170, 2014.

[15] C. A. Ardagna, R. Asal, E. Damiani, and Q. H. Vu, "From Security to Assurance in the Cloud: A Survey," *ACM Computing Surveys*, vol. 48, no. 1, pp. 2:1–2:50, 2015.

[16] F. Liu, J. Tong, J. Mao, R. Bohn, J. Messina, L. Badger, and D. Leaf, "NIST Cloud Computing Reference Architecture," (special publication 500-292), National Insitute of Standards and Technology (NIST), Gaithersburg, MD, September 2011.

[17] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A View of Cloud Computing," *Communications of the ACM*, vol. 53, no. 4, pp. 50– 58, 2010.

[18] N. Bitar, S. Gringeri, and T. J. Xia, "Technologies and Protocols for Data Center and Cloud Networking," *IEEE Communications Magazine*, vol. 51, no. 9, pp. 24–31, 2013.

[19] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog Computing and Its Role in the Internet of Things," in *Proceedings of the ACM SIGCOMM Mobile Cloud Computing Workshop (MCC)*, (Helsinki), pp. 13–16, August 2012.

[20] I. Stojmenovic, S. Wen, X. Huang, and H. Luan, "An overview of Fog computing and its security issues," *Concurrency and Computation: Practice and Experience*, 2015.

[21] S. Yi, Z. Qin, and Q. Li, "Security and Privacy Issues of Fog Computing: A Survey," in *Proceedings of the 10th International Conference on Wireless Algorithms, Systems, and Applications (WASA)*, (Qufu, China), pp. 685–695, August 2015.

[22] "ETSI Network Functions Virtualisation Industry Specification Group, NFV ISG." http://www.etsi.org/technologies-clusters/technologies/nfv, 2016.

[23] E. Hernandez-Valencia, S. Izzo, and B. Polonsky, "How Will NFV/SDN Transform Service Provider OpEx?," *IEEE Network Magazine*, vol. 29, no. 3, pp. 60–67, 2015.

[24] B. Han, V. Gopalakrishnan, L. Ji, and S. Lee, "Network Function Virtualization: Challenges and Opportunities for Innovations," *IEEE Communications Magazine*, vol. 53, no. 2, pp. 90–97, 2015.

[25] ETSI, "ETSI GS NFV 002: Network Functions Virtualisation (NFV); Architectural Framework," Specification RGS/NFV-002, ETSI, Decem- ber 2014.

[26] M. Pearce, S. Zeadally, and R. Hunt, "Virtualization: Issues, secu- rity threats, and solutions," *ACM Computing Surveys*, vol. 45, no. 2, pp. 17:1–17:39, 2013.

[27] D. Sgandurra and E. Lupu, "Evolution of Attacks, Threat Models, and Solutions for Virtualized Systems," *ACM Computing Surveys*, vol. 48, no. 3, pp. 46:1–46:38, 2016.

[28] G. Pék, L. Buttyán, and B. Bencsáth, "A Survey of Security Issues in Hardware Virtualization," *ACM Computing Surveys*, vol. 45, no. 3, pp. 40:1–40:34, 2013.

[29] P. Simmonds, C. Rezek, and A. Reed, "Security Guidance for Critical Areas of Focus in Cloud Computing," tech. rep., Cloud Security Alliance (CSA), 2011.

[30] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," *Journal of Network and Computer Applications*, vol. 34, no. 1, pp. 1–11, 2011.

[31] D. Zissis and D. Lekkas, "Addressing cloud computing security issues," *Future Generation Computer Systems*, vol. 28, no. 3, pp. 583–592, 2012.

[32] J. Moura and D. Hutchison, "Review and analysis of networking challenges in cloud computing," *Journal of Network and Computer Applications*, vol. 60, pp. 113–129, January 2016.

[33] J. P. Sterbenz and P. Kulkarni, "Diverse Infrastructure and Architecture for Datacenter and Cloud Resilience," in *Proceedings of the IEEE International Conference on Computer Communications and Networks (ICCCN)*, (Nassau, Bahamas), pp. 1–7, August 2013. (invited paper).

[34] A. S. da Silva, P. Smith, A. Mauthe, and A. Schaeffer-Filho, "Resilience support in software-defined networking: A survey," *Computer Networks*, vol. 92, Part 1, pp. 189–207, December 2015.

[35] I. Ahmad, S. Namal, M. Ylianttila, and A. Gurtov, "Security in Software Defined Networks: A Survey," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2317–2346, 2015.

[36] I. Alsmadi and D. Xu, "Security of Software Defined Networks: A survey," *Computers & Security*, vol. 53, pp. 79–108, September 2015.

[37] M. C. Gorla, V. M. Kamaraju, and E. K. Çetinkaya, "Network Attack Experimentation using OpenFlow-enabled GENI Testbed (poster)," in *23rd GENI Engineering Conference (GEC 23) Demo and Poster Session*, (Champaign, IL), June 2015.

[38] ETSI, "ETSI GS NFV-SEC 001: Network Functions Virtualisation (NFV); NFV Security; Problem Statement," Specification DGS/NFV- SEC001, ETSI, October 2014.

[39] ETSI, "ETSI GS NFV-SEC 002: Network Functions Virtualisation (NFV); NFV Security; Cataloguing security features in management software," Specification DGS/NFV-SEC002, ETSI, August 2015.

[40] ETSI, "ETSI GS NFV-SEC 003: Network Functions Virtualisation (NFV); NFV Security; Security and Trust Guidance," Specification DGS/NFV-SEC003, ETSI, December 2014.

[41] ETSI, "ETSI GS NFV-SEC 004: Network Functions Virtualisation (NFV); NFV Security; Privacy and Regulation; Report on Lawful Interception Implications," Specification DGS/NFV-SEC004, ETSI, September 2015.

[42] ETSI, "ETSI GS NFV-SEC 009: Network Functions Virtualisation (NFV); NFV Security; Report on use cases and technical approaches for multi-layer host administration," Specification DGS/NFV-SEC009, ETSI, December 2015.

[43] R. Krishnan, D. Krishnaswamy, and D. McDysan, "Behavioral Security Threat Detection Strategies for Data Center Switches and Routers," in *Proceedings of the 34th IEEE International Conference on Distributed Computing Systems Workshops (ICDCSW)*, (Madrid), pp. 82–87, June 2014.

[44] L. Jacquin, A. Lioy, D. Lopez, A. Shaw, and T. Su, "The Trust Problem in Modern Network Infrastructures," in *Cyber Security and Privacy* (F. Cleary and M. Felici, eds.), vol. 530 of *Communications in Computer and Information Science*, pp. 116–127, Springer International Publishing, 2015.

[45] Y.-D. Lin, P.-C. Lin, C.-H. Yeh, Y.-C. Wang, and Y.-C. Lai, "An Extended SDN Architecture for Network Function Virtualization with a Case Study on Intrusion Prevention," *IEEE Network Magazine*, vol. 29, no. 3, pp. 48–53, 2015.

[46] C.-N. Kao, S. SI, N.-F. Huang, I.-J. Liao, R.-T. Liu, and H.-W. Hung, "Fast Proxyless Stream-Based Anti-Virus for Network Function Virtualization," in *Proceedings of the 1st IEEE Conference on Network Softwarization (NetSoft)*, (London), pp. 1–5, April 2015.

[47] J. Deng, H. Hu, H. Li, Z. Pan, K.-C. Wang, G.-J. Ahn, J. Bi, and Y. Park, "VNGuard: An NFV/SDN Combination Framework for Provisioning and Managing Virtual Firewalls," in *Proceedings of the IEEE Conference on Network Function Virtualization and Software Defined Network (NFV-SDN)*, (San Francisco, CA), pp. 107–114, November 2015.

[48] P. Yasrebi, S. Monfared, H. Bannazadeh, and A. Leon-Garcia, "Security function virtualization in software defined infrastructure," in *Proceedings of the IFIP/IEEE International Symposium on Integrated Network Management (IM)*, (Ottawa, ON), pp. 778–781, May 2015.

[49] P. Yasrebi, S. Bemby, H. Bannazadeh, and A. Leon-Garcia, "VNF Service Chaining on SAVI SDI," in Proceedings of the First EAI International Conference on Future Access Enablers for Ubiquitous and Intelligent Infrastructures (FABULOUS), (Ohrid, Republic of Macedonia), pp. 11–17, September 2015.

[50] H. Jang, J. Jeong, H. Kim, and J.-S. Park, "A Survey on Interfaces to Network Security Functions in Network Virtualization," in *Proceedings of the 29th IEEE International Conference on Advanced Information Networking and Applications Workshops (WAINA)*, (Gwangiu, Korea), pp. 160–163, March 2015.

[51] M. Bouet, J. Leguay, T. Combe, and V. Conan, "Cost-based placement of vDPI functions in NFV infrastructures," *International Journal of Network Management*, vol. 25, no. 6, pp. 490–506, 2015.

Biography

Egemen K. Çetinkaya is an Assistant Professor of Electrical & Computer Engineering at Missouri University of Science and Technology (formerly known as University of Missouri-Rolla). He received his Ph.D. in Electrical Engineering from the University of Kansas in 2013. He received his B.S. degree in Electronics Engineering from Uludağ University (Bursa, Turkey) in 1999 and the M.S. degree in Electrical Engineering from the University of Missouri- Rolla in 2001. He held various positions at Sprint as a support, system, and design engineer from 2001 until 2008. His research interests are in resilient networks. He is a senior member of the IEEE, Communications Society, HKN, a member of ACM SIGCOMM, and Sigma Xi.

IEEE Computer Society

IEEE computer society
CELEBRATING 70 YEARS

Celebrating its 70th anniversary this year, IEEE Computer Society is the computing industry's unmatched source for technology information and career development. The Society offers a comprehensive array of industry-recognized products, services, and professional opportunities. Known as the community for technology leaders, IEEE Computer Society's vast resources include membership, publications, a renowned digital library, training programs, conferences, and top-trending technology events. Visit www.computer.org for more information on all products and services.

IEEE 802

The history of computer networking technologies is rich with innovation and rapid progress. This is due in no small part to the Society's creation of the IEEE 802 LAN/MAN Standards Committee (LMSC) in 1980, chartered to develop and maintain networking standards and recommended practices.

The Computer Society publishes more than a dozen magazines that represent the best in current research, development, and timely information, and publishes and co-sponsors more than 20 peer-reviewed technical journals. The *MyComputer* app serves the mobile world by delivering magazine articles to you on just those topics you desire. The *myCS* app organizes all your magazine subscriptions for easy access and reading.

As a professional education resource, the Computer Society offers a wide selection of review and special topic courses for certifications. This includes *SWEBOK V3*, the internationally respected *Guide to the Software Engineering Body of Knowledge*. Recently launched, *Quartos Online Courses* are peer-reviewed, online learning modules that quickly bring technology professionals up-to-date on the latest developments in hot technologies such as Big Data and Cybersecurity.

The Computer Society sponsors a wide range of geographically diverse technical conferences, symposiums, and workshops. These provide computing professionals with innovative forums to facilitate the identification, creation and exchange of peer-reviewed scientific and technological knowledge.

TechIgnite
A ROCK STARS OF TECHNOLOGY EVENT

A premier event on the IEEE Computer Society calendar is *TechIgnite*, a rock star event and expo-- an action-packed two days of acumen from industry leaders. Steve Wozniak, founder of Apple Computer, and Grady Booch, Chief Scientist of Software Engineering at IBM will headline *TechIgnite* by participating in fireside chats. Other expert speakers will share strategic insights that address current industry concerns and meet future challenges. The event will be held 21-22 March 2017 in San Francisco. For more information, visit www.computer.org/techignite.

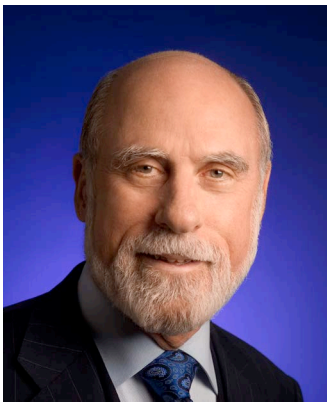
IEEE COMPSAC
1977 - 2016
40th Anniversary

The Computer Society's 40th International COMPSAC Conference takes place in Atlanta, Georgia from 10-14 June 2016. COMPSAC is the IEEE Computer Society Signature Conference on computers, software, and applications. It is a major international forum for academia, industry, and government to discuss research advancements, emerging problems, and future trends in computer and software technologies and applications. This year's theme is "*Connected World: New Challenges for Data, Systems, and Applications*." For more information, go to https://www.computer.org/portal/web/COMPSAC2016.

Coming July 2016:

Future Leaders Forum - A Groundbreaking Opportunity for Learning, Growing and Networking

In July 2016, IEEE-USA, in collaboration with Tulane University, presents Future Leaders Forum, a first-of-its-kind event that will be heating up the streets of New Orleans, bringing together industry, academic and future luminaries in the STEM field. Future Leaders Forum is focused on early career entrepreneurs, innovators and thinkers in the technology fields; enabling attendees to meet world-renowned technology leaders and learn how to become one.



IEEE-HKN Eminent Member, Vint Cerf

Vint Cerf, Vice President and Chief Internet Evangelist for Google, will be kicking off the meeting as the first of many exciting speakers. Others include Jonathan Chew, a Project Coordinator with Walt Disney Imagineering; Tracy Chou, a Software Engineer with Pinterest; William "Whurley" Hurley, IBM Master Inventor and Co-founder of Chaotic Moon Studios and Honest Dollar (who recently planned a dinner for President Barack Obama at this year's South by Southwest in Austin); Lisette Titre-Montgomery, a video game developer for such games as Sims4 and The Simpsons; and Tiago Sousa, a Lead Renderer Programmer for the legendary video game DOOM.

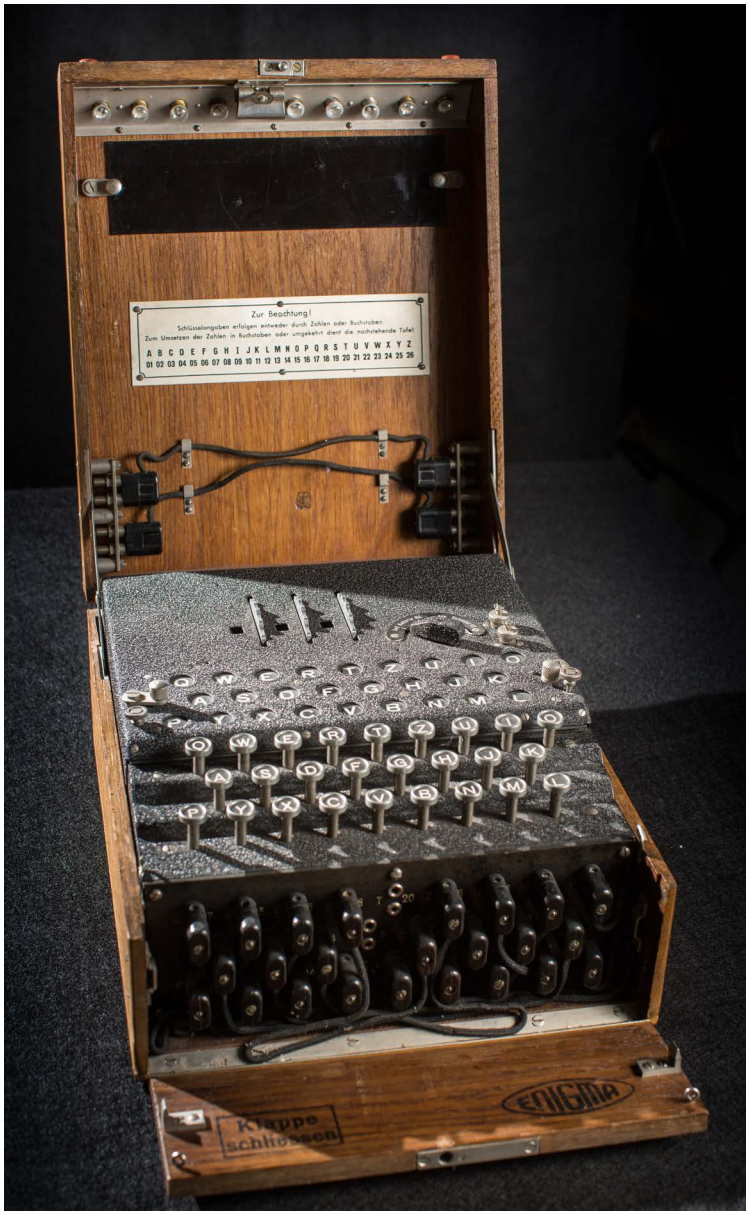
Speakers will present both TEDx-style talks, along with panel discussions, ranging in topics from addressing common challenges faced by young professionals, to empowerment within diverse work environments. In the afternoons, attendees will have the opportunity to break out into "Learning Labs." Led by professionals, these sessions relate to everything from prototyping to storytelling.

No trip to New Orleans is complete without exciting evening activities that will allow attendees to soak in its acclaimed (and even infamous) culture. From trips down the Natchez in an authentic New Orleans steamboat, to a tour of a Mardi Gras float factory and sunset dinner in an antebellum mansion, to live bands, there will be endless opportunities throughout the event to give attendees a classic New Orleans experience.

Future Leaders Forum will run from Thursday, 28 July to Saturday, 30 July 2016. Please visit the website at http://futureleaders.ieeeusa.org/ for more information about speakers, registration, lodging and partnership opportunities. We look forward to seeing you in New Orleans in July. Laissez les bons temps rouler!

The Enigma Machine

The Enigma Machine design was invented by Arthur Scherbius, a German electrical engineer, in the early 1900's. Enigma Machines are electro-mechanical devices for encrypting and decrypting communication; the operating principle of which is letter substitution. The positions of internal rotors determine the alphabetic substitution, and the rotor position changes for each subsequent letter. The choice of rotors used, the initial settings, and variable operating procedure determine the overall complexity and security of the coding. This approach led to improve Enigma machines that were heavily used by the German military during World War II. The figure shows a period Engima machine.



Three-Rotor Enigma Machine. Image courtesy of The Museum of World War II, Boston, MA.

Polish mathematicians, Marian Rejewski, Jerzy Różycki, and Henryk Zygalski, did early work toward deciphering the Engima approach as members of the Polish Cipher Bureau, and later collaborated with British code breakers at Bletchley Park, U.K. These efforts, aided by captured machines and Enigma operator carelessness, resulted in the successful deciphering of numerous German messages and contributed to ending the war. In recognition of their contributions, IEEE honored Rejewski, Różycki, and Zygalski with an IEEE Milestone in 2014, and the Bletchley Park Program with a separate IEEE Milestone in 2003. The recognition plaques are located in the Bletchley Park Museum (U.K.), respectively. Details are given at the Engineering and Technology History Wiki (supported by the IEEE History Center):

http://ethw.org/Milestones:First_Breaking_of_Enigma_Code_by_the_Team_of_Polish_Cipher_Bureau,_1932-1939

and

http://ethw.org/Milestones:Code-breaking_at_Bletchley_Park_during_World_War_II,_1939-1945

The IEEE Milestone Program is administered by the IEEE History Center, IEEE History Committee. Milestones honor significant achievements in the history of electrical and electronics engineering.

For further study, S&T Geotronics LLC (http://www.stgeotronics.com) offers an Engima replica kit. See, S. Cass, "A Simple Engima," *IEEE Spectrum*, 52(1) 19-20 (2015).

2016 IEEE-HKN Student Leadership Conference

The annual IEEE-HKN Student Leadership Conference is a signature program of the Society, and is an opportunity for chapters from around the globe to meet with other officers, members, faculty advisers, members of the Board of Governors, and staff. The conference includes opportunities for professional development, leadership training, networking, and fun activities!

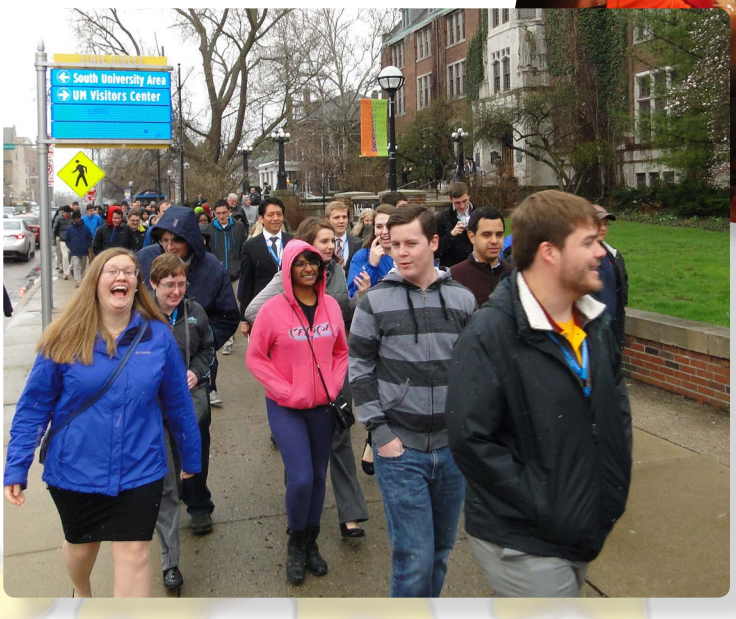
The 2016 Student Leadership Conference, hosted by the Beta Epsilon Chapter, University of Michigan, was held on 1-3 April at the University in Ann Arbor, MI, U.S. Over 190 attendees, representing 47 chapters, enjoyed an exciting weekend of events and programs including a presentation on EPICS in IEEE, presented by Ray Alcantara (EPICS in IEEE Program Manager). Keynote Speakers included: Dug Song, (CEO/Co-Founder of Duo Security); Elie Track (CEO of nVizix); Burt Dicht (IEEE Director, University Programs); Cass Kuhl (High Voltage Electrical Power System Manager, NASA Glenn Research Center); Rich Gray (Manager, U.S. Power Systems Solutions, S&C Electric Company); Michael Hand, III (R&D Engineer, Ford Motor Company); and an Entrepreneurship Panel led by Rob Malda, also known as "Commander Taco", creator of the website Slashdot.org.

IEEE-HKN
Student Leadership Conference 2016

Photo Credit: Dallas Ostin

◀ 2016 SLC attendees in front of University of Michigan's Michigan Union Building. A bit of trivia…John F. Kennedy first proposed the idea for the Peace Corps during his 1960 campaign in front of this building. ▼ SLC Audience

▼ Touring U Michigan



The weekend's activities included a reception and presentation at the Ann Arbor Distillery; trips into Ann Arbor to experience local nightlife, arcades, and "Wolverine" hot spots. Sunday featured a tour to the "Big House" University of Michigan Stadium and the University of Michigan's north and central campuses, and ended with lunch for the attendees.

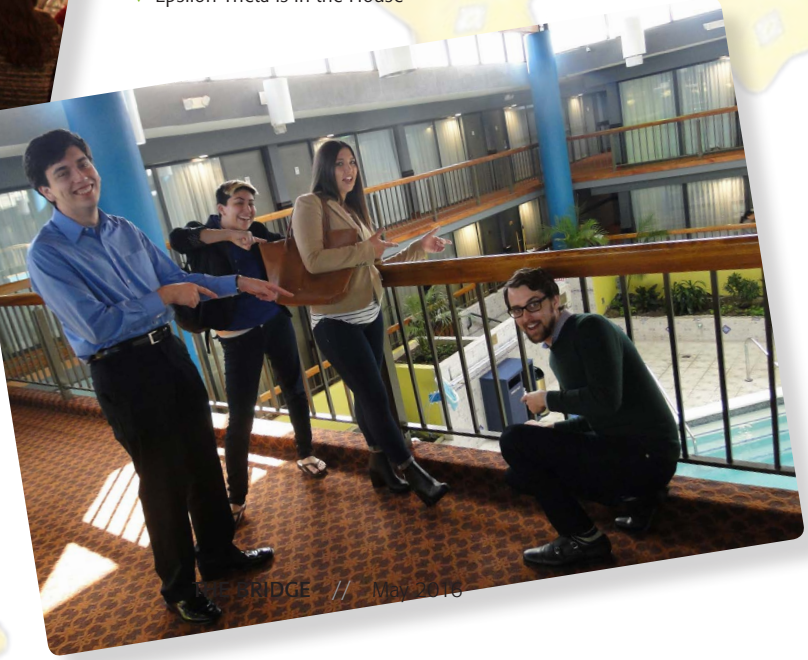
▲ HKN Stars

▼ Getting Serious about Giving Back--EPICS in IEEE

▲ Entrepreneurship Panel and Audience

▼ Epsilon Theta is in the House

▲ Snowing around the Campus



On behalf of the Beta Epsilon Chapter at the University of Michigan, we'd like to thank everyone that came to Ann Arbor to join us for the Student Leadership Conference. Focusing on building a balanced engineer, we heard from speakers from across our profession. Yes -- great presentations, food, tours, and fun -- but most importantly, we met new people and got to know one another! As summer approaches and our thoughts turn to the next academic year, we hope that you will keep the fire of ingenuity burning and that you return to your campuses in the fall with a renewed dedication to making IEEE-HKN a shining light on your campus.

▶ Rebooting Computing at the Distillery
▼ Huge Konference Now

▲ Delta Epsilon at SLC
▼ Elie Track Rebooting Computing Conference October 2016

▲ NASA Swag

For those of you that are graduating this year, congratulations on your accomplishment! We hope you will return as an alumnus to next year's conference and share your experiences, as both a student leader and a working professional, with the next generation of electrical and computer engineers -- computer scientists too!

-Kyle Lady & Michael Benson
2016 HKN Student Leadership Conference Co-chairs

Iota Phi Induction Ceremony - A Historic Moment at West Point

by: Nancy Ostin, Director, IEEE-HKN

At the invitation of IEEE President & CEO, Colonel Barry Shoop, IEEE-HKN President, S.K. Ramesh and I attended the Iota Phi Chapter induction ceremony at the United States Military Academy - West Point on 4 April 2016. Congratulations to the cadets and officers who were inducted, and thank you to the officers and members of Iota Phi for their warm welcome and the precision performance of the induction ritual.

This marks the first time that the IEEE President, IEEE-HKN President, and IEEE-HKN Director have all been present at a chapter induction ceremony. The day following the ceremony COL Shoop took Ramesh and me on a tour of the beautiful campus and facilities at West Point. We were able to visit the labs, observe the students working on their capstone projects, and experience the first engineering program in the US with state-of-the-art facilities of this unique program.

It was an honor to attend the Iota Phi ceremony and to be given a tour of West Point by COL Shoop. On behalf of Ramesh and IEEE-HKN, a huge thank you for the personal invitation.

IEEE-HKN Iota Phi Chapter at West Point. Center: S.K. Ramesh, IEEE-HKN President; Right Center: IEEE President and CEO, Barry Shoop; Left Center: Director, IEEE-HKN, Nancy Ostin

Iota Phi Induction Ceremony

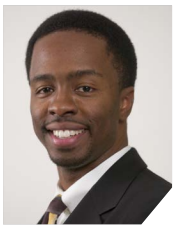
New Editorial Board Members

Dr. John Seiffertt is an Assistant Professor of Computer Science at Truman State University in Kirksville, Missouri, U.S.

John previously taught in the ECE department at the Missouri University of Science and Technology, after receiving his PhD in Computer Engineering from that institution. His research is in the areas of computational intelligence and agent-based modeling.

Dr. Seiffertt has published work in several IEEE Transactions journals, presented at international conferences, and authored the Springer books *"Unified Computational Intelligence for Complex Systems"* and the forthcoming *"Digital Logic for Computing."* With interests across the field, from embedded systems to Turing machines, John is an award-winning teacher committed to helping undergraduates in their personal and professional growth as they become the next generation of technologists on their way to helping to improve our world.

Marcus A. Huggans, PhD



Dr. Marcus A. Huggans is a Senior Director of External Relations at the National GEM Consortium. He is a native of St. Louis, Missouri. He received his BS degree in Electrical Engineering and his MS & PhD in Engineering Management at the Missouri University of Science and Technology previously know as University of Missouri - Rolla (UMR). Dr. Huggans is an alumnus of the GEM Fellowship Program.

Dr. Huggans served as the Director of the Student Diversity and Academic Support Program at Missouri (S&T). Under his leadership, S&T experienced unprecedented growth in the recruitment of under-represented minority students in the areas of science and engineering. At GEM, Marcus recruits and conducts graduate programming to encourage under-represented minority students to pursue their graduate degrees in science, technology, engineering, and applied mathematics (STEM) fields; he has extensive experience in the STEM field with over twenty years of working in the industry. He has worked for 3M Company, AT&T Bell Laboratories, Department of Justice-Federal Bureau of Investigation (FBI), and Texas Instruments, Inc.

Currently, Dr. Huggans resides in Dallas, TX with his wife Melanie, daughter Hannah, and son Ellis.

New Chapter Installations

"I sincerely promise that I will live up to, in word and in deed, the principles for which IEEE-Eta Kappa Nu stands. To the members now and to those to come after, I bind myself to the faithful observance of these promises. I give my solemn word of honor." These were the words spoken by all new inductees.

Welcome to the new Chapters, Charter Members, and Faculty Advisors installed to date this year:

Mu Theta Chapter - Chulalongkorn University, Pathumwan, Bangkok, Thailand - Installed 7 March 2016
Mu Delta Chapter - Eastern Washington University, Cheney, WA - Installed 9 March 2016
Mu Epsilon Chapter - Singapore University of Technology and Design (SUTD), Singapore - Installed 8 January 2016
Mu Zeta Chapter - Western Washington University, Bellingham, WA - Installed 15 January 2016

The University and Charter Members are honored to create these Chapters of IEEE-Eta Kappa Nu. The Chapters will provide a channel that will be used to support students, as well as honoring and giving recognition to those who will join their Chapters in the future.

The Chapter members will motivate, encourage and set an example for other students by exhibiting the three central ideas of IEEE-HKN: 1) **Scholarship**, which includes common sense and resourcefulness; 2) unimpeachable **Character,** including sound judgment, ethical behavior and a willingness to work hard; and 3) a positive **Attitude** and outlook on life, including tolerance for others and dependability. Through these actions and conduct, these Chapters aim to improve their schools, aid and assist their communities, and contribute to the engineering profession as a whole.

Welcome Back!

IEEE-HKN is proud to welcome back these reactivated chapters:

Kappa Xi Chapter - University of South Florida
Iota Omega Chapter - California State University, Fullerton

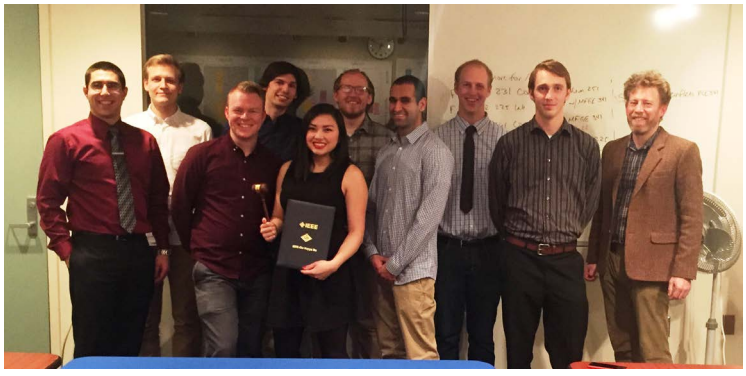
We thank the faculty advisors, department chairs, and student members of these Chapters for their dedication to reactivate their Chapters.

If you know of a chapter that would like to resume active status, we are eager to work with you. Please contact Nancy Ostin, Director, IEEE-HKN, at n.ostin@ieee.org.

Mu Theta Chapter - Chulalongkorn University, Pathumwan, Bangkok, Thailand

Mu Delta Chapter - Eastern Washington University, Cheney, WA

Mu Epsilon Chapter - Singapore University of Technology and Design (SUTD), Singapore



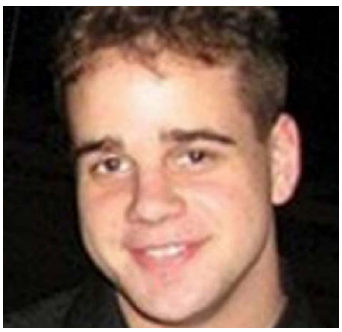
Mu Zeta Chapter - Western Washington University, Bellingham, WA

SUNY-Stony Brook - Theta Mu Chapter… Making a Difference

IEEE-HKN chapters make an impact on their members, universities, and their community. On Valentines' Day 2016, the IEEE-HKN SUNY-Stony Brook Chapter created a "Wall of Love" where people could post notes about things they love. The "Wall" was present at their University's *Involvement Fair* in their engineering building. A short video of the "Wall" can be found at: https://www.youtube.com/watch?v=d5MRnelnj5k
Students sold LED roses and boxes of chocolates to help raise money for the Artem Ayzen Fund.

Wall of Love

Artem Ayzen was a gifted engineer and student at Stony Brook University. Before he came to Stony Brook, Artem was torn between architecture and engineering. Architecture, like engineering, celebrates the creation of beautiful, practical, and useful things. Though he chose to major in engineering, Artem remained steadfast to his beautiful and original creations. His palette contained microprocessors, LEDs, and circuit boards, and he became a master of practical, economical, and innovative works.


Artem Ayzen 1990-2014

To celebrate and honor Artem's memory, a competition was held to come up with an invention, project, or idea related primarily to a STEM field. The competition was for Stony Brook students, with teams headed by students in the College of Engineering and Applied Sciences. The project was judged based on its originality, artistry, practicality, impact, and ability to honor the cross-disciplinary interests of their treasured friend and colleague. All money raised was put toward a scholarship to fund the winning team's project to help it become a reality.

How is your Chapter making a difference? Each year IEEE-HKN chapter members tutor other students, mentor underclassmen, organize extra labs, assist with homework, develop and present technical programs and career fairs, and in addition, organize STEM activities and reach out into their communities. How is your chapter making a difference? Please be sure to let us know at info@hkn.org


Artem taught students to make LED flowers

Adrian Sutinjo

MEMBER PROFILE

Adrian Sutinjo received his BSEE degree from Iowa State University (1995), his MSEE degree from the University of Missouri-Rolla (now, Missouri S&T) (1997), and his PhD degree in electrical engineering from the University of Calgary, Canada (2009).

From 1997 to 2004, he was an RF Engineer for Motorola (in the Chicago area) and Murandi Communications Ltd. (Calgary, Canada); from 2009 to 2011, a Postdoctoral Research Associate at the University of Calgary, and from 2012 to 2014, a Senior Research Fellow with the International Centre for Radio Astronomy Research (ICRAR) at Curtin University, Bentley, Western Australia.

At ICRAR/Curtin, Adrian worked with low-frequency aperture arrays (LFAA); this work was a part of a multinational effort towards the Square Kilometre Array (SKA) LFAA. Since 2015, he has been a Senior Lecturer in the Department of Electrical and Computer Engineering at Curtin University. His research interests include antennas, RF and microwave engineering, electromagnetics, and radio astronomy engineering.

How has Eta Kappa Nu (IEEE-HKN) impacted your life? Your career?

These qualities inspire me to perform my very best every day:

"…members of IEEE-Eta Kappa Nu (IEEE-HKN): possess an unimpeachable character; are able to make use of the knowledge and information acquired; have the capacity and willingness for hard work; work in harmony with all types of people; and have a genial nature."

What inspired you to choose the engineering field?

I have always been intrigued by waves and propagation; particularly ones you can't see, such as radio waves. As a child, walkie-talkies and remote-controlled cars fascinated me. I wondered how voice and information traveled through space. This led to a hobby in electronics in my teenage years, and to a major in Electrical Engineering in university.

What do you love about engineering?

I love how engineers solve problems through the right mixture of theory and practice. Theory lets us understand the interplay among critical parameters; practice helps us select the appropriate theory to employ in a given problem. Knowing the right mixture comes with experience. I enjoy seeing these dynamics at play in projects that I have been a part of.

Whom do you admire and why?

My grandmother -- Despite living through adversities during World War II in Dutch East Indies (now, Indonesia), including the period of Japanese occupation, she remained the most generous and positive person I had ever known. She emerged from that experience determined, and afterwards,

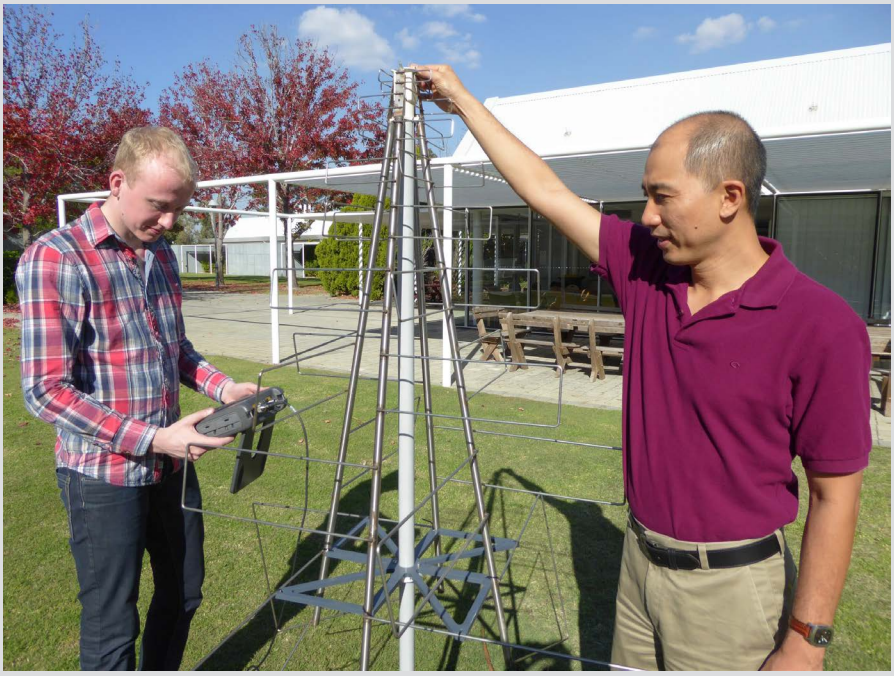
went on to found a successful family business. I admire her for being determined, yet generous.

In your opinion, what has been the greatest change in engineering since you were a student?

I have definitely witnessed an explosion in computing in terms of capability and ease of access. When I started, I had to complete programming assignments in university computer labs on VAX terminals. I can now run, on a laptop, much more extensive calculations with off-the-shelf software packages at speeds unimagined back then. Along with that, I have also seen a revolution in test equipment technology. We can now purchase a handheld instrument that used to occupy racks of space 20 years ago. And yes, we can nicely save and display lots of data without having to use the plotter!

I wish I had known…

The importance of clear thinking--particularly in large projects. Writing down a clear set of requirements, priorities, and objectives helps this process. Many times complex projects involving multiple personnel, long timelines, and large budgets lose sight of these and flounder.



Rene Baelemans and Adrian. Example of a prototype log-periodic "SKALA" antenna for LFAA* developed by the Cavendish Laboratory, Cambridge University, U.K.

* For a summary of recent work in low-frequency radio astronomy prototyping in Western Australia, please refer to Sutinjo, A.; Colegate, T.; Wayth, R.; Hall, P.; de Lera Acedo, E.; Booler, T.; Faulkner, A.; Feng, L.; Hurley-Walker, N.; Juswardy, B.; Padhi, S.; Razavi-Ghods, N.; Sokolowski, M.; Tingay, S.; Vaate, J., "Characterization of a Low-Frequency Radio Astronomy Prototype Array in Western Australia," in *Antennas and Propagation, IEEE Transactions on* , vol.PP, no.99, pp.1-1, doi: 10.1109/TAP.2015.2487504

Be knowledgeable in fields related to your specialization--see the "big picture."

Best advice for new graduates…

Pursue excellence in your work; see how you can go the extra mile. Learn to write and speak clearly about what you are doing. Never stop learning; education is a lifelong process. Be knowledgeable in fields related to your specialization--see the "big picture."

From your perspective, what's the next BIG advance in engineering?

Engineering has improved our convenience greatly with the ease of connectivity we now enjoy. It is likely that the world of personal electronics and software will continue to grow and offer us more. However, I think there will be increasing attention paid to optimizing the use of resources. As the world's population continues to grow, the questions of sustainable energy and renewable resources will become more pressing. This will be a matter beyond personal convenience; it affects humanity as a whole.

STUDENT PROFILE

Christian Ladigoski

Christian Ladigoski resides in Smithtown, NY, and is a senior at Hofstra University in Hempstead NY majoring in Electrical Engineering. He is President of the IEEE-HKN Lambda Xi Chapter at Hofstra, and is also President of the IEEE Student Branch.

Christian has significant academic and professional achievements; he is a member of Hofstra's Dean's List, and won the Leadership Award for WRHU Radio (2015). He was also selected as a member of the Hofstra Fall Court for his overall academic and professional excellence.

Christian completed his internship with NBC, and is currently interning with Disney and the ABC Corporation.

What has it meant to you to be inducted IEEE-HKN?

I believe that being a part of IEEE-HKN makes me recognize my potential as an academic student and as a person. IEEE-HKN recognition goes beyond the experiences of the classroom; you realize the supportive network and the group of like-minded individuals that only strive to be the best and change the world for the better!

Why did you choose to study the engineering field?

Two main reasons: 1) I always saw myself as someone who was curious about everything. I always asked the question, "How do things work?" Sometimes, I'd ask my Dad a million questions; sometimes he was able to answer, other times he would tell me to "figure it out and discover it yourself." With this curiosity and my already given interest in math and science, engineering seemed to be the perfect fit to unlock those questions; and 2) I chose Electrical Engineering specifically for my passion for music and sound! As a kid, I always had a good ear for things and loved to create music, sound design for films, and creative sounds. I wanted to take that other step to learn how sound is developed from energy, to an experience for people to listen to!

What do you love about engineering?

Engineering gives me the chance to explore the base knowledge of all applications, energy, and processes that all people use on a daily basis. Knowing that we live in a technology age where our generation is solely dependent on its applications, it's best to know how it's put together and how it works. There is always something new to learn; I appreciate the broad spectrum of topics and applications we learn about from computer, power, signal, circuits and design. My favorite topics include RF, Radar, Signal Processing, Communications, and anything to do with frequency!

What is your dream job?

My dream job comes with two answers and comes with a surprise to most reading this: 1) to be a CEO/CTO of a major media/entertainment company; 2) to be working in a technical

Christian at ABC Corporation

broadcast/audio role for a TV/film company. The reason why is because I know that with my technical and media backgrounds, I can pursue two passions at once -- by combining technology and media into one industry.

Whom do you admire (professionally and/or personally) and why?

People like Walt Disney, Steve Jobs, Bob Iger, and Steve Burke because they may not have been the biggest technical minds, but they were innovative in the design and creation of major media companies. They are the engineers of creating great content, great people and a great life!

I also personally admire my mother, my best friends, and my girlfriend, because they are the most inspirational and supportive people I have in my life right now. They are always encouraging and caring, and see me push myself. I appreciate to unlimited ends how much they care for what I am doing in my career -- wherever it takes me.

What is the next BIG advance in engineering?

I believe the focus will be toward Artificial Intelligence and Neurology, as well as applications in computers and Robotics Technology. I believe there will be a continuing acceleration of technology advances that will better our lives and tasks, while making computers smarter and faster.

What is the most important thing you've learned in school?

I've learned at school and in my major, "There is always a solution to every problem." I realized that while something can be complex, there are always solutions and conclusions. Where many people can come face to face with problems on a daily basis, I have learned to take a step back, analyze and assess the problem, and figure out the best solution. It could deal with academics, people, events, etc. Whatever it may be, it has taught me to be responsible for solving problems that best benefit people and society.

Christian during his internship at NBC

What advice would you give to other students entering college and considering studying your major?

I would tell students that if they are considering studying Electrical Engineering, they must be prepared to understand that it requires a specific mind-set. Being great at math and science is one thing, but you also have to be curious, never stop asking questions, and always pursue the solution -- even if it takes forever to figure out. Being in this discipline is a lot of hard work, but can also be very rewarding when knowing how to apply it to real situations.

Also, start talking with professors and IEEE members, and create informational interviews for yourself (the reason I got my internships). Taking the step forward outside of the classroom will benefit you in the long run. Also remember to keep your mind open; because it isn't just a math problem where there is only one solution, sometimes with design, you have to consider multiple solutions.

2017 IEEE-HKN Board of Governors

The Nominations and Appointments Committee of IEEE-HKN invites all active chapters to submit nominations for the following open positions on the 2016 Board of Governors.

According to the governing documents of IEEE-HKN, nominations can be made electronically or in writing to the IEEE-HKN Nomination and Appointments Committee at info@hkn.org or to IEEE-HKN, 445 Hoes Lane, Piscataway, NJ 08854 U.S., Attn: N&A Committee. The deadline for nominations is 30 June.

1-Year Term:

President-Elect

Student Representative

3-Year Term:

Governor: Regions 1-2*

Governor: Regions 7-10*

Governor-at-Large

**Nominations can only be made by chapters in the regions they represent.*
The IEEE-HKN Operations Manual can be found on the website at
http://www.ieee.org/education_careers/education/ieee_hkn/about/operations_manual.pdf

2014-2015 IEEE-HKN Outstanding Chapter Awards

The Outstanding Chapter Award is presented annually to IEEE-HKN chapters in recognition of excellence in their chapter administration and programs. Recipients are selected on the basis of their annual chapter report. Winning chapter reports showcase their chapter's activities in an individualized manner, and provide multiple views and instances of the work that brought their chapter's activities to life. Of critical concern to the Outstanding Chapter Awards evaluation committee in judging a chapter are activities to: improve professional development; raise instructional and institutional standards; encourage scholarship and creativity; provide public service to the community; and generally further the established goals of IEEE-HKN. The awards were presented at a special reception on 21 March 2016, during the Electrical and Computer Engineering Department Heads Association (ECEDHA) Annual Conference in La Jolla, CA.

Group photo of 2015 Outstanding Chapter awardees. Nancy Ostin, Director, IEEE-HKN and S.K. Ramesh, President, IEEE-HKN Board of Governors (front center)

Collectively, our IEEE-HKN chapters contributed 53,750 hours of service to others. What an amazing impact we have on fellow students, our universities and the communities we serve!

The IEEE-Eta Kappa Nu (IEEE-HKN) Board of Governors has conferred on the following IEEE-HKN Chapters the 2014-2015 IEEE-HKN Outstanding Chapter Award:

Arizona State University	Epsilon Beta Chapter
Binghamton University	Kappa Epsilon Chapter
Georgia Institute of Technology	Beta Mu Chapter
Iowa State University	Nu Chapter
Kansas State University	Beta Kappa Chapter
Lehigh University	Chi Chapter
Massachusetts Institute of Technology	Beta Theta Chapter
Mississippi State University	Gamma Omega Chapter
Missouri University of Science & Technology	Gamma Theta Chapter
North Carolina State University	Beta Eta Chapter
Purdue University	Beta Chapter
SUNY - New Paltz	Kappa Omicron Chapter
Texas A&M University - Kingsville	Zeta Beta Chapter
UCSI University	Mu Alpha Chapter
University of Arizona	Iota Xi Chapter
University of California Berkeley	Mu Chapter
University of California, Los Angeles	Iota Gamma Chapter

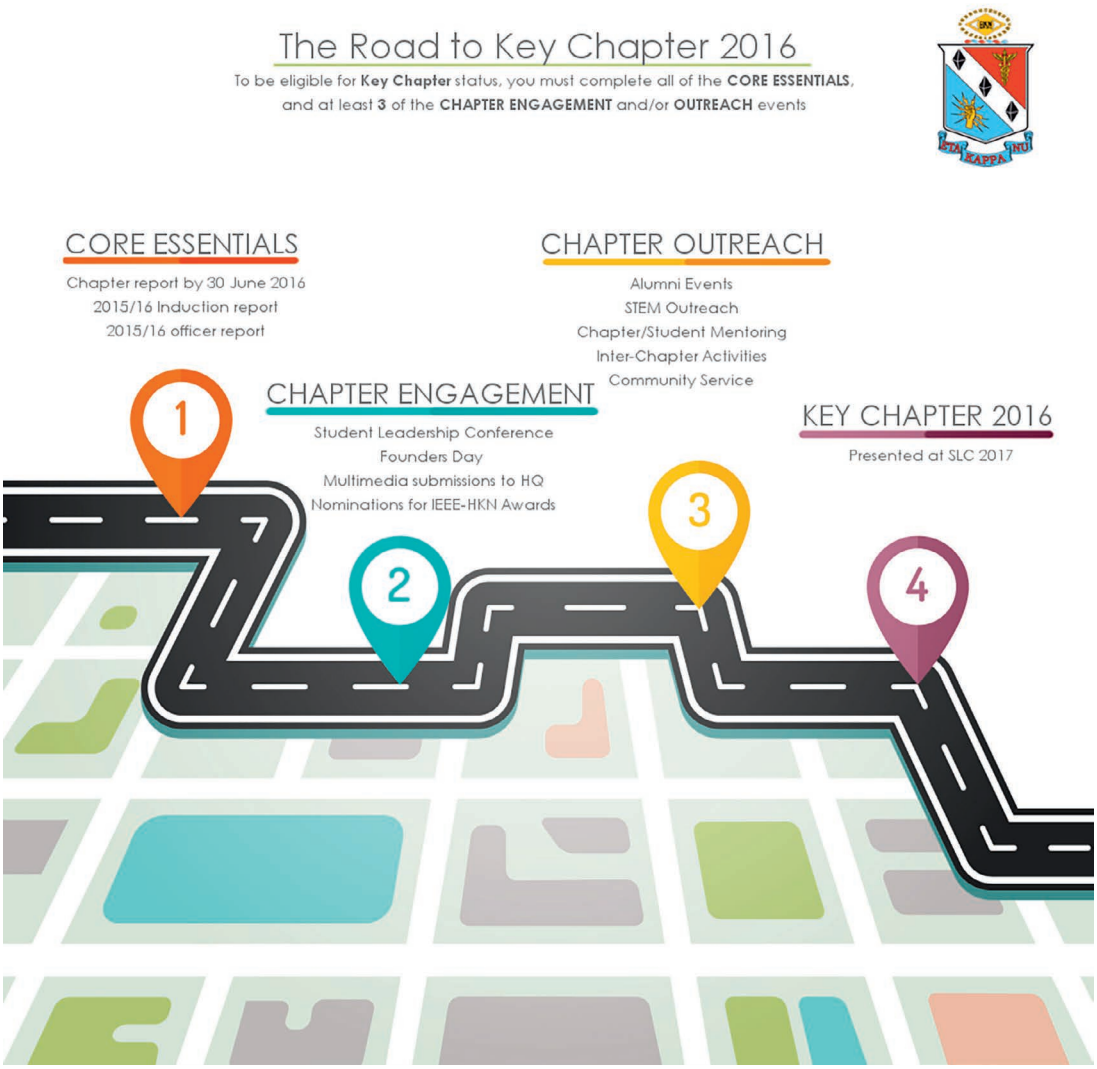
University of Colorado at Boulder
University of Hawaii at Manoa
University of Michigan
University of Missouri
Wichita State University

Rho Chapter
Delta Omega Chapter
Beta Epsilon Chapter
Iota Chapter
Epsilon Xi Chapter

How can your chapter be selected as an "Outstanding Chapter?" You must submit your annual chapter report; be sure to count all of your service hours and complete all of the required information at http://goo.gl/forms/Pd4RVZiN3c

Direct questions to info@hkn.org or call us toll free at (800) 406 2590.

Left to Right: Khalil Najafi, ECEDHA BoD; Martin Cooper, IEEE-HKN Eminent Member; Athina Petropulu, ECEDHA BoD; Irwin Jacobs, IEEE-HKN Eminent Member; Nancy Ostin, Director, IEEE-HKN; S.K. Ramesh, President IEEE-HKN; Max Nikias, President, USC; and John Janowiak, ECEDHA BoD.



IEEE-HKN Outstanding Student Award

The Alton B. Zerby and Carl T. Koerner Outstanding Electrical and Computer Engineering Student Award recognizes outstanding scholastic excellence and high moral character, coupled with demonstrated exemplary service to classmates, university, community, and country. The 2015 Outstanding Student Award was presented to Sarah Rose Kouroupis at a dinner ceremony on 21 March 2016, during the Electrical and Computer Engineering Department Heads Association (ECEDHA) Annual Conference in La Jolla, CA.

Sara Kouroupis, originally from Ellicott City, MD, completed her undergraduate degree at Auburn University. She graduated from the Honors College with a bachelor's degree in Electrical Engineering, and a minor in Business Engineering Technology.

While at Auburn, Sara held leadership positions in organizations including: the Eta Kappa Nu XI Chapter; the Society of Women Engineers; the Student Alumni Association; and the University Program Council. She also worked at the Auburn University Recreation and Wellness Center where she taught group fitness classes and performed administrative duties. In 2015, Sara received the Auburn University College of Engineering President's Award, and was also the Auburn University Electrical Engineering Student of the Year.

Sara is currently employed by the Johns Hopkins Applied Physics Laboratory, working in the Space Department on the Space-Based Kill Assessment. There, she performs optical sensor calibration tests and models signature data. Sara is also enrolled in a master's program at Johns Hopkins University to earn her graduate degree in Electrical Engineering.

Read: "Award Winning Student Sara Kouroupis Encourages Girls to Follow STEM Passions" in U.S. News and World Report.

Outstanding Student Award Recipient, Sara Kouroupis

Share Your IEEE-Eta Kappa Nu Pride

Official Society Merchandise Now Available

Medal $20	Honor Stole $20
Three Pin Types:	Honor Chord . . . $30
Crest $12	6" Table Covers . $99
Emblem $12	Key Pendant . . . $14
Key $12	Scarf $22
	Necktie $25

Save $10 by purchasing the "honor combo" one honor cord and one honor stole for $40

Save $21 by purchasing 10 of the same style pin for $99

All items available at the IEEE-HKN store at:
bit.ly/IEEEHKNstore

IEEE
Advancing Technology for Humanity

IEEE-Eta Kappa Nu Reminders

Chapter Management News

All Chapter management forms are now available for digital submission at www.hkn.org!

Required Forms

- Student Inductee Documentation – For each Induction Ceremony held
- Notice of Election of Officers – Submit this form every time Chapter Elections are held.
- Annual Chapter Report – Deadline: 30 June

Awards

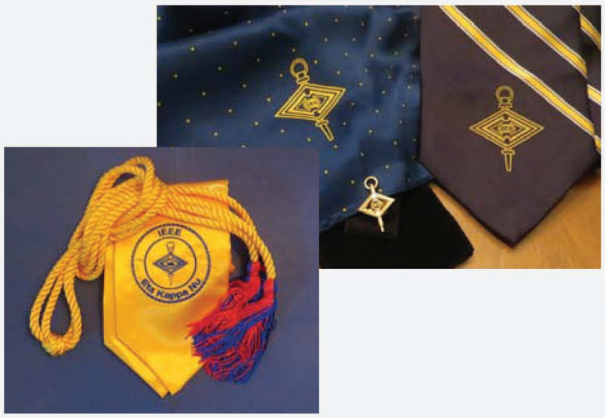
- Outstanding Young Professional Award Nomination Form – Deadline: The Monday following 30 April
- Outstanding Student Award Nomination Form – Deadline: 30 June
- Outstanding Teacher Award Nomination Form – Deadline: The Monday following 30 April
- Karapateoff Outstanding Technical Achievement Award Nomination Form – Deadline: The Monday following 30 April
- Outstanding Chapter Award Nomination – Deadline: 30 September

Other Forms

- New Pledge Form – Submit pledge information and IEEE-HKN Headquarters will send pledges a personal invitation to the submitting Chapter!
- Professional Member Induction Form – For non-student new inductees.
- IEEE-HKN Certificate Replacement Order Form

IEEE-HKN Store

- **Honor Stoles & Cords** – Order early to ensure timely delivery! Rush orders accepted.
- **Pins**
- **Logo Clothing**



Order Online Today!

Online Forms and Payments

You can submit all forms and payments online. If paying with a check, first submit your form online, then mail your check to IEEE-HKN Headquarters. If you have questions, please email info@hkn.org or call U.S. Toll Free +1 800 406 2950 or worldwide +1 732 465 5846.

Like us on Facebook:
www.facebook.com/IEEE.HKN

Follow us on Twitter:
twitter.com/IEEE_EtaKappaNu

Connect with us on LinkedIn:
IEEE-Eta Kappa Nu

facebook twitter LinkedIn

Phone U.S. Toll Free: +1 800 406 2590 Outside the U.S. call: +1 732 465 5846

Email: info@hkn.org Website: www.hkn.org

Chapter News: Let us know what is happening at your chapter!