Security and Trustworthiness of Modern Cyber-physical Systems

Dr. Dimitrios Damopoulos Computer Science School of Computing



March 2021

About me



Cybersecurity Education needs to start very early...



Last 15 years



Today: Inter-connected world





In 2017 was predicted that 20.4 billion IoT devices will be online by 2020

2020: A significant year for many reasons

- Remote work
- Blockchain and Al
- Apple and Google COVID-19 contact tracing system
- Cyber Attacks
- IoT Cybersecurity Improvement Act of 2020



Cyber-physical Era

• A **cyber-physical system** refers to any networkconnected instrumentation that also interacts with the physical world.



Cyber-physical Ecosystem



Issues & Challenges



Illustration: J. D. King

Are we prepared for the

Cyber-Physical Era ?



Today's Goal: Raise Awareness

- How Security & Trustworthiness in an essential part of:
 - -Cyber-physical systems security
 - -AI / ML Trustworthiness



What is Machine Learning?

- Machine Learning is a branch of Artificial Intelligence based on the idea that systems can:
 - -learn from data
 - -identify patterns
 - -make <u>decisions</u> with minimal human intervention



Cyber-physical Systems Security



Trustworthy Cyber-physical System

- Systems must be **trustworthy** to ensure that the technology is used to benefit humanity
- Software Security
- Hardware Security
- Network Security
- Cloud Security
- Smartphone / IoT Security / CPS
- Digital Forensics

- AI / ML trustworthiness
- Standards & Frameworks
- Compatibility Legacy system
- Privacy Law Ethics
- Management
- Education





Built-in Security Mechanisms

- Secure Boot Chain
- Data Execution Prevention
- Address Space Layout Randomization
- Sandbox
- Code Signing Enforcement
- Runtime Process Security



Smart Homes & IoT Security

		$\mathcal{O}_{\mathcal{V}}$		\bigcirc	₽ĵo	G		$\mathbf{\hat{\mathbf{x}}}$
Chip	OS& Service	Hardware Root of Trust	Defense in Depth	Small TCB	Dynamic Compartments	Certificate-based Auth.	Failure Reporting	Renewable Security
MT3620	Azure Sphere		· *	·	··· *	·····		····
Espressif ESP32	RTOS & ?			E Cost	1			
Marvell 88MW300/2	RTOS & ?	() 				.		
Qualcomm QCA4010	RTOS & ?	F		Final 2023	1000 COS			.
Broadcom BCM43907	RTOS & ?			المعادمة الم	المعالم			
TI CC3220x	RTOS & ?	F	111	i t		iii: * *		

🗰 📭 🖙 Full, Partial, or No Silicon support 👘 🏶 📽 📽 = Full, Partial, or No OS support 🛛 🛋 🖒 🗁 = Full, Partial, or No Cloud Security Service support



Trust Cyber-physical Systems



Al Trustworthiness



AI Trustworthiness

- People will not be willing to engage and trust **AI systems** without:
 - Accuracy & Performance
 Privacy Ethics Ownership
 - Data & Model Validation
 - ML Fairness
 - Adversarial Machine Learning
 - Explainable AI
 - Digital Forensics



Some Examples

ranslate		Turn off instant	t translation	
rortuguese English French Detect language 👻	+	English Portuguese Turkish 🕶 Translate		
She's a professor. He's a babysitter	×	O bir profesör. O bir bebek bakı	ICISI	Hotel A get
i) 📰 *	36/5000	☆ □ •) ≺	🖋 Suggest an edit	with a r
Translate		Turn off instar	nt translation	Hotel B get
Portuguese English Turkish Detect language	*	English Portuguese Turkish 🕶 Translate		with a r
O bir profesör. O bir bebek bakıcıs	SI ×	He's a professor. She's a baby	sitter	
		- 5 0 4		
¶ ∎ *	36/5000	X U 4) %	// Suggest an edit	

Hotel A gets average 3.2

with a mix of mostly 3 and 4

Hotel B gets average 3.2

with a mix of mostly 1 and 5



Adversarial Machine Learning

 Adversarial examples are malicious inputs designed to <u>fool</u> Machine Learning models







Security & Trust in CPS



Holistic Security & Trust







Hardware Security



AI/ML Trustworthiness



Data Pipeline Security



Currently

- An AI Updatable Hardware-based IDS
- Chain of Trust in Data Pipelines for Digital Investigation
 - -Quantum-resistant Encryption Scheme (PKI) for CPS
- Al Trustworthiness
 - -Bias evaluation
 - -Adversarial attacks
 - -Transfer Learning



An Al Updatable Hardware-based IDS

- Simulated Buffer Overflow (Arm)
- Canary Detection (FPGA)



- Currently:
 - IoT Malware detection system
 - Transfer Learning
 - Side-Channels



Quantum-resistant Encryption Scheme for PKI

- A hardware/software implementation of a quantum resistant encryption algorithm
 - 3DES
 - -AES
- A hardware/software implementation of a Blockchain in zero trust - SHA, Elliptic Curve





AES Performance Analysis







Chain of Trust in Data Pipelines for Digital Investigation



SECURE

Certificate

Chain of Trust in Data Pipelines for Digital Investigation



AI Trustworthiness

- Transfer & Reinforcement Learning
 - -Bias evaluation
 - Adversarial attacks
- Models based on:
 - -Random Forest
 - -Neuron Networks



Open Research Directions

• So many 🙄

Multilayer issue
 ✓ Explore hardware and software vulnerabilities
 ✓ Side-channels
 ✓ Updatable and transferable security

- -Trust in AI / DL Learning
- -Holistic Intrusion Detection



Final Remarks

- Trustworthiness, Cybersecurity, Education
 - -Develop processes and tools for the Cyber-physical ecosystem capable to evaluate the trustworthiness of a system
 - Cybersecurity
 - Al

- Cybersecurity & AI Trustworthiness in Education



ThankYou!

Dr. Dimitrios Damopoulos damopoulos@southalabama.edu

