Security in Embedded Systems

Embedded Parallel Computing Seminar, SS12

Viktor Vasilev and Amirfarzad Azidhak

March 2, 2012

Introduction

- Brief description about our seminar.
- Brief description about hacking.
- Network attack.
- Device attack.

Brief description about hacking

- What is definition of hacking?
- Who is hacker?
- Different types of hackers.
- Different way of hacking.
- Some reason for hacking.
- Some resources to know better about hacking.

What is definition of hacking?

- **Hacking** means finding out weaknesses in an established system and exploiting them (Breaking into computer systems).

Who is hacker?

- A computer hacker is a person who finds out weaknesses in the computer and exploits it.

Different types of hackers

- White hat: A white hat hacker breaks security for non-malicious reasons, for instance testing their own security system.
- Gray hat: A Grey Hat Hacker may surf the internet and hack into a computer system for the sole purpose of notifying the administrator that their system has been hacked.
- Black hat: A Black Hat Hacker is a hacker who "violates computer security for little reason beyond maliciousness or for personal gain.

Different way of hacking

- Network hacking.
- Device hacking.

Some reason for hacking

- Profit
- Protest
- Challenge
- Penetration test.
- ….

Some resource to know better about hacking

- http://www.securityfocus.com/
- http://www.zone-h.org/
- http://www.exploit-db.com/

Network attacks

- Interception
  - Network sniffing
- Fabrication
  - Insert malformed messages
  - Replay old messages
- Modification
  - Man-in-the-middle-attacks
- Interruption
  - Denial-of-service
  - Network flooding
  - Redirection

Interception

- Network sniffing
  - Network sniffing is a method of using specialized hardware and software to access information that isn’t being sent to someone or analyzing networks to which individuals don’t have legitimate access.

Interception

- Solution
  - Encryption of transmitted data
    - The IP Security (IPsec):

      has been specified as an extension to the **IP protocol**. IPsec provides mutual entity authentication and data confidentiality, integrity, and freshness. For key exchange, the Internet Key Exchange protocol is used.
    - Secure sockets layer (SSL) :

      Secure sockets layer (SSL) and its successor transport layer security (TLS) are used to **protect communication between two entities**. During the initial handshake, the entities are authenticated, and a **secured channel** that guarantees data confidentiality, integrity, and freshness is established.
    - virtual private network (VPN) :

      VPN is a logical network that is built upon a physical host network. A VPN is transparent to the connected devices. Secure VPNs use a **tunneling protocol** that provides a **secured channel**. A popular secure VPN implementation is OpenVPN which makes use of TLS.

Fabrication

- Insert malformed messages
  - A malformed message is any kind of invalid or **non-standard message**, skillfully formed by the attacker in order to exploit and eventually take advantage of, any implementation gap or dysfunction might exist in the target system.
- Replay old messages
  - A replay attack is a form of network attack in which a **valid data** transmission is maliciously or fraudulently **repeated** or delayed.

Fabrication

- Solution
  - Session tokens:
    - A session token is a **unique identifier** that is generated and sent from a server to a client to **identify the current interaction session**.
  - One-time passwords:
    - A **one-time password** (OTP) is a password that is valid for only one login session or transaction.
  - Time stamping:
    - A **timestamp** is a sequence of characters, denoting the date or time at which a certain event occurred

Modification

- Man-in-the-middle-attacks
  - the man-in-the-middle attack (often abbreviated MITM) is a form of active eavesdropping in which the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a **private connection**, when in fact the **entire conversation is controlled by the attacker.**

Modification

- Solution
  - Secure channel
    - virtual private network (VPN)
    - The IP Security (IPsec)
    - Secure sockets layer (SSL)
    - Proxy
      - SOCKet Secure (**SOCKS**) is an Internet protocol that routes network packets between a client and server through a proxy server.

Interruption

- Denial-of-service
  - A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a computer or network **resource unavailable** to its intended users.
- Network flooding
  - when a large enough number of packets (the droplets in a stream of data) are flowing through the network that **regular data cannot be sent** in a normal speed and fashion.
- Redirection
  - **Change the destination address** and redirect packet to another destination.

DoS attacks

- DoS attacks can be classified into two different categories:
  - **host-based DoS attacks** :an adversary may try to interrupt the operation of a single network node by wasting its system resources.
  - **network-based DoS attacks** :the network itself may be target of DoS attacks.

DoS attacks

- DoS prevention
- DoS detection
- DoS countermeasures

DoS prevention

- Using Client Puzzle Protocol (CPP)
  - The idea of the CPP is to require all clients connecting to a server to correctly **solve a mathematical puzzle** before establishing a connection, if the server is under attack. After solving the puzzle, the client would **return the solution to the server**, which the server would quickly verify, or reject and drop the connection. The puzzle is made simple and easily solvable but requires at least a **minimal amount of computation** on the client side.

DoS detection

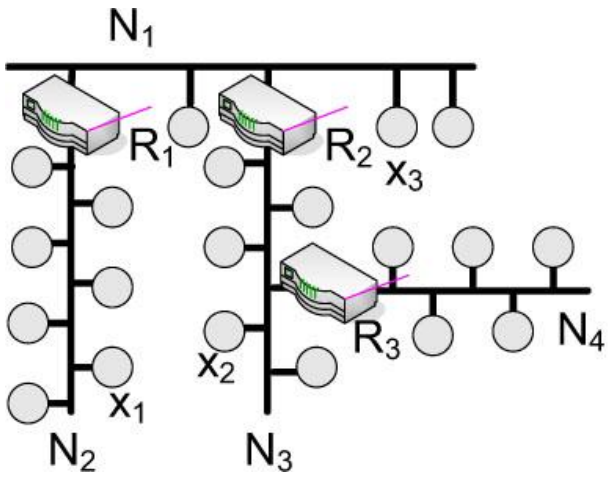
- Using intrusion *detection system* ***(IDS)***
  - commonly consist of four components:
    - ***Data gathering component*** *:* responsible for collecting the data by observing the network traffic.
    - ***Data processing component****:* concerned with processing the collected data and deciding whether abnormal behavior is present.
    - ***Data storage unit:*** in charge of collecting the results and storing the observed data (communication traces).
    - ***Response unit:*** responsible for initiating actions to minimize the consequences of an attack.

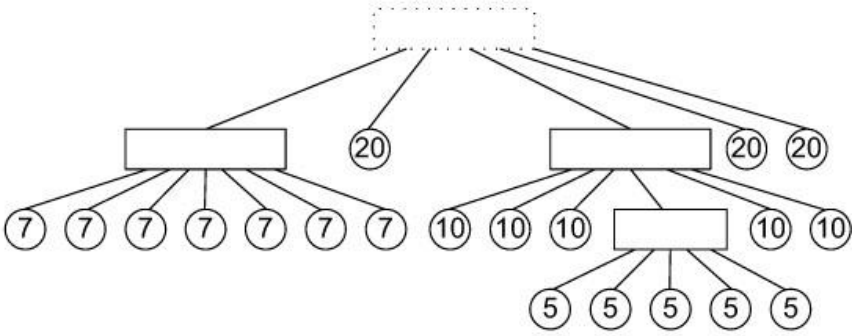
DoS countermeasures

- To achieve this, the source(s) of the DoS attack have to be identified and **isolated from the rest of the network**.
- closely related to the **physical topology** of the affected
  - **star topologies:** an isolation can be accomplished by cutting the communication line to the source(s) of the attack.
  - **wireless networks**: the isolation highly depends not only on the logical topology (e.g., star, mesh) but also on the used communication model (e.g., peer-to-peer or coordinator-to-peer). The basic idea is to isolate an affected zone and to find routes that **bypass this zone.**
  - **wired line or free topology**: an isolation can only be achieved by decoupling the whole network segment.

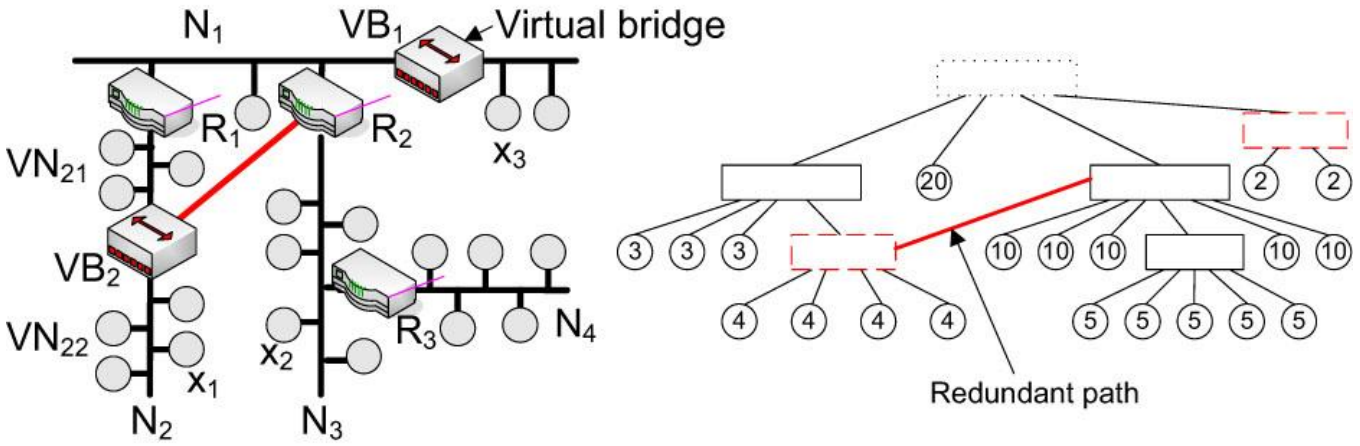
DoS risk factor (DoS-RF)

- To estimate the damage





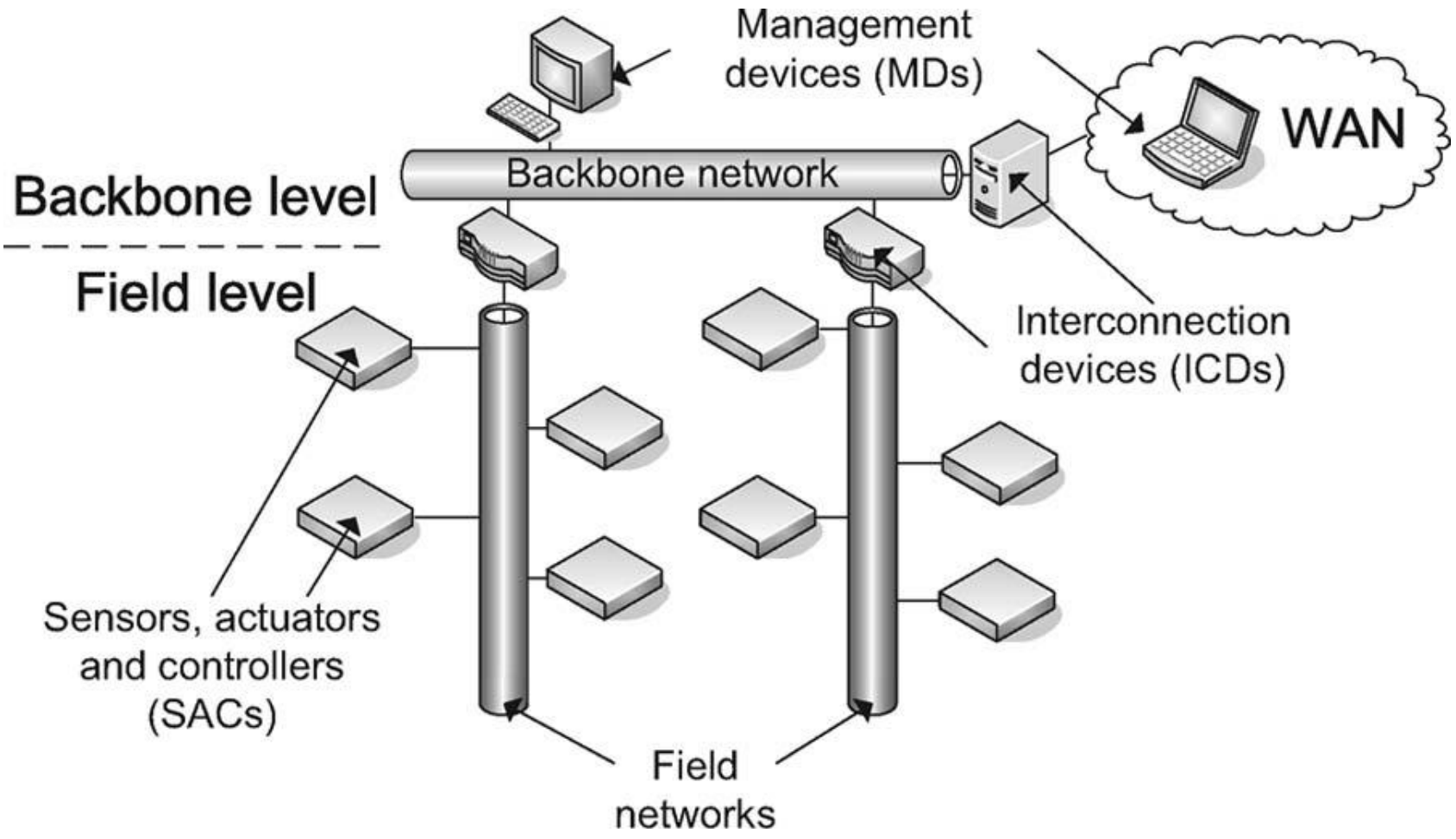
Solution for DoS-RF



- *virtual network segments* by placing a so called *virtual bridge.*

- Decrease the amount of DoS-RF by using redundant interconnections between virtual bridges and interconnection devices.

Building Automation systems



Building automation network.

Building Automation systems

- five potential attack targets:
  - **Field network:** An adversary may try to interfere with the data being exchanged among control applications.
  - **Backbone network:** The data transmitted across network borders are concentrated there. Thus, an adversary may gain a global view of the entire system.
  - **SAC:** An adversary may directly access SACs to manipulate the behavior of the hosted control applications by changing configuration parameters.
  - **ICD:** An adversary may attack the application running on the ICD to get access to the data passing through the ICD.
  - **MD:** An adversary may attack an MD by manipulating the operator software to gain management access to SACs or ICDs.

Challenges for Providing Security

- limited system resources
- **IP networks** in BANs is reserved to the backbone level. At the field level, predominantly **non-IP** field buses are used
- control data typically transmitted in BANs have a **small volume** (on the order of bytes) with perhaps soft **real-time requirements** (system).
- In the IT/office domain, the data volume to be **transferred is commonly high** (on the order of mega- or gigabytes) with usually **no real-time** requirements.
- **untrusted environments :**BANs devices often operate in untrusted environments where **physical access.**
- **Update:**BAS has to be kept operable for years or even decades. Due to the intended long lifetime, the possibility to **update** the software running on the devices has to be provided. This update mechanism also offers an additional attack point that has to be protected against unauthorized use.

SECURITY IN BUILDING AUTOMATION STANDARDS

- BACnet
- LonWorks
- KNX
- IEEE 802.15.4
- ZigBee

SECURITY IN BUILDING AUTOMATION STANDARDS

- **BACnet**: offers several services to prevent unauthorized interception, modification, and fabrication of the exchanged data. These mechanisms use the symmetric Data Encryption Standard (DES) algorithm and a trusted key server, which is responsible for generating and distributing session keys.
- **Weaknesses:**
- The initial secret key management is not defined.
- Reuse of old session keys is possible since the lifetime is not limited.
- DES is no longer secure.
- **BACnet Addendum:** Advanced Encryption Standard (AES), the Keyed–Hash message authentication code (MAC) (HMAC) algorithm, and a unique message identifier in combination with a time stamp.

SECURITY IN BUILDING AUTOMATION STANDARDS

- **LonWorks:** provides a four-step challenge-response mechanism to counteract modification and fabrication attacks.
- A sender which intends to authenticate a transmission asserts the authentication bit of its message. Receivers reply with a 64-b random number. The sender returns a 64-b hash value calculated over the content of the message and the random number using a shared key. The receiver performs the same calculation and compares the results.
- **Weaknesses:**
- Interception of confidential data cannot be avoided.
- The identity of the receiver is not verified.
- The authentication protocol is inefficient in large groups due to the limited key length.
- The cryptographic algorithm is not secure.
- Key management services are not defined.
- Each node can use only a single key.

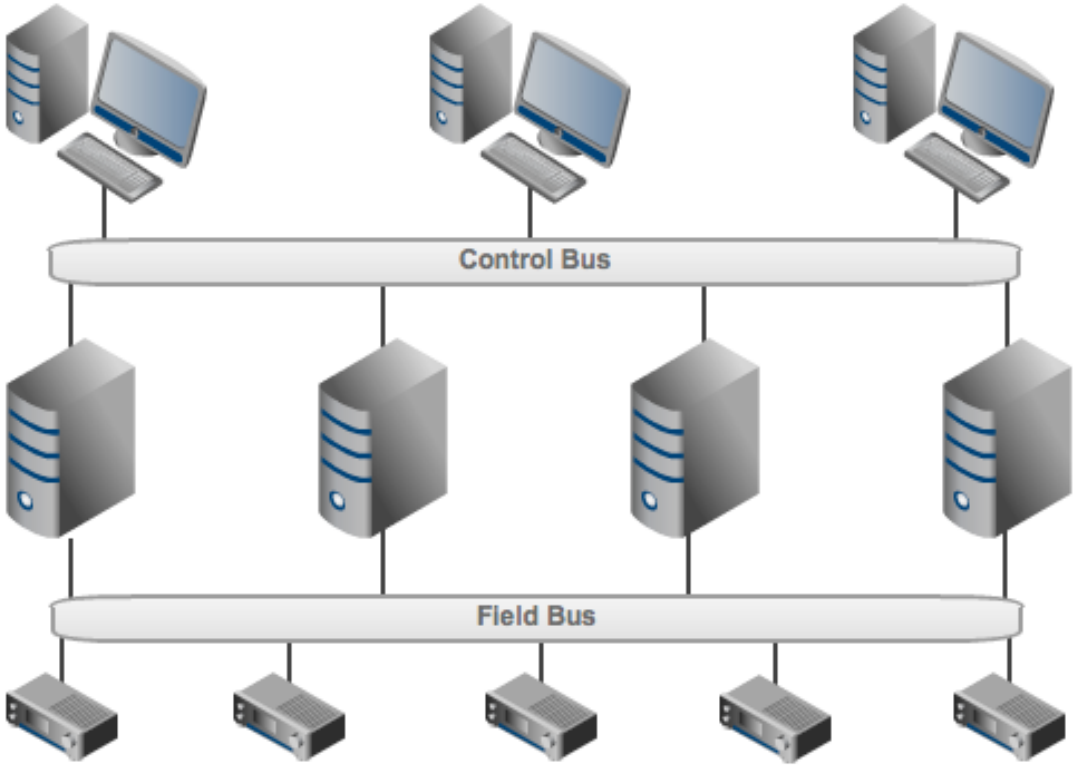
SECURITY IN BUILDING AUTOMATION STANDARDS

- **KNX:** does not offer mechanisms to avoid network attacks. It only provides a basic access control scheme which can be used to limit the management access to devices. Up to 255 different access levels can be defined, each of them associated with a different set of privileges. Access levels, a 4-B password can be specified.
- **Weaknesses:**
- The keys are transmitted in clear text.
- There are no mechanisms to manage keys in a secure manner.
- KNX's single management tool Engineering Tool Software (ETS) uses only one key for the whole installation.
- Injection of messages after successful authentication cannot be avoided.

SECURITY IN BUILDING AUTOMATION STANDARDS

- **IEEE 802.15.4:2006:** offers security services at the link layer that use CCM∗ as combined **encryption** and **authentication** block cipher mode.
- **ZigBee 2007:** utilizes the IEEE 802.15.4:2003 transmission services of the data link layer. However, ZigBee 2007 does not use the security mechanisms provided by IEEE 802.15.4:2003 they are completely replaced by a more advanced security concept. This concept supports the use of different key types and provides advanced key management services. Again, CCM∗ is used as a cryptographic algorithm.

Process control systems



HMI

Control Computers

PLCs

Highly simplified representation of a process control network

Process control systems

- Critical infrastructures have used two kinds of control systems:
  - supervisory control and data acquisition (**SCADA**) systems that quickly gather remote field data.
  - distributed control systems (**DCS**) that manage automated manufacturing processes.

Vulnerability of process control systems

- Operators of process control systems used to believe they were **invulnerable** to cyber attack **for two main reasons:**
  - The first reason is the assumption that PCS are **isolated from the internet.**
  - Second is that PCS generally use proprietary protocols and specialized hardware **not compatible with ordinary computers** and common network protocols like Ethernet and TCP/IP.
- 2006 Black Hat Conference
  - unprotected wireless access point, used it to access the plant's business network, and from there accessed the plant's control network using a ten-year old exploit.

Process control systems at nuclear power plants

- These plants generally have process control systems, often **designed by the same companies** that provide these systems to non-nuclear power plants.
- they often choose to continue **using their original control systems** rather than upgrade. A nuclear PCS can be in service for twenty to thirty years.
- nuclear plants **prefer to use tested technologies** so researchers did not get to do "bleeding edge" research.

proof of concept

- **Davis-Besse worm infection**
- **Browns Ferry shutdown(**was not the result of a cyber attack**)**
- **Hatch automatic shutdown**
- **Stuxnet**

Davis-Besse worm infection

- Davis-Besse nuclear power plant near Oak Harbor, Ohio. The **Slammer** worm traveled from a consultant's network, to the corporate network,then to the process control network for the plant. The **traffic** generated by the worm clogged the corporate and control networks. For **four hours and fifty minutes**, plant personnel could not access the Safety Parameter Display System (SPDS), which shows sensitive data about the reactor core collected from coolant systems, temperature sensors, and radiation detectors.
- it **did not affect analog readouts** on the equipment itself.
- a consultant had created a **connection behind the firewall** to the consultancy's office network.
- In response, First Energy set up a **firewall** between the corporate network and the plant control network.

Browns Ferry shutdown

- The August 19, 2006, shutdown of Unit 3 at the Browns Ferry nuclear plant near Athens, Alabama.
- Unit 3 was manually shutdown after the **failure of** both reactor **recirculation pumps** and the condensate **demineralizer controller**. Without the recirculation pumps, the power plant could not cool the reactor, making a shutdown necessary to avoid melting the reactor core.
- Both kinds of devices have **embedded microprocessors** that can communicate data over Ethernet.
- A device using **Ethernet broadcasts data**.
- control network produced **more traffic** than the PLC and VFD controllers could handle.

Hatch automatic shutdown

- simple actions can have unexpected results. On March 7, 2008, Unit 2 of the Hatch nuclear power plant near Baxley, Georgia, automatically shutdown after an engineer applied a **software update** to a single computer on the plant's business network. The computer was used to collect diagnostic data from the process control network; the update was designed to **synchronize data** on both networks. When the engineer rebooted the computer, the synchronization program **reset the data** on the control network. The control systems interpreted the reset as a sudden drop in the reactor's water reservoirs and initiated an automatic shutdown.
- Plant operators do not fully understand the **dependencies between network devices.**

Stuxnet

- The Stuxnet attack against the Iranian nuclear program demonstrates the impact that a **adversary with a detailed knowledge** of process control systems can have on critical infrastructures.
- Stuxnet is believed to have **destroyed 984 centrifuges** at Iran's uranium enrichment facility in Natanz.
- Stuxnet may have been designed specifically for that **purpose**.
- The Stuxnet worm **targeted specific PCS** components used in the Iranian centrifuge cascades:
  - frequency converter manufactured by Iranian firm Fararo Paya
  - frequency converter manufactured by Finland's Vacon
  - the S7-315 and S7-417 programmable logic controllers made by Siemens.
- The PLCs controlled the frequency converters to modulate the speed at which the centrifuges spun. Stuxnet commanded the PLCs to **speed up and slow down** the spinning centrifuges, destroying some of them, while **sending false data to plant operators** to make it appear the centrifuges were behaving normally.
- These products are **general PCS components** not unique to the Iranian nuclear program.
- it was programmed to disrupt only systems that had the **same configuration** as the centrifuge cascade used at Natanz.

Conclusion

- There is **not only one way** to protect our network against cyber attacks because the **type** of the attacks are **different**.
- Networks are **not immune** from attack when they are **not connected** to the internet.
- Networks are **not immune** from attack when they are different from **ordinary networks**.
- **Countermeasures** that eliminate or prevent security threats and attacks **in advance** have to be implemented.

THE END

- Thanks for your attention.

REFRENCES

- Refrences
  - Security in Building Automation Systems(Wolfgang Granzer, Fritz Praus, and Wolfgang Kastner, *Member, IEEE)*
  - The Vulnerability of Nuclear Facilities to Cyber Attack(*Brent Kesler)*
  - Denial-of-Service in Automation Systems (Wolfgang Granzer, Christian Reinisch, Wolfgang Kastner Vienna University of Technology, Automation Systems Group*{w,cr,k}@auto.tuwien.ac.at)*
  - http://en.wikipedia.org/wiki/Replay_attack
  - http://en.wikipedia.org/wiki/One-time_password
  - http://en.wikipedia.org/wiki/Man-in-the-middle_attack
  - http://en.wikipedia.org/wiki/Client_Puzzle_Protocol