CENTERS OF ACADEMIC EXCELLENCE IN CYBERSECURITY
CAE
COMMUNITY

CAP Center Program Review

Kevin Kornegay
Dr. Eugene DeLoatch Endowed Professor & CAP Center Director
Morgan State University
kevin.kornegay@morgan.edu
https://www.morgan.edu/cap

CAP
MORGAN™
CYBERSECURITY ASSURANCE AND POLICY CENTER

Outline

- Vision & Mission
- Center Structure
- Subject Matter Expertise
- Research
- Funding Overview
- Technology Transfer Activity
- Academic Programs
- Outreach & Workforce Development
- A Few Highlights
- What’s Next?

CAP Center Vision & Mission

- **Vision** - To be a national leader in hardware and software security through excellence in education and innovation.

- **Mission** - Provide the intelligence community with knowledge, methodology, solutions, and a highly skilled workforce to protect our nation’s cyber-physical infrastructure.

Our Journey

- NSF RISE Grant, 2014, $1M
- CREAM Lab founded in 2014 (2000 sq-ft)
- NSA Summer Research Program in 2016
- NSA/DHS CAE launched in 2016
- MECE Program launched in 2017
- Cybersecurity Assurance & Policy (CAP) Center launched in 2018 (Occupy 2 floors in McMechen Hall)

Our Journey (Cont.)

- NCAE-C in Cybersecurity Defense Redesignation in 2021
    - Cycle II: Plan of Study (PoS) Validation – ECE Dept. has successful ABET Accreditation Review in 2020 (Next review in 2026)

      “My reviewer comments regarding MSU’s Program of Study are provided as part of this report. I would especially like to recognize the excellent job MSU did in their straightforward documentation in completing this application.

      I want to commend Dr. Kevin Kornegay, MSU’s Point of Contact (POC), on the quality of this application. I feel confident that MSU’s application for CAE-CDE Program of Study Validation will be approved.” 03/03/2021
    - Cycle III: Designation approved for 5 more years until Fall 2027

CAP Center Faculty and Staff

- Dr. Kevin Kornegay, UC-Berkeley, ECE Dept., Hardware RE
- Dr. Ketchiozo Wandji, GWU, ECE Dept., Software RE
- Dr. Monireh Degabchian, GMU, CS Dept., Network Security
- Dr. Onyema Osuagwu, Illinois, ECE Dept., Artificial Intelligence
- Dr. Cliston Cole, Illinois, ECE Dept., Secure Communications
- **New faculty member in policy joining July 1, 2023**
- 8 Affiliate Faculty from from SoE, SoB, and SMCNS
- 3 Post-Doctoral Researchers
- 5 Visiting Research Scientists (NSA, JHUAPL)
- 2 Visiting Faculty (NSA, NIST)
- Business Manager, IT Manager, Director of Outreach & Engagement, Administrative Assistant

Subject Matter Expertise

- Secure Embedded Systems Design
- Hardware Reverse Engineering (e.g., SCA, FI)
- Software Reverse Engineering (e.g., Ghidra, QEMU)
- Hardware and Software Security
- Secure Autonomy/Trustworthy AI

Sponsors/Collaborations

- Cadence
- Center for Equitable Artificial Intelligence and Machine Learning Systems (**CEAMLS**)
- National Institute of Standards and Technology (**NIST**)
- National Security Agency
- National Science Foundation
- Sandia National Laboratory
- Applied Research Laboratory for Intelligence and Security (**ARLIS**)
- Johns Hopkins University Applied Physics Laboratory
- Leidos
- The MITRE Corporation
- Georgia Tech Research Institute (**GTRI**)
- Arizona State University, Brown, CalTech, Columbia, Dartmouth, GaTech, George Mason, JHU, Illinois, Michigan, MIT, Princeton, RPI, Stanford, Tufts, UMD, VaTech, Purdue, and USC

2020 Sponsored Research Funding

Sponsor	Jul - Sept	Oct - Dec	Jan - Mar	April - Jun	Total
	Q1	Q2	Q3	Q4	
Autodesk	$30,000.00		$50,000.00		$80,000.00
NSF	$264,559.00				$264,559.00
NSA	$150,000.00				$150,000.00
NSA	$161,602.00				$161,602.00
GTRI/NSA		$171,345.00			$171,345.00
GTRI/NSA		$475,000.00			$475,000.00
GTRI/NSA				$123,000.00	$123,000.00
ARLIS #1	$100,000.00				$100,000.00
ARLIS #2			$150,000.00		$150,000.00
TAMU/NSA					$0.00
NSF					$0.00
Keysight			$20,000.00		$20,000.00
Nist	$96,000.00				$96,000.00
mitre		$39,400.00			$39,400.00
Its					$0.00
Arliss #3			$112,500.00		$112,500.00
Arlis #5			$100,000.00		$100,000.00
NSA			$100,000.00		$100,000.00
	$802,161.00	$685,745.00	$532,500.00	$123,000.00	$2,143,406.00

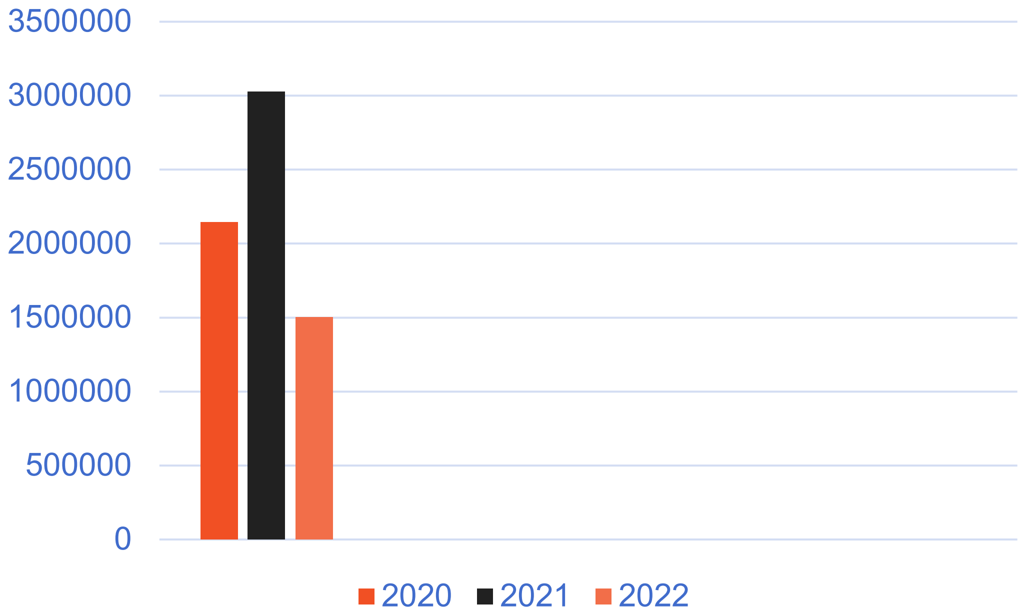
2021 Sponsored Research Funding

Sponsor	Jul - Sept	Oct - Dec	Jan - Mar	April - Jun	Total
Autodesk	Q1	Q2	Q3	Q4	
NSF			$43,000.00		$43,000.00
	$264,559.00				$264,559.00
NSF	$2,200,200.00				$2,200,200.00
GTRI/NSA					$0.00
GTRI/NSA		$147,000.00			$147,000.00
GTRI/NSA				$123,000.00	$123,000.00
					$0.00
ARLIS					$0.00
ARLIS			$20,000.00		$20,000.00
Keysight				$50,000.00	$50,000.00
Cadence				$50,000.00	$50,000.00
Shift 5	$96,000.00				$96,000.00
Nist		$33,600.00			$33,600.00
mitre					$0.00
					$0.00
Its					$0.00
Arliss #3					$0.00
Arlis #5					
NSA	$2,560,759.00	$180,600.00	$63,000.00	$223,000.00	$3,027,359.00

2022 Sponsored Research Funding

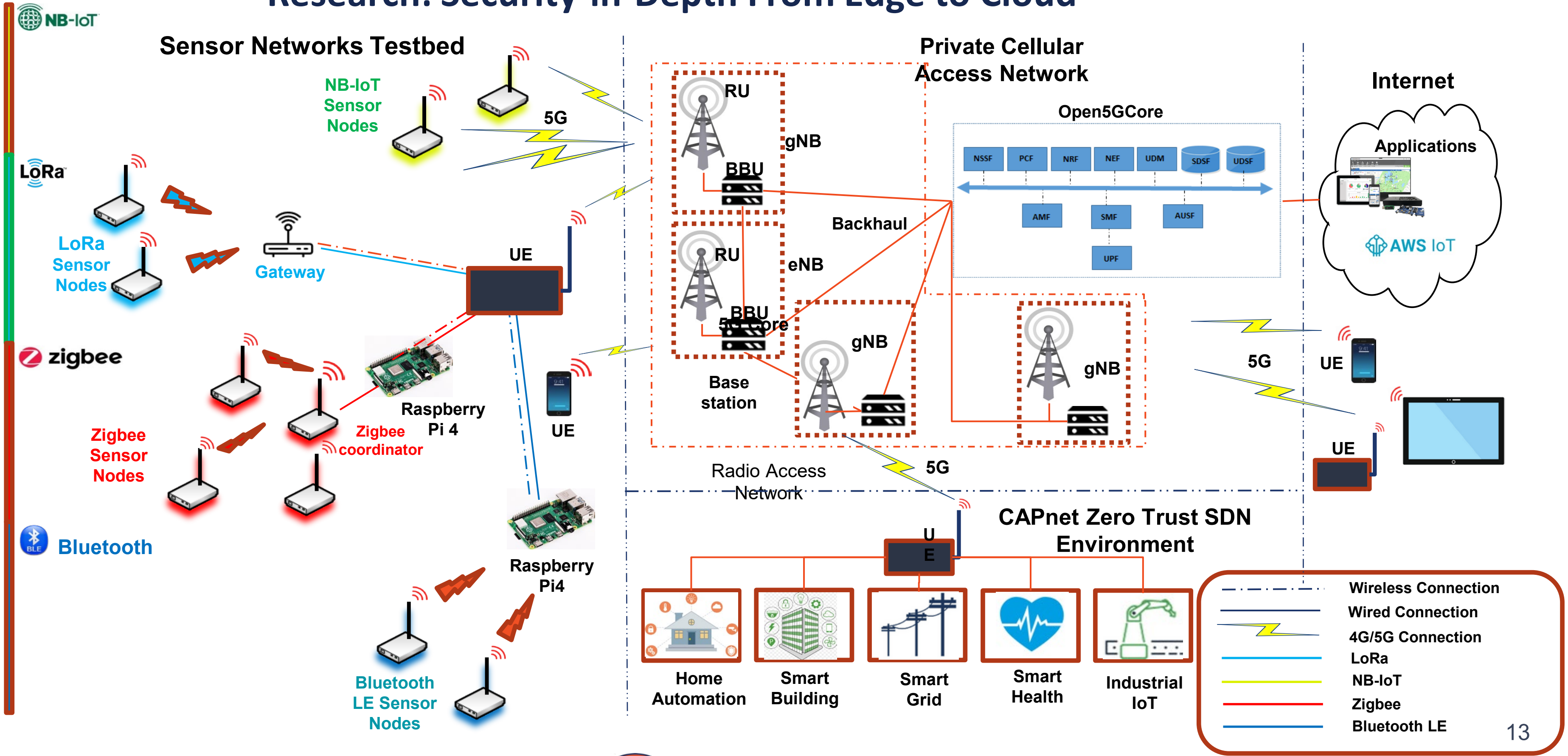
Sponsor	Jul - Sept	Jul - Sept	Jul - Sept	April - Jun	Total
	Q1	Q2	Q3	Q4	
NSF	$264,559.00				$264,559.00
NSF	$271,000.00				
NSA	$68,000.00				$68,000.00
BAH	$183,000.00				$183,000.00
Leidos	$60,000.00				$60,000.00
ARLIS	$25,000.00				$25,000.00
ARLIS	$15,000.00				$15,000.00
ARLIS	$15,000.00				$15,000.00
MIPS	$100,000.00				$100,000.00
Nist	$70,000.00				$70,000.00
NSA	$100,000.00				$100,000.00
Autodesk	$43,000.00				$43,000.00
Mitre	$36,000.00				$36,000.00
NGC	$75,000.00				$75,000.00
APL	$175,000.00				$175,000.00
	$1,500,559.00	$0.00	$0.00	$0.00	$1,500,559.00

Funding Trajectory



*** A 41% increase from 2020 to 2021**

Research: Security-in-Depth From Edge to Cloud



NIST Lightweight Cryptographic (LWC) Competition

- The National Institute of Standard and Technology (NIST) initiated its study of NIST-approved standard cryptographic primitives on constrained devices.
- The first workshop associated with this study was held in 2015, and a second in 2016
- The finding of the study conducted was publish in NISTIR 8114 report in 2017
- In 2017 a drafted white paper *Profiles for the Lightweight Cryptography (LWC) Standardization Process* was proposed to the community to elicit feedback
- In 2019 a call for participation in the LWC Competition
- Currently there are 10 Finalists

IoT Device Vulnerabilities

An unintended channel for monitoring or operating a device resulting from its physical interface.

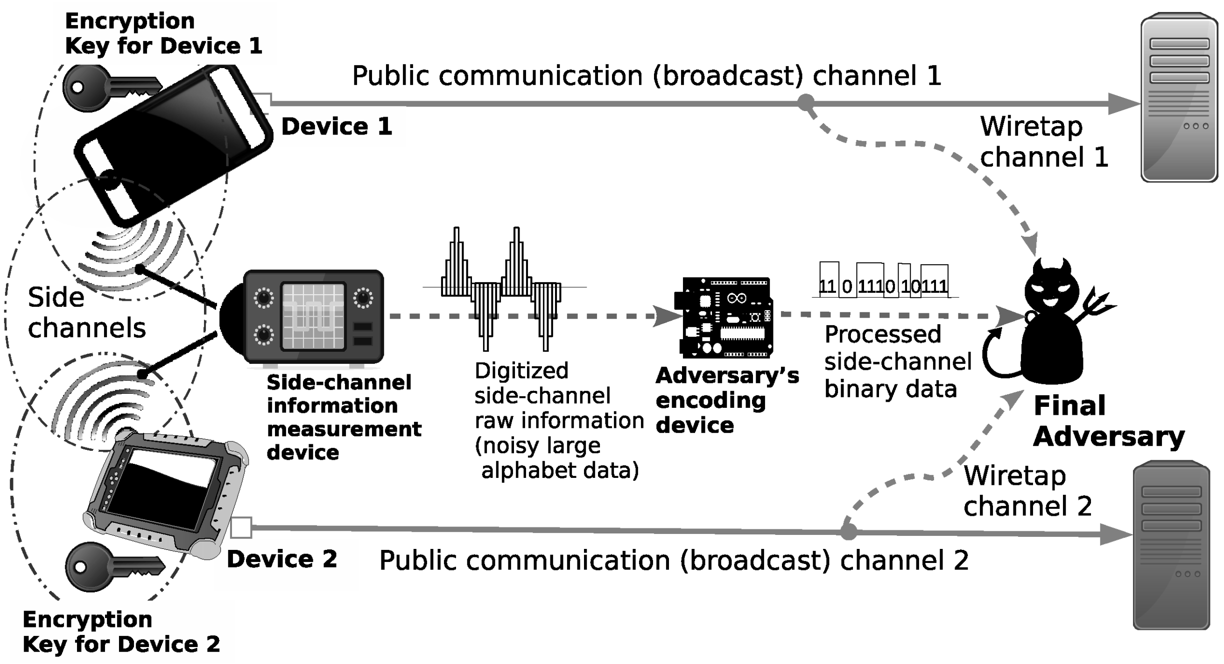
Intended

- Keyboard
- Screen
- Card Reader
- Audio
- USB
- Bluetooth/WiFi
- Power

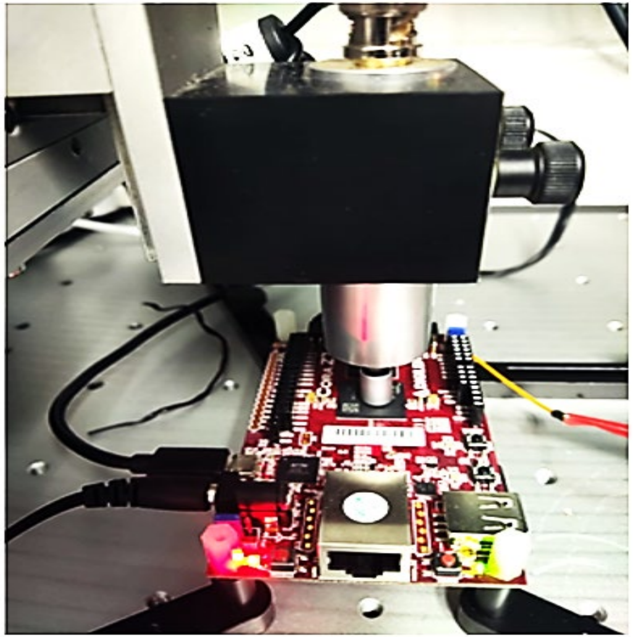
Unintended

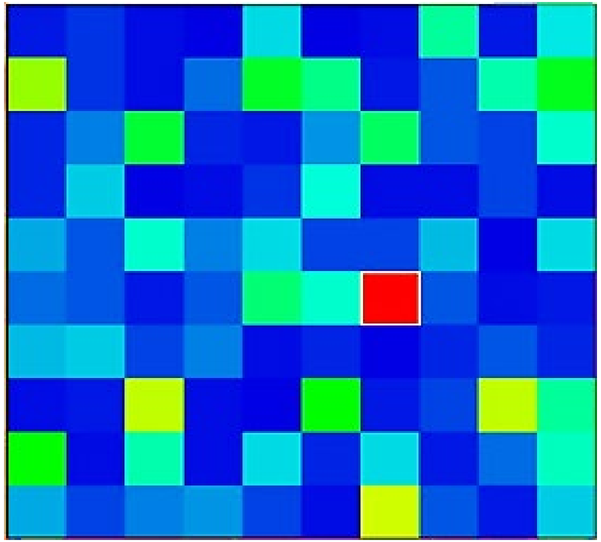
- Power Consumption
- EM Radiation
- Sound
- Temperature
- Time
- Light

Side Channel Attack


Encryption Key for Device 1
Public communication (broadcast) channel 1
Device 1
Wiretap channel 1
Side channels
Side-channel information measurement device
Digitized side-channel raw information (noisy large alphabet data)
Adversary's encoding device
11 0 1110 10111
Processed side-channel binary data
Final Adversary
Wiretap channel 2
Device 2
Public communication (broadcast) channel 2
Encryption Key for Device 2

Experimental Setup and Heat Map





Technology Transfer

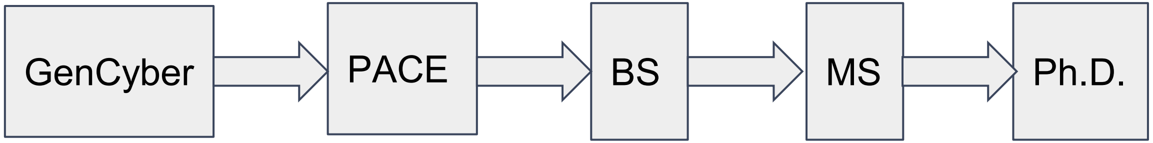
- OTT Innovation of the Year Award, 2/22/2022, Hailu Belay and Kevin Kornegay, “*Smart Antenna System*”
- OTT Innovation of the Year Award, 11/9/2022, Tsion Yimer and Kevin Kornegay, “*Detection and Survival Method against Adversarial Attacks on Automated Systems.*”

1. K.T. Kornegay et al., “*Decentralized Root-of-Trust Framework for Heterogeneous Networks*,” U.S. patent no. 10,831,894, issued November 10, 2020.
2. H. Kassa, K.T. Kornegay, “*Adaptive Energy-efficient Cellular Networks*,” U.S. patent no. 11,240,752, issued February 1, 2022.

Technology Transfer

- Maryland Industrial Partnerships (**MIPS**) - brings the inventive minds and extensive laboratory resources of the University System of Maryland to bear on creating the new products that feed the growth of Maryland businesses
    - ***Linthicum-based*** Clarity Cyber LLC ***and*** **Professor Kevin Kornegay*****, Electrical and Computer Engineering Department, Morgan State University:*** prototyping and evaluating VISPR, the company's secure processor for Internet of Things (IoT) devices, which addresses secure code execution issues, mitigating potential ransomware and other attacks. MIPS/company contributions: $90K/$10K.

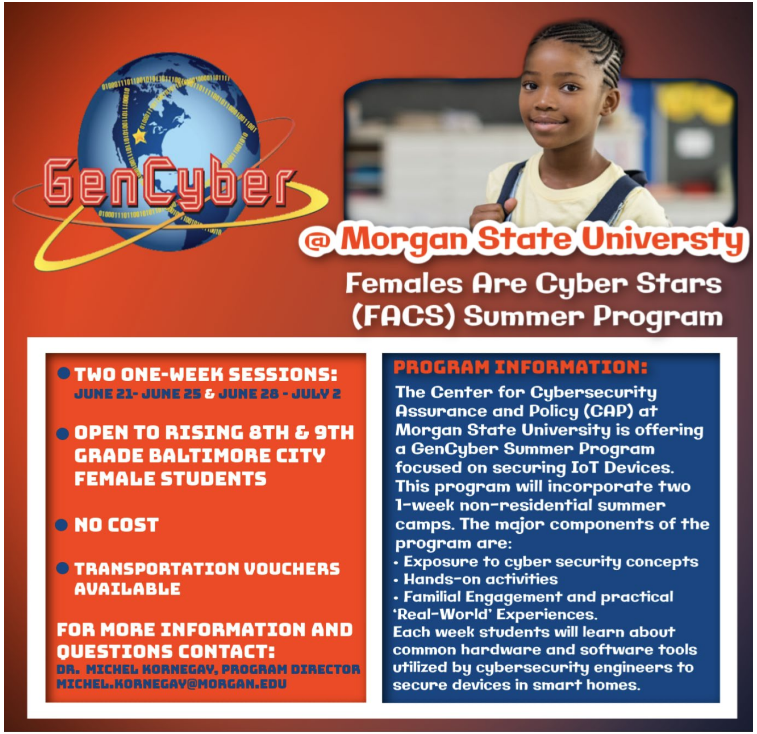
Outreach & Workforce Development



GenCyber → PACE → BS → MS → Ph.D.

1. National Science Foundation Scholarship for Service, Research Experience for Undergraduates, Secure & Trustworthy Cyberspace Frontier Center, NIST PREP, etc.
2. Academic, industry, and government partnerships that provide internships, summer research experiences, and professional mentoring
3. Peer mentoring and recruiting
4. Semester and capstone projects that offer industry mentors, internships, skills development, job opportunities

GenCyber



GenCyber

@ Morgan State Universty

Females Are Cyber Stars (FACS) Summer Program

- TWO ONE-WEEK SESSIONS: JUNE 21- JUNE 25 & JUNE 28 - JULY 2
- OPEN TO RISING 8TH & 9TH GRADE BALTIMORE CITY FEMALE STUDENTS
- NO COST
- TRANSPORTATION VOUCHERS AVAILABLE

FOR MORE INFORMATION AND QUESTIONS CONTACT:
DR. MICHEL KORNEGAY, PROGRAM DIRECTOR
MICHEL.KORNEGAY@MORGAN.EDU

PROGRAM INFORMATION:

The Center for Cybersecurity Assurance and Policy (CAP) at Morgan State University is offering a GenCyber Summer Program focused on securing IoT Devices. This program will incorporate two 1-week non-residential summer camps. The major components of the program are:

- Exposure to cyber security concepts
- Hands-on activities
- Familial Engagement and practical 'Real-World' Experiences.

Each week students will learn about common hardware and software tools utilized by cybersecurity engineers to secure devices in smart homes.

Pre-Freshmen Accelerated Curriculum in Engineering (PACE) Program

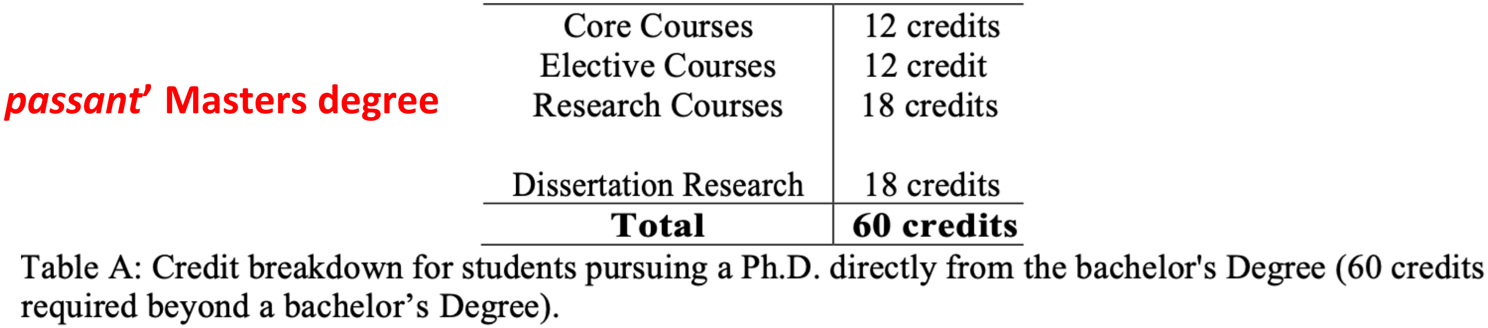
- A 5-week comprehensive and intensive summer program
- Prepare students for Morgan State University’s Placement Test
- Provide students with accelerated learning of pre-calculus to become calculus ready
- Provide the students the opportunity to conduct and analyze experiments
- Improve students’ communication skills, both written and oral
- Develop appropriate study skills, strategies, and habits for success in an engineering major
- Develop students’ critical thinking skills (e.g., analysis, synthesis, and evaluation)
- Develop students' ability to draw reasonable inferences from observation
- Develop students' ability to work in a team environment
- The top 10 students are chosen and paired with an undergraduate mentor (typically a High School Alum) to work in the CREAM Lab and given a $5K scholarship

Cyber Academic Programs

- BS in Electrical and Computer Engineering with a cybersecurity concentration (NSA Center of Academic Excellence in Cyber Defense).
- Ph.D./MS Program in Secure Embedded Systems (NSA Center of Academic in Research)

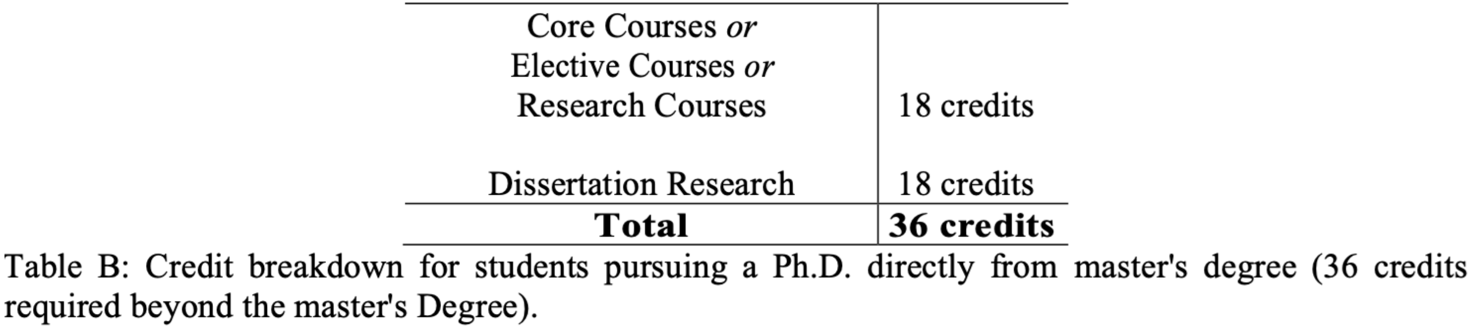
Ph.D. in Secure Embedded Systems

With ‘*en passant*’ Masters degree



Core Courses	12 credits
Elective Courses	12 credit
Research Courses	18 credits
Dissertation Research	18 credits
Total	**60 credits**

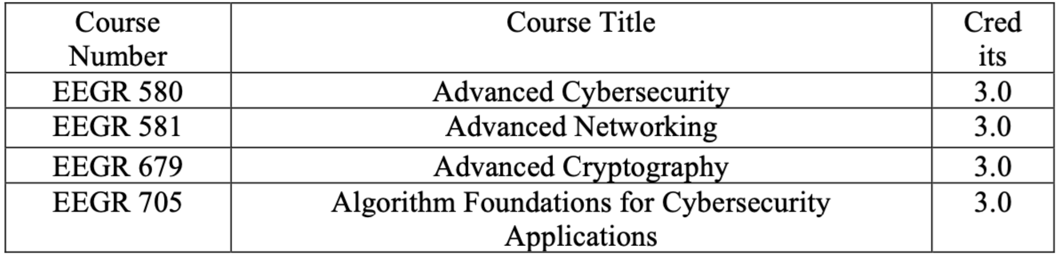
Table A: Credit breakdown for students pursuing a Ph.D. directly from the bachelor's Degree (60 credits required beyond a bachelor’s Degree).



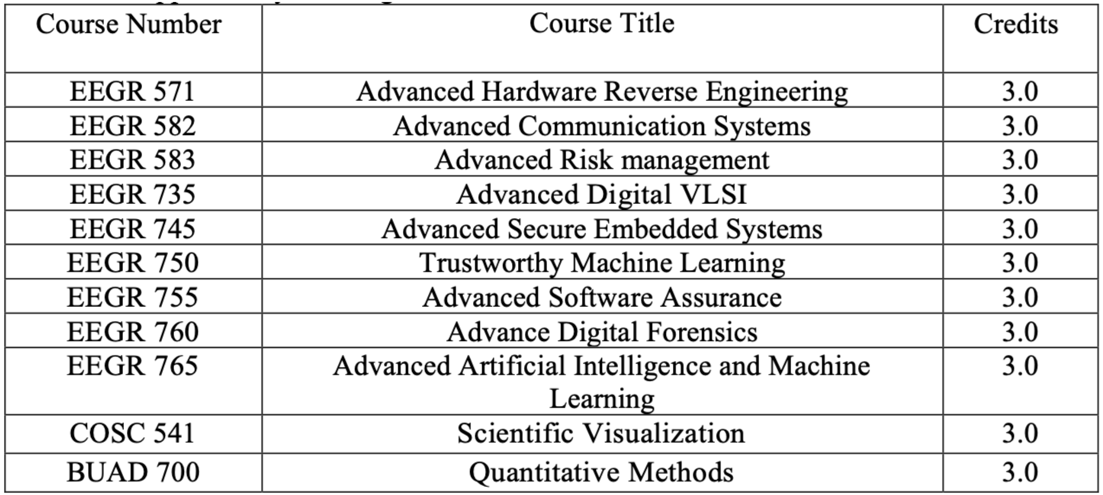
Core Courses *or* Elective Courses *or* Research Courses	18 credits
Dissertation Research	18 credits
Total	**36 credits**

Table B: Credit breakdown for students pursuing a Ph.D. directly from master's degree (36 credits required beyond the master's Degree).

Ph.D. in Secure Embedded Systems



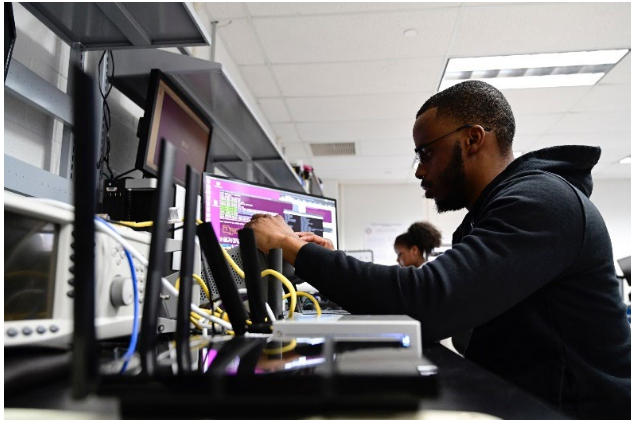
Course Number	Course Title	Credits
EEGR 580	Advanced Cybersecurity	3.0
EEGR 581	Advanced Networking	3.0
EEGR 679	Advanced Cryptography	3.0
EEGR 705	Algorithm Foundations for Cybersecurity Applications	3.0



Course Number	Course Title	Credits
EEGR 571	Advanced Hardware Reverse Engineering	3.0
EEGR 582	Advanced Communication Systems	3.0
EEGR 583	Advanced Risk management	3.0
EEGR 735	Advanced Digital VLSI	3.0
EEGR 745	Advanced Secure Embedded Systems	3.0
EEGR 750	Trustworthy Machine Learning	3.0
EEGR 755	Advanced Software Assurance	3.0
EEGR 760	Advance Digital Forensics	3.0
EEGR 765	Advanced Artificial Intelligence and Machine Learning	3.0
COSC 541	Scientific Visualization	3.0
BUAD 700	Quantitative Methods	3.0

Table H: Elective Courses

CAP Scholar Skill Profile



Cryptography

- Asymmetric Encryption
- Symmetric Encryption
- Message Authentication Codes

Communications

- Wireless/wired networks
- Protocols and standards

Policy

- Privacy

Software

- Operating Systems
- Virtual Machines
- Programming Languages
- AI/Machine Learning
- Reverse Engineering

Hardware Assurance

- System-on-Chip (SoC)
- Trusted Platform Modules
- Software Defined Radio
- Software Defined Networks
- Reverse Engineering

Workforce Impact

- **23 Ph.D. Students**
- **30% Women**
  - **83% US Citizens**
  - ***4 Ph.D. students graduated on 05/19/2022 from Ph.D. in Secure Embedded Systems program (Joining NSA, JHUAPL, NIST, CAP)***
- Prestigious National Graduate Fellowships
  - 3 DoD Cybersecurity Scholarship Recipients (2 Ph.D., 1 MS)
  - 4 NSF CyberCorps Ph.D. Scholars (3 Ph.D., 1 BS)
  - 5 GEM Doctoral Fellowships (3 Full, 2 Associate)
  - 1 MITRE Scholar
  - 3 NIST PREP Scholars (1 PostDoc)
- 21 MS Students
- 40+ Undergraduate Student Researchers

Highlights

- Dr. Kornegay was appointed by the Secretary of Commerce to serve on the **NIST IoT Advisory Board**
- Sixteen Technical journal/conference publications (including the best presentation award at the 2022 IEEE Artificial Intelligence & Pattern Recognition Workshop)
- One patent and filed three Intellectual Property Disclosures (IPD)
- New collaborations: Brown University (Home Healthcare **NSF** ERC), Columbia University (SRC/DARPA JUMP Center), George Mason (NSF NSF-DoD 5G Convergence Accelerator), Purdue University (NSF Expeditions Center)
- Seven Secure Embedded Systems Ph.D. students gave lightning talks at the NSA Cybersecurity Collaboration Center to Directors of the Cybersecurity and Research Directorates and associated hiring managers in early May 2022 – all seven students received conditional job offers (CJO)
- Five Secure Embedded Systems Ph.D. students gave lightning talks at Sandia National Labs and received job offers
- Invited Talks: **NSF** SaTC PI Meeting, the 2022 **DHS/NSA** CAE in Cybersecurity Symposium, University-Industry Demonstration Partnership Webinar, MITRE eCTF Awards Ceremony Speaker, Stanford-UCSF Distinguished Speaker Series in Biomedical Engineering, George Washington University, and UMass-Amherst
- Dr. Kornegay published a book chapter entitled ”Perception of Cyber Threat in Autonomous Intelligent Cyber-Defense Agents” with Dr. Alexander Kott (Editor, Chief Scientist, Army Research Lab). Co-Authors: Dr. Kofi Nyarko (Morgan), Dr. Ahmad Ridley (NSA)

What’s Next?

- Continue to grow our stature in the intelligence community via new partnerships
- Continue to develop new collaborations with other state-funded centers, universities, and industry
- Become a **DHS/NSA** Center for Academic Excellence in Research (CAE-R)
- Increase undergraduate/graduate recruitment
- Hire replacement for faculty vacancy
- Spring 2023 CAP Advisory Council meeting
- Commence CAP Distinguished Lecture Series in Spring 2023
- Launch CAP Newsletter in Spring 2023
- Become a national center in cybersecurity (e.g., National Science Foundation Engineering Research Center and Navy Multidisciplinary University Research Initiatives (MURI) programs)