Industrial revolution 4.0.
How to keep up the pace and do not fall of cyber threats’ victim

Andrey Nikishin
Special Projects Director, Future Technologies, Kaspersky Lab
REVOLUTION OR EVOLUTION?
Да здравствует социалистическая революция!
INDUSTRIAL REVOLUTIONS
LAST REVOLUTION -- INTERNET
1.0 Water and Steam Power
2.0 Electrical energy
3.0 Electronic & IT Systems
4.0 Cyber - Physical

1800 1900 2000
ENTERPRISE 4.0

- Totalized flow
- Fluid density
ENTERPRISE 4.0
BENEFIT OR THREAT?
ENTERPRISE 4.0 DEVICES

So, WTF is HART?

• Highway Addressable Remote Transducer Protocol
• Industrial protocol.
• Developed by Rosemount in mid-1980s.
• Supported by Hart Communication Foundation
• Different physical layers: Current Loop, Wireless (802.15.4), RS-485, HART-over-IP.
• Mainly used for communicating between software/PLC and RTUs (originally transmitters)
• Mostly used on power plants, chemical factories, oil & gas industry
• HART isn’t as secure as they have been telling you. Sniffing and injecting in current loop is possible. Even skilled industrial engineers have been caught.

Jari says
January 22, 2014 at 13:55

It is not about vulnerability in HART, rather a good example of bad engineering in building the HART stack. I’d say it is just another lack of input verification. Moreover, no sane people use HART-IP protocol needs deep redesign to make it more secure and reliable.
THREATS: VEHICLE CONTROL TAKEOVER

Then 0-day vulnerability in infotainment system was exploited to gain remote control.
AUTOMOTIVE TRENDS

More Functions
- Entertainment
- Navigation
- Driving assistance
- Apps

More efficient Hardware
- High-Performance CPU
- Multicore

Connectivity
- Services
- Cloud
- CE Integration

Standards
- Android
- Linux
- GENIVI
- AUTOSAR
DATE CODE: 132011

SERIAL NUMBER: RTS422256H
Terrorists could hack pacemakers like in Homeland, say security experts

Forensic medicine and security specialists have joined forces to develop software to spot if pacemakers have been hacked
NO FRIENDS. ONLY FOES.
PRESENT CYBER THREATS TRENDS

» Highly targeted attacks
» Sophisticated attacks aka A(dvanced) P(ersistent) T(reat)
» State sponsored attacks (cyber espionage and Cyber sabotage)
» Hacktivism and cyber hooligans
» Traditional crime meets Cyber crime
FUTURE TRENDS?

The Myth of Cyberterrorism

There are many ways terrorists can kill you--computers aren't one of them.

Art by Mike Werner
FUTURE TRENDS?

- All above plus:
  - Cyber war
  - Cyber terrorism
  - Attacks on Internet of Things
FUTURE TRENDS?

All above plus:

- Cyber war
- Cyber terrorism
- Attacks on Internet of Things
- Attacks on Cyber-Physical devices
- Attacks on connected devices
WHAT TO DO?

Now:

➢ Use any available technical measures to protect existing infrastructure
➢ Use any organisational measures to protect existing infrastructure
➢ Maintain cyber security culture
➢ Trainings etc
➢ Legislation and regulations
➢ Everything we are talking about these days
WHAT TO DO?

Strategically:

➤ All new devices has to be design with cyber security in mind
➤ All of the system designed in pre-internet era have to be redesign and redevelop
➤ All old devices have to be upgraded with new ones
➤ Yes, it is expensive. Yes, it will take time, Yes, private sector and government have to work together
➤ No, there is no other way
WHAT A PRIVATE DATA IS?

- E-mail address
- Passport or credit card number?
- Date of Birth?
- Internet browser history?
- Heart rate?
- Number of steps made during a day?
- Meter reading?
- Phone book?
- Duration of one’s sleep?
- Route to work?

How can we protect privacy in a world where coffee makers and refrigerators have their own Twitter account?
THANK YOU VERY MUCH!

Andrey Nikishin
Kaspersky Lab