Cybersecurity Topics and Vulnerability Management - ICS and IT security -

Part2:
Testing for and countering vulnerabilities

Smart Community Summit 2014

19th June ’14

Cyber Defense Institute, Inc.

How the stuff is being made

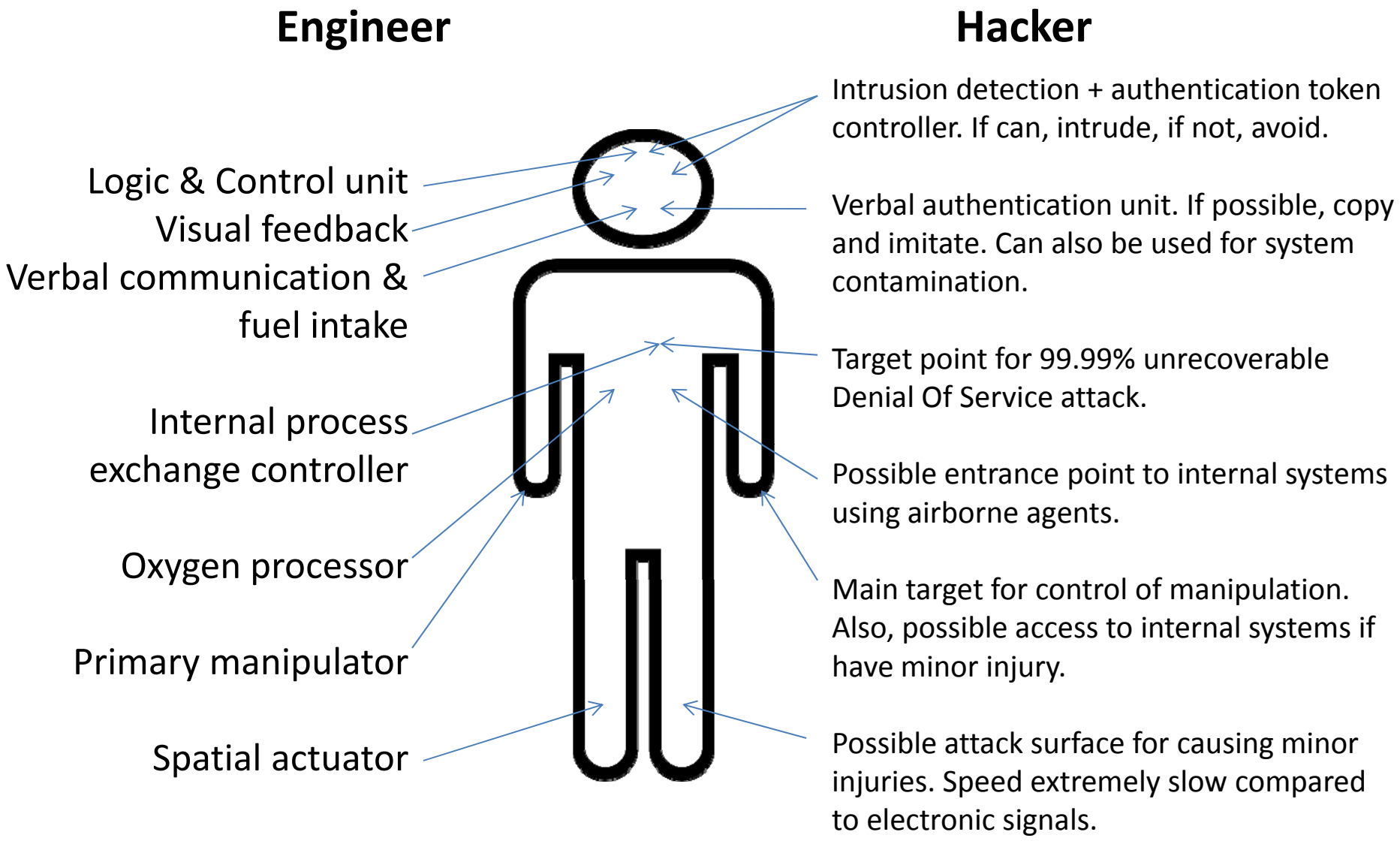
IT

- build, install, use, rebuild, reinstall, repeat.
- lifespan: couple of years

ICS

- build, install, operate and maintain. as long as you can
- lifespan of a system: couple of decades

Engineer vs. hacker



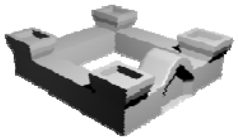
The present state

(from the standpoint of security)

IT

- Cloud-based services, account password leaks, malicious and fake services are common
- Extensive methodology about testing for vulnerabilities
- Way too many solutions to choose from, (but none of them perfect)
- “Instability” is it’s hidden nature

ICS



- Security is mostly achieved by segregation, because operational needs come always first
- Separate components can be made secure by minimalism, but usually are working separately
- Relatively few people have hands-on working knowledge about real systems
- “Perpetual” is the goal

And recently those systems are starting to merge through “smart” technologies...

Adding danger to the mix: Current state of things+ hackers

How bad it can get?

IT

- Your PC used for BitCoin mining by a someone.. OR
- Everybody's bank account emptied, airplanes grounded due to virus in airline company's office, all existing webcams and phones turned into massive surveillance network

ICS

- Stealing electricity without paying for it.. OR
- Mass murder of millions by deliberately damaging water dam controls and other critical systems (fortunately not happened yet!)

Patching the holes

IT way

- Click on the “Update” button
- Create another, clean VPS instance, migrate data, switch IP’s and be done with that
  - don't even have to touch the machinery in the rack

ICS way

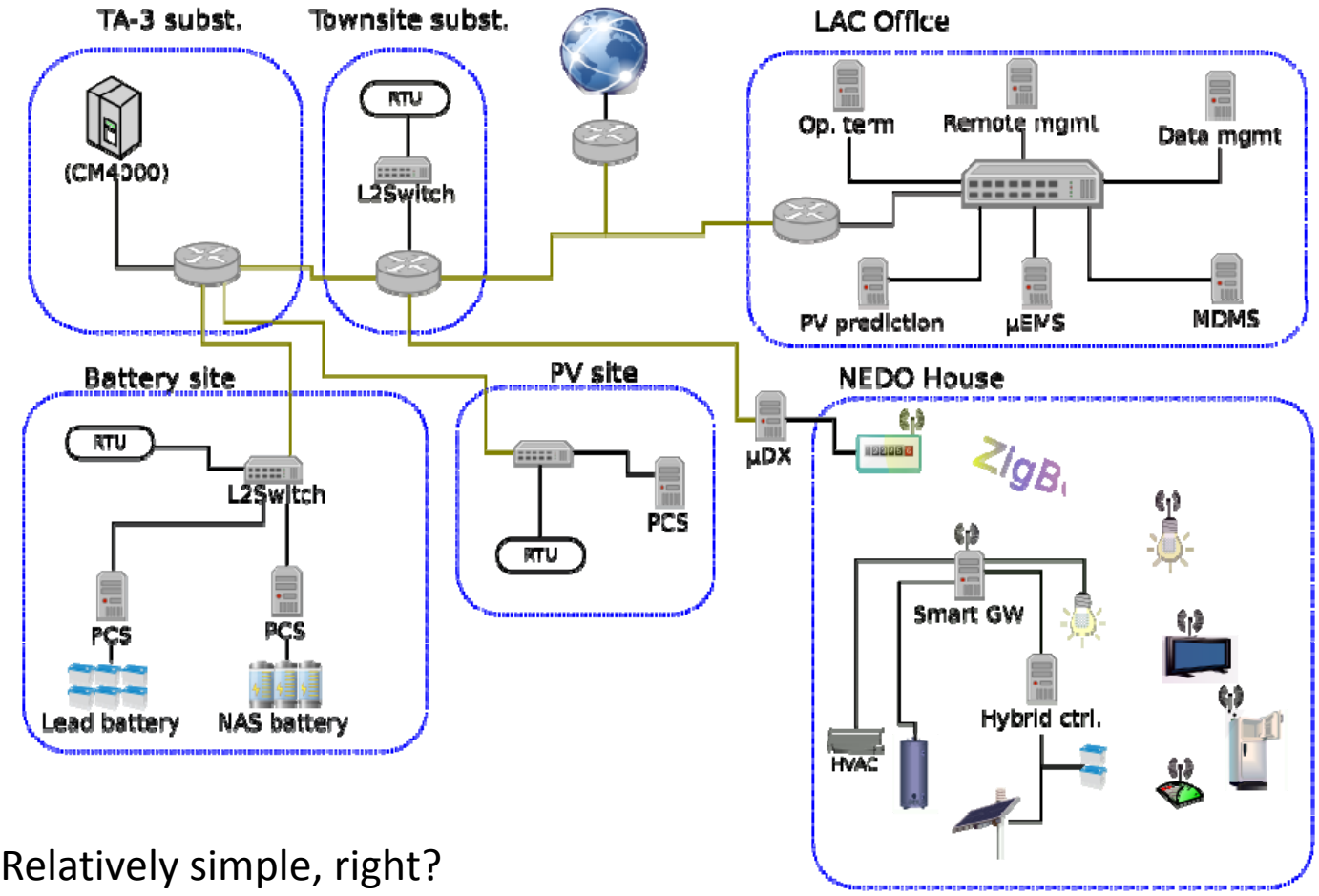
- ... let's better not change anything, as that might disturb the operation of primary functions
  - and it actually costs quite a bit to change any component or setting because of extensive testing requirements and hardware-based deployment

Security test for ICS-like systems

Multi-phase approach

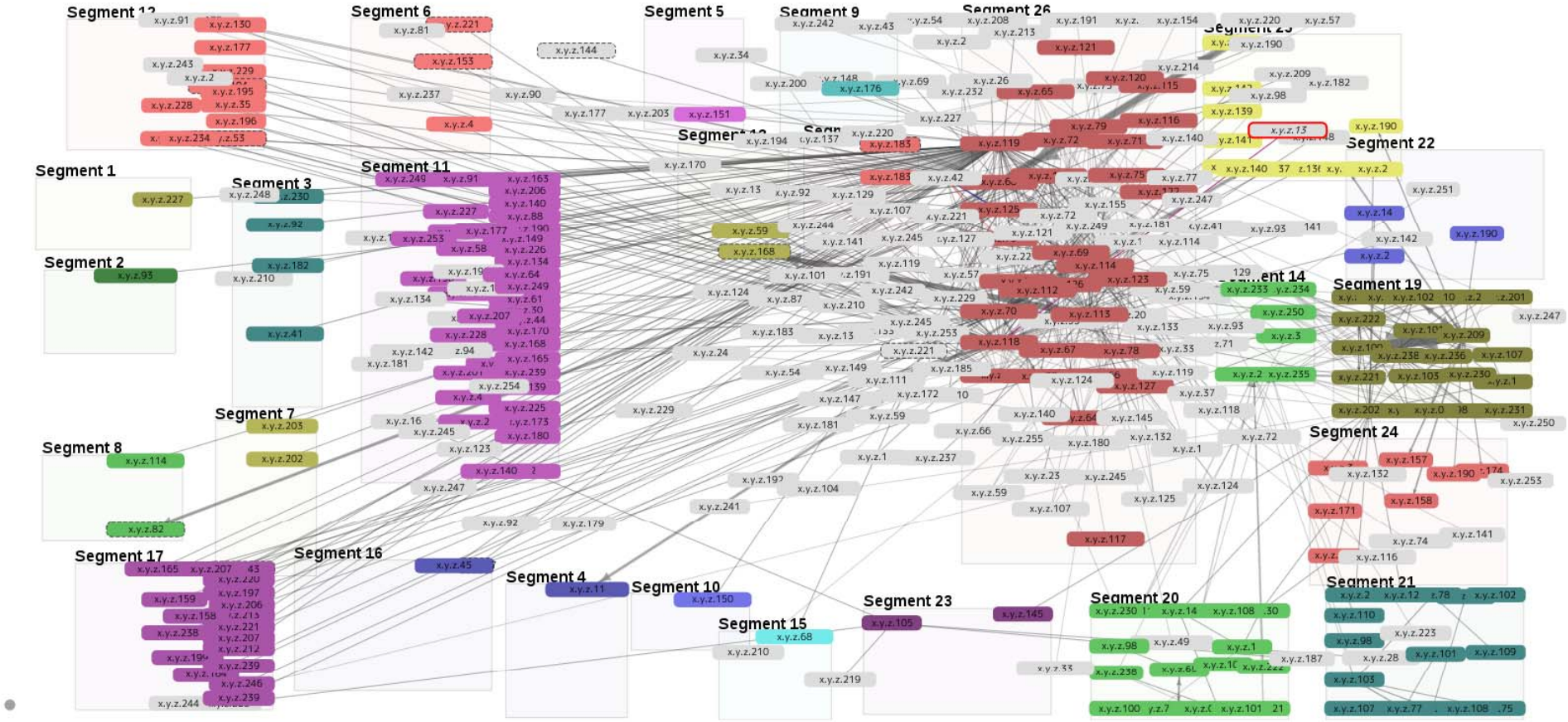
- break everything you can
  - in controlled lab environment
  - generally against individual components
  - while it is still possible to fix and revert
- do not break anything
  - in real-world setup
  - mostly just checking out data based on first phase
  - confirming that previously reported problems have been actually fixed

Network at glance



Relatively simple, right?

Network in more detail



- 1000+ interconnections…
- 40+ different protocols…
- 100+ GB traffic per day…

"Uhm… it should be here somewhere .. I think.."

Findings

- Some critical, some High and several low level direct vulnerabilities found, actually less than expected
- Old methods don’t play well with new standards (esp. when crypto is involved)
- Properly sectioning the system internally will help greatly to reduce risk from questionable components
- Testing individual components before is crucial because of operational risks and inertia
- Systems need to be ready to be tested, and for proper testing results time have to be allocated for it, no matter what.
- Everybody who participated got awareness boost and speck of knowledge how to be more secure in the future.

Steps towards permanent security

- IT engineers have to learn lifetime-span software design
- ICS engineers have to learn using evolving designs
- ICS management have to be aware of the risks
  - Keep an eye on hackers' workbench
  - See what is happening around you
  - Know well what is happening in your own system, and know how close it is to critical condition
- Act now or never, because later is just too late!

About the slides

Cyber Defense Institute, Inc.

Lauri Korts-Pärn <lauri@cyberdefense.jp>

Email: sales@cyberdefense.jp

Tel: +81-3-3242-8700
Web: www.cyberdefense.jp/en