Report - 6th Annual Workshop

IGF Dynamic Coalition on the Internet of Things

IoT Global Good Practice
www.iot-dynamic-coalition.org

The 6th workshop of the IGF Dynamic Coalition of the Internet of things was held in Dresden Germany July 14-15 2017. The meeting was by invitation; a list of attendees is provided in an appendix to this report. This meeting was the sixth in a series of meeting designed to bring together experts, specialist and others to discuss issues related to aspects of global good practice in the Internet of Things.

The session was divided into 4 themes:

Session 1 Digital Identifiers

The discussion goes back to the beginning of discussions. From the first meetings to this one, one of the issues revolves around the argument over which identifiers should be used in IoT and under whose governance they will fall. The perennial question whether the normal internet identifiers of IP addressing and DNS names are sufficient or whether some newer like Digital Object Identifiers, also known as Handles with the Digital Object Architecture (DOA), should be used.

The group heard an update on the work being done in the ITU-T to support the handle architecture. It was mentioned that the ITU in principle does not endorse a specific technology. It was mentioned that identifiers were needed at every layer of the IoT architecture. The ITU-T related standardization activities in IoT identification, in principle focuses developing architectures and systems with a minimum set of requirements. These include, for instance, the identifiers' uniqueness, immutability, persistence, and resistance to typical forms of attacks like forgery, cloning, and tampering. It was also noted that the IoT identification landscape currently lacks coherence and interoperability. It was made clear that the work being done on IoT and Handles is not a standard that is enforced, but rather one that depends on the member states adoption, any standard developed by any technical Standards Development Organization (SDO) is not mandatory in nature, and the ITU-T is no exception. It is up to the sole discretion of the administrations and interested parties to adopt the developed standards and implement them. In ITU-T, standards are termed Recommendations. This is sometimes confused with outcomes of ITU-R processes, where the work often has the force of treaty.

Study group 20 of the ITU-T has consolidated IoT work and it's applications including smart cities and communities. Surprise was expressed by some at the meeting that DOA had become a hot issue. It was questioned as to whether the issue was technical or political. On the technical side, some of the issue mentioned included that the protocol had not yet been proven on a large scale scalable system, though it had been shown to work well for some specified content areas. It was stated that the ITU-T does not see DOA as a replacement for DNS, but as a solution for some other areas where there have been some problems identified with existing technology, examples offered included the persistence of the identifiers, the problem of broken links, and the difficulties of adding state information (like location info, security keys, &c.) in the resolution system. These aspects were said to be aspects which are seamlessly included in Digital Object Architecture (DoA) as currently being studied and standardized in the ITU.. The suggestion was made was that it was a possible solution for some class of problems and that it should be studied and not feared.

Any study relies on first identifying the problems and and requirements for their solutions.

This requires first coming to agreements on the definition of IoT. Part of this issue relies on first coming to agreement on whether the Iot is an overlay on existing infrastructure, as most applications, or a different sort of problem altogether. One argument is that the Internet is about people and human communication whereas the IoT is about machine to machine communication, but for others, IoT also includes interaction between “Things” and people. The point raised in the discussion that the reputed founder of the IoT had a different vision than the Internet. There was no agreement about the extent to which IoT devices needed

internet connectivity. The argument that "IoT is about machine to machine" is seen by some as a reason why the IoT needs a different type of identifier. One issue was presented on IPv6 challenges with regards to IoT deployments related to the size of most IoT datalink frames and the size of IPv6 headers. However, the discussion was multi-faceted and it was agreed that more discussions and studies were needed to identify and solve practical challenges related to IoT deployments. RFC6282 (6LoWPAN) and RFC7400 defined Generic Header Compression (GHC) were mentioned in response.. And little time was spent on further defining IoT beyond "connected objects". The discussion was multi-faceted and it was agreed that more discussions and studies were needed to identify and solve practical challenges related to IoT deployments.

Two basic viewpoints were made. One considers that IoT is indeed an application on top of the Internet that uses a different set of programing techniques and data management algorithms. The other, considers it totally a different thing, with some common elements perhaps. It was argued that since IoT contains so many complementing and different aspects (like AI, Big Data, analytics, etc.) this indicates that it is not an application running on top and that it indeed entails a different architecture, and this new architecture may require a different set of identifiers at different levels of abstraction.

One of the distinctions made was that new identifiers are defined all the time and have many local uses. The IP architecture is able to work with these in the URI/URN extension as long as they are are established according to the rules for URI/URN. Part of the discussion revolved around understanding identifiers and the overloading of IP addresses as both identifiers and addresses.

While the ITU-T forswears the DOA as a replacement for DNS, another question is the need of the IoT to serve connections between people and machines as well as between machines. The Internet provides more than just point to point communication but allows a richer set of innovation and communication. Even when there are different identifiers in use locally in IoT environments, it may be necessary to gate to the Internet itself in order to be able to use the information from the IoT and to control it from remote locations and to avoid becoming an isolated island.

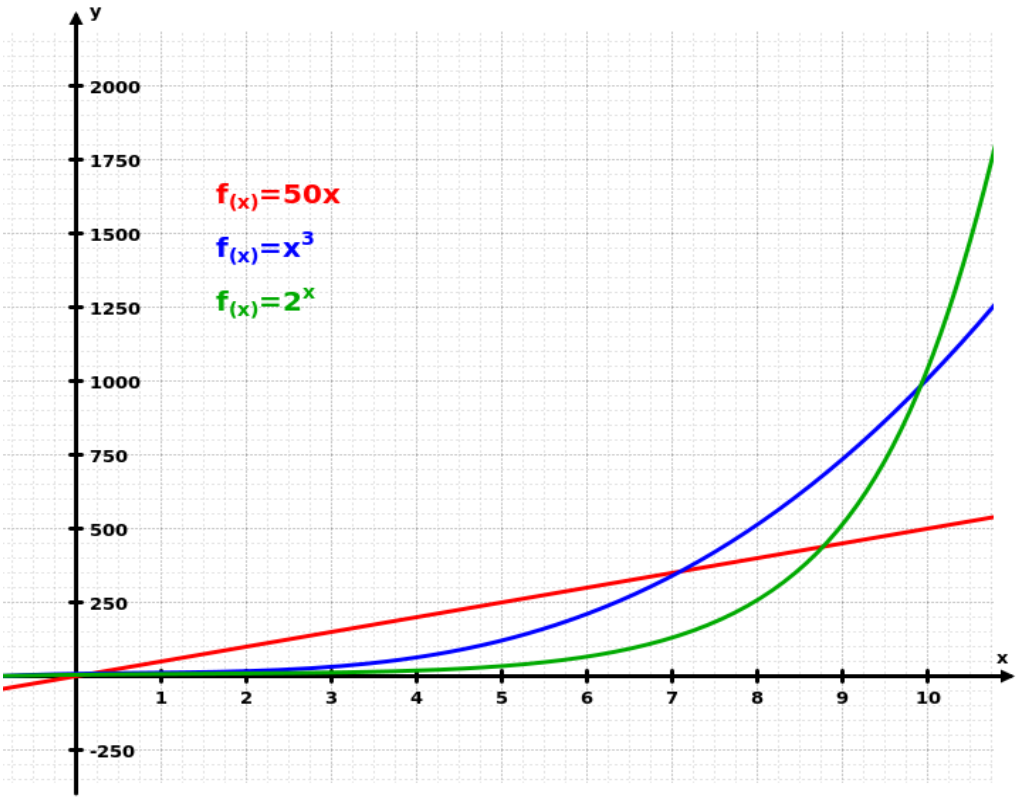
The discussion accepted that the IoT as a technological ecosystem needs effort to consolidate and rather integrate with existing legacy systems and infrastructures. In moving forward we need to strengthen collaboration, multi stakeholders engagement and analyze the true impediments of realizing a consolidated and an interoperable ecosystem. In the end identifiers may be a smaller part of the conversation although they do seem to occupy a large political mindshare. Some of the more important issues may stem from the eventual pervasive use of artificial expertise and artificial intelligence as well as the collection, manipulation and storage of massive quantities of data. Policy issue regarding the accountability for the action of artificially intelligence systems is one of the large ethical decisions that still needs to be understood.

There was also a recognition that requirements are often application specific with the IoT not being a single ecosystem. Different requirements often require different ways to solve the problems.

Last, but not least, it was not fully clear how the governance of DOA was organised. There were questions raised during the meeting on the relationship of DONA with the ITU

Session II Setting standards for minimum security requirements and how to deal with "old" connected objects (that may be not secure)

A blog was written introducing the topic: http://thingsonip.blogspot.cz/2017/07/what-is-in-value-of-security-for-things.html . The discussion started with an explanation based on the blog.



Three laws were proposed that are derivatives of Metcaff's Law:

> **Law I (Eflactem's Law):** *The cost of attacks from a group of nodes grows proportional to the number of vulnerable nodes in that group times the nodes in the entire Internet.*
>
> ***Law II:*** *The potential value of a network of application nodes grows proportional to the square of nodes having an ability to participate in the application.*
>
> ***Law III:*** *The value of a network of application nodes grows proportional to the square of nodes having an ability to participate in the application, minus the cost of attacks number of vulnerable nodes in that network times the nodes in the entire Internet.*

The laws describe the relation between the value of things and the value of applications in relation to the cost of attacks on the Internet.

In IoT the value of access to things can be higher for an attacker than to those who deploy and legitimately use the things. This is because compromised nodes can be used to build many different kinds of attacks

against other parties in the Internet. When things are less likely to be compromised, it decreases the opportunity for attack. Thus the issue becomes how to convince the manufacturers who make things to make them secure.

One of the hoped for future trends is that there be a security assessment of all things that may be attached to the Internet, where people look at the utility of the whole system not just the cost to the manufacturer or those costs passed on to the user.

The issue also has an aspect of consumer choice: how does one measure against the social utility model? Who establishes security and determines the security model that consumers and others should be required to use. This is related to the question of what motivates users to turn on security even though it often involves, effort, cost and even efficiency of their equipment. These issue merge into the question of whether people can be motivated to buy security since by and large people will pick the lowest cost and effort that will achieve their ends, and security tends to drive the cost of equipment up and tends to require additional effort. It was indicated that battery life (limitation) can be affected by additional security measures, this shortening the lifetime of the battery thus the functioning of the "Thing" another reason to opt out of additional security measures, other than those that have become a precondition for use.

One model that may help is the 'collaborative security' model where the burden for security does not fall on individual actors but partially on each actor in chain. Norms are developing but whether people and companies can be 'nudged' into accepting them remain a question. One hope is that examples of good behavior (setting standards of good practice) and a bit of positive propaganda can help create a societal awareness and inclination toward security related behaviors. And it will be important to assume responsibility to be there where it can be taken - recognising that end users can be expected to take some action as well, they cannot be expected to be security experts and take responsibility for complex actions in order to secure the systems they use.

Regulation was also discussed, but in general it was accepted that regulation can only work if its is accepted as necessary. When regulation is not generally accepted and in support of common norms, it is only applicable to those who accept it, others will find a way to work around the regulatory framework. Self-regulation is important in this, yet is not always observed by all involved parties. In some larger project, top down effort can work. This was said to be the case in centrally planned smart cities. But it was generally accepted that regulation only works when the consumer desire it.

This led to a discussion of the use of incentives in cases where the consumer desires and the security drive were misaligned. There was also discussion of the side effects of regulatory behavior and the need to mitigation in addition to prevention in the security field. Everything will never be completely safe on the Internet, so there is always a need to also understand how to minimize the cost of successful attacks and facilitate recovery: a risk management approach.

There was a consideration that since economics does not explain altruistic behavior, the combination of the analysis done by Arkko in his blog and the collaborative model might be of use.

Session III Dealing with exploit of vulnerabilities and cyber warfare

This session focused on infrastructure. Two differences between the Internet and other conflict areas is that the Internet is largely privately owned and borderless.

Unfortunately, it has too many single points of failure and vulnerability, and the battle has moved from the traditional forms of warfare to private armies, mercenaries, capable of utilizing the vulnerabilities. The line between criminal behavior and war has faded. With lines having blurred it was asked, must there be state involvement for it to be war?

Attribution was discussed as necessary, but was also described as very difficult to impossible, in particular when it concerns state players. Naming and shaming is useful with states if attribution could be sufficiently proven. As for industry, this has become clearer with legislation emerging about the obligation to publish breaches that compromises personal data. With new legislation (e.g. GDPR in Europe) and a higher appreciation of "value" of personal data around the world, the costs for not defending against breaches go up which leads to more commitment in companies for protecting data.

In discussion it was considered that it was important to distinguish between industry and consumer. The Internet has become a critical infrastructure that intertwines with (or becomes an intrinsic part of) other critical infrastructures such as energy, water, transport, public services, thus vulnerabilities in the core Internet affect all critical infrastructures and can be used to attack the network.

Attacking the protocol infrastructure is considered 'impossible' as the shared fate property would affect the attacker as well as the attacked. And yet, impossible attacks happen all the time.

The threat model in cyber war scenarios is not necessarily one of nation against nation so much as it is feudal, with independent groups of attackers picking political targets of convenience. The security vulnerability of nearly all device in the IoT make them prime. The fact that IoT devices are largely programed on the same few systems, makes them even more susceptible. While attacks have been going on and continue to go on, when they become life threatening they are addressed, otherwise they are often treated as so much noise, paranoia, or the growing pains of a new technology.

The uncertainty makes determining whether a cyberattack can be seen as aggression under section 2, which activate article 5,1 reason for asymmetric response. Especially in the case where innocent IoT devices become part of bot armies for rent at reasonable process, it is impossible to determine whether an attack is merely criminal or an act of aggression equivalent to an act of war or terrorism.

The situation is one where attribution cannot be determined with any degree of certainty, if at all. In such an environment establishing international treaties and covenants becomes more difficult if not impossible. The discussion explored the notion of norm setting in the absence of enforceable international law.

The problem with norms is that everyone has a different set of them. One group setting norms is not necessarily accepted by another. The question becomes whether it is possible to establish norms using a

variant of the multistakeholder model. This is also a challenge as currently processes are largely multilateral, processes laden with politics and incapable of adapting quickly to changing circumstance.

Whether norms or international law, however, guidelines and rules need to be technology neutral, both in order to stand the test of time but also to avoid creating market winners and losers.

Security, however, is no longer an option in the IoT. Devices are everywhere, the proliferation of IoT throughout industry and into innumerable consumers home is a collective risk that must be addressed by all. Even when it is possible to manage IoT devices in a secure way, many users do not activate the security features. Should users be educated? Are they responsible for the security of their devices? What can be reasonably expected from them?

The discussion ended on the question of what could be done to make progress? Many conferences, commissions and studies have already occurred, and yet there is no apparent progress. What are the necessary conditions for security and how can these be created? Are there alternatives to the current efforts?

Session IV Liabilities in case of security or privacy breaches – Who is responsible, who carries the costs?

Liability and responsibility in the case of security is unclear and varies by sector and jurisdiction, each country and business operating in its own silo. The group discussed the possibility of breaking out of the siloes and developing a wider shared sense of responsibility and liability. In the US the FTC has taken a common law approach to cyber security cases. Massive breaches are beginning to change that approach since appeals courts in the U S are beginning to weigh in.

The NIST cybersecurity agreement, which provides guidance for private sector actors, was discussed and described as a good roadmap that, while voluntary, has been well adopted.

The relationship between privacy and security was discussed and were described as not opposite sides of the coin as they are customarily described. It was stated that one can't have privacy without security, nor security without privacy. There was general agreement that the US was behind Europe in terms of privacy though the GDPR might change the discussion even in the US. One problem with comparing the situation in the US and Europe concerned the fact that in the EU privacy is a fundamental human right that cannot be traded away, while in the US it can be traded away voluntarily with informed consent.

Three categories of risk with corresponding mediation were discussed

- preventable risk which is susceptible to rule based compliance
- strategy risk which affects business decisions and requires actively management
- external risk which requires outside control

The issue of insurability was discussed, with the question of whether the need for insurance leads to the creation of norms. One issue that makes this discussion difficult is that there is no actuarial data for insurance calculations. One reason for this is that breaches aren't disclosed, if at all possible, especially by companies that do not want the press. Iin order to improve, security breaches need responsible disclosure. The issue of attribution, discussed earlier in the meeting was also a significant factor. Another question raised is whether insurance stimulates a compliance attitude rather than improving security culture within an organization.

One question that was left pending was whether programmers should be liable for being hacked.

A final point was made about the importance of empowering data protection commissioners so that they could handle complaints of data being leaked.

Conclusions

The meeting ended with a general view that many questions had been explored but that there was a long way to go before having answers, for some definition of answer.

Overall, it is clear that the core of the Internet is susceptible to increasing attacks, including state actors (cyber warfare) and criminal actors. The vulnerabilities in the Internet continue to exist and need to be addressed by the appropriate parties. In this, the challenges are manyfold:

- Liability is strongly related to specific jurisdictions. Liability across jurisdictions requires a better understanding of the harm related to criminal behavior or negligence, on “who is responsible”, and on “what can be expected from the responsible party. Who can reasonably be expected to be responsible for taking specific security measures? For sure the end user cannot take full responsibility, yet has a role, too. It would be important to come to a common understanding of “what can be expected” from different players in the value chain;
- Attribution is a major challenge, yet trusted/respected attribution may have a good impact on behaviour of actors. It is not clear yet how this can be done in a widely acceptable way);
- Insurability of risk would help, yet will need to be based on a good understanding of those risks, and that does not exist widely, yet. Working towards this would help getting better insights in risks and their costs, and would help making the costs for security more explicit;

The output from these discussions would be brought into the ongoing discussions of the Dynamic Coalition, starting with an update of the Global Good Practice on IoT paper (see DC IoT website) and taking this forward to the upcoming IGF in Geneva.

Appendix – list of participants

Walter	Mattauch	DLR Project Management agency
Carsten	Schiefner	All Things Internet. And Internet of Things.
Nigel	Hickson	ICANN
Larry	Strickling	independent
Ramy	Ahmed Fathy	ITU-T SG20
William	Drake	University of Zurich
Olivier	Crépin-Leblond	ISOC UK England
Jari	Arkko	Ericsson
Dan	Caprio	The Providence Group
Michael	Rotert	eco
Olaf	Kolkman	Internet Society
Marco	Hogewoning	RIPE NCC
Dan	Caprio	The Providence Group
Peter	Koch	DENIC eG
Rainer	Rodewald	Bündnis Privatsphäre Leipzig
Tatiana	Tropina	Max Planck Institute for Foreign and International Criminal Law
Maarten	Botterman	GNKS Consult BV
Kaveh	Ranjbar	RIPE NCC
Avri	Doria	independent
Sandra	Hoferichter	Medienstadt Leipzig e.V.
Wolfgang	Kleinwächter	Medienstadt Leipzig e.V.