Topic 2

SANS ICS Cyber Kill Chain, and the MITRE ATT&CK Framework for ICS

Dr Diarmuid Ó Briain

Version: 1.1

SETU
Ollscoil
Teicneolaíochta
an Oirdheiscirt
South East
Technological
University

Dr Diarmuid Ó Briain

Table of Contents

Illustration Index

1 Objectives

By the end of this topic, you will be able to:

- Understand and apply the SANS Cyber Kill Chain for Industrial Control Systems (ICS) and MITRE ATT&CK framework to analyse real-world ICS cyberattacks.
- Identify and analyse the unique cybersecurity challenges faced by ICS systems.
- Develop comprehensive threat models for ICS systems to identify, prioritise, and mitigate potential attack vectors.
- Evaluate the effectiveness of ICS security controls in preventing and mitigating cyber threats.

2 Introduction

The SANS Cyber Kill Chain for ICS is a framework for understanding and preventing cyber attacks on ICS. It breaks down the attack process into seven phases: Reconnaissance, Weaponisation, Delivery, Exploitation, Installation, Command and Control, and Actions on Objectives. By understanding these phases, security professionals can develop effective mitigation strategies to protect ICS from attack.

MITRE ATT&CK is a framework, developed by a non-profit organisation MITRE in 2013, to consider each stage of the cyberattack lifecycle from the perspective of the attacker. It is a globally accessible knowledge base of adversary Tactics, Techniques, and Procedures (TTP) based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.

The SANS Cyber Kill Chain for ICS is a practical framework for ICS security professionals, as it is tailored to the specific needs of ICS systems. It forms a bases for, and is a subset of, the MITRE ATT&CK Framework. The MITRE ATT&CK Framework is more comprehensive and provides a more detailed understanding of attack techniques.

3 SANS Cyber Kill Chain for ICS

3.1 What is a Kill Chain

A kill chain is a structured procedure for identifying, engaging, and neutralising an enemy to achieve a desired outcome. The US Department of Defence (DoD) targeting doctrine outlines the phases of this process as F2T2EA:

1. Locate suitable adversary targets for engagement
2. Pinpoint their exact location
3. Track and monitor their movements
4. Select the appropriate weapon or asset to produce the desired effects
5. Engage the adversary
6. Evaluate the results.

This is a comprehensive, end-to-end process that is often referred to as a "chain" because any one breakdown in the sequence can halt the entire operation.

3.2 Advanced Persistent Threats

Conventional network defence tools, such as Intrusion Detection Systems (IDS) and anti-virus software, are designed to detect and respond to known vulnerabilities in computer systems. However, the increasing sophistication and persistence of cyberattacks have rendered these traditional approaches ineffective against Advanced Persistent Threats (APT).

APTs are meticulously planned and executed cyberattacks that involve well-resourced and skilled adversaries. These attackers target specific organisations with highly sensitive information, such as intellectual property, customer data, or government secrets, and employ advanced tools and techniques to evade detection and maintain access for extended periods.

Conventional IDS and anti-virus software often rely on signatures or patterns to identify malicious activity. However, APT attacks often employ zero-day exploits, vulnerabilities that are not known to software vendors and are therefore not yet patched. Additionally, APT attackers often use custom malware that is specifically designed to bypass traditional security defences.

Traditional network defence approaches, which primarily focus on protecting against known vulnerabilities, are becoming increasingly ineffective in the face of sophisticated cyber threats such as APTs. Instead of relying solely on signatures and patterns to identify malicious activity, organisations must adopt a more proactive and intelligence-driven approach to cyber defence.

Intelligence-driven Computer Network Defence (CND) leverages knowledge about adversaries and their TTPs to create a feedback loop that empowers defenders to gain an information advantage over attackers. By understanding the stages of an attack, mapping adversary TTPs to appropriate defence measures, identifying patterns that link individual intrusions to broader campaigns, and continuously gathering intelligence, defenders can proactively anticipate and neutralise attacks.

Institutionalising an intelligence-driven CND approach significantly reduces the likelihood of successful intrusions, informs investment decisions in network defence resources, and provides valuable metrics to assess performance and effectiveness. This intelligence-based approach is crucial in the face of APTs, as it goes beyond vulnerability mitigation to address the threat component of risk as well.

3.3 The Intrusion Kill Chain

The intrusion kill chain is a framework, developed at Lockheed Martin, for understanding and preventing cyberattacks. It breaks down the attack process into a series of stages, each of which represents a specific goal that the attacker must achieve in order to succeed [1].

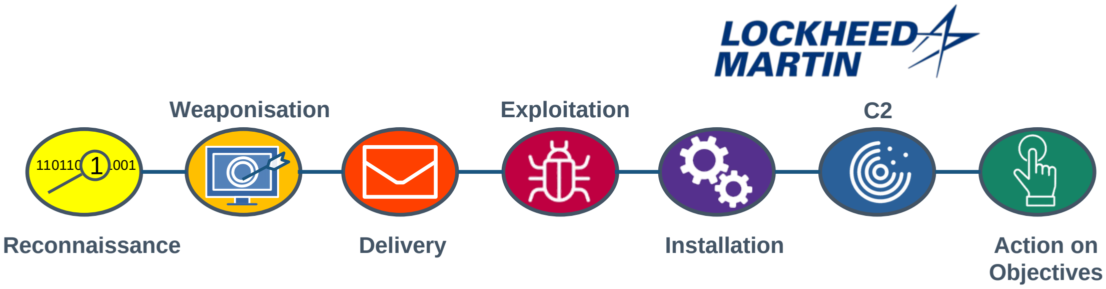


Figure 1: Intrusion Kill Chain

1. Reconnaissance

In the reconnaissance stage, the attacker gathers information about the target organisation and its systems. This information can be obtained from a variety of sources, such as public records, social media, and corporate websites. The goal of reconnaissance is to identify vulnerabilities that the attacker can exploit to gain access to the target system.

2. Weaponisation

Once the attacker has gathered enough information, they begin to develop a malicious payload. This payload is the code that will be used to exploit the vulnerabilities in the target system. The payload can be a variety of things, such as a virus, worm, or Trojan horse.

3. Delivery

The next step is to deliver the payload to the target system. This can be achieved in a variety of ways, such as through email, flash-drive, or network exploitation. The goal of delivery is to get the payload onto the target system so that it can be executed.

4. Exploitation

Once the payload is on the target system, the attacker attempts to exploit the vulnerabilities that they have identified. This involves using the payload to execute malicious code and gain access to the system.

5. Installation

After gaining access to the system, the attacker installs malware or other malicious software. This software gives the attacker control of the system and allows them to carry out their objectives.

6. Command and Control

The attacker establishes a Command and Control (C2) communication channel with the compromised system so they can control it remotely. This allows the attacker to steal data, install more malware, or launch other attacks.

7. Actions on Objectives

The final stage of the intrusion kill chain is where the attacker carries out their objectives. This could involve stealing data, disrupting operations, or damaging the system.

By aligning enterprise defensive capabilities with the specific processes an adversary undertakes to target that enterprise, the intrusion kill chain transforms into a model for actionable intelligence. Defenders can evaluate the performance and effectiveness of these actions, and devise investment roadmaps to address any capability gaps. At its core, this approach is the perfect example of intelligence-driven CND, which hinges on informed security decisions and measurements based on a deep comprehension of the adversary.

3.4 SANS Cyber Kill Chain for ICS

The SANS Cyber Kill Chain for ICS builds upon the foundation of the Lockheed Martin Intrusion Kill Chain, providing a more specific and nuanced framework for understanding and preventing cyberattacks on ICS. It expands upon the seven phases of the original kill chain, tailoring them to the unique characteristics and vulnerabilities of ICS environments. This more granular approach allows security professionals to develop targeted mitigation strategies that effectively address the specific risks posed by ICS cyberattacks [2].

3.4.1 Stage 1

The initial phase of an ICS cyberattack, as illustrated in Figure 2, bears resemblance to espionage or intelligence operations. It shares parallels to the actions covered in Lockheed Martin's Cyber Kill Chain, often aiming to acquire knowledge about the ICS, understanding the system, and establishing methods to breach internal perimeter safeguards or gain access to production environments.

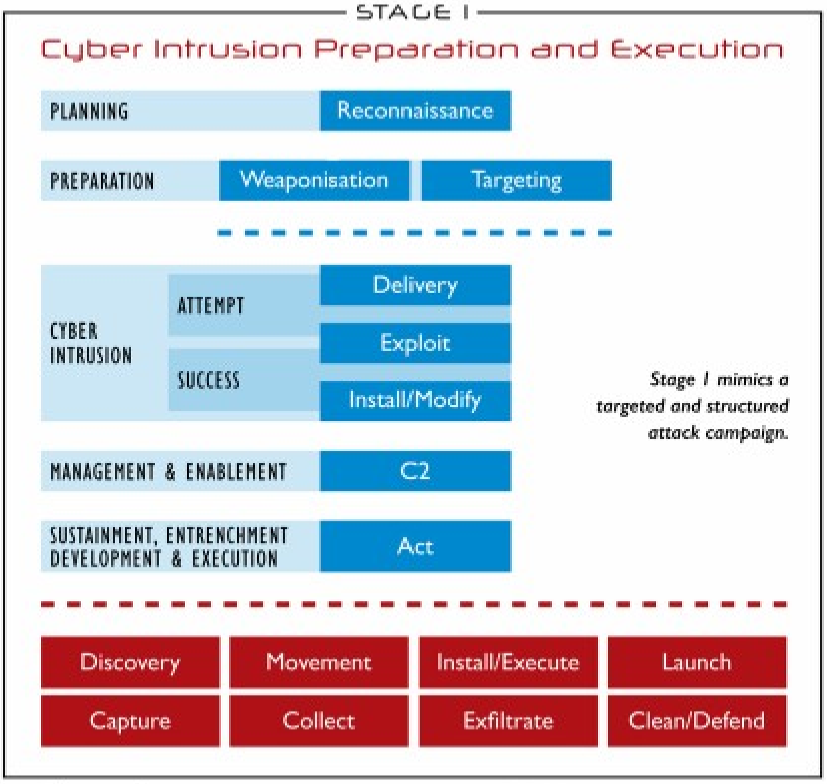


Figure 2: SANS Cyber Kill Chain - Stage 1

Planning phase: marks the commencement of the attack operation, initiated with reconnaissance efforts. Reconnaissance entails the meticulous gathering of information about the target, a process often facilitated by Open-Source INTelligence (OSINT) tools, such as Google and Shodan. These tools enable attackers to delve into publicly available data, including public announcements, social media profiles, and company websites.

The objective of this initial reconnaissance phase is to uncover weaknesses and identify information that can assist attackers in their subsequent targeting, delivery, and exploitation endeavours. This valuable information can encompass human, network, host, account, and protocol details, as well as insights into organisational policies, procedures, and processes.

For ICS environments, reconnaissance extends beyond basic information gathering. Attackers may meticulously research ICS technical vulnerabilities and features, seeking to understand the susceptibility of the target's processes and operating model to exploitation. Passive reconnaissance techniques, often referred to as foot-printing, capitalise on the vast volumes of information available online to discreetly gather intelligence about the target. This may involve mapping publicly or privately accessible attack surfaces, analysing activity patterns, and determining operating system software versions via routine queries.

Attackers often attempt to blend into the background noise of routine Internet traffic to conceal their reconnaissance activities. The publicly available information about organisations plays a significant role in shaping the target options available to adversaries, and defenders have no control over whether their organisations are deemed worthy of attack. Therefore, proactive measures to minimise the exposure of sensitive information and strengthen security posture are crucial for ICS environments.

Preparatory phase: comprises two crucial aspects: weaponisation and targeting. Weaponisation involves the deliberate modification of innocuous files, such as documents, to enhance their malicious capabilities. This often involves embedding exploits within files such as Portable Document Format (PDF) files, but it can also extend to exploiting inherent file features, such as macros in Microsoft Word documents.

Target identification and selection also occur during this phase. In military language, targeting entails analysing and prioritising potential victims, then devising appropriate attack strategies to achieve specific objectives. Cyber attackers make calculated decisions about the attack method based on a cost-benefit analysis, considering the effort required, likelihood of success, and risk of detection.

Weaponisation and targeting are not always mutually exclusive. In certain cases, attackers may uncover valid credentials for direct network access, eliminating the need for weaponisation. Alternatively, adversaries may weaponise their capabilities to target a broad range of potential victims, delaying the selection of a specific target until initial access is gained. This strategy offers greater flexibility and adaptability in the attack plan.

Cyber Intrusion phase: In this phase the attacker will attempt to infiltrate the defender's network or system. This encompasses the delivery of malicious payloads, such as phishing emails or exploits for existing access vulnerabilities. Once initial access is gained, attackers install capabilities like remote access Trojans to establish a persistent presence. Defenders should adopt a threat-informed approach to identify and mitigate intrusions, recognising that malware is not always the sole method employed by attackers.

Management and Enablement phase: After gaining initial access the attacker will establish C2, using methods such as a connection to the previously installed capability or abusing trusted communications such as the Virtual Private Network (VPN). Capable and persistent actors often establish multiple C2 paths to ensure connectivity is not interrupted if one is detected or removed. It is important to note that C2 methods do not always require a direct connection that supports a high frequency of bidirectional communication. Some access to protected networks, for example, may rely on one-way communication paths and require more time to move information out and deliver commands or code in.

Attackers often establish C2 by hiding in normal outbound and inbound traffic, hijacking existing communications. In some cases, attackers establish C2 by implanting equipment to establish their own communication bridge. With managed and enabled access to the environment, the adversary can now begin to achieve his or her goal.

Sustainment, Entrenchment, Development, and Execution phase: The adversary acts to achieve their goals. This may involve gathering information, moving laterally within the network, installing additional capabilities, launching attacks, capturing data, exfiltrating data, and employing anti-forensic techniques.

3.4.2 Stage 1 summary

Stage 1 is the most direct mapping to a breach in traditional Information Technology (IT) networks and can be bypassed if defenders have Internet-facing ICS components or information from a compromised third-party. In stage 1 of an ICS cyber attack the attacker carries out reconnaissance, preparation activities and and cyber intrusion such that they can establish C2.

ICS cyber attacks are unique because ICS components are designed for specific engineering and process requirements, making it difficult for attackers to exploit them without extensive knowledge. However, connecting ICS to the Internet directly undermines the inherent security advantages of a properly architected ICS. Defenders must carefully design and integrate systems to maintain these advantages. For instance, integrating safety systems into the same network as operations significantly reduces the attacker's effort and detection opportunities. With a well-designed ICS, even those with limited security features, attackers can find it challenging to achieve their goals. This underscores the importance of ICS security in preventing disruptions and safeguarding critical infrastructure.

3.4.3 Stage 2

Stage 2, as illustrated in Figure 3, presents the attacker with the opportunity to use the knowledge gained in Stage 1 to develop and test specific meaningful attacks on the ICS. Unfortunately, due to sensitive equipment it is possible that Stage 1 operations could lead to an unintended attack. This is a significant risk for a nation-state cyber operation because such an attack may be perceived as intentional and have unforeseen consequences. For example, an attempt to actively discover hosts on an ICS network may disrupt necessary communications or cause communication cards to fail. Simple interactions with ICS applications and infrastructure elements may result in unintentional outcomes. This activity would still be contained within Stage 1 and be an unintended effect in the Sustainment, Entrenchment, Development, and Execution phase. Intentional attacks take place in Stage 2 and are illustrated in Figure 3.

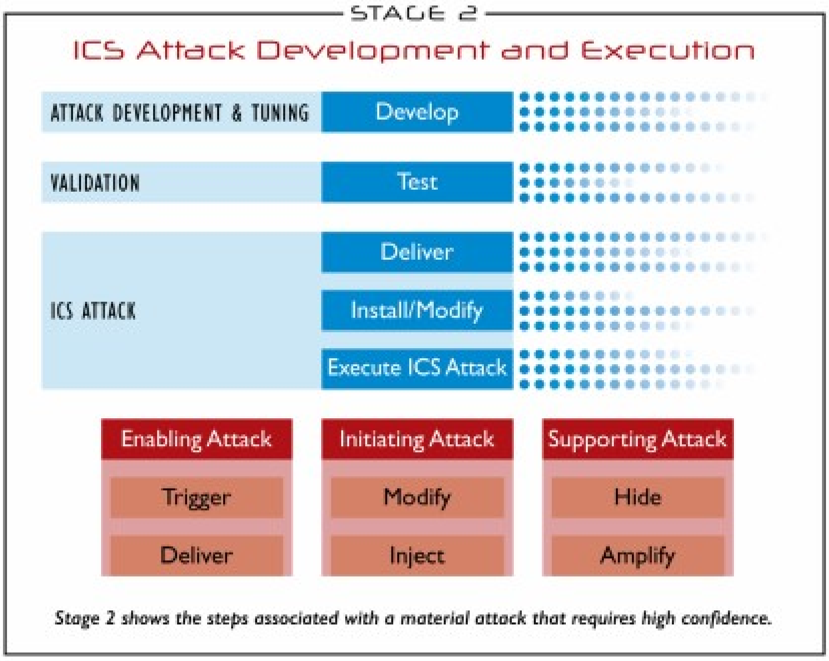


Figure 3: SANS Cyber Kill Chain - Stage 2

Attack Development and Tuning phase: Stage 2 of an ICS cyber attack involves attack development and tuning, where the attacker tailors their capabilities to exploit specific vulnerabilities in the target system and achieve their desired objectives. This development is often conducted using exfiltrated data, acquired during the first stage. Only highly confident attackers, with a low perception of defender awareness, will engage in live in-production testing of their attack code. This makes it challenging for defenders to detect adversary activities during this stage. Additionally, due to the need for extensive development and testing, there may be significant delays between the completion of Stage 1 and the initiation of Stage 2 operations.

Validation phase: After developing their attack capability, the attacker enters the Validation phase, where they test their code on similar or identically configured systems to ensure its effectiveness and reliability. This is crucial for attacks that require precise timing and execution, such as Denial-of-Service (DOS) attacks. For more complex or impactful attacks, the adversary may acquire physical ICS equipment or software components to conduct thorough testing. While this level of validation may be difficult for typical defenders to detect, government agencies with access to industry sources can potentially identify unusual equipment acquisitions, which could signal the start of Stage 2 operations following an established Stage 1 intrusion.

ICS Attack phase: The final stage of an ICS cyber attack is the Execution phase, where the adversary unleashes their tailored capabilities to achieve their desired objectives. This may involve multiple attack components, such as enabling, initiating, or supporting actions, to manipulate specific elements of the ICS process. Attackers may utilise tactics, such as spoofing state information, to deceive plant operators and maintain a facade of normality while carrying out their malicious activities.

The complexity of ICS attacks varies based on system security, process type, safety measures, and attacker objectives. Simple DoS attacks are easier, while manipulation and re-attacks are more difficult. Attackers aim to cause physical harm, equipment damage, formula modifications, or recipe manipulations.

Attacks on ICS systems can be categorised into four main types:

- **Loss**
  - **of view**: access is prevented to process information
  - **of control**: unintended process changes are caused
- **Denial**
  - **of view**: process information is misrepresented
  - **of control**: preventing manipulation of process parameters
  - **of safety systems**: prevention of safety systems activation
- **Manipulation**
  - **of view**: process information is altered
  - **of control**: specific process changes are forced
  - **of safety systems**: the modification of safety parameters
  - **of sensors and instruments**
- **Activation**
  - **of safety systems:** unconventional triggering of safety protocols

The impacts of ICS attacks differ from those on traditional IT systems. In IT, DoS can be disruptive to business operations, but in ICS, manipulation of sensors or processes can pose a significant threat to safety and human life.

ICS operations must understand the full range of potential attack scenarios, which extend beyond power grid failures and dam overflows. Attacks could also include the release of hazardous materials, degradation of manufacturing products, or financial losses due to unusable product. A proactive approach to the identification and assessment of potential attack scenarios is crucial for the development of effective mitigation strategies and minimising the impact of potential attacks.

3.5 Summary

The ICS Cyber Kill Chain is a model that helps defenders understand the phases of an adversary's campaign into an ICS. This model can be used to identify opportunities for detection, remediation, and defence. ICS networks are more defensible than traditional IT networks, but it is important to maintain this defensible architecture by limiting the integration of safety systems with operations networks and removing ICS components from direct Internet access.

4 MITRE ATT&CK for ICS

4.1 What is ATT&CK?

Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) is a framework that categorises cyber attacks into TTPs, specific actions or steps that attackers take to achieve their goals [3]. The framework offers extensive information that previously was only available from documented APTs or through the experiences that security personnel had gained from lived incidents [4].

ATT&CK is organised into eight phases:

- **Reconnaissance**: The attacker gathers information about the target.
- **Initial Access**: The attacker gains access to the target's network or system.
- **Execution**: The attacker executes code on the target's system.
- **Persistence**: The attacker makes sure that they can maintain access to the target's system.
- **Privilege Escalation**: The attacker gains higher levels of access on the target's system.
- **Lateral Movement**: The attacker moves laterally within the target's network.
- **Collection**: The attacker collects data from the target's system.
- **Exfiltration**: The attacker exfiltrates data from the target's system.

Each phase of the ATT&CK framework is divided into tactics, which are high-level goals that attackers pursue. For example, the **Reconnaissance phase** has the following tactics:

- **Discovery**: The attacker discovers information about the target and its environment.
- **Weaponisation**: The attacker prepares malware or exploits.
- **Delivery**: The attacker delivers the malware or exploit to the target.

Each tactic is then divided into techniques, which are specific actions or steps that attackers take to achieve their goals. For example, the **Discovery tactic** has the following techniques:

- **Network Mapping**: The attacker maps the target's network.
- **Data Credential Discovery**: The attacker discovers data and credentials.
- **Domain Discovery**: The attacker discovers the target's domain structure.

There are many benefits to using ATT&CK, including:

- **Improved threat awareness**: ATT&CK can help organisations to understand the TTPs that attackers use, which can help them to identify and defend against attacks.
- **Better threat detection**: ATT&CK can be used to develop threat detection signatures and rules.
- **More effective threat response**: ATT&CK can be used to develop incident response playbooks.
- **Improved communication about threats**: ATT&CK is a common language that can be used to communicate about threats between different organisations.

ATT&CK can be used for:

- **Threat modelling**: ATT&CK can be used to model the threats that an organisation faces.
- **Threat intelligence**: ATT&CK can be used to collect and analyse threat intelligence.
- **Vulnerability assessment**: ATT&CK can be used to assess an organisation's vulnerabilities to specific TTPs.
- **Incident response**: ATT&CK can be used to guide incident response activities.

5 MITRE ATT&CK Matrices

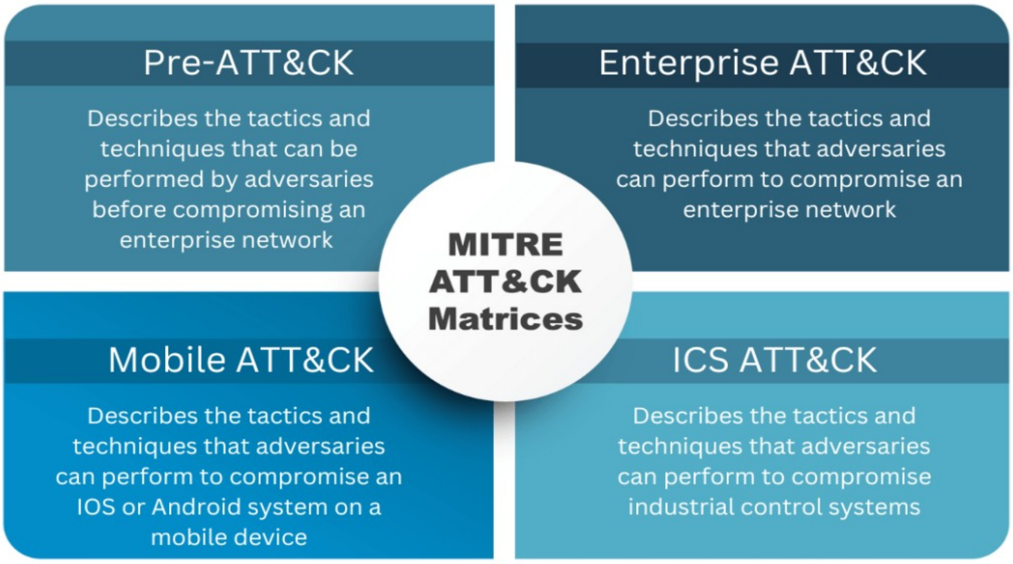

Pre-ATT&CK
Describes the tactics and techniques that can be performed by adversaries before compromising an enterprise network
Enterprise ATT&CK
Describes the tactics and techniques that adversaries can perform to compromise an enterprise network
MITRE ATT&CK Matrices
Mobile ATT&CK
Describes the tactics and techniques that adversaries can perform to compromise an IOS or Android system on a mobile device
ICS ATT&CK
Describes the tactics and techniques that adversaries can perform to compromise industrial control systems

Figure 4: MITRE ATT&CK Matrices

Figure 4 is a diagram that illustrates the different types of cyber attacks. It is divided into four main categories:

1. **Pre-ATT&CK** describes the tactics and techniques that can be performed by adversaries before compromising an enterprise network. This includes things such as reconnaissance, weaponisation, and delivery.
2. **Enterprise ATT&CK** describes the tactics and techniques that adversaries can perform to compromise an enterprise network. This includes things such as exploitation, installation, persistence, and credential access.
3. **Mobile ATT&CK** describes the tactics and techniques that adversaries can perform to compromise an iOS or Android system on a mobile device. This includes things such as reconnaissance, exploitation, and credential access.
4. **ICS ATT&CK** describes a specialised version of the MITRE ATT&CK framework that is designed for understanding and defending against cyberattacks on ICS.

The MITRE ATT&CK framework and matrices are valuable tools for understanding cyber attacks. It can help organisations to identify and defend against attacks by providing a common language and taxonomy for discussing threat intelligence.

5.1 Pre-ATT&CK

The attacker begins by gathering information about the target, such as their network infrastructure, security posture, and employee habits. To achieve this social engineering techniques may be employed to trick employees into revealing sensitive information or clicking on malicious links. Once enough information has been gathered, the attacker will prepare the attack through activities such as developing malware, creating phishing emails, or exploiting vulnerabilities in the target's systems.

5.2 Enterprise ATT&CK

The attacker delivers their attack to the target's network or system, typically through phishing emails, exploiting vulnerabilities, or using stolen credentials. Once access has been gained to the target's system, they will try to establish persistence. This means making sure that they can maintain access to the system even after the initial attack.

The next step for the attacker is to try escalate privileges. This means gaining higher levels of access to the system, such as administrator privileges facilitating movement laterally within the target's network, moving from one system to another without being detected.

At this stage the attacker will then collect data from the target's system, typically including sensitive information such as personal data, financial data, or intellectual property.

As a final step data will be exfiltrated from the target's system. This may be achieved by sending it to a remote server or copying it to a removable storage device.

5.3 Mobile ATT&CK

Similarly to the Enterprise ATT&CK, the attacker begins by gathering information about the target's mobile device. This may include the device's model, operating system, and applications. Again, as with enterprise systems, once the attacker has gathered enough information, they will prepare the attack typically by developing malware, creating phishing emails, or exploiting vulnerabilities in the device's operating system.

The attack is then delivered to the target's mobile device, typically through phishing emails, exploiting vulnerabilities, or using stolen credentials. Once access has been gained access to the target's device, the attacker will try to establish persistence by making sure that they can maintain access to the device even after the initial attack.

The attacker will then try to escalate to root privileges and with this level of access, they will then move laterally within the device, moving from one app to another without being detected.

The attacker will then collect data such as personal data, financial data, or location data, from the device.

Finally, the attacker will exfiltrate the data from the device by sending it to a remote server or copying it to a removable storage device.

6 MITRE ATT&CK for ICS

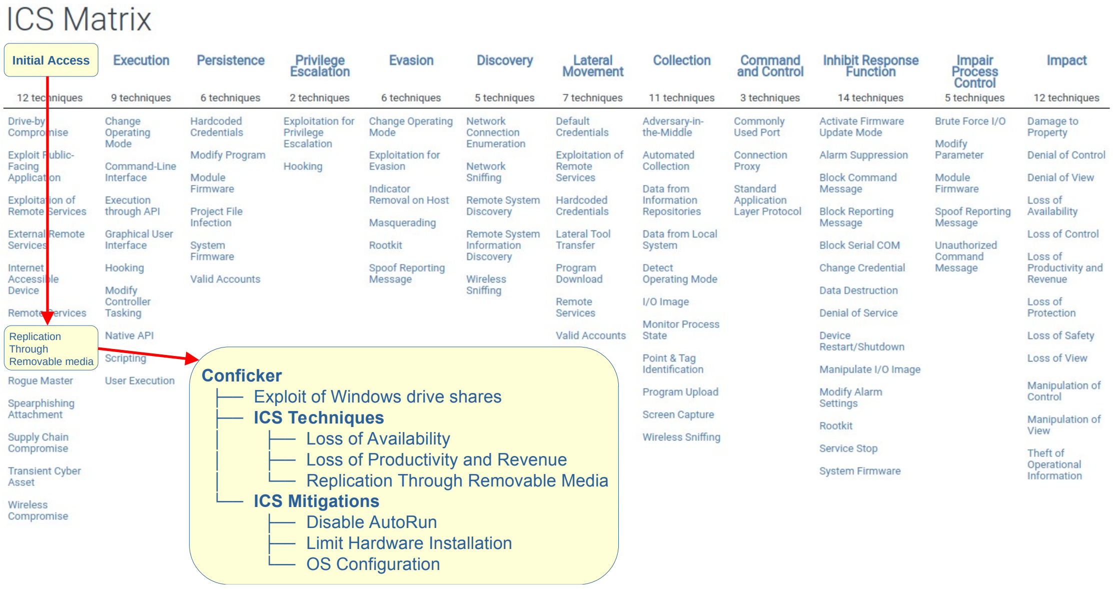
MITRE ATT&CK for ICS is the subject of this topic [5] [6]. The ATT&CK framework for ICS environment is separate to the enterprise level framework as the technologies employed are different. Attacks, on ICS, follow a different methodology and motivation from enterprise attackers. ATT&CK for ICS was initially released in January 2020, with the current version 14 released on October 31st, 2023. This offers focus on 12 separate tactics, 81 techniques as well as 52 different mitigations. Here is a list of the 12 tactics employed in the framework:

- TA0108 – Initial Access
- TA0104 – Execution
- TA0110 – Persistence
- TA0111 – Privilege Escalation
- TA0103 – Evasion
- TA0102 – Discovery
- TA0109 – Lateral Movement
- TA0100 – Collection
- TA0101 – Command and Control
- TA0107 – Inhibit Response Function
- TA0106 – Impair Process Control
- TA0105 – Impact

Each Tactic cover the ***why*** of an attack, the objective of performing an attack. Tactics serve as a higher-level notation for the actions being carried out during an attack, such as privilege escalation. Each tactic has documented Techniques and Procedures to implement the tactic and mitigations to prevent the attack.

- **Techniques:** Techniques cover the ***how*** and ***what*** an adversary gains when carrying out an action and can often be a single step in a string of activities to achieve goal. Each tactic category contains multiple techniques being used to gain the tactical advantage.
- **Sub-Techniques:** Sub-techniques offer a granular description of a technique, are more specific in description and often platform or operating system specific.
- **Procedures:** Procedures offer particular instances of how a technique or sub-technique has been used and can offer several additional behaviours in the way they are performed.
- **Mitigations:** Mitigations offer ***what to do*** when under attack so are countermeasures that may help prevent the adversary from achieving their goal.

6.1 Example



ICS Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
12 techniques	9 techniques	6 techniques	2 techniques	6 techniques	5 techniques	7 techniques	11 techniques	3 techniques	14 techniques	5 techniques	12 techniques
Drive-by Compromise	Change Operating Mode	Hardcoded Credentials	Exploitation for Privilege Escalation	Change Operating Mode	Network Connection Enumeration	Default Credentials	Adversary-in-the-Middle	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Exploit Public-Facing Application	Command-Line Interface	Modify Program	Hooking	Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	Automated Collection	Connection Proxy	Alarm Suppression	Modify Parameter	Denial of Control
Exploitation of Remote Services	Execution through API	Module Firmware		Indicator Removal on Host	Remote System Discovery	Hardcoded Credentials	Data from Information Repositories	Standard Application Layer Protocol	Block Command Message	Module Firmware	Denial of View
External Remote Services	Graphical User Interface	Project File Infection		Masquerading	Remote System Information Discovery	Lateral Tool Transfer	Data from Local System		Block Reporting Message	Spoof Reporting Message	Loss of Availability
Internet Accessible Device	Hooking	System Firmware		Rootkit	Wireless Sniffing	Program Download	Detect Operating Mode		Block Serial COM	Unauthorized Command Message	Loss of Control
Remote Services	Modify Controller Tasking	Valid Accounts		Spoof Reporting Message		Remote Services	I/O Image		Change Credential		Loss of Productivity and Revenue
Replication Through Removable media	Native API					Valid Accounts	Monitor Process State		Data Destruction		Loss of Protection
Rogue Master	Scripting						Point & Tag Identification		Denial of Service		Loss of Safety
Spearphishing Attachment	User Execution						Program Upload		Device Restart/Shutdown		Loss of View
Supply Chain Compromise							Screen Capture		Manipulate I/O Image		Manipulation of Control
Transient Cyber Asset							Wireless Sniffing		Modify Alarm Settings		Manipulation of View
Wireless Compromise									Rootkit		Theft of Operational Information
									Service Stop		
									System Firmware		

```
Conficker
 ├── Exploit of Windows drive shares
 ├── ICS Techniques
 │    ├── Loss of Availability
 │    ├── Loss of Productivity and Revenue
 │    └── Replication Through Removable Media
 └── ICS Mitigations
      ├── Disable AutoRun
      ├── Limit Hardware Installation
      └── OS Configuration
```

Taking the ***TA0108 – Initial Access***, consider the ***Techniques*** used for this Tactic.

- TA0817 – Drive-by Compromise
- TA0819 – Exploit Public-Facing Application
- TA0866 – Exploitation of Remote Services
- TA0822 – External Remote Services
- TA0883 – Internet Accessible Device
- TA0886 – Remote Services
- ***TA0847 – Replication Through Removable Media***
- TA0848 – Rogue Master
- TA0865 – Spear-phishing Attachment
- TA0862 – Supply Chain Compromise
- TA0864 – Transient Cyber Asset
- TA0860 – Wireless Compromise

From these Techniques explore the ***TA0847 – Replication Through Removable Media*** procedures. There are two, for the purpose of the exercise select:

- ***S0608 – Conficker, an exploit of Windows drive shares***
- S0603 – Stuxnet, able to self-replicate by being spread through removable drives.

Information on this computer worm can be accessed. Three techniques, within the ICS domain, can be found:

- ICS T0826 – Loss of Availability
- ICS T0828 – Loss of Productivity and Revenue
- ICS T0847 – Replication Through Removable Media

For example, ICS T0847 was the cause of a shutdown of the Gundremmingen nuclear power plant in Germany in 2016, on Chernobyl's 30th anniversary. RWE, the plant's operator, shut down the power plant as a precaution. On this occasion, the malware affected only the computer IT systems and not the ICS or Supervisory Control and Data Acquisition (SCADA) equipment that interacts with the nuclear fuel.

This **Conficker exploit** can be mitigated by:

- M0942 – Disable or Remove Feature or Program – disable AutoRun
- M0934 – Limit Hardware Installation – Limit hardware such as USB drives
- M0928 – OS Configuration

If it does happen, a **Conficker attack** can be detected by:

- DS0016 – Drive Creation – Monitor for new drives or mount points.
- DS0022 – File Access – Monitor for files accessed on removable media.
- DS0009 – Process Creation – Monitor for new processes from removable media.

7 Threat Models

A threat model is a process that helps organisations identify, assess, and prioritise cybersecurity threats. It involves understanding the potential threats that an organisation faces, the likelihood of those threats being realised, and the potential impact of those threats if they are realised. Threat models can be used to inform security decisions, such as which security controls to implement and where to focus security resources.

A threat model can be used for a variety of purposes, including:

- **Identifying and prioritising risks**: Threat models can help organisations to identify the most serious risks they face and to prioritise their security efforts accordingly.
- **Developing security controls**: Threat models can be used to develop specific security controls to mitigate the identified risks.
- **Communicating security risks**: Threat models can be used to communicate security risks to stakeholders, such as senior management and board members.
- **Preparing for incidents**: Threat models can be used to develop incident response plans to respond to security incidents.

By implementing mitigation strategies, such as those identified in Figure 5 for *Conficker*, organisations can significantly reduce their risk of being compromised by this computer worm and other similar attacks.

7.1 Sample threat model

Threat model
S0608 – *Conficker*, an exploit of Windows drive shares

Threat Actor

- **Type**: APT
- **Motivation**: Gain unauthorised access to systems and networks to steal data, disrupt operations, or conduct espionage
- **Capabilities**: Highly skilled technical expertise, advanced tools and techniques, sophisticated attack methods

Attack Vector

- **Method**: Exploiting vulnerabilities in Windows drive shares
- **Vulnerability**: MS08-067, a vulnerability in the Server Message Block (SMB) protocol that allows attackers to execute arbitrary code on vulnerable systems
- **Exploit**: *Conficker*, a worm that exploits the MS08-067 vulnerability to spread to other systems through shared drives

Attack Path

- **Reconnaissance**: The attacker gathers information about the target system, such as its network configuration and vulnerabilities.
- **Delivery**: The attacker sends a malicious file to the target system, often disguised as a legitimate file.
- **Exploitation**: When the victim opens the malicious file, the **Conficker** worm is executed, allowing the attacker to gain control of the system.
- **Installation**: The worm installs itself on the system and spreads to other systems through shared drives.
- **Persistence**: The worm creates persistence mechanisms to ensure that it remains active on the system even after reboots.
- **Lateral Movement**: The worm moves laterally through the network, infecting other systems and gaining access to sensitive data.
- **Collection**: The worm gathers sensitive data from the infected systems, such as personal information, financial data, and intellectual property.
- **Exfiltration**: The worm exfiltrates the stolen data to the attacker's command and control server.

Mitigation Strategies

- **Patch systems promptly**: Keep all systems patched with the latest security updates, including the MS08-067 patch.
- **Disable unnecessary shares**: Disable unnecessary network shares to reduce the attack surface.
- **Implement strong access controls**: Enforce strong access controls on shared drives, restricting access to authorised users only.
- **Use Intrusion Detection and Prevention Systems (IDS/IPS)**: Deploy IDS/IPS systems to detect and block malicious activity on the network.
- **Educate employees about cybersecurity threats**: Educate employees about cybersecurity threats and how to identify and avoid suspicious emails and attachments.
- **Implement a vulnerability management program**: Regularly scan systems for vulnerabilities and prioritise patching the most critical ones.
- **Use endpoint security solutions**: Deploy endpoint security solutions to detect and block malware infections.

Figure 5: Threat Model for Conficker

8 Exercise

Objective: To familiarise students with the MITRE ICS ATT&CK matrix and its application in understanding and defending against cyberattacks on ICS.

- Assign each student one of the ICS ATT&CK tactics.
- Research and summarise the key techniques and procedures associated with their assigned tactic.
- Present their findings to the class.
- Facilitate a discussion among the groups to compare and contrast the different tactics and their associated techniques.

Additional Activities:

- Develop a threat model for a specific ICS system, identifying and mapping the potential attack paths that could be used by adversaries.
- Research and evaluate ICS security controls that can be implemented to mitigate the risks associated with the different ICS ATT&CK tactics.
- Researching real-world cyberattacks on ICS systems and analysing how the attackers employed the tactics and techniques described in the matrix.
- Developing a deeper understanding of the specific vulnerabilities and attack vectors that are relevant to ICS systems.
- Keeping up-to-date with the latest updates to the MITRE ICS ATT&CK matrix and its application in the ever-evolving cybersecurity landscape.

Assessment:

Assessment on your ability to:

- Identify and explain the key concepts of the MITRE ICS ATT&CK matrix.
- Summarise the key techniques and procedures associated with their assigned tactic.
- Compare and contrast the different tactics and their associated techniques.
- Develop a threat model for an ICS system and identify potential attack paths.
- Evaluate ICS security controls and their effectiveness in mitigating risks.
- Apply knowledge of the ICS ATT&CK matrix to pass the knowledge gained to others.

Create a presentation as part of the assessment, and using it as a tool, create a video to explain what you found that meets the given objective.

9 Bibliography

[1] E. M. Hutchins, M. J. Cloppert, and R. M. Amin, ‘Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains’, *Leading Issues in Information Warfare & Security Research*, vol. 1, no. 1, p. 80, 2011.

[2] M. J. Assante and R. M. Lee, ‘The industrial control system cyber kill chain’, *SANS Institute InfoSec Reading Room*, vol. 1, p. 24, 2015.

[3] A. Di Pinto, ‘Your Guide to the MITRE ATT&CK Framework for ICS’. Nozomi Networks, Nov. 08, 2023. Accessed: Aug. 08, 2023. [Online]. Available: https://www.nozominetworks.com/blog/your-guide-to-the-mitre-attack-framework-for-ics/

[4] B. E. Strom, A. Applebaum, D. P. Miller, K. C. Nickels, A. G. Pennington, and C. B. Thomas, ‘Mitre att&ck: Design and philosophy’, in *Technical report*, The MITRE Corporation, 2018.

[5] O. Alexander, M. Belisle, and J. Steele, ‘MITRE ATT&CK for industrial control systems: Design and philosophy’, *The MITRE Corporation: Bedford, MA, USA*, vol. 29, 2020.

[6] D. K. Zafra, ‘Hello From the OT Side!’, 2020.

[1] A. Di Pinto, ‘Your Guide to the MITRE ATT&CK Framework for ICS’. Nozomi Networks, Nov. 08, 2023. Accessed: Aug. 08, 2023. [Online]. Available: https://www.nozominetworks.com/blog/your-guide-to-the-mitre-attack-framework-for-ics/

[2] B. E. Strom, A. Applebaum, D. P. Miller, K. C. Nickels, A. G. Pennington, and C. B. Thomas, ‘Mitre att&ck: Design and philosophy’, in *Technical report*, The MITRE Corporation, 2018.

[3] O. Alexander, M. Belisle, and J. Steele, ‘MITRE ATT&CK for industrial control systems: Design and philosophy’, *The MITRE Corporation: Bedford, MA, USA*, vol. 29, 2020.

[4] D. K. Zafra, ‘Hello From the OT Side!’, 2020.