An Indirect Attack on Computing Infrastructure through Targeted Alteration on Environmental Control

Keywhan Chung

P.I.s: Professor Zbigniew Kalbarczyk, Professor Ravishankar Iyer

Collaborators: Dr. Valerio Formicola, NCSA, Facilities and Services

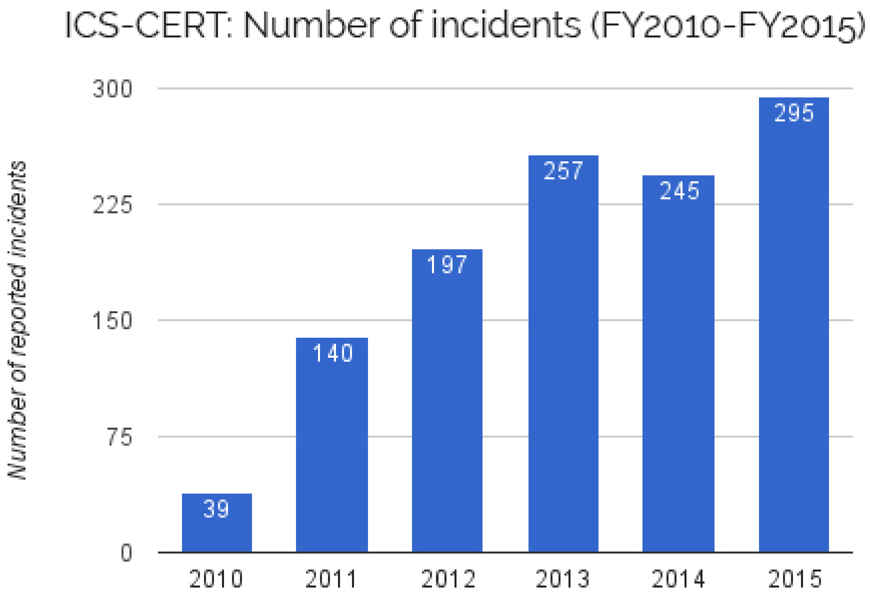
Sep. 28, 2016

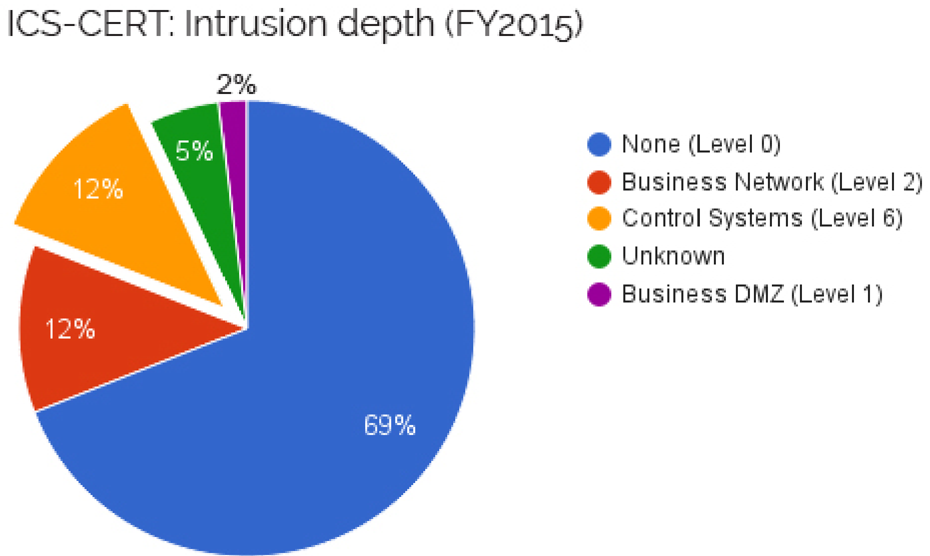
Keywhan Chung, Valerio Formicola, Alexander Withers, Adam Slagell, Zbigniew Kalbarczyk, Ravishankar Iyer, "Attacking Supercomputers Through Targeted Alteration of Environmental Control: A Data Driven Case Study," The International Workshop on Cyber-Physical Systems Security, IEEE CNS'16

Cyber Physical Systems Under Attack

- Security becoming critical
- No different for Cyber Physical Systems
- Increased number of (**reported**) incidents

- Though majority are trivial (Level0), significant portion of attackers **reach control system level** (12%, 2015)





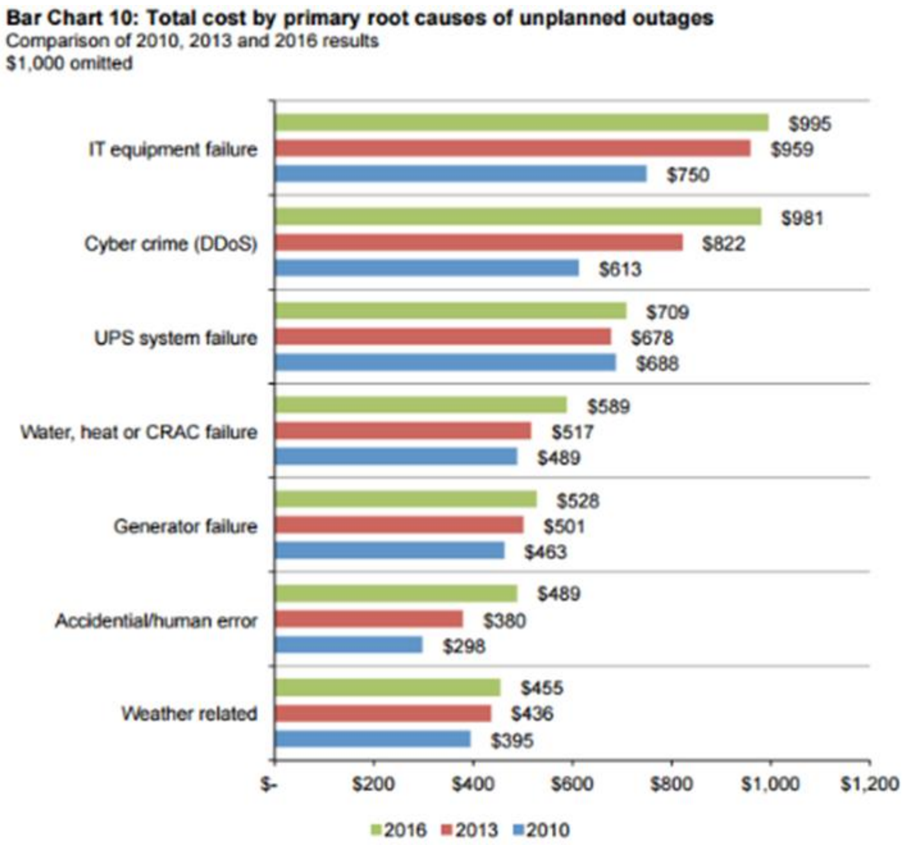
What to do with CLOUDs?

Dependency of Computer Infrastructure on CPSes

- Control on the surrounding CPSes critical for keeping the infrastructure (data center) up and running
- **Significant outage cost** related to surrounding CPSes

Cause in CPS	Cost (%)	Cause in SYS	Cost (%)
Power	26%	Equipment Failure	21%
Water/Heat/AC	12%	Cyber Attack	21%

An attack on CPS can bring down the computing infrastructure (data center)

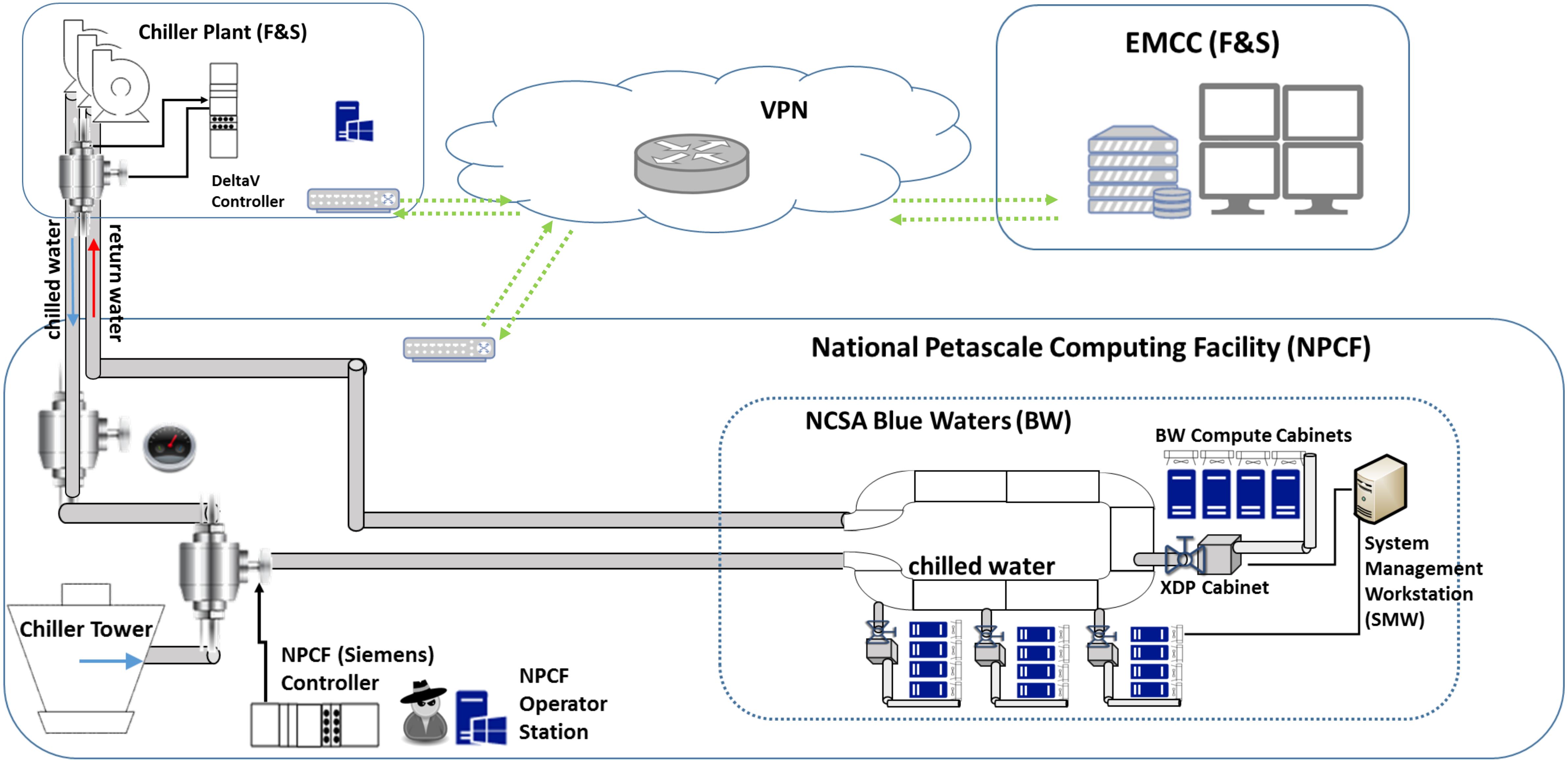


Cost of Data Center Outages, Ponemon Institute Research Report
sponsored by Emerson Network Power

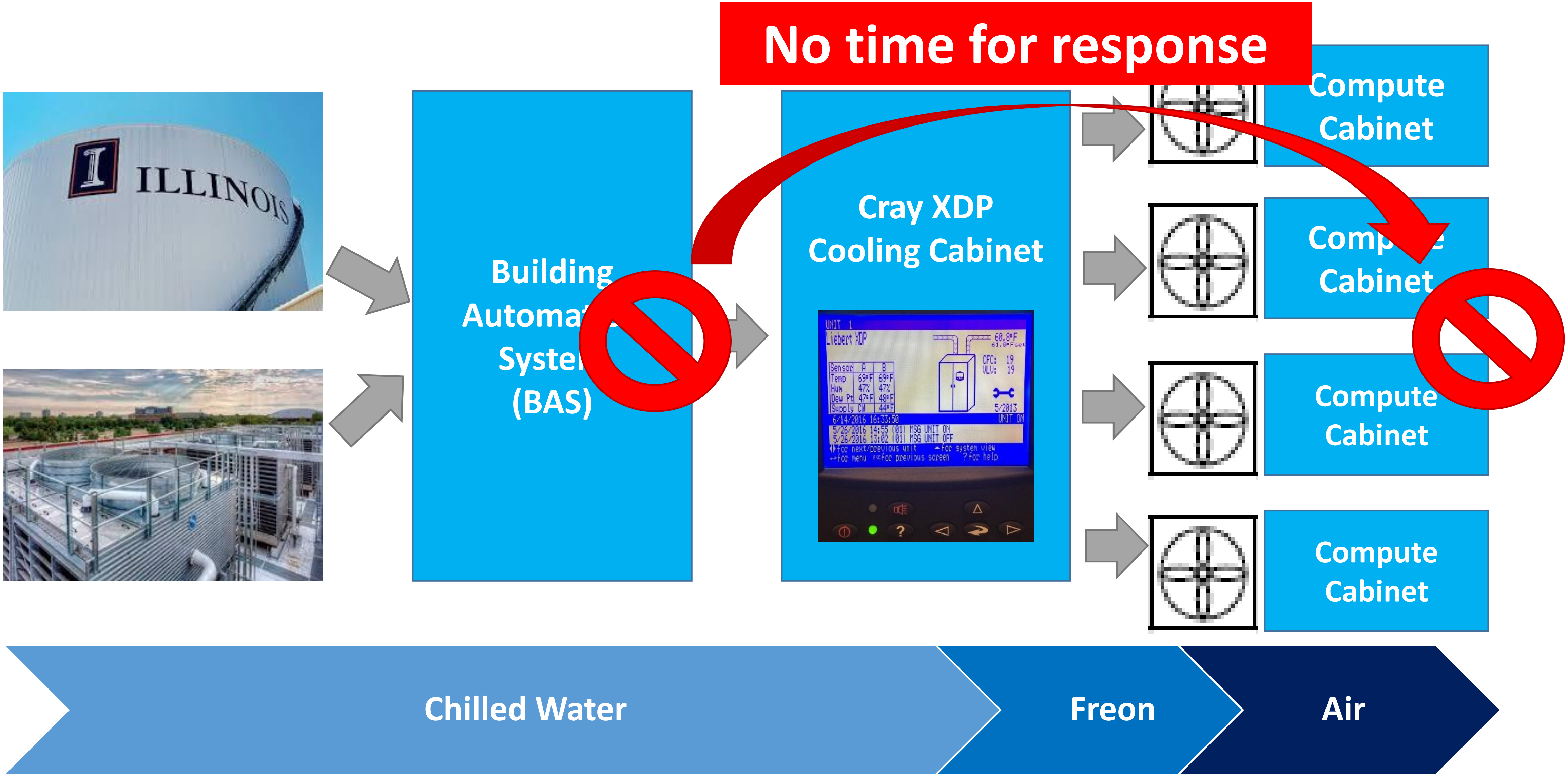
Proposed Attack Model

- An **indirect attack** on the Computing Infrastructure through alteration of the **CPS**
  - Often, Computing Infrastructure itself is well-hardened
    - e.g., Blue Waters: No successful Cyber Attack within 4yrs of operation
  - Relatively weak security of CPSes despite high dependency
    - e.g., 2-factor authentication for remote access to BW
  - Bypass the monitoring system of the computing infrastructure
- A **hard to detect attack** by minimizing the trace of the attack
  - Study the operation of failures and emulate/trigger the failure scenarios
  - Likely to be underestimated as an accidental failure in the physical system

Blue Waters Cooling System



Blue Waters Cooling System



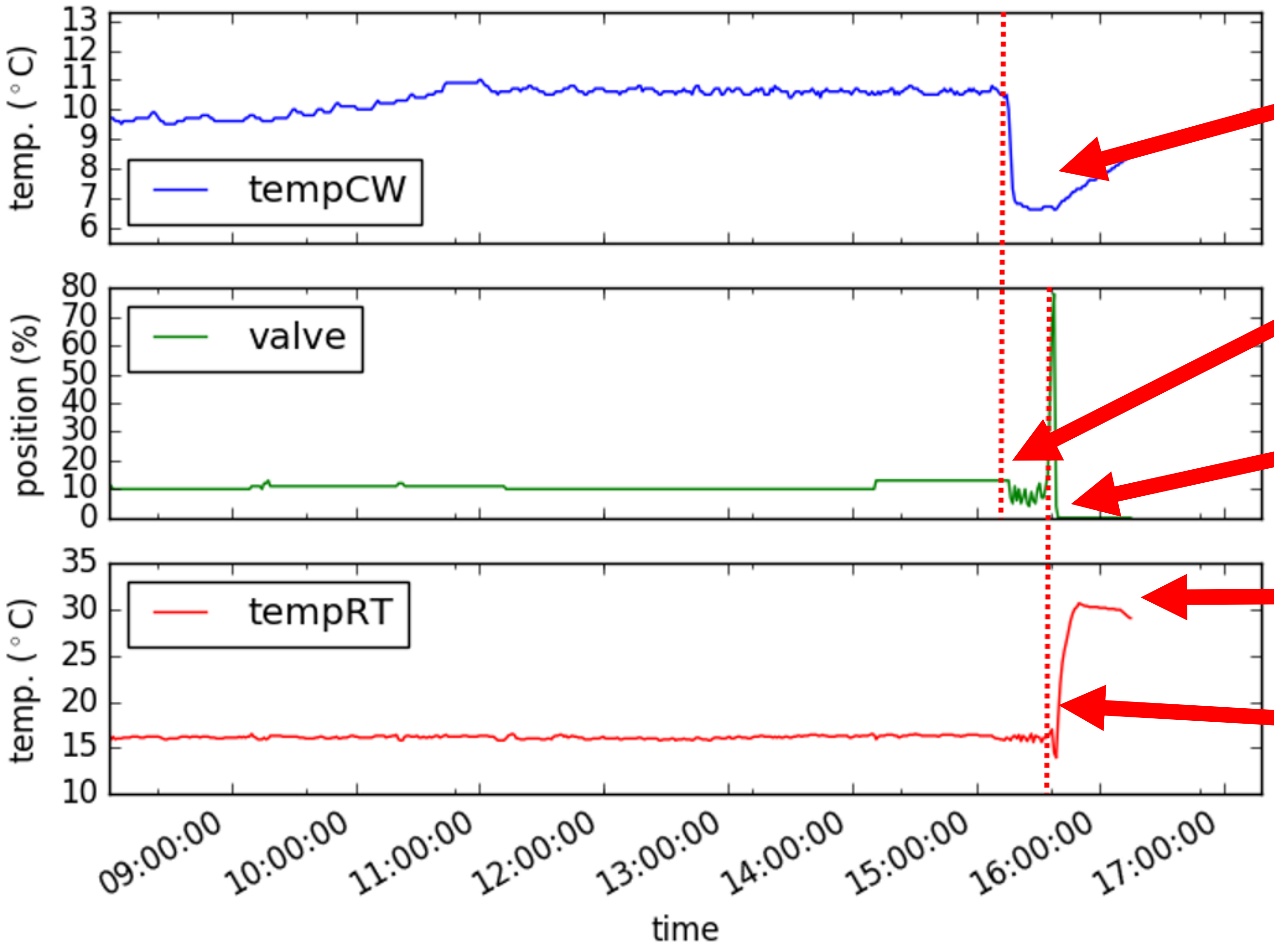
Study on Blue Waters Failures

- **Data**: Failure/Incident Report: Jul. 2013 ~ May 2016, XDP logs
  - Total of **5K** incidents due to H/W, S/W, etc. failure
  - 2.73% (148 out of 5,419) of total incidents account for cooling system related failures:
    - XDP cooling cabinet (valve, pump, gasket, temp. sensor failure)
    - Issues related to the building/campus utility supply
    - Fan shutoff of XE computing cabinets

	2013	2014	2015	2016	%
XDP: Valve	0	13	7	19	*53.42*
XDP: Gasket	0	17	10	2	*39.73*
XDP: Pump Ctrl	0	0	0	1	*1.37*
XDP: Temp. Sensor	0	0	2	0	*1.37*
XE: Fan Shutoff	0	1	0	0	*2.74*
BAS: Facilities	0	0	0	1	*1.37*
Total	0	31	17	23	

What Failure Scenarios can the attacker utilize?

Scenario #1: Loss of Ctrl on Water Valve Actuator



Transition in source of CW cause rapid change in temperature

XDP tries to regulate the cooling capacity by changing valve position

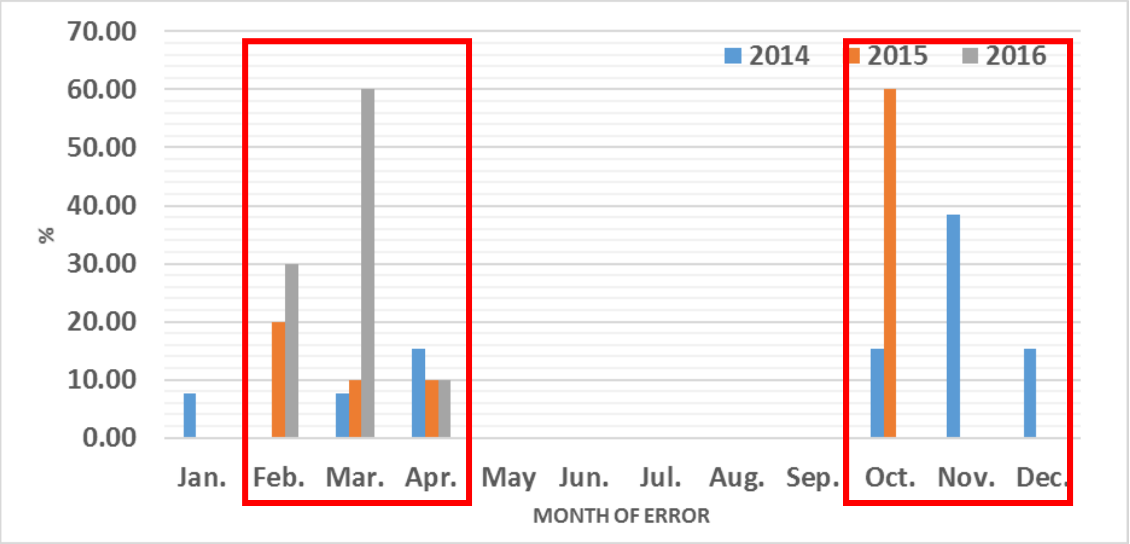
Valve get stuck in CLOSE, XDP looses control

Computing Cabinet temperature exceeding threshold triggers EPO

XDP looses cooling capacity

Scenario #1: Loss of Ctrl on Water Valve Actuator

- XDP valve failure account for ~50% of the failures related to ENV ctrl.
  - Likely fail, especially during certain seasons
  - NPCF transitions between two sources
    - Summer: Campus
    - Winter: Building Cooling Tower
    - **Spring & Fall: ?**



- A frequent change in CW temp. likely to cause a failure in the valve

Scenario #2: Change in Chilled Water Pressure

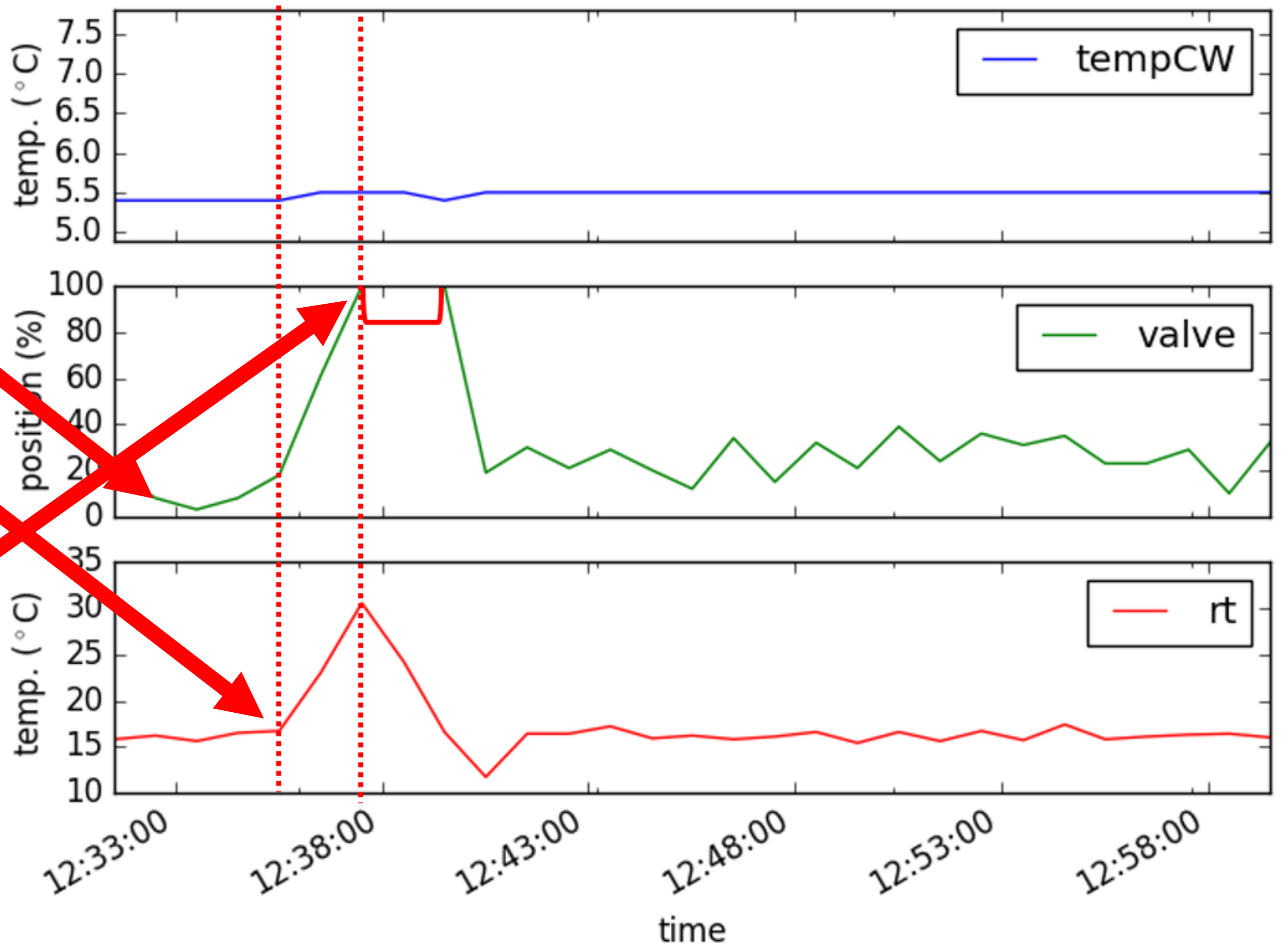
Campus Facilities and Services perform maintenance process cause an increase in CW pressure

BAS and XDP regulates to the change

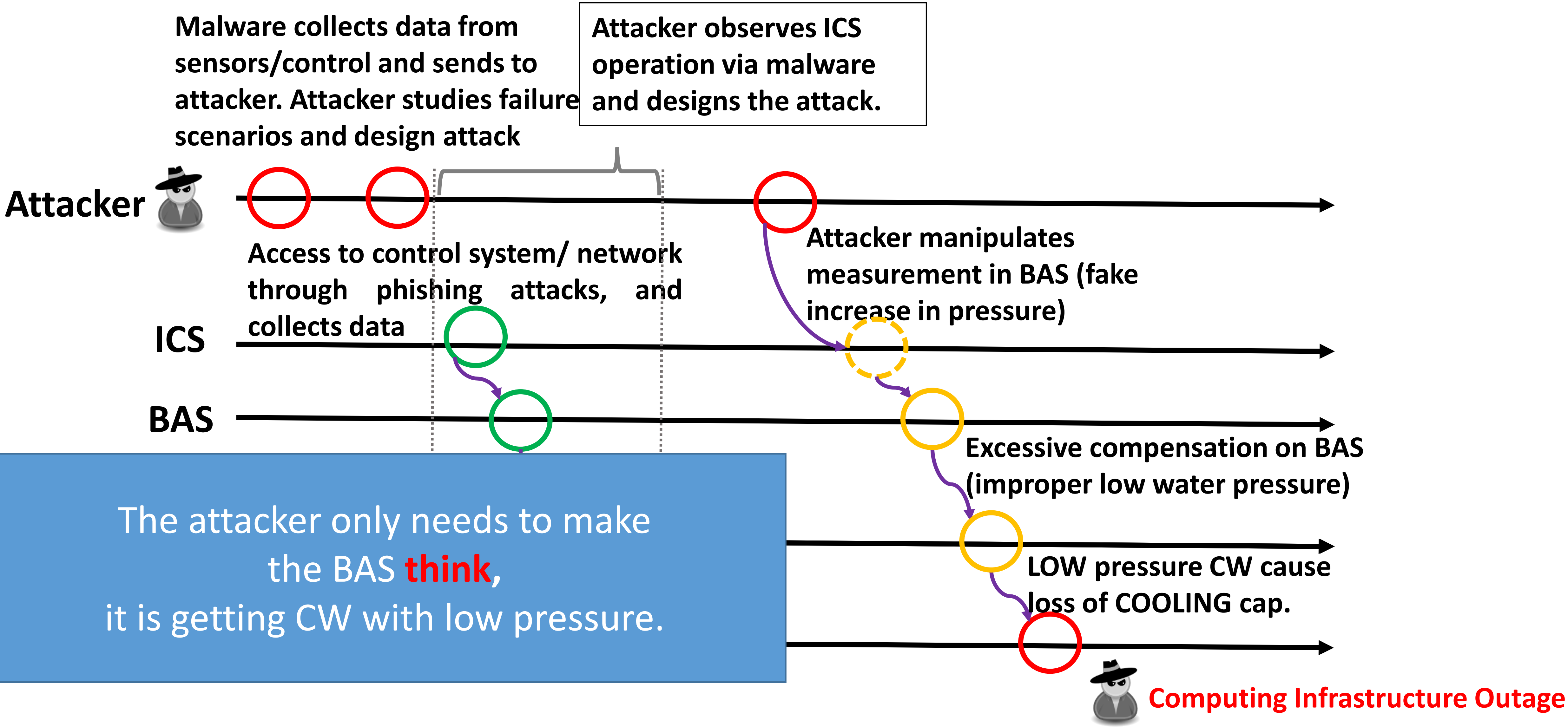
End of maintenance process drops the pressure to normal, but CW pressure reaching XDP lower than requirement (because of the regulation)

XDP tries to compensate loss of Cool. cap. but reaches physical limitation

Computing cabinets with high work load reach temp. limit, and EPO triggered



Attack Scenario utilizing Fail #2

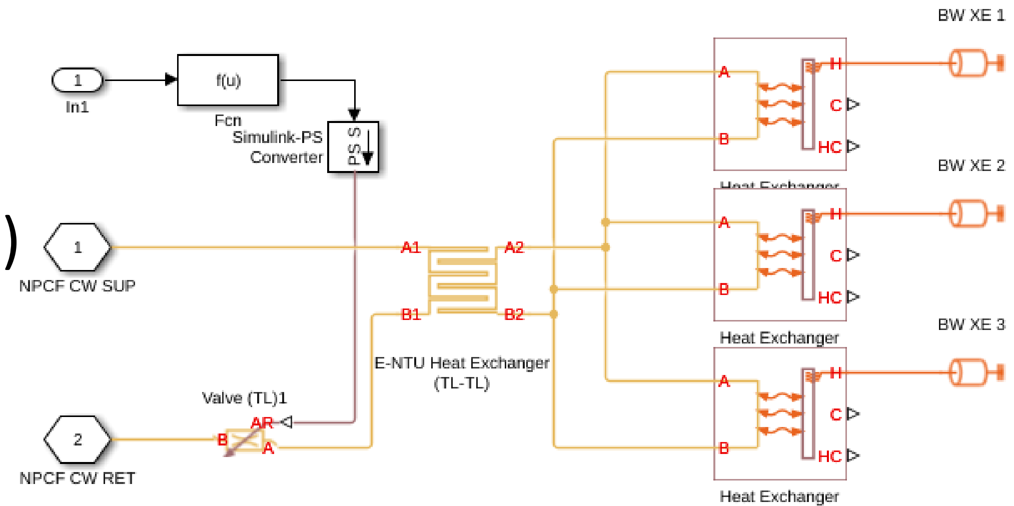


The attacker only needs to make the BAS **think**, it is getting CW with low pressure.

Work in Progress..

- Study on ICS network protocols to exploit vulnerabilities
- Model the ICS and build a **simulator**
  - Study the control system
  - To be tested with BAS operation data/logs
- Implementation of the attack
  - Study the impact of the attacks
  - Possible mitigation within ICS
- Design of detection/mitigation methods
  - Monitoring on different layers (NCSA, BroIDS)
  - Preemptive attack and response (AttackTagger)

<>Date	Time	Point_1	Point_2	Point_3	Point_4	Point_5	Point_6	Point_7	Point_8	Point_9	Point_10
8/31/2016	0:00:00	ON	70.59	OFF	63.8	0	76.5	ON	61.8	ON	65.3
8/31/2016	0:00:00		70.59		63.7	0	76.5		61.5		65.3
8/31/2016	0:10:00		70.52		63.6	0	76.5		61.4		65.34
8/31/2016	0:20:00		70.59		63.5	0	76.5		61.6		65.59
8/31/2016	0:30:00		70.56		63.8	0	76.5		62.8		65.66



Conclusion

- Increased threat on CPSes
- Significant dependency of Computing Infrastructures on CPSes
- **Security of CPS impact security of Computing Infrastructure**
- Attackers can deploy a SMART attack by:
  - Deploying an **indirect attack** through the CPS
  - A careful design of an attack **to simply trigger a failure scenario**
  - w/o enough traces and investigation, can be **treated as a accidental failure**
- **CPS security into consideration**
  towards secure computing infrastructure design