*Gebruikerscommissie – 28 April 2016*

# Common Industrial control systems attack methodes, targets & their consequences

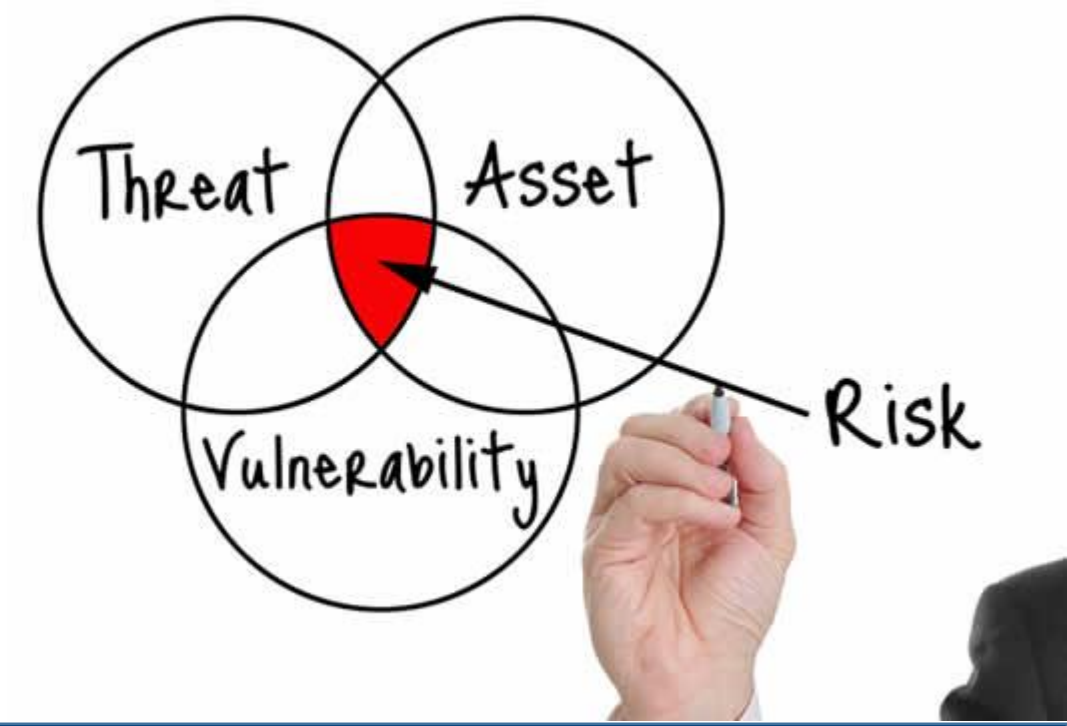
Ing. Hendrik Derre

agentschap voor Innovatie
door Wetenschap en Technologie

# Common Industrial control systems attack methodes, targets & their consequences

# Common Industrial control systems attack methodes, targets & their consequences

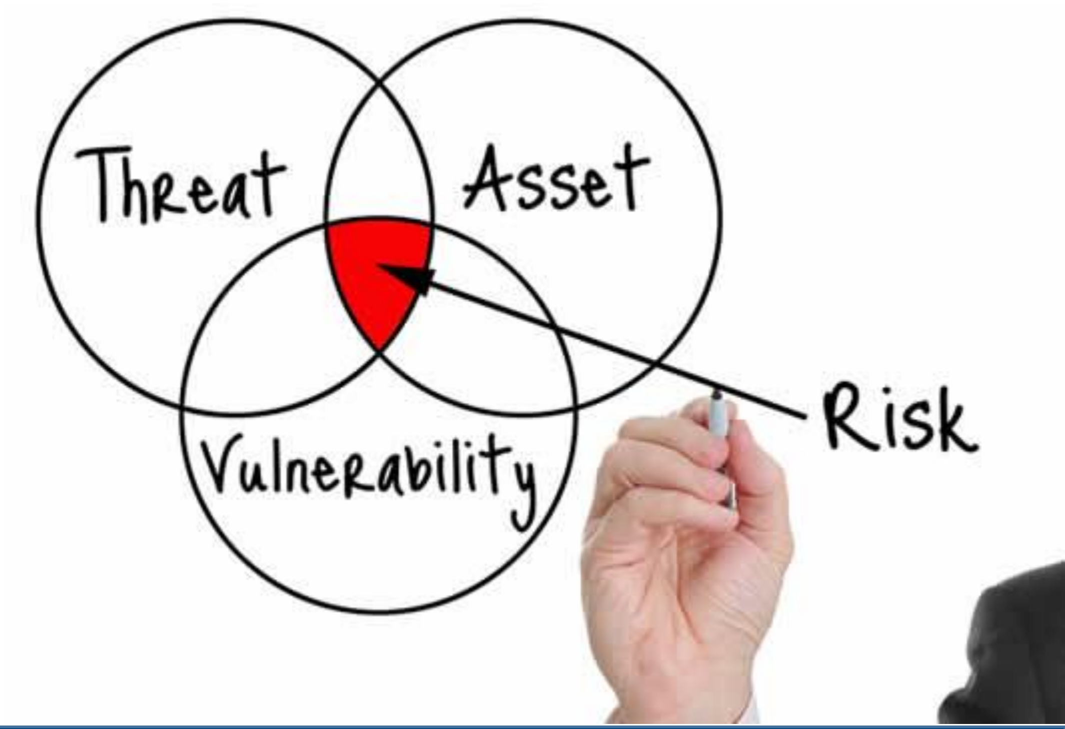
*“Risk management is the foundation of cyber security”*



# Common Industrial control systems attack methodes, targets & their consequences

**What is risk:**

- The likelihood of a give threat event
- Exercising a particular “potential” vulnerability of an asset
- With resulting consequences that impact operation of the assets



# Common Industrial control systems attack methodes, targets & their consequences

## Common ICS attack Methodes

# Common Industrial control systems attack methodes, targets & their consequences

**Common ICS Attack Methodes:**

- Man-in-the-middle attacks (MitM)
- Replay attacks
- Denial-of-service attacks (DoS)
- Compromising the HMI
- Compromising the Engineering Workstation
- Social Engineering

# Common Industrial control systems attack methodes, targets & their consequences

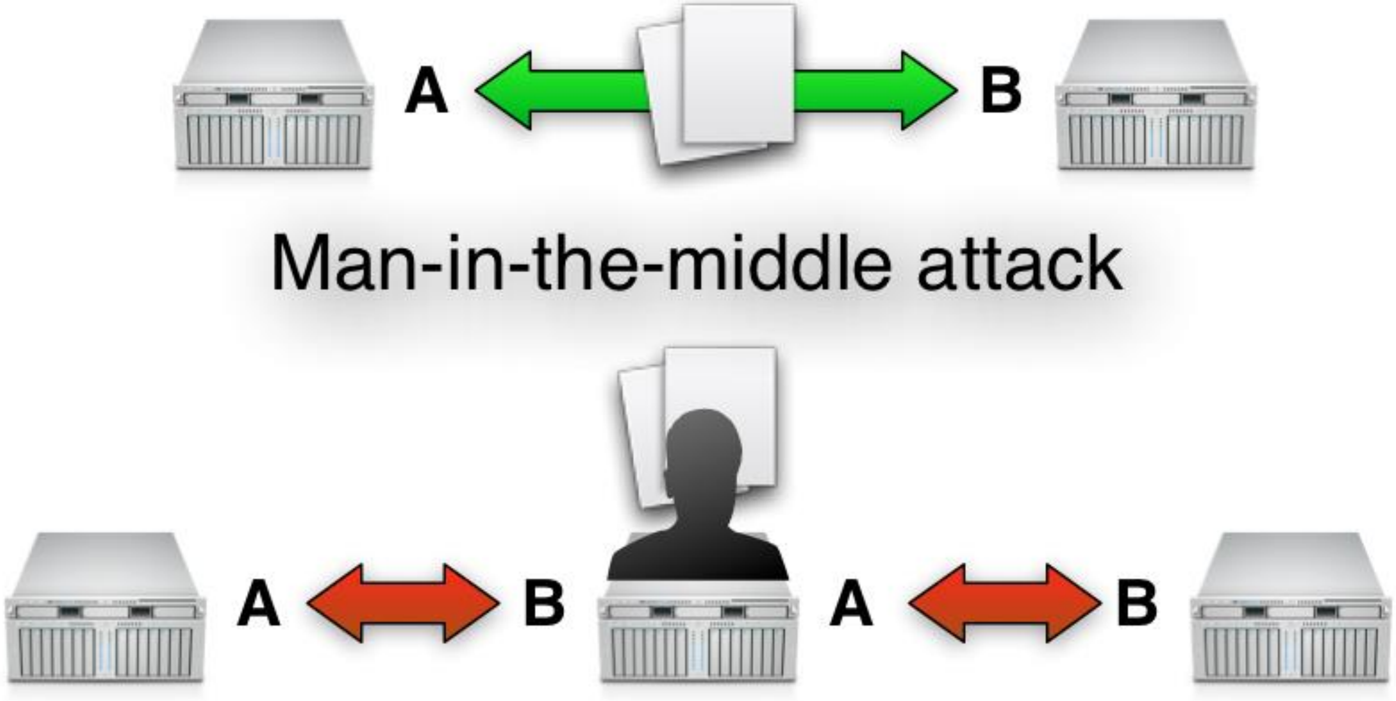
**Common ICS Attack Methodes:**

- *Man-in-the-middle attacks (MitM)*
- Replay attacks
- Denial-of-service attacks (DoS)
- Compromising the HMI
- Compromising the Engineering Workstation
- Social Engineering

# Common Industrial control systems attack methodes, targets & their consequences

**Common ICS Attack Methodes:**

- *Man-in-the-middle attacks (MitM)*



# Common Industrial control systems attack methodes, targets & their consequences

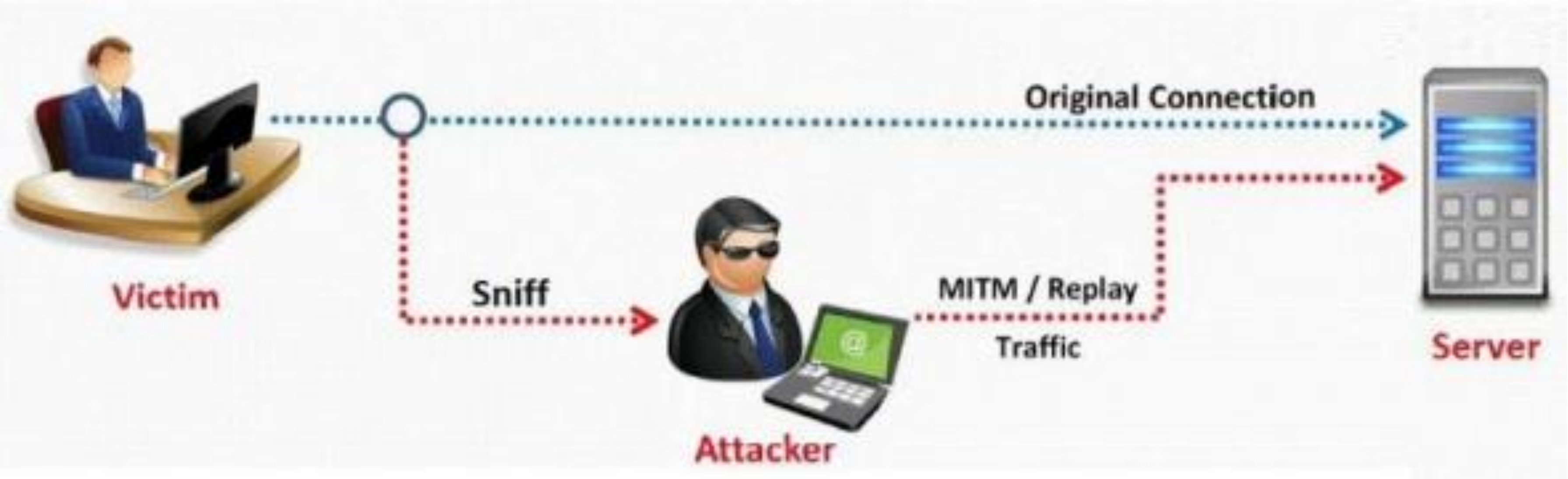
**Common ICS Attack Methodes:**

- Man-in-the-middle attacks (MitM)
- *Replay attacks*
- Denial-of-service attacks (DoS)
- Compromising the HMI
- Compromising the Engineering Workstation
- Social Engineering

# Common Industrial control systems attack methodes, targets & their consequences

**Common ICS Attack Methodes:**

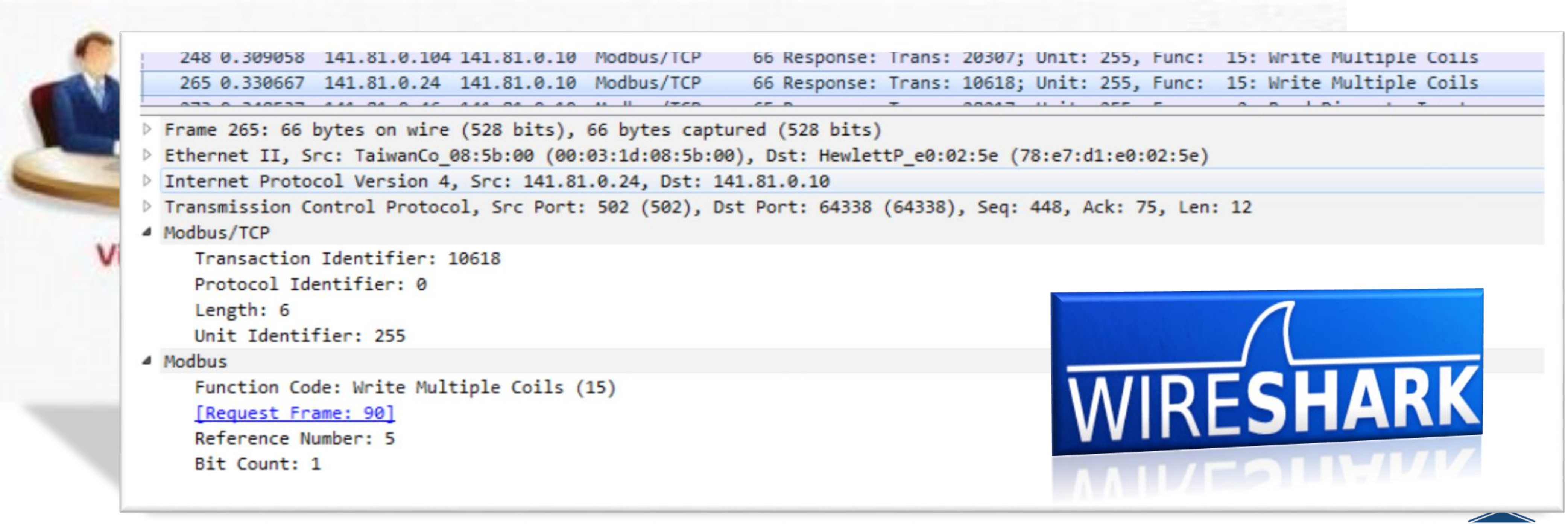
- *Replay attacks*



# Common Industrial control systems attack methodes, targets & their consequences

## Common ICS Attack Methodes:

- *Replay attacks*



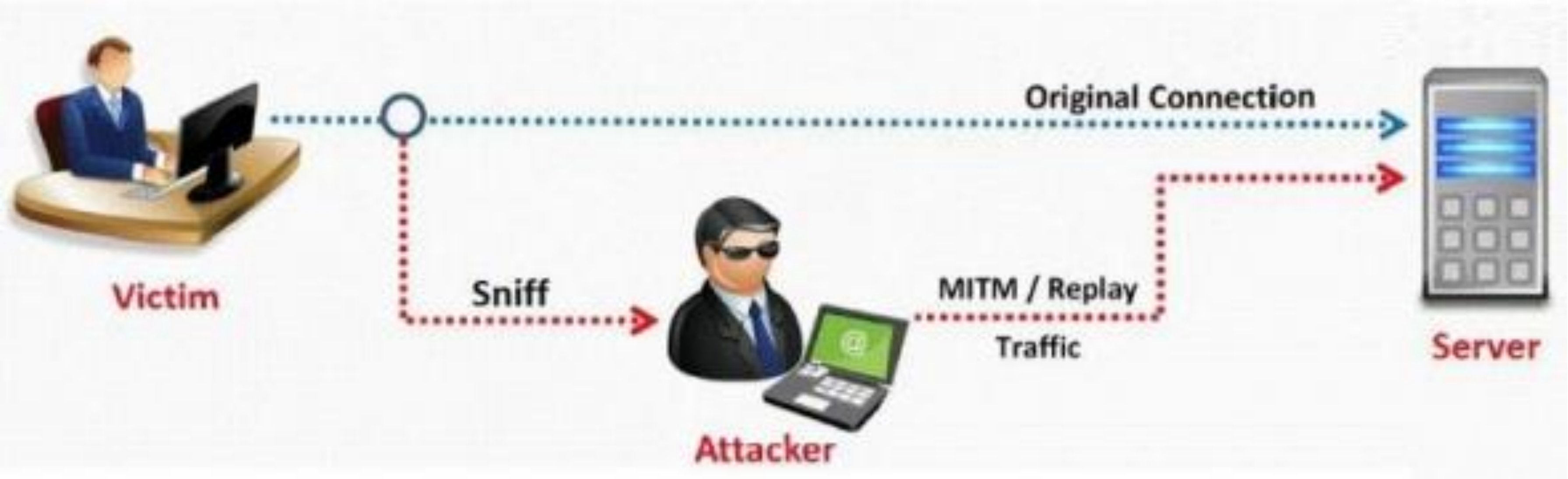
```
  248 0.309058  141.81.0.104 141.81.0.10  Modbus/TCP    66 Response: Trans: 20307; Unit: 255, Func:  15: Write Multiple Coils
  265 0.330667  141.81.0.24  141.81.0.10  Modbus/TCP    66 Response: Trans: 10618; Unit: 255, Func:  15: Write Multiple Coils

▷ Frame 265: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
▷ Ethernet II, Src: TaiwanCo_08:5b:00 (00:03:1d:08:5b:00), Dst: HewlettP_e0:02:5e (78:e7:d1:e0:02:5e)
▷ Internet Protocol Version 4, Src: 141.81.0.24, Dst: 141.81.0.10
▷ Transmission Control Protocol, Src Port: 502 (502), Dst Port: 64338 (64338), Seq: 448, Ack: 75, Len: 12
◢ Modbus/TCP
    Transaction Identifier: 10618
    Protocol Identifier: 0
    Length: 6
    Unit Identifier: 255
◢ Modbus
    Function Code: Write Multiple Coils (15)
    [Request Frame: 90]
    Reference Number: 5
    Bit Count: 1
```

# Common Industrial control systems attack methodes, targets & their consequences

**Common ICS Attack Methodes:**

- *Replay attacks*



# Common Industrial control systems attack methodes, targets & their consequences

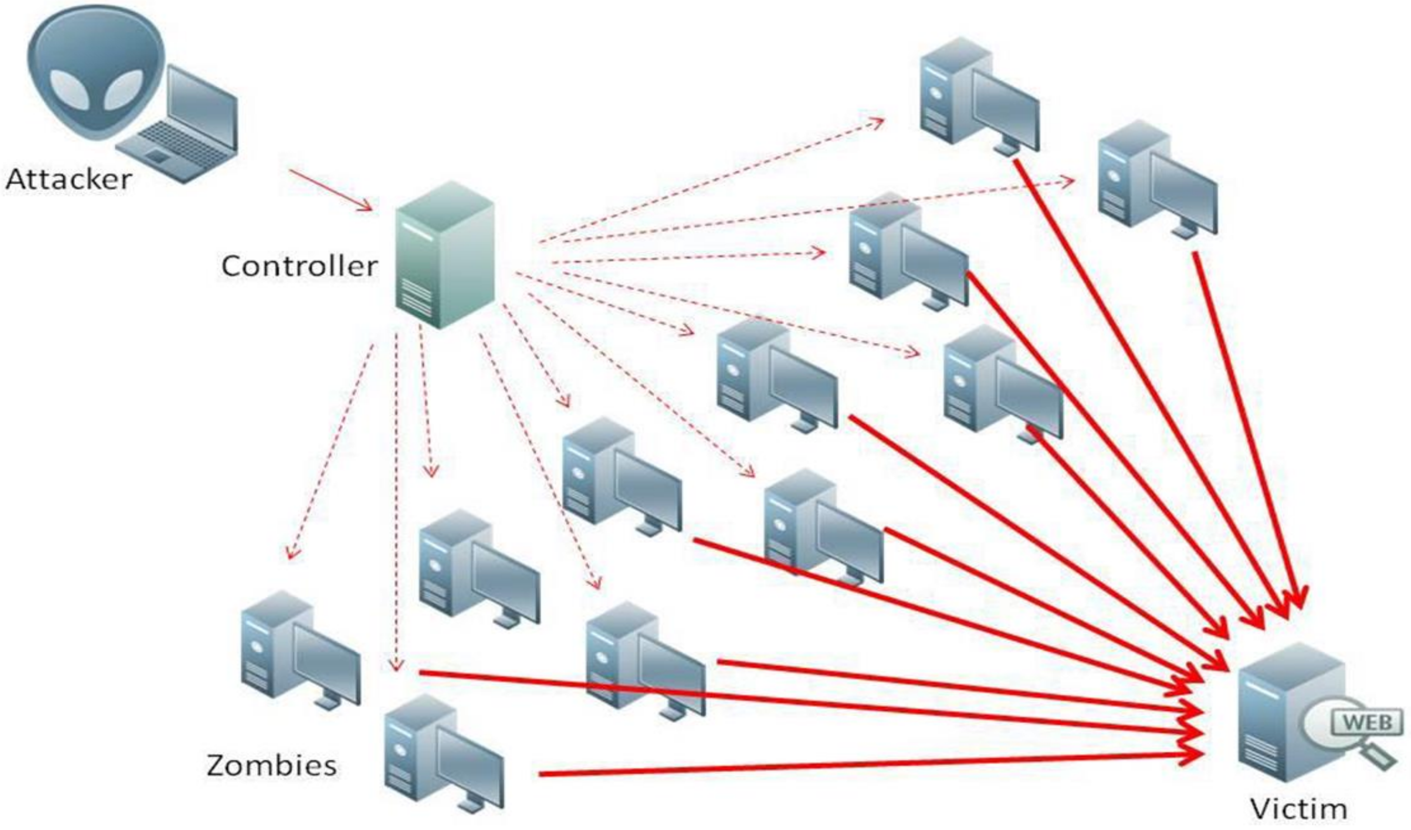
**Common ICS Attack Methodes:**

- Man-in-the-middle attacks (MitM)
- Replay attacks
- *Denial-of-service attacks (DoS)*
- Compromising the HMI
- Compromising the Engineering Workstation
- Social Engineering

# Common Industrial control systems attack methodes, targets & their consequences

## Common ICS Attack Methodes:

- *Denial-of-service attacks (DoS)*



# Common Industrial control systems attack methodes, targets & their consequences

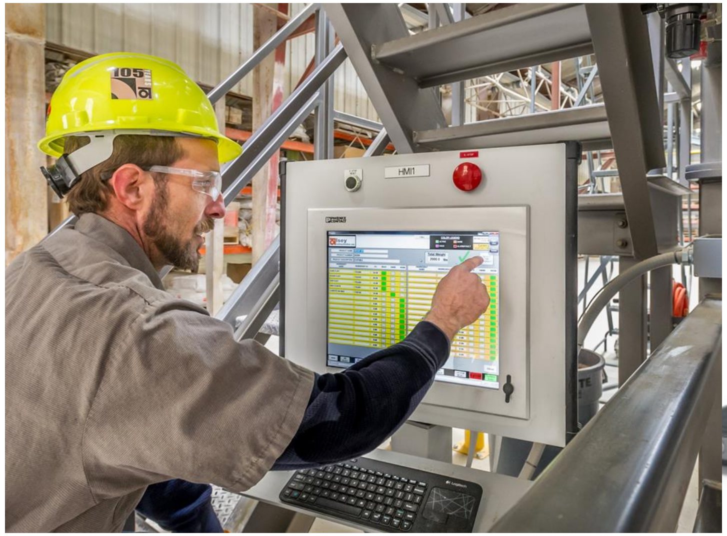
**Common ICS Attack Methodes:**

- Man-in-the-middle attacks (MitM)
- Replay attacks
- Denial-of-service attacks (DoS)
- *<u>Compromising the HMI</u>*
- *<u>Compromising the Engineering Workstation</u>*
- Social Engineering

# Common Industrial control systems attack methodes, targets & their consequences

**Common ICS Attack Methodes:**

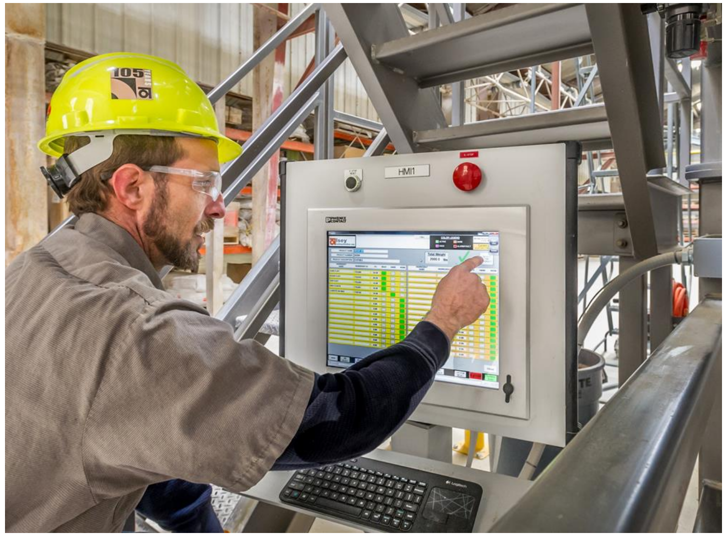
- *Compromising the HMI*
- *Compromising the Engineering Workstation*

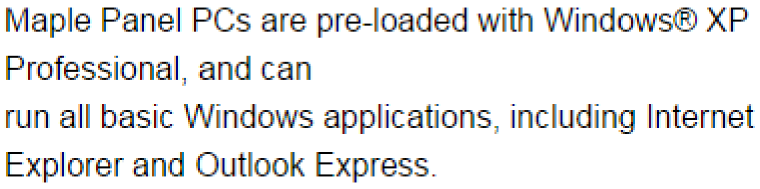


# Common Industrial control systems attack methodes, targets & their consequences

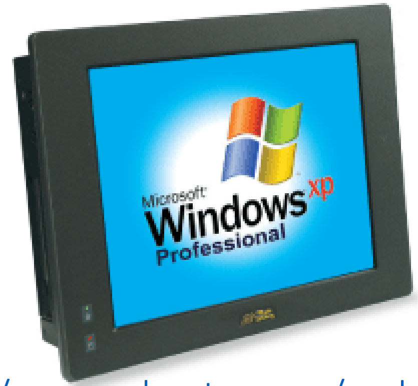
## Common ICS Attack Methodes:

- *Compromising the HMI*
- *Compromising the Engineering Workstation*





Maple Panel PCs are pre-loaded with Windows® XP Professional, and can run all basic Windows applications, including Internet Explorer and Outlook Express.



http://www.maplesystems.com/products/panel-pc/software.htm

# Common Industrial control systems attack methodes, targets & their consequences

## Common ICS Attack Methodes:

- *Compromising the HMI*
- *Compromising the Engineering Workstation*

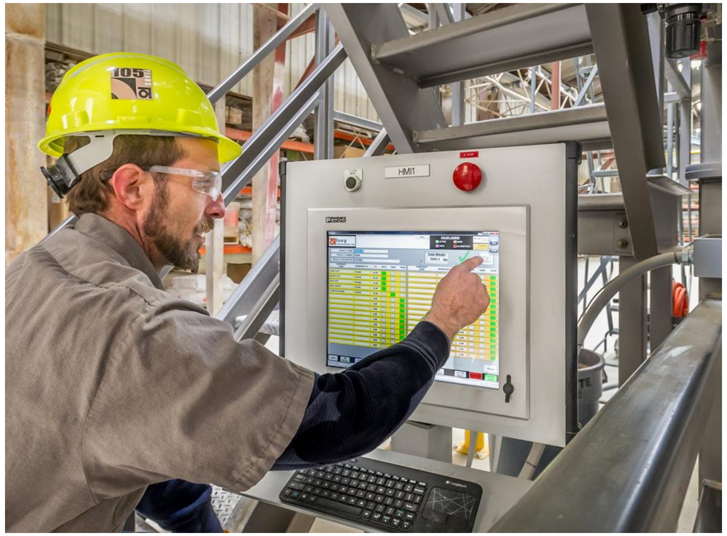
Maple Panel PCs are pre-loaded with Windows® XP Professional, and can
run all basic Windows applications, including Internet

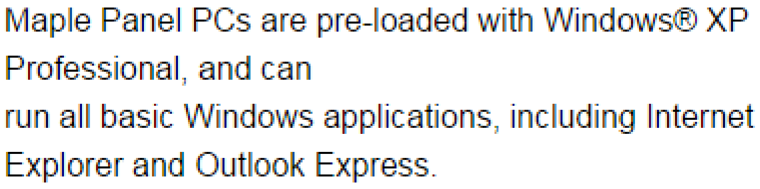
http://www.maplesystems.com/products/panel-pc/software.htm

# Common Industrial control systems attack methodes, targets & their consequences

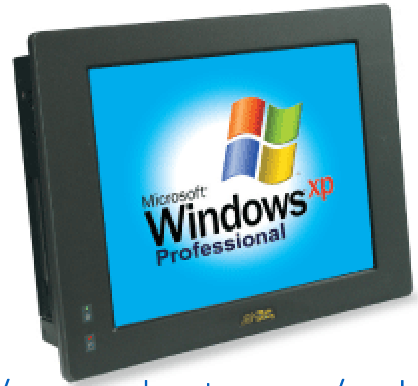
**Common ICS Attack Methodes:**

- *Compromising the HMI*
- *Compromising the Engineering Workstation*





Maple Panel PCs are pre-loaded with Windows® XP Professional, and can
run all basic Windows applications, including Internet Explorer and Outlook Express.



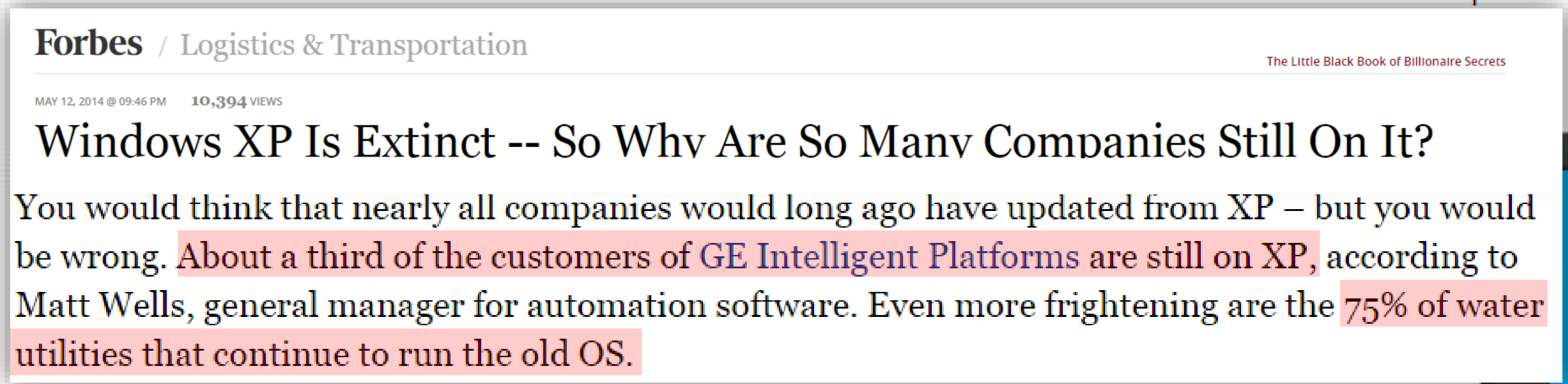
http://www.maplesystems.com/products/panel-pc/software.htm

# Common Industrial control systems attack methodes, targets & their consequences

## Common ICS Attack Methodes:

- *Compromising the HMI*
- *Compromising the Engineering Workstation*

Maple Panel PCs are pre-loaded with Windows® XP Professional, and can
run all basic Windows applications, including Internet Explorer and Outlook Express.



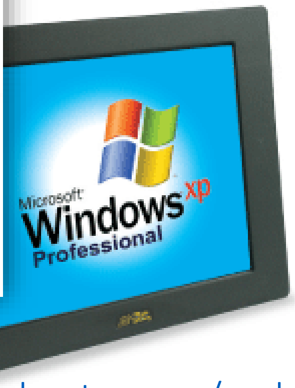
**Forbes** / Logistics & Transportation

The Little Black Book of Billionaire Secrets

MAY 12, 2014 @ 09:46 PM 10,394 VIEWS

### Windows XP Is Extinct -- So Why Are So Many Companies Still On It?

You would think that nearly all companies would long ago have updated from XP – but you would be wrong. About a third of the customers of GE Intelligent Platforms are still on XP, according to Matt Wells, general manager for automation software. Even more frightening are the 75% of water utilities that continue to run the old OS.



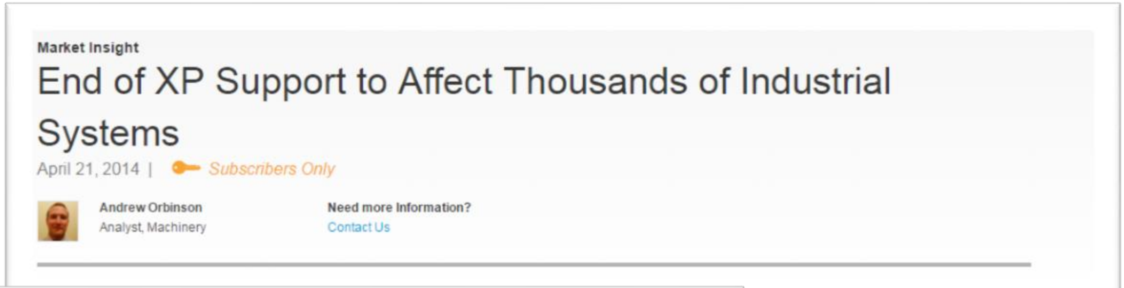
http://www.forbes.com/sites/robertbowman/2014/05/12/windows-xp-is-extinct-so-why-are-so-many-companies-still-on

http://www.maplesystems.com/products/panel-pc/software.htm

# Common Industrial control systems attack methodes, targets & their consequences

**Common ICS Attack Methodes:**

- *Compromising the HMI*
- *Compromising the Engineering Workstation*



Market Insight

End of XP Support to Affect Thousands of Industrial Systems

April 21, 2014 | Subscribers Only

Andrew Orbinson
Analyst, Machinery

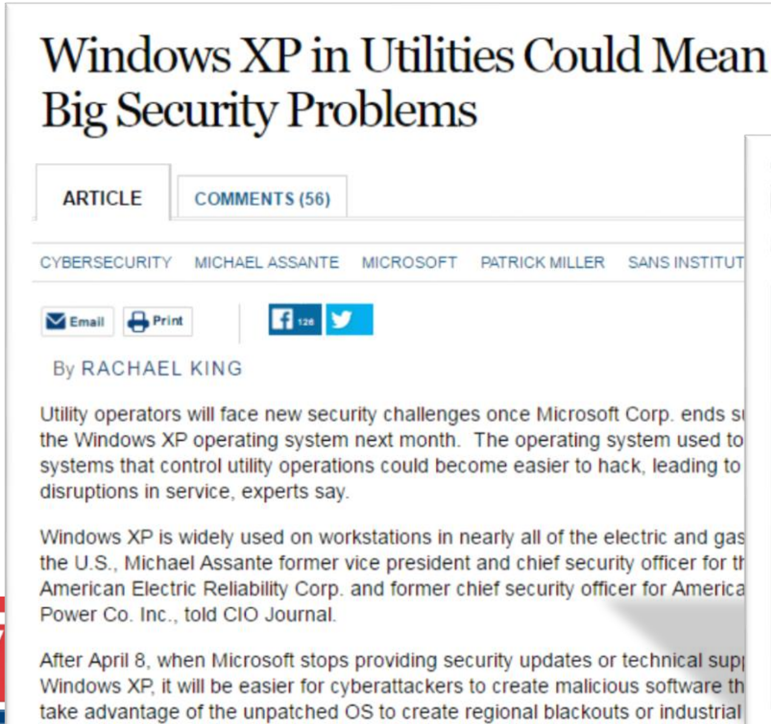
Need more Information?
Contact Us

h security updates or technical support for

cted, and it is important that you migrate to

many companies that have implemented
is most widely used in industrial automation,
users.

thout the ongoing security updates to
ating system. Such threats exist to
distributed control systems (DCS).



## Windows XP in Utilities Could Mean Big Security Problems

ARTICLE | COMMENTS (56)

CYBERSECURITY MICHAEL ASSANTE MICROSOFT PATRICK MILLER SANS INSTITUT

By RACHAEL KING

Utility operators will face new security challenges once Microsoft Corp. ends su the Windows XP operating system next month. The operating system used to systems that control utility operations could become easier to hack, leading to disruptions in service, experts say.

Windows XP is widely used on workstations in nearly all of the electric and gas the U.S., Michael Assante former vice president and chief security officer for th American Electric Reliability Corp. and former chief security officer for America Power Co. Inc., told CIO Journal.

After April 8, when Microsoft stops providing security updates or technical sup Windows XP, it will be easier for cyberattackers to create malicious software th take advantage of the unpatched OS to create regional blackouts or industrial

ECH

## Windows XP: Old Platforms Die Hard, Security Risks Live On

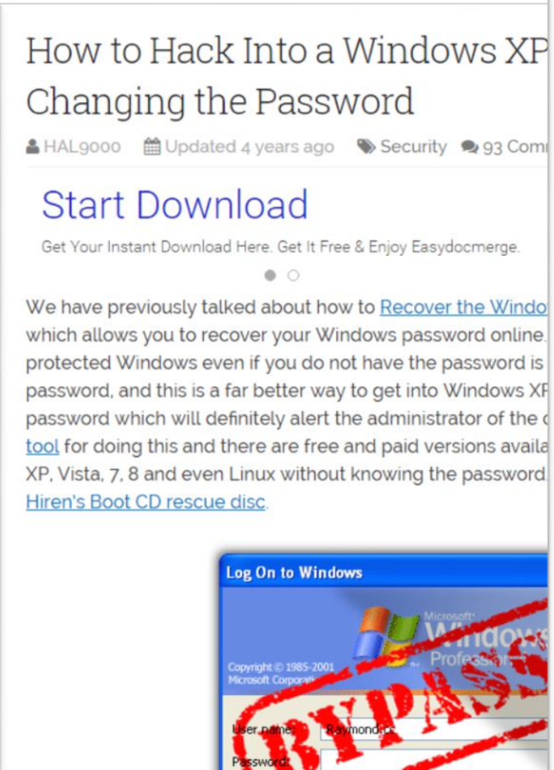
tilities, Banks Have Been Slow to Upgrade Machines, ATMs

Microsoft Windows xp Professional
Microsoft Windows xp Professional
Microsoft Windows xp Professional
For professional clients only.
Invesco Euro Equity Fund*
Invesco Euro Structured Equity Fund*

# Common Industrial control systems attack methodes, targets & their consequences

## Common ICS Attack Methodes:

- *Compromising the HMI*
- *Compromising the Engineering Workstation*



How to Hack Into a Windows XP
Changing the Password

HAL9000 Updated 4 years ago Security 93 Com

Start Download

Get Your Instant Download Here. Get It Free & Enjoy Easydocmerge.

We have previously talked about how to Recover the Windo
which allows you to recover your Windows password online.
protected Windows even if you do not have the password is
password, and this is a far better way to get into Windows XP
password which will definitely alert the administrator of the c
tool for doing this and there are free and paid versions availa
XP, Vista, 7, 8 and even Linux without knowing the password.
Hiren's Boot CD rescue disc.

Log On to Windows
Microsoft Windows Professional
Copyright © 1985-2001 Microsoft Corporation
User name: Raymond.cc
Password:
BYPASS

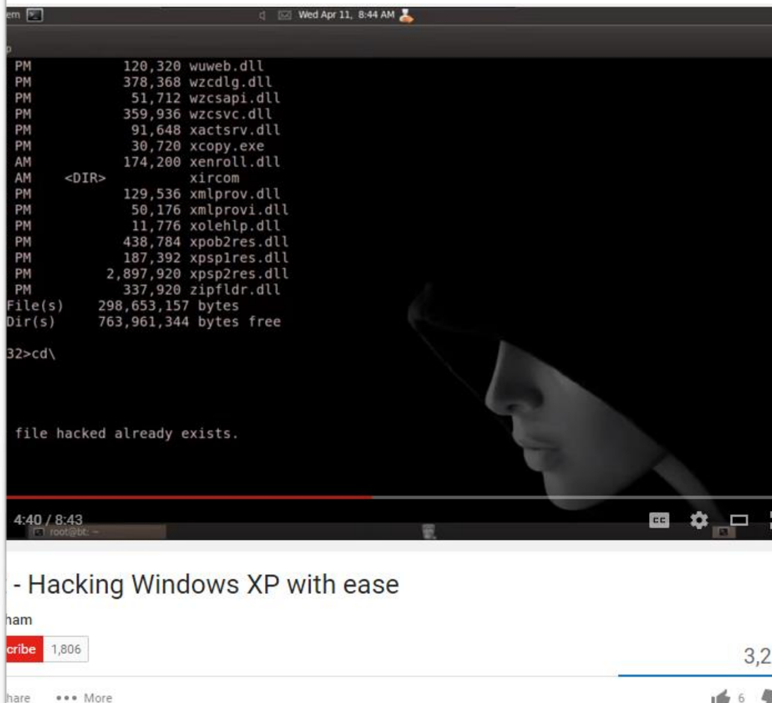
Hack Like a Pro: How to Exploit and Gain Remote Access to PCs Running Windows XP

Posted By occupytheweb 17K 2 years ago

Free WLAN Buyer's Pack
Find The Appropriate WLAN Solution For Your Organization Through 2016.

In my first installment in this series on professional hacking tools, we downloaded and installed Metasploit, the exploitation framework. Now, we will begin to explore the Metasploit Framework and initiate a tried and true hack.

Before we start hacking, let's familiarize ourselves with Metasploit so that when I use certain terms, we all understand them to mean the same thing. When first looking at the Metasploit Framework, it can be a bit



```
 PM           120,320 wuweb.dll
 PM           378,368 wzcdlg.dll
 PM            51,712 wzcsapi.dll
 PM           359,936 wzcsvc.dll
 PM            91,648 xactsrv.dll
 PM            30,720 xcopy.exe
 AM           174,200 xenroll.dll
 AM    <DIR>          xircom
 PM           129,536 xmlprov.dll
 PM            50,176 xmlprovi.dll
 PM            11,776 xolehlp.dll
 PM           438,784 xpob2res.dll
 PM           187,392 xpsp1res.dll
 PM         2,897,920 xpsp2res.dll
 PM           337,920 zipfldr.dll
File(s)    298,653,157 bytes
Dir(s)     763,961,344 bytes free

32>cd\



 file hacked already exists.
```

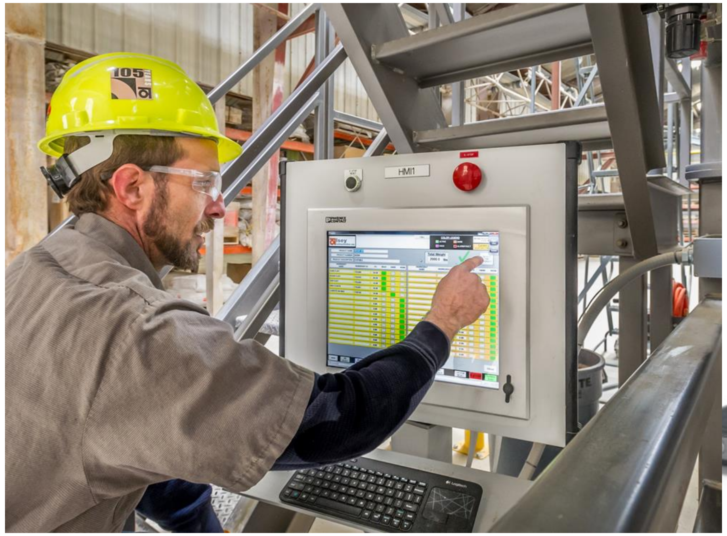
- Hacking Windows XP with ease

ham

# Common Industrial control systems attack methodes, targets & their consequences

**Common ICS Attack Methodes:**

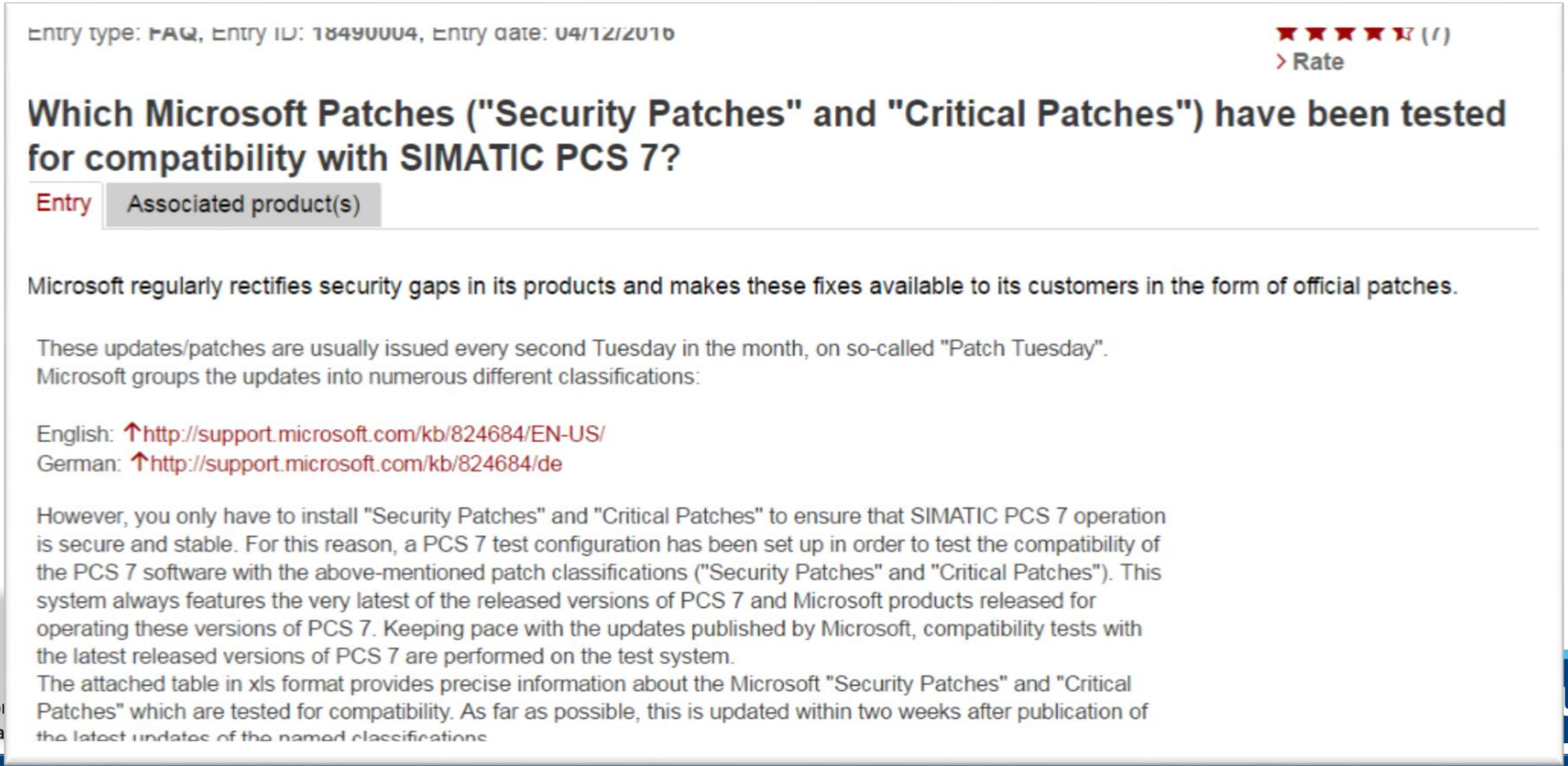
- *Compromising the HMI*
- *Compromising the Engineering Workstation*



# Common Industrial control systems attack methodes, targets & their consequences

**Common ICS Attack Methodes:**

- *Compromising the HMI*
- *Compromising the Engineering Workstation*



Entry type: FAQ, Entry ID: 18490004, Entry date: 04/12/2016

★★★★☆ (7)
› Rate

## Which Microsoft Patches ("Security Patches" and "Critical Patches") have been tested for compatibility with SIMATIC PCS 7?

Microsoft regularly rectifies security gaps in its products and makes these fixes available to its customers in the form of official patches.

These updates/patches are usually issued every second Tuesday in the month, on so-called "Patch Tuesday".
Microsoft groups the updates into numerous different classifications:

English: ↑http://support.microsoft.com/kb/824684/EN-US/
German: ↑http://support.microsoft.com/kb/824684/de

However, you only have to install "Security Patches" and "Critical Patches" to ensure that SIMATIC PCS 7 operation is secure and stable. For this reason, a PCS 7 test configuration has been set up in order to test the compatibility of the PCS 7 software with the above-mentioned patch classifications ("Security Patches" and "Critical Patches"). This system always features the very latest of the released versions of PCS 7 and Microsoft products released for operating these versions of PCS 7. Keeping pace with the updates published by Microsoft, compatibility tests with the latest released versions of PCS 7 are performed on the test system.
The attached table in xls format provides precise information about the Microsoft "Security Patches" and "Critical Patches" which are tested for compatibility. As far as possible, this is updated within two weeks after publication of the latest updates of the named classifications.

# Common Industrial control systems attack methodes, targets & their consequences

**Common ICS Attack Methodes:**

- Man-in-the-middle attacks (MitM)
- Replay attacks
- Denial-of-service attacks (DoS)
- Compromising the HMI
- Compromising the Engineering Workstation
- *Social Engineering*

# Common Industrial control systems attack methodes, targets & their consequences

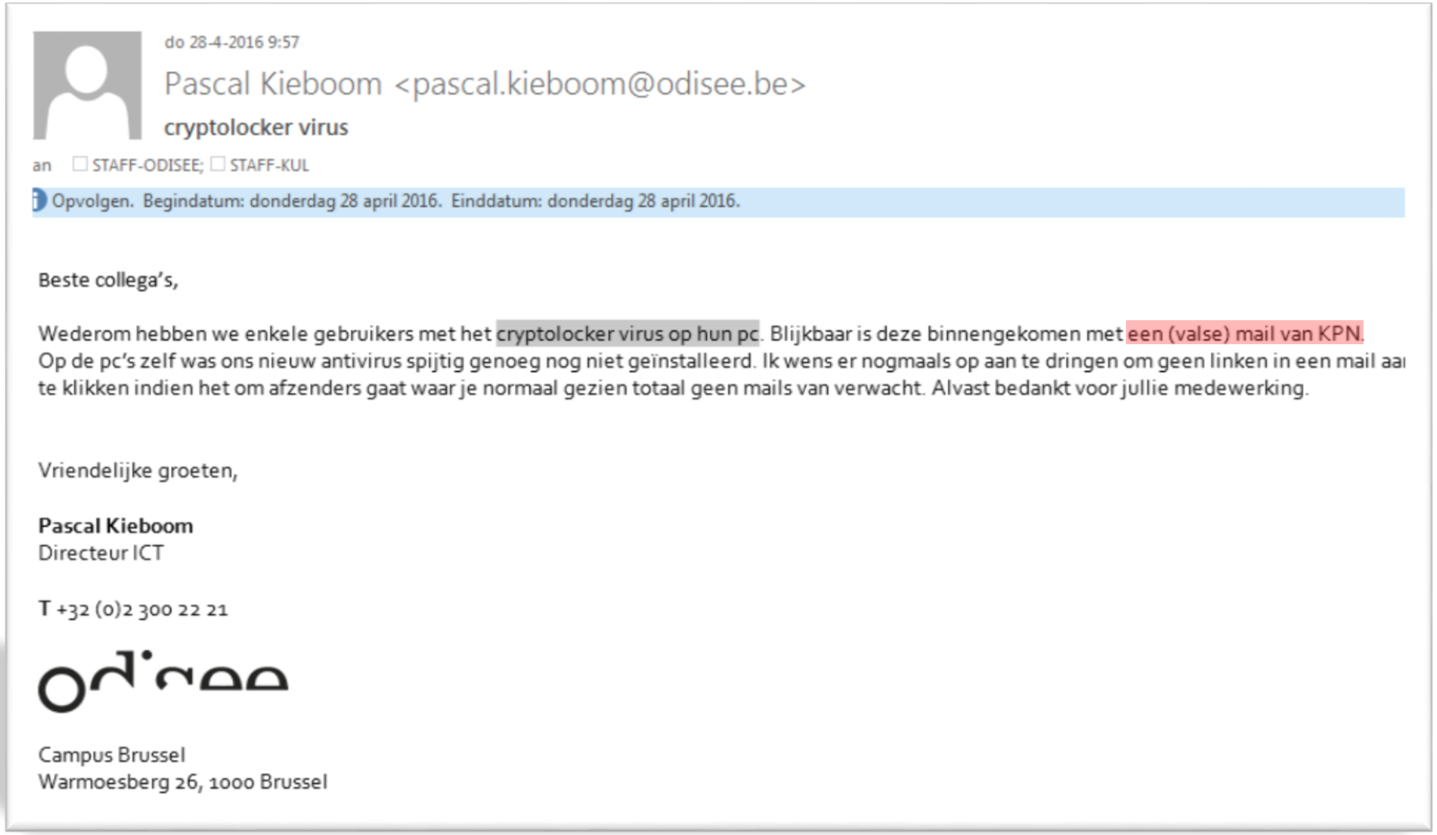
**Common ICS Attack Methodes:**

- *Social Engineering*
  - Phishing
  - Spear Phishing
  - Vishing (voice)
  - Smishing (sms)
  - Mining Social media
  - …

# Common Industrial control systems attack methodes, targets & their consequences

## Common ICS Attack Methodes:

- *Social Engineering*
  - **Phishing**
  - Spear Phishing
  - Vishing (voice)
  - Smishing (sms)
  - Mining Social media
  - …



do 28-4-2016 9:57

Pascal Kieboom <pascal.kieboom@odisee.be>

cryptolocker virus

an □ STAFF-ODISEE; □ STAFF-KUL

Opvolgen. Begindatum: donderdag 28 april 2016. Einddatum: donderdag 28 april 2016.

Beste collega's,

Wederom hebben we enkele gebruikers met het cryptolocker virus op hun pc. Blijkbaar is deze binnengekomen met een (valse) mail van KPN. Op de pc's zelf was ons nieuw antivirus spijtig genoeg nog niet geïnstalleerd. Ik wens er nogmaals op aan te dringen om geen linken in een mail aa te klikken indien het om afzenders gaat waar je normaal gezien totaal geen mails van verwacht. Alvast bedankt voor jullie medewerking.

Vriendelijke groeten,

**Pascal Kieboom**
Directeur ICT

T +32 (0)2 300 22 21

Campus Brussel
Warmoesberg 26, 1000 Brussel

# Common Industrial control systems attack methodes, targets & their consequences

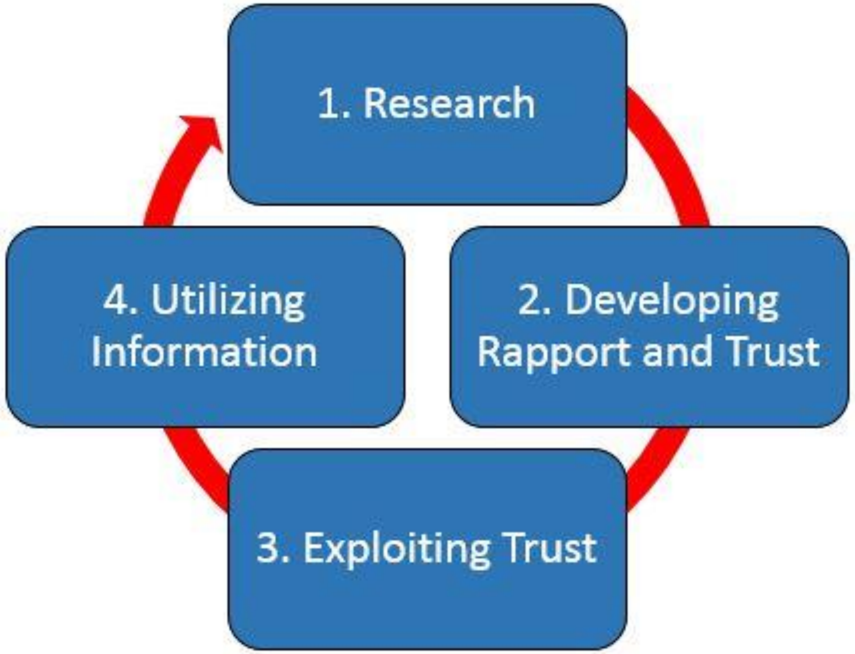
**Common ICS Attack Methodes:**

- *Social Engineering*
  - Phishing
  - Spear Phishing
  - Vishing (voice)
  - Smishing (sms)
  - Mining Social media
  - …

# Common Industrial control systems attack methodes, targets & their consequences

**Common ICS Attack Methodes:**

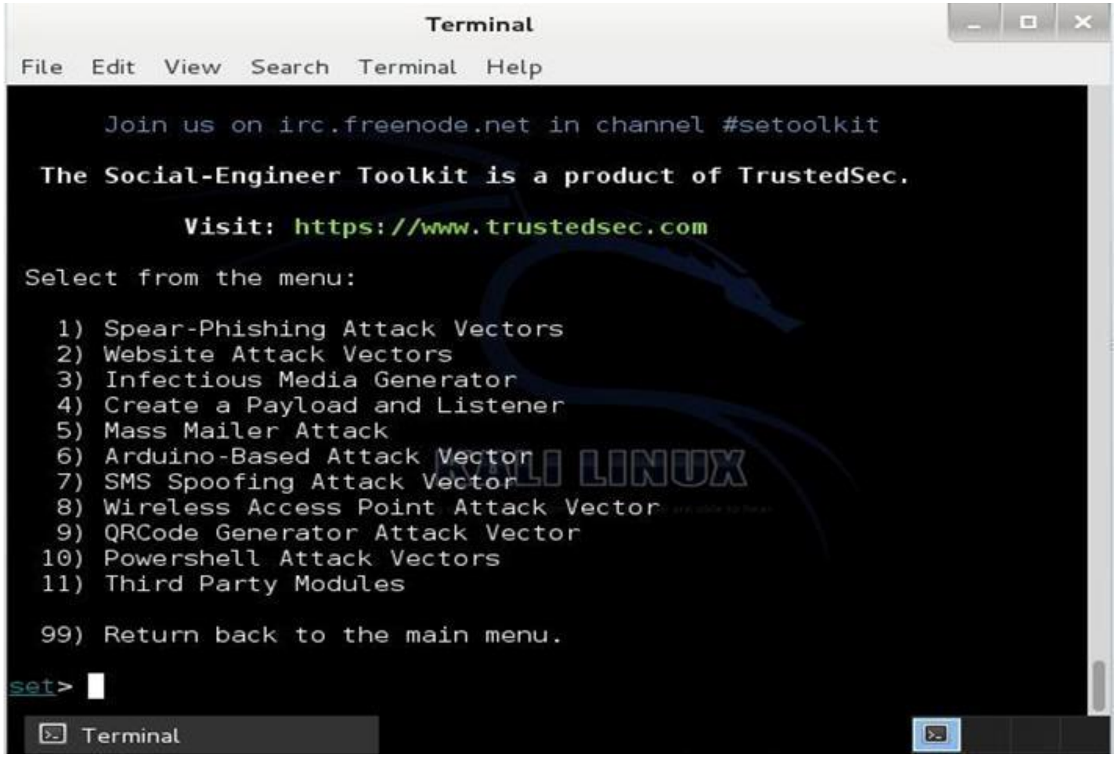
- *Social Engineering*



# Common Industrial control systems attack methodes, targets & their consequences

## Common ICS Attack Methodes:

- *Social Engineering*



```
     Join us on irc.freenode.net in channel #setoolkit

 The Social-Engineer Toolkit is a product of TrustedSec.

           Visit: https://www.trustedsec.com

Select from the menu:

  1) Spear-Phishing Attack Vectors
  2) Website Attack Vectors
  3) Infectious Media Generator
  4) Create a Payload and Listener
  5) Mass Mailer Attack
  6) Arduino-Based Attack Vector
  7) SMS Spoofing Attack Vector
  8) Wireless Access Point Attack Vector
  9) QRCode Generator Attack Vector
 10) Powershell Attack Vectors
 11) Third Party Modules

 99) Return back to the main menu.

set>
```

https://www.trustedsec.com/social-engineer-toolkit/

# Common Industrial control systems attack methodes, targets & their consequences

## The potential impact of succesfull cyber-attacks

# Common Industrial control systems attack methodes, targets & their consequences

**The potential impact of succesfull cyber-attacks:**

**VIEW**

- Denial of View (DoV)
- Manipulation of View (MoV)
- Loss of View (LoV)

# Common Industrial control systems attack methodes, targets & their consequences

**The potential impact of succesfull cyber-attacks:**

<u>**VIEW**</u>

- **Denial of View (DoV)**
- Manipulation of View (MoV)
- Loss of View (LoV)

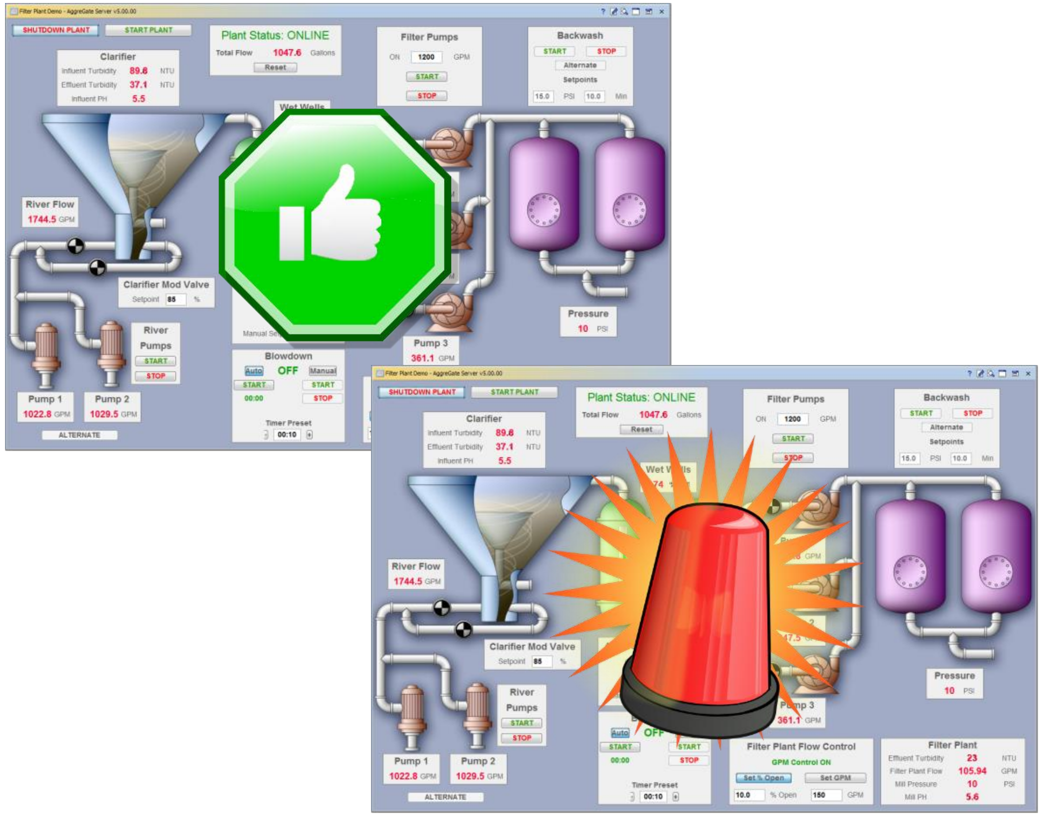
No connection

# Common Industrial control systems attack methodes, targets & their consequences

## The potential impact of succesfull cyber-attacks:

**VIEW**

- Denial of View (DoV)
- **Manipulation of View (MoV)**
- Loss of View (LoV)



agentschap voor Innovatie
door Wetenschap en Technologie

# Common Industrial control systems attack methodes, targets & their consequences

**The potential impact of succesfull cyber-attacks:**

**VIEW**

- Denial of View (DoV)
- Manipulation of View (MoV)
- **Loss of View (LoV)**

# Common Industrial control systems attack methodes, targets & their consequences

**The potential impact of succesfull cyber-attacks:**

**Control**

- Denial of Control (DoC)
- Manipulation of Control (MoC)
- Loss of Control (LoC)

# Common Industrial control systems attack methodes, targets & their consequences

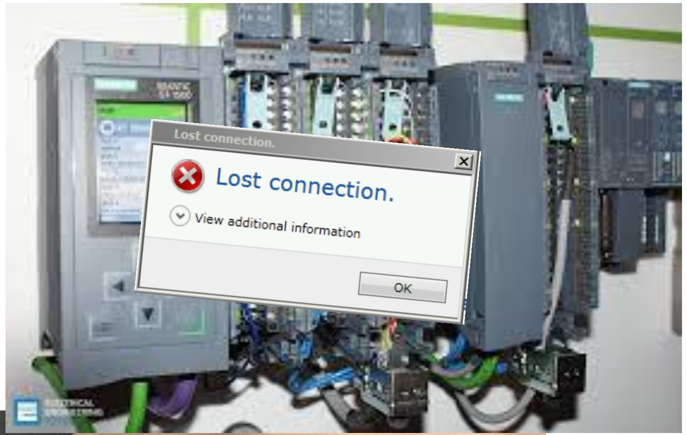
## The potential impact of succesfull cyber-attacks:

<u>Control</u>

- **Denial of Control (DoC)**

- Manipulation of Control (MoC)

- Loss of Control (LoC)



Lost connection.

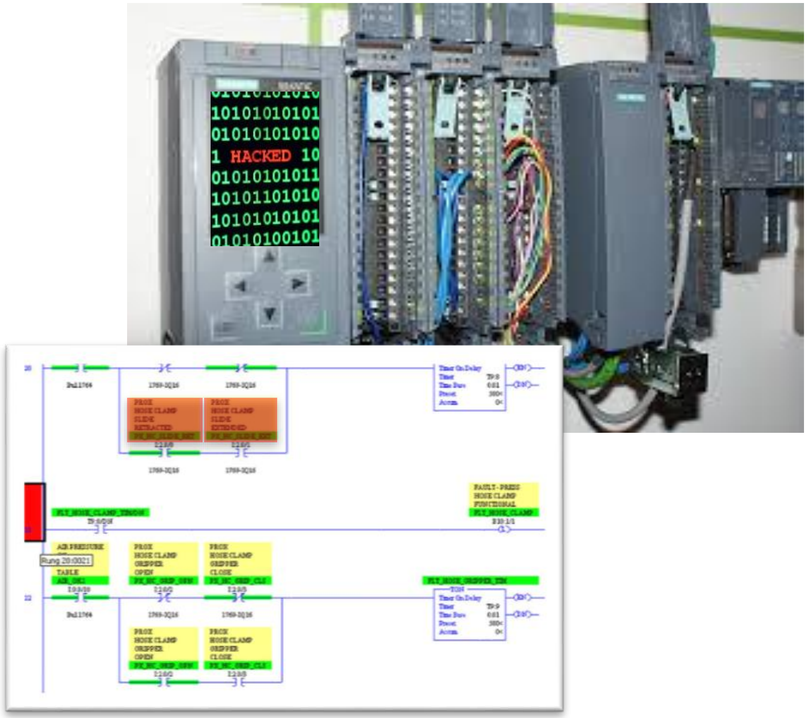
Lost connection.

View additional information

OK

# Common Industrial control systems attack methodes, targets & their consequences

**The potential impact of succesfull cyber-attacks:**



**<u>Control</u>**

- Denial of Control (DoC)
- **Manipulation of Control (MoC)**
- Loss of Control (LoC)

# Common Industrial control systems attack methodes, targets & their consequences

**The potential impact of succesfull cyber-attacks:**

<u>**Control**</u>

- Denial of Control (DoC)
- Manipulation of Control (MoC)
- **Loss of Control (LoC)**

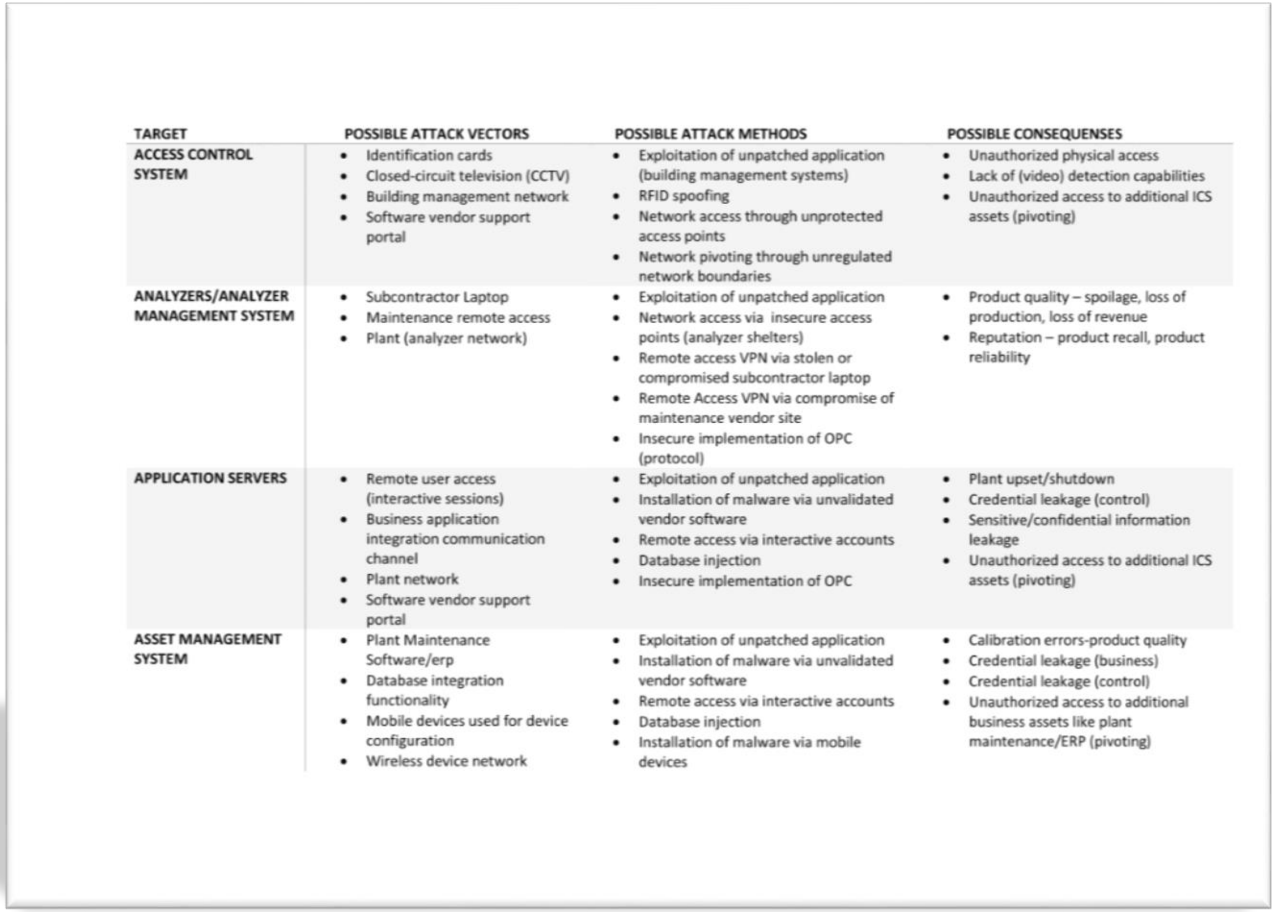
# Common Industrial control systems attack methodes, targets & their consequences

## Common ICS targets

# Common Industrial control systems attack methodes, targets & their consequences

**List of common industrial targets:**

- Access control system
- Application servers
- Condition monitoring system
- Controller (PLC)
- Data Historian
- Directory services
- Engineering workstation
- Environmental controls
- Slave devices
- Operatior workstations (HMI)
- Scada servers
- Safey systems
- User
- ….



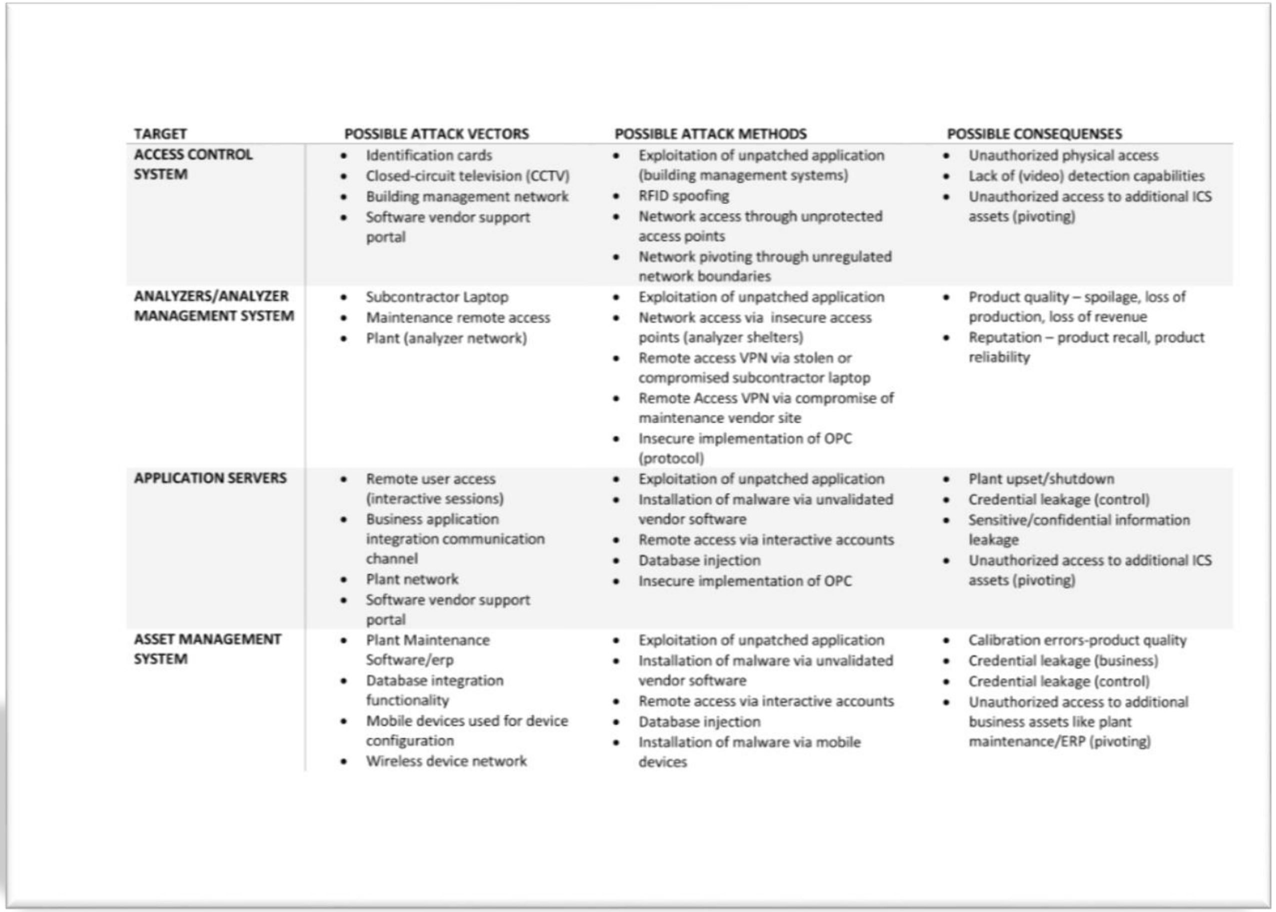
| TARGET | POSSIBLE ATTACK VECTORS | POSSIBLE ATTACK METHODS | POSSIBLE CONSEQUENSES |
|---|---|---|---|
| ACCESS CONTROL SYSTEM | • Identification cards<br>• Closed-circuit television (CCTV)<br>• Building management network<br>• Software vendor support portal | • Exploitation of unpatched application (building management systems)<br>• RFID spoofing<br>• Network access through unprotected access points<br>• Network pivoting through unregulated network boundaries | • Unauthorized physical access<br>• Lack of (video) detection capabilities<br>• Unauthorized access to additional ICS assets (pivoting) |
| ANALYZERS/ANALYZER MANAGEMENT SYSTEM | • Subcontractor Laptop<br>• Maintenance remote access<br>• Plant (analyzer network) | • Exploitation of unpatched application<br>• Network access via insecure access points (analyzer shelters)<br>• Remote access VPN via stolen or compromised subcontractor laptop<br>• Remote Access VPN via compromise of maintenance vendor site<br>• Insecure implementation of OPC (protocol) | • Product quality – spoilage, loss of production, loss of revenue<br>• Reputation – product recall, product reliability |
| APPLICATION SERVERS | • Remote user access (interactive sessions)<br>• Business application integration communication channel<br>• Plant network<br>• Software vendor support portal | • Exploitation of unpatched application<br>• Installation of malware via unvalidated vendor software<br>• Remote access via interactive accounts<br>• Database injection<br>• Insecure implementation of OPC | • Plant upset/shutdown<br>• Credential leakage (control)<br>• Sensitive/confidential information leakage<br>• Unauthorized access to additional ICS assets (pivoting) |
| ASSET MANAGEMENT SYSTEM | • Plant Maintenance Software/erp<br>• Database integration functionality<br>• Mobile devices used for device configuration<br>• Wireless device network | • Exploitation of unpatched application<br>• Installation of malware via unvalidated vendor software<br>• Remote access via interactive accounts<br>• Database injection<br>• Installation of malware via mobile devices | • Calibration errors-product quality<br>• Credential leakage (business)<br>• Credential leakage (control)<br>• Unauthorized access to additional business assets like plant maintenance/ERP (pivoting) |

# Common Industrial control systems attack methodes, targets & their consequences

**List of common industrial targets:**
*PDF listing for each target*

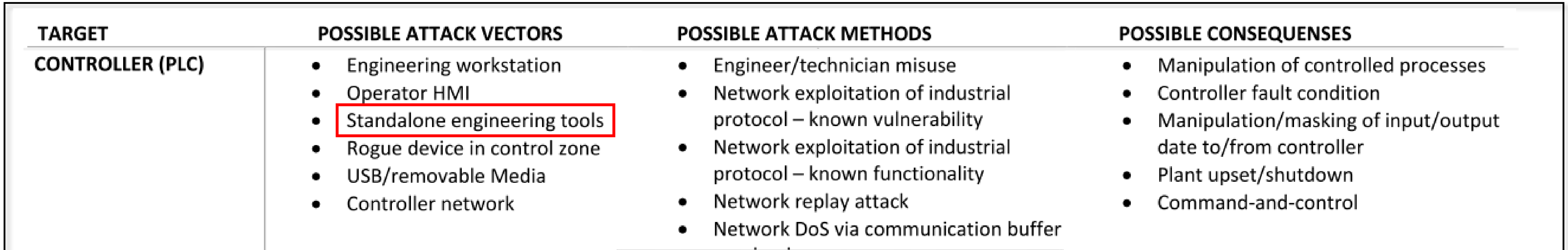
- Possible Attack Vectors
- Possible Attack Methods
- Possible Consequences

ICS Attack Targets.pdf

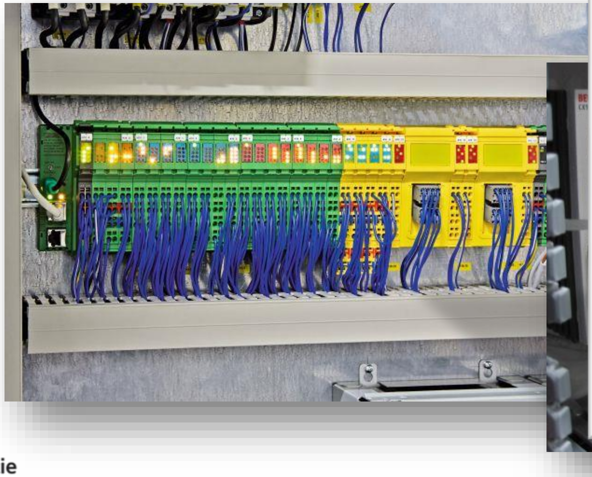


| TARGET | POSSIBLE ATTACK VECTORS | POSSIBLE ATTACK METHODS | POSSIBLE CONSEQUENSES |
|---|---|---|---|
| **ACCESS CONTROL SYSTEM** | • Identification cards<br>• Closed-circuit television (CCTV)<br>• Building management network<br>• Software vendor support portal | • Exploitation of unpatched application (building management systems)<br>• RFID spoofing<br>• Network access through unprotected access points<br>• Network pivoting through unregulated network boundaries | • Unauthorized physical access<br>• Lack of (video) detection capabilities<br>• Unauthorized access to additional ICS assets (pivoting) |
| **ANALYZERS/ANALYZER MANAGEMENT SYSTEM** | • Subcontractor Laptop<br>• Maintenance remote access<br>• Plant (analyzer network) | • Exploitation of unpatched application<br>• Network access via  insecure access points (analyzer shelters)<br>• Remote access VPN via stolen or compromised subcontractor laptop<br>• Remote Access VPN via compromise of maintenance vendor site<br>• Insecure implementation of OPC (protocol) | • Product quality – spoilage, loss of production, loss of revenue<br>• Reputation – product recall, product reliability |
| **APPLICATION SERVERS** | • Remote user access (interactive sessions)<br>• Business application integration communication channel<br>• Plant network<br>• Software vendor support portal | • Exploitation of unpatched application<br>• Installation of malware via unvalidated vendor software<br>• Remote access via interactive accounts<br>• Database injection<br>• Insecure implementation of OPC | • Plant upset/shutdown<br>• Credential leakage (control)<br>• Sensitive/confidential information leakage<br>• Unauthorized access to additional ICS assets (pivoting) |
| **ASSET MANAGEMENT SYSTEM** | • Plant Maintenance Software/erp<br>• Database integration functionality<br>• Mobile devices used for device configuration<br>• Wireless device network | • Exploitation of unpatched application<br>• Installation of malware via unvalidated vendor software<br>• Remote access via interactive accounts<br>• Database injection<br>• Installation of malware via mobile devices | • Calibration errors-product quality<br>• Credential leakage (business)<br>• Credential leakage (control)<br>• Unauthorized access to additional business assets like plant maintenance/ERP (pivoting) |

# Common Industrial control systems attack methodes, targets & their consequences



| TARGET | POSSIBLE ATTACK VECTORS | POSSIBLE ATTACK METHODS | POSSIBLE CONSEQUENSES |
|---|---|---|---|
| CONTROLLER (PLC) | • Engineering workstation<br>• Operator HMI<br>• Standalone engineering tools<br>• Rogue device in control zone<br>• USB/removable Media<br>• Controller network | • Engineer/technician misuse<br>• Network exploitation of industrial protocol – known vulnerability<br>• Network exploitation of industrial protocol – known functionality<br>• Network replay attack<br>• Network DoS via communication buffer | • Manipulation of controlled processes<br>• Controller fault condition<br>• Manipulation/masking of input/output date to/from controller<br>• Plant upset/shutdown<br>• Command-and-control |



# Common Industrial control systems attack methodes, targets & their consequences