Some notes on pentesting

Robert Malmgren, ROMAB
Senior security consultant
rom@romab.com
+46-708-330378

Why discuss pentests in a SCADA context: **Reasons**

- It has good entertainment or drama value: Seeing is believing
- CSO need budget boost?
- Political fight between CIO / IT operations and the people running the process IT system?
- Used to arm wrestle with the vendor?
- Security researchers / consultants on a PR trip?
- Technical hubris?
- Real reasons: e.g. changes in IT landscape, moving from island to full integrations with business IT systems.

Caveat emptor!

- **Obtaining** security-by-testing is a broken perception
  - test cases might be incomplete or wrong
  - tests might not reflect original or contemporary risk analysis
  - testers might not be skillful enough or having a bad day
  - test tools might not work as anticipated
  - Usage of another IP adress, other user name or different software version might render very different results
  - etc

- But the alternatives are not realistic...
  - Security-obtained-because-software-based-on-standards
  - Pipe dreams, i.e. flawlessly designed software maintained by flawless operators
  - Certification will ensure all security bugs are non-existent.

  Yeah, right....

The problems with pentests

- Many automated tools...
  - ...is unfit to use in **that** sensitive environment, e.g. to demanding
  - ...is not transparent, hence can you trust the software you plan to run
  - ...does not include support for **that old** vulnerabilities
  - ...certainly is not capable of testing **that** proprietary protocol
  - ...does not provide the answers to some of the fundamental quesitons, e.g. quality of risk assessment
- **The lack of positive results does not equal a secure system**

Technical assessments

- Can include pentest parts, but also includes
  - visual checks of physical & logical setup
  - manual checks of system/application/infrastructrure setup & configuration
  - interviews sometime reveal more than technical tests, e.g. politics behind design decisions.
- The important part here is that audit/assessments are much more than pentests alone

Information sharing

"The good guys have CERT, and the bad guys have IRC. Game over"

Marcus Ranum, anno 1995

Interpretation: We are **always lagging behind** in terms of knowledge of the latest vulnerabilities, or having the option to schedule an update window for the latesf patches, etc

This, of course, is not only valid for pure information, but more imporantly for source code, attack tools, etc.

Open vs unpublished research

- Since SCADA security is labled Critical infrastructure & National security government labs vulnerability findings will not end up in an open source vulnerability scanner near you, hence **you** will not find all flaws even with the latest scanner version.

- SCADA/PCS vendors still have a long way to go to understand Internet age vulnerability handling, e.g. rapid response, being able to co-operate with flaw finders, having the right mindset for open or honest discussions with customers or third parties.

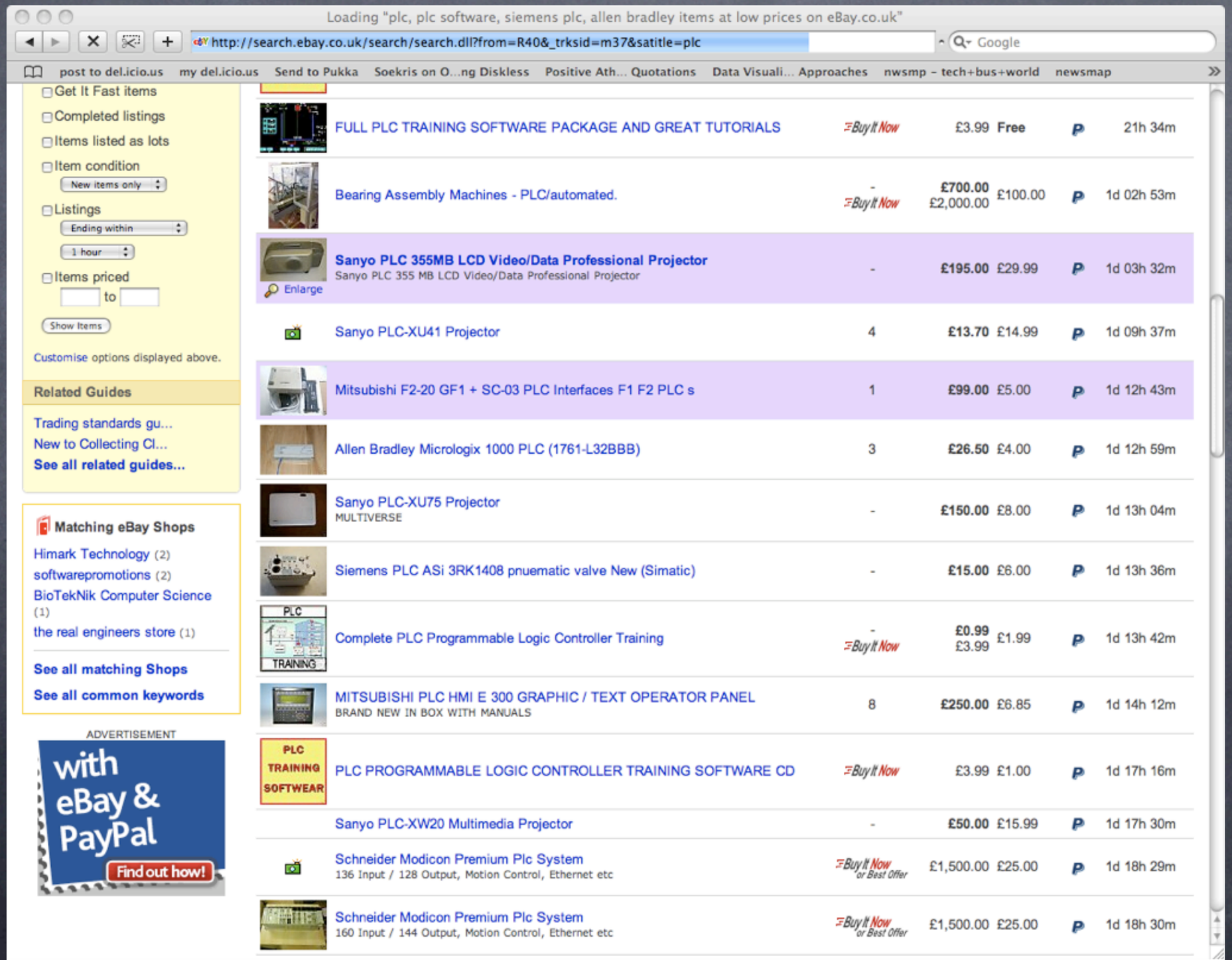
How to run the tests

- Black box & unannounced <-> White box & in cooperation with responsible staff on-site
- In a live environment some extra precautions must be taken:
  - Just target single-nodes in HA setups, ie netscans are dangerous
  - Using debug or test features of the setup
  - Some equipment might need to be disabled during the test session
  - Having people (vendor reps, operators, etc) on-call to be able to switch to manual routines or disaster recovery

Summary

- Doing pentests is really great, if.....
  - ...done for the right reasons
  - ...the right precautions and safety measures are done
  - ...if you're ready to test your disaster recovery plan
  - ...having the right tests cases, right selection of tools and relevant checks
  - ...and using the methodology, still knowing that its built-in drawbacks
- The results from pen tests is more useful if combined into a more complete technical assessment

Still people rely on the obscurity factor



Still people rely on the obscurity factor

LAPTOP WITH PLC/HMI/SCADA COMMISSIONING MACHINE on eBay, also...Business, Offic

http://cgi.ebay.co.uk/ws/eBayISAPI.dll?ViewItem&ssPageName=STRK:MEWA

post to del.icio.us | my del.icio.us | Send to Pukka | Soekris on O...ng Diskless | Positive Ath... Quotat

View larger picture

Winning bid: **£720.00**

Ended: **04-Mar-08 14:48:45 GMT**
Postage costs: To Sweden -- Not specified
Post to: United Kingdom
Item location: Birmingham, West Midlands, United Kingdom
History: 4 bids
Winning bidder: 6890chapman (242)

You can also: Email to a friend

Listing and payment details: Show

Description (revised)

Item Specifics
Condition: **Used**

Dell inspiron 3800 renowed for its super stable operation in the workplace and in the field

Comes with windows 2000 and all the following PLC Automation software fully installed and activ

- Allen Bradley RSLOGIX 500
- Allen Bradley RSLOGIX 500 trainer
- Allen Bradley RSLOGIX 500 Emulate
- Allen Bradley RSLOGIX 5
- Allen Bradley RSLOGIX 5000 Enterprise "The expensive one"
- Allen Bradley RSLOGIX 5000 trainer
- Allen Bradley RSLOGIX 5000 Emulate
- Allen Bradley RSLINX full version not lite version
- Allen Bradley panel builder 32 hmi software
- Allen Bradley RSView 32 supervisor edition with 100K tags
- Allen Bradley RSView studio enterprise
- Allen Bradley Automated desktop
- Allen Bradley Fieldbus
- Allen Bradley Ladder 5
- Allen Bradley Ladder 500
- Allen Bradley RSMacc
- Allen Bradley control flash upgrade software

LAPTOP WITH PLC/HMI/SCADA COMMISSIONING MACHINE on eBay, also...Business, Office Industrial (end time 04-Mar-08 14:48:45 GMT)

http://cgi.ebay.co.uk/ws/eBayISAPI.dll?ViewItem&ssPageName=STRK:MEWAX:IT&item=2602

Google

post to del.icio.us | my del.icio.us | Send to Pukka | Soekris on O...ng Diskless | Positive Ath... Quotations | Data Visuali... Approaches

- Fuji FLEX_PLC
- Nais FPSOFT
- Full CITECT SCADA package including runtime and work licence
- Kepware
- Mac 50 software for misubishi HMI "older version"
- E-designer for Mitsubishi HMI "new versions"
- Mitsubishi HMI tools
- Mitsubishi remote access View
- Mac programmer plus for mac 10 mac 50 mac 90 etc
- Mitsubishi Melsec GX developer
- Mitsubishi GX simulator
- Mitsubishi GT works GOT HMI range
- Siemens logo
- Toshiba TCPRGROS
- Toshiba TSPC robot software
- Zelio
- Crouzet millennium
- Gmwin for LG and IMO plc
- Idec WINDLR
- Idec WINDLGC
- Idec Wind I/O-Nv
- Omron syswin plc
- Omron sysdrive
- Siemens Prodave S7
- Mitsubishi programming manuals
- Mitsubishi books

Plus full IEE 16th edition test and inspection software and certificate printing software forms etc.

CableCalc Pro wiring and distribution software and certification software that covers from substation to end of line with fuse breaker sizing cable

Include the award winning AUTOMATION STUDIO software for full design and test of almost any project

Also CADDY+ software for wiring and documentation manuals etc.

Turbofast Cad software and some automotive software and tools.