UN Internet Governance Forum (IGF)

Dynamic Coalition on Internet Standards, Security & Safety - IS3C

Making the Internet more secure and safer

Working Group 1: Security by Design - Internet of Things (IoT)

Embedding security in IoT design

Mission Statement

1. The problem - the challenge - the opportunity

The security and safety of the Internet of Things (IoT) is an ongoing challenge and the global Internet stakeholder community is paying a lot of attention to developing solutions for enhancing the security of IoT devices and applications. However, despite common goals many of the current initiatives and processes for discussing and developing IoT security solutions are fragmented with various platforms and regional and national stakeholder groups working independently[1]. A list of commonly accepted challenges for standardising the security and stability of IoT systems is provided at Appendix A to this statement.

Contributions to these various institutional and regional initiatives for the development of technical solutions are being made by a variety of business, government, academic and technical experts from the standards-making bodies. The UN IGF[2] provides the opportunity to bring together these experts from stakeholder constituencies in all geographical regions.

The IS3C[3] is a stakeholder coalition that uniquely aims to address the gaps in the global deployment of security-related standards. The coalition's work on advancing IoT standards deployment contributes to the IGF's objectives of advancing the digital transformation of economies in support of the UN's sustainable development goals.

The coalition established this sub-group on IoT under its Working Group 1: Security by Design with the specific aim of:

- reviewing current security-related IoT initiatives and practices worldwide;
- developing a coherent package of global recommendations and guidance for embedding security by design in the development of IoT devices and applications. These will be communicated to decision-takers as IGF outcomes.

2. Possible solutions - outlines of potential outcomes

WG1 agreed to undertake research on the following questions:

1) What are the main challenges in order to achieve a unified approach towards IoT security and safety? These could include:
    - gaps in architecture;
    - competing protocols;
    - poor or deficient security specifications;
    - lack of centralised ID management;
    - need for a basic trust model.

2) What do current best initiatives and requirements for IoT security by design take into account when planning, launching and evaluating projects, standards and regulations?

3) What are the practicable avenues for the communication and deployment of IoT security by design best practices?

3. Work plan - timeline and milestones - roll-out

The development of recommendations and guidelines by the coalition for the implementation of IoT security-related standards and best practice relies on attracting experts and specialists from a wide range of stakeholders and industry players. IS3C agreed that it is important to review and study the widest possible experience and take into account variations in the experience of different countries in cybersecurity and online safety.

WG1's Sub-group on IoT meets online at 4-6 weekly intervals with open invitations to any interested stakeholders to attend.

January – May 2022

- Outreach to contact interested stakeholders and engage working group members.
- Meetings with academic experts in the IoT security field.
- Preparation of the research proposal on current security-by-design policy documents based on a worldwide sample of IoT policies and initiatives.
- Research team recruitment and planning meetings.
- Initial desk research of samples of national policies from all geographical regions.

June - October 2022

- Research team compiles a repository of national policies, laws, regulations and related policy documents published by various governmental and regulatory bodies worldwide. These policies include references to general and specific tools/good practices for making the IoT ecosystem more secure.

- Comparative review and analysis of the main policy and regulatory provisions and related best practices, taking into account examples of data security best practices, relevant industry and consumer codes of practice, product safety legal requirements and relevant consumer protection initiatives such as product labelling schemes.

November - December 2022

- Drafting of the research report with policy recommendations, common best practices and guidelines.
- Presentation of the draft research report during the IS3C session at the UN IGF in Addis Ababa.
- IS3C holds open external stakeholder consultations on the report's conclusions and recommendations.

January - February 2023

- WG1's review of the external stakeholders' responses.
- Advice submitted to the IS3C leadership for finalising the research outcomes and best practice recommendations.
- Publication of IS3C's final report of the research project.
- Dissemination of the policy recommendations and best practice guidance in regional and national presentations to policymakers and decision-takers in the technical community, governments and business.

4. Contacts for further information

WG1 Chair: Nicolas Fiumarelli
nicolas.fiumarelli@is3coalition.org nicocamarao@gmail.com

WG1 Vice-Chair: Sam Goundar
sam.goundar@is3coalition.org sam.goundar@gmail.com

IS3C Coordinator: Wout de Natris
wout.denatris@is3coalition.org denatrisconsult@hotmail.nl

IS3C Senior Policy Adviser: Mark Carvell
mark.carvell@is3coalition.org markhbcarvell@gmail.com

To become a member and subscribe to the IS3C mail list (including WG1) please register at: https://mail.intgovforum.org/mailman/listinfo/dc-isss_intgovforum.org

---

Updated: 21 November 2022