The Daily Hacker:

Pivot & Bytes

Thursday, September 30, 2021

What's Inside:

- **Welcome from Cyber Huntsville's Jamie Miller**
- **Did You Know?** ***Fun Facts.***
- **Welcome from the NAC-ISSA's Nisheeth Agrawal & Steve Pratt**
- **Conference Happenings**
- **Technical Track Feature Article: Modeling Cyberattacks with Extended Petri Nets**
- **Today's Blog Post: Hacking Memoirs: The Big Casino!**
  - **Joshua Crumbaugh, Chief Hacker/CEO, PhishFirewall™ PeopleSec®**

Jamie Miller, President Cyber Huntsville/President Mission Multiplier

Dear National Cyber Summit Attendee,

On behalf of the Cyber Huntsville organization, thank you for attending this year's National Cyber Summit (NCS)! Despite the on-going concern poised by COVID-19 and a global pandemic, this year's NCS is poised to be the biggest and best yet. We realize that this result is due to your commitment to the cybersecurity industry, and your passion for identifying and developing solutions

for the nation's most serious cybersecurity issues. This commitment and passion are what drives our community to come together in the face of adversity, and what makes the annual NCS conference so special. As President of the Cyber Huntsville organization, we are proud to be the primary sponsor for this year's event.

Over the next few days, we get to hear from world class cyber thought leaders like the CIO of the US Army (Dr. Raj Iyer); the CISO of Optum, United Healthcare Group (Allison Miller); the Former Director of the Defense Intelligence Agency (Lieutenant General Robert Ashley); the Principal Security Architect of Amazon Web Services (Merritt Baer); the Executive Assistant Director, Criminal, Cyber, Response, and Services Branch, Federal Bureau of Investigation (Brian Turner); the Principal Cyber Advisor of the US Navy (Chris Cleary); the Executive Director of Women in Cybersecurity (Lynn Dohm); and the Godfather of Linux, Board Chair of the Linux Professional Institute (Jon "Maddog" Hall); along with special guest, Mr. Paul Puckett, the Director, Enterprise Cloud Management Office, for the US Army. This is a spectacular line-up of speakers, and I can't wait to hear their perspectives and commentary.

For those of you wondering what the Cyber Huntsville organization is all about, we are a 501c-6 (not-for-profit) organization that brings together industry leaders from the government, industry, and academic arenas to help solve the most pressing cybersecurity challenges for our community and for the nation. Our goals are to drive economic growth and advancement through industry collaboration and engagement, increase and promote the cyber workforce and the next generation of "cyber warriors", and to drive innovation by seeing new ideas for future cybersecurity technologies and solutions. We represent hundreds of our member organizations and thousands of individuals who seek to inform the evolution of cybersecurity. We are proud to have created a cyber-center of excellence for our local community and continue to help fuel its continued growth.

To acknowledge the tireless commitment and leadership of our organization, I would like to acknowledge the Cyber Huntsville Executive Committee and Board Directors:

- Jamie Miller, President
- Larry Burger, Executive Vice President
- Shelly Amanik, Board Secretary, Director of Membership
- Chris Patty, VP – Finance
- Ben Denton, VP – Operations
- Gary Anglin, VP – Advisory Council
- Nichole O'Brien, VP – Outreach
- Nisheeth Agrawal, VP – Education, Workforce and Development
- Judy Darwin, VP – National Cyber Summit
- Emily Jones, Director – Economic Development
- Brian Lynn, Director – Exercises
- Rob Goldsmith, Director – Advisory Council
- Brianna Fannin, Director – Events
- Gerry Norris, Director – Marketing
- Tommy Morris, Director – Education
- Matt Osborne, Director – Workforce Development
- Rodney Robertson, Director – Government Affairs

The Cyber Huntsville organization is open to everyone and all organizations, so we highly encourage you to get involved. Please feel free to come by our booth (#624) to talk to our members to learn how you can play a part in our organization. There are so many fun and exciting ways to contribute and add value to our special community. Please consider becoming a member today and participate in exciting future events like our upcoming "Cyber Gala", simulated Cyber Test and Exercises, Job Fairs, and get access to world class cyber luminaries and companies and organizations.

We look forward to meeting you. Please enjoy the conference and thank you for your efforts to help solve today's and tomorrow's cyber challenges!

Cheers,

Jamie Miller

Cyber Huntsville President, Mission Multiplier, CEO

Did You Know? Fun Facts.

[put a cloud or some outline around Did you Know?]

The first rocket that sent man to the moon was developed in Alabama--- Saturn V at the Marshall Space Flight Center in Huntsville, Alabama

Windshield Wipers were first designed and created in Alabama in 1903

Alabama was the first place to celebrate Mardi Gras in 1708

Nisheeth (Nick) Agrawal, President, NAC-ISSA

Steve Pratt, Vice President, NAC-ISSA

A Message from the President & Vice-President

North Alabama Chapter of Information Systems Security Association (NAC-ISSA)

Welcome to the 2021 National Cyber Summit! We are delighted to have you here. The National Cyber Summit is the nation's most innovative cyber security-technology event offering unique educational, collaborative, and workforce development opportunities for industry visionaries and rising leaders. The North Alabama Chapter of ISSA (Information System Security Association) is one of the founding organizations of the National Cyber Summit and has been actively involved since the beginning. ISSA is the community of choice for international cyber security professionals dedicated to advancing individual growth, managing technology risk, and protecting critical information and infrastructure.

The North Alabama Chapter of ISSA consists of over 200 members. We believe in helping our community and helping each other. We can help you earn and track your CPEs while providing networking opportunities with fun and interesting people in your profession. NAC-ISSA helps you get recognized in the community for your unique qualities and skills. We have monthly luncheons with top cyber security speakers introducing our community to the latest security technology and tools. In addition to the National Cyber Summit, NAC-ISSA hosts BSides Huntsville and Rocket Secure cyber conferences each year, connecting you with the best trainings and speakers all year.

Thank you again for attending National Cyber Summit. Our Board of Directors and members look forward to seeing you during this week. Please stop by our booth and say hello. Below is a list of our elected and appointed Board of Directors.

Other Board of Directors of the NAC-ISSA:

Anthony Hale – Treasurer***, Jartinez Boston*** – Secretary, ***Phil Lee*** – Membership and Events Director, ***Jeremy Tourville*** – Equipment and Cyber Range Director, ***Mark Wensyel*** – Web Director, ***David Cybuck*** – BSides Director, ***Marie Held*** – Director at Large, ***Mark Brown*** – Director at Large, ***Gina Holman*** – Director at Large

Conference Happenings

Thursday, September 30th, 2021

What?	When?	Where?
Exhibition Hall Open	**7:00am to 5:00pm**	**Exhibition Hall**
Summit Registration and Information Desk	**7:00am to 4:00pm**	**South Hall Foyer**
Huntsville Street Party	**7:00am to 3:30pm**	**Exhibition Hall, Booth #625**
Women's Breakfast **Sponsored by Deloitte** ***Kamilah Smith, Deloitte*** ***Lynn Dohm, Women in Cybersecurity (WICYS)*** ***Heather Riley, Deloitte*** ***Tonya Ugoretz, FBI***	**7:00am to 8:00am**	**Exhibition Hall-Main Stage**
Networking Breakfast **Sponsored by ASRC Federal**	**7:00am-8:00am**	**Exhibition Hall**
Cyber Cup Challenge	**8:00am to 12:00pm**	**Exhibition Hall**
Opening Remarks	**8:00am-8:15am**	**East Hall**
Keynote Presentation: ***Merritt Baer-*** ***Amazon Web Services***	**8:15am to 9:00am**	**East Hall**
Keynote Presentation: ***Chris Cleary, Principal Cyber Advisor, Navy***	**9:00am to 9:45am**	**East Hall**
Networking Break and Lightning Rounds	**10:00am-10:15am**	**Exhibition Hall**

		Stage 1-Persistence Persistence Persistence: System Firmware Attacks **Stage 2- The Supply Chain Integrity Program of the DIB**
Networking Break and Lightning Rounds	**10:30am-10:45am**	**Exhibition Hall** **Stage 1-Complete CMMC Compliance-A Guaranteed Comprehensive Approach** **Stage 2- Digital Forensics as a Private Investigative Tool**
Keynote Speaker: ***Allison Miller, Chief Information Security Office, Optium Senior Vice President, Global Cybersecurity Office-Optimum Health Group***	**10:45am-11:30am**	**East Hall**
Keynote Luncheon: ***LTG Robert Ashley, Former Director, Defense Intelligence Agency***	**11:45-1:00pm**	**North Hall 2**
Networking Lunch	**11:45-1:00pm**	**Exhibition Hall**
Lightning Rounds	**12:00pm-12:15pm**	**Exhibition Hall** **Stage 1-CyberKnights-Talent Assessment, Development and Retention** **Stage 2- CodeValor-A DevSecOps Tool**
Research Track	**1:15pm-4:00pm**	**North Hall Salon**
Main Stage Panel:	**1:15pm-2:15pm**	**Exhibition Hall Main Stage**

"Blockchain Technology Panel: A Cybersecurity Perspective of Blockchain Technology"---*Moderator: Corey Petty-PhD Chief Security Officer of Status* **Panelists:** **Tom Fuhrman, VECTORmv LLC** **Peder Muller, Chief Systems Architect** **Micahel Solomon, PhD-University of the Cumberlands**		
Breakout Track Sessions: Advanced Manufacturing/SCADA/Supply Chain **"Industry 4.0 and the Industrial Revoltuion"---*Paul Juras, Babson College***	**1:15pm-2:00pm**	**Ballroom 3**
Breakout Track Sessions: Redstone Arsenal Cyber Ecosystem **Remarks by Brad Thomason, Director-Threat Systems Management Office**	**1:15pm-2:00pm**	**Ballroom 4**
Breakout Track Sessions: Technical **"Adversarial-Oriented Approaches to Assessing Risk & Security with NIST 800-172A"----*Dr. Stanley Barr, MITRE & Todd helfrich, Attivo Networks***	**1:15pm-2:00pm**	**Ballroom 1**

Breakout Track Sessions: Advanced Manufacturing **"Cybersecurity Resliency in Manufacturing"----*Nic Cofield, Jackson Thornton Technologies***	**2:15pm-3:00pm**	**Ballroom 3**
Breakout Track Sessions: Redstone Arsenal Cyber Ecosystem **"Missile Defense System Cybersecurity Resiliency Strategy"---*Linda Palmer, Missile Defense Agency***	**2:15pm-3:00pm**	**Ballroom 4**
Breakout Track Sessions: Technical **"Continuous Monitoring for Non-Standard Devices-"---*Bill Floria, FBI***	**2:15pm-3:00pm**	**Ballroom 1**
General Breakout Track Sessions: **"Cyber Risk is Business Risk: How the FBI Can Help"--- *Bryan Vorndran, FBI***	**2:15pm-3:00pm**	**Ballroom 2**
Sponsored Session: System High **"Defense Cyber Operations Panel: Today's Capabilities and Tomorrow's Promise"--- *Moderated by Matt Walker-Deloitte*** **Panelists:** **Tommy Morris, PhD-University of Alabama Huntsville** **Bradley Horton, U.S. Army Threat Systems Management Office** **Ryan Roberts, Deloitte**	**2:45pm-3:45pm**	**Exhibition Hall-Main Stage**

Dr. Casey Wardynski, Former Assistant Secretary-Army for Manpower and Reserve Affairs		
Networking Break	**3:00pm-3:30pm**	**Exhibition Hall**
Raffle and Awards Must be present to win!	**4:00pm-4:45pm**	**Exhibition Hall**

Due to the present dynamic environment, some sessions may be subject to change. For the most up-to-date schedule with any changes can be found on the following QR Code.

Scan this QR code to see the detailed agenda and/or the speaker information

Modeling Cyberattacks with Extended Petri Nets

Authors:
Mikel D. Petty1, Tymaine S. Whitaker1, E. Michael Bearss1, John A. Bland1, Walter Alan Cantrell2, C. Daniel Colvett1, and Katia P. Maxwell3
1University of Alabama in Huntsville, 2Lipscomb University, 5Athens State University

1. Introduction and motivation

Cybersecurity has become an urgent concern. Society is increasingly reliant on computer systems for nearly all aspects of life. There are many threats to those computer systems and the data they contain, including privacy invasion, financial theft, infrastructure sabotage, and election tampering. Motivated by the growing importance of cybersecurity issues, cybersecurity modeling is an active research area, with a wide range of applications and methods.

A team of researchers from three universities, including Athens State University, is conducting several interrelated projects that together form an integrated research program in cyberattack modeling. All of the projects are using an extension of Petri nets as the cyberattack modeling formalism.

2. Background

Petri nets were first formalized in 1962. Petri nets can model discrete, dynamic, and distributed systems. The semantics of Petri nets are oriented towards modeling sequence, concurrency, and synchronization in processes, networks, and workflows. The Petri nets formalism has proven to be highly flexible and extensible, and many applications exist.

In their standard form, Petri nets consist of places and transitions, connected by arcs; the places may contain tokens. A place represents a state or condition in the system or process being modeled by the Petri net. If a place contains a token, that state or condition is interpreted as true. The presence or absence of tokens in the places of a Petri net is referred to as the Petri net's marking. A Petri net's marking when its execution begins is its initial marking. A transition represents an action or event that may change the state or condition of the system. Transitions may have one or more input places, denoted

by arcs directed from the place(s) to the transition, and one or more output places, denoted by arcs directed from the transition to the place(s). If all of a transition's input places contain a token, that transition is said to be enabled. Enabled transitions may fire, which is interpreted as the action represented by the transition occurring. When a transition fires, a token is removed from each of its input places and a token is added to each of its output places. The change in the marking of the Petri net that results from the firing is interpreted as a change in the state of the system or process the Petri net is modeling as a result of the action represented by the firing transition occurring.

In this research program, an extension of Petri nets, referred as PNPSC nets (Petri Nets with Players, Strategies, and Costs) has been developed. PNPSC nets model the dynamic states of system and the events that occur during an attack on that system as markings and transition firings in the PNPSC net respectively. The PNPSC formalism is able to model the essential elements of cyberattacks, including computer systems, their vulnerabilities, the actions taken by competing players to exploit or eliminate those vulnerabilities, and the relative costs of taking those actions. To do so, the PNPSC formalism includes several features of particular relevance to cyberattack modeling. A firing rate associated with each transition specifies the likelihood of an enabled transition firing. Higher rates result in an increased likelihood of firing. Players represent the attacker, defender, and system user in cyberattacks. The players have goals, represented as markings in the PNPSC net that they wish to achieve. The competing players seek to adjust the rates of transitions to influence the sequence of firings, and thus ultimately the markings reached, in order to achieve their goals. To represent the fact that an attacker or defender may not be aware of the complete state of the computer system, each player is only aware of the marking of a subset of the PNPSC net's places, referred to as the player-observable places. Players have strategies, which are their responses to specific markings of the PNPSC net, in the form of desired changes to transitions' firing rates. However, players may not change the rates of any transition in the PNPSC net. Rather, each player has a defined set of player-controlled transitions. A player may only change the rates associated with the transitions that player controls. The players' actions have costs, which abstractly represent the time, effort, skill level, and expense of the action.

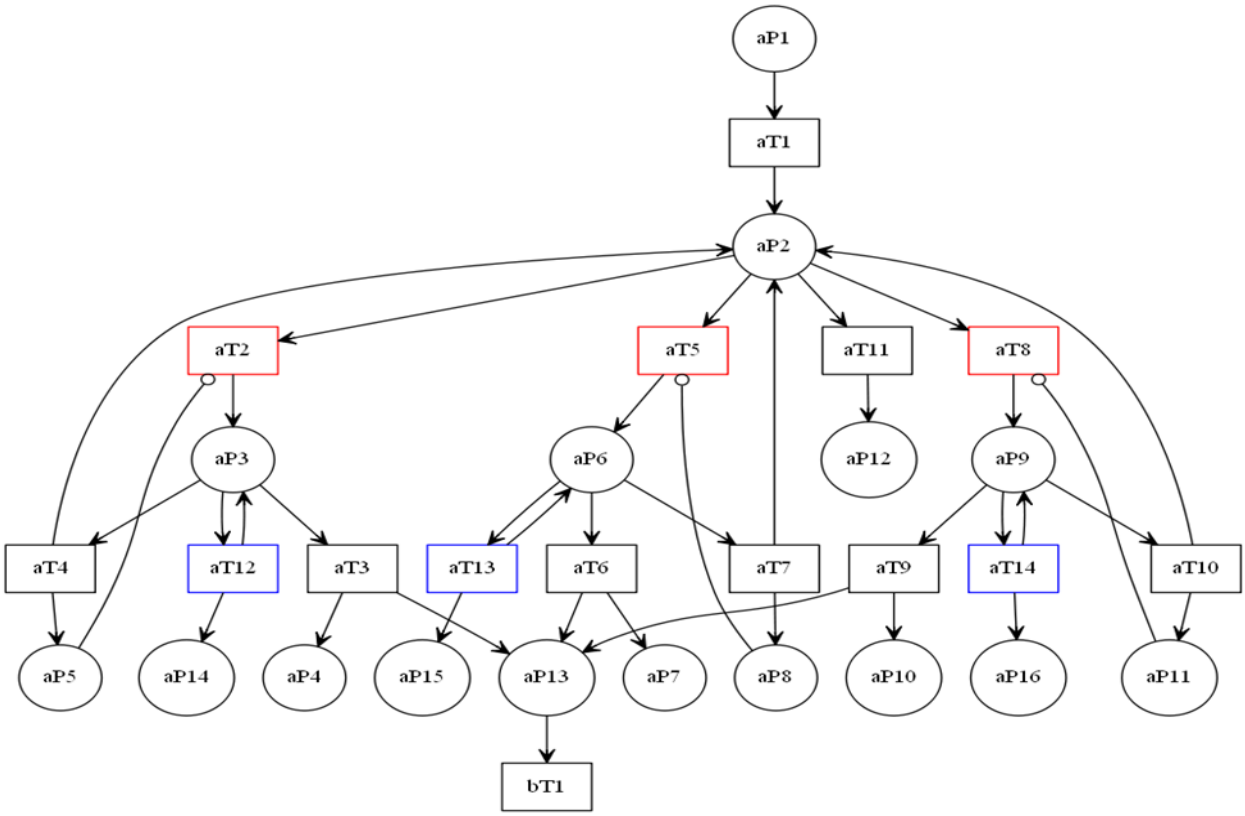
3. Research program projects

The overall PNPSC research program currently consists of five interrelated projects. The MITRE-maintained Common Attack Pattern Enumeration and Classification (CAPEC) is a database documenting known cyberattack patterns. Each CAPEC entry describes a specific type of cyberattack; for example, its entries include Cross-Site Scripting (CAPEC-63),

SQL Injection (CAPEC-66), and Spear Phishing (CAPEC-163). The CAPEC database entries are available in two forms: human-readable text, which is displayed online, and XML, which can be downloaded and processed. In the first project, CAPEC entries are converted automatically into executable PNPSC nets that model the attacks described in the entries. The XML version of a CAPEC entry is input to a Python script that produces an executable PNPSC net.

The PNPSC nets generated in the first project are considered component models, rather than complete models, because each models only a single type of cyberattack. Most computer systems to be modeled could be vulnerable to more than one type of attack, and so multiple component models must be combined to fully represent the system. Thus the cyberattack component models generated in the first project must be integrated or composed, to produce complete models of target computer systems. The second project is concerned with enabling those compositions. Doing so requires that the component models be defined so as to be composable, i.e., to included places and transitions that serve as "connectors" and allow the PNPSC nets to be connected. The connectors must be designed to preserve

the modeling semantics of the component models and pass needed stated information through the connections. Moreover, before the component models can be composed they must be selected, i.e., the correct models needed to model a target computer system must be selected from a repository of all component models.



In the third project, the model of the target computer system are verified and validated. Verification is the process of determining whether a model's implementation is consistent with its specification. In this work, PNPSC nets are verified by comparing them to their corresponding CAPEC entries. Methods to do so include analysis of the formal properties of the PNPSC nets and verifying the net's reachable markings against allowable attack states described using predicate calculus. Validation is determining the degree to which a model's behavior and output are consistent with the system or phenomenon being modeled. The PNPSC nets are validated against actual cyberattacks using methods that include manual execution of attack sequences represented in the PNPSC net and face validation using panels of cybersecurity subject matter experts.

In the fourth project, the validated model is executed to simulate cyberattacks. Multiple iterations of a simulated attack are executed to support a machine learning algorithm. The algorithm learns which actions to take, i.e., which transition rates to change for the different observable markings of the PNPSC net, so as to accomplish the goals of either the attacker or the defender. The machine learning algorithm is designed to be either an attacker or a defender, and its learning process is intended to be robust even if opposed by player that is also learning. The first phase of this project used simple reinforcement learning with an ε-greedy policy and a restriction on transition firing rates to reduce the state space. Work is now underway on more sophisticated machine learning algorithms, such as Deep-Q learning, that can operate with more full-featured and complex models, such as continuous state spaces.

The attack patterns in the CAPEC database are described primarily from the attacker's perspective. The actions taken by the attacker, and the possible effects and results of those actions, are the focus of the CAPEC entries. Consequently, the PNPSC nets generated from the CAPEC database are also attacker-centric. However, actions taken by an active defender before and during a cyberattack can certainly affect the attack's outcome. Moreover, system users, who are attempting to use the computer system for practical applications can also be affected by an ongoing attack or the defenses put in place to prevent one. In the fifth project, representations of defender actions and strategies and user actions and effects are being added to the PNPSC nets.

4. More information

For more information on this research program, please contact Ms. Katia P. Maxwell, Athens State University, katia.maxwell@athens.edu, or Dr. Mikel D. Petty, University of Alabama in Huntsville, at pettm@uah.edu

Today's Feature Blog Post-

Hacking Memoirs: The Big Casino!

By Joshua Crumbaugh

It was a lovely day in Las Vegas, Nevada. The sun shone brightly overhead, and the clouds made for a perfect backdrop. I couldn't have asked for better weather! Too bad this was work and not a vacation.

I had been hired by a casino to test their security for anything that could be improved. I arrived at the casino early to check in and scope things out. I stood there and watched cameras on the premises of the casino survey every inch of the place and capture everyone's face. I couldn't help but have this feeling of anxiety as I saw the countless armed guards. Security was heavily patrolling the casino and conveying codes through their walkie-talkies. It was clear that there were eyes everywhere, but would they notice a sophisticated attack, or would they be blind to anything more than card counting or armed robbery?

The Bellhop took my luggage and escorted me to my room, I couldn't help but notice the many layers of security as we made our way through the corridors. The walk to the room was a bit of a blur, but I remember the bell hop asking me question after question about my equipment. Honestly, all I could do is think that maybe I had bitten off more than I could chew. So far, they really seemed to have their act together…, but if former engagements had taught me anything it was never to judge a book by its cover. Before I knew it, we were at my room, the bellhop seemed a bit annoyed at the fact I had ignored his questions about my equipment. I wondered if he was going to report me to security. He dropped my bags by the front door and excused himself. It wasn't long before my phone began to vibrate, an email from management of the casino, dinner at 5pm sharp. I looked down at my watch to see the time, I had one hour before I needed to be at dinner.

I was in the process of hanging up some of my suits and giving myself a mental pep talk when I noticed a hidden panel at the top left of the closet. It was like it was just waiting on me!

I opened the panel to find a network router. When I plugged into the router, I immediately noticed that I wasn't on a guest network, but instead was on the casino's primary data network. The excitement began to set in, could it really be this simple? I had hacked numerous casinos over the years, but never this high profile of one and certainly not this heavily armed. How could this highly secure casino have made such a serious mistake? Had they not heard of network segmentation? With the newfound access I began working my magic; I would be able to infiltrate their computers from the comfort of my hotel room without having to leave or deal with armed guards. I felt like a true spy! I'd finally found the perfect loophole in their security.

A knock at my hotel door. I look down at my watch to notice it was 10 till 5. I placed the panel back in the closet and quickly shoved my equipment under the bed. Another knock, "Mr. Crumbaugh we are here to take you to dinner". I dusted off my suit and gave myself a quick glance in the mirror that hung by the entrance, took a deep breath, and opened the door. There were 2 men in matching polo shirts sporting the casinos logo. They were short and stern and asked that I come with them. We made our way through several dimmed hallways. I was surprised there didn't seem to be much security once I was in the employee only area. At one point the taller guy told me stop wondering and made a comment about how it would be cheating if I hacked anything while I was in the employee area with him. I must admit I was feeling a little frustrated at this point as I was the one hired to perform a job, instead I felt I was being treated like a hostile who might make him look bad. I hoped for his sake he wasn't in charge of network security.

I was finally seated in a board room, an older man entered the room, and went directly into business, with barely an introduction. He began bragging about their physical as well as cybersecurity and how they had never been breached. He was their head of security, and he was accompanied by another man who oversaw the casino's cybersecurity. He went onto say he that he had heard my keynote "How to rob a bank over the phone" and when he did his research on me he learned that I was of the world's leading social engineers and ethical hackers. He goes on to tell me that this is why he hired me. The way he told it his CFO had been pushing for a penetration test due to PCI compliance and he wanted to use it as an opportunity to prove that his security was impenetrable and could not be hacked by as be put it the "world's best smooth-talking hacker." I couldn't help but grin as I swallowed

an evil laugh, thinking about how this man had no idea that I was already in their network, and as soon as I was back to my room, it wouldn't be long before I had complete control of the casino.

Finally, dinner was over, the man walked over to me and said "you have one week Mr. Crumbaugh". He shook my hand and disappeared from the board room.

Back at my room, I immediately changed into pajamas and order some desert and beer from room service. Finally, I was ready to get pull an all-nighter and pwn this casino. It had become personal; my reputation was on the line! I grabbed my equipment out from underneath the bed and plugged into the router. In a matter of several hours, I had mapped out their entire network and compromised their exchange server. I was even able to run mimikatz and scrape over 70% of their user's passwords from memory in clear text. I love hacking Exchange servers because you often get huge payouts by scaping memory. Who needs to crack passwords when you can pull them plain text. There were 123 people with the password Password1! Impenetrable, more like swiss cheese. At this rate I wouldn't need a week, I could be ready to present by the next morning. There were administrative credentials in the Exchange dump and I knew it was only a matter of hours before I would have full control of their critical systems.

I was sitting there abusing my access and digging into their network when I discovered that they had vulnerable surveillance cameras all over the casino! It turned out to be too easy to hack them. Within just a few hours I had control of multiple critical systems and I was about to have their security cameras. I ran an exploit which cracked the password to the security camera and of course they reused the password so I now had access to every security camera on the casino network. I had eyes everywhere. This was turning out to be an epic engagement.

Now that my access was secure and I didn't have to worry about losing it, I decided it was time to abuse my access to their player management system. Knowing that casinos often comp their high rollers with suites, I upgraded myself to chairman status as a player recently recruited away from a competing casino. Yes, they really do have recruiters. I headed down to the front desk and used my social engineering skills. I explained that there must have been a mistake because I was expecting a suite. She saw that my initial room was comped (since I was working for the casino) and after a quick review of my status, she apologized for the mishap and asked the bellhop to escort me to my new room. A short walk and elevator ride later he swung open the double doors to my new suite and handed me a room key. This wasn't just any suite but a penthouse on a top floor with breathtaking views of the strip, a private balcony with hot tub, two bedrooms and a living room where they had everything from fresh fruit to champagne waiting for me. " Your luggage will be here shortly, if there's anything else you need, just let us know," he handed me a card with a private number and told me to call down when I was ready to play so they could take me to the private tables on the top floor. I began exploring my space more and took a moment to take in the view from the balcony it was truly breathtaking. A knock at the door just as I was beginning to relax. My luggage had arrived.

Now that I had proper quarters, a couple hours of sleep, and complete control of their network, it was time to see if I could physically break into secure areas.

I walked into the casino, looking like a respectably dressed businessman with an expensive suit and carrying a black leather laptop bag and folio. I knew that they'd be changing shifts any minute

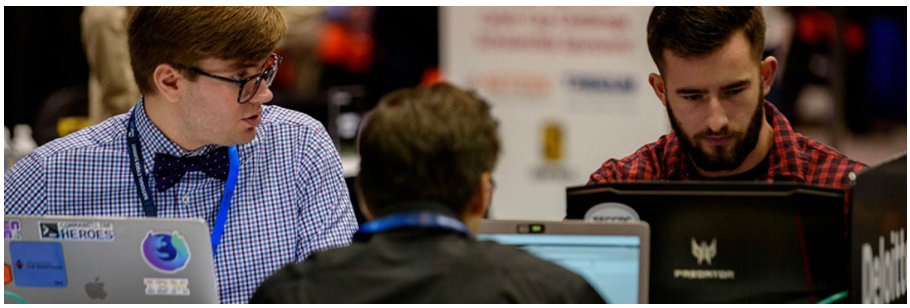
now, so I tailgated through security while there was a lot of traffic going in and out. When I approached the money cage, I see a lady flirting with the security guard, so I decide to see if I can clone her RFID badge. So, I introduce myself and tell them I'm an auditor from the state and that I'm turned around and looking for a bathroom. While I do this, I get my folio close to the lady's badge that was hanging from her waste and feel a slight vibration. That means it was successful. I head to the bathroom and program my badge with her access codes. When I get back, she's still talking with the security guard, so I jokingly say "fancy meeting you here" as I walk past them and swipe my new badge to unlock the door. The security guard looked my way but heard the beep unlocking the door and went back to his conversation.

I was shocked that they let me get so far. But you know, he was flirting and guard tends to forget that people in suits are a threat since they're used to common criminals who typically look the part. Now that I was in the money cage, I took some pictures as evidence to put in the report and made my way out. My work here was almost done, and I couldn't wait for their response.

Since I was already in a restricted area, I took this opportunity to look at their infrastructure from the inside. The only thing left to do was get access to the datacenter itself and physically plug in one of my devices. Luckily for me, they had a motion trigger unlock sensor on their server room door, and I was able to slide an envelope attached to a wire hanger under the door to get it to unlock. Once inside, I took a selfie for the report and then returned to my room.

So, aside from the casino putting an access panel in guest rooms, why was I able to get into the money cage and data center so easily? It's because of social engineering. Social engineering is the act of manipulating people into doing things that they would not normally do, but the definition should really include blinding people to things that are right in front of their eyes as well. The term "social engineer" was originally used to describe someone who manipulates other people out of their money. Since then it has evolved to include many other definitions. Today, social engineers are often hired by companies to test security systems and find their weaknesses before criminals or nation states do.

The main goal of social engineering is to use deceit and manipulation to fool someone into revealing sensitive information. There are many different types of social engineering attacks, but some common ones include phishing, vishing, and smishing.



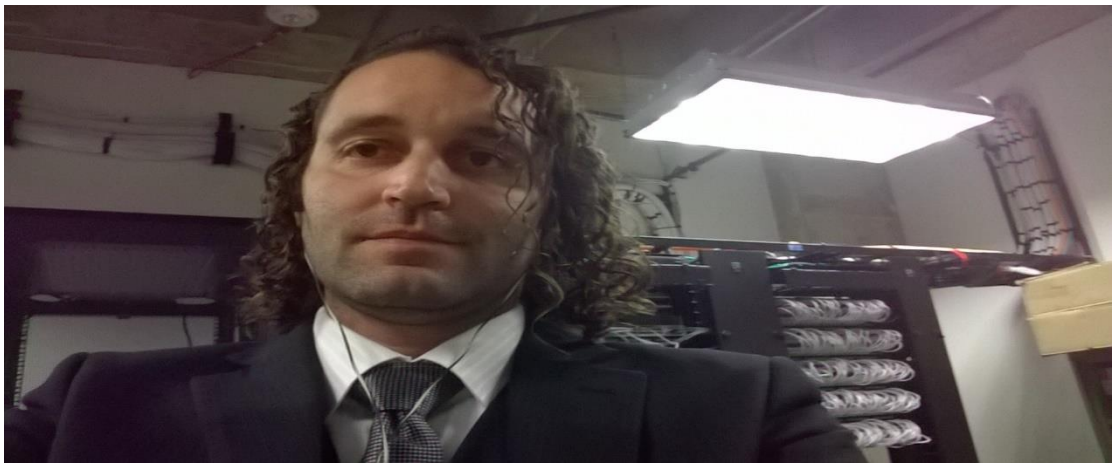


Figure 4 - The actual selfie!

Phishing involves sending users an email with a link or attachment that contains malware or other harmful content, which they may unknowingly open if they click on it. Vishing is similar to phishing because it uses a very similar attack; however, they receive phone calls instead of victims receiving emails.

It's never been more important than it is now to audit your defenses and determine how effective your security is. How would your company do if it were tested today?

Joshua Crumbaugh
Chief Technology Officer
PhishFirewall

About Joshua:
Joshua Crumbaugh is one of the world's most famous hackers. He's an engaging and internationally respected cybersecurity subject matter expert, published author, and keynote speaker. During Joshua's ethical hacking career, he has never encountered a single network that could keep him or his teams out. He uses these experiences to educate and entertain audiences with real life hacking stories that captivate the audience. His experience in all things social engineering led him to realize something had to change. This realization led him to found PhishFirewall.

About PhishFirewall
PhishFirewall is the world's first fully automated AI-driven anti-phishing solution. We personalize education, training, and phishing simulations to dramatically lower phishing risks. Our product has been designed to help organizations significantly reduce their level of exposure to ransomware attacks by using artificial intelligence insights that find and correct individual phishing vulnerabilities. Unlike other anti-phishing solutions on the market today, our product drives click rates well below 1% - even for those with a high propensity for clicking.

NCS
National Cyber Summit

Note from the Editor-

It is so great to have everyone back *'in person'* at our conference this year! In the interest of making our conference even more special for this return, we thought it might be of interest to our attendees to have a daily conference newsletter. So, we are piloting something a bit different this year and debuting a new conference publication titled, "*The"Daily Hacker: Pivot & Bytes*."

This publication brings together information about the hosts of the event: 1) National Cyber Security Summit Foundation, 2) Cyber Huntsville and 3) NAC-ISSA describing the organizations and how you can get involved, as well as a full listing of Conference Happenings, Feature Technical Articles and Blog Posts, as well as 'Fun Facts' about our community and state.

We hope you enjoy this new publication! Also, we are greatly interested in your feedback about this *new addition* to our conference offerings.

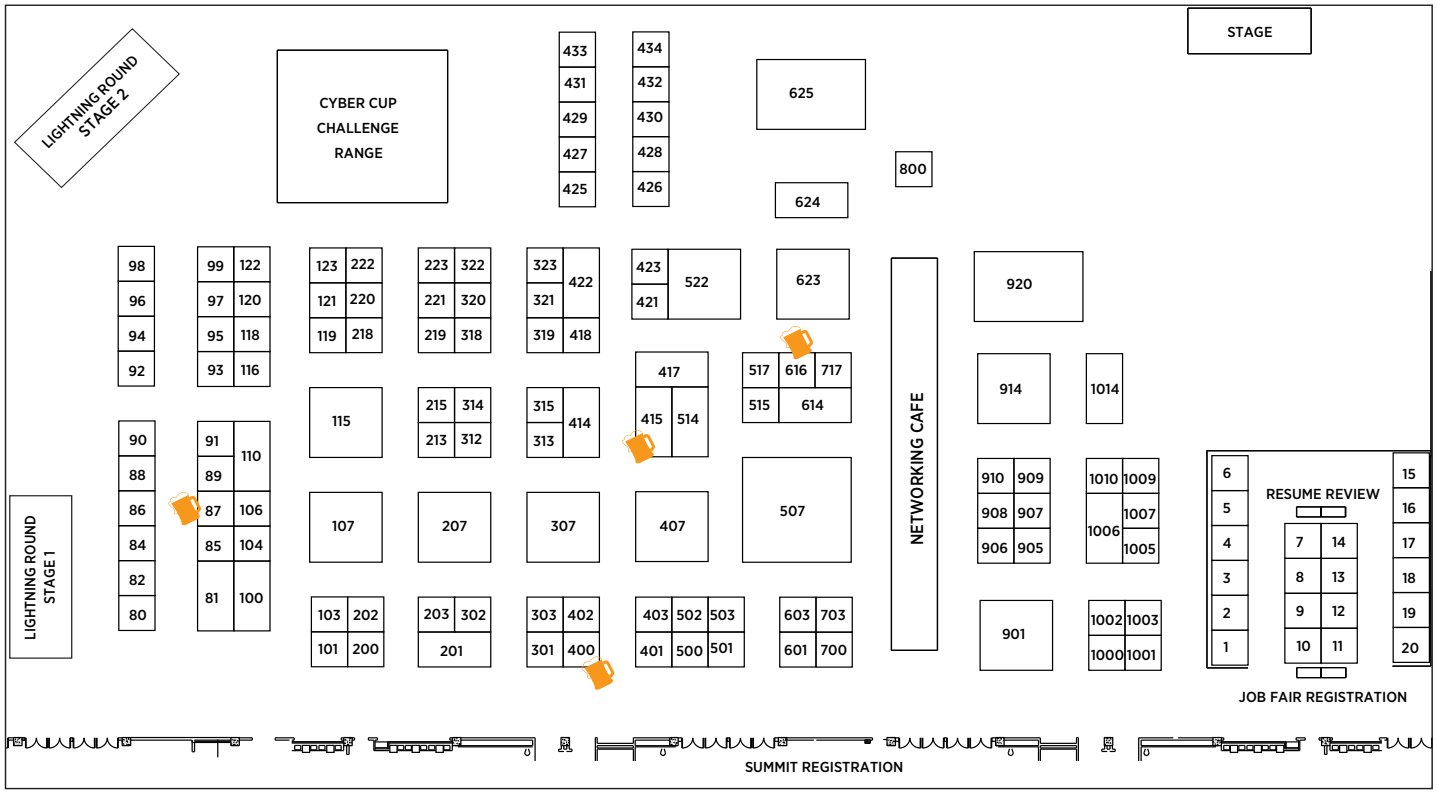
Best,

Dr. Kim LaFevor, DBA, SHRM-SCP, SPHR, IPMA-SCP, NDCCDP
National Cybersecurity Summit Foundation-Board of Directors
Senior Executive to the President for Strategy & Innovation-Athens State University

National Cybersecurity Conference Team

Pub Crawl Participating Booths

Tuesday 5:30 - 7:30 p.m.



Accenture 1014
Acropolis Security, LLC 123
Advanced Systems Development, Inc. 321
AFCEA Huntsville Chapter 429
Air Force CyberWorx 303
All Points LLC 415
ASmartPlace 625
Aspis 85
ASRC Federal 905
Athens State University 421
Attivo Networks 87
Auburn University Executive MBA Program 323
Auburn University Huntsville Research Center 430
Axellio 104
Bevilacqua Research Corporation 213
BigBear.ai 93
Bitglass Inc. 616
Black Data Processing Associates Huntsville Chapter 425
BluVector, A Comcast Company 86
Brockwell Technologies Inc. 700
Checkmarx Inc. 401
Cintel, Inc 515
COLSA Corporation & ISC(2) Huntsville Chapter 201
Columbia Southern University 501
CompTIA 313
Comxi World, LLC 219
CyberReach 427
Davidson Technologies Inc. 623
DC BLOX 703
Deltek 319
DESE Research Inc. 100
Dynatrace 94
Dynetics Inc. 307
ECS Federal 920
Elasticsearch, Inc. 80
Exabeam 1003
Expel 119
F1 Solutions Inc 414
Federal Bureau of Investigation (FBI) 507
Five Stones Research Corporation 1006
Flashpoint 1010
Gray Analytics 418
GSA 423
Guidehouse 1001
Harmonia Holdings Group, LLC 907
Hexagon | PAS, now part of Hexagon 1005
HORNE Cyber 318
IDS International 90
IHSE USA, LLC 302
Integration Innovation Inc. i3 417
Intuitive Research and Technology Corporation 514
JRC Integrated Systems 96
LBMC Information Security 314
LogiCore Corporation 1000
LSI 320
MAD Security 223
ManTech 106
MartinFederal 1002
Millennium Corporation 107
Missile Defense Agency 218
Mission Multiplier 503
Mississippi State University 101
Motorola Solutions, Inc. 91
NDCA- National Defense Cyber Alliance 431
Needling Worldwide, LLC 909
Netivity, Inc. 81
Netsecuris LLC 121
NICCS 98
nLogic 601
Noblis Inc. 221
Noetic Strategies Inc 402
Nokomis, Inc. 122
North Alabama Works 432
OASYS, INC. 103
Peerless Tech Solutions 517
PeopleTec Inc. 115
Pluralsight 99
Polarity 222
PreVeil and H2L Solutions Inc. 422
Quantum Research International 207
Radiance Technologies Inc. 522
Raytheon Technologies 403
Recorded Future 202
Red Hat 95
Riverstone Solutions 906
RockITek 901
Rugged Portable Computers 315
SANS Institute 116
Scalable Network Technologies Inc. 200
Scientific Research Corporation 110
SecureStrux 84
SecurIT360 97
Sentar 407
Sepio Systems 92
Serco 502
ShadowDragon 322
Simple Helix 312
Snowflake Inc. 500
Stealth 910
Steel Point Solutions 120
Sterling 82
Summit 7 Systems Inc. 603
System High Corporation 614
The CyBUr Guy Podcast 800
Training Concepts 301
Trideum Corporation 220
U.S. Army ROTC 717
U.S. Space & Rocket Center Education Foundation 428
UAH Center for Cybersecurity Research and Education 88
UAH College of Professional Studies, Professional Development 118
UAH Graduate Admissions 426
Ultra 914
University of Alabama Executive MBA 215
Varonis Systems Inc. 908
Verity Integrated Systems dba Security Solutions 89
WiCyS 434
Xyston, Inc. 400