Internet Service Providers' and Individuals' Attitudes, Barriers, and Incentives to Secure IoT

Nissy Sombatruang[1] Tristan Caulfield[2] Ingolf Becker[2] Akira Fujita[1]
Takahiro Kasama[1] Koji Nakao[1] Daisuke Inoue[1]

USENIX 2023

[1]National Institute of Information and Communications Technology
[2]University College London

The Authors

NICT CYBERSECURITY Laboratory

UCL

Introduction and Background

Overview

The adoption of *Internet of Things* devices is growing rapidly

- IoT provides many benefits to consumers and businesses

However...

- Unsecured IoT devices pose risks to individuals and networks
- Securing IoT is challenging
- Many stakeholders have a role to play in securing IoT: manufacturers, government, ISPs, businesses, researchers, and individuals
- Many of these stakeholders lack expertise, knowledge, resource, or incentive

This work focuses on two stakeholders, **ISPs** and **individuals** — in **Japan**

We look at **attitudes**, **barriers**, and **incentives** of these stakeholders

The role of ISPs

ISPs can and do make a difference, especially in identifying, notifying, and quarantining the infected customer[1]

- Walled gardens (where allowed) can be used to quarantine and notify customers, but highly disruptive

ISPs can also have a role *before* compromise:

- ISPs can scan for vulnerable IoT devices and isolate them from the Internet before they are compromised[2]
- Government agencies can scan for vulnerable or infected IoT devices and ask the ISPs to notify the owner of these devices to take actions to remediate

[1] Asghari, Eeten, and Bauer, "Economics of fighting botnets: Lessons from a decade of mitigation".
[2] Dietz et al., "IoT-botnet detection and isolation by access routers".

Context: The NOTICE Project

NOTICE: National Operation Towards IoT Clean Environment

- An ongoing nationwide project to identify and remediate vulnerable and infected IoT devices in Japan
- The National Institute of Information and Communications Technology (NICT) identifies vulnerable or compromised IoT devices
- Participating ISPs are informed and assume the responsibility of identifying and notifying their customers who own the devices

The study

Research questions

We look at two key stakeholders in the IoT ecosystem: **ISPs** and **individuals**.

Three research questions:

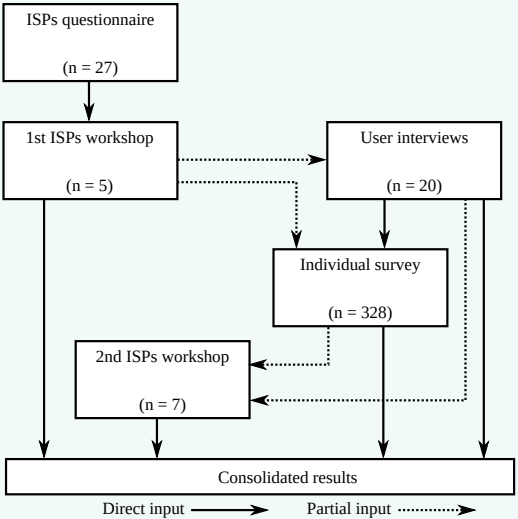
Q1 *What are ISPs' and individuals' attitudes towards the security and privacy of IoT?*

(Attitudes: concerns, perceptions, commitment, views of other stakeholders)

Q2 *What are the barriers that prevent ISPs and individuals to keep IoT secure?*

Q3 *What are the incentives to encourage ISPs and individuals to keep IoT secure?*

Methodology: Interviews, Surveys, and Workshops



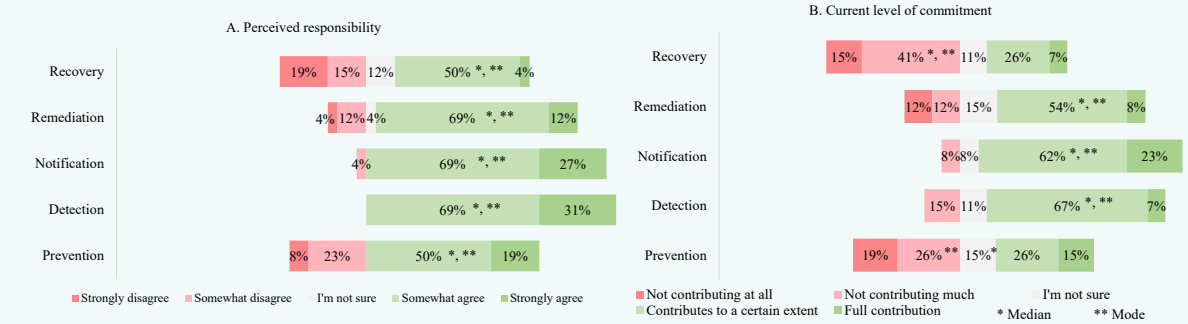
Iterative participatory action research

- ISP Questionnaire
- 1st ISP Workshop
- Individuals interviews
- Individuals survey
- 2nd ISP Workshop

Results

ISPs attitudes

- Perceived responsibility and current level of commitment:



- ISPs believe they are well-placed to do notification and detection
- Most concerned about service disruptions and service continuity, prevention or recovery is secondary

ISP views on Improving IoT Security

- Internal barriers
  - Staffing, particularly at smaller ISPs
  - Executive buy-in, particularly at large ISPs
- External barriers
  - Individuals are careless & unable to secure devices
  - IoT Device makers build insecure devices
- Notification barriers
  - Tech: dynamic IP addresses
  - Social: not up-to-date contact details; account holder is not device owner
- Solutions
  - Better tech to detect and remediate
  - Device makers secure IoT
  - Regulatory changes to allow ISPs to restrict more traffic
  - Better awareness: get notified users to actually fix their devices

Individual Views to improve IoT Security

- Mostly not concerned about IoT security
- Uncertain about the likelihood and impact of compromise
- Very average security behaviours
- Remediating compromised IoT
  - Don't know what to do/where to start (74%)
  - Easier to replace (28%), fixing is not worth the time/stress (28%)
  - 26% had tried to fix things; of these, only 21% had no problems doing so
- How to improve the situation
  - Experience negative consequence of IoT attacks themselves or hear about them from friends
  - No other party is particularly seen as particularly responsible
- Views on ISP initiatives
  - 55% support notification; 54% notify & block suspicious traffic
  - 58–73% of participants are willing to pay for additional services to secure the home IoT

Macro socio-technical challenges

- Keeping IoT secure is not a priority for ISPs and individuals
- Many stakeholders that need to work together: NOTICE project encouraged collaboration
- An effective government is at the heart of solutions
  - Many of the barriers and incentives are external to ISPs and individuals
  - Encourage collaboration
  - Change the law to allow ISPs to lawfully monitor and block suspicious IoT traffic
  - Provide subsidy/rewards/recognition to ISPs
  - Increase the visibility of regulation around IoT
- Empower those that can make a difference

Thanks!

Internet Service Providers' and Individuals' Attitudes, Barriers, and Incentives to Secure IoT

Nissy Sombatruang[1] Tristan Caulfield[2] Ingolf Becker[2] Akira Fujita[1]
Takahiro Kasama[1] Koji Nakao[1] Daisuke Inoue[1]

USENIX 2023

[1]National Institute of Information and Communications Technology
[2]University College London