Acknowledgements

We want to recognize the following groups and organizations for their input and participation in this working group. We appreciate everyone’s support, contribution, and encouragement over the last year.

Consumer Technology Association, Device Authority, Ice Miller LLP, National Telecommunications and Information Administration, The Niskanen Center, Online Trust Alliance, OutSecure Inc., SAP, The Providence Group, Trusource Labs, Venable LLP.

Introduction

The Internet of Things (IoT) provides a wide array of opportunities to integrate and interconnect technology in our daily lives. As part of a growing global infrastructure, IoT presents many security challenges, some understood but many that are new. Devices integrated with the physical environment is a considerable area of concern given the serious impact they may have on life and property. Addressing these challenges and concerns requires a multi-stakeholder process, involving industry, consumers, and governments to align and collaborate.

This document will inform stakeholders of an approach to identifying and analyzing incentives and barriers associated with IoT security upgradability and patching. Stakeholders are defined broadly in order to ensure that all viewpoints are accounted for to the extent possible. In particular, this paper will appeal to stakeholders who are keen to characterize the upgradeability and patching capabilities of IoT systematically, or to stakeholders who want to gain deeper insight to augmenting incentives or diminishing barriers to improve IoT security upgradability and patching.

Market adoption of IoT has been aggressive and is expected to continue. While IoT scenarios with national defense or life-and-death criticality are now receiving attention from governments and standards organizations, the security implications associated with consumer-based IoT scenarios remain the subject of ongoing debate. One critical area of concern is how to keep up with device security through patching and upgrades. The National Telecommunications and Information Administration (NTIA) within the Department of Commerce has brought together stakeholders to engage and discuss the potential of appropriate patching and upgrades to keep IoT devices secure. NTIA recognizes the industry today lacks sufficient consensus on ‘a set of common, shared terms or definitions…to standardize descriptions of security upgradability or a set of tools to better communicate security upgradability.’[1]

To extend the stakeholder engagement process, several working groups have been established as part of the initiative. This paper represents the Incentives and Barriers working group, where the core topic to contemplate is *how do we foster greater adoption of appropriate patching and updating practices?* Different forces will lead to stakeholders either embracing or resisting IoT device patching capability.

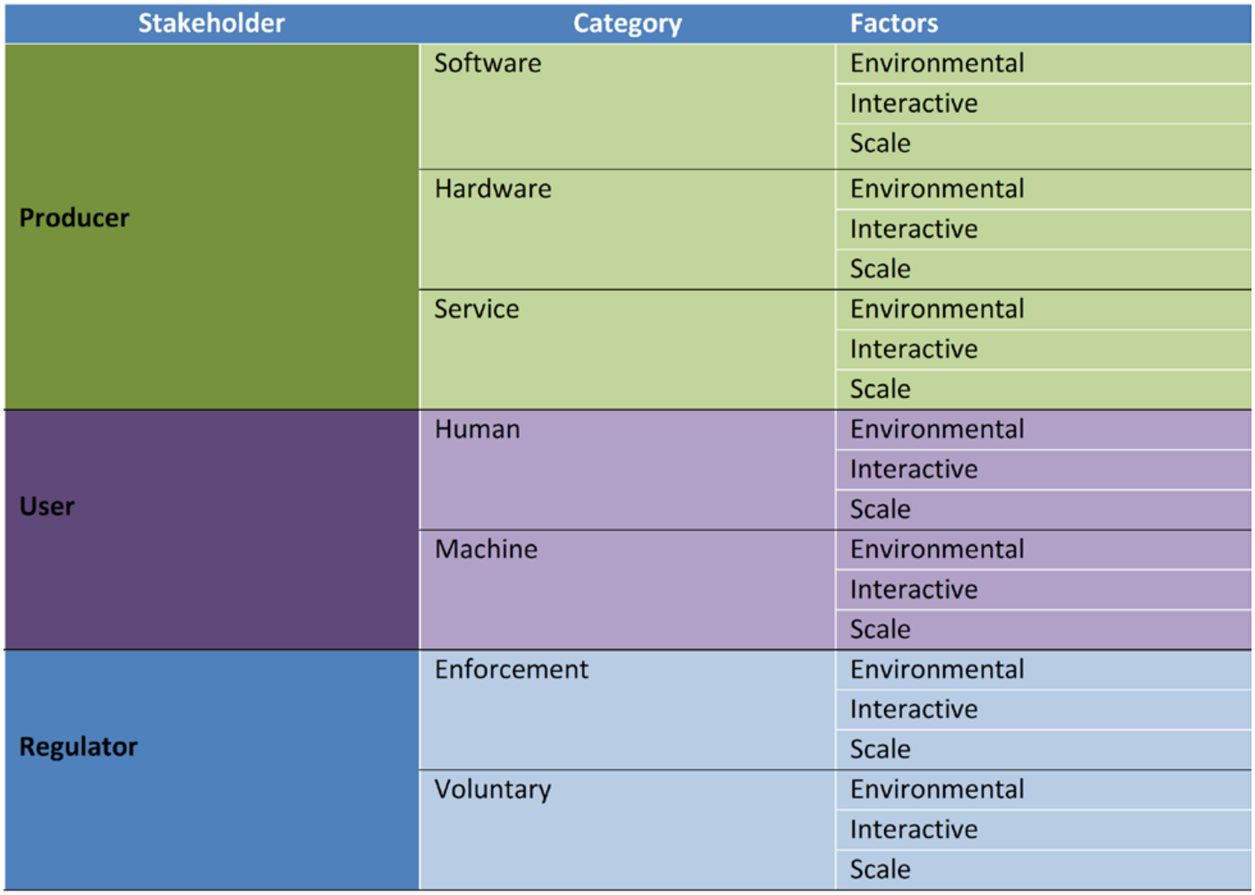
This purpose of this paper is to initiate a dialog among IoT producers, government and industry policy makers, researchers, and civil society advocates while avoiding prescriptive recommendations or best-practice guidance. Instead, this paper proposes an approach to analyze security concepts in IoT scenarios. Multiple stakeholders are involved in IoT use-cases, often beyond the conventional sense of technology actors. It is important to realize the existence of these actors as stakeholders plays a vital role in the success of IoT.

[1] https://www.ntia.doc.gov/blog/2016/increasing-potential-iot-through-security-and-transparency

Stakeholder Taxonomy

By its very nature, IoT is cross-societal, which means that any progress towards making it more secure and reliable relies on multiple stakeholder interaction. While considerable work is being done to develop and implement technical solutions and discuss regulatory mechanisms to tackling the security challenges posed by IoT, much of it is presented with little discussion as to who the stakeholders are, nor their needs and wants.

Here we have summarized the stakeholders and their respective characterization in a taxonomy. Our intention in developing this taxonomy was to be both broad and concise. Being broad allows us to consider a wide range of stakeholders in the IoT ecosystem, and being concise permits us to focus on each stakeholder with sufficient detail to be meaningful and actionable.



Stakeholder	Category	Factors
Producer	Software	Environmental
		Interactive
		Scale
	Hardware	Environmental
		Interactive
		Scale
	Service	Environmental
		Interactive
		Scale
User	Human	Environmental
		Interactive
		Scale
	Machine	Environmental
		Interactive
		Scale
Regulator	Enforcement	Environmental
		Interactive
		Scale
	Voluntary	Environmental
		Interactive
		Scale

This taxonomy assumes that knowledge of the barriers and incentives in IoT upgradability and patching will inform stakeholders on the trade-offs involved in negotiating effective solutions. There are three levels of granularity identified: stakeholder, category, and factors.

First, there are three main stakeholder groups:

- **Producer:** Designs and/or manufactures hardware or software components of IoT products in whole or in part, or a provider whose service(s) is essential to expected product function.
- **User:** An individual, organization or machine that implements and/or interacts with one or more IoT products in any given context.
- **Regulator:** Any entity granted the authority to require or recommend, via enforcement or voluntary adoption, one or more standards pertaining to the expected features and functionality of an IoT product, either specifically or categorically.

Second, each stakeholder group consists of multiple categories:

- **Producer [Software]**
- **Producer [Hardware]**
- **Producer [Service]**
- **User [Human]**
- **User [Machine]**
- **Regulator [Enforcement]**
- **Regulator [Voluntary]**

Finally, all categories are informed by the same three factors:

- **Environmental:** Protocols, restrictions, and/or conditions imposed by peripheral considerations the IoT product is operating in.
- **Interactive:** Stakeholder interaction of varying complexity and frequency, and can be intentional or unintentional.
- **Scale:** Can incorporate both breadth and depth. Breadth concerns the broad range of product(s) to remain in support and patchable. Depth concerns how legacy technology can remain in support and patchable while capable of still performing as expected.

Use Cases

The use cases in this section are meant to be illustrative of how the taxonomy defined above might be applied in specific contexts. It is worth noting that whether a point of discussion is an incentive or barrier is often contextual.

For example, giving users the ability to customize the software of a smart device could be a barrier for the producer (loss of control, increase support calls) but an incentive for consumers (increase in control, special features). Going a step further, the fact that the user sees the customization capability as an incentive to buy the smart product, may be enough of an incentive to the producer to outweigh the barriers.

This contextual dependency and interplay can get complex. The intent of these use cases is to demonstrate how the taxonomy can assist with identifying discrete points for consideration while recognizing that the final business decision involves the interplay across multiple stakeholders, categories, and factors.

The authors encourage others to build additional use cases and refine the approach.

Use Case 1

Context: Commercial dishwasher for use in small to medium sized restaurants. Bug in dishwasher software could allow someone to bypass authentication and take control of the dishwasher, causing water overflow, extended heating cycles, or complete non-function, resulting in potential physical and business harm.

Producer [Hardware]: Industrial dishwasher manufacturer

- Capabilities: Sensors and control servos, including water flow and heating elements.

Producer [Software]: Smart Dishwasher software developer

- Capabilities: Command and control; telemetry; mobile app

Producer [Service]: Internet service provider

- Capabilities: Internet connectivity to support **Producer [Software]** capabilities

User [Human]: Owner of restaurant

- Capabilities: Push the buttons; operate the mobile app

<u>Producer [Software]</u>
In deciding whether to make the dishwasher software upgradable/patchable, the software producer has several factors to consider, as below:

Factor	Barrier	Incentive
Environmental	• Tracking device ownership is difficult • Internet connectivity isn't assured or reliable	• Improve Operation/New Features • Bug fixes • Integration with smart home
Interactive	• Consumer "jail-break" and/or factory reset • Consumer perception of control and privacy	• Improve user experience
Scale	• Support of legacy versions	

<u>User [Human]</u>
Here, the human user is the owner of the restaurant, who is going to be using the dishwasher daily. The factors are used to represent influences to the decision-making process. Note that in

this case, the Interactive category keys on the same idea that the dishwasher can be updated/patched. How the user views this depends on their attitude, comfort level with the technology, and plans for future use. This is predicated on the notion that most updateable/patchable devices can also receive custom code from users, not just the producer. Therefore, an enterprising restaurant owner may want to load custom software onto their dishwasher for some reason. On the other hand, stories of bad updates “bricking” other dishwashers may chase them away.

Factor	Barrier	Incentive
Environmental	● Possibly more expensive than “dumb” dishwasher	● “Cool” factor ● Integration with other smart devices
Interactive	● Perceived loss of control ● “Hackable”	● Perceived increase in control ● “Hackable”
Scale	● NA	● Automated management across multiple dishwashers

For each factor, the barriers and incentives are weighed against each other to inform the final decision regarding whether the inclusion of upgrade/patch capability is a good business decision, as discussed in the next section.

Regulator [Enforcement]

One potential regulator in this use case might be the Consumer Product Safety Commission (CPSC) who is charged with “…protecting the public from unreasonable risks or injury or death associated with the use of the thousands of types of consumer products under the agency’s jurisdiction.”[2]

Given that the dishwasher may be compromised to cause physical harm in the form of fire and water damage, the CPSC may choose to weigh in on potential vulnerabilities. Unlike the Producer and User stakeholders, in this example, the CPSC is focused narrowly on the relative safety of the device, rather than attempting to influence specific features or long term viability of the device.

[2] https://www.cpsc.gov/About-CPSC

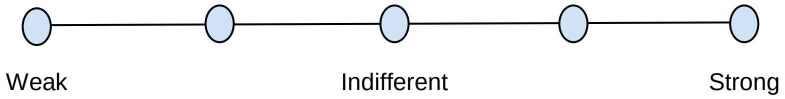
Factor	Barrier	Incentive
Environmental	● Desire to not harm innovation	● Ensure that dishwasher operates within established safety parameters
Interactive	● Desire to not harm innovation or dictate features	● Can user inadvertently cause harm through use of the dishwasher?
Scale	● NA	● NA

The above is purely an example. The authors do not represent the CPSC or claim to understand how they may or may not choose to engage.

Incentive-Barrier analysis within and across stakeholders

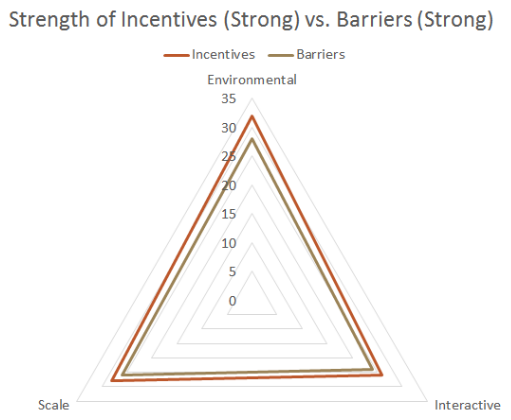
A good use case will articulate the corresponding incentives and barriers to upgradability and patching of IoT devices. Yet, a use-case alone does not provide any mechanism to analyze incentives and barriers. To do so, it is critical to contemplate how incentives can overcome barriers to create a win-win situation for improvements in upgradability and patching.

An initial step is to *quantify* qualitative data depicted in the use-cases. For instance, to borrow from psychometrics measurements, a Likert scale can help us to scale different incentives and barriers along a defined spectrum.



For every incentive and barrier identified, it is possible to associate a relative strength. For instance, a weak incentive can be associated with a score of (0), whereas a strong incentive can be associated with a maximum score of (35).

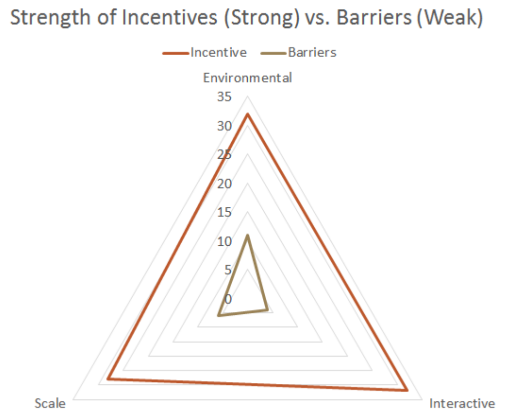
With quantification, it is possible to analyze incentives and barriers within and across stakeholders. The intention is to mix-and-match and identify opportunities to compromise or collaborate, such that incentives can be leveraged to address barriers. Four sample scenarios below will illustrate the different possibilities.



Scenario 1: Strong Incentives and barriers within a single stakeholder

In this scenario, a stakeholder is believed to have strong incentives and strong barriers among all factors. For example, a **[Producer | Software]** finds providing new features to users is important *[interactive | incentive]* (value = 26), and is expected to support the device for several years *[scale | incentive]* (value = 29). On the other hand, the same **[Producer | Software]** finds new features and patches introduce new vulnerabilities *[environmental | barrier]* (value = 27). Additional strong *[environmental | incentive]*, *[interactive | barrier]*, and *[scale | barrier]* are available which lead to the pattern on the left.

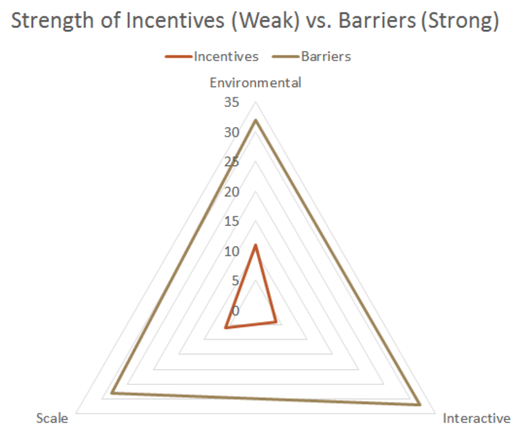
This is a rare scenario where strong incentives in *all* factors are matched with strong barriers in *all* factors. The stakeholder **[Producer | Software]** may be open to changes, yet on their own, may not be motivated to change the status quo.



Scenario 2: Strong Incentives with weak barriers within a single stakeholder

In this scenario, a stakeholder has strong incentives against weak barriers in all factors. For example, a **[Producer | Hardware]** finds providing new features to users is important *[interactive | incentive]* (value = 32), and is expected to support the device for several years *[scale | incentive]* (value = 29). Yet, the same **[Producer | Hardware]** finds new features and patches are not likely to introduce new vulnerabilities *[environmental | barrier]* (value = 10). Additional strong *[environmental | incentive]*, weak *[interactive | barrier]*, and weak *[scale | barrier]* are available which lead to the pattern on the left.

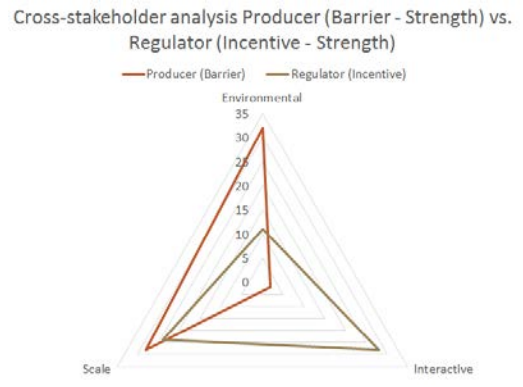
Thus, the stakeholder **[Producer | Hardware]** is likely to leverage new features and patches to improve security practice, or is very willing to do so upon request.



Scenario 3: Weak Incentives with strong barriers within a stakeholder

In this scenario, the opposite has happened. A stakeholder faces strong barriers against weak incentives in all factors. For example, a **[Regulator | Voluntary]** may face a strong *[environmental | barrier]* where its lack of enforcement power renders the regulator without formal authority to influence (value = 32). Meanwhile, the **[Regulator | Voluntary]** may face little incentive in *[interactive | incentive]* as stakeholders may not appraise its effort as a regulating advocate (value = 5). Additional strong *[interactive | barrier]*, *[scale | barrier]*, with weak *[environmental | incentive]*, and *[scale | incentive]* are available which lead to the pattern on the left.

Without other stakeholder collaboration, the **[Regulator | Voluntary]** will face difficulties to institute changes.



Scenario 4: Cross-stakeholder analysis - Producer (Barrier) and Regulator (Incentive)

The three scenarios above are rare and for illustrative purpose only. They show the extremes where stakeholders have very similar strengths in barrier and incentive among all factors.

Yet, stakeholders' barriers and incentives are dynamic. A realistic scenario will look like the left, where incentives and barriers are overlapping in varying degree among the three factors. It compares barriers for a **[Producer | Service]** with incentives for a **[Regulator | Enforcement]**.

To analyze the situation, **[Producer | Service]** has a weak *[interactive | barrier]* (value = 3) whereas **[Regulator | Enforcement]** has a strong *[interactive | incentive]* (value = 28). When we analyze these two stakeholders to identify opportunities to collaborate, the scenario will be analogous to scenario 2 above. They can be expected to achieve an 'easy win' to institute change on the interactive front.

Meanwhile, **[Producer | Service]** has a strong

	[environmental | *barrier]* (value = 32) while **[Regulator | Enforcement]** has a weak *[environmental* | *incentive]* (value = 6). This observation is analogous to scenario 3 above. The verdict here is to look for alternative stakeholders where their environmental incentive and barrier are compatible to institute change. Finally, **[Producer | Service]** has a strong *[scale* | *barrier]* (value = 29) whereas **[Regulator | Enforcement]** also has a strong *[scale* | *incentive]* (value = 20). This case is similar to scenario 1. The incentive of one stakeholder could be a good complement to the barrier of another stakeholder. It is worth exploring where collaboration opportunities could exist to overcome some of the *[scale* | *barrier]* faced by **[Producer | Service]**.

Applications, Discussions and Future Directions

In IoT security upgradability and patching, respective barriers and incentives faced by stakeholders will determine whether effort to improve IoT security would succeed or not. As an ongoing dialog, we welcome opinions and suggestions to revise the stakeholder taxonomy. Are there any stakeholder group missing? Will the current taxonomy be sufficient to include most stakeholders, either living beings, or machines?

Secondly, the use of psychometrics measurements may draw criticism when the perceived strength of incentives and barriers are subjective, or fail to capture the associated qualitative meaning in full. The meaning and characteristics of barriers and incentives are also relative and subjective. The use of psychometrics is appropriate where, at a minimum, the quantification of perceived barriers and incentives will facilitate deeper discussion with stakeholders; new possibilities may yield to overcome barriers, either within-self or across stakeholder groups.

IoT security upgradability and patching will remain a critical topic in the foreseeable future. The changes that stakeholders manage to institute will determine how prevalent the issue is to different IoT scenarios. Changes could lead to a variety of possible outcomes - policies, regulations, laws, technical implementations, architectural standardization, and more. Based on the work proposed above, further work and exploration should investigate how stakeholders across different disciplines could leverage incentives to influence and overcome barriers with one another.