Popular science summary of the PhD thesis

PhD student	Ricardo Yaben Lopezosa
Title of the PhD thesis	Identifying systemic cyber-security weaknesses in Internet-facing OT and consumer IoT networks
PhD school/Department	Department of Applied Mathematics and Computer Science

Science summary

Cyber-attacks are becoming more frequent and more damaging, yet many Internet-connected devices still lack even basic security protections. From smart home systems and industrial controllers to healthcare and energy infrastructure, millions of devices are directly exposed to the Internet with weak access control, outdated software, or no maintenance at all. This PhD thesis investigates why such cyber-security weaknesses persist, how they can be identified at scale, and how their risks can be mitigated.

The thesis focuses on Internet of Things (IoT) and Operational Technology (OT) devices (i.e, systems that control physical processes such as manufacturing equipment and critical infrastructure). Using Internet-wide measurement techniques (i.e., scanning the whole Internet), the research develops and applies new methods to systematically identify exposed devices and detect signs of misconfiguration, abandonment, and obsolescence. More than ten protocol-specific probes are proposed, enabling the detection of security problems that go beyond well-known vulnerabilities and instead reflect long-term neglect and poor security management.

The thesis also presents a modular framework that supports large-scale Internet measurements and continuous monitoring: DICE, a Device Identification and Classification Engine. This framework enables reproducible research, supports responsible vulnerability disclosure, and helps translate measurement results into actionable insights for maintainers and operators.

Overall, this research advances our ability to measure, understand, and manage cyber-security risks in Internet-connected systems. Its methods and tools can be used by researchers, regulators, and security practitioners to better assess exposure, improve monitoring practices, and support evidence-based policy and defense strategies in an increasingly connected world.

Please submit the summary to the department PhD coordinator together with your thesis