



Markus Braendle, Ragnar Schierholz, ABB

Integrating Product Robustness Testing into the Development Lifecycle

ICSJWG 2010 Fall Conference

© ABB Group
November 1, 2010 | Slide 1

Power and productivity
for a better world™ **ABB**

*Program testing can be used to show the presence
of bugs, but never to show their absence!*

The fundamental limitations of testing - Edsger Wybe Dijkstra, 1972

© ABB Group
November 1, 2010 | Slide 2

ABB

Robustness testing @ ABB – the beginnings

Testing done to get attention

- Not very well-defined -> use whatever tools can be found online
(which are not automatically deleted by AV because of corporate IT-policy)
- Goal: show developers that their box can actually crash
(and crash badly)

Testing driven by corporate research

- Broad testing done to show overall need
- Goal: evaluate need for and benefit of robustness testing

Testing done to meet certification requests

Robustness testing @ ABB – today ABB's device security assurance center



Formally established centralized & independent testing facility

Formalized part of all device development

Assures well-defined, consistent approach

Utilizes commercial, open-source and proprietary tools

Employs 5 full time “testers”

In 2010: > 120 tests performed / planned

Challenges

Finding the right setup

Dedicated, trained testers

- Having the right mindset
- Technology evangelists
- In the beginning focus on security know-how
- Today: more and more product know-how needed

Independence from development units to assure objective testing

Support from management

Challenges

Product management

In the mind of the product managers:

- You are just adding unnecessary costs
- You are just delaying product release
- There is no real market demand
- Results will make them look bad (early on testing results were treated strictly confidential)

Challenges Product management

Getting their support:

- Show that testing improves product reliability and quality
- Show and explain test reports to them
- Show that information sharing helps them
- Cover costs centrally
- (get their competitiveness going)

Challenges Development teams

In the mind of the developers:

- You are telling them THEIR code is faulty
- You have no understanding of their system
- You are just adding to their workload
- What you do is OUT OF SPEC!!!
- Will at most cause a process or device to reboot

Challenges Development teams

Getting their support:

- Show that you can help fix found issues
- Raise awareness, e.g. explain how a buffer overflow can be exploited or show how you can completely crash their device
- Go after their crown jewels, i.e. crash the protection function and not the web server
- Make testing as easy, cheap and quick as possible

Challenges Fixing the found issues

Keys to success:

- Formally integrate testing into development process
- Possibility to reproduce faults in development centers
 - without need for all the testing equipment
 - without need for in-depth know-how of security tools
- Fundamental understanding by developers
- Acknowledging fixed issues after next test cycle

Negative factors:

- Many issues are part of 3rd party components, e.g. communication stack of OS
- Faults found long time after code was written
- Faults found close to product release

Limitations Technical

Testing is not 100% consistent

- Same device tested with same testing tools can result in different findings!
- Different configuration can result in different findings
- testing needs to be done continuously

No single tool has comprehensive coverage

- Different tools will find different issues
- use of multiple tools improves quality of findings

Testing of clients is (rarely) supported

- ABB developing proprietary tools

Certification

Purpose of certification

- Solve the information asymmetry to prevent market failure
Security properties of a product are difficult to assess for a customer (hidden characteristics)
- Reduce the transaction costs in procurement
Make the selection process easier to differentiate qualified suppliers from the non-qualified suppliers

History of certification

- Various types of security certification attempts have been tried in the IT industry, most have failed to deliver the expected value
- Learn from the history to prevent its repetition

Certification

Issues found with certification programs

- Certification criteria
 - Must be meaningful measurements of actual security property¹
 - Must be transparent so the principal can check for fit
 - Must take the context of use into account
- Race to the bottom
 - Certification labs only compete on price, but have no liability
 - Incentive is to reduce cost by lax testing / auditing
- Adverse selection
 - Only vendors who can't demonstrate security with more meaningful and context-specific signals will pursue certification
- Lifecycle coverage
 - Recertification dilemma with new vulnerabilities or attack paths

© ABB Group
November 1, 2010 | Slide 13

¹ See also S. Pfleeger and R. Cunningham, "Why Measuring Security Is Hard," *IEEE Security & Privacy Magazine*, vol. 8, 2010, pp. 46-54, and further references in the full paper to be published with ICSJWG material



Lessons learned

Test long enough, you'll find security issues

Organization / top management support is essential

Need for security training paramount to successful program

Run awareness campaigns, e.g. workshops,

Have security experts/managers sign-off on tests, code review, etc.

© ABB Group
November 1, 2010 | Slide 14



Robustness testing @ ABB – today ABB's device security assurance center



- Formally established centralized & independent testing facility
- Employs 5 full time “testers”
- Assures **well-defined, consistent** approach
- Utilizes commercial, open-source and proprietary tools
- **Formalized** part of all device development
- In 2010: > **120 tests** performed / planned

© ABB Group
November 1, 2010 | Slide 15

ABB

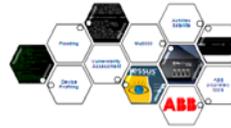
Robustness testing @ ABB – Tomorrow

Development Centers

- Increased security know-how
- Early & constant testing
- Testing in more complex system environment



Device security verification center



- Formally established centralized & independent testing facility
- Employs 5 full time “testers”
- Assures **well-defined, consistent** approach
- Utilizes commercial, open-source and proprietary tools
- **Formalized** part of all device development
- In 2010: > **120 tests** performed / planned

© ABB Group
November 1, 2010 | Slide 16

ABB

Conclusions

Security testing can be used to show the presence of **vulnerabilities**, but never to show their absence!

Some security geek

© ABB Group
November 1, 2010 | Slide 17



Contact information

Dr. Markus Braendle

Division Cyber Security Manager
Power Systems

ABB Inc.

940 Main Campus Drive
Raleigh, NC 27606
Phone 919 856 2418
Mobile 919 780 8513
E-Mail: markus.braendle@us.abb.com



Dr. Ragnar Schierholz

Principal Scientist
Industrial Software Systems

ABB Switzerland

Corporate Research
Segelhofstr. 1K
CH-5405 Baden 5 Dättwil
Phone +41 58 586 82 97
E-Mail ragnar.schierholz@ch.abb.com



© ABB Group
November 1, 2010 | Slide 18



Power and productivity
for a better world™

