RSAConference2015
Abu Dhabi | 4–5 November | Emirates Palace

SESSION ID: CIN-W08

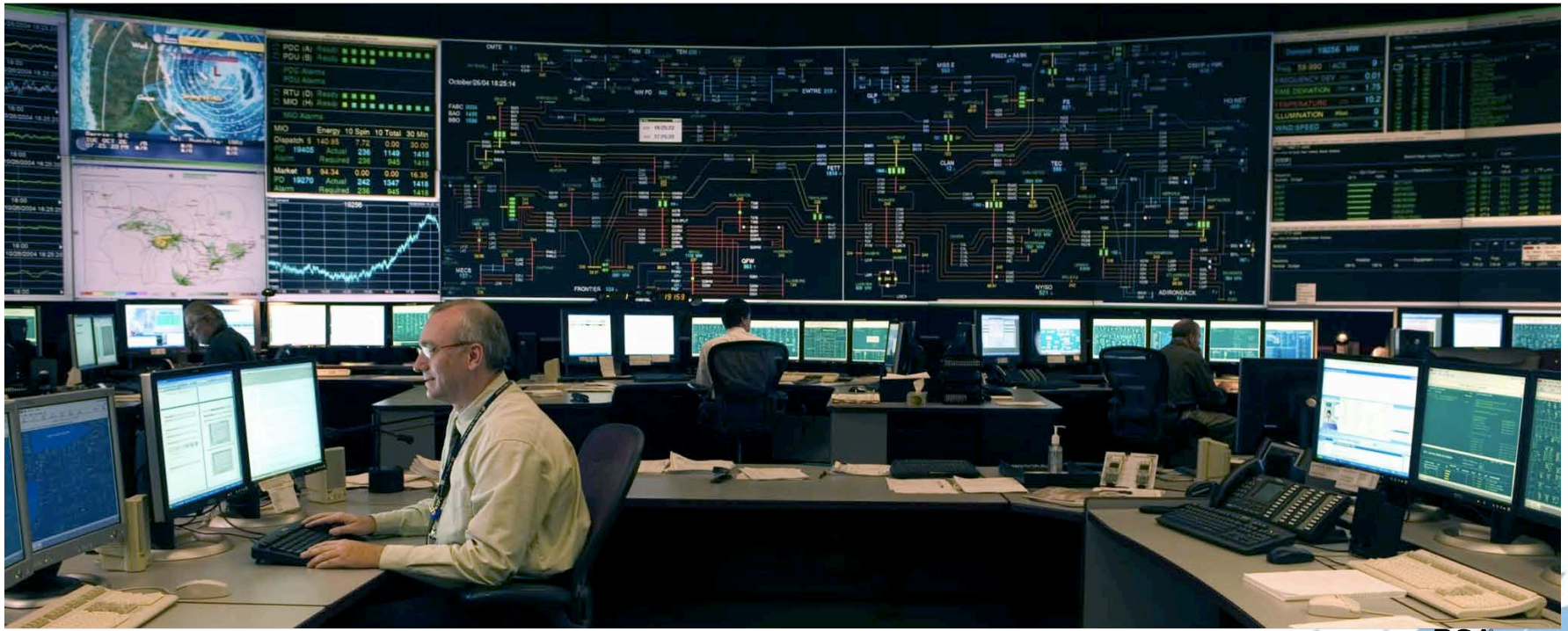
False Data Injection Attacks on Industrial Control Systems

Dimitrios Serpanos[1] and Howard Shrobe[2]

[1]Principal Scientist, Qatar Computing Research Institute – HBKU
[2]Principal Research Scientist, CSAIL, MIT

Industrial Control Systems (ICS)

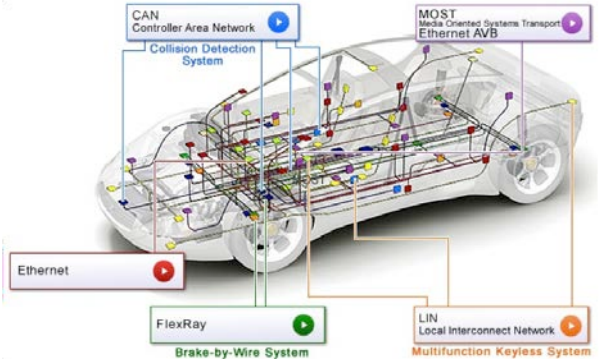
Monitoring Critical Infrastructure

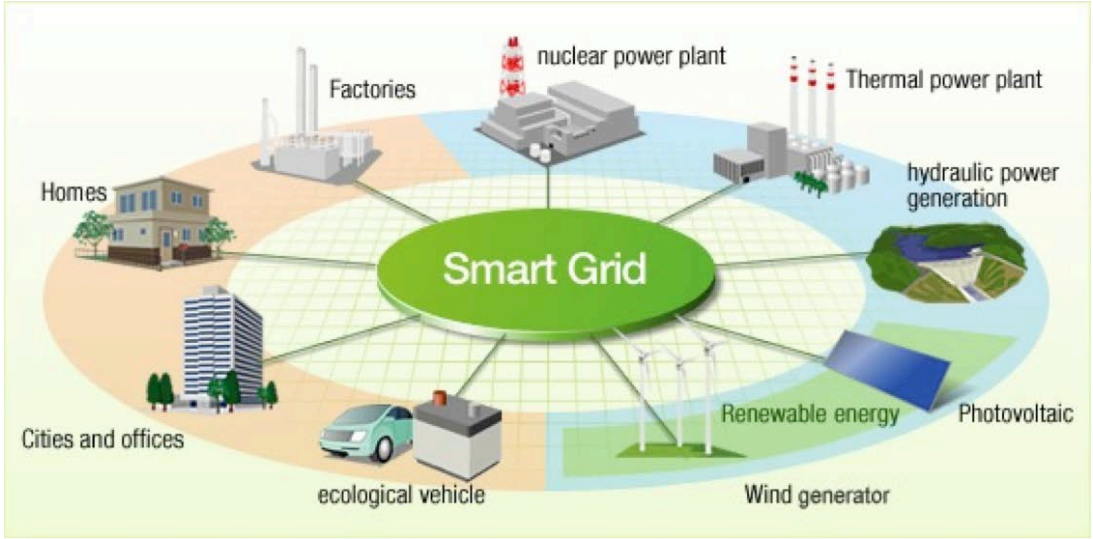


ICS are Cyber-Physical Systems

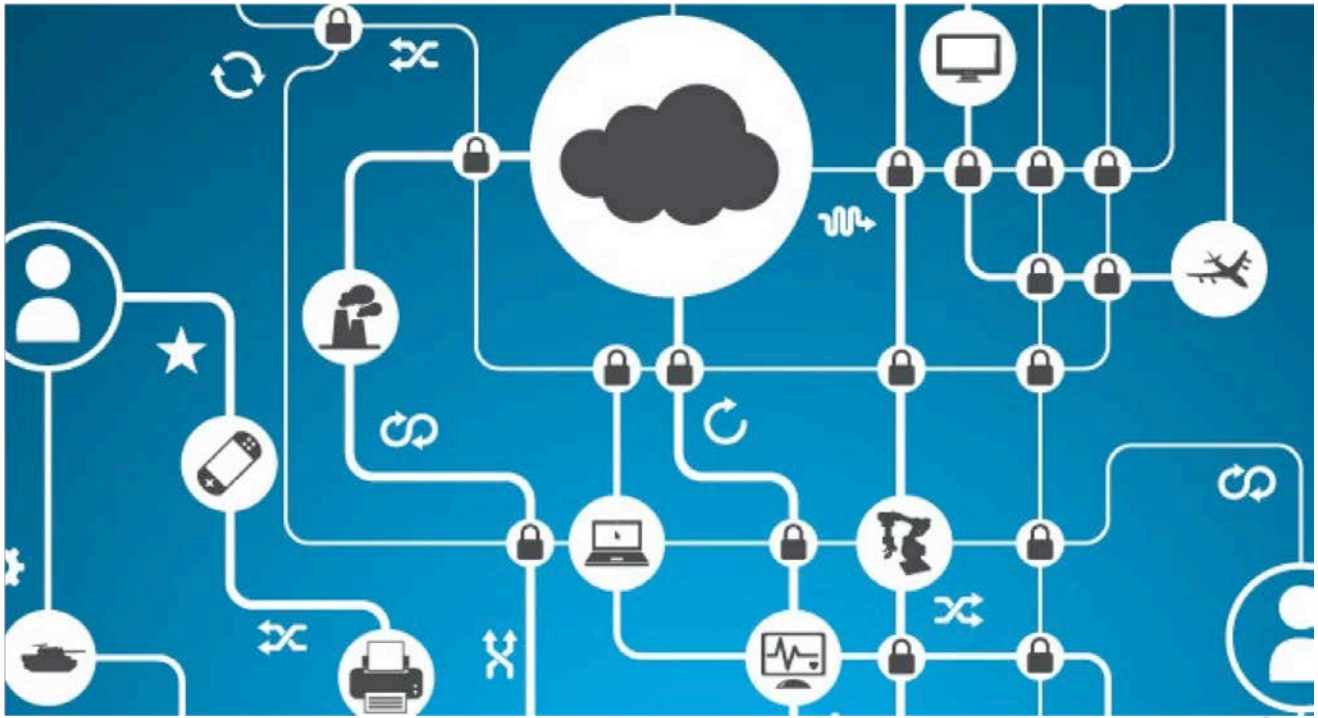
- Computation + Physics
- Algorithms + Logic + Control + …
- Inter-disciplinary emerging area

Cyber-Physical Systems

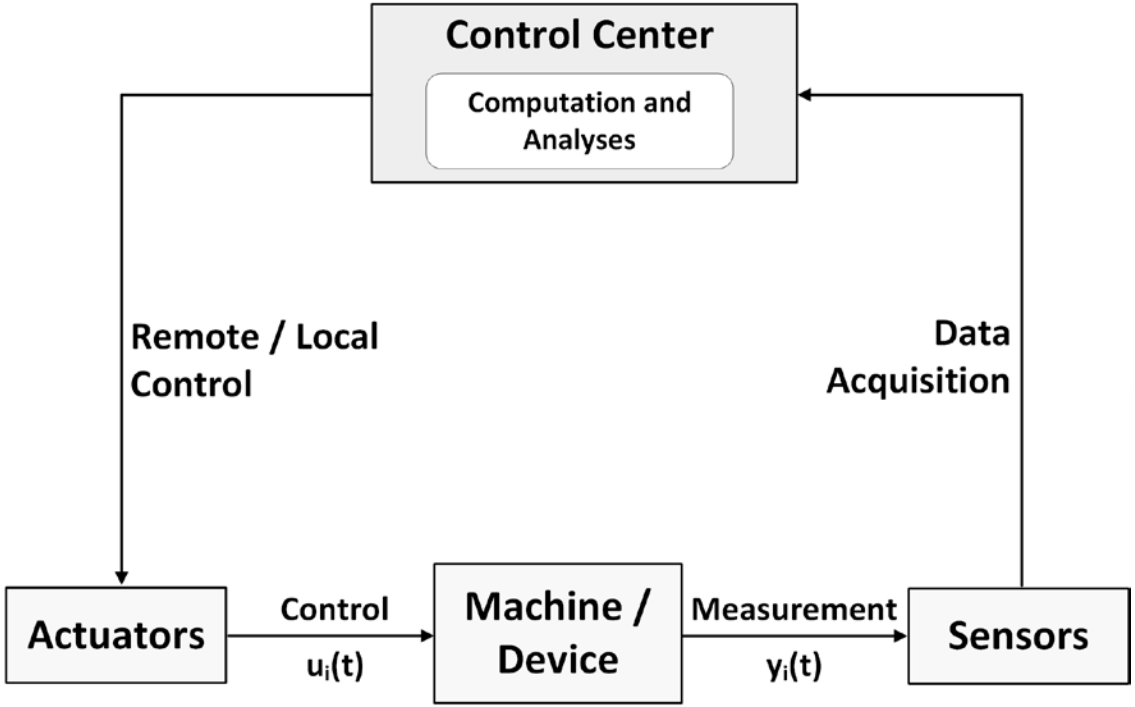




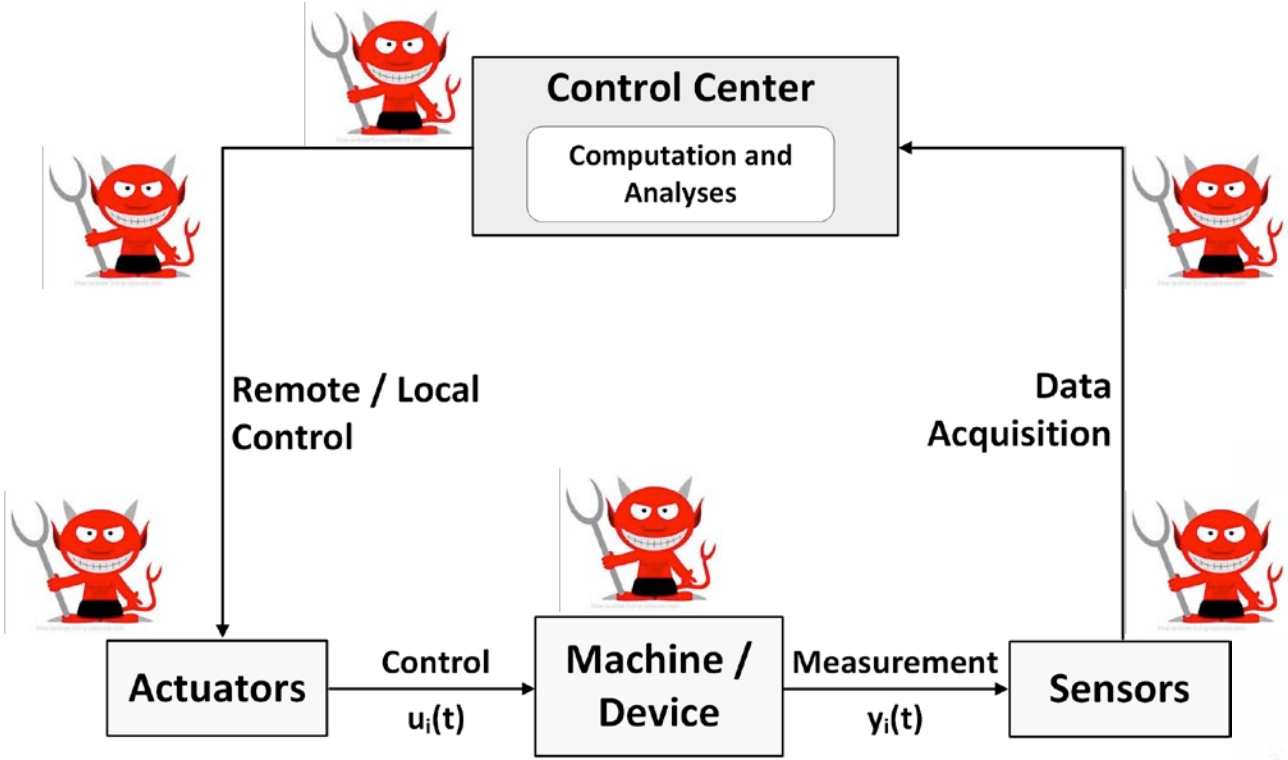
Networked ICS/CPS Systems



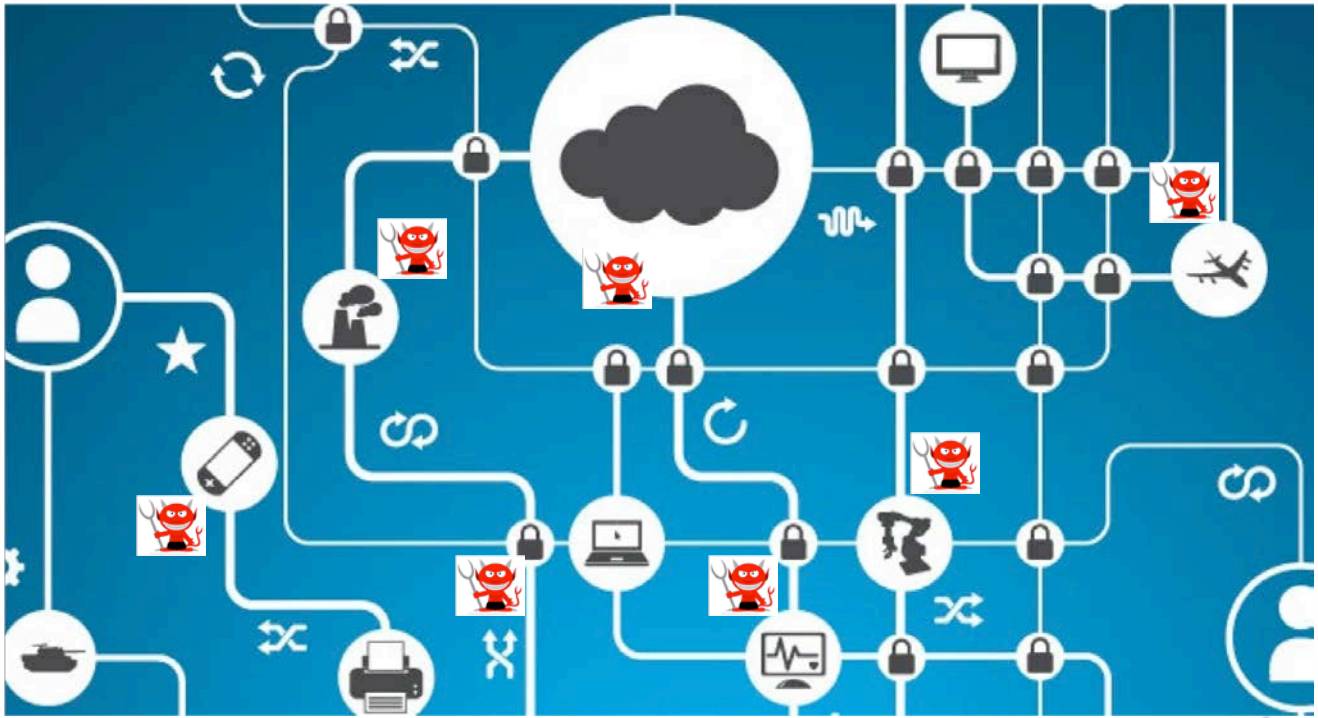
ICS Control Loop



ICS Control Loop Attack



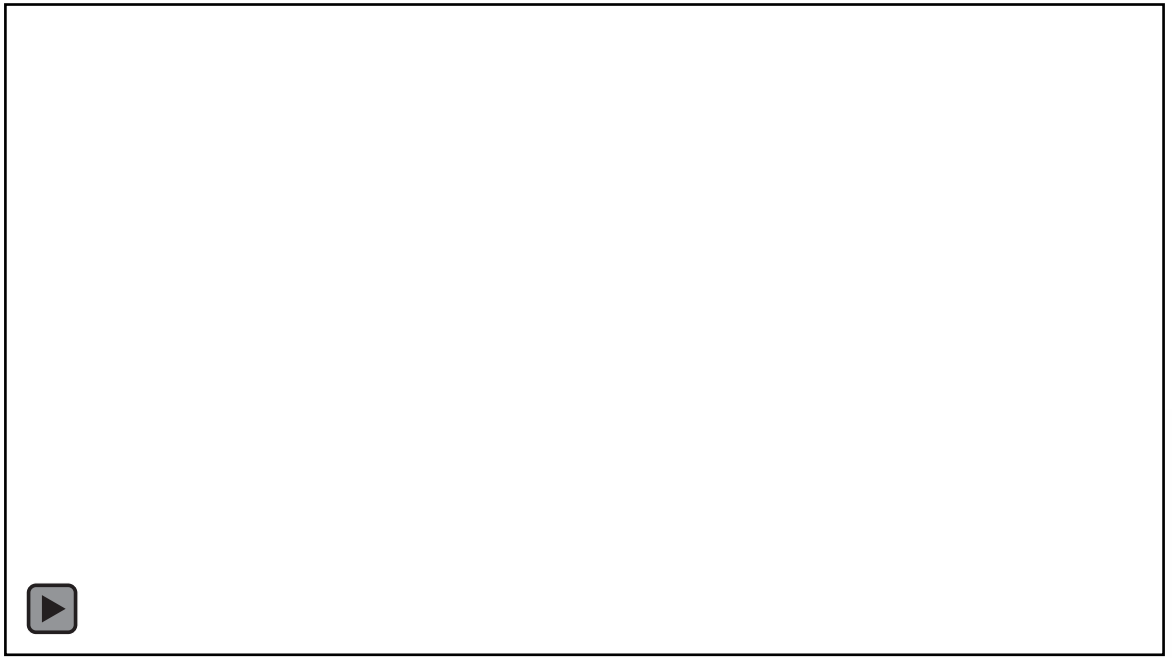
ICS Network Attack Surface



IT vs. OT

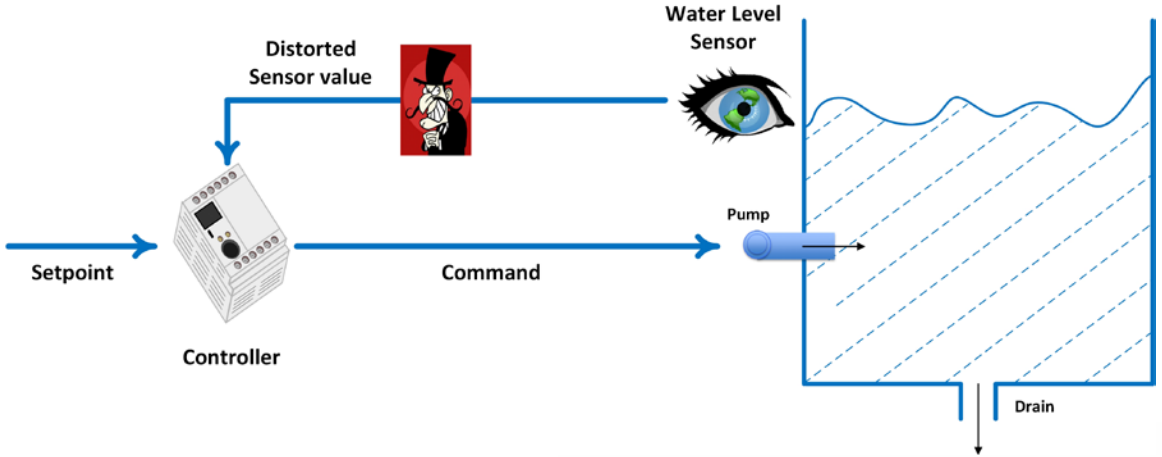
	Information Technology	Operational Technology
Purpose	Process transactions, provide information	Control or monitor physical processes and equipment
Architecture	Enterprise wide infrastructure and applications (generic)	Event driven, real time, embedded hardware and software (custom)
Interfaces	GUI, web browser, terminal and keyboard	Electromechanical, sensors, actuators, coded displays, hand-held devices
Ownership	CIO and IT	Engineers, technicians, operators and managers
Connectivity	Corporate network, IP based	Control networks, hardwired twisted pair and IP based
Role	Supports people	Controls machines

Cyberattacks on ICS



ICS Attack Classification

- Computational attacks
- **False data injection attacks**



Attack examples

Insert wrong commands (computational) – Overwrite sensor value (false data injection)

Stuxnet: Worm hits computers of staff at Iran nuclear plant

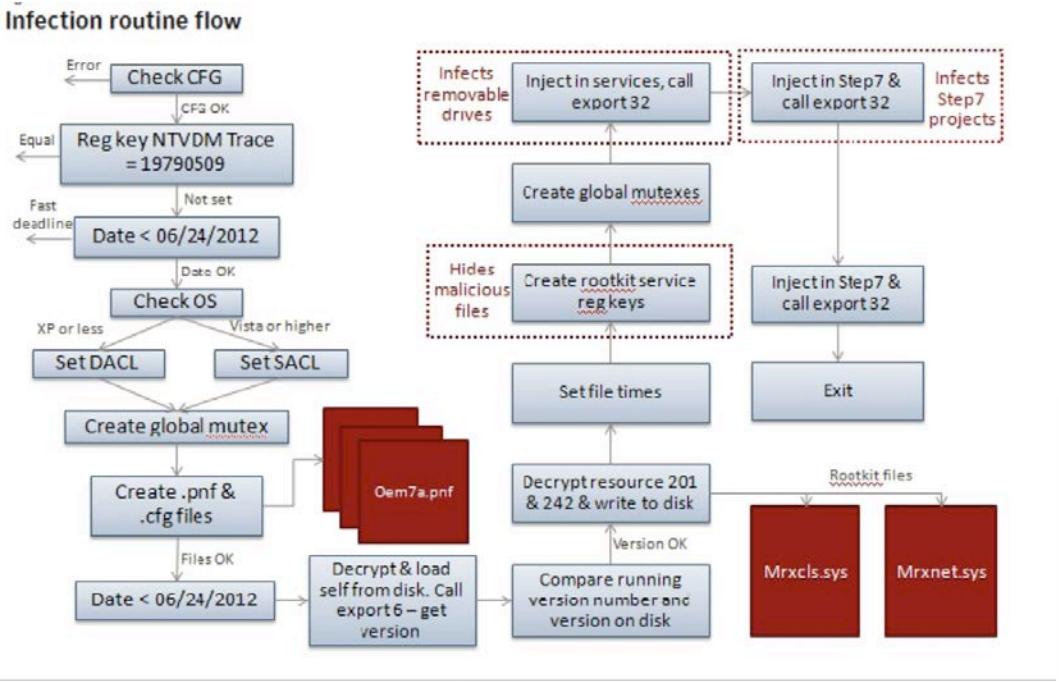
By NASSER KARIMI (AP) – July 27

TEHRAN, Iran — A complex computer worm capable of seizing control of industrial plants has affected the personal computers of staff working at Iran's first nuclear power station weeks before the facility is to go online...

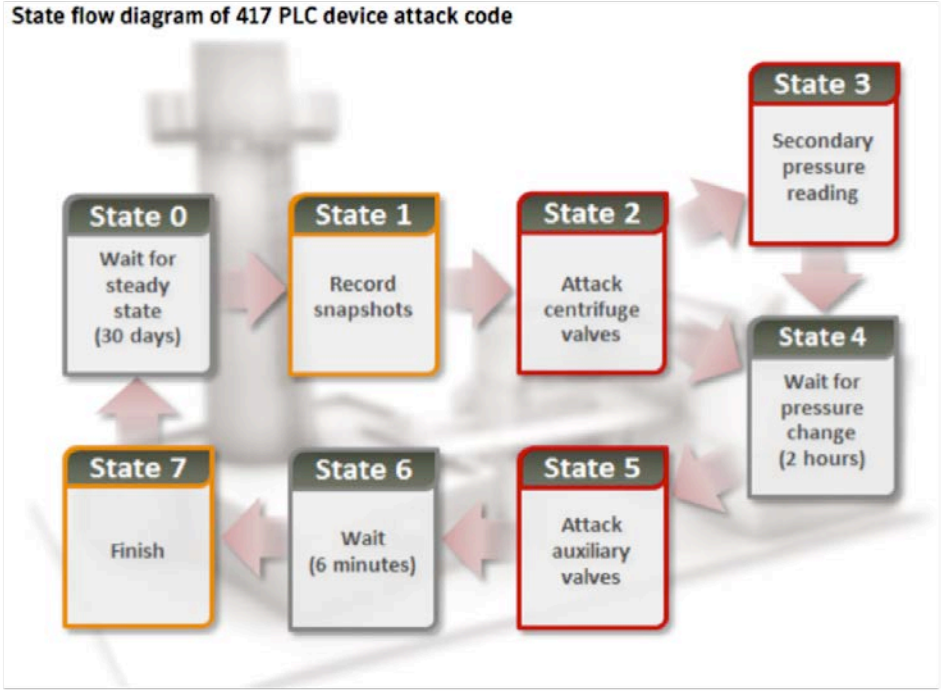
The project manager at the Bushehr nuclear plant, Mahmoud Jafari, said a team is trying to remove the malware from several affected computers, though it "has not caused any damage to major systems of the plant," the IRNA news agency reported.

It was the first sign that the malicious computer code, dubbed Stuxnet, which has spread to many industries in Iran, has also affected equipment linked to the country's nuclear program…

Stuxnet attack



Stuxnet: Final stage of attack



Maroochy water system attack

- VB was employee of Hunter Watertech, an Australian firm that installed SCADA radio-controlled equipment
  - Hunter Watertech installed radio-controlled sewage equipment for the Maroochy Shire Council in Queensland, Australia (touristic rural area with natural beauty)
  - VB applied for a job with the Maroochy Shire Council
  - VB walked away from a “strained relationship” with Hunter Watertech
  - The Maroochy Shire Council decided not to hire him
  - VB decided to get even with both the Council and his former employer
- VB issued radio commands to the sewage equipment (at least 46 occasions)
  - 800,000 liters of raw sewage spilled into local parks, rivers and even the grounds of a hotel
  - Marine life died, the creek water turned black and the stench was unbearable for residents

Tehama Colusa Canal Incident

RISI - The Repository of Industrial Security Incidents

12/10/15 23:50

at his hearing. He was sentenced to 10 years imprisonment.

Impact:

The intrusion cost the TCCA more than $5,000 in damages.

Harrisburg Water Treatment Incident

Metcalf Sniper Attack

- Attack on PG&E's Metcalf Transmission Substation outside San Jose, CA
- April 16, 2013: gunmen fired on 17 electrical transformers
  - Damage: $15 million
- Before the attack, AT&T fiber-optic telecom cables were cut
- Piles of rocks found indicating scouting of firing positions

Metcalf Sniper Attack Timeline (Wikipedia)

- 12:58 a.m. AT&T fiber-optic telecommunications cables were cut not far from U.S. Highway 101 just outside south San Jose.
- 1:07 a.m. Some customers of Level 3 Communications, an Internet service provider, lost service. Cables in its vault near the Metcalf substation were also cut.
- 1:31 a.m. A surveillance camera pointed along a chain-link fence around the substation recorded a streak of light that investigators from the Santa Clara County Sheriff's office think was a signal from a waved flashlight. It was followed by the muzzle flash of rifles and sparks from bullets hitting the fence.
- 1:37 a.m. PG&E confirms received an alarm from motion sensors at the substation, possibly from bullets grazing the fence.
- 1:41 a.m. Santa Clara County Sheriff's department received a 911 call about gunfire, sent by an engineer at a nearby power plant that still had phone service.
- 1:45 a.m. The first bank of transformers, riddled with bullet holes and having leaked 52,000 gallons of oil, overheated - at which time PG&E's control center about 90 miles north received an equipment-failure alarm.
- 1:50 a.m. Another apparent flashlight signal, caught on film, marked the end of the attack. More than 100 shell casings of the sort ejected by AK-47s were later found at the site.
- 1:51 a.m. Law-enforcement officers arrived, but found everything quiet. Unable to get past the locked fence and seeing nothing suspicious, they left.
- 3:15 a.m. A PG&E worker arrives to survey the damage.

New direction: Hybrid Program Correctness

- Formal methods
  - Hardware and software systems
  - Design, synthesis and verification
  - Complexity management
- ICS and CPS considered as hybrid programs

- Hybrid program

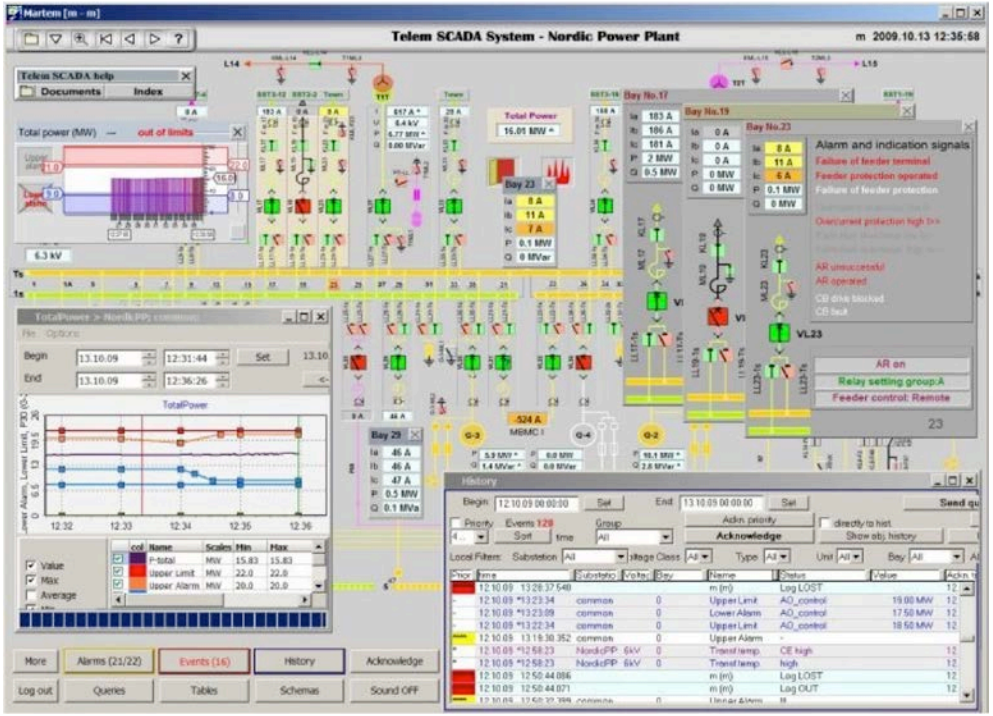
```
while (1) {
    sensor(x,z);  //attack?
    control(z,u); //attack?
    plant(x,u);   //attack?
}     //safe and secure?
```

- Attacks are special inputs or modifications
- Security is a class of properties of these programs

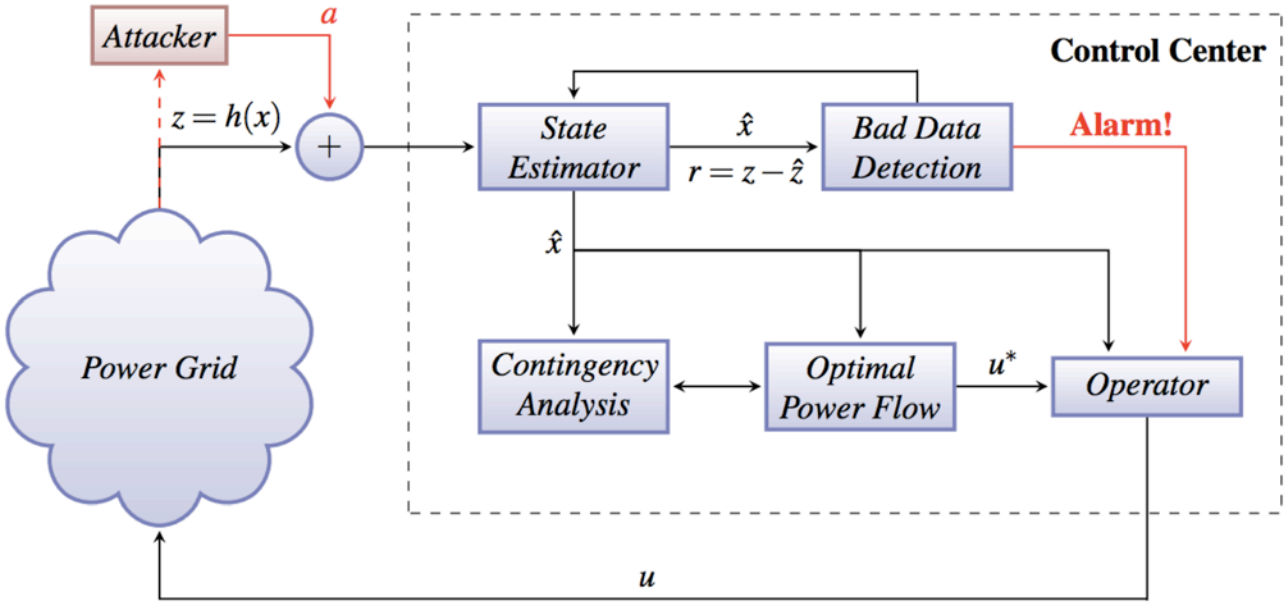
Hybrid Program Analysis

- Find out if the program satisfies specific properties
- Identify security/safety properties
- Counter-examples are attack vectors

False Data Injection Attacks on Smartgrids



False Data Injection Attack for State Estimation



False Data Injection Attack

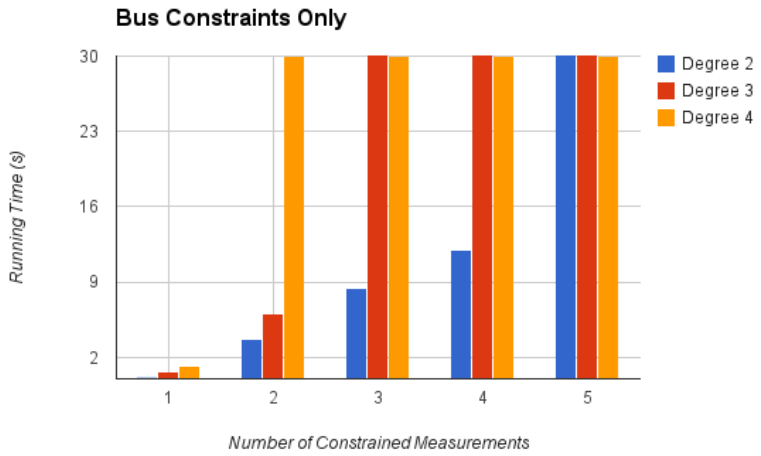
- Feed fake measurement data to the system
- Avoid being detected as bad data
- Mislead the controllers
- The attacks can be local (each control unit) or global (the whole control network)

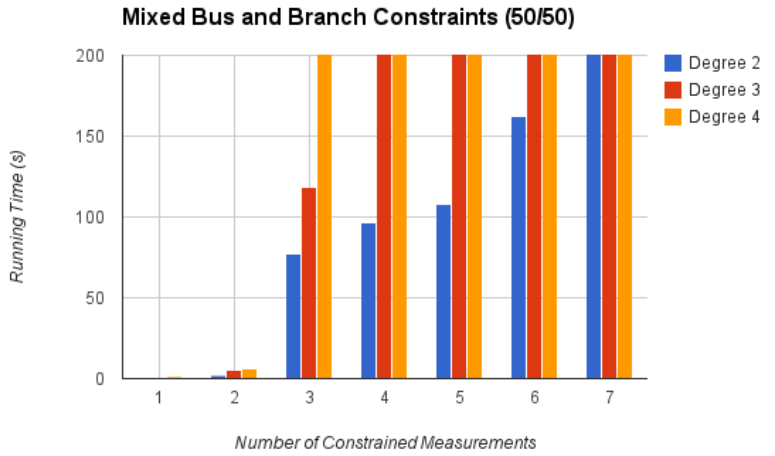
Results

- Although AC state estimation is much harder to attack (NP-hard), our tools can find plenty of attack vectors on realistic power grid models.
- Observations
  - Local structures are simple and easily exploited
  - Existing monitoring mechanisms are weak

Analysis of benchmarks

IEEE benchmarks





Apply What You Have Learned Today

- Next week you should:
  - Identify the critical ICS systems within your organization
- In the next 3 months you should:
  - Identify the sensors that provide critical information to your processes
  - Identify the persons/roles who can intervene to your critical processes
  - Define appropriate controls for intervention to critical processes
  - Perform vulnerability analyses for the critical processes
- In 6 months you should:
  - Introduce appropriate constraints to processes in order to lift vulnerabilities
  - Implement the controls that protect intervention to critical processes by individual operators

Conclusions

- ICS security is extremely challenging
- We are developing a general framework for CPS security that generalizes both software program analysis and fault detection methods
- We have shown vulnerability in realistic nonlinear power grid models
- Future designs of industrial systems should take these results and methods into account

Team

- Howard Shrobe (MIT)
- Armando Solar-Lezama (MIT)
- Sicun Gao (MIT)
- Muhammad Taimoor Khan (QCRI)
- Anastasios Fragopoulos (QCRI)

RSAConference2015

Abu Dhabi | 4–5 November | Emirates Palace

Thank you!