Cyber-Physical Systems Security

- ISDA Research
  - Transdisciplinary research groups, a holistic and cross-cutting curriculum, and a state of the art security-related operations center
  - Allow Virginia Tech's cutting-edge faculty to further innovate over multiple disciplines
  - Realizing the breadth of security risks around the world: environmental, technological, and human threats
  - Recognizes the need to understand the integrated nature of both the sources of and possible solutions to these security threats
  - Focuses on four broad areas of security that incorporate and integrate numerous traditional approaches for understanding issues related to personal, communal, national, and global security.

- Cyber-Physical Systems Security
  - A cyber-physical system (CPS) involves the interconnection of the digital world, the physical world, and humans interacting with both worlds.
  - Automation to self-driving cars, and the breadth of technology increases every day with new innovations.
  - Optimize our environment through analytics and efficiencies
  - Also open up major new attack vectors for hackers and could seriously compromise our privacy.
  - Within this research thrust we seek to understand and address fundamental security and privacy challenges in the Internet of Things (IoT) and intelligent infrastructure.

Lightning Talks
Speaker: Ahmed Abdelhadi, PhD
Research Assistant Professor
email: aabdelhadi@vt.edu

Research Interests:
- Security and Privacy of Cyber Physical Systems (CPS)
- Bio-manufacturing Process
- Smart Grid
- Internet of Things (IoT)
- Wireless Systems

Approach: Multi-Layer CPS Security
- Cryptography
- Machine Learning
- Data Mining
- System Control
- Robust Statistics

Multi-Layer Cyber Physical System Security

Secure Authentication and Encryption
Secure Communications
CAN Bus Security
Cyber-Attack: Resilient Controller

Secure Authentication and Encryption
Secure Communications
CAN Bus Security
Cyber-Attack: Resilient Controller

Integrated Security Destination Area: Research Topics

Michael Fowler
Research Faculty
Aerospace Systems Lab, Hume Center
mifowler@vt.edu

- Integrated Security Research Interests
  - Counter-Side Protection
  - Autonomous Systems & Mission Orchestration
  - Autonomous Systems Security
  - Autonomous Intelligent Testing of Cyber Physical Systems
  - Security on Graphs

- Research supported by
  - NAVAIR / VTAC
  - DARPA
  - ONR
  - AFRL
Goals and impact

Quantum computing
• Breaking RSA cryptosystem

Secure quantum communications
• Quantum key distribution
• Quantum networks

Approaches

Quantum networks

Notable publications

Quantum control for quantum computing
• Barnes & Das Sarma, PRB, 90, 035306 (2014)
• Barnes et al., Scientific Reports 5, 12660 (2015)
• Economou & Barnes, PRB 91, 164406(R) (2015)

Secure quantum communications
• Buterakos, Barnes, Economou, arXiv:1612.03869
• Economou & Dev, Nanotechnology 27, 504001 (2016)

Adaptive Response to Advanced Persistent Threats

Nathan Lau, Assistant Professor, ISE
nathan.lau@vt.edu

Real-Time Scheduling for CPI Protection

Tam Chantem
tchantem@vt.edu
Walid Saad, ECE, walids@vt.edu

- Research interests: game theory, cyber-physical systems, wireless networks, machine learning, and security issues across.
- Wireless security: jamming, eavesdropping, etc.
- Cyber-physical systems security
  - Science and foundations
  - Threats and coordinated attacks
  - Applications: smart grid, Internet of things, drones, transportation, etc.
- Smart cities and big data
  - Resilience of smart cities in face of security and emergency
  - Critical infrastructure protection
  - Adversarial machine learning

Lynn Abbott  Computer Engineering  abbott@vt.edu

Biometric Authentication
- Fingerprints
- Cardiovascular signals
VT IT Security Office and Lab

- Randy Marchany
- IT Security Lab Director
- VT IT Security Officer
- 1300 Torgersen
- http://security.vt.edu
- marchany@vt.edu
- Students work with live data and assist analysis dealing with cyber attacks against VT
- Research done using data collected by the ITSL/ITSO

Prof. Kyriakos G. Vamvoudakis
Department of Aerospace and Ocean Engineering

- Research brings together optimal and adaptive control, reinforcement learning, cyber-physical security, data analytics.

For papers please see: http://www.dept.aoe.vt.edu/~kyriakos/

Implementation Security

Patrick Schaumont
schaum@vt.edu

Demonstrator: FAME chip

Open Challenges
- Attacker and Threat Models
- Metrics
- Design Composition and (Formal) Verification
- Security across Hardware/Software Abstraction
- Design Automation for Secure Implementation
- Trusted Hardware
- Energy Efficiency and Performance
Discussion

1. What major projects or sponsored research opportunities would you like to work on?
   - What other expertise would help you improve your project(s)?

2. What are some major obstacles to your ability to work on these major projects?
   - How can the ISDA help you or your team?
   - What faculty hiring would help bring your research/group/center to the next level?
   - Are there any gaps in research expertise needed?