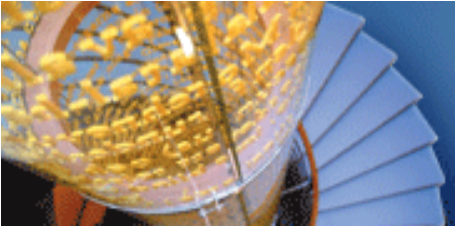


HALMSTAD UNIVERSITY

Hot, aktörer och metoder
Lektion 2

Urban Bilstrup

E 508

Urban.Bilstrup@ide.hh.se

Outline

- Aktörer
- Effektmatris
- Advanced Persistent Threats
- Cyberwar
- Konsekvenser
- Sannolikhet v.s Konsekvens
- Säkerhet i Industriella Nätverk
- Sårbarhets och Risk Bedömning
- Attack process

Fyra Aktörer*

”Dagens och framförallt morgondagens IT-angrepp kommer från resursstarka och kunniga aktörer. Dessa har uttalade mål och syften med sina angrepp, till exempel underrättelseinhämtning, ekonomisk brottslighet, industrispionage och olika former av påverkan (sabotage och utslagning av hela samhällsfunktioner). **Det är viktigt att ha god kunskap om aktörerna för att kunna bekämpa It-angrepp på ett effektivt sätt**.”* Aktörerna kan delas in i fyra grupper:

- 1. Främmande makt
- 2. Organiserad brottslighet
- 3. Terrorister
- 4. Enskilda aktörer

*Trender och utmaningar idag och imorgon, FRA

Främmande makt

Idag är det offentligt att många nationer förbereder sina försvarsorganisationer för framtida storskaligt ”cyber krig”, för att förstå omfattningen av den här aktiviteten skall man beakta att exempelvis Amerikanska flygvapnet (USAF) har inrättat en ny division (24th air force) som omfattar 6000-8000 personer som är dedikerade cyberkrigare (cyber warriors). Det här kan uppfattas som ren science fiction men är officiella fakta. Amerikanska flygvapnet ändrade 2005 sin uppdragsdefinition till att omfatta cyberspace, “The mission of the United States Air Force is to deliver sovereign options for the defense of the United States of America and its global interests – to fly and fight in Air, Space and Cyberspace”. Ett annat exempel är att Nord Korea, som Internetsammanhang brukas se som ett svart hål, har flera militära enheter för cyberkrigsföring omfattande ett tusental personer. Liknande kapaciteter finns i Kina, Ryssland, Israel osv., hur dessa är organiserade och vilka uppgifter de har är mera oklart. Att en del länder utför kvalificerat industrispionage står också utan allt tvivel, under en offensiv hacker attack troligen från Kina kallad ”Titan rain” laddades det ner mellan 10 och 20 terrabyte (10 000 - 20 000 gigabyte) av information från Pentagon och olika företag kopplade till den Amerikanska försvarsindustrin.

Se 24th AIR FORCE hemsida, http://www.24af.af.mil/index.as (120102)
http://www.af.mil/news/story.asp?id=123013440 (120102)
R.A. Clarke och R. K. Knake, Cyber war – The next threat to national security and what to do about it, HarperCollins Publisher, 2010.
J. McNamara Secrets of Computer Espionage – Tactics and Countermeasures, Wiley, 2003.
R.A. Clarke och R. K. Knake, Cyber war – The next threat to national security and what to do about it, HarperCollins Publisher, 2010.

Organiserad brottslighet

Den organiserade brottslighetens aktiviteter vad gäller dataintrång är förmodligen relativt begränsade i Sverige, det finns dock tecken på en förändring. ”[Bosse] Norgren uppskattar de riktigt vassa blågula hackarna till en handfull och säger att en del av dem "anlitas" av organiserad brottslighet från de forna öststaterna”[1]. Internationellt ser bedömningarna lite annorlunda ut, i den årliga rapporten Data breach Investigation report från Verizon Buisness hävdare man att i 58 % av de fallen, som de har med i sin rapport för 2010, leder källan till organiserad brottslighet. Vidare anser man sig ha bevis för att en hel del av dessa intrång härstammar ifrån östra Europa. Av de 761 fall av dataintrång Verizon har med i 2011 års rapport[2] var källan geografisk identifierat i 88 %, av dessa härstammade 65 % från Östra Europa, 19 % från Nord Amerika, från 6 % Syd/Sydöstra Asien, 4 %, 3 % Östra Asien, 2 % Västra Europa, och 1 % från övrigt Världen.

[1] Tina Magnergård Bejers, Allt fler hackar för pengar, DN Ekonomi, 12 April 2011.
[2] W.H. Baker et.al., 2011 Data Breach Investigation report, Verizon Buisness, 2011.

Terrorister

Vad gäller den här gruppen av brottslingar finns inga tecken på aktiviteter när det gäller dataintrång i Sverige. I övrigt beror det väldigt mycket på hur man definierar vad terrorism är, om man följer gängse lagar i Sverige är det mycket tveksamt om det idag finns något tydligt fall i hela världen där terrorister har varit inblandade i någon form av dataintrång . Däremot finns det en utsprid skräck för ett framtida så kallat digitalt 9/11 attentat. Det som är skrämmande är att styrsystemen av så kallade kritisk infrastruktur: elnätet, vattendistribution, reningsverk, telekommunikation, signaleringen för tåg, tunnelbana osv. ofta indirekt är uppkopplade mot Internet. Vilket medför att det finns en potential risk för att utföra digitala sabotage som har en direkt fysik påverkan i den verkliga världen, exempelvis skapa en ”black out” i det svenska elnätet. Utförs ett sådant dataintrång och styrsystemen manipuleras på ”rätt” sätt skulle det kunna ta veckor innan man skulle kunna få igång elnätet igen på grund av förstörda ställverk osv. Ett exempel på en liknande attack är den så kallade STUXNET ”attacken” mot IRANs anläggningar för urananrikning, där någon nation (misstankarna går mot Israel och USA) lyckades göra ett dataintrång och manipulera styrsystemen sätt så att flera centrifuger för urananrikning förstördes. Men i det fallet är det troligen mer frågan om en militär attack än ett terrorsistbrott, i vart fall ur västvärldens perspektiv.

Eric D. Knapp, Industrial Network Security – Securing Critical Infrastructure Networks for Smart Grid, SCADA and other Industrial Control Systems, Syngress, 2011.
STUXNET, N.Y. Times, 15 Januari, 2011.

Enskilda förövare

Stereotypen för den här typen av brott, är en socialt missanpassad tekniskt intresserad yngre man som tillbringat större delen av sitt liv framför en dator. Men i realiteten finns en salig blandning av människotyper som håller på med den här typen av verksamhet, Tabell 1. De flesta hackare inte drivs av pengar utan snarare av spänningen i att lyckas tas sig in i någon dator, ju svårare desto bättre. Den här typen av individer är ofta kända på nätet under pseudonym eftersom man gärna skryter om sina tilltag. Men som sagt en del av dessa förövare gör det för pengar och hyr gärna ut sina kunskaper till andra aktörer.

Man identifierat nio olika typer IT-brottslingar som ägnar sig åt dataintrång, se Tabell 1. Sammanfattningsvis kan man säga man att ålderspannet och typerna av personer som är verksamma inom det här området är mycket bredare än den stereotypa bild som ofta pressenteras av media, där det alltid tycks handla om ungdomar. Vilket i och för sig kanske speglar den grupp som ofta åker dit för den här typen av brott. Två grupper döljer sig bakom myndigheter och till vilken grad och vilka typer av brott dessa begår är inte lätt att svara på.

D. Goldberg och L. Larsson, Svenska hackare: en berättelse från nätets skuggsida, Nordstets, 2011.

R. Chiesa, S. Ciappi and S. Ducci, Profiling Hackers – The science of criminal profiling as applied to the world of hacking, Auerbach Publishing Inc., 2008.

Nio kategorier av hackers*

Förövartyp	Beskrivning	Ensam/grupp	Mål	Motivation
Wannabe Lamar	9-18 år, vill vara hacker man har inte kunskaperna	Grupp	Slutanvändare	**För att skryta för kompisar**
Script Kids	10-18 år, använder andras mjukvara, så kallade skript, för att göra dataintrång	Grupp	Enkla mål	För att få ut aggressioner och få uppmärksamhet
Cracker	17-30 år, förstör så mycket som möjligt i de datorsystem han/hon tar sig in i	Ensam	Privata företag	För att visa makt och få uppmärksamhet
Ethical hacker	15-50 år, mycket duktig, jobbar ofta i säkerhetsbranschen	Ensam (eller i grupp forskning)	Stora företag, utmaningar	Nyfikenhet, för att göra världen bättre
Quiet, paranoid, skilled hacker	16-40 år, tystlåten. parnoid, mycket specialiserad	Ensam	Efter personliga behov	Nyfikenhet, egoism, eller specifika personliga motiv
Cyber warrior	18-50 år, legosoldat	Ensam	Företag, organisationer, slutanvändare	För pengar
Industrial spy	22-45 år, spion, har ofta någon form av konsultverksamhet	Ensam	Företag av alla slag	För pengar
Goverment agent	25-45 år jobbar åt underrättelsetjänst	Ensam eller i grupp	Myndigheter, strategiska företag, organisationer, individer	Som jobb
Military Hacker	25-45 år, anställd av försvarsmakt för att kriga på Internet	Ensam eller i grupp	Myndigheter, strategiska företag och system kopplade till kritisk infrastruktur	Som jobb

*Raoul Chiesa, Stefania Ducci and Silvio Ciappi, “Profiling Hackers – The Science of Criminal Profiling as Applied to the world of Hacking” CRC press 2009.

(Yet another) Fyra Aktörer*

“Aktörer och anatgonister I cybervärlden kan delas in efter fyra olika kategorier: från relativt harmlösa men jobbiga dito till betydligt farligare och dödligare såsom:”*

- Script kiddies
- Crackers, hackers och “hacktivister”
- Cyber terrorister
- Insiders

*Roland Heickerö & Dan Larsson, *Terror online – Cyberhot och Informationskrigsföring*, Conopsis Förlag, 2008.

Effekt Matris[1]

	Physical arena	Information arena	Cognitive domain
Physical effects	Interruption, destroy electronics and sensors, affect transmission and access links, derive robots, system failure	Interrupted communication, denial of services; DOS.	Fragmented communication, decreased amount of information, reduced analysis capability
Syntax effects	Hacking, cracking virus, trojans, spam, interception, exploit, bugging illegal misuse of information system	Attack logic of system, delay and distortion of information	Mistrust against systems
Semantic effects	Mass medial maneuvers, planted information, mutilation of sensor data	Deception and manipulation of information (disinformation)	Changed situation awareness, mistrust against and questioned of information, inability for decision making

Roland Heickerö "Some aspects on cyber war faring in information arena and cognitive domain", 11th ICCRTS Cambridge September 28

Advanced Persistent Threats (APT)*

- "The term is commonly used to refer to cyber threats, in particular that of Internet-enabled espionage using a variety of intelligence gathering techniques to access sensitive information, but applies equally to other threats such as that of traditional espionage or attack."

- "Individuals, such as an individual hacker, are not usually referred to as an APT as they rarely have the resources to be both advanced and persistent even if they are intent on gaining access to, or attacking, a specific target."

*http://en.wikipedia.org/wiki/Advanced_persistent_threat

Advanced Persistent Threats (APT)

Actors behind advanced persistent threats create a growing and changing risk to organizations' financial assets, intellectual property, and reputation by following a continuous process:

- Target specific organizations for a singular objective
- Attempt to gain a foothold in the environment, common tactics include spear phishing emails.
- Use the compromised systems as access into the target network
- Deploy additional tools that help fulfill the attack objective
- Cover tracks to maintain access for future initiatives

Advanced Persistent Threats (APT)

Cyberwarfare

- **Cyberwarfare** refers to politically motivated hacking to conduct sabotage and espionage.
- It is a form of information warfare sometimes seen as analogous to conventional warfare although this analogy is controversial for both its accuracy and its political motivation.
- Defined "cyberwarfare" as "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption."

Jämnförelse APT och Cyberwar

Table 3.3 Distinctions between APT and Cyber War

APT Qualities	Cyber War Qualities
Often uses simple exploits for initial infection	Uses more sophisticated vectors for initial infection
Designed to avoid detection over long periods of time	Designed to avoid detection over long periods of time
Designed to communicate information back to the attacker using covert command and control (C2)	Designed to operate in isolation, not dependent upon remote command and control (C2)
Mechanisms for persistent operation even if detected	Mechanisms for persistent operation or reinfection if detected
Not intended to impact or disrupt network operations	Possible intentions include network disruption

APT och Cyberwar

Table 3.4 Information Targets of APT and Cyber War	
APT Targets	**Cyber War Targets**
Intellectual Property	
Application code	Certificates and authority
Application design	Control protocols
Protocols	Functional diagrams
Patents	PCS command codes
Industrial Designs	
Product schematics	Control system designs and schematics
Engineering designs and drawings	Safety controls
Research	PCS weaknesses
Chemicals and Formulas	
Pharmaceutical formulas	Pharmaceutical formulas
Chemical equations	Pharmaceutical safety and allergy information
Chemical compounds	Chemical hazards and controls

Konsekvenser

Table 3.1 The Potential Impact of Successful Cyber Attacks

Incident Type	Potential Impact
Change in a system, operating system, or application configuration	Introduction of command and control channels into otherwise secure system
	Suppression of alarms and reports to hide malicious activity
	Alteration of expected behavior to produce unwanted and unpredictable results
Change in programmable logic in PLCs, RTUs, or other controllers	Damage to equipment and/or facilities
	Malfunction of the process (shutdown)
	Disabling control over a process
Misinformation reported to operators	Causing inappropriate actions in response to misinformation that could result in a change in programmable logic
	Hiding or obfuscating malicious activity, including the incident itself or injected code (i.e., a rootkit)
Tampering with safety systems or other controls	Preventing expected operations, fail safes, and other safeguards with potentially damaging consequences
Malicious software (malware) infection	May initiate additional incident scenarios
	May impact production, or force assets to be taken offline for forensic analysis, cleaning, and/or replacement
	May open assets up to further attacks, information theft, alteration, or infection
Information theft	Sensitive information such as a recipe or chemical formula are stolen
Information alteration	Sensitive information such as a recipe or chemical formula is altered in order to adversely affect the manufactured product

Sannolikhet v.s. konsekvens

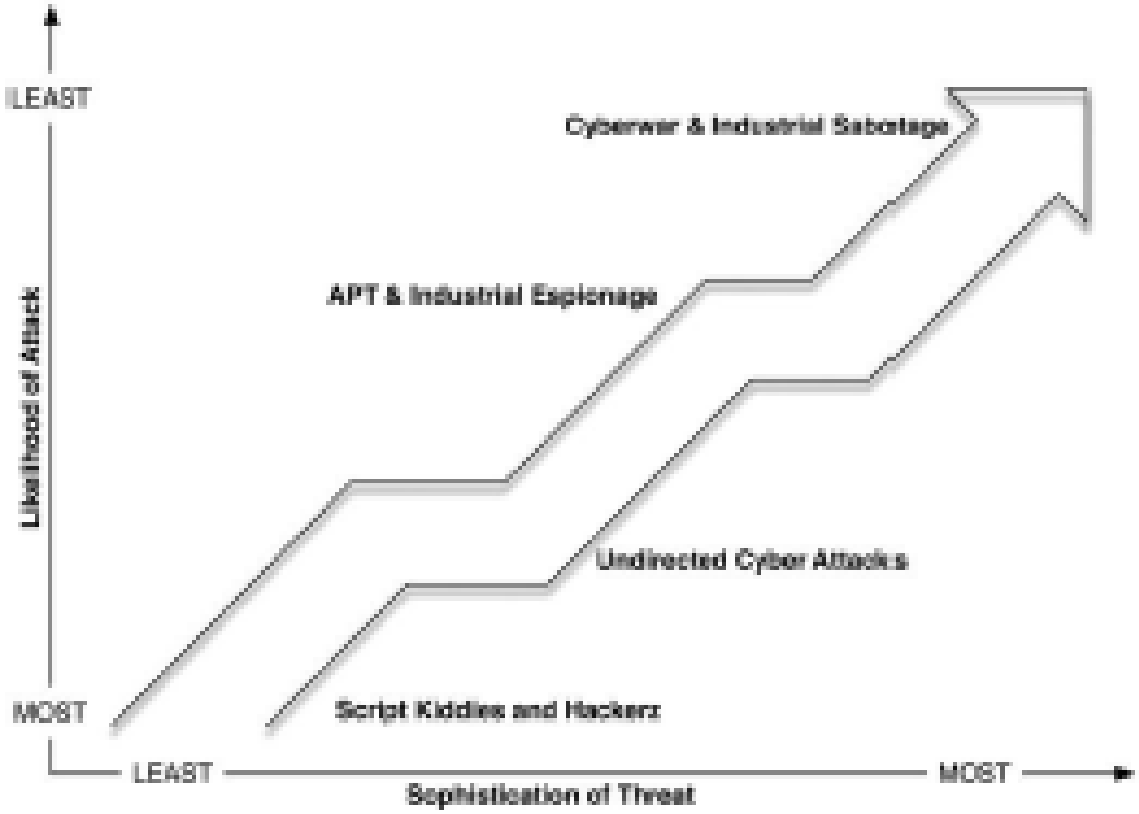


FIGURE 2.2

Likelihness versus Consequence of a Targeted Cyber Attack.

Säkerhet i Industriella nätverk

- Because industrial systems are built for reliability and longevity, the systems and networks used are easily outpaced by the tools employed by an attacker.
- An industrial control system may be expected to operate without pause for months or even years, and the overall life expectancy may be measured in decades.
- Attackers, on the contrary, have easy access to new exploits and can employ them at any time.

Säkerhet i Industriella nätverk

- Many industrial systems are built using legacy devices, in some cases running legacy protocols that have evolved to operate in routable networks.

- Before the proliferation of Internet connectivity, web-based applications, and real-time business information systems, energy systems were built for reliability.

- Physical security was always a concern, but information security was not a concern, because the control systems were air-gapped—that is, physically separated with no common system (electronic or otherwise) crossing that gap.

Säkerhet i Industriella nätverk

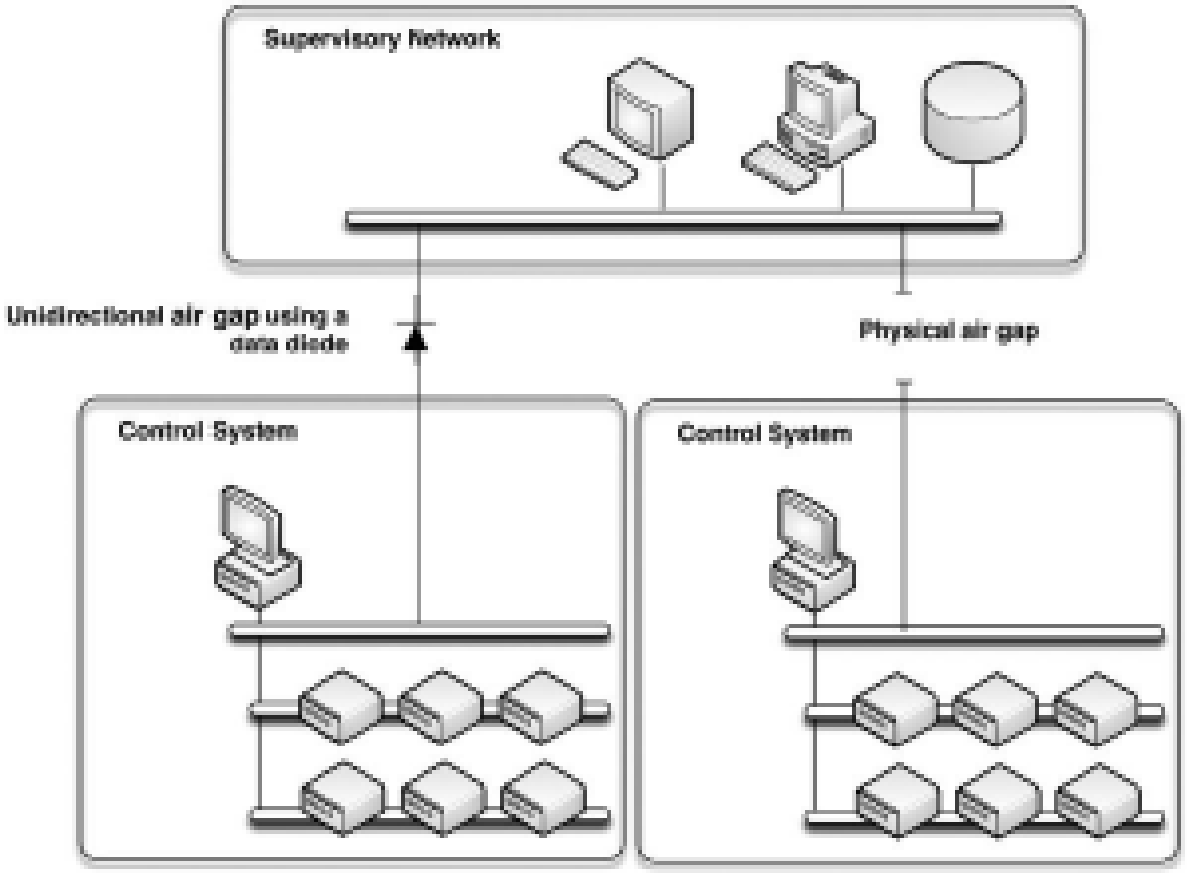


FIGURE 3.1

Air Gap Separation.

Säkerhet i Industriella nätverk

- The average number of days between the time when the **vulnerability** was disclosed publicly and the time when the vulnerability was discovered in a control system was 331 days: almost an entire year.

- Worse still, there were cases of vulnerabilities that were over 1100 days old, nearly 3 years past their respective "zero-day."[1]

[1]. J. Pollet, Red Tiger, Electricity for free? The dirty underbelly of SCADA and smart meters, in: Proc. 2010 BlackHat Technical Conference, Las Vegas, NV, July 2010.

Säkerhet i Industriella nätverk

- Ideally, the air gap would still exist, and it would still apply to digital communication, but in reality it does not.
- As the business operations of industrial networks evolved, the need for real-time information sharing evolved as well.
- Because the information required originated from across the air gap, a means to bypass the gap needed to be found.
- Typically, a firewall would be used, blocking all traffic except what was absolutely necessary in order to improve the efficiency of business operations.

Säkerhet i Industriella nätverk

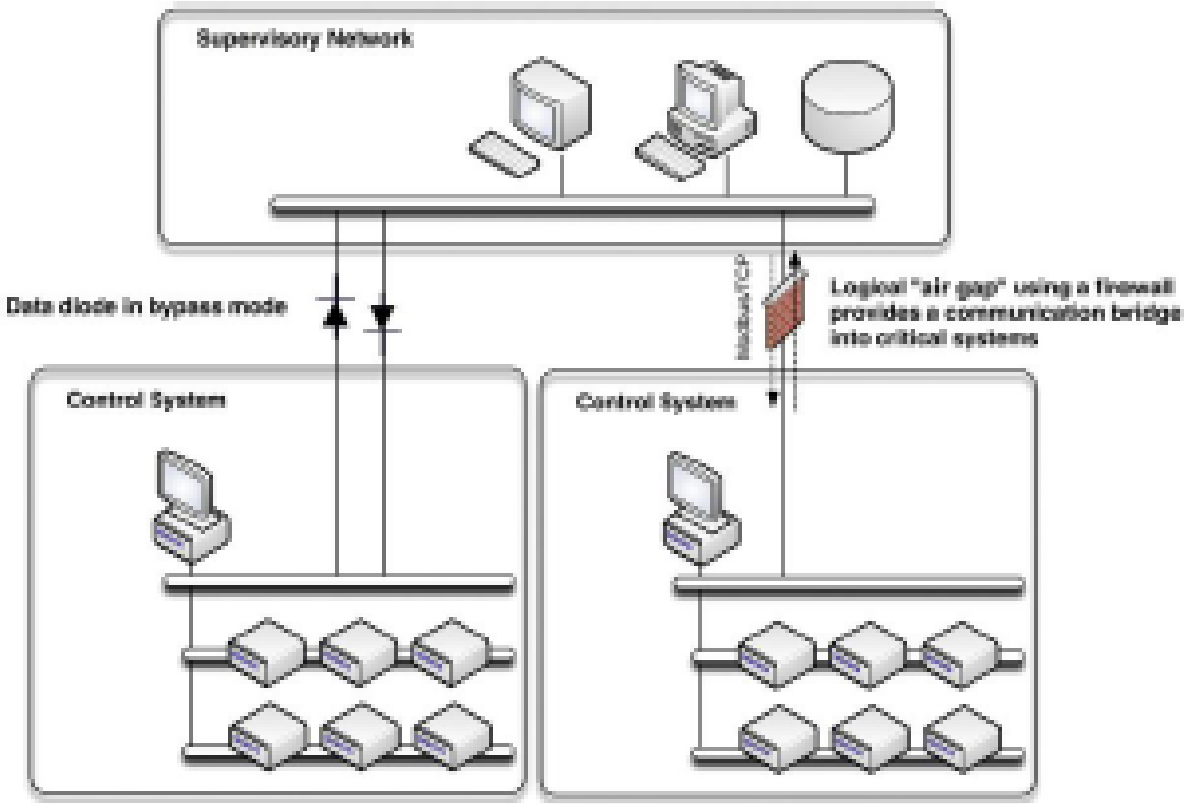


FIGURE 3.2

The Reality of the Air Gap.

Säkerhet i Industriella nätverk

- It should not be a surprise that there are well-known vulnerabilities within control systems.
- Control systems are by design very difficult to patch.
- By intentionally limiting (or even better, eliminating) access to outside networks and the Internet, simply obtaining patches can be difficult.
- Because reliability is paramount, actually applying patches once they are obtained can also be difficult and restricted to planned maintenance windows.

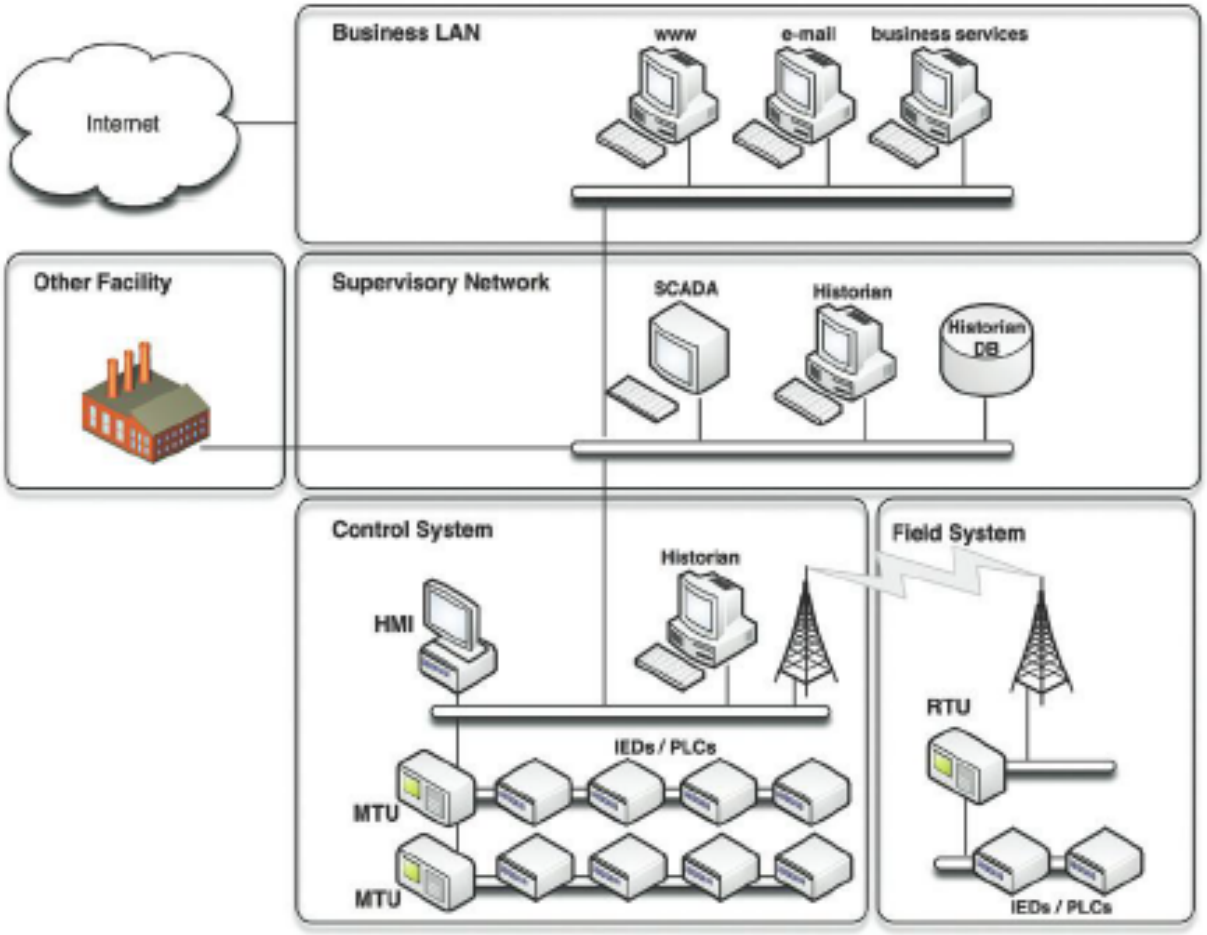
Sårbarhets och Risk Bedömning

- In order to protect an industrial network from attack, it is important to understand how an attacker might approach an industrial network, gain access, and ultimately gain control.
- The basic hacking methodology and techniques of "**identify**, **enumerate**, and **penetrate**" are often discussed within the context of a typical Ethernet and Transmission Control Protocol/Internet Protocol (TCP/IP) enterprise network.
- However, in industrial networks, the methodology holds true but the techniques are a little bit different different. The entry points and attack vectors into an industrial system, the vulnerabilities of industrial systems, devices and protocols, and the exploits built against them must be understood before these systems can be effectively secured.

Attack process

- While the basic hacking methods apply to industrial networks, there are additional considerations—at all stages of an attack—when targeting a control system.
- Industrial control systems utilize specialized systems and protocols, present new opportunities to an attacker.
- Enterprise network hacking methods are often available, presenting a greater overall attack surface.

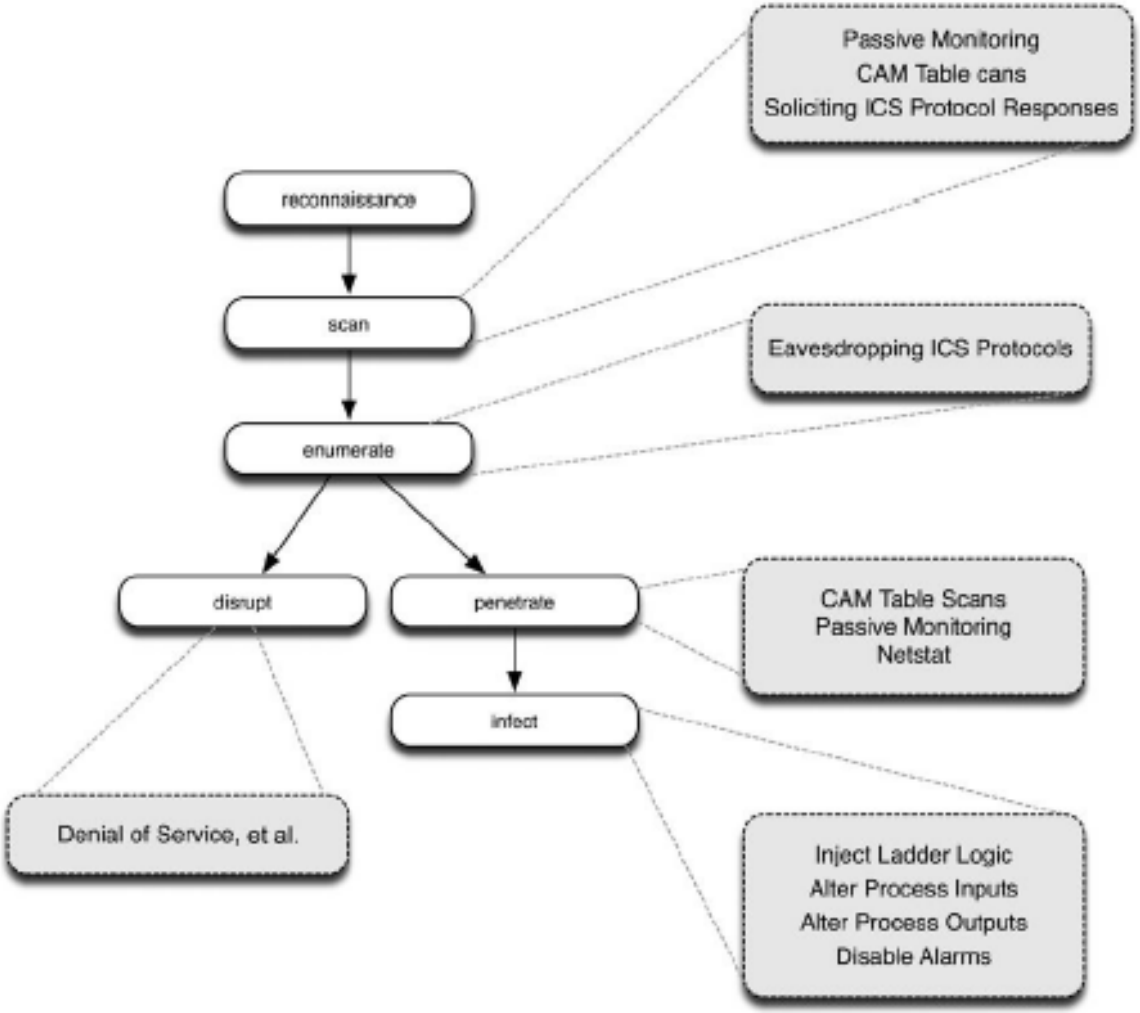
Attack process – Targeted System



Attack process – Control System Assets

- Intelligent Electronic Devices (IED)
- Remote Terminal Units (RTUs)
- Programmable Logic Controllers (PLCs)
- Human Machine Interface (HMI)
- Control System Assets
- Supervisory Management Workstations
- Data Historians
- Business Information Consoles
- Dashboards

Attack process



Attack process – Reconnaissance

- Industrial networks, protocols, assets, and systems are specialized. They are not commonly available, so an attackers first intent on infiltrating an industrial system may focus reconnaissance efforts on **information about the specific systems in use**.
- As with enterprise hacking, reconnaissance can focus on public information about a company in order **to learn the types of control system assets being used**, the shift change schedule, and what other companies partner, service, or trade with the target company.
- Because many asset vendors use different and sometimes proprietary industrial protocols, knowing the **specific assets** used within the control system can indicate to an attacker what to look for in terms of systems, devices, and protocols.

Attack process – Reconnaissance

- Any server, network switch or router, or other networked device using HTTP, FTP, SSH or Telnet is for example indexed by SHODAN (shodanhq.com).
- As a result, devices utilizing SCADA protocols over any of these services can be identified.
- This is an important step, as control systems are not easily procured, and therefore not easily reverse-engineered to find vulnerabilities.
- By understanding the control system devices in use the attacker is able to look for existing well-known vulnerabilities, or acquire device-specific research about the device through **backchannels** in order to determine vulnerabilities or backdoors.

Attack process – Scanning

- A network scan can identify hosts as well as the ports and services those hosts are using.
- The results of the scan can quickly identify SCADA and DCS communications, allowing the attacker to focus on these items.

Attack process – Scanning

Table 6.1 SCADA and DCS Well-known Ports and Services

Port	Service
102	ICCP
502	Modbus TCP
530	RPC
593	HTTP RPC
2222	Ethernet/IP
4840	OPC UA
4843	OPC UA over TLS/SSL
19,999	DNP-Sec
20,000	DNP3
34,962–34,964	Profnet
34,980	EtherCAT
44,818	Ethernet/IP