THE UNIVERSITY OF MEMPHIS
Center for Information Assurance

FedEx INSTITUTE OF TECHNOLOGY
THE UNIVERSITY OF MEMPHIS

Research-Driven Cybersecurity Education & Training

Prof. Dipankar Dasgupta, IEEE Fellow

Director: Center for Information Assurance

A NATIONAL CENTER OF ACADEMIC EXCELLENCE (CAE-CD / CAE-R)

Center website: cfia.memphis.edu

Cyber Citizen: Responsibilities

Vender responsibility | **ITD responsibility** | **User responsibility**

Sw/Hw/OS/App | System Security Configuration | User Behavior

Search Design Flaws/Bugs | **Exploit Security Holes** | **User Behavior/ Insider Threats**

Secure Design/Release Patch | Security updates/ Holistic Protection | STOP-THINK-CONNECT

SELLING CYBER VULNERABILITIES

backdoor

memory leak

Faulty hardware/ software

New Business

Vulnerability Finders & Seller

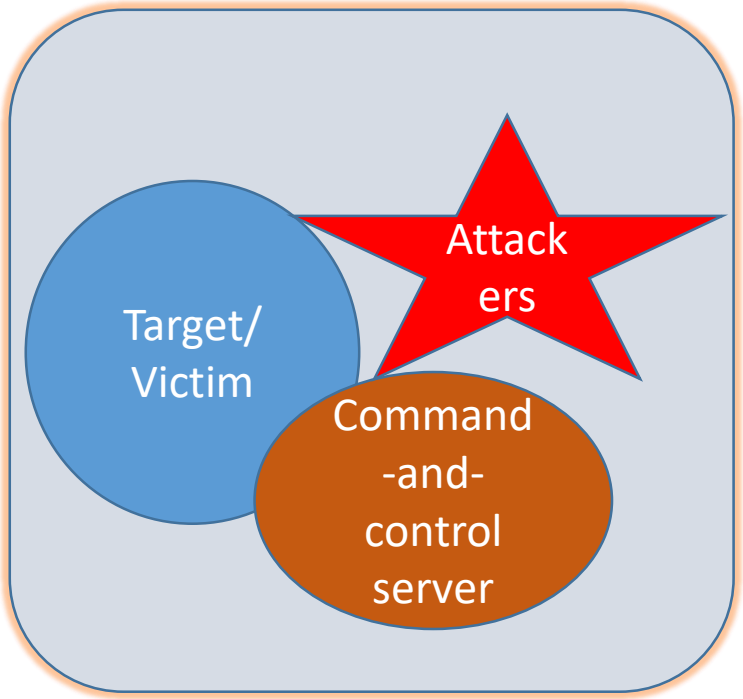
criminal hackers

security firm

nation states

ethical/white hat

MORDERN DAY MALWARE & CYBER THREATS



Attackers have different motivation and goals while targeting different sectors:

- Destroy/damage/Disruption
- Takeover control
- Spying/cybersurveillance
- Data breach--Exfiltrate sensitive/private data
- Seek Ransom

Need Research-based knowledge update for Cybersecurity Education and Training to deal with emerging Threats!

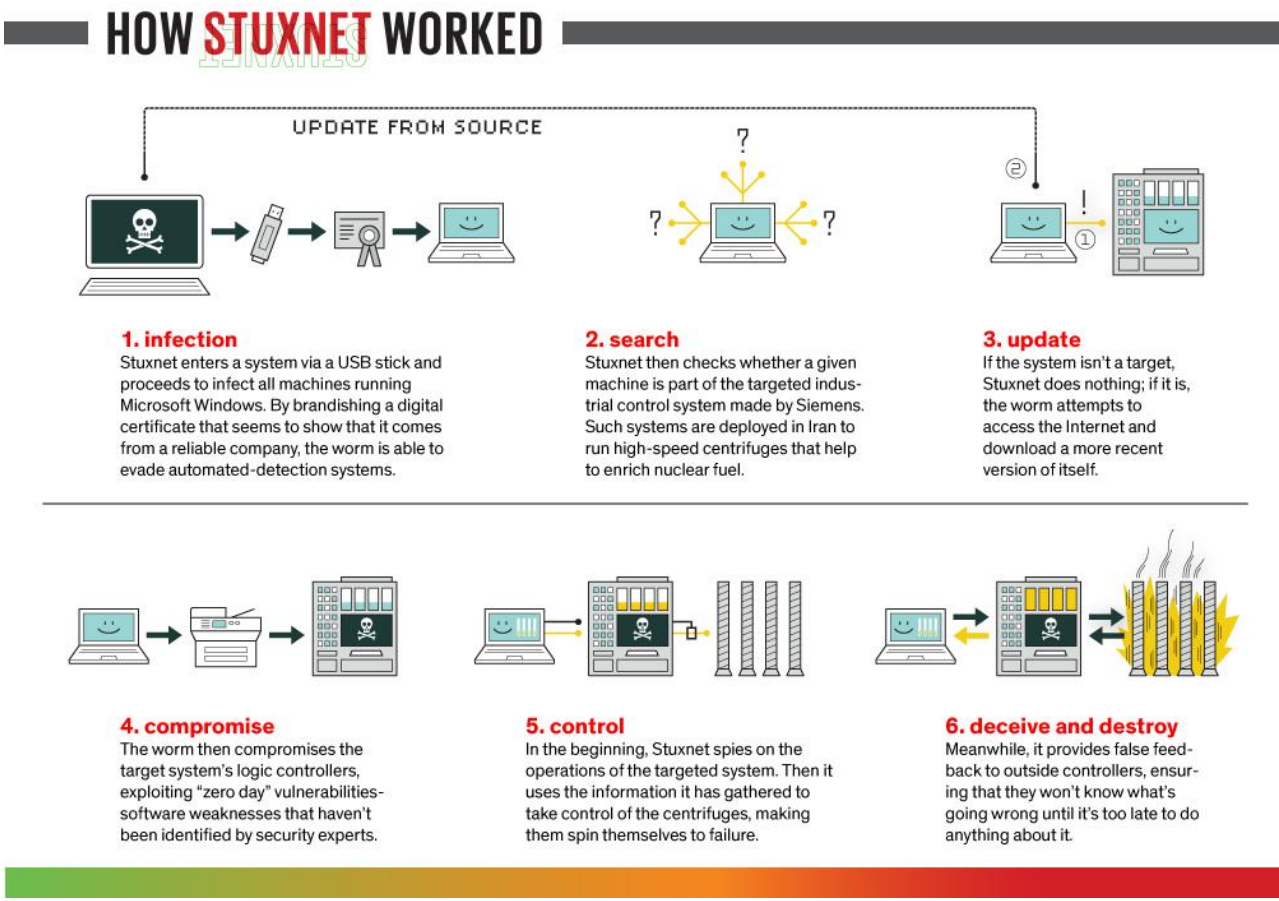
The Real Story of Stuxnet (2010)

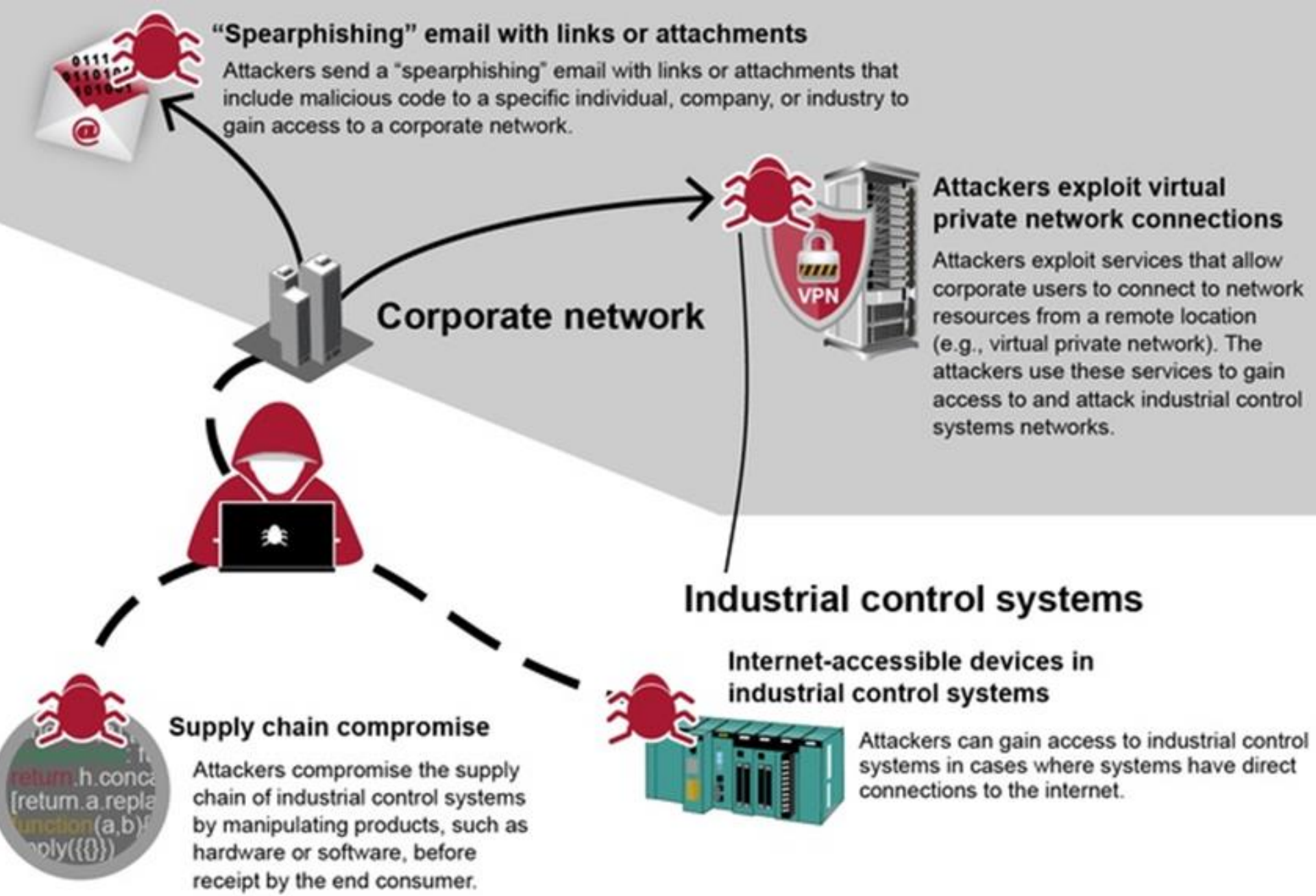
By David Kushner, IEEE Spectrum

Beginning of Modern day Malware and attacks

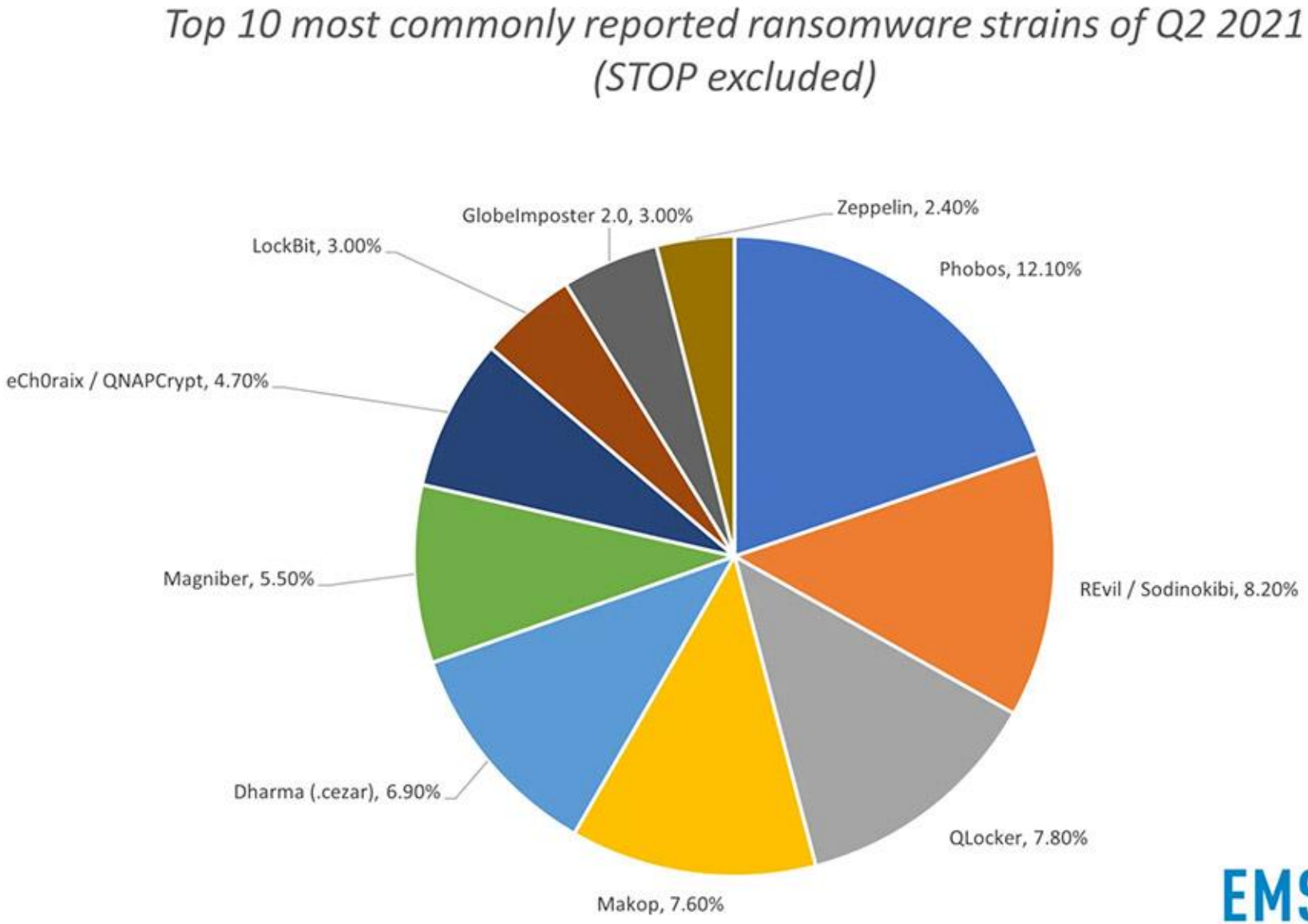
Four zero-day exploits.

- MS windows vul^{n} exploits spread via USB drive, then spread onto the network.
- shared print-spooler vulnerability is used to spread in networks with shared printers
- other two vulnerabilities have to do with privilege escalation, designed to gain system-level privileges
- subvert Siemens systems running centrifuges in nuclear plants



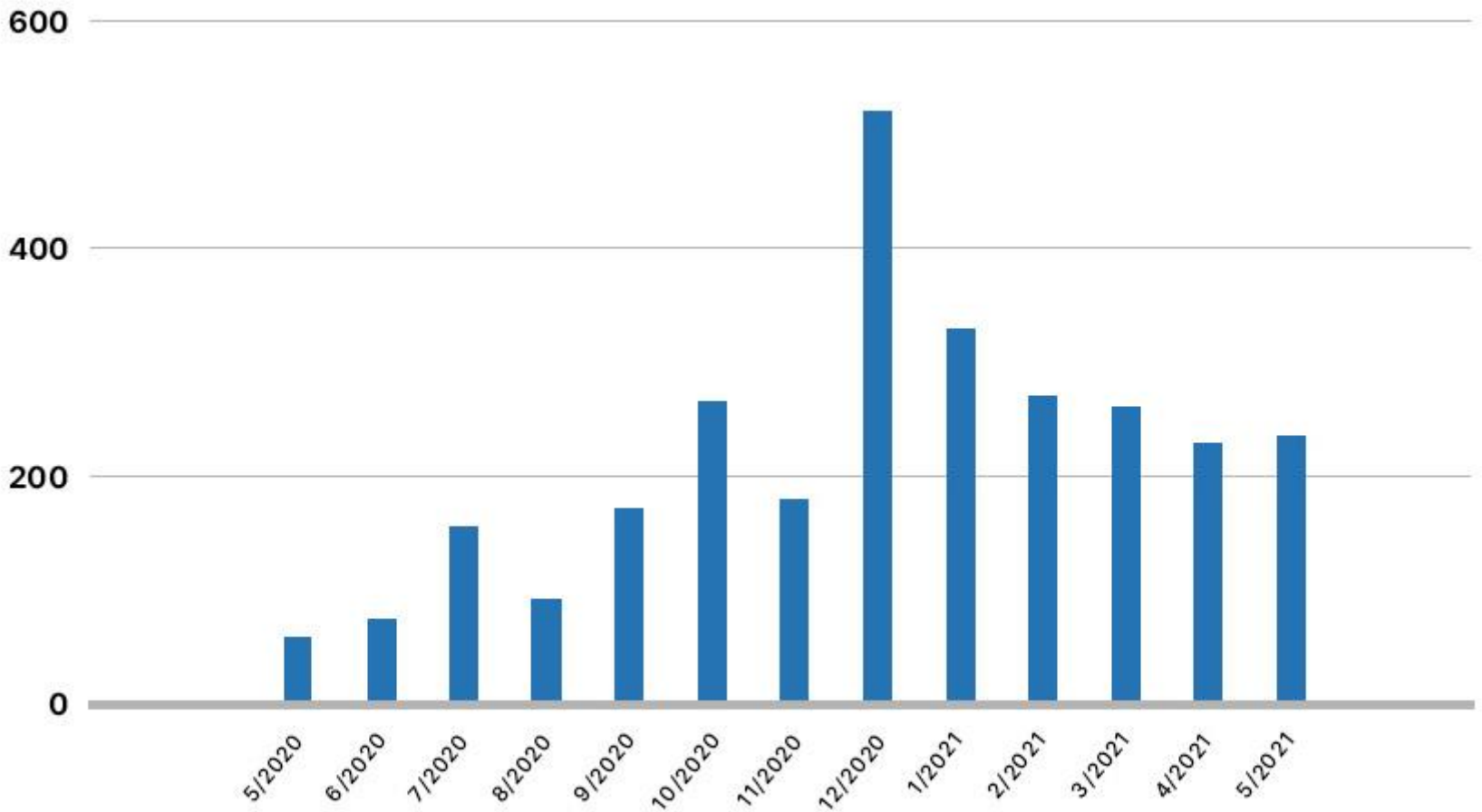


Source: GAO analysis of industry and federal documents. | GAO-21-81



Ransomware-as-a-service operations such as Revil (accounts for 10% of global incidents)

Count of known ransomware victims by month (Source: Recorded Future)



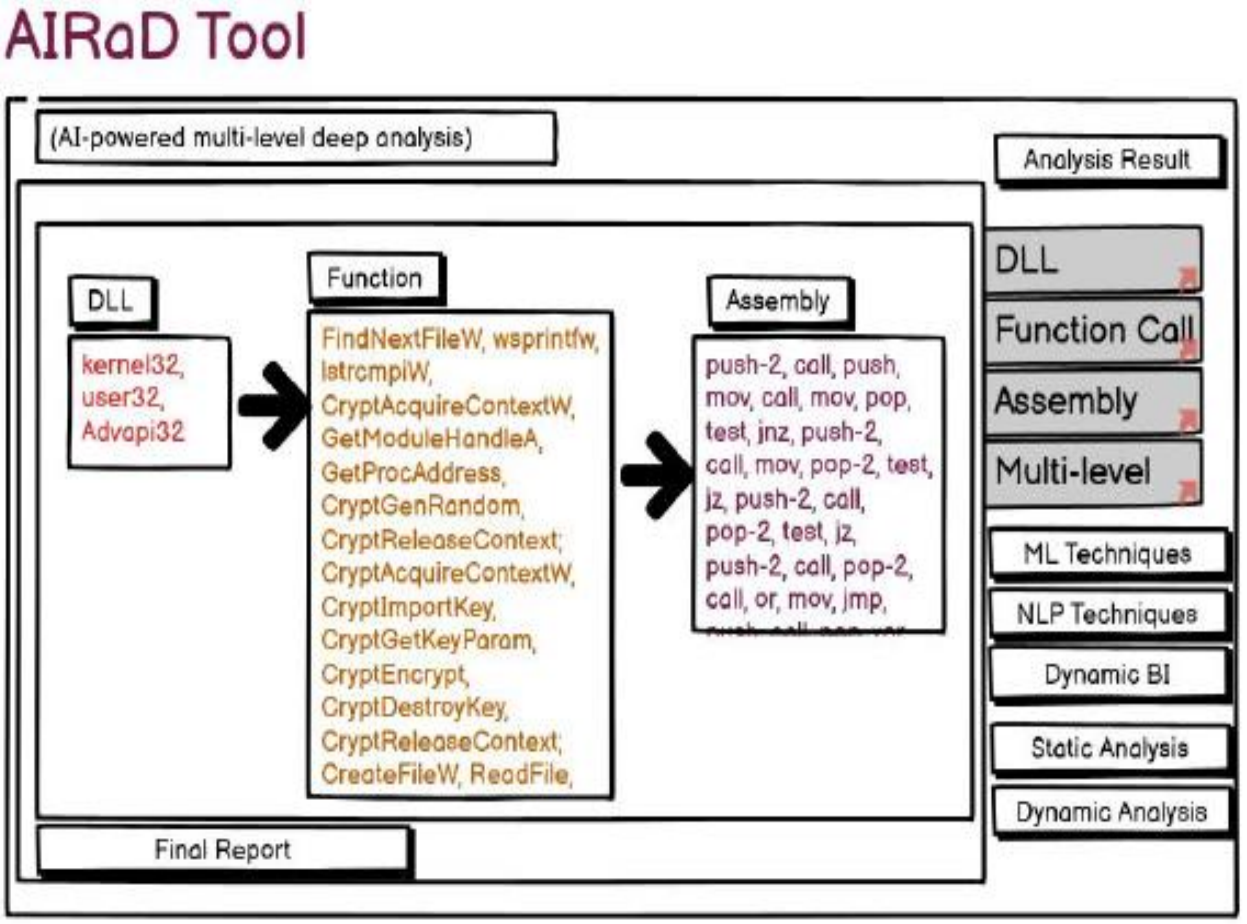
State Department, DHS Focus on Ransomware Threats to Critical Infrastructure

Scott Ferguson (Ferguson_Writes) • July 15, 2021

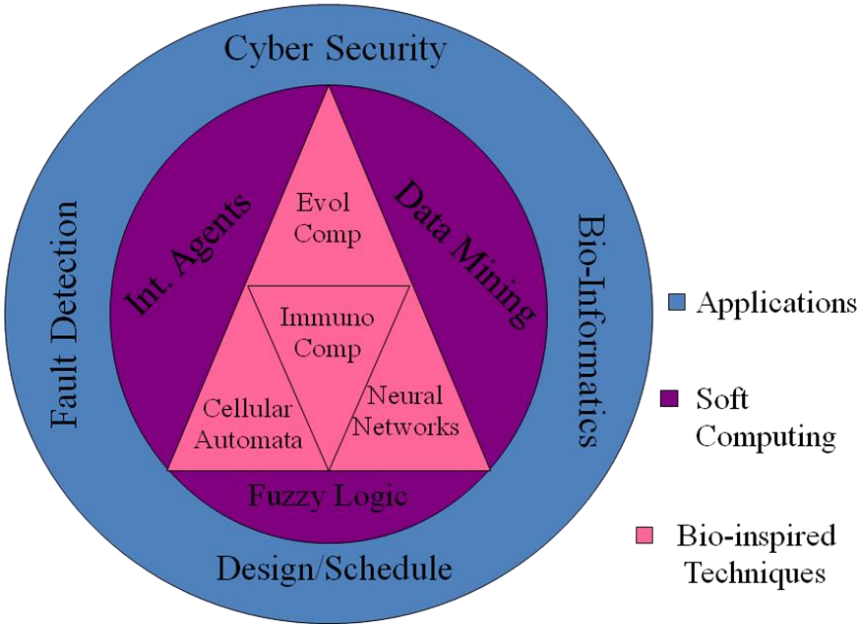
AI-Powered Ransomware detection (AIRaD) tool

By Subash Poudyal and Dipankar Dasgupta, published at HoT SoS, 2021.

- This tool leverages AI techniques to identify the distinguishing behavioral chains in Malware detection.
- The snapshot shows the GUI of multi-level analysis of Ransomware executables.



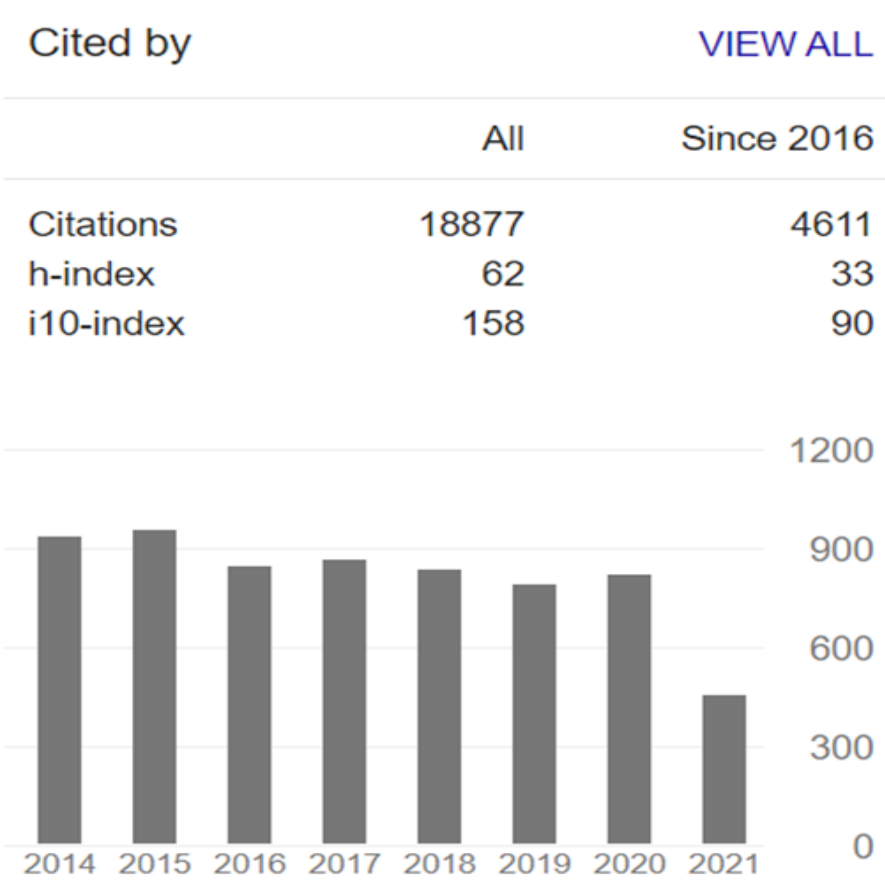
My Research Publications



Conducting multidisciplinary/ collaborative research

Dasgupta's research citation statistics as shown in Google Scholar (accessed on July 16, 2021).

300+ Publications (& 5 patents)



CfIA Recent Projects

(more than $20M Collaborative Funding)

IARPA Negative Authentication Systems (NAS)

NSA Adaptive Multi-Factor Authentication (A-MFA)

NSF Puzzle Based Cyber Security Learning To Enhance Defensive Skills of Front-Line Technicians

NSA GenCyber Boot Camp 2016-2018

MIDDLE SCHOOL CAMP June 12–16 | HIGH SCHOOL CAMP July 19–23

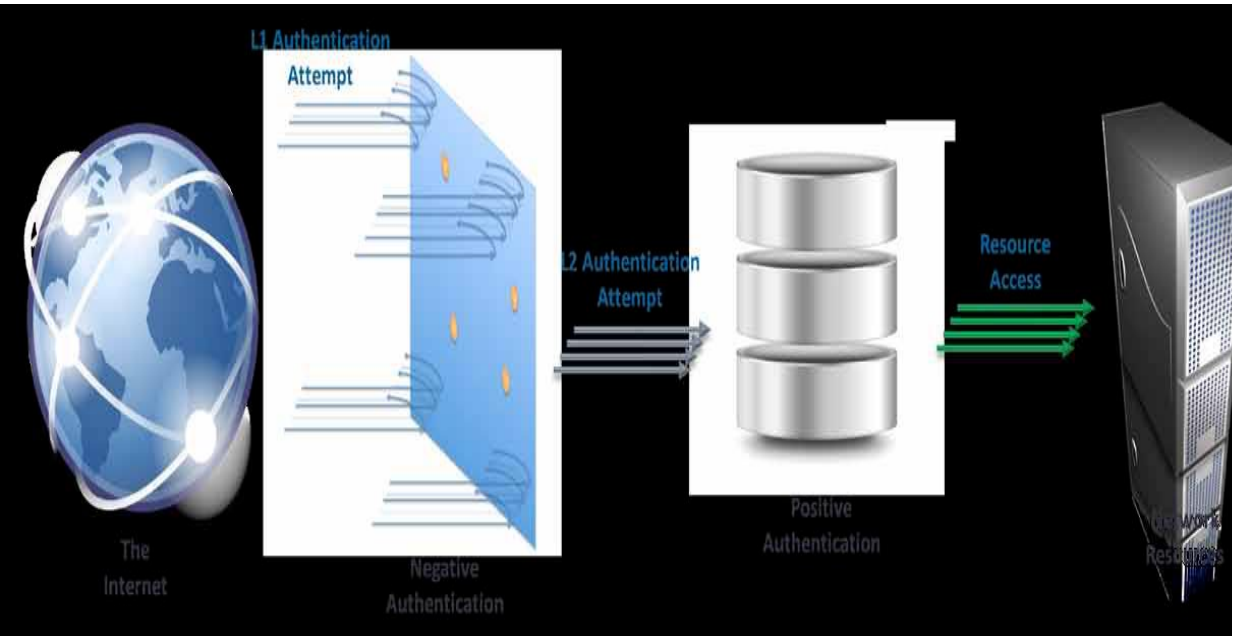
Cyber Ambassador Summer Camp for High School (2019-21)

FEMA Cyber Security Training Programs (since 2006)

ROTC Cyber Security Training Program

THE UNIVERSITY OF MEMPHIS
Center for Information Assurance

Negative Authentication System (NAS)



IARPA Project: Multi-layered Authentication System

Video of NAS: https://vimeo.com/98054594

THE UNIVERSITY OF MEMPHIS
Center for Information Assurance

Adaptive Multi-Factor Authentication (A-MFA)

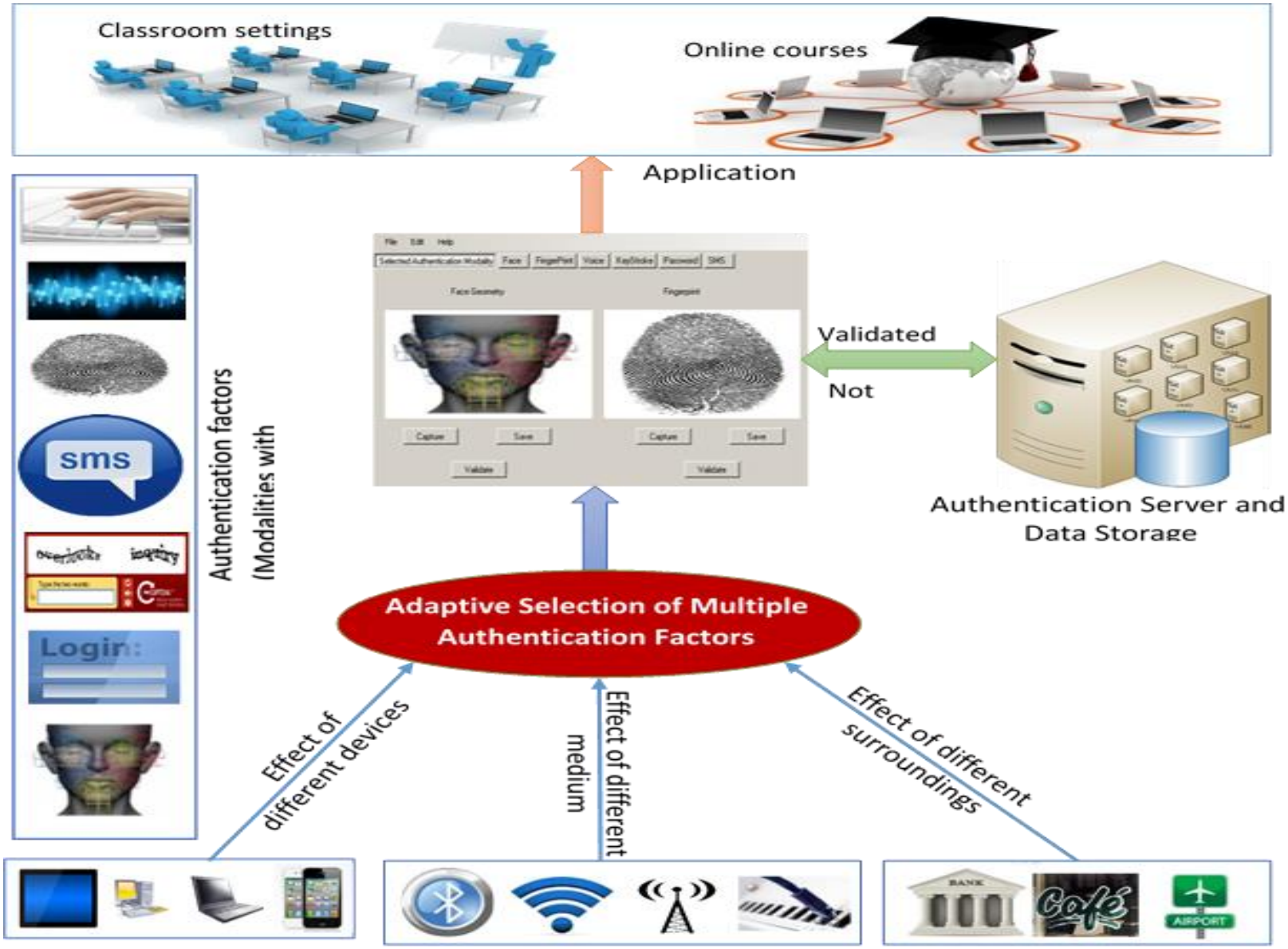
- This greatly enhances security without changing the user experience.
- However, when an unauthorized user attempts to gain access with stolen credentials and the additional factors and behaviours normally seen don't line up, the login is prevented and challenged.
- The selection of multiple authentication factors are conducted adaptively considering

Operating devices

Connected Media

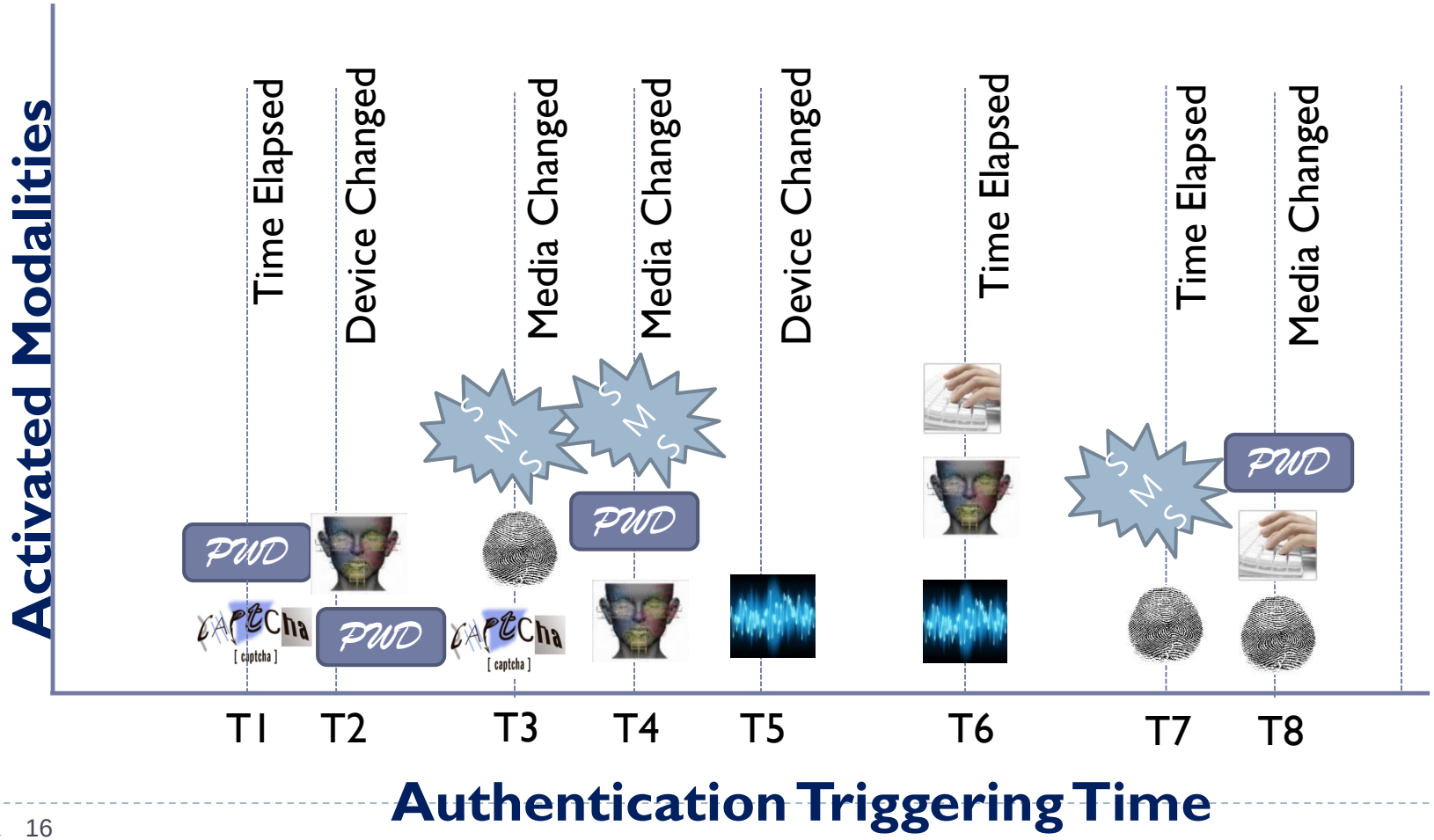
Surrounding Conditions/Environment

Overall Concept of A-MFA



THE UNIVERSITY OF MEMPHIS
Center for Information Assurance

Auth Modality Activation Pattern



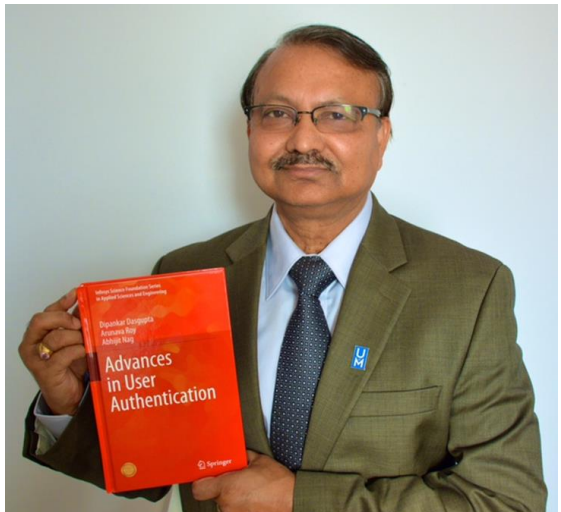
A-MFA: Important Features

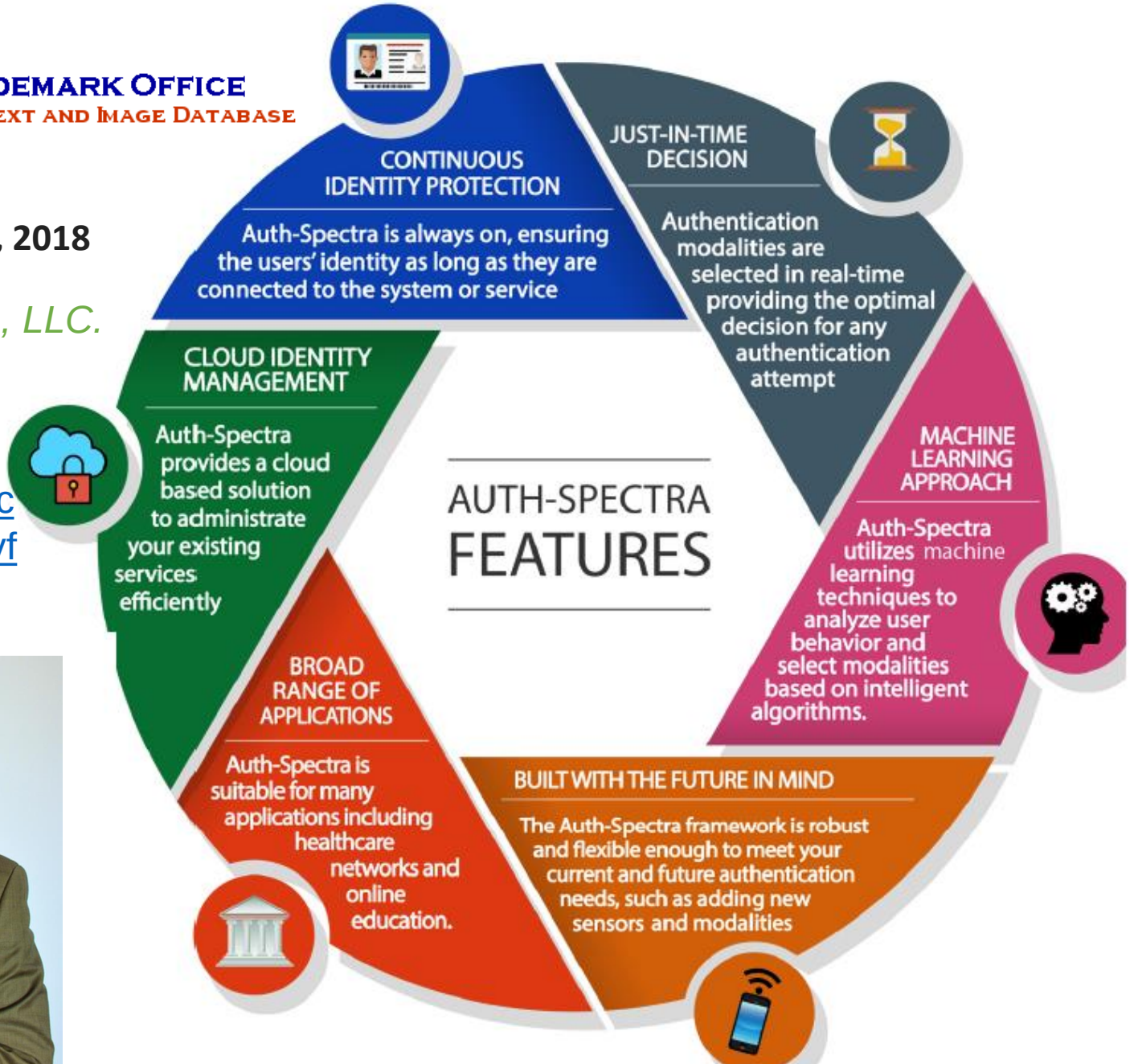
US PATENT & TRADEMARK OFFICE
PATENT APPLICATION FULL TEXT AND IMAGE DATABASE

Patent # 9,912,657
Issue Date: March 6, 2018

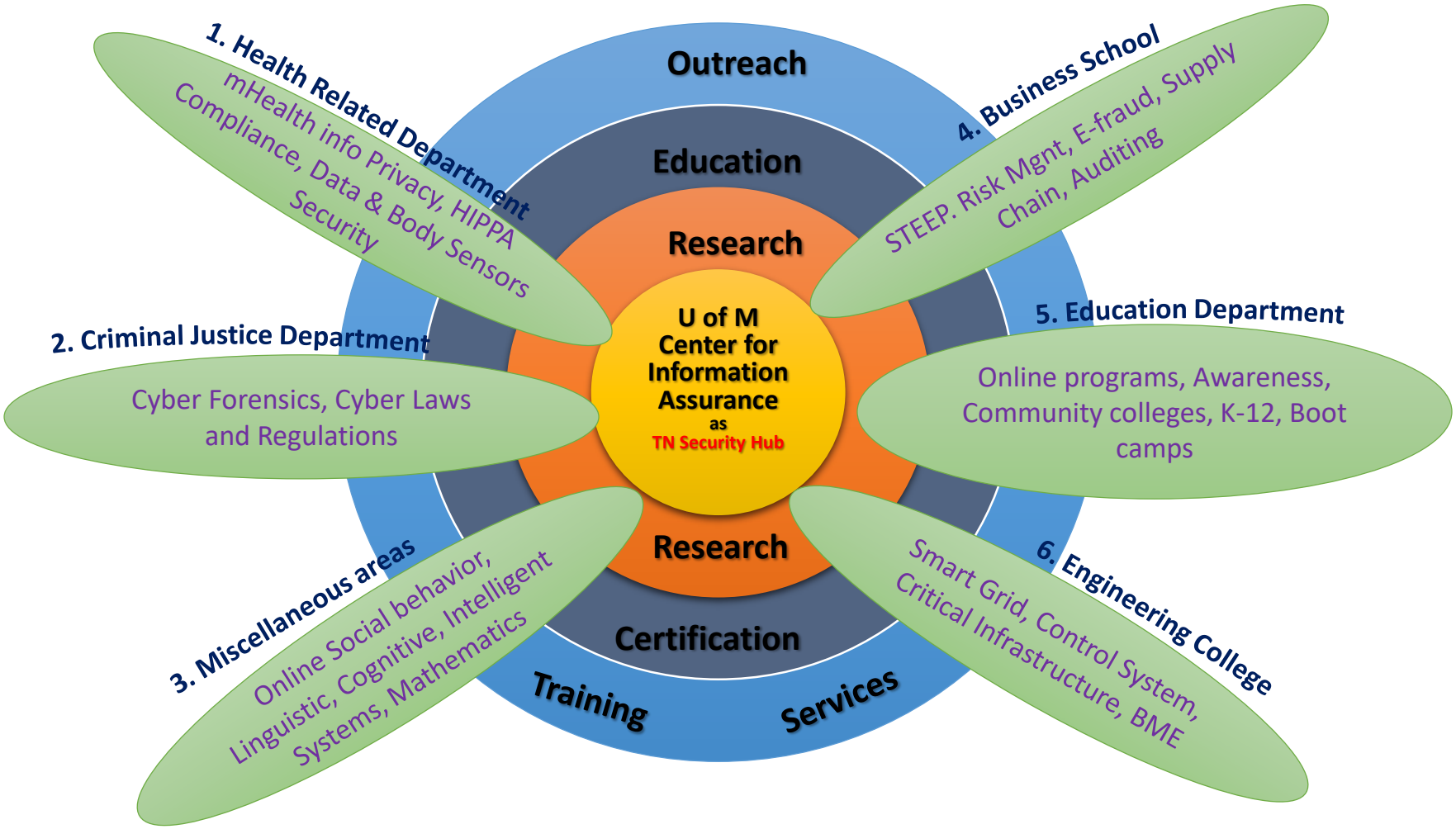
Licensed by i2chain, LLC.

Prototype Demo available at Youtube: https://www.youtube.com/watch?v=x7i2w5vfzYY





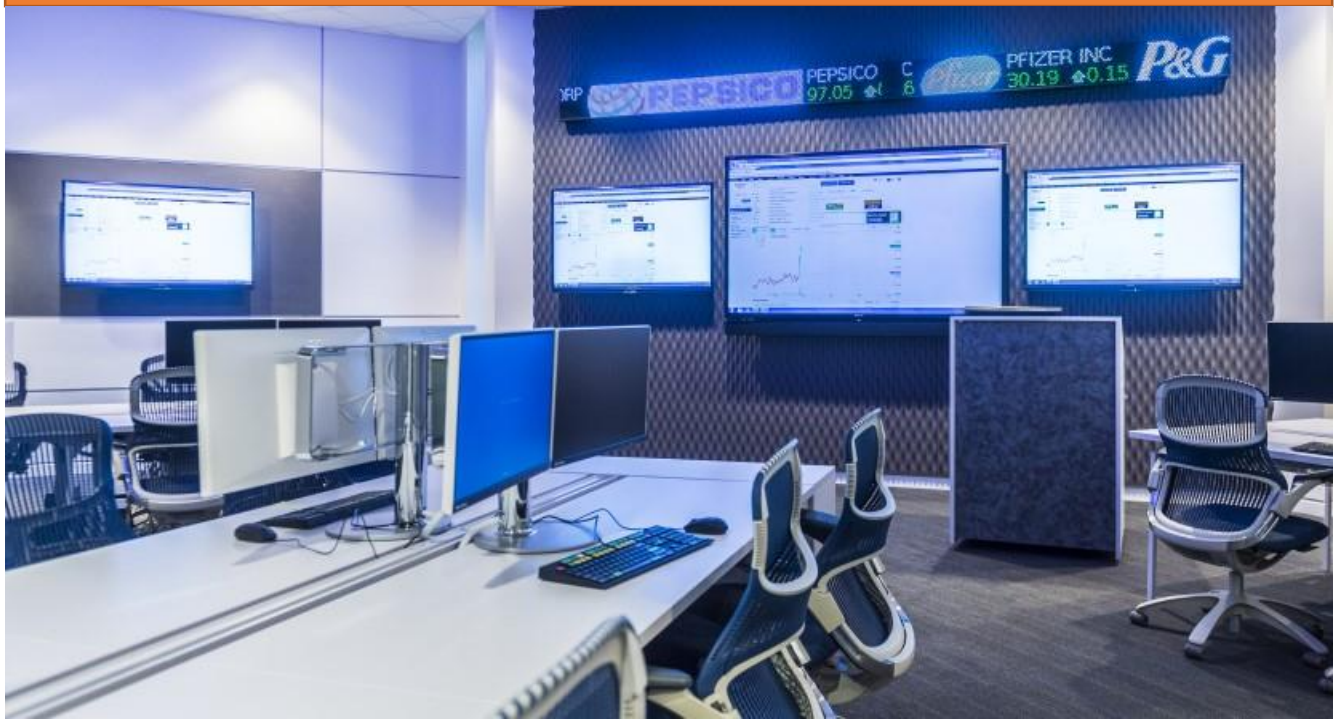
CfIA Multi-Disciplinary Collaboration



CAST Active Research Projects

1. Collaborative Monitoring of Moving Target Defense Mechanisms for Cloud Computing (Sajjan Shiva)
2. Investigation and Testing of Cyber Security in Protective Relay System of Smart Power Distribution Grid (Mohd Hasan Ali, Dipankar Dasgupta)
3. Exploring Cyber Security Issues and Solution for Energy Storage at Smart Microgrid System (Mohd Hasan Ali, Dipankar Dasgupta)
4. Mitigating Ransomware Attacks by Leveraging Isolation Techniques (Bo Chen, Dipankar Dasgupta)
5. Protecting Data Security in Smart Internet-of-Things (IoT) Environments (Lan Wang)
6. Impact of Privacy Data Events on Consumer (George Deitz, Mehdi Amini, Subhash Jha)
7. Design of Gamification for Information Security Awareness and Compliance: An Empirical Study in the Context of Phishing Emails (William Kettinger, Jong Lee, Chen Zhang)
8. Corporate Governance Effectiveness and Cyber Security Risk Assessment and Management (Zabi Rezaee, Joseph Zhang)
9. Senior Hospital Administrators' Challenges on Emerging Cyber Security in Healthcare: An Exploratory Study using Q-Methodology (Soumitra Bhuyan, Marian Levy, Dipankar Dasgupta)

Financial Infrastructure Stability and Cyber-security (FISC) Center



Goal is to identify systemic threats to financial infrastructure stability and market resiliency by applying big data analytics and advanced statistical techniques to financial data.

THE UNIVERSITY OF MEMPHIS
Center for Information Assurance

Puzzle Based Cyber Security Learning To Enhance Defensive Skills of Front-Line Technicians

Funded by National Science Foundation, NSF- ATE Award Numbers 1406992/ 1406853

The goal of this project is to improve the effectiveness of cyber security education through puzzle-based learning (PBL), expanding student knowledge and problem solving skills through the stimulation of their cognitive abilities. PBL has already proven effective in many STEM learning environments including mathematics, physics, and computer science as an interesting and effective way of learning complex logic and abstract concepts. Cyber security has increasingly become important due to the escalating sophistication and frequency of online attacks, as well as the consequences of these attacks for various organizations and their infrastructures. This PBL project utilizes various approaches (simulations, interactive graphics, games, etc.) to improve defensive skills that will not only teach students how to protect specific systems, but also how to protect entire classes of systems that provide similar services, but with differing hardware/software components and architectures.

For more information about PBL-SEC project visit:
http://cfia.memphis.edu/pbl-sec/

Jackson State Community College

THE UNIVERSITY OF MEMPHIS
Center for Information Assurance

Collaborative Project:
Jackson State Community college and The University of Memphis

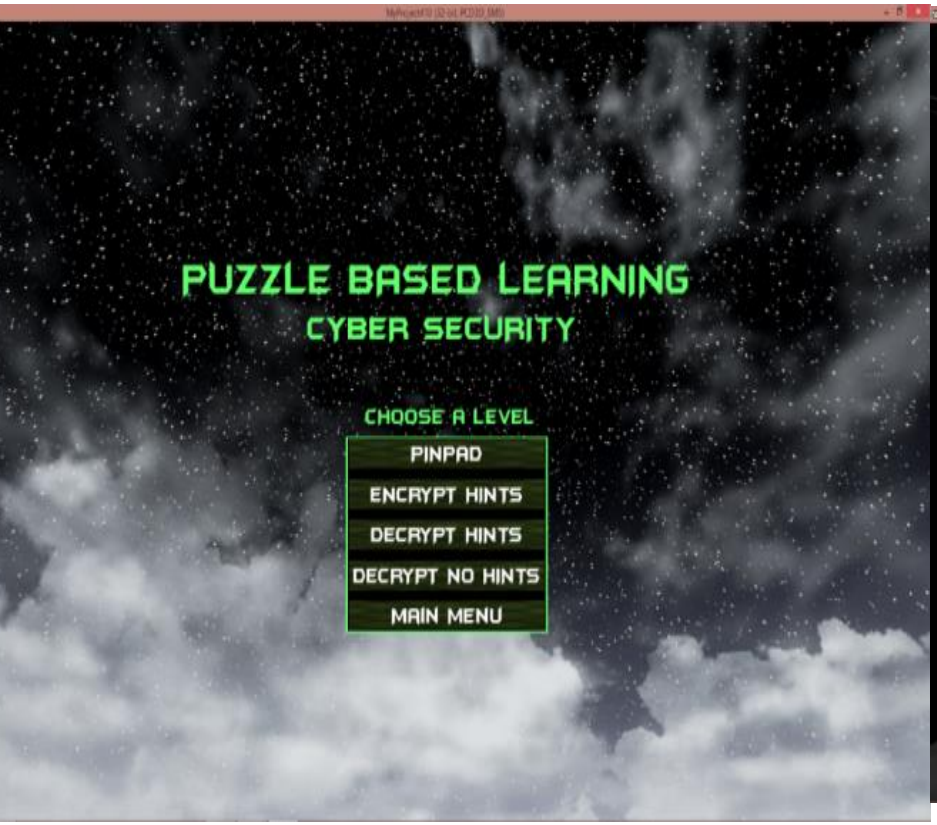
Targeted Audience:
Community College Students pursuing careers in computer networking and security fields

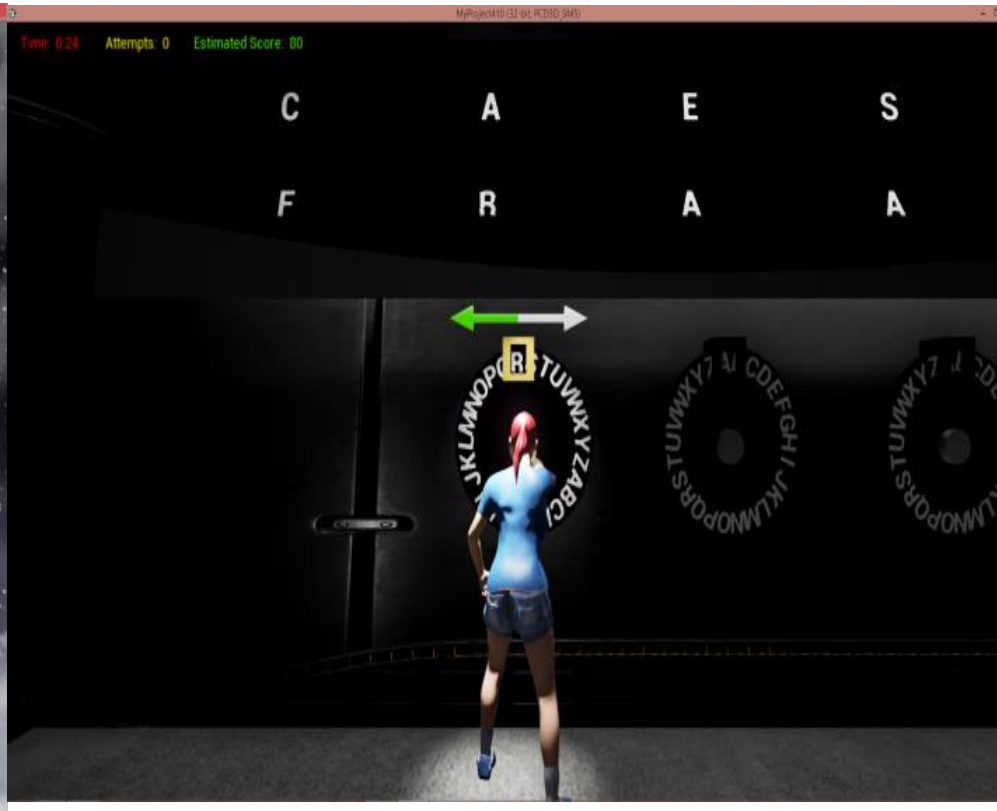
PRINCIPAL INVESTIGATORS:

Prof. Thomas L. Pigg
Dean of Allied Health and CIS/Professor of CIS
Jackson State Community College (JSCC)
Email: tpigg@jscc.edu

Prof. Dipankar Dasgupta
Director, Center for Information Assurance
The University of Memphis
Memphis, TN 38152-3240
Email: dasgupta@memphis.edu

NSF Project on Puzzle-Based Learning (PBL):





ACT Online Program: A DHS/FEMA Project ($4.2M)

Developing a multi-track, multi-level cyber security training program that will prepare

- **Information system**
- **Professionals**
- **and law enforcement officers**

To identify
prevent
protect against
respond to
and recover

from

from cyber attacks at the federal, state and local levels and businesses.

THE UNIVERSITY OF MEMPHIS
Center for Information Assurance

Web-based Course Module

act online

Star Legacy Model: Designed based on Anchored Instruction

- **Challenge**
  - The Challenge is a short scenario (in a real world setting) that trainees ordinarily see first upon entering a module
- **Thoughts**
  - Contains several rhetorical questions about the Challenge scenario that are designed to further stimulate the trainee's thinking.
- **Resources**
  - learners can access multiple learning resources that address various aspects of the challenge.
- **Self-Assessment**
  - learners are provided an opportunity to confirm their understanding of materials presented in *Resources using formative assessment questions* with progressive remediation.
- **Wrap-Up**
  - used to provide students with answers to the rhetorical questions posed in "Thoughts", and also provides students with a second scenario which illustrates the concepts covered by the module.

ACT Cybersecurity Training Catalog

Track 1 IA General/Non-Technical	*Track 2* IA Technical/IT Professional	*Track 3* IA for Business Professionals
Information Security for Everyone TEI Course #: AWR-175-W	Information Security Basics TEI Course #: AWR-173-W	Business Information Continuity TEI Course #: AWR-176-W
Cyber Ethics TEI Course #: AWR-174-W	Secure Software TEI Course # AWR-178-W	Information Risk Management TEI Course # AWR-177-W
Cyber Law and White Collar Crime TEI Course #: AWR-168-W	Network Assurance TEI Course #: AWR-138-W	Cyber Incident Analysis and Response TEI Course # AWR-169-W
Understanding Social Engg. Attacks (USEA) TEI Course #: AWR-367-W	Digital Forensics Basics TEI Course # AWR-139-W	Cyber Identity & Authentication (CIAA) TEI Course#: AWR-384-W
End-User Security & Privacy (ESP) (coming soon)	Mobile Device Security & Privacy (MDSP) TEI Course #: AWR-385-W	Examining Adv. Persistent Threats (EAPT) TEI Course #: AWR-403-W

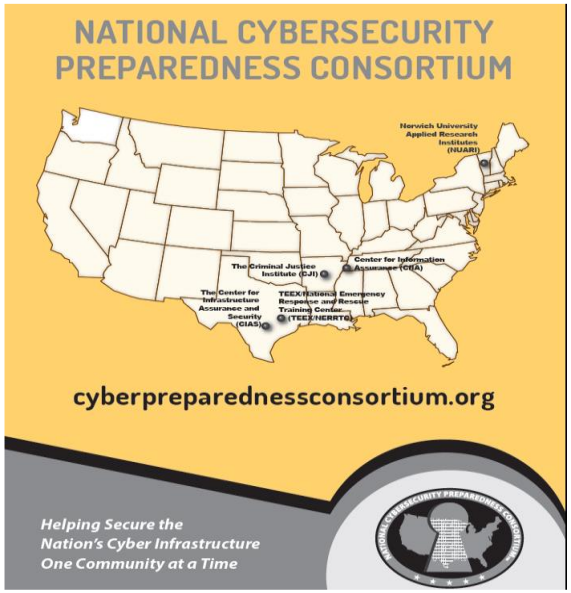
Total 15 ACT Online courses (updated regularly) are now available FEMA-TEEX website. More than 50,000 people completed these courses since 2009.

FedEx Institute of Technology
The University of Memphis

THE UNIVERSITY OF MEMPHIS. | Center for Information Assurance

Student Success: National CyberSEED 2016 Competition

UM/CfIA National-Level Collaboration



http://www.cyberpreparednessconsortium.org/

NCPC Consortium members:

- **The University of Texas at San Antonio**
- **The University of Memphis**
- **The University of Arkansas**
- **Norwich University**
- **Texas A&M University**

Follow NCPC activities in LinkedIn

CAE IN CYBERSECURITY COMMUNITY

NATIONAL CYBERWATCH CENTER

CENTER FOR CYBERSECURITY AT THE UNIVERSITY OF WEST FLORIDA

Collaborative Research Opportunities

- **NSF Resilient & Intelligent NextG Systems (RINGS) , July 29, 2021**
- NSF-21-500: Secure and Trustworthy Cyberspace (9/30/2021)
- NSF-21-597: SaTC Frontiers LOI-9/7/21(Full:11/17/2021)
- DHS-21-CISA-127-CWDT001: Cybersecurity Workforce Development and Training Pilot for Underserved Communities (Due August 25, 2021)
- Energy Sector Self-Reliance BAA

  BAA-OAA-E3-ENERGY-2020 (2/05/2022)
- DARPA Information Innovation Office (I2O) Office-wide.

  HR001121S0010 (10/28/2021)
- NSF 21-585: Program on Fairness in Artificial Intelligence in Collaboration with Amazon (August 3, 2021)
- NSF-20-570: Industry-University Cooperative Research Centers Program (IUCRC), 9/8/2021
- NSF-20-584:Research Experiences for Teachers (RET) in Engineering and Computer Science, 915/21
- NSF-21-591: Computer and Information Science and Engineering (CISE) Research Initiation Initiative (CRII), Due 9/20/2-21.

National Science Foundation (NSF) Convergence Accelerator Expo 2021, scheduled virtually July 28 – 29, 2021

2021 IEEE Symposium on Computational Intelligence in Cyber Security (IEEE CICS)

at

2021 IEEE SYMPOSIUM SERIES ON COMPUTATIONAL INTELLIGENCE (IEEE SSCI)

December 4- December 7, 2021, Orlando, Florida

URL: https://attend.ieee.org/ssci-2021/

DEADLINES:

- **Special Track/Session Proposal: May 28, 2021 (Deadline passed)**
- **Paper Submission: August 6, 2021**

Symposium Chair: Dipankar Dasgupta, IEEE Fellow, The University of Memphis, USA

Co-Chair: Kaushik Roy, North Carolina A&T University, USA.

THANK YOU!