Security assessment of critical infrastructure

Rikard Bodforss, Founding partner Bodforss Consulting AB

BODFORSS

Who am I?

...I wasn’t always an IT-manager...

Listen to Säkerhetspodcasten!

BODFORSS

Securing human rights

BODFORSS

Promised deliverables

- Preamble
- Passive test methods
- Active test methods
- Choosing method and approach
- Summary

BODFORSS

Preamble

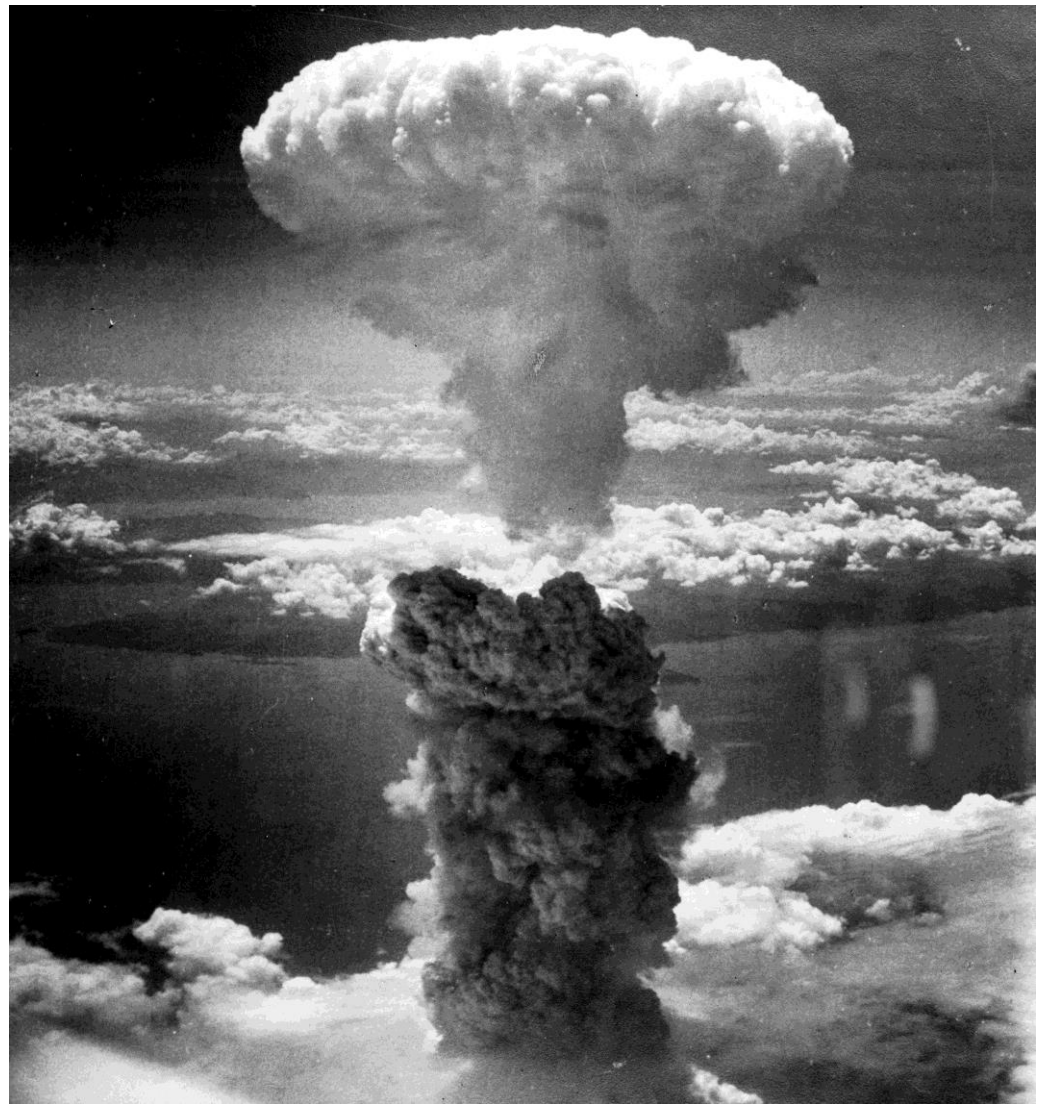
BODFORSS

Why do we test security?

BODFORSS

What could possibly go wrong?

BODFORSS



BODFORSS

A brief summary of the state of academic research on the subject…

Activity	Usual Actions for IT	Preferred Actions for SCADA
Identification of hosts, nodes, and networks	Ping Sweep (e.g. nmap)	1. Examine CAM tables on switches. 2. Examine router config files or route tables. 3. Physical verification (chasing wires). 4. Passive listening or IDS (e.g. snort) on network.
Identification of services	Port Scan (e.g. nmap)	1. Local port verification (e.g. netstat). 2. Port scan of a duplicate, development, or test system.
Identification of vulnerabilities within a service	Vulnerability Scan (e.g. nessus, ISS, etc…)	1. Local banner grabbing with version lookup in CVE. 2. Scan of duplicate, development, or test system.

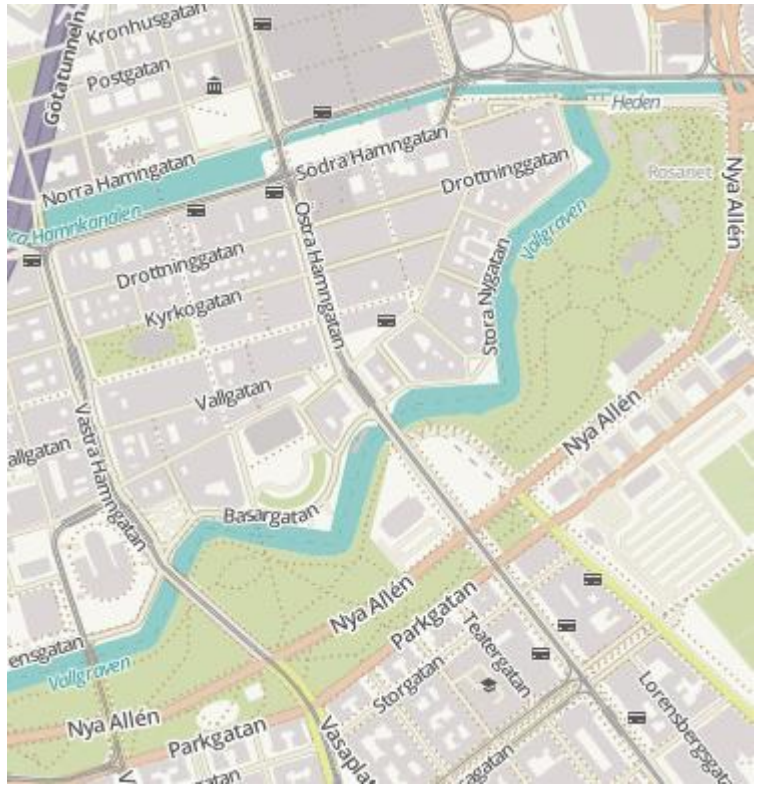
Passive methods

BODFORSS

Pen-test?

BODFORSS

The map v/s the real world

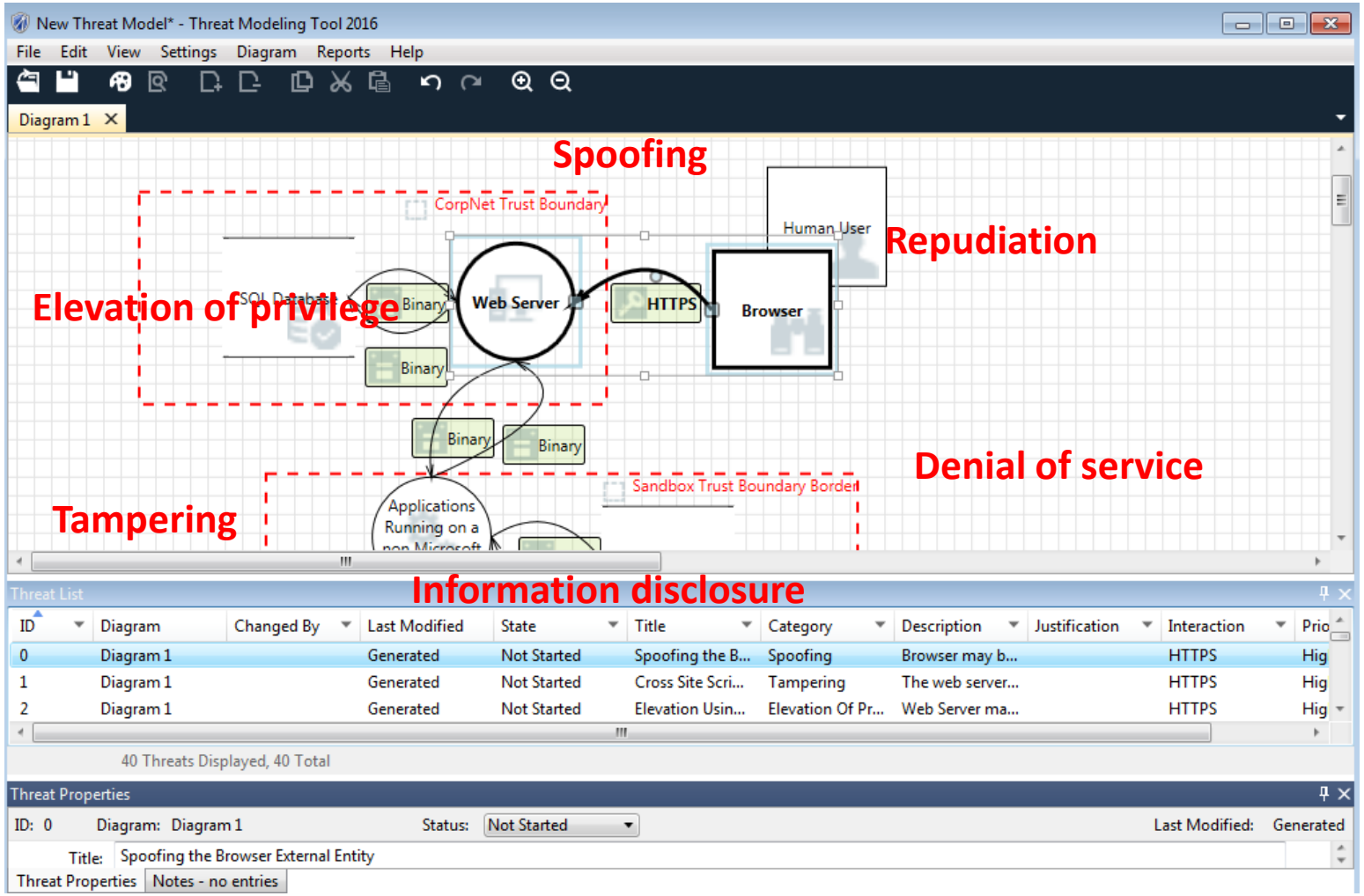


BODFORSS

Identify the weak links

BODFORSS

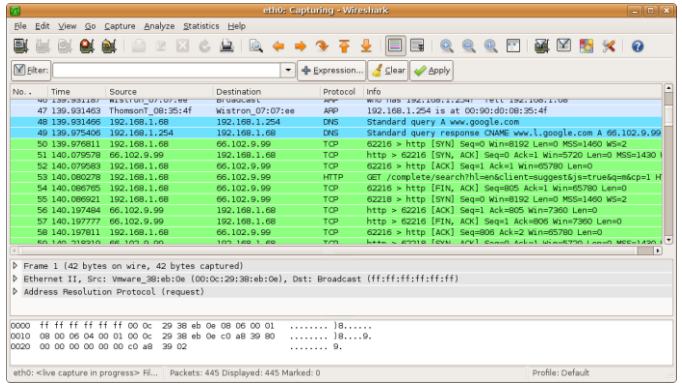
Identify attack vectors



BODFORSS

More passive methods

- Log analysis
- Wireshark, Sniffer, etc.
- Monitor ports
- Passive wireless tools
- Config file analysis
- System charts
- Process inventory
- Protocol analyzers for I2C, RS232, RS485, etc.
- Etc….



BODFORSS

Drawbacks with passive methods

- Won’t find everything
- False sense of security
- Demands skills, experience and competence
- Time consuming

Active test methods

BODFORSS

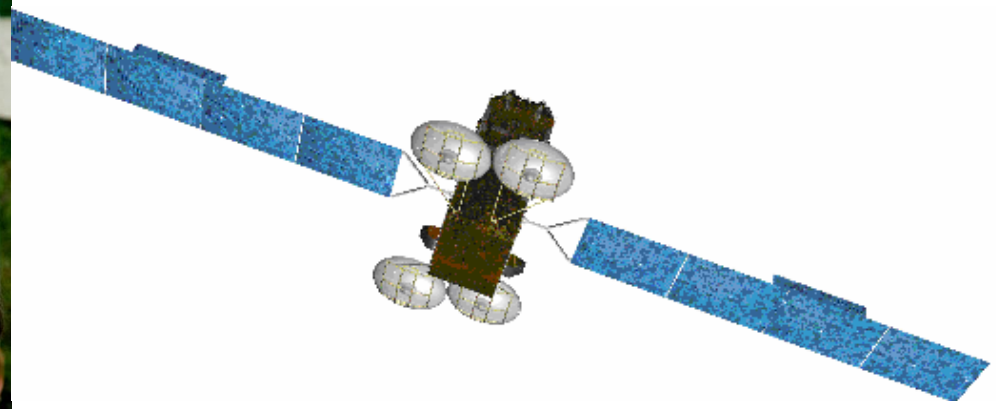
Target analysis

BODFORSS

Test systems

BODFORSS

FAT/SAT



BODFORSS

Virtualization

BODFORSS

Active methods

- Test systems (PHYSICALLY separated)
- Virtualization in lab environment (PHYSICALLY separated)
- FAT tests at supplier
- SAT tests on pre-production systems
- Shodan.io on your own networks
- Hack someone else (Just KIDDING!!!!!)

BODFORSS

Problems with active methods

- Lab is always a lab
- Real world and map don’t match
- Oops… I thought those systems were running on separate environments…

BODFORSS

Choosing methods

BODFORSS

It all comes down to risk appetite and scope

- Your mileage may vary…
- There are many ways to skin a cat….
- ”It depends…”

BODFORSS

Who should perform the tests?

- Internal or external
- If external, check for reference assignments
- Security clearance for sensitive infrastructure?
- Competence

BODFORSS

Summary

And some final thoughts

Trust, but verify

BODFORSS

Nobody is an expert on everything

- Share intel with colleagues in the business
- Hire help if you don’t have all the pieces in the puzzle
- Become friends with the automation engineers
- Create teams and networks
- Cooperate with the suppliers
- Constant improvements (PDCA)
- Work strategically and proactively with risk management

BODFORSS

Network and cooperate

- Learn from colleagues and peers in the business
- Form expert teams with specialists from both the business side and from the suppliers
- Attend conferences and network meetings
- Share knowledge and data

BODFORSS

Further reading (and listening)

- http://energy.sandia.gov/wp-content//gallery/uploads/sand_2005_2846p.pdf
- https://scadahacker.com/library/
- https://www.msb.se/scada
- http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf
- https://ics-cert.us-cert.gov/Standards-and-References
- https://www.microsoft.com/en-us/sdl/
- http://www.rics.se/
- http://www.sakerhetspodcasten.se/

BODFORSS

Thank you for listening!

Rikard Bodforss

Twitter: @rbodforss

Web: www.bodforss.se

www.sakerhetspodcasten.se

Email: rikard.bodforss@bodforss.se

Tel: +46-70 312 33 11

BODFORSS