For a European Cyber-Security Research Infrastructure

ICRI 2014

Research Infrastructures for Global Challenges

April 2, 2014

Athens

Joseph Sifakis

EPFL, Lausanne and CRI, Grenoble

Greek National Council for Research and Technology

Rationale

- Modern economies increasingly rely on ICT for all aspects of daily life. ICT is key to economic development and social welfare. Their impact will accelerate into the future.

- Networked ICT systems have opened new areas for exploitation by intruders and other disruptive elements.

- Cybersecurity threats exploit the increased complexity and connectivity of critical infrastructure systems, placing a nation's security, economy, public safety and health at risk.

- Unfortunately, today's systems are typically not well suited for applications with critical trustworthiness requirements – Cyber-security is a top priority in all developed countries

- Europe needs infrastructure to support research on
  - predicting, identifying, mitigating and preventing cyber security breaches before they occur
  - analyzing, responding to attacks and resolving breaches that take place

Challenges and Impact

- Safer and more secure internet – develop technology for securing communications infrastructure against cyber-attack and resultant cyber-crime
- Protection of critical infrastructures including resource distribution networks e.g. energy and water, as well as banking, health, administration infrastructures
- Development of cutting-edge research requires large-scale experiments on specific infrastructure , international collaboration, and sophisticated and costly equipment
- Training of a cybersecurity workforce for the future- There is a well-documented shortage of general and highly qualified cybersecurity experts
- Contribution to the ongoing effort for development of cyber-security standards for security evaluation and certification
- Provide advice and support for governments and organizations on policing, policy and new legislation

Needed Infrastructure and Facilities

- Ready access to specific networking infrastructure and databases for which new security processes, storage infrastructure and stringent audit capabilities can be tested
  - Data Analytics: The analysis of complex data and behaviors in these large scale-systems can also address issues of provenance, attribution, and discernment of attack patterns
  - Automated Indicator Sharing: provide organizations with timely, actionable information that they can use to detect and respond to cybersecurity events as they are occurring

- Advanced tools and processes to monitor, protect and assess conformity to security standards
  - Test beds in which new devices might be tested in isolation or within the context of networks with the aim of detecting and understanding vulnerabilities
  - Authentication and authorisation infrastructure for individuals and devices that is proven secure and interoperable
  - Conformity assessment infrastructure methods and tools
  - Immersive modelling and simulation centres in which human behaviour of individuals and groups can be facilitated and studied

- Analysis and evaluation of emerging and disruptive technologies and their impact on future cyber security