27 Jun 2023

Cyber-Physical Systems

Attack and Defence of a modern power system

Dr Martin Henry Higgins

UNIVERSITY OF OXFORD

Lecture Overview

- Set the scene on why power system attacks are so interesting?
- Outline of some interesting power system attacks cases namely; Stuxnet, Aurora and Ukraine.
- Discussion on deception style attacks and Moving Target Defences.
- DSbD project at the University of Oxford.

Cyber-Physical

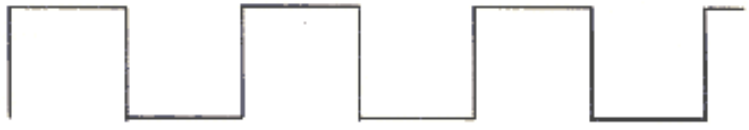
- Cyber: deal in absolutes. 0/1, yes or no ect. . . binary outcomes
- Physical: continuous measurements. Think weight, temperature, waveforms ect. . .
- Cyber-Physical – interaction between the two

UNIVERSITY OF OXFORD

Cyber and Physical

Physical: Continuous Random Profile

Cyber: Quantised



UNIVERSITY OF OXFORD

Self Driving Vehicles

UNIVERSITY OF OXFORD

Manufacturing

Networked Systems

Such as the power system. . ..

UNIVERSITY OF OXFORD

ROYAL HOLLOWAY UNIVERSITY OF LONDON

The New York Times

U.S. Escalates Online Attacks on Russia's Power Grid

Cyber Autopsy Series: Ukrainian Power Grid Attack Makes History

EDITORS' PICK | May 15, 2020, 05:56am EDT | 10,700 views

Cyber Attack On U.K. Electricity Market Confirmed: National Grid Investigates

Hackers are hitting Israel's energy sector with a 'severe cyber attack'

UNIVERSITY OF OXFORD

Motivation for Research

Ukraine power cut 'was cyber-attack'

11 January 2017 Share

Ukraine's energy grid has been attacked twice by hackers

A power cut that hit part of the Ukrainian capital, Kiev, in December has been judged a cyber-attack by researchers investigating the incident.

The blackout lasted just over an hour and started just before midnight on 17 December.

The cyber-security company Information Systems Security Partners (ISSP) has linked

Invisible weapon

In four steps, Stuxnet infiltrated a nuclear factory undetected, then hunted down and destroyed its target. But how?

The Aurora Power Grid Vulnerability and the BlackEnergy Trojan

Posted on: July 12, 2018 Posted in: Critical Infrastructure, Security
Posted by: William "Bill" Malik (CISA VP Infrastructure Strategies)

At recent Industrial IoT security briefings, th Aurora vulnerability has come up repeatedl Attendees ask, "is our country's power grid safe How can we protect the grid? What is Aurora' This post provides a look at Aurora, and th BlackEnergy attack that can exploit Aurora.

In March 2007, the US Department of Energy demonstrated the Aurora vulnerability. (See this video from CNN of the actual test. https://www.youtube.com/watch?v=fJyWngDco3g). What is happening?

An electric generator spins an electromagnet (the rotor) inside a coil of wire (the stator) to creat electric power. The energy spinning the rotor can come from falling water in a hydroelectric powe dam, from burning oil in a diesel generator, from steam created by nuclear fission in a nuclear powe plant, or from the wind in a windmill. That electric power feeds the power grid for distribution to home and businesses.

RUSSIAN HACKERS HAVEN'T STOPPED PROBING THE US POWER GRID

UNIVERSITY OF OXFORD

Motivation

- Power Grids and are an increasing popular line of assault
- High profile attacks against Russia, Ukraine, Israel and potentially Argentinian systems
- Hackers can be hired at a cost of 25-30 USD per hour to attack a system. For the price of one Apache helicopter (which you may never get to use) you could hire a team to work 24 hours per day for over 100 years.

Why Attack a Power System?

- Probably the most critical networked system we have?
- Water, sanitation, communications, defence networks… all downstream of the power system.
- So from a chaos perspective… it is a great target!

Typical targets

- SCADA network – which lends access to circuit breakers, real-time monitoring systems and other networked devices.
- Control centres themselves – anything which can inhibit the abilities of system operators to respond.
- Distributed poorly protected assets – such as meter measurements which can be attacked at low risk.

Ukraine power cut 'was cyber-attack'

11 January 2017

UNIVERSITY OF OXFORD

Ukraine - Consequences

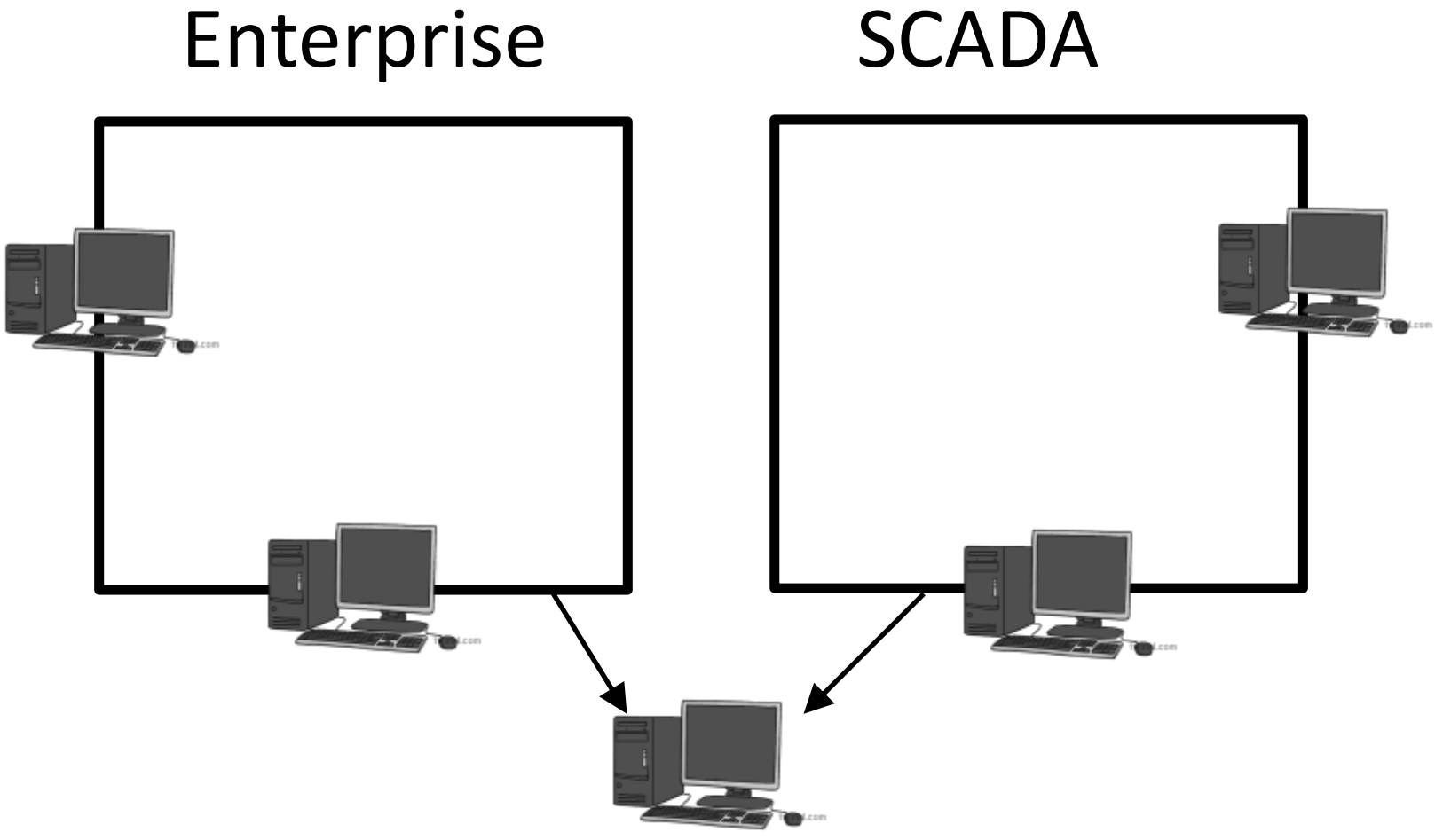
- On 23 December 2015, hackers remotely compromised information systems of three energy distribution companies in Ukraine and temporarily disrupted the electricity supply to consumers.
- 30 substations (7 110kv substations and 23 35kv substations) were switched off, and about 230,000 people were without electricity for a period from 1 to 6 hours.
- SCADA Networks left completely fried and usable for months due to the killdisc.

Ukraine - Attack Profile

- Got access to the corporate networks via the use of basically phishing emails
- Found an overlapping network got access to the SCADA network
- Turned everything off, killed disced all the SCADA network supported with DoS to phone networks to prevent recovery
- Intrusion period took about 3 months, 300k people left without power for a couple of hours. SCADA network took months to recovery.

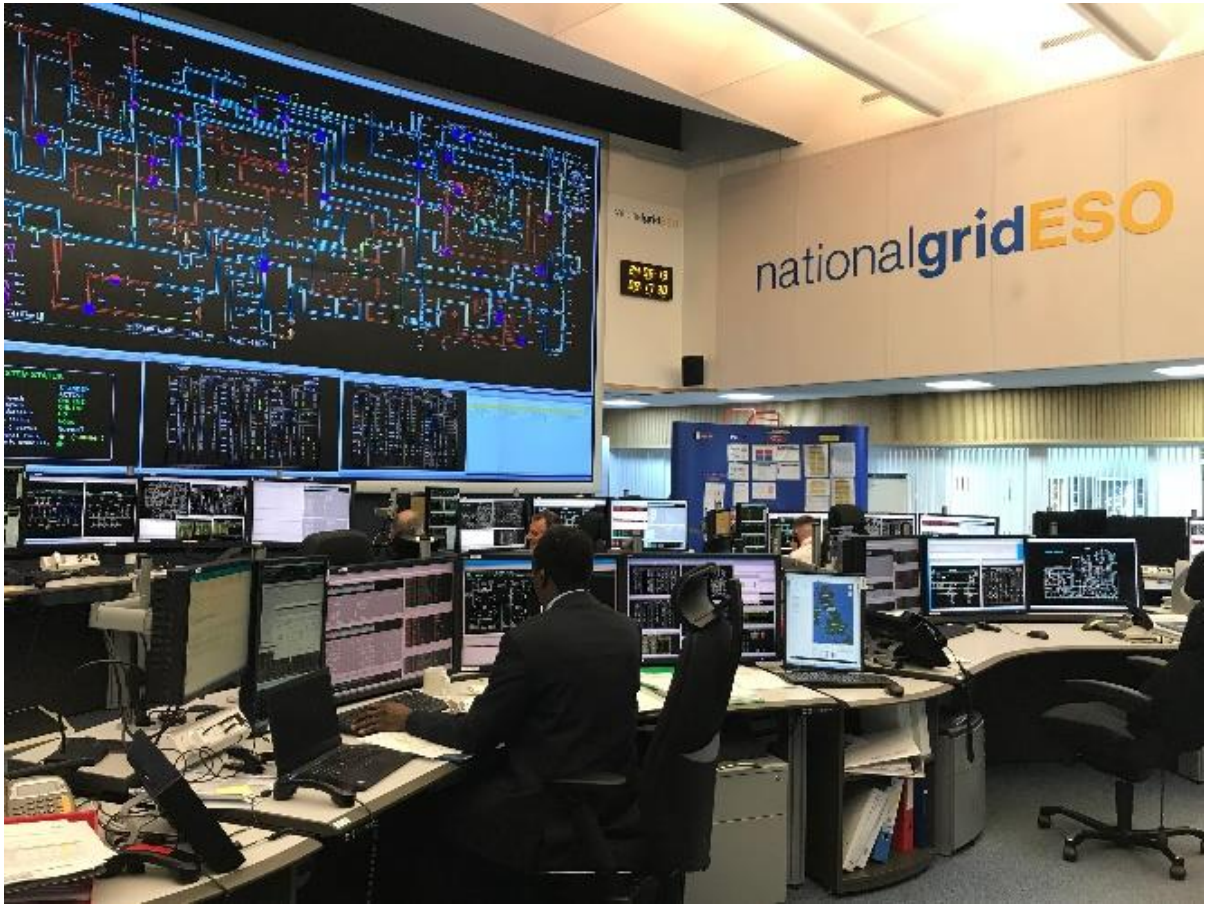
UNIVERSITY OF OXFORD

Ukraine



UNIVERSITY OF OXFORD

Ukraine



UNIVERSITY OF OXFORD

Ukraine

- Top down style of attack i.e. gone for the system operator control systems and consequently got access to virtually everything downstream.
- As opposed to a bottom up approach which might involve attack distributed system assets.


UNIVERSITY OF
OXFORD


STUXNET

Stuxnet

- Attack against the Iranian nuclear centrifuge. Probably the first example of a true deception style attack in an industrial context
- Targets the PLCs (logic controllers) which control the automation of systems processes
- Targeted a very specific controller software (Siemens Step7) that was used inside the Iranian nuclear centrifuges

UNIVERSITY OF OXFORD

Targeted Nuclear Centrifuge

UNIVERSITY OF OXFORD

Centrifuge

- Used for enriching the Uranium (separating the U-235 from the U-238)
- Spins very quickly
- Allows you to separate out the different isotopes of different mass

Stuxnet's Attack Vector

- Stuxnet then forced a change in the centrifuges rotor speed trending up and then trending down. Causing the centrifuges to break overtime.
- It also replayed old measurement datasets back to the system operator (replay attack). Effectively showing normal operation.
- In this way the damage caused by the attack looked like routine faults and the attack vector was completely hidden.

UNIVERSITY OF OXFORD

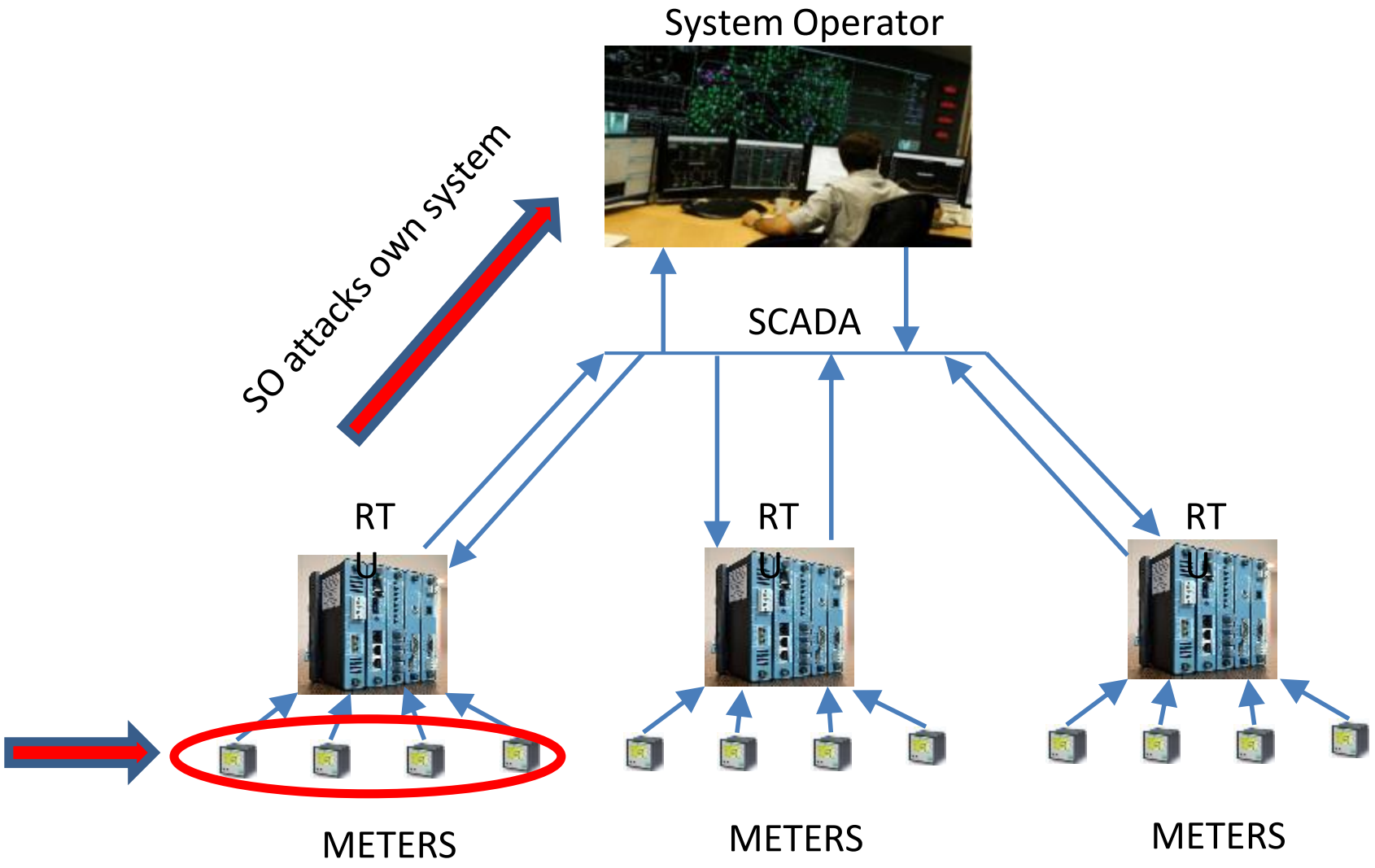
Deception Attack

- Effectively a deception attack fooling the system operator into seeing something wrong and consequently acting on it.
- The replay style vector Stuxnet used we might call a False Data Injection.
- We think these might be possible in the power system also…

UNIVERSITY OF OXFORD

False Data Injection Attacks

- To inject false data into distributed meter measurements in order to replicate a scenario which will damage the grid.
- Effectively a deception attack fooling the system operator into seeing something wrong and consequently acting on it.



Few bottom up defences exist.

UNIVERSITY OF OXFORD

Consequences

- Line Overloading – Burning out lines by masking line overloads from central system operator.
- Load Shedding – Self imposed and unnecessary load sheds to ‘protect’ the wider system
- Blackouts – Cascading failures which lead to system wide brownouts and blackouts
- Financial Manipulation – Taking advantage of optimal power flow to gain market advantages

Outcomes

- System operator can be fooled into seeing whatever you want them to see. You can effectively engineer almost any outcome you want from the SO…
- However these attacks are dependent on a good understanding of network interactions therefore if we can invalidate the attackers knowledge we can evaluate these attacks
- We explore a method of doing this called ‘Moving Target Defence’ wherein the underlying system is literally changed to evaluate attacks

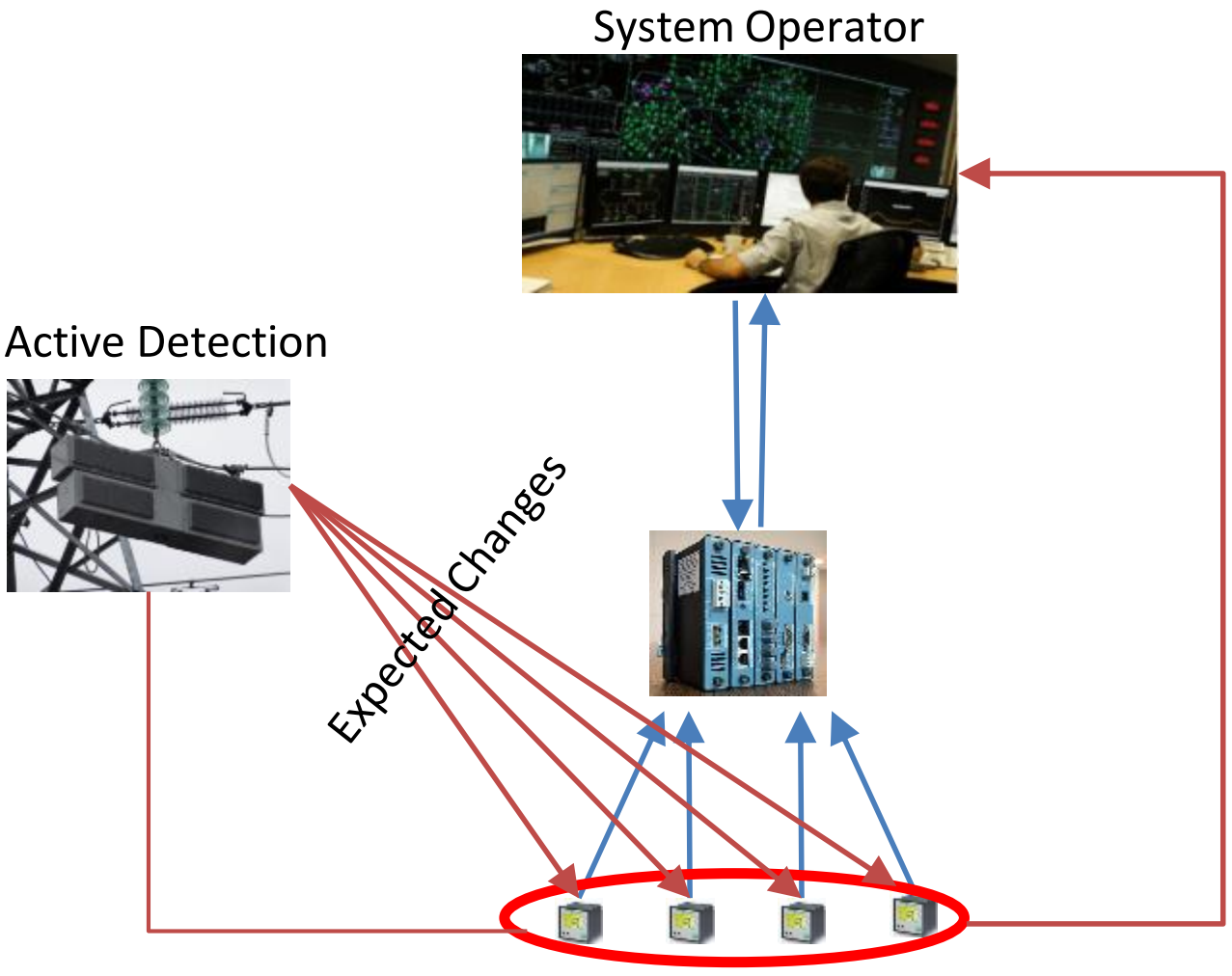
Moving Target Defences

- Using the system to protect the system. We physically change the system by altering topology to invalidate the attackers knowledge of the system.
- Imposing changes at the physical layer to provide extra protections to the cyber layer.

Moving Target Defences

In the power system we can do this in two ways:

- Breaking or changing the interconnections… how stuff is connected (usually done through circuit breakers)
- Leaving the interconnections the same but changing how they interact (resistances, inductances ect…)


System Operator
Active Detection
Expected Changes

Moving Target Defences - Advantages

- You can evaluate these type of stealthy style FDI attacks which utilise the system information to stay hidden
- They are also much better at evaluating replay style attacks. Stuxnet simply replayed plausible data an MTD protocol would likely have evaluated it
- Secondary benefits regular use of system assets can ensure they still work, prevent stuff like stiction in circuit breakers because they are regularly being used.

Moving Target Defences - drawbacks

- Infrastructure costs – you have to install the devices which implement your MTD
- Operational costs – your now using these devices sub optimally so probably costing yourself ongoing operation
- Potential to actually draw attention to high value targets… MTD can be quite obvious if implemented naively so might actually be used for the attacker to prioritize targets.

UNIVERSITY OF OXFORD

Aurora Power Grid Vulnerability

- Attack type which targets circuit breaker control
- Rather than simply turn stuff off this vulnerability uses quick control of the circuit breaker to bring the generator out of phase with the network
- This destroys the generator via the torques induced on the generator and their impact on the generator.

UNIVERSITY OF OXFORD

Aurora Power Grid Vulnerability

Imperial College London

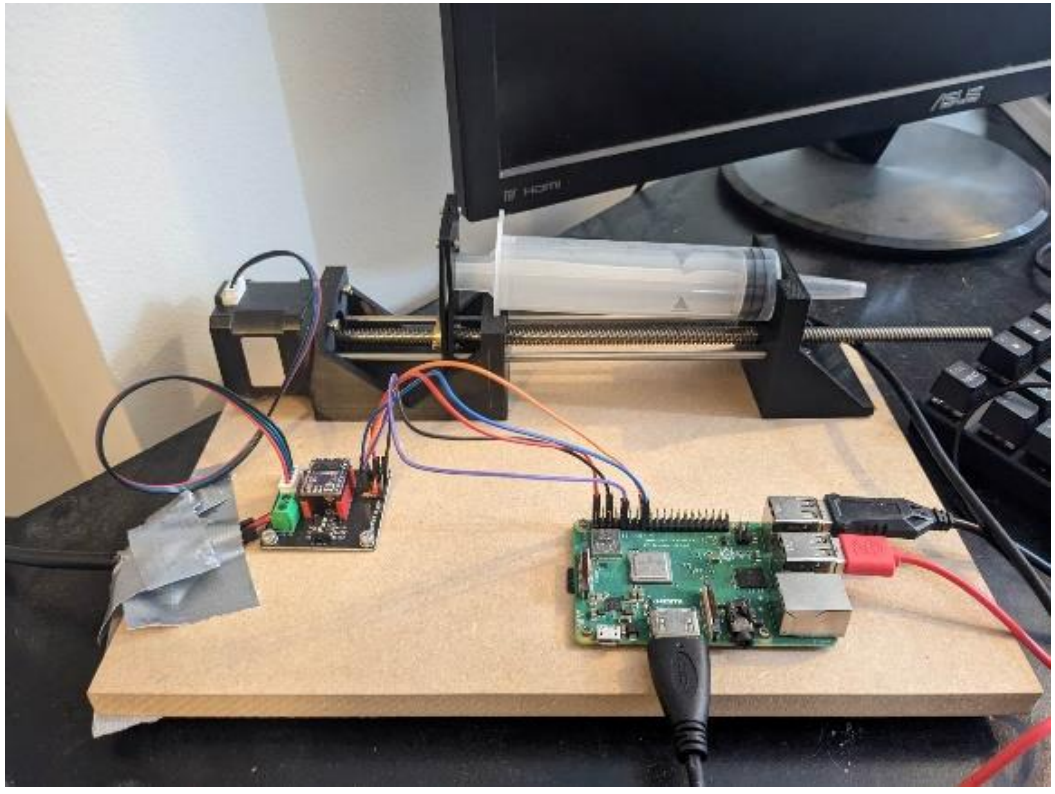
DSbD

Digital Security By Design

- CHERI – Capability Enhance Risc Instructions with aim for delivering secure software by design.
- Connect – post quantum secure mesh style VPN which aims to deliver secure networking.
- ARM Morello Boards – which aims to provide secure hardware and memory protection.
- Cyber-physical systems research primarily across energy, automotive and medical devices.

Imperial College London

Medical Use Case Demonstrator (bad)



Home made 3d printed remote syringe using raspberry pi

Imperial College London

Medical Use Case Demonstrator (bad)

- Controllable remote syringe made by myself using a 3d printer.
- Front end produced in python with a c-program which runs the password comparison.
- This code has a specific vulnerability which makes it susceptible to buffer overflow attacks.

Imperial College London

Medical Use Case Demonstrator (good)

Harvard 22 connected with ARM Morello Board

Imperial College London

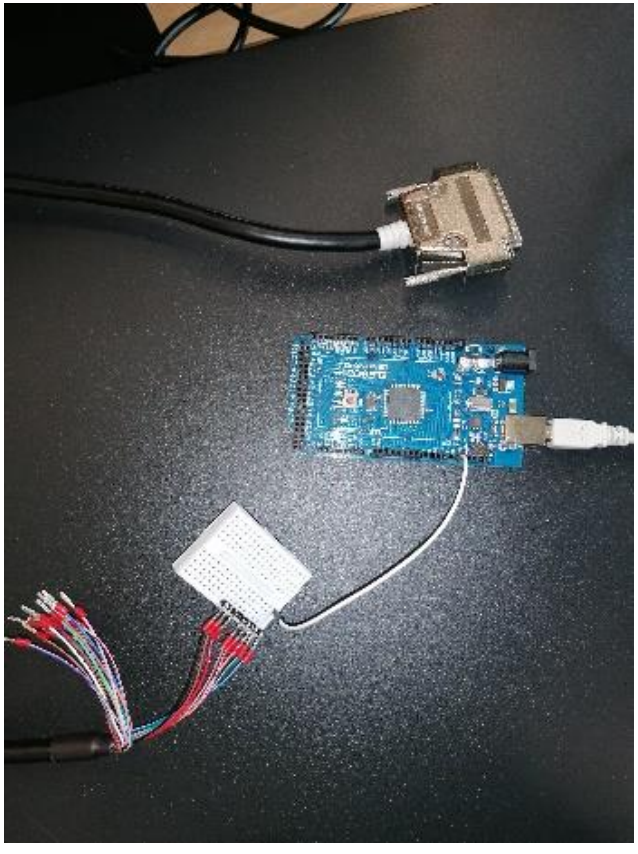
Medical Use Case Demonstrator (good)

- Using the Arm Morello board the buffer overflow attack should be completely impossible to execute.
- Integrated post-quantum VPN will also add additional network security.

Imperial College London

Old Boxes Protected by New Tech

- For example the medical demonstrator runs on outdated RS-232 25 pin configs
- Having to interface it with an Arduino controller and manually set hi/low to get a remote pump action.
- Originally this thing was built in 1996 older than most of the PhD students!



Imperial College London

DSbD

Collaboration Opportunity

- Get a dedicated researcher from the University of Oxford to build a demonstrator for your tech, for free!
- Marketing opportunities through the DSbD network through stuff like CHERI-con ect…
- Ability to implement your tech on the latest Arm Morello security boards. Boast the latest in memory security for your tech.

Questions to martin.higgins@eng.ox.ac.uk