Internet Governance Forum (IGF)
Dynamic Coalition on Internet Standards, Security & Safety (DC-ISSS)
Making the Internet more secure and safer

Working Group 1: Security by Design
Sub-Group on 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 standardizing 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 DC-ISSS[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 has established this sub-group on IoT under its Working Group 1: Security by Design with the specific aim of:

i) reviewing current security-related IoT initiatives and practices worldwide;
ii) 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.

---

[1] A sample of IoT policies from around the world has been started by WG1 https://docs.google.com/document/d/1Lwsd_ZDKTtGvexkBZyre6yHicZpeIWVD7YFBzoDeap8/edit

[2] For background on the Internet Governance Forum (IGF) and the intersessional roles of the dynamic coalitions, see: https://www.intgovforum.org/multilingual/index.php?q=filedepot_download/4099/481

[3] More information about the DC-ISSS is available at: https://www.intgovforum.org/multilingual/content/dynamic-coalition-on-internet-standards-security-and-safety-dc-isss

2. *Possible solutions - outlines of potential outcomes*

There are three key research questions which the WG1 Sub-group on IoT will work on:

1. What are the main challenges towards a unified approach towards IoT security and safety? These could include:
a) gaps in architecture;
b) competing protocols;
c) poor or deficient security specifications;
d) lack of centralised ID management;
e) 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 WG1 Sub-group on IoT will meet online with meetings convened at 4-6 weekly intervals with open invitations to any interested stakeholders to attend.

<u>January-June 2021</u>

- Establishment of the WG1 Security by Design - Sub-group on IoT and appointment of its Chair and Vice-chair.
- Sub-group members hold open consultations with stakeholders on its aims, research questions, modalities and proposed outcomes;
- Sub-group members invite experts to participate in its meetings to develop answers to the research questions.

<u>July-September 2021</u>

- The IoT Sub-group reviews the collation of research materials on previous and current relevant national and international initiatives and projects iand starts drafting the outcome documents comprising recommendations and guidelines.

<u>October-November 2021</u>

- Submission of WG1 Subgroup on IoT outcomes to the DC-ISSS membership for review by all coalition members.

- Members of the Sub-group review the responses of the coalition members and finalise the texts for posting on the DC-ISSS website.

December 2021-January 2022

- Presentation of WG1 Subgroup on IoT outcomes at the DC-ISSS session during the UN IGF in Katowice.
- Open external stakeholder consultation held by the DC-ISSS on the finalised Sub-group outcomes.
- Review of the external stakeholders' responses by the Sub-group members and advice submitted to the DC-ISSS leadership on finalisation.
- Publication and dissemination by DC-ISSS of the finalised Sub-group outcomes for roll-out of communication in regional and national presentations to decision-takers worldwide .

4. Participation and outreach

The development and implementation by the coalition of IoT security-related standards and best practice relies on attracting experts and specialists from a wide range of stakeholders and actors. It will be important to review and study the widest possible experience and this will necessarily take into account variations in the experience of different countries in cybersecurity and online safety.

Based on the principles of openness and consensus in achieving the outcomes of its work, in its research the Sub-group on IoT will collate inputs relating initiatives from existing IoT policy initiatives, projects and processes. Contributions will be sought from leading actors in the cybersecurity field worldwide, including national and international cybersecurity agencies, intergovernmental and non-governmental organisations with a direct interest in IoT security, technical standards bodies and IoT and 5G research groups.

The Sub-group on IoT will accordingly consult and involve in its work representatives of the ITU, ICANN, ISOC, national and regional IGFs, regional Internet registries, industry vendors, and other professional bodies, as well as academic experts.

5. Chair, Vice-chair contact details

- Chair: Mr Yuri Kargapolov yvk@uanic.net https://www.linkedin.com/in/yuri-kargapolov-24937b44/
- Vice-chair: Ms Lim, May-Ann, MayAnn@trpc.biz

Date: 22 June 2021

Appendix A:

Common Challenges in Standardizing the Security and Stability of IoT Systems

Standardizing the security and stability of IoT systems includes the following challenges::

1. The security issues for IoT systems are largely problematic today due to the gaps of architecture and the global model. This is referring to the disadvantages of the four-level model "devices-networks-services -applications" (Overall Functional Architecture Model and IoT Reference Model) which is described in various standards.

2. The challenge of the variety of heterogeneous protocols and IDs that are used in IoT solutions and correspond to the ability to simultaneously ensure the safety of the management of thousands of sensors and actuators. This problem concerns the interaction between a large set of IoT objects which today do not have effective protection and security.

3. Related to this is the fragmentation of the best current practices for secure and safety development, and the tension between IoT security and data/consumer protection regulation as exemplified in EU consumer protection proposals for legislation relating to IoT security.

4. Deficiency of specification of the safety and security aspects in models that describe the properties and structure of digital entities. In particular, the task of how these properties can be used comprehensively in the interaction of digital objects in the operation of IoT systems. For example, the management and maintaining the operation of thousands devices and the security and safety features relating to single sign-on actions.

5. The problems associated with a third party role within the current IoT architecture (e.g. provider identity) which needs to retain information about the critical elements of access to digital objects between the consumer and the data source in the IoT systems. A standard that separates and describes the management properties of identifiers and identification processes may help to resolve these issues.

6. The desirability of establishing basic trust in the operation of IoT processes.