

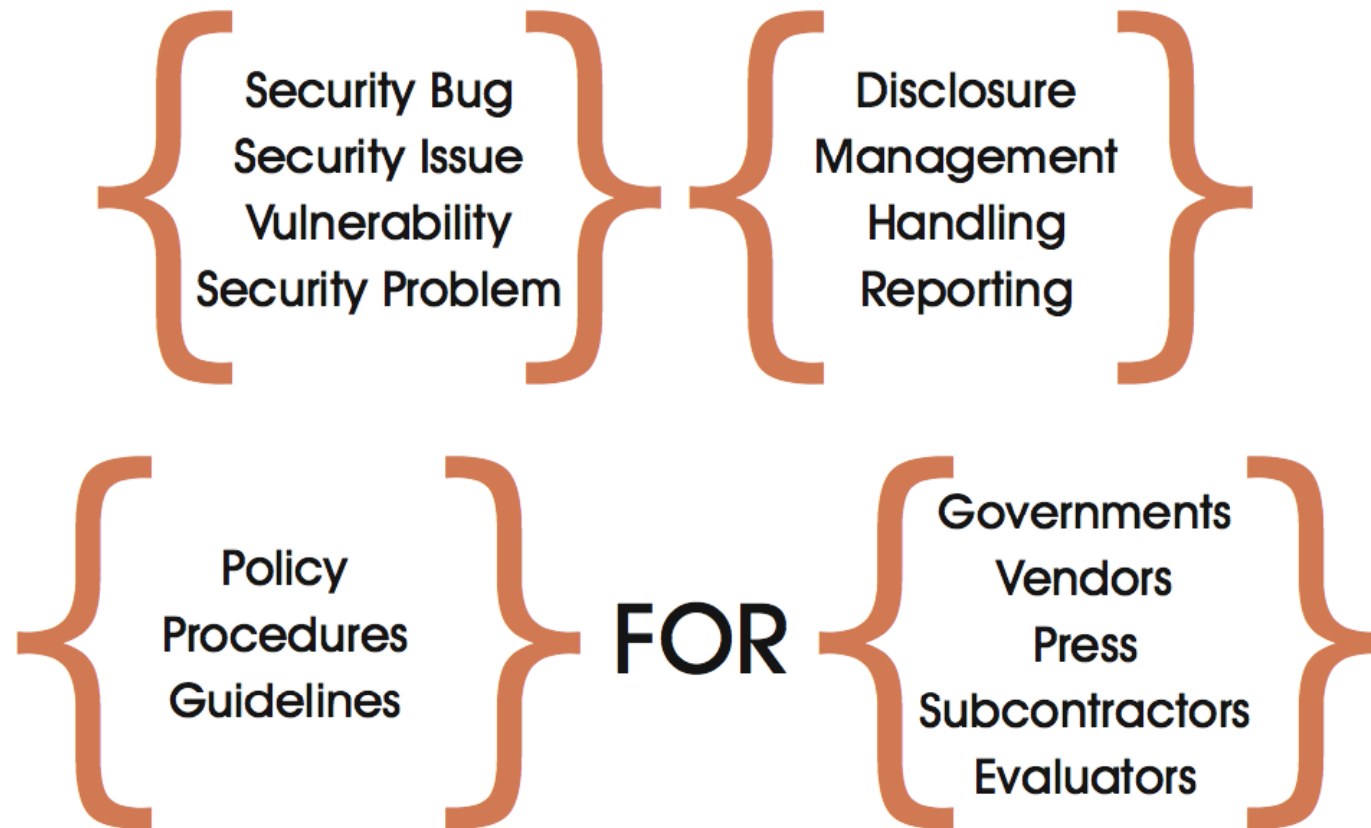
# Setting the Scene: State of play on vulnerability disclosure

Juha Röning, Marko Laakso, Juhani Eronen\*

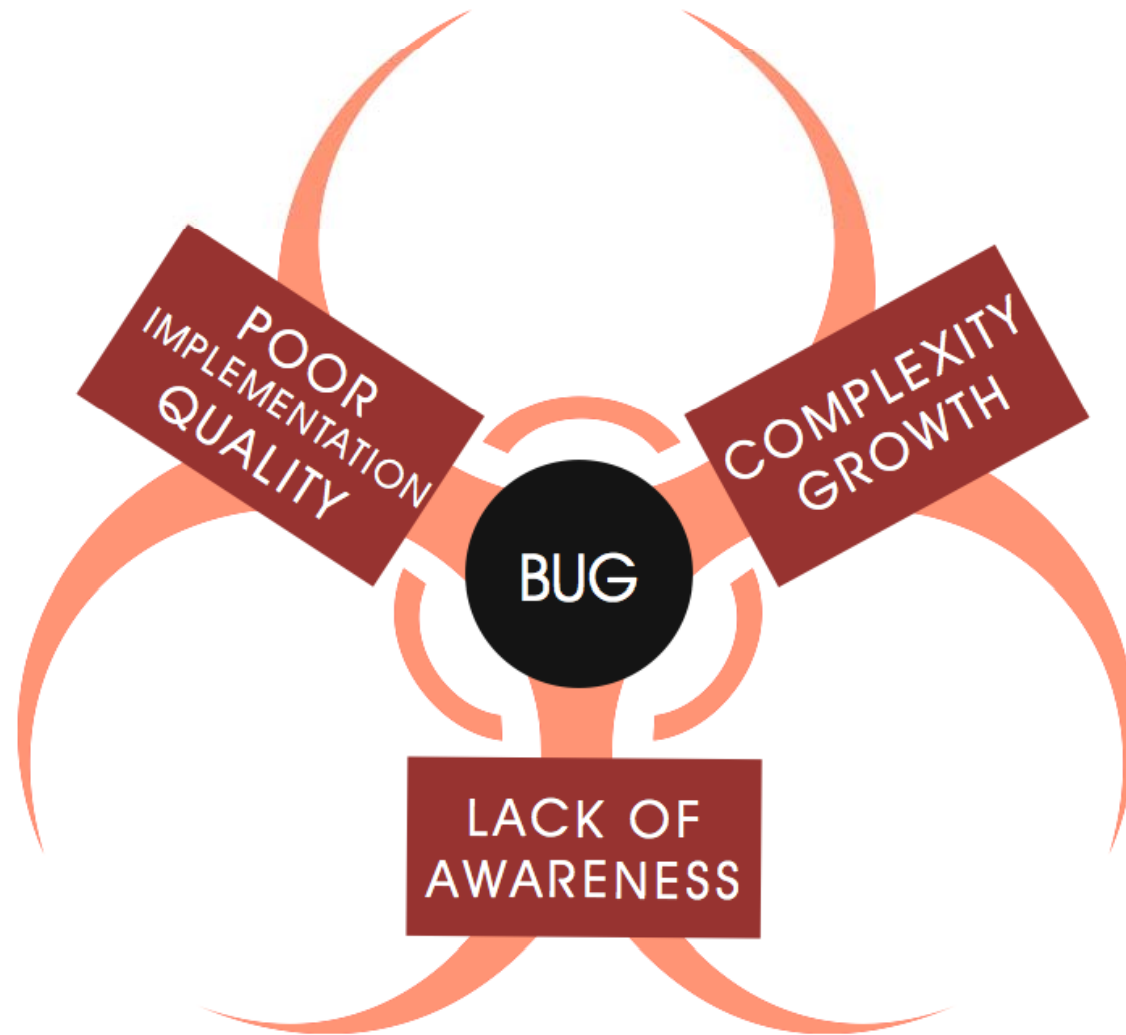
Oulu University Secure Programming Group Department of  
Electrical and Information Engineering [ouspg@ee.oulu.fi](mailto:ouspg@ee.oulu.fi)

\*Finnish Communications Regulatory Authority FICORA  
[juhani.eronen@ficora.fi](mailto:juhani.eronen@ficora.fi)

# Same challenge many names



# Same root problem – the bug (vulnerability)



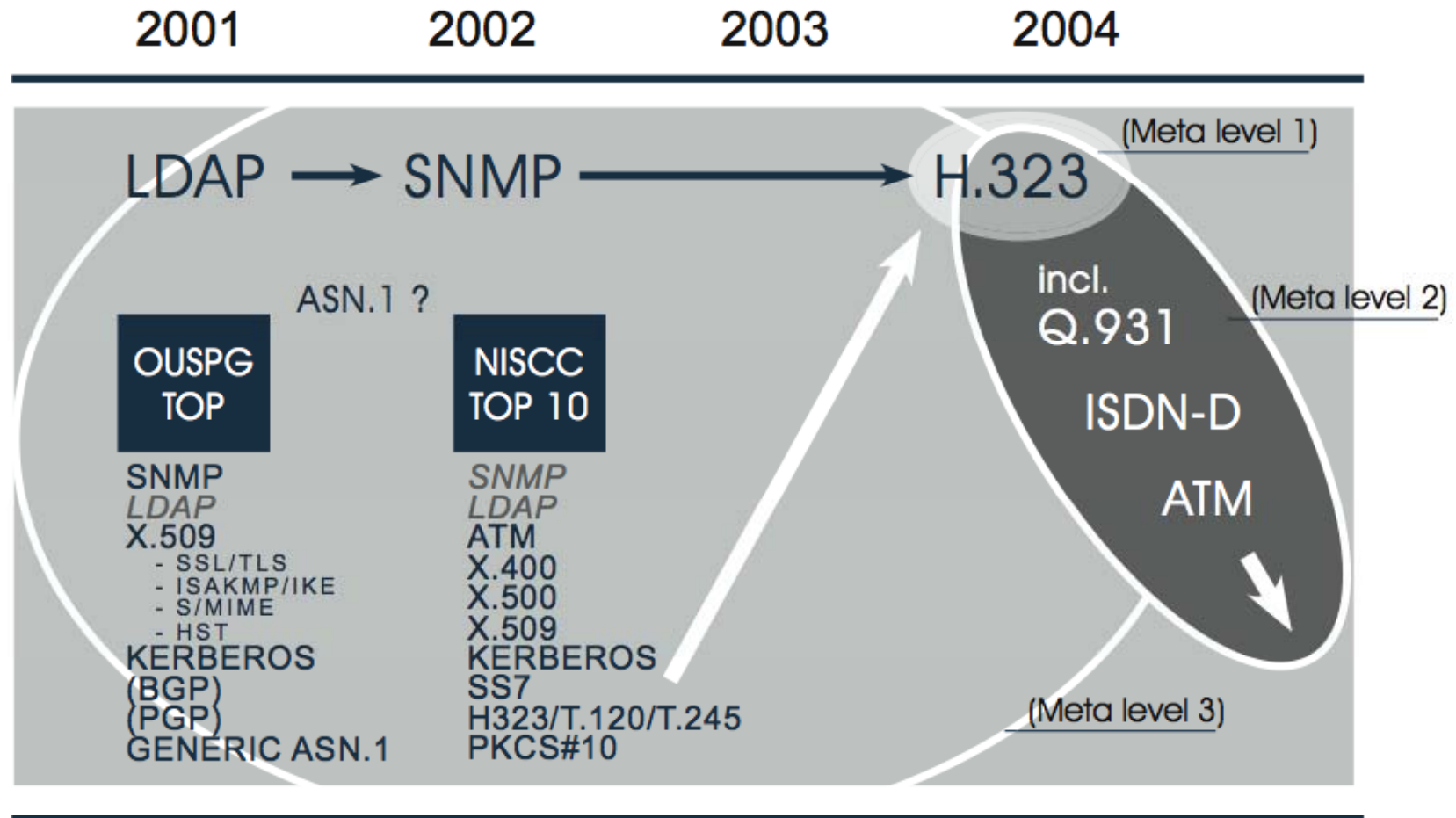
# Not simple to eradicate

- Technical means to tackle the problem
  - ~1 problem
  - ~10 programming/software engineering paradigms (impact in 100 years, needs least resources)
  - ~100 programming languages
  - ~1 000 fundamental ways to shoot yourself in foot
  - ~10 000 popular SDKs/libraries
  - ~100 000 flawed programming books, examples and guidelines
  - ~1 000 000 systems/programs under development
  - ~100 000 000 legacy system (impact almost now, needs infinite resources)
  - ~10 000 000 programmers (Asia!)
- Architecture & Requirements
  - *Security as a new box or bubble* problem -> complexity++
- **Awareness/economics/liability/incentives** ("low" hanging fruit)
- Testing/Validation/Source Code Analysis

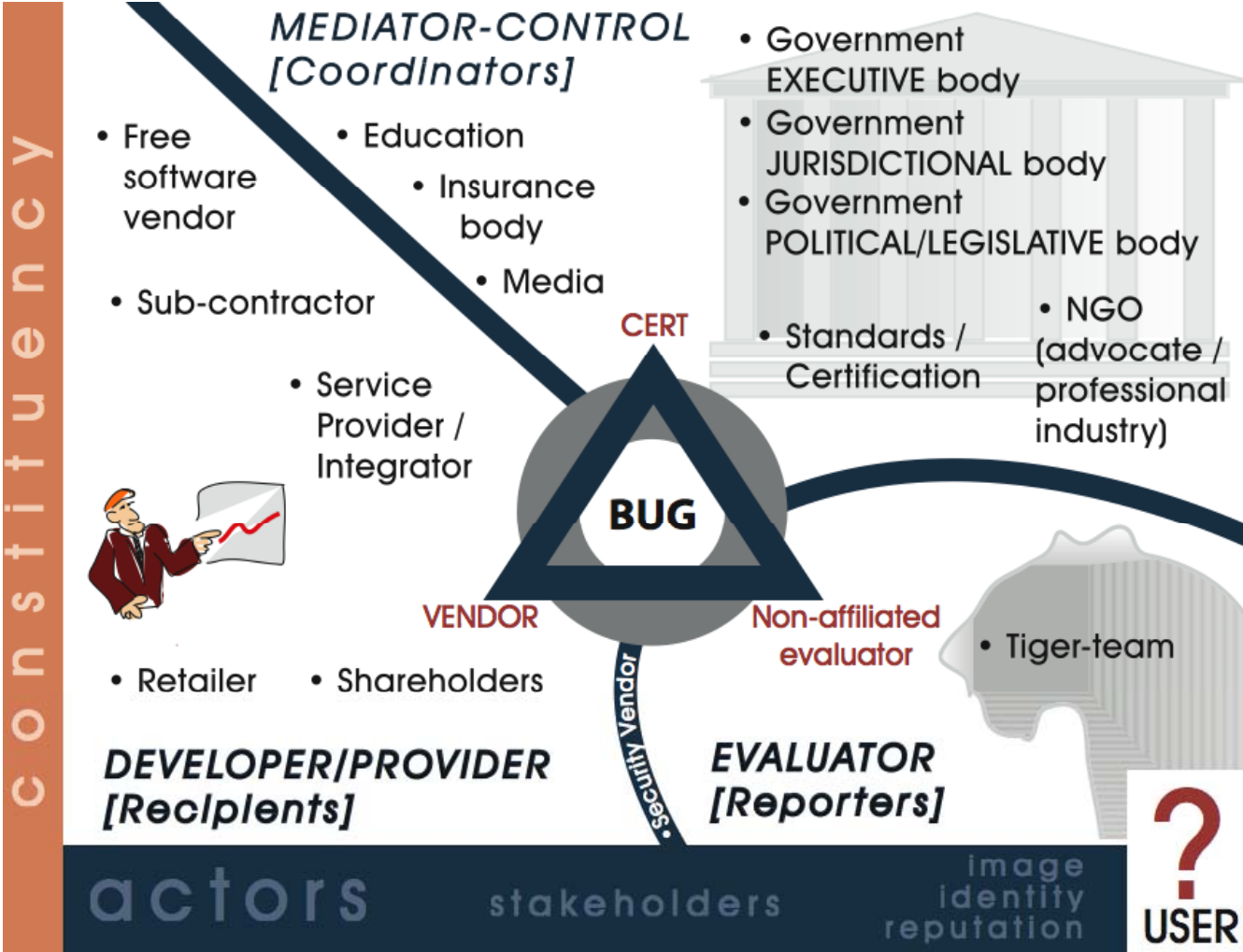
# Metalevels

OUSPG META LEVEL 4	?
OUSPG META LEVEL 3	Single scheme in multiple protocols / protocol families
OUSPG META LEVEL 2	Single protocol embedded in multiple protocol families
OUSPG META LEVEL 1	Single protocol, multiple implementations by multiple vendors
TRADITIONAL APPROACH	Single vendor, single implementation, single vulnerability

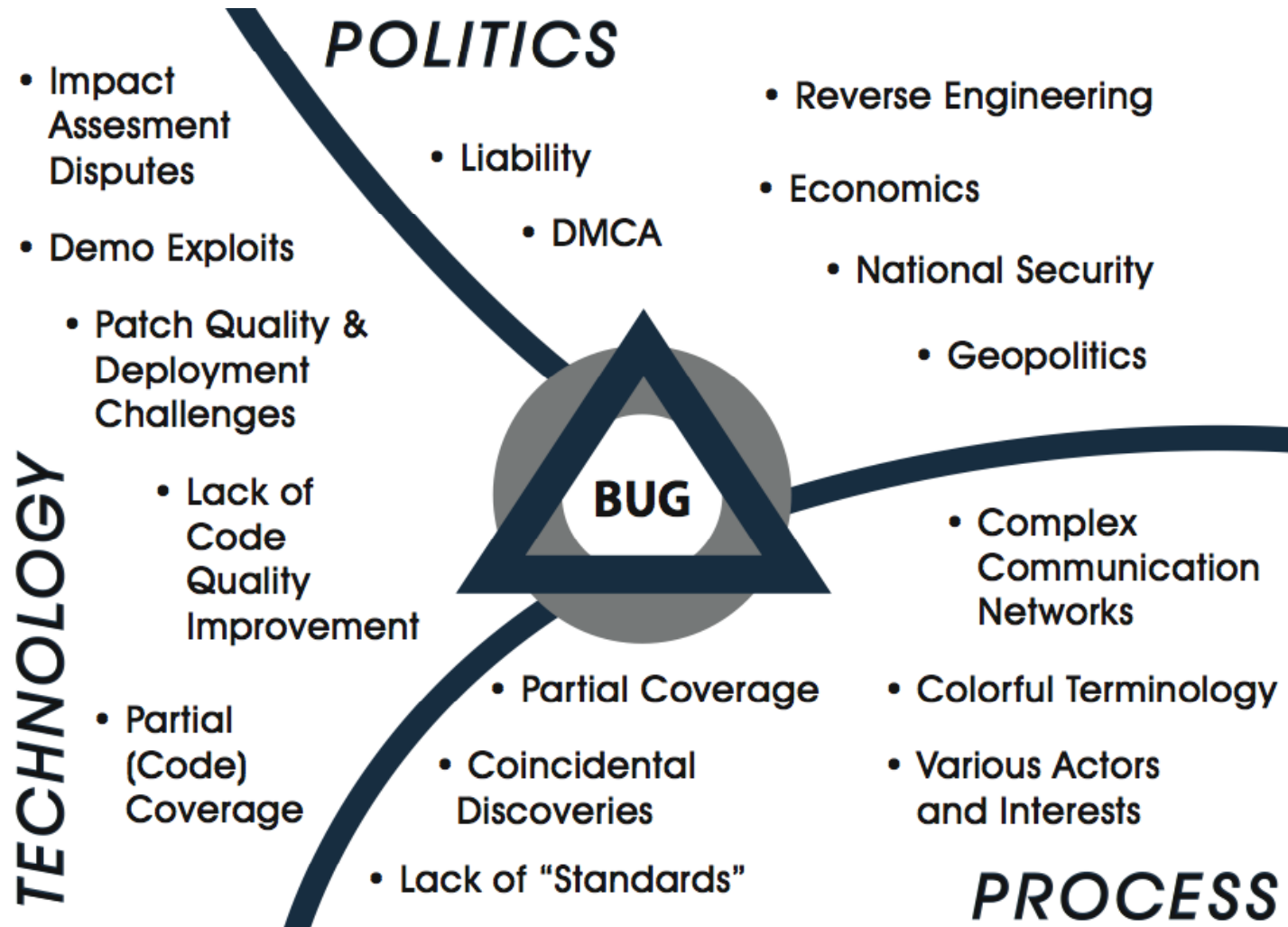
# Multilevel challenge



# Many stakeholders



# Not just technical issue



# Lessons learned

- We have been vulnerable and we will be for foreseeable future
  - Lets learn to live with it and practice for days when impact will be more profound
- Vulnerability scene complexity is perplexing (technical metalevels, stakeholders, ecosystem, process and policitics)
  - Strict and inflexible policies would not help us to deal with changing complex threats
- There is no simple or feasible technical solution, incentives are the low hanging fruit
  - For vendors, operators, coordinators, service providers and researchers
- We need to raise the maturity level of vulnerability scene
  - Shared best practices, awareness and research need development and support
- Support already existing responsible activity
  - See e.g. [Vulnerability Disclosure Framework](#)
  - A recommendation by the National Infrastructure Advisory Council to the President of the United States

# DNS Vulnerability repair

