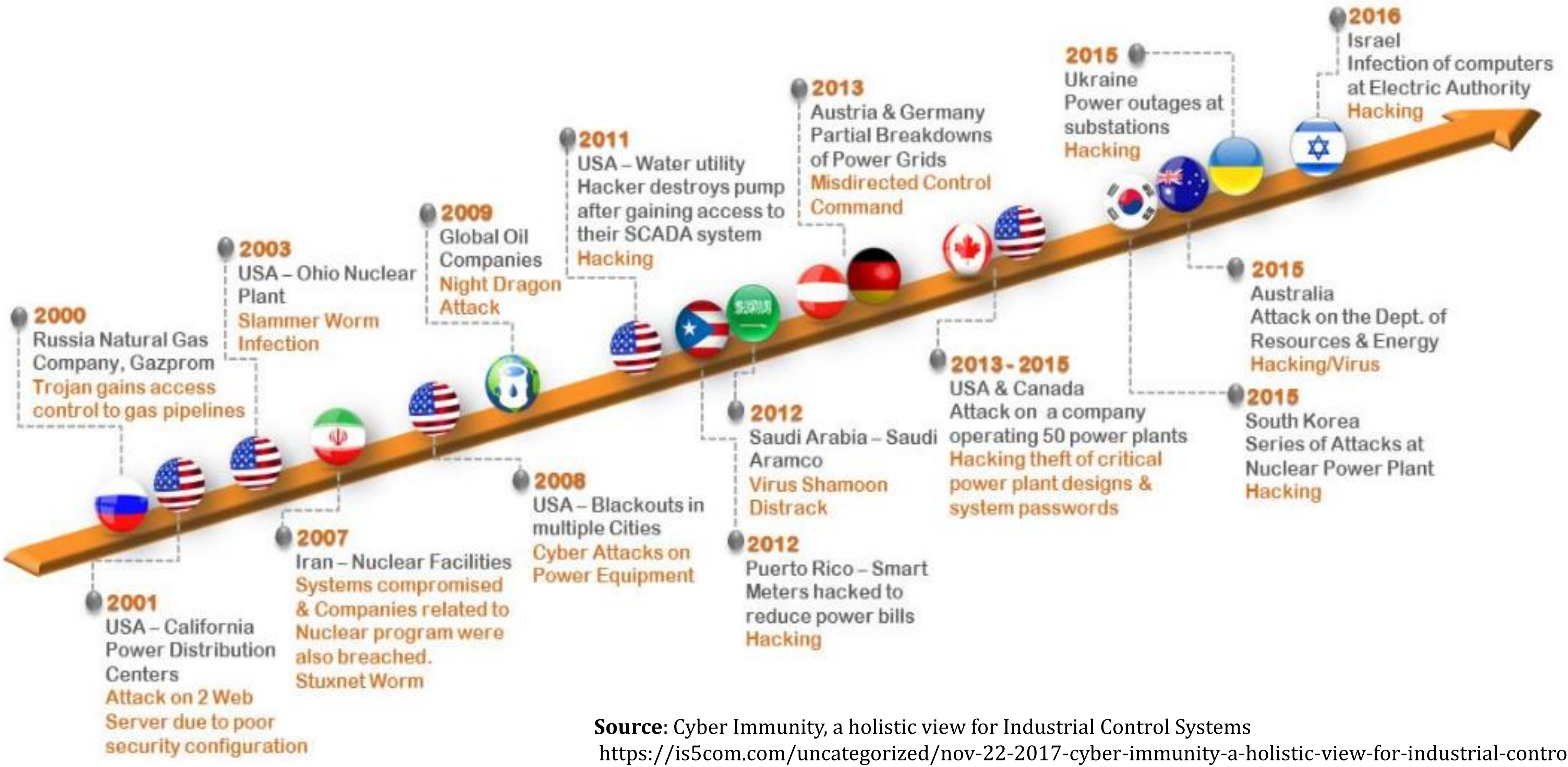
Towards a More Resilient and Secure EPICS

EPICS Collaboration Meeting June 2019
ITER Cadarache, France

SENA HOUNSINOU, PH.D.
EMBEDDED SYSTEMS SECURITY LAB
HOWARD UNIVERSITY

History of Cyber criminal Attacks in ICS



2000
Russia Natural Gas Company, Gazprom
Trojan gains access control to gas pipelines

2001
USA – California Power Distribution Centers
Attack on 2 Web Server due to poor security configuration

2003
USA – Ohio Nuclear Plant
Slammer Worm Infection

2007
Iran – Nuclear Facilities
Systems compromised & Companies related to Nuclear program were also breached.
Stuxnet Worm

2008
USA – Blackouts in multiple Cities
Cyber Attacks on Power Equipment

2009
Global Oil Companies
Night Dragon Attack

2011
USA – Water utility
Hacker destroys pump after gaining access to their SCADA system
Hacking

2012
Saudi Arabia – Saudi Aramco
Virus Shamoon Distrack

2012
Puerto Rico – Smart Meters hacked to reduce power bills
Hacking

2013
Austria & Germany
Partial Breakdowns of Power Grids
Misdirected Control Command

2013 - 2015
USA & Canada
Attack on a company operating 50 power plants
Hacking theft of critical power plant designs & system passwords

2015
South Korea
Series of Attacks at Nuclear Power Plant
Hacking

2015
Australia
Attack on the Dept. of Resources & Energy
Hacking/Virus

2015
Ukraine
Power outages at substations
Hacking

2016
Israel
Infection of computers at Electric Authority
Hacking

Source: Cyber Immunity, a holistic view for Industrial Control Systems
https://is5com.com/uncategorized/nov-22-2017-cyber-immunity-a-holistic-view-for-industrial-control-systems/

Motivation & Goal

How we got here

- Hyper-connectivity
- Threat to major Industrial Control Systems
- Traditional Perimeter System Protection (Gateway, Password auth.)

Our goal

Hardening EPICS software to ensure security of scientific cyberinfrastructure which controls scientific instruments

Expected Outcomes

EPICS

- ✓Adopt security measures early in software development cycle
- ✓Enhance cybersecurity capabilities
- ✓Create a resilient scientific infrastructure for high energy physics research

EPICS Community

- ✓Adoption of security best practices
- ✓Creation of set of security tools
- ✓Discovery and mitigation of potential vulnerabilities

WHAT WE WILL COVER

- Threats considered
- Proposed approach
- Status of our project

Threat Models

T0 – The Unintentional Threat

- Accidental Disruption of Scientific Operations
- Modification of PV Values
- Loss of Integrity of Scientific Experiments

Threat Models

T0 – The Unintentional Threat

T1 – The Malicious Adversaries (untargeted, common)

- Destabilization of IOCs
- Modification of PV values in the IOC database
- Disruption of scientific mission of EPICS site

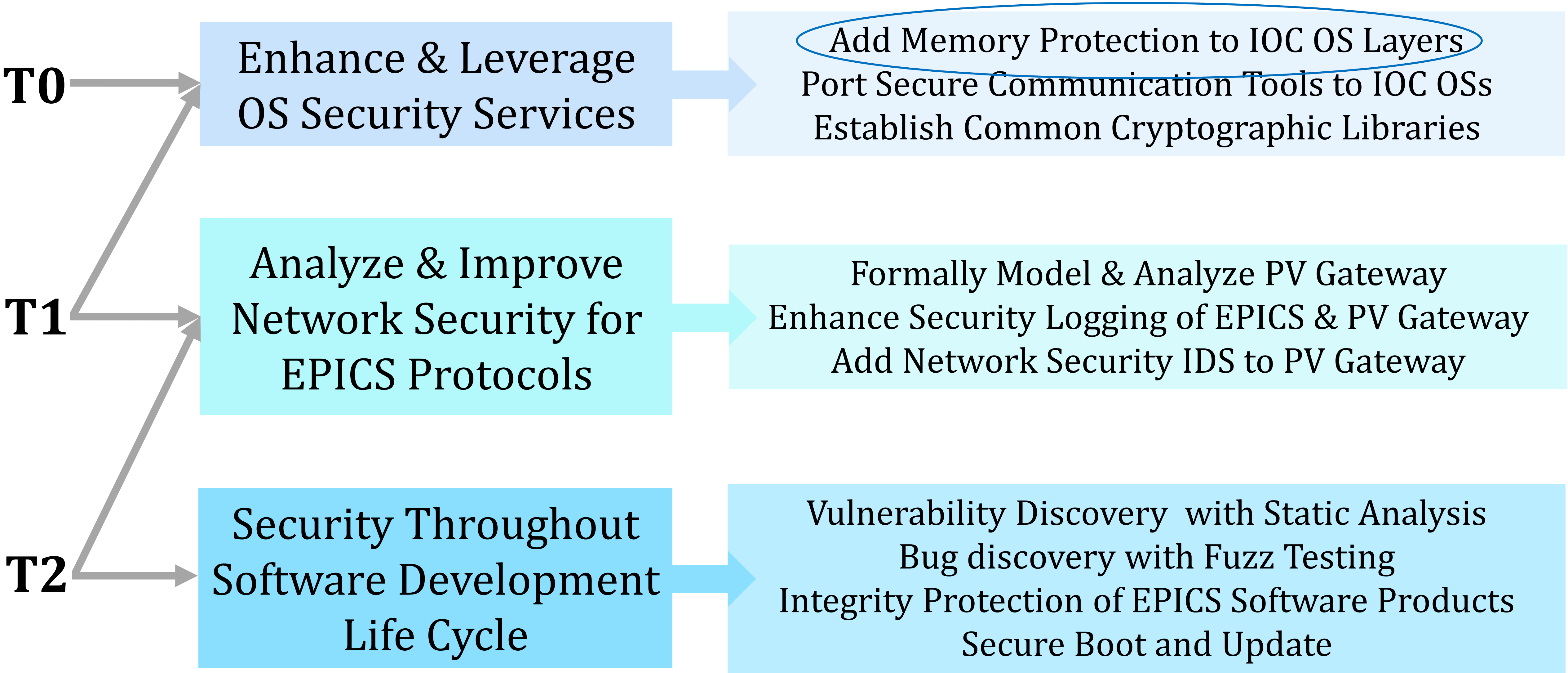
Threat Models

T0 – The Unintentional Threat

T1 – The Malicious Adversaries (untargeted, common)

T2 – The State Actors (targeted attacks, costliest)

- Undermine IOCs
- Cause long-term damage to physical infrastructure
- Inject malicious code in open-source software development supply chain
- Tamper with release software products to instrument malware into downloadable binary images



T0

Enhance & Leverage OS Security Services

- Add Memory Protection to IOC OS Layers
- Port Secure Communication Tools to IOC OSs
- Establish Common Cryptographic Libraries

T1

Analyze & Improve Network Security for EPICS Protocols

- Formally Model & Analyze PV Gateway
- Enhance Security Logging of EPICS & PV Gateway
- Add Network Security IDS to PV Gateway

T2

Security Throughout Software Development Life Cycle

- Vulnerability Discovery with Static Analysis
- Bug discovery with Fuzz Testing
- Integrity Protection of EPICS Software Products
- Secure Boot and Update

Project Status: Memory Protection

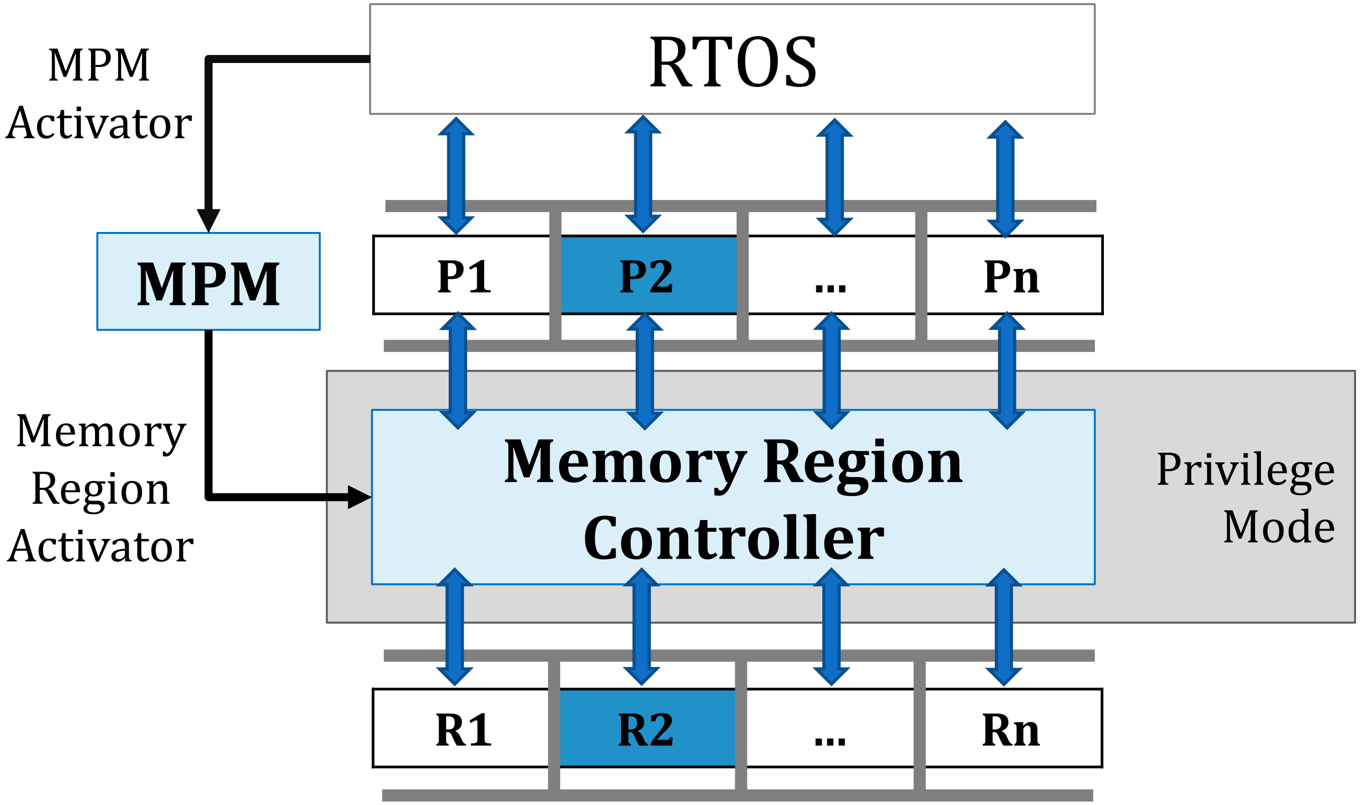
Current Memory Protection in EPICS

- Memory management in GPOSs
- Available protection for VxWorks
- Non-existent in RTEMS

Desired Features

- Flexible (can be used with different OSs)
- Optional (for OSs with memory management unit)
- Low overhead
- Low performance degradation

Memory Protection Module (MPM) Design



Our Team

Prajjwal Dangal | Uchenna Ezeobi | Abiola Ogundeko

Sena Hounsinou (sena.hounsinou@howard.edu)

Embedded Systems Security Lab

Howard University

Gedare Bloom, Ph.D.

University Of Colorado at Colorado Springs