International Academy, Research, and Industry Association (IARIA) Tutorial

Advanced Cyber Topics

Tutorial Session I

Instructors: Dr. Thomas J. Klemas and Dr. Steve Chan

18 November 2018

Facilitating Decision-Making Via Deep Insights

Decision Engineering Analysis Laboratory

San Diego
Cambridge

Tutorial Syllabus

Section 1: Cyber Assessment, Cyber Frameworks, Machine Learning (25 min)

- Cyber Ranges
- Cyber Assessment
- Cyber Frameworks
- Machine-Aided Applications

Section 2: Cyber Robustness, Adaptation, Countermeasures and Analytics (25 min)

- Video #1: Whitebox Orientation for Software Cyber Robustness (15 min)
- Lessons Learned from Cyber Efforts amidst Ever-Increasing Cycles of Adaptation
- Anti-Systems (Countermeasures)
- Predictive Analytics

Section 3: Artificial Intelligence, Creativity, Mutation, Traffic Analysis, Information Sharing (25 min)

- Video #2: Hybridizing Artificial Intelligence Systems with Human Intuition as well as Open Source and Non-Open Source Components (15 min)
- Lessons Learned for Maximal Cyber Creativity to mitigate High Adversarial Mutation Rates.
- Traffic Analysis (Baselining, Pattern and Anomaly Detection)
- Information Sharing (Target of Choice or Target of Chance)

Section 4: Ideation for Future Cyber Innovation (5 min)

- Audience participation with Instructor moderation
- Cyber Survey (Time Allowing)

Tutorial Instructor Background

- Dr. Thomas Klemas
  - Alumnus of MIT
  - Numerous publications in Computational Electromagnetics, Radar, Open System Architecture, Data Analytics, Cyber Technology, Sustainability and Resilience
  - Directed MIT Advanced Computational Modeling & Simulation Program and MIT Computational Modeling Collaboration
  - Variety of senior advisory and leadership positions
  - Co-Founder and VP of Analytics2Insight
  - IARIA Fellow, Steering Committees (Cyber and Data Analytics), Keynote Speaker, Panelist, Session Chair, Instructor
  - Director, Decision Engineering Analysis Laboratory
- Dr. Steve Chan
  - Alumnus of MIT and Harvard University.
  - Numerous publications on Prototype Frameworks, Decision Engineering, Data Analytics, Cyber Electromagnetic Technology, Sustainability and Resiliency
  - Co-Founded various centers and served as Chief Architect and/or CTO; Advisor for the MIT Advanced Computational Modeling & Simulation Program, MIT Computational Modeling Collaboration
  - Former Strategic Development Advisor to several Fortune 500 firms and Scientific Advisor for various Silicon Valley companies
  - Variety of Special Advisor and Chief Architect functional roles for government
  - IARIA Fellow, Steering Committees (Cyber and Data Analytics), Keynote Speaker, Panelist, Session Chair, Instructor
  - Director, Decision Engineering Analysis Laboratory

Section 1: Cyber Assessment, Cyber Frameworks, Machine Learning

- Cyber Ranges
- Cyber Assessment
- Cyber Frameworks
- Machine-Aided Applications

Cyber Ranges

- Computational resources: Data center or cloud
- Hypervisor
- Construct virtual machines
  - Emulate arbitrary hardware and operating systems
  - Computers: clients, servers, tools
  - Devices: routers, switches
  - Firewalls, proxies
- Network
- Services

Cyber Range Example

- Illustrate Range Model Diagram
- Subnet description
- Cybersecurity tools subnet
- Services
- Networking devices

Web Interface to Cyber Range Model

- Web-based access console
- Login
  - Username
  - Password
- Access virtual range via interface

Web Interface Details

- Event planner determines visibility of virtual machines that comprise a particular range model
- Virtual machines (VM) visible in web-interface emulate physical access
  - You can “sit down at the console” and log in if the VM is visible
  - You can still access other VM’s using tools (example: ssh)
- Click on VM icon to access that VM
- Additional information can be provided
  - Event instructions
  - Network diagram

Web Interface: Accessing a particular VM

- Log into console
- Linux: Opens window with terminal or desktop view
- Windows: Opens window with desktop icon view
- Type commands or click icons (depending) to access VM capabilities

Web Interface: Accessing cyber tools

- Log into console
- Open browser
- Access tool console using browser
- Type queries to harness tool
  - Queries for investigation searches
  - Plots, Charts, etc for visualization of results
  - Examples
    - Centralized, aggregated data: Kibana, SGUIL
    - Direct access grep of proxy log

Web Interface: Management of Events

- Invite users to events
- Assigning visibility permissions to users

Section 1: Cyber Assessment, Cyber Frameworks, Machine Learning

- Cyber Ranges
- Cyber Assessment
- Cyber Frameworks
- Machine-Aided Applications

Introduction to Assessment

- Protection
  - Important but limited (e.g. insider threat)
  - Importance of assessment
- Adversary is already on your network
  - Monitoring and detection
  - Hunt and pursuit
  - Investigation
  - Respond
  - Recovery
- Individual: knowledge, skills, abilities, and persistence
- Team: Leadership, organization, communication, teamwork, dutifulness

Beneficial Capabilities

Evaluating Domain-specific Skills and more general Abilities of Individuals
- Mapping Questions to Frameworks to provide Specialty Scoring
- Provide Knowledge, Skills, Ability, and task sub-scores

Multiple Classification Systems
- Based on Job Task Analysis
- Customer categorization frameworks
- Traditional Frameworks

Composition of Teams
- Evaluate areas of strength and gap areas
- Build teams that are equal levels
- Compose special teams that are designed for maximal performance

Determine topics for training and order of importance

Section 1: Cyber Assessment, Cyber Frameworks, Machine Learning

- Cyber Ranges
- Cyber Assessment
- Cyber Frameworks
- Machine-Aided Applications

Cybersecurity Frameworks Introduction

- National Initiative for Cybersecurity Education (NICE)
- National Institute of Standards and Technology (NIST) Cybersecurity Framework
- Center for Internet Security (CIS) Controls
- ISO/IEC 27000 family - Information security management systems
- Gunnery Tables
- Mission Essential Tasks (METs)
- And many more, each with a specific focus

National Initiative for Cybersecurity Education (NICE)

- Motivate & implement robust environment for cybersecurity (CS) education, training, workforce development
- Foundational element for Risk Management Process
- Hierarchical Framework
  - High level categories
  - Job Specialties
  - Work Roles
  - Knowledge, Skills, Abilities (KSAs)
  - Tasks
- Goal: Increase skilled CS professionals

National Institute of Standards and Technology (NIST) Cybersecurity Framework

- Executive Order “Improving Critical Infrastructure Cybersecurity” Feb 12, 2013
- Industry standards and best practices
- Hierarchical Framework
  - Functions
  - Categories
  - Subcategories
- Foundation for risk management process
- Key Benefits
  - Describe current cybersecurity (CS) posture
  - Describe CS target state
  - Identify and prioritize improvement opportunities
  - Assess progress toward target state
  - Communicate in common language about CS risk

Cybersecurity Framework Benefits

- Frameworks provide common nomenclatures
- Foundation for Risk Management Process
- Key Benefits of Workforce Framework
  - Job Task Analysis
  - Hiring
  - Revectoring
  - Training
  - Identification of Leadership Potential
- Example: ANSI Certifications and Certificates
  - Certification of Personnel
    - ISO/IEC 17024: ~ 400 requirements
    - Proficiency certification, Licensing
    - Topics: Fairness, Validity, Reliability (Cut Scores, Psychometrics)
  - Certificate Program
    - ASTM E2659: ~100 requirements
    - Coursework
    - Topics: Quality of Instructors, Learning Outcomes, Auditing (Offeror Stability)

Section 1: Cyber Assessment, Cyber Frameworks, Machine Learning

- Cyber Ranges
- Cyber Assessment
- Cyber Frameworks
- Machine-Aided Applications

Machine-Aided Cybersecurity Applications

- Spam filters, web-site blockers
- Malware detection and identification
- Monitoring-aid
- Anomaly detection
  - User behaviors
  - Network traffic
- Rapid interim response
- Decision support

Fundamentals of Machine-Aided Decision Making

- Task automation requires that computers interact with environments
- Detect objects
- Compute statistics on object class distribution
- Determine object classes or categories
- Classify objects
- Compute statistics on object class distribution
- Expert system rules guide automated decision making
- Anomaly detection tools
  - Generate additional insights
  - Provide suggestions to operators
  - Alert human operators of required interventions

Elements of Pattern Recognition And Machine Learning

Description of Details

- Potential Data Sources
  - Email
  - Files, Folders
  - Log data
  - Packet traffic data
- Potential Features
  - Source/Destination IP addresses
  - Traffic direction
  - Source/Destination ports
  - Source/Destination netmasks
  - Source/Destination protocols
  - Port, file, folder, registry blocking. Processes to include/exclude
  - Payload
- Potential Approaches
  - Signature-based methods, Linear Decision Analysis, Support Vector Machines, Bayesian Classifiers, Partitioning, Clustering, Neural Networks
  - Machine Learning: Supervised, Semi-supervised, Unsupervised

Introduction to Clustering

- Specific examples and closely related concepts
  - Partitioning
  - Typology, Taxonomy
  - Unsupervised learning
  - Learning without a teacher
- Key issues
  - Limited or no availability of training data
  - Select features, proximity measure, and criteria for clustering
  - Determine number of clusters
- Potential Benefits
  - Reduction / Compression
  - Hypothesis building: inferring and testing of ideas
  - Prediction

Fundamentals of Clustering 1

- K-means algorithm
  1. Key parameter: number of clusters, K
  2. Select feature vector and proximity metric
  3. Compute K random cluster centers
  4. Assign each data point or vertex to the closest of the K clusters
  5. Recompute cluster centers based on mean of feature vectors of assigned vertices
  6. Return to step 4 and repeat subsequent steps until convergence
- Frequently, K-means hybrids with other approaches can achieve faster, better results
  - Training points to determine number of clusters, pick centers
  - Repeated K-means with different K, number of clusters, and a cluster-quality criterion can be used to determine best K

Fundamentals of Clustering 2

- Spectral Clustering
- Spectral-based partitioning into 2 clusters
  - Feature vector
  - Proximity metric
    - Example 1: gaussian function of distance between feature vectors of node m and node n
    - Example 2: cosine similarity vector product of feature vectors for node m and n
  - Similarity Matrix: $S_{mn} = proximity(node\ m, node\ n)$
  - Cut Description
  - Normalized Cut Description
  - Laplacian matrix: L = D-A
  - Eigenvector associated with second smallest eigenvalue
- Hierarchical application of spectral-based partitioning

Section 2: Cyber Robustness, Adaptation, Countermeasures and Analytics

- Video #1: Whitebox Orientation for Software Cyber Robustness (15 min)
- Lessons Learned from Cyber Efforts amidst Ever-Increasing Cycles of Adaptation
- Anti-Systems (Countermeasures)
- Predictive Analytics

Section 3: Artificial Intelligence, Creativity, Mutation, Traffic Analysis, Information Sharing

- Video #2: Hybridizing Artificial Intelligence Systems with Human Intuition as well as Open Source and Non-Open Source Components (15 min)
- Lessons Learned for Maximal Cyber Creativity to mitigate High Adversarial Mutation Rates.
- Traffic Analysis (Baselining, Pattern and Anomaly Detection)
- Information Sharing (Target of Choice or Target of Chance)

Section 4: Ideation for Future Cyber Innovation

- Audience participation with Instructor moderation
- Cyber Survey (Time Allowing)

THANK YOU FOR YOUR PARTICIPATION

Facilitating Decision-Making Via Deep Insights

Decision Engineering Analysis Laboratory

San Diego
Cambridge