sEptu

Industrial (ICS) Cybersecurity

November, 2020

Background

- The Programmable Logic Controller (PLC) – a micro-controller combined with a range of I/O (input/output) channels - was invented by Dick Morley in 1968

- This invention arguably kicked off the 3rd Industrial Revolution, by properly introducing computers to industry

The PLC is one of the main components in Industrial Control Systems (ICS), a computerised system for integration of hardware, software and network connectivity that is used throughout all industrial sectors, including energy, water, transport, manufacturing and pharmaceuticals

- ICS replaced the bulky, expensive and inflexible controls that were used before

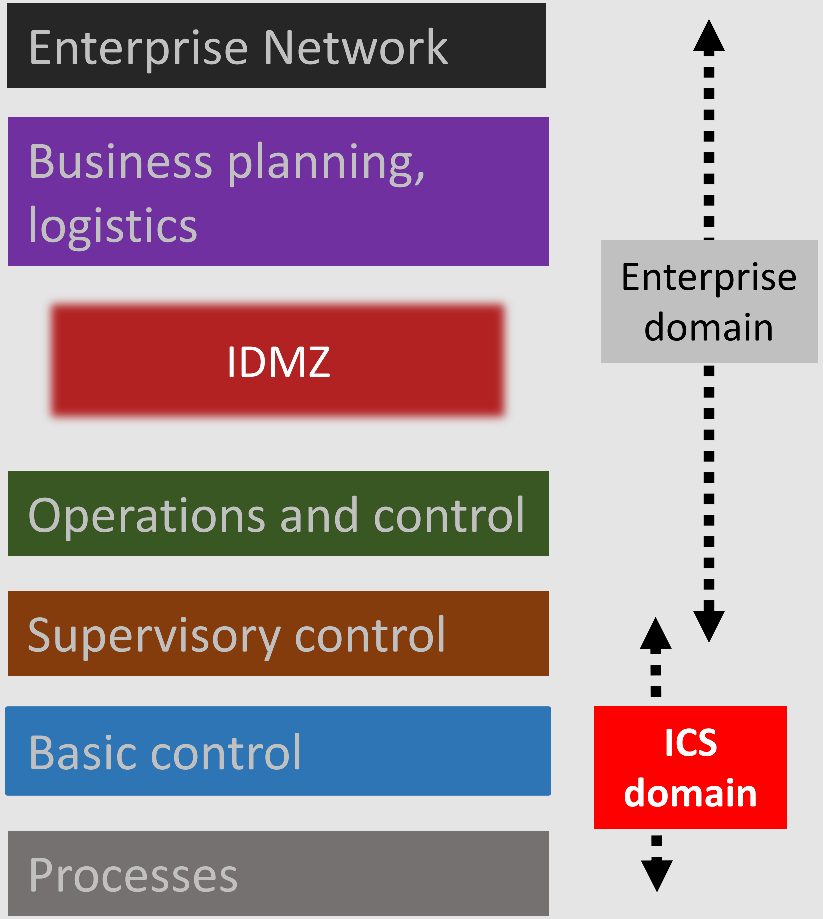
- Features of ICS:
  - Flexible, programmable, modular
  - Easily maintained and appropriately robust for industrial conditions (dirt, vibration etc)
  - Allows coordination of equipment and components spread over a wide area (e.g. a power grid) - Supervisory Control and Data Acquisition or SCADA

The Purdue Model ('Purdue Enterprise Reference Architecture')

- **A reference model for ICS security. Shows the IT and OT (operational technology) networks, and the relationship between them, in an organisation that uses computerised production technology**

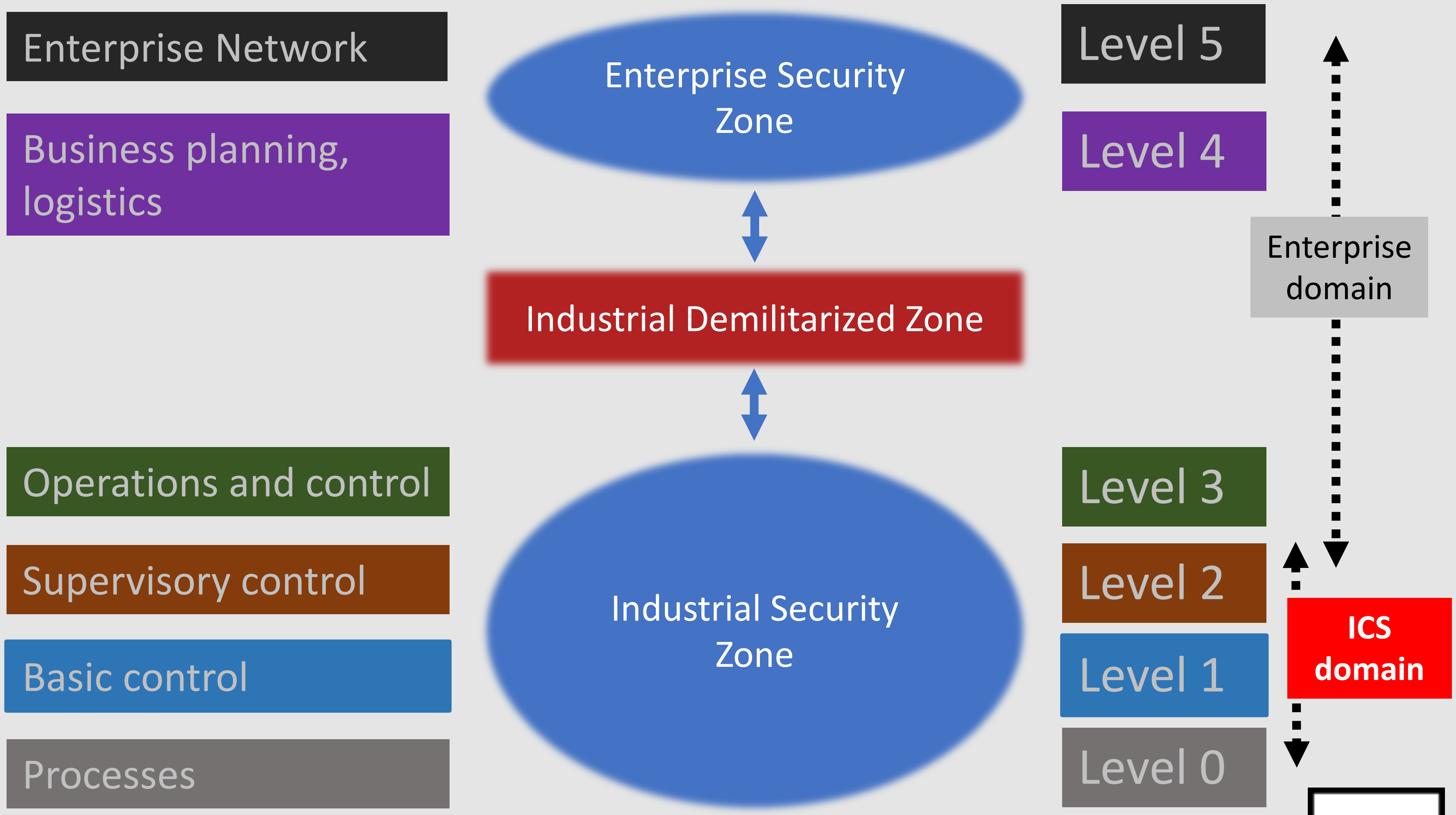
- **Helps to understand the role of ICS in the organisation, and ways that it may be exposed to cyberattack**

- **[The hierarchical structure of the Purdue Model, which was developed in the 1990s, is arguably becoming deprecated as networks become less 'hub-and-spoke' and more cloud-based, but remains relevant]**



ICS Architecture (Purdue Model)

- **Level 4: Business-related activities e.g. shipping, inventory**
- **Level 3: Manage production workflow**
- **Level 2: Supervise, monitor and control processes: PLCs and similar components, SCADA**
- **Level 1: Sensing and manipulating processes: Sensors, Actuators**
- **Level 0: The actual physical processes e.g. production of power**



Enterprise Network — Level 5

Business planning, logistics — Level 4

Enterprise Security Zone

Industrial Demilitarized Zone

Industrial Security Zone

Operations and control — Level 3

Supervisory control — Level 2

Basic control — Level 1

Processes — Level 0

Enterprise domain

ICS domain

One more slide on the Purdue Model:

Level 5

Level 4

The IT network as we currently know it. Internet, email, Microsoft Office etc.

IDMZ

Where IT and OT are separated, using firewalls, proxies and – in some cases of very high security – 'air gaps' across which no data can pass (in theory at least)

Level 3

Manufacturing operations systems, where the 'big picture' of production workflow is managed using operating systems such as Windows

Level 2

SCADA software – possibly being used far away from the plant - monitors and controls physical processes. Distributed Control Systems (DCS), PLCs, HMIs (Human-machine interfaces) and other devices are used in the plant itself, communicating using ICS protocols such as Modbus and Profinet

Level 1

Intelligent devices including actuators and sensors operate at this level. They may be connected over the internet (IoT) with their operator and vendor simultaneously.

Level 0

The physical process that's going on – e.g. producing cars or electricity

ICS vulnerabilities

- **IT network vulnerabilities**

  Attackers targeting the ICS network normally approach it via the corporate IT network (Enterprise Security Zone). Therefore, vulnerabilities there such as poor email security or weak authentication can represent an indirect problem for the connected ICS network

- **Weak Protocols**

  ICS systems protocols (communications methodologies analogous to HTTP), such as Modbus, were not designed with security in mind, and do not use encryption or authentication/integrity checks. This exposes them to a number of possible exploits, including ‘replay attacks’ whereby the attacker records data packets that they observe on the network (‘sniffing’) and then repeats modified versions of the packets in order to send malicious commands to a device

- **Hard to apply normal IT security mitigations to ICS systems and devices**

  See following slide

- **Insider Threat**

  Lack of authentication and encryption controls on ICS networks means that disgruntled or criminal employees have pretty much unlimited access to devices and could cause serious disruption

sEptu

Issues applying IT security to ICS

- **Old devices**

  Many ICS devices are legacy components that are tens of years old. They are often fragile and with limited memory, meaning that it’s hard to make changes to them or patch them

- **Processes require continuous, real-time communication that can be fragile**

  It’s not recommended to use intrusive security software e.g. IPS (intrusion prevention systems) on ICS networks as this may disrupt connectivity and the process

- **Safety-related restrictions**

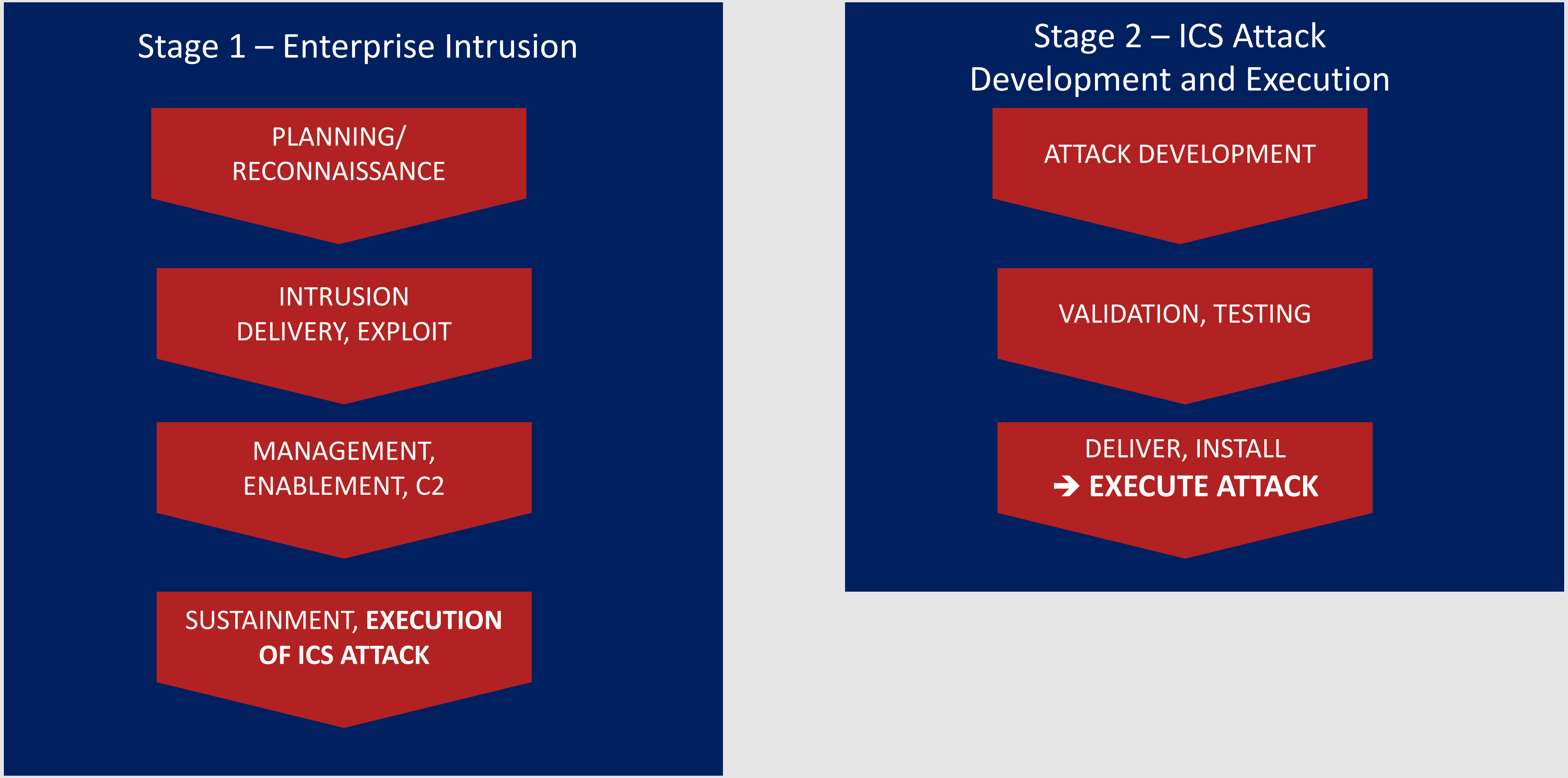
  Password authentication on ICS devices exposes the organisation to the risk that an employee forgets their password under stress, gets locked out of the network, and cannot remediate potentially dangerous problems

- **Uptime requirements**

  Many industrial processes are 24/7 and expensive to interrupt, meaning that there is very little time for patching and software maintenance on devices

ICS Cyber Kill Chain

- Cyber Kill Chain concept created in 2011 by Hutchins, Cloppert and Amin at Lockheed Martin, based on a military approach to evaluation of possible attack strategies and ways to defend against them
- Often used to analyse how an adversary might exploit ICS security vulnerabilities



Stage 1 – Enterprise Intrusion

PLANNING/ RECONNAISSANCE

INTRUSION DELIVERY, EXPLOIT

MANAGEMENT, ENABLEMENT, C2

SUSTAINMENT, **EXECUTION OF ICS ATTACK**

Stage 2 – ICS Attack Development and Execution

ATTACK DEVELOPMENT

VALIDATION, TESTING

DELIVER, INSTALL **→ EXECUTE ATTACK**

sEptu

ICS Cyber Kill Chain - the typical path of an ICS attack

STAGE ONE

- PLANNING PHASE
  Reconnaissance using tools such as Shodan (a search engine for internet-connected devices) and other techniques in order to determine the optimal attack strategy, including the ‘easiest way in’ (attack vector)

- PREPARATION
  Tasks such as ‘weaponization’ (preparing malware) and targeting (e.g. selecting spear-phishing targets)

- INTRUSION, ENABLEMENT
  Infiltrate the IT network, get installed there (e.g. with a remote access trojan) and establish external contact (command and control or C2)

- SUSTAINMENT, EXECUTION
  Escalate privileges and traverse, with objective being a path to the ICS network such as an engineering PC that has connections to both IT and ICS networks

STAGE TWO

- ATTACK DEVELOPMENT AND VALIDATION
  Development of appropriate attack techniques based on exfiltrated data regarding devices, configuration and operating procedures on ICS network. These techniques are typically validated on test systems and equipment

- ICS ATTACK
  Attack capability is delivered and installed, and the ICS is attacked. Possible objectives include denial of service (economic impact of downtime) and disruption of control, view or safety (which would probably cause physical damage and possibly loss of life)

sEptu

Examples of ICS attacks 2000-2014

- **Maroochy Water, Australia (2000)**

  This attack was by an insider – a disgruntled employee of the company - who took advantage of his access to SCADA software and systems to hack around 150 sewage pumping stations, and caused more than 250,000 gallons of untreated sewage to be released into waterways and local parks

- **STUXNET (discovered 2010, probably in development since 2005)**

  Almost certainly the work of Israel's military signal intelligence unit 'Unit 8200' in collaboration with the USA, this is one of the most sophisticated strains of malware yet devised. It's also one of the first that was specifically designed to attack ICS, and in particular Siemens SCADA systems and PLCs. It caused centrifuges in Iran's Natanz nuclear facility to spin at varying destructive speeds that ultimately caused them to break up, and disrupted the production process

- **German steel mill (2014)**

  The German government has not released details of which company was the victim of this attack. Attackers infiltrated the corporate network via targeted spearphishing emails, and then traversed to the ICS network. It appears that they had a good understanding of the company's ICS and the underlying steel production process, and were able to cause a number of control system failures with the result that the plant was severely damaged

Examples of ICS attacks 2015-2020

- **Ukraine power grid (2015 and 2016)**

  The Ukrainian power grid suffered two separate cyberattacks that are widely believed to be the work of an APT (advanced persistent threat) group backed by the Russian government. These attacks – thought to be the first against power infrastructure - are representative of the cyber-risks that power and gas grids are exposed to generally. They included 'telephone denial-of service' attacks on the utility's call centre to prevent customers reporting the outage

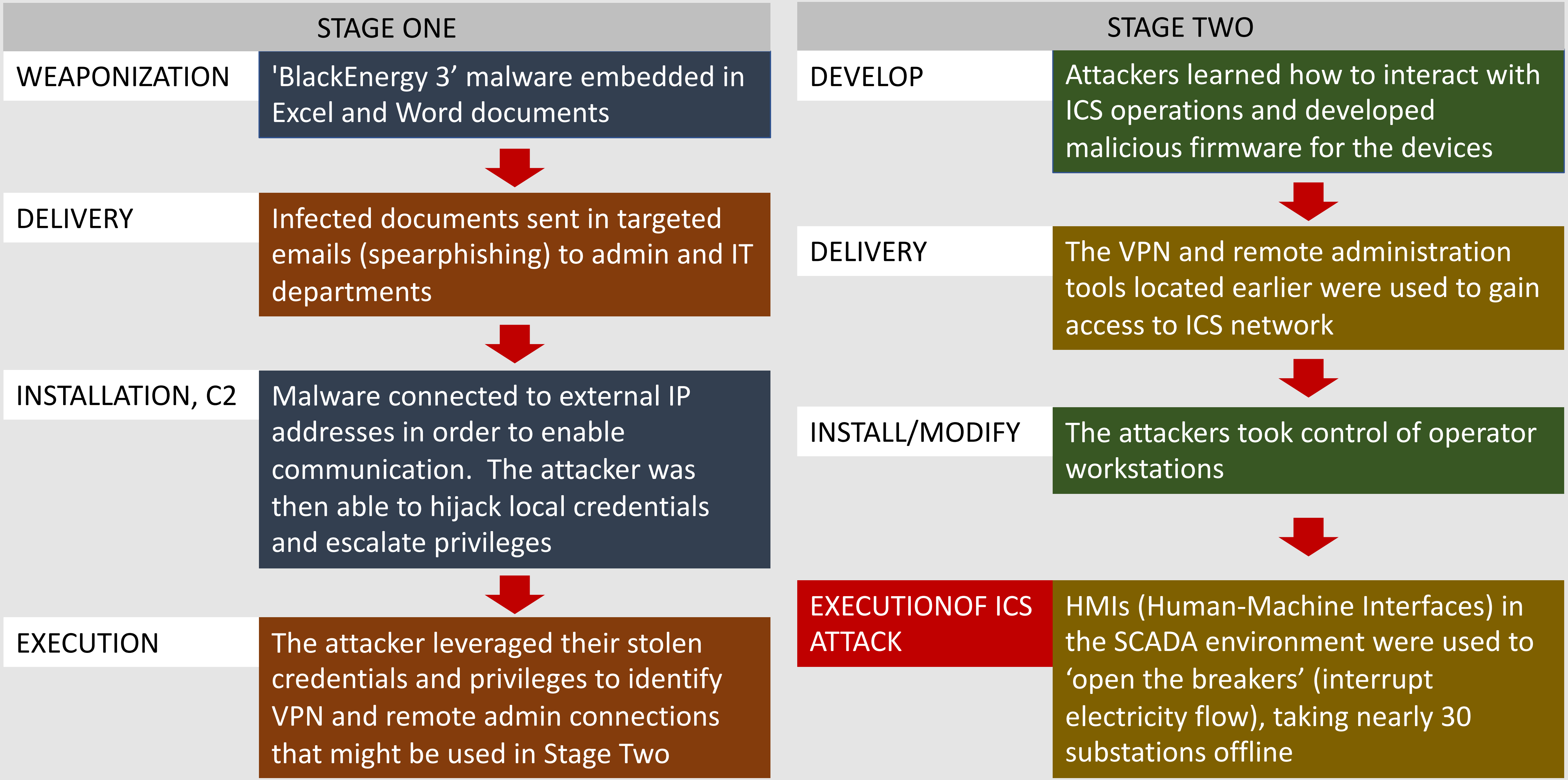
- **'Triton' malware attack on Saudi oil refinery (2017)**

  A similar APT group infiltrated the ICS network of the Saudi Petro Rabigh refinery with a specialised form of malware called Triton. This specifically targets Triconex Safety Instrumented System (SIS) controllers - made by Schneider Electric - that trigger alarms and emergency stops in processes which are exceeding risk limits. The attack took the refinery offline for a week and nearly caused a major explosion. Triton, like Stuxnet, continues to turn up from time to time

- **Israeli water infrastructure (June 2020)**

  A number of attacks were made on the SCADA systems that operate wastewater treatment facilities and pumping stations across Israel, possibly with the intention of raising water chlorine to dangerous levels. Israel was reported to 'link' these attacks to Iran – and Iran's industrial facilities themselves suffered a suspiciously high number of explosions and fires in the following months

ICS attack example: Second Ukrainian Power Grid Attack (2016)



STAGE ONE

WEAPONIZATION: 'BlackEnergy 3' malware embedded in Excel and Word documents

DELIVERY: Infected documents sent in targeted emails (spearphishing) to admin and IT departments

INSTALLATION, C2: Malware connected to external IP addresses in order to enable communication. The attacker was then able to hijack local credentials and escalate privileges

EXECUTION: The attacker leveraged their stolen credentials and privileges to identify VPN and remote admin connections that might be used in Stage Two

STAGE TWO

DEVELOP: Attackers learned how to interact with ICS operations and developed malicious firmware for the devices

DELIVERY: The VPN and remote administration tools located earlier were used to gain access to ICS network

INSTALL/MODIFY: The attackers took control of operator workstations

EXECUTIONOF ICS ATTACK: HMIs (Human-Machine Interfaces) in the SCADA environment were used to 'open the breakers' (interrupt electricity flow), taking nearly 30 substations offline

ICS security solutions I

- **Physical security**
  - ICS systems are normally hard to access from the corporate network or internet, so attackers may try to access the site physically in order to install malware from a USB key or similar (see Stuxnet). Therefore physical security is an important consideration

- **Security of the enterprise network**
  - Attackers often try to infiltrate the enterprise network - for example via spearphishing emails. That means that security on these vectors is very important: Security Awareness Training and Email Security against spearphishing, Multi-Factor Authentication on VPN and remote desktop, regular patch updates etc

- **Network segmentation**
  - Includes physical network separation, filtering (based on IP, device type, current state of operation etc.), logical separation using e.g. unidirectional gateways that only allow logical communications to go one way

sEptu

ICS security solutions II

- **Inventory**
  - A software solution should be used to identify assets and create a complete inventory of devices and systems on the ICS network, including metadata on manufacturer, model name and firmware version, so that this inventory can be monitored for vulnerabilities and changes

- **Network and device monitoring, logging and auditing**
  - Events on devices and traffic on the ICS network monitored by a passive packet analyser
  - This data passed to a SIEM (Security Information and Event Management) system that applies signature-based inspection, machine-learning techniques, correlation analysis and other procedures to look for potentially malicious activity

- **Device and system hardening; whitelisting**
  - Devices are ‘hardened’ by selecting maximum security configuration settings, disabling unnecessary ports and protocols (e.g. telnet, SSH)
  - ‘Whitelist’ necessary applications that can run on ICS devices and systems and don’t allow others

Relevant guidance and frameworks

- **(EU) The Directive on security of network and information systems (NIS Directive)**
  - First piece of EU-wide legislation on cybersecurity
  - Aimed at ‘operators of essential services’ such as energy and water treatment

- **(UK) National Cyber Security Centre Cyber Assessment Framework**
  - Guidance for organisations responsible for vitally important services and activities

- **(UK) OG86 – Cyber Security for Industrial Automation and Control Systems**
  - Guidance from the HSE (Health and Safety Executive) aimed at the energy sector

- **(US) NIST-800-82 – Guide to Industrial Control Systems Security**
  - One of the major US guidances regarding ICS security, from NIST

- **ISO/IEC 62443, ISO/IEC 62351**
  - International industry standards aimed at improving security in Industrial Automation and Control Systems (IACS) and power systems management

- **Mitre ATT&CK ICS**
  - Mitre ATT&CK Enterprise Matrix is very popular among security professionals as a tool for assessing completeness and appropriateness of an organisation’s IT security
  - This version was released in January 2020, and shows ‘the tactics and techniques that cyber adversaries use when attacking industrial control systems’

sEptu

For more information: robin.long@septu.tech