Current challenges in testing methods for IoT solutions

Miroslav Bures
Czech Technical University in Prague
Czech Republic

QRS 2017 Prague March 25th 2017

Program of this session

- Current challenges in IoT quality – a global view.
  - *Which aspects in IoT are considered the most challenging?*
- A recent survey in Czech industry IoT providers
  - *Which methods/tools the industry needs for ensuring quality of IoT solutions?*
- What do you consider as a priority in IoT quality in accord to your experience?
  - *A short discussion and experience sharing*
- Preliminary results of a literature mapping study in IoT QA
  - *What is being researched currently?*
  - *Which areas we consider as not covered yet?*
- A short introduction to “QA Framework for IoT solutions project”

Current challenges in IoT quality

Security

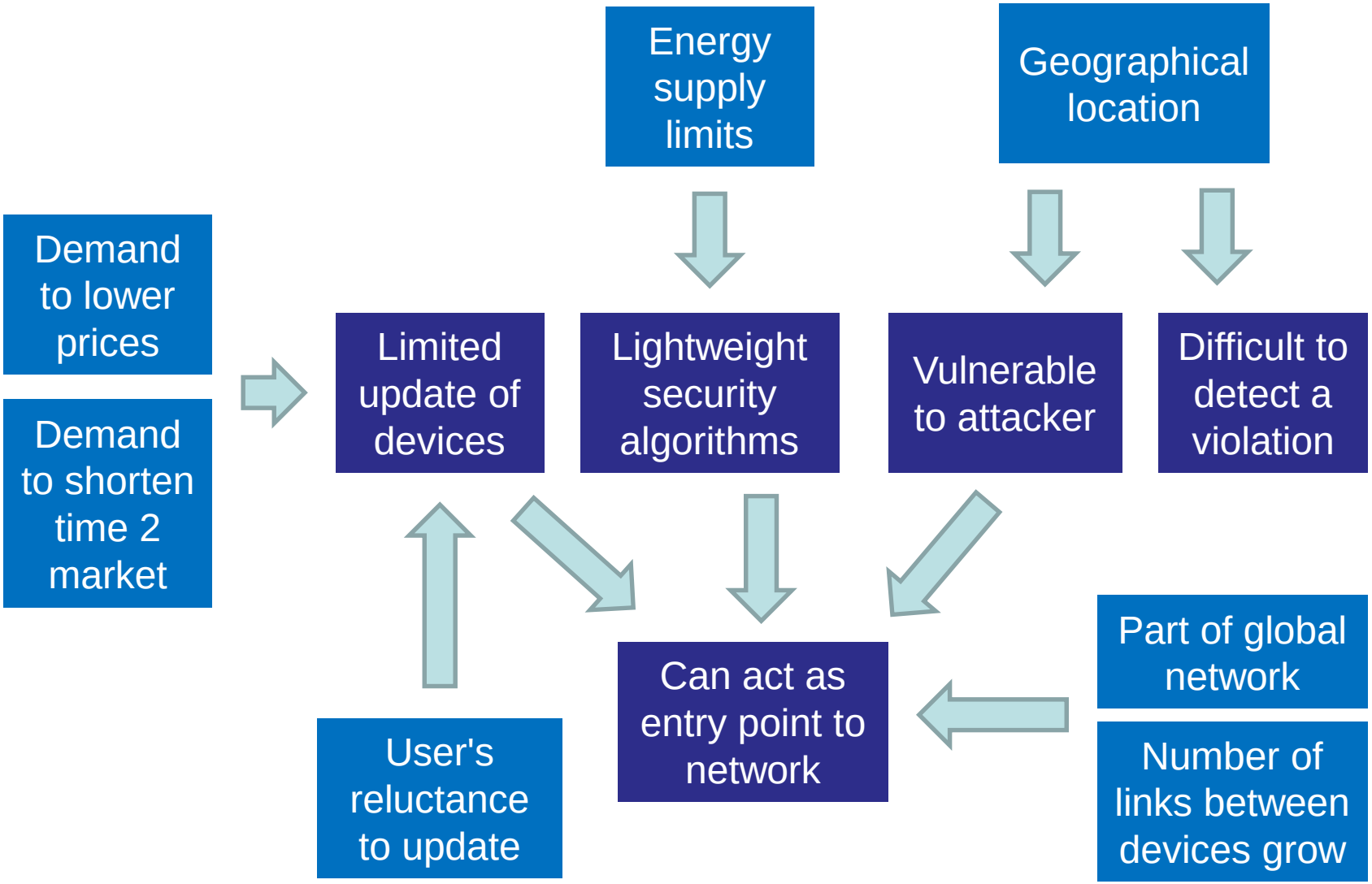
Features of IoT solutions

- Demand to lower prices of IoT devices
- Pressure to shorten time to market
- Updates of IoT devices online can be impossible
- Energy consumption issues → lightweight security algorithms
- Number of links between devices grows
- User can have low insight into internal mechanism of a device
- If a device is updated, user can have low control about the updates
- Some devices in places, where can be easilly acessed by attacker
- IoT devices connected to whole internet
- IoT devices with voice recognition / embedded cameras
- Home-made devices not implementing industry standards

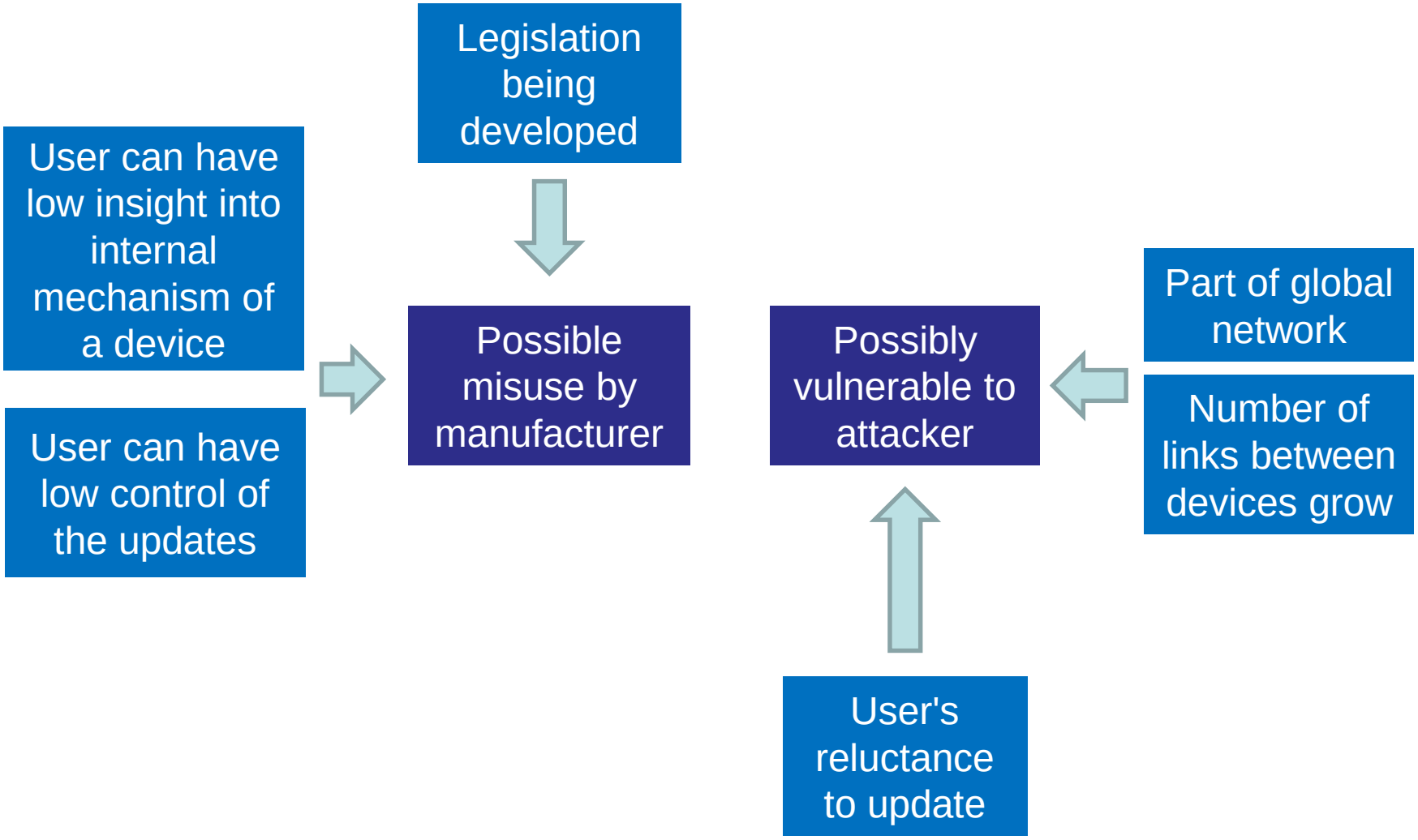
Consequences

- Possible security problems of IoT devices
- IoT devices can serve as a weakpoint to get to whole network

Issue 1: IoT device as a weak entry point to network



Issue 2: IoT device violating user's privacy



Privacy

Features of IoT solutions

- Various personal data can be collected
- Legislative issues being discussed in parallel with technology development
- Part of IoT devices don't have interface to accept contractual conditions
- Local legislations vs. global solution

Consequences

- Opportunities to misuse of personal data are increasing
- Low user's insight into data privacy mechanism
- Possible user's digital portrait reconstruction
- Division between public and private space can become less strict
- Would there be services available for the users who don't accept data collection?

Data being collected

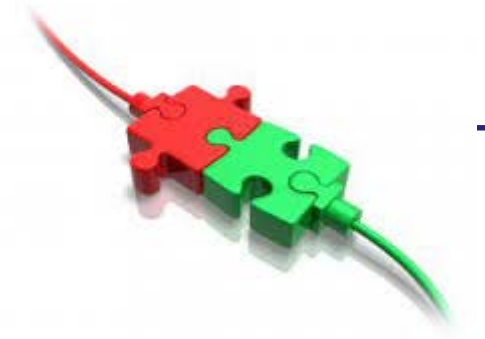
Current web/mobile cloud applications:

- User's interest – browsing history
- Online shopping
- Geolocation
- ...

IoT can add more:

- Personal health information
- Eating habits
- Voice recognition
- Image recognition
- More detailed geolocation

Interoperability



Features of IoT solutions

- Various protocols used – IPv6, Bluetooth, ZigBee, proprietary industry protocols, ...
- Updates of IoT devices online can be impossible → number of versions grows
- Intentional "vendor lockout" is also possible

Consequences

- A combinational explosion of various devices and protocols to test
- Increased demand to integration testing
- Testing requirements spans also to hardware and protocols (in Internet, we consider them tested already)

Reliability of service

Features of IoT solutions

- Dependency of user to the network service grows
- Users get used to the service and their demands for service availability continously grow

Consequences

- We need to test more intensely:
  - Behaviour of IoT soulution under limited connection
  - Transactionality of the applications, resp. failover management

Heterogenity

What is IoT?

- Various possible applications and architectures are in place:
  sensor networks,
  smart cars with sharing,
  whitegood connected to web,
  personal devices,
  ...

Consequences

- Is it possible to generalize a IoT specific testing methodology?

A survey among the Czech IoT industry

Challenging quality aspects

Which of the quality aspects of the IoT do you consider the most challenging?

1. Security issues
2. Privacy issues
3. Performance issues
4. Interoperability, missing or insufficient standards, proprietary standards vs. internet standards
5. Legislation issues
6. Behavior of the system under limited network connection
7. Integration issues
8. Number of various configurations and types of the end nodes, making the solution hard to test om all these combinations
9. Focusing of test efforts efficiently to important aspects and critical parts of the infrastructure

Challenging quality aspects

	company/business					
	#1	**#2**	**#3**	**#4**	**#5**	**#6**
	Smart cars	**White Goods**	**Smart TVs**	**Infrastructure**	**Infrastructure**	**R&D**
1 Security	**HIGH**	**HIGH**	**LOW**	**MEDIUM**	**HIGH**	**HIGH**
2 Privacy	**HIGH**	**HIGH**	**HIGH**	**MEDIUM**	**MEDIUM**	**MEDIUM**
3 Performance	**HIGH**	**MEDIUM**	**HIGH**	**MEDIUM**	**LOW**	**HIGH**
4 Interoperability	**HIGH**	**HIGH**	**HIGH**	**HIGH**	**MEDIUM**	**HIGH**
5 Legislation	**MEDIUM**	**LOW**	**MEDIUM**	**HIGH**	**LOW**	**HIGH**
6 Limited connection	**HIGH**	**HIGH**	**MEDIUM**	**HIGH**	**HIGH**	**HIGH**
7 Integration	**HIGH**	**LOW**	**MEDIUM**	**MEDIUM**	**MEDIUM**	**HIGH**
8 Configurations	**HIGH**	**HIGH**	**HIGH**	**HIGH**	**HIGH**	**MEDIUM**
9 Test effort focus	**HIGH**	**LOW**	**HIGH**	**HIGH**	**MEDIUM**	**HIGH**

Challenging quality aspects

	company/business						
	#1	**#2**	**#3**	**#4**	**#5**	**#6**	
	Smart cars	**White Goods**	**Smart TVs**	**Infrastructure**	**Infrastructure**	**R&D**	**SCORE**
4 Interoperability	3	3	3	3	2	3	**17**
6 Limited connection	3	3	2	3	3	3	**17**
8 Configurations	3	3	3	3	3	2	**17**
1 Security	3	3	1	2	3	3	**15**
2 Privacy	3	3	3	2	2	2	**15**
9 Test effort focus	3	1	3	3	2	3	**15**
3 Performance	3	2	3	2	1	3	**14**
7 Integration	3	1	2	2	2	3	**13**
5 Legislation	2	1	2	3	1	3	**12**

Demands for testing methods

Which principal parts of QA methodology for IoT you need the most?

1. **Test strategy** guidelines
2. **Prioritization mechanism** and way to determine intensity of testing efficiently
3. **Specific test design techniques** reflecting specifics of IoT allowing to create efficient test case scenarios
4. Guidelines, **which parts of the tests to automate** and how
5. Mechanism for **automated generation of test cases** specifically tailored for IoT solution
6. Framework for **efficient automated integration testing** of the IoT solution
7. Set of **integration mockups** and connectors to handle various IoT devices during IoT testing
8. Support of **Continuous Integration process** for development of IoT solutions
9. Semi-automated or **automated reporting** mechanism for test results

Demands for testing methods

	company/business					
	#1	**#2**	**#3**	**#4**	**#5**	**#6**
	Smart cars	**White Goods**	**Smart TVs**	**Infrastructure**	**Infrastructure**	**R&D**
1 Test strategy	HIGH	HIGH	HIGH	HIGH	HIGH	HIGH
2 Test prioritization	HIGH	MEDIUM	HIGH	HIGH	HIGH	MEDIUM
3 Test design techniques	HIGH	HIGH	HIGH	MEDIUM	MEDIUM	HIGH
4 What to automate	MEDIUM	HIGH	HIGH	MEDIUM	LOW	HIGH
5 Automated gen. of TCs	HIGH	HIGH	HIGH	HIGH	HIGH	MEDIUM
6 Aut. integration tests	MEDIUM	HIGH	HIGH	LOW	MEDIUM	MEDIUM
7 Integration mockups	LOW	LOW	LOW	HIGH	MEDIUM	MEDIUM
8 CI compliance	MEDIUM	HIGH	HIGH	LOW	MEDIUM	MEDIUM
9 Automated reporting	MEDIUM	HIGH	HIGH	HIGH	MEDIUM	HIGH

Demands for testing methods

		company/business						
		#1	**#2**	**#3**	**#4**	**#5**	**#6**	
		Smart cars	**White Goods**	**Smart TVs**	**Infrastructure**	**Infrastructure**	**R&D**	**SCORE**
1	Test strategy	3	3	3	3	3	3	**18**
5	Automated gen. of TCs	3	3	3	3	3	2	**17**
2	Test prioritization	3	2	3	3	3	2	**16**
3	Test design techniques	3	3	3	2	2	3	**16**
9	Automated reporting	2	3	3	3	2	3	**16**
4	What to automate	2	3	3	2	1	3	**14**
6	Aut. integration tests	2	3	3	1	2	2	**13**
8	CI compliance	2	3	3	1	2	2	**13**
7	Integration mockups	1	1	1	3	2	2	**10**

What you consider as a priority?

(a discussion)

Challenging quality aspects

Which of the quality aspects of the IoT do you consider the most challenging?

1. Security issues
2. Privacy issues
3. Performance issues
4. Interoperability, missing or insufficient standards, proprietary standards vs. internet standards
5. Legislation issues
6. Behavior of the system under limited network connection
7. Integration issues
8. Number of various configurations and types of the end nodes, making the solution hard to test om all these combinations
9. Focusing of test efforts efficiently to important aspects and critical parts of the infrastructure

Are there another challenges by your experience?

Demands for testing methods

Which principal parts of QA methodology for IoT you need the most?

1. **Test strategy** guidelines
2. **Prioritization mechanism** and way to determine intensity of testing efficiently
3. **Specific test design techniques** reflecting specifics of IoT allowing to create efficient test case scenarios
4. Guidelines, **which parts of the tests to automate** and how
5. Mechanism for **automated generation of test cases** specifically tailored for IoT solution
6. Framework for **efficient automated integration testing** of the IoT solution
7. Set of **integration mockups** and connectors to handle various IoT devices during IoT testing
8. Support of **Continuous Integration process** for development of IoT solutions
9. Semi-automated or **automated reporting** mechanism for test results

Other possible QA challenges?

1. Quality of big data processes?
2. Usability testing?

State of the art
Research challenges

Current literature survey

Databases searched:

1. Springer
2. Elsevier
3. ACM
4. IEEEE
5. Scopus

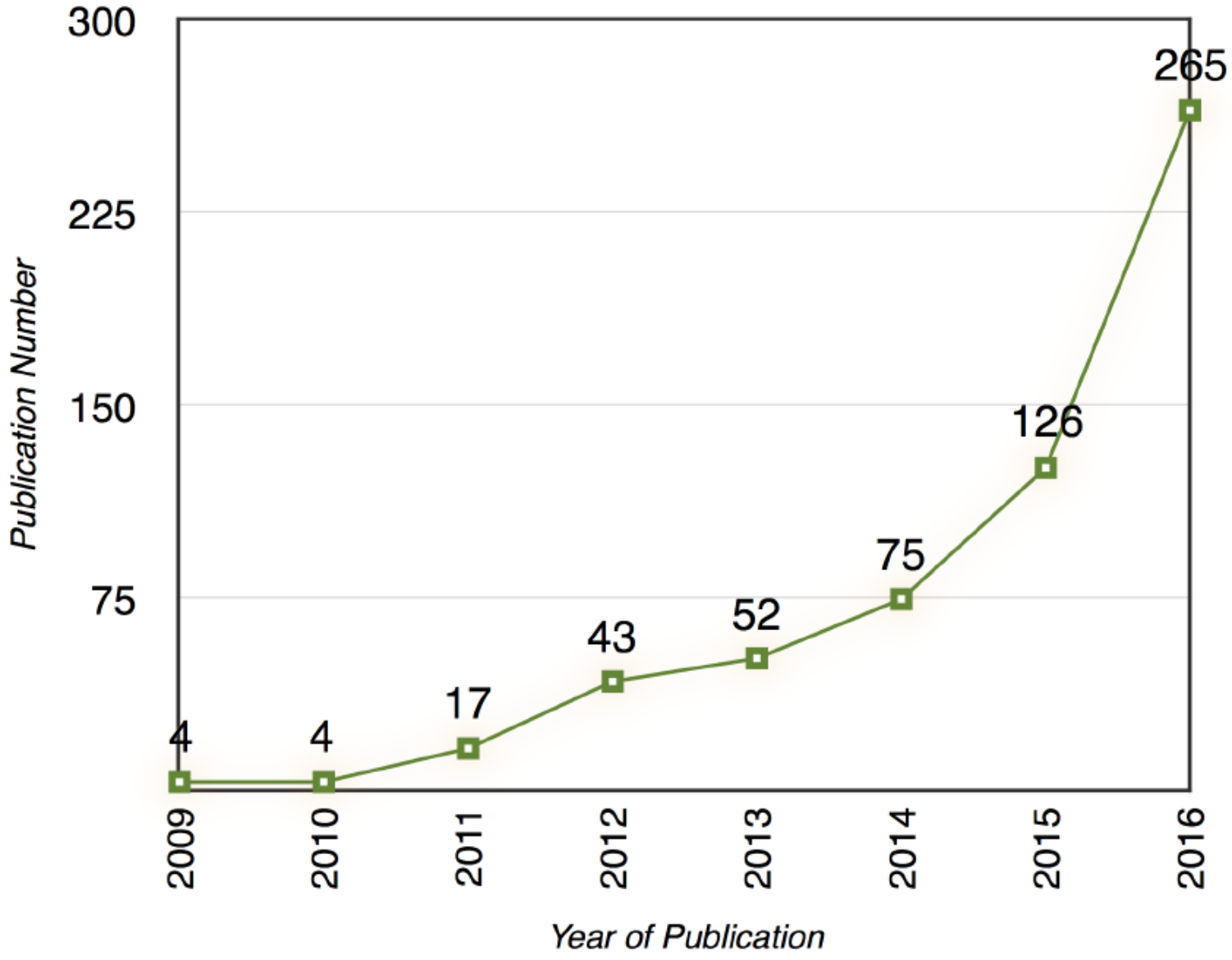
From curently ongoing study, results shall not be present in the final slides published on workshop web

Approx. 600 papers analyzed

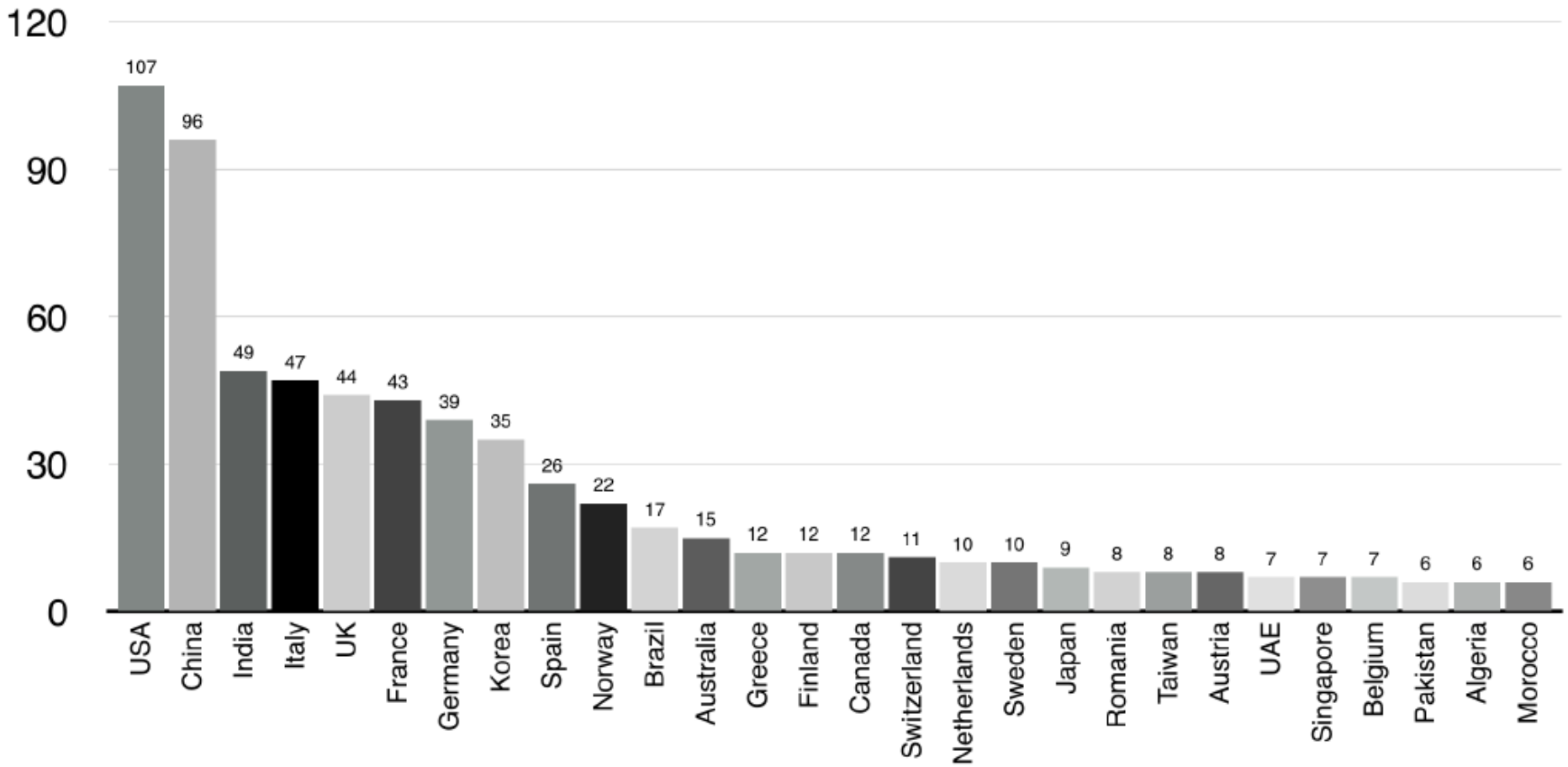
After filtering by relevance and present results – approximate numbers:

Secure architectures	180
Privacy and trust	80
Opinion papers	60
Security testing	50
QA and testing	50
Testbeds	45
General about security	40
Quality and security challenges	15
Performance	10

QA in IoT publication trends



QA in IoT publication trends



QA and testing methods

Areas identified:

- Challenges
- General testing lifecycle

- Model-based testing
- Model checking
- Run-time verification

- Reliability models

- Testing of protocols
- Simulation of the devices

- Test Beds and Testing Frameworks

- Usability testing

- Performance testing

Research opportunities

Discussion:

CIT using the Feature Models for IoT

Workflow (graph paths-based MBT) tailored to IoT reliability specifics

Extension of SUT models to network and physical layer

Technical background for well orchestrated integration testing

QA Framework for IoT solutions project

Project goal

To develop an efficient framework for IoT quality assurance

- Respecting specifics of IoT domain
- Focusing on variety of platforms problem
- Strongly focused on test automation: give manual work to machines
- Model-based testing focused: don't waste one day thinking about the test cases – model the situation one hour instead and let the machine work
- Based on strong know-how and best practices in the QA domain
- Compliant to CI principles

The IoT QA framework

Methods part

- Setting the efficient test strategy
- Determining optimal intensity of testing for various IoT system parts
- Automating the creation of test cases
- Assessing an optimal level and types of test automation

Technical part

- Enhanced JUnit based framework for IoT specific integration testing
- Efficient mock-ups and simulators for specific IoT devices
- CI-compliant automated IoT testing framework and testbed

Project details

Industry and R&D parties welcomed to cooperate and share the project results

Project partners

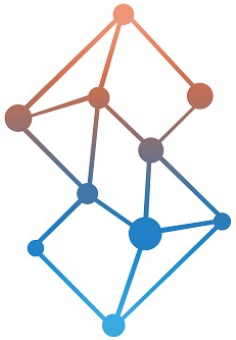
- Czech Technical University in Prague
- RedHat Czech Republic

Timing

- 2017-2021

Contact

Miroslav Bures
STILL – Software Testing IntelLigent Lab
Dept. of Computer Science
FEE, Czech Technical University in Prague
miroslav.bures@fel.cvut.cz
http://still.felk.cvut.cz



STILL
Software Testing IntelLigent Lab