Integrated Security Destination Area Workshop May 19 2017

Research Breakout Sessions

Cyber-Physical Systems Security

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 that the breadth of security risks around the world includes environmental, technological, and human threats
    - Recognizes the need to understand the integrated nature of both the sources of and possible solutions to these 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

Multi-Layer Cyber Physical System Security

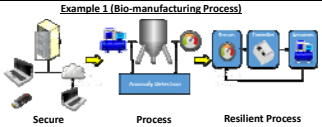
Speaker: **Ahmed Abdelhadi, PhD**
Research Assistant Professor
email: aabdelhadi@vt.edu

Research Interests:
- Security and Privacy of Cyber Physical Systems (CPS)
  - Bio-manufacturing Process
  - Machine to Machine (M2M) Communications
  - Smart Grid
  - Internet of Things (IoT)
  - Wireless Systems

Approach: Multi-Layer CPS Security

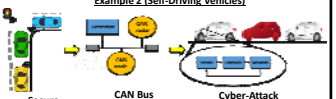
Cryptography | **Machine learning Data Mining** | **System Control Robust Statistics**

Example 1 (Bio-manufacturing Process)

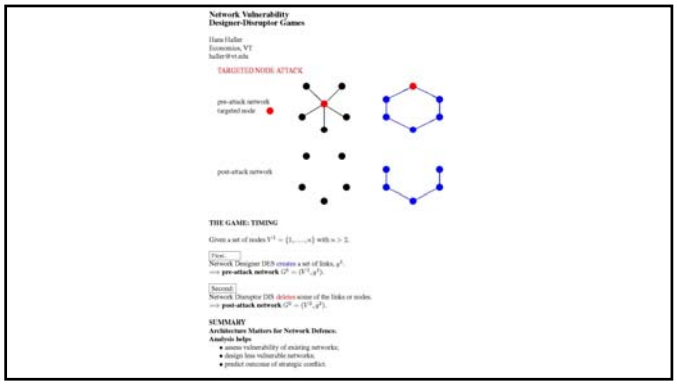


Secure Authentication and Encryption | **Process Anomaly Detection** | **Resilient Process Controller**

Example 2 (Self-Driving Vehicles)



Secure Communications | **CAN Bus Anomaly Detection** | **Cyber-Attack Resilient Controller**



Network Vulnerability Designer-Disruptor Games

Hans Haller
Economics, VT
haller@vt.edu

TARGETED NODE ATTACK

pre-attack network
targeted node

post-attack network

THE GAME: TIMING

Given a set of nodes $V^1 = \{1, \ldots, n\}$ with $n > 2$.

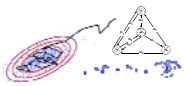
First:
Network Designer DES creates a set of links, g^1.
$\Longrightarrow$ **pre-attack network** $G^1 = (V^1, g^1)$.

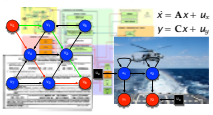
Second:
Network Disruptor DIS deletes some of the links or nodes.
$\Longrightarrow$ **post-attack network** $G^2 = (V^2, g^2)$.

SUMMARY
Architecture Matters for Network Defence.
Analysis helps
- assess vulnerability of existing networks;
- design less vulnerable networks;
- predict outcome of strategic conflict.

Integrated Security Destination Area: Research Topics

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





- **Integrated Security Research Interests**
  - Counter–UAV 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

Quantum Information Technologies for Security

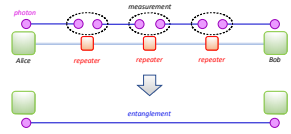
Edwin Barnes & Sophia E. Economou, Virginia Tech

Goals and impact

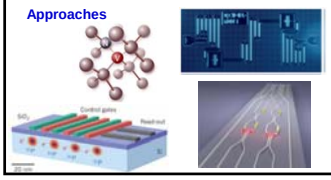
Quantum computing
- Breaking RSA cryptosystem

Secure quantum communications
- Quantum key distribution
- Quantum networks

Quantum networks



Approaches



Notable publications

Quantum control for quantum computing

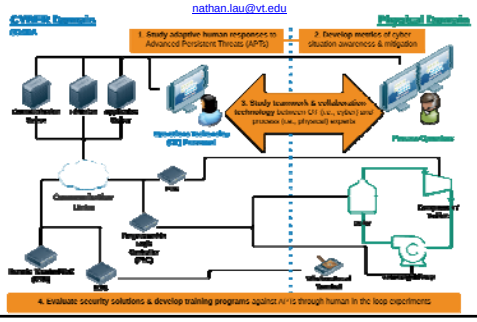
- Barnes & Das Sarma, PRL **109**, 060401 (2012)
- Barnes et al., Scientific Reports **5**, 12685 (2015)
- Economou & Barnes, PRB **91**, 161405(R) (2015)

Secure quantum communications

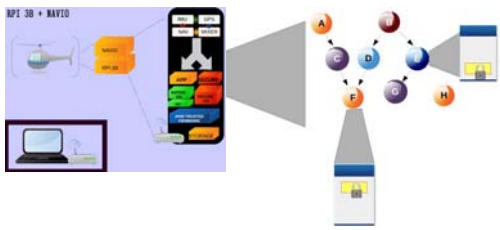
- Buterakos, Barnes, Economou, arXiv:1612.03869
- Economou & Dev, *Nanotechnology* **27** 504001 (2016)

Adaptive Response to Advanced Persistent Threats

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

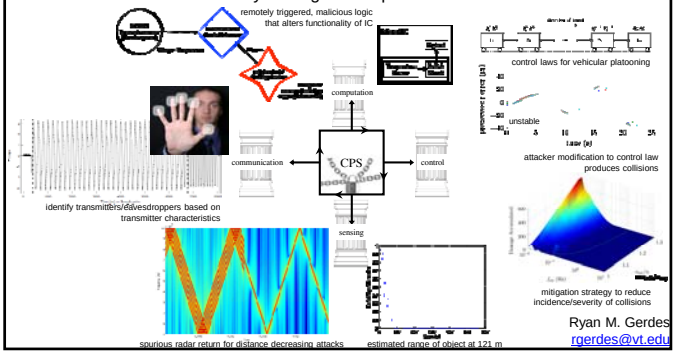


Real-Time Scheduling for CPI Protection



Tam Chantem
tchantem@vt.edu

research theme: resiliency strategies for cps in adversarial environments



Ryan M. Gerdes
rgerdes@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
  - Humans 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

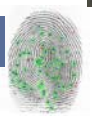
11

Lynn Abbott Computer Engineering *abbott@vt.edu*

Biometric Authentication

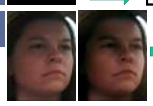
- **Fingerprints**
- **Cardiovascular signals**

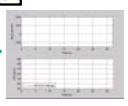
Temporal analysis of fingerprints



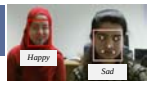
Authentication using ECG and PPG

Remote PPG





Facial expression recognition



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 (kyriakos@vt.edu)
Department of Aerospace and Ocean Engineering

VirginiaTech
Invent the Future

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

Specifically my research proposed:

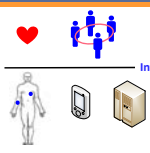
- Online learning algorithms for optimal control, H-infinity control, multi-player games (multiple control inputs) with state feedback.
- Algorithms for optimal trajectory tracking and adversarial input attenuation.
- Defined model-free (Q-learning) optimization algorithms (that self-heal, self-optimize and resist attacks) where the agents are in Nash and at the same time in consensus even when perturbed by persistent adversarial inputs. Only local information needed.
- Intermittent learning algorithms (bandwidth effective), for networked control systems.
- Game-theoretic security of cyber-physical systems, detection, mitigation and estimation in adversarial environments.

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

College of **Engineering**

Implementation Security

Patrick Schaumont
schaum@vt.edu



Bits
Trust

Information Security

Physics
Truth

- Brute Force Security
- Computational Security
- **Implementation Security**
  - Side-channel leakage
  - Controlled Faults
  - Physical Tamper
  - Anti Counterfeiting

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?