Towards Resilient Cyber-Physical Control Systems

Gabriel Salles-Loustau, Saman A. Zonouz
Rutgers University – ECE department – 4N6 Research Group

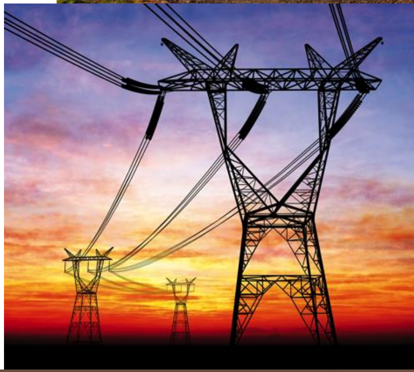
Global SIP – 15 Dec. 2015

Cyber-Physical Critical Infrastructures

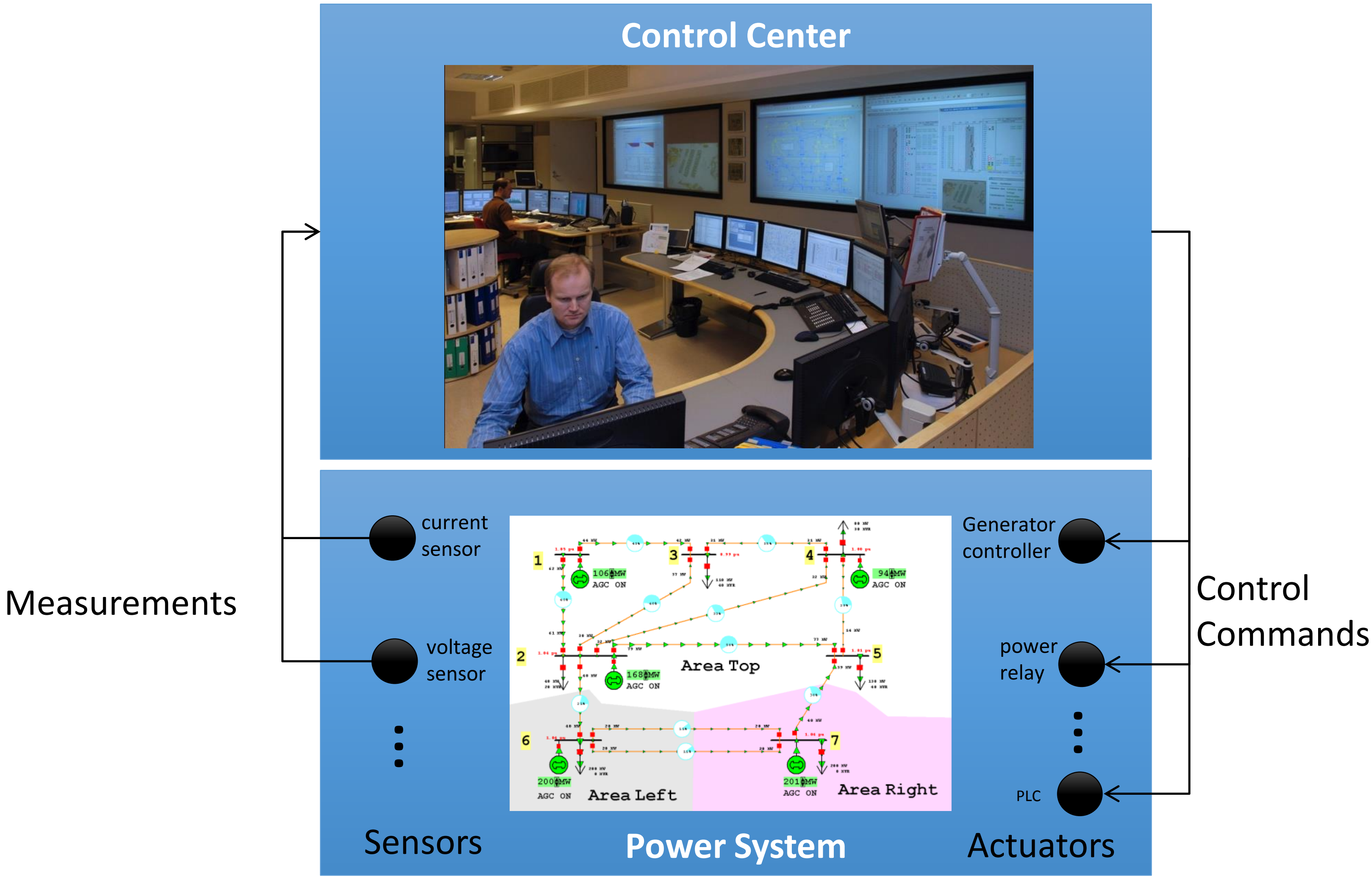
- Infrastructures of
  - *Collaborating computational elements monitoring/controlling physical entities*
  - *Essential for the functionality of the society and economy*

- Examples
  - *Electricity grid, water supply, gas/oil production, transportation systems, healthcare, automotive, safety-critical aerospace, etc.*

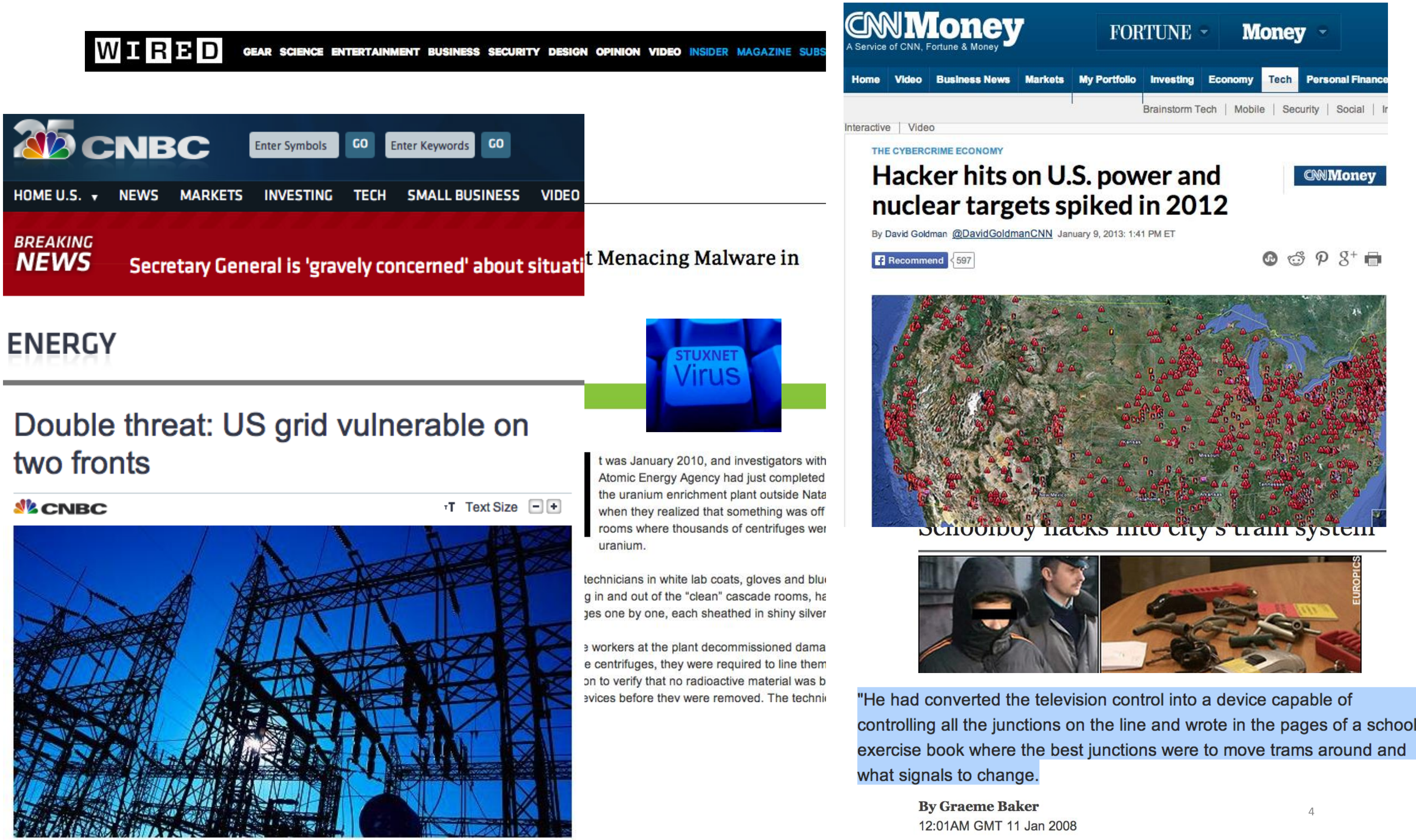





Example: Power-grid Infrastructure



Growing Critical Infrastructure Attacks



WIRED GEAR SCIENCE ENTERTAINMENT BUSINESS SECURITY DESIGN OPINION VIDEO INSIDER MAGAZINE SUBS

t Menacing Malware in

t was January 2010, and investigators with
Atomic Energy Agency had just completed
the uranium enrichment plant outside Nata
when they realized that something was off
rooms where thousands of centrifuges wer
uranium.

technicians in white lab coats, gloves and blu
g in and out of the "clean" cascade rooms, ha
jes one by one, each sheathed in shiny silver

workers at the plant decommissioned dama
e centrifuges, they were required to line them
on to verify that no radioactive material was b
evices before they were removed. The techni

CNBC Enter Symbols GO Enter Keywords GO
HOME U.S. NEWS MARKETS INVESTING TECH SMALL BUSINESS VIDEO
BREAKING NEWS Secretary General is 'gravely concerned' about situati

ENERGY

Double threat: US grid vulnerable on two fronts

CNBC Text Size

CNNMoney A Service of CNN, Fortune & Money FORTUNE Money
Home Video Business News Markets My Portfolio Investing Economy Tech Personal Finance
Brainstorm Tech | Mobile | Security | Social | Interactive | Video

THE CYBERCRIME ECONOMY

Hacker hits on U.S. power and nuclear targets spiked in 2012

By David Goldman @DavidGoldmanCNN January 9, 2013: 1:41 PM ET

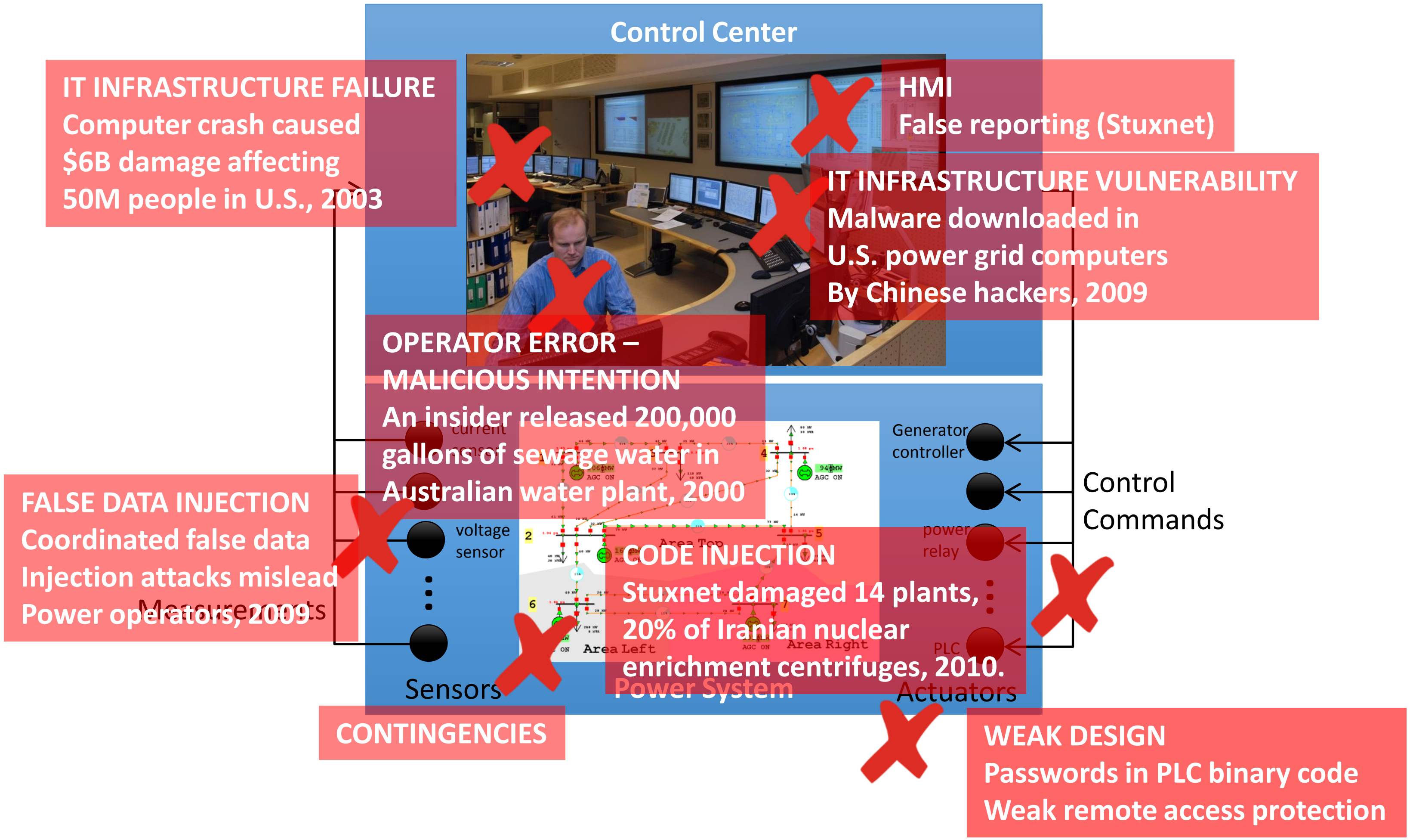
Recommend 597

Schoolboy hacks into city's tram system

"He had converted the television control into a device capable of controlling all the junctions on the line and wrote in the pages of a school exercise book where the best junctions were to move trams around and what signals to change.

By Graeme Baker
12:01AM GMT 11 Jan 2008

Attack Surfaces



CPS Security Solutions

- Trustworthy architectures
  - *Agencies recommendations: NIST, NERC*
  - *Code verification: Trusted Safety Verifier*
- Online security assessment
  - *Contingencies assessment for security or safety, for cyber of physical system, multiple contingencies*
  - *Contingencies response depending on threat levels*
- Cyber-Physical Attack Detection
  - *Specific to cyber or physical infrastructure*
  - *Leverage sensors*
  - *Few solutions focus on both aspects*
- Proactive Cyber-Physical Intrusion Tolerance
  - *Intrusion tolerance and automated response*
  - *Attack-graph templates*

Adapting the Security Model

- IT security models are well studied
  - Wide range of security models
  - Wide range of tools

- IT security models generally do not fit CPS
  - *<u>Cost</u>: might not be possible in some scenarios (availability, real-time)*
  - *<u>Precision</u>: might not suit well physical threads (rogue commands)*

Cyber System’s Input-Based Detection Mechanism

- Tight dependency between the control center and the physical system
- Events on physical system corresponds to inputs given to the control center
  - *Operator input, configuration file change, PLC code change, etc*

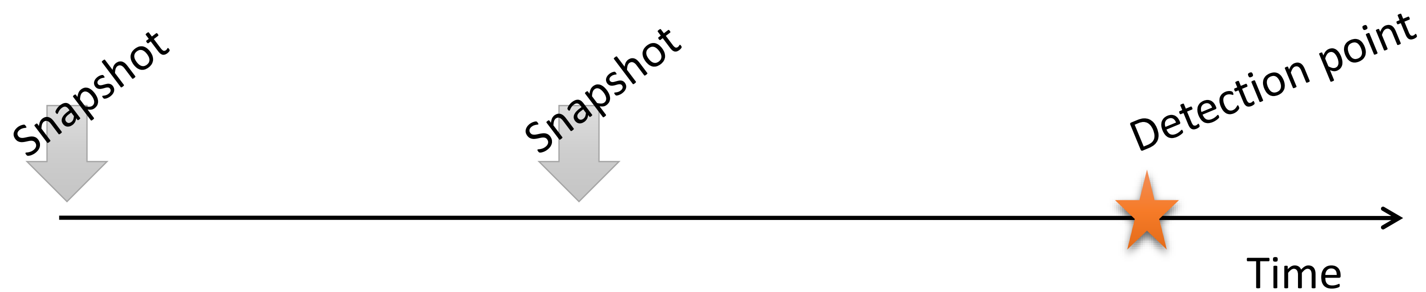
Cost: <u>deploy cost-optimal IT security sensors</u>

- Physical system model: architecture + specifications
- Validate safety features
- Analyze inputs as a vector for safety violation

Precision: <u>Identify inputs that violate safety requirement of the physical entities</u>

How it works

- Assumption
  - *Periodic snapshots*
  - *System input logs*
  - *Safety verifier (TSV) acts as an IDS*

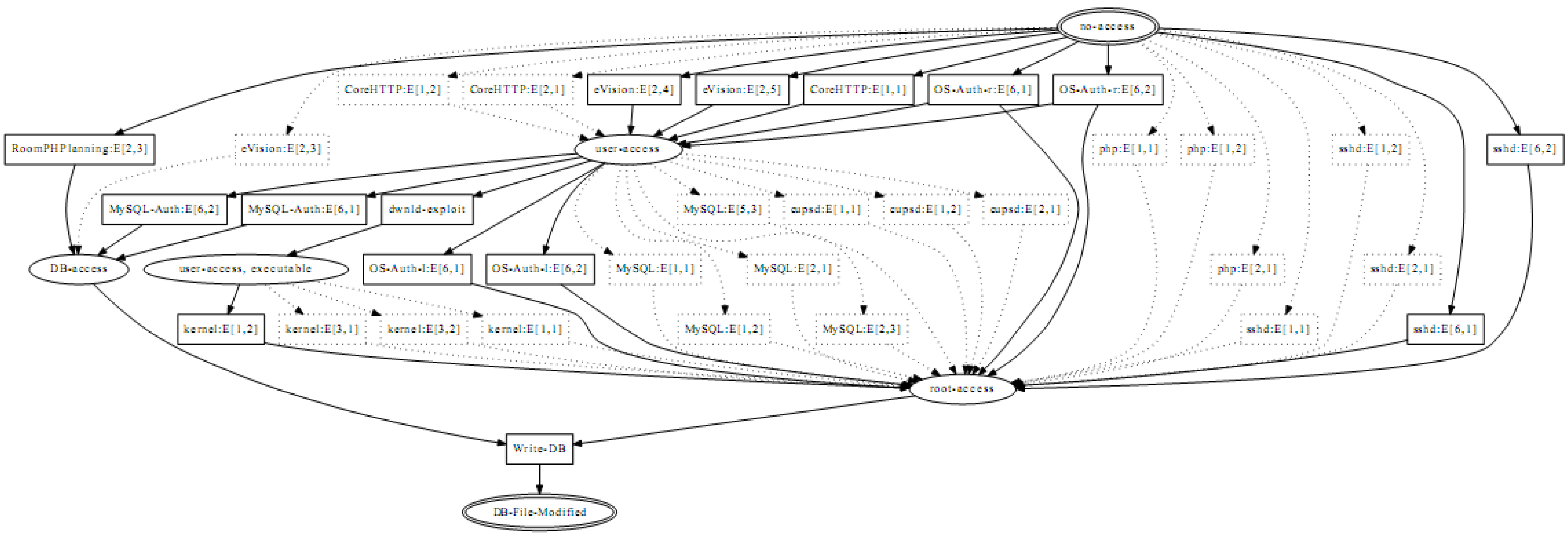


Attack-Graph Templates

- Essentially, a **privilege escalation graph (i.e., DAG)**
  - *States are subset of privileges held by the attacker*
  - *State transitions are privilege escalations*
    - Accomplished via a *vulnerability exploitation*

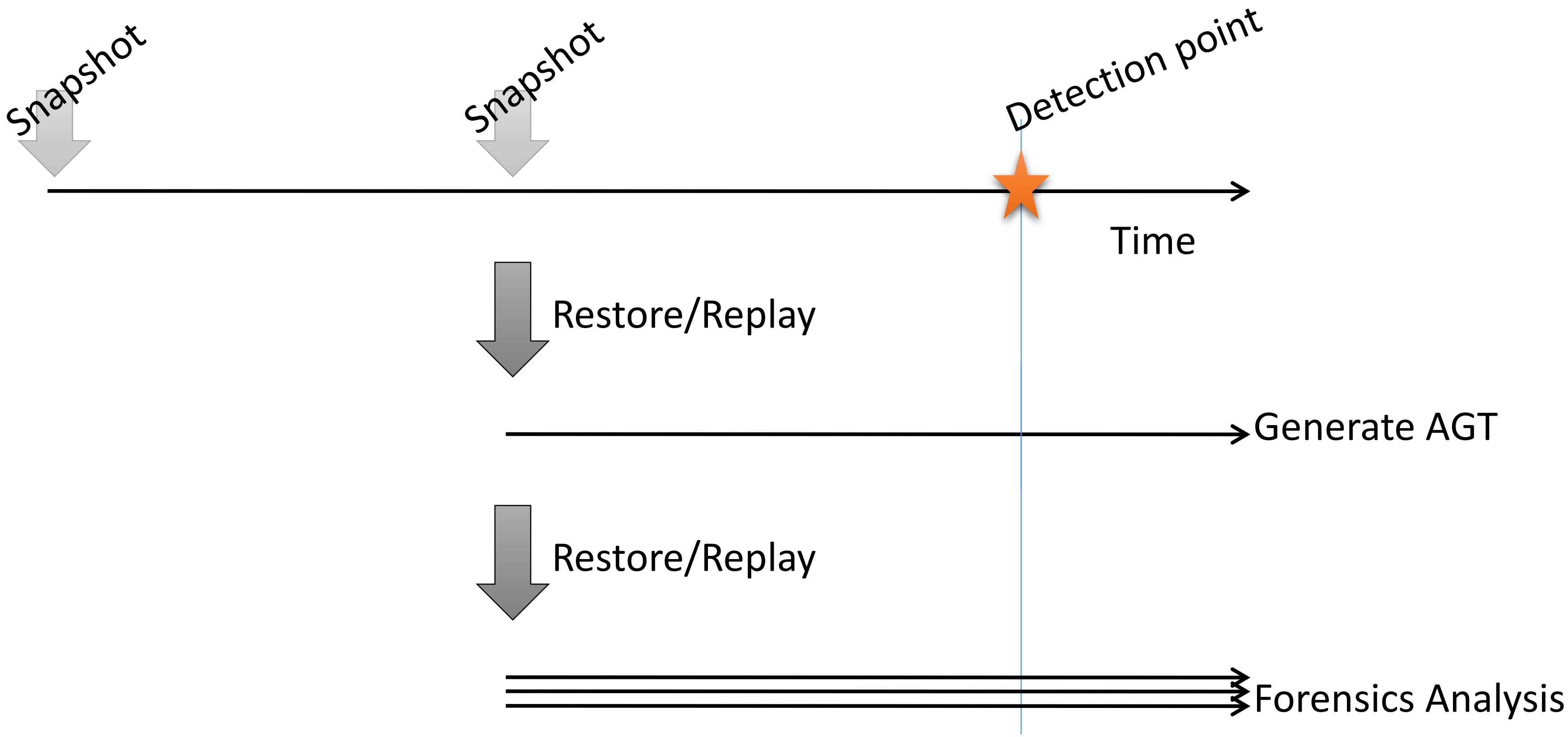
- AGT includes all possible (known and potentially-unknown) attack paths in the system
  - *From the initial state, i.e., no-access*
  - *To the state with required privileges to cause an attack consequence, i.e., detection point*

A Sample AGT

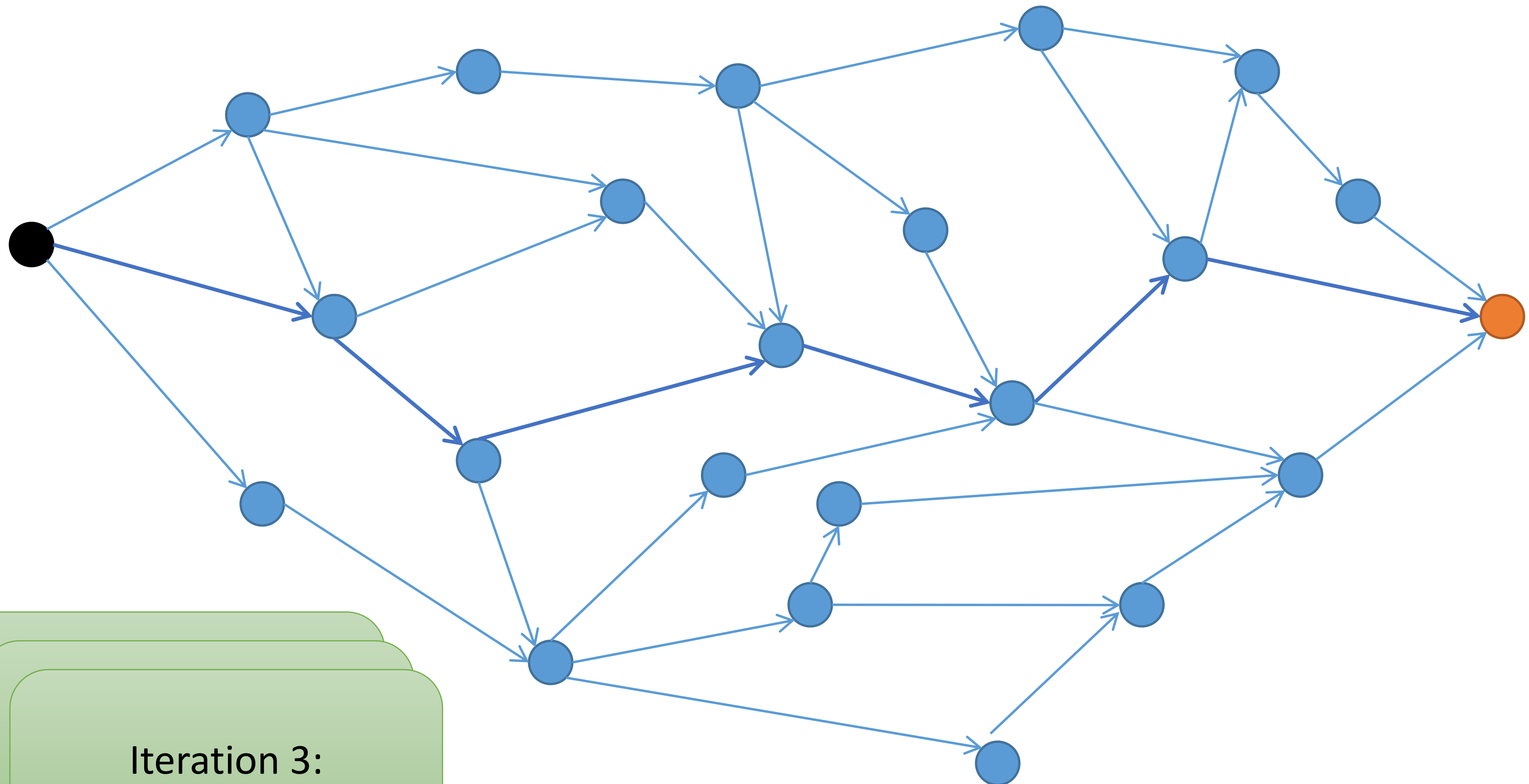


no-access
CoreHTTP:E[1,2]
CoreHTTP:E[2,1]
eVision:E[2,4]
eVision:E[2,5]
CoreHTTP:E[1,1]
OS-Auth-r:E[6,1]
OS-Auth-r:E[6,2]
RoomPHPlanning:E[2,3]
eVision:E[2,3]
user-access
php:E[1,1]
php:E[1,2]
sshd:E[1,2]
sshd:E[6,2]
MySQL-Auth:E[6,2]
MySQL-Auth:E[6,1]
dwnld-exploit
MySQL:E[5,3]
cupsd:E[1,1]
cupsd:E[1,2]
cupsd:E[2,1]
DB-access
user-access, executable
OS-Auth-l:E[6,1]
OS-Auth-l:E[6,2]
MySQL:E[1,1]
MySQL:E[2,1]
php:E[2,1]
sshd:E[2,1]
kernel:E[1,2]
kernel:E[3,1]
kernel:E[3,2]
kernel:E[1,1]
MySQL:E[1,2]
MySQL:E[2,3]
sshd:E[1,1]
sshd:E[6,1]
root-access
Write-DB
DB-File-Modified

How it works


Snapshot
Snapshot
Detection point
Time
Restore/Replay
Generate AGT
Restore/Replay
Forensics Analysis

Intrusion Forensics: Example



Iteration 3:
IDS_3

Detection-Capability Matrix: System-sensors Tools Cost Comparison

Detection Policy	**Symbol: Mechanism**	**Cost**	**Detector**
Information flow analysis	Tnt: Taint tracking	Very High	TEMU
Input investigation	FW: Feature-based packet monitoring	Very Low	Firewalls
	Snrt: Content-based packet monitoring (stateless)	Medium	`Snort`
	App: Application-based IDS (stateful)	Medium	`Secerno`
Execution monitoring	ClSt: Control Violation: call stack monitoring	High	callstack monitoring
	CtFl: Control Violation: control flow integrity monitoring	High	Control-Flow Integrity
	DtFl: Data Violation: data flow monitoring	Very High	`MemCheck`
Consequence detection	AV: Malicious code: executable integrity checking	Low	`ClamAV`
	Hst: Host-based detection systems	Low	`Samhain`
	Stat: Statistical anomaly-based	Low	`Zabbix`

Detection-Capability matrix of system detection tools

	Buff	DngPtr	FmtStr	ShlMC	SQLIn	CodIn	DirTrv	CSS	HttpHdr	HttpRsp	TcTu	SymRc	CSFor	ClkJk	FTPBnc	WrmFtg	BlmVic	Race	PwdDic	Encrypt
Tnt	H	M	H	M	C	L	H	C	M	M	L	L	H	H	H	N	N	N	N	N
FW	L	N	L	N	N	L	N	N	L	L	N	N	L	L	L	N	N	N	M	M
Snrt	M	N	M	M	M	M	M	N	M	M	N	N	N	N	M	N	N	N	H	H
App	H	L	H	H	H	H	H	L	C	C	N	N	N	N	H	N	N	N	H	H
ClSt	C	M	H	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
CtFl	C	H	H	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
DtFl	L	L	L	M	C	L	H	C	M	M	L	L	H	H	H	N	N	N	N	N
AV	N	N	N	N	N	M	N	N	N	N	H	H	N	N	N	L	L	L	N	N
Hst	L	L	L	N	N	H	N	N	N	N	H	H	N	N	H	M	M	L	N	N
Stat	M	M	L	N	N	L	N	N	N	N	N	N	N	N	H	N	N	N	H	H

Incident Response

- Based on the attack vector detected
  - *Roll-back to the previous healthy state of the system*
  - *Deploy specific lightweight IPS tools*
  - *Etc*

Conclusion

- Various threads are specific to cyber-physical system
- Security measures need to be adapted to the thread
  - *For CPS, **safety** is a key feature*
- Leverage the *dependence between physical and IT infrastructure*
  - ***Detection function as a safety check***
  - *Leverage **performance of the IT system security tool***
  - *Low-cost root analysis and incident response via **Detection-Capability matrices***

Questions?