IPFGI 2018 – Aveiro – 17 Outubro 2018

IPFGI 2018

Universidade de Aveiro – 17 Outubro

Sessão

GOVERNAÇÃO, CONFIANÇA, PRIVACIDADE E DESAFIOS NA ERA DA IOT

Moderador: **Augusto Casaca**, INESC-ID/IST

Keynote: **Henrique João Domingos**, ISOC-PT

Participantes no painel:

Luis Lamela, GoLabs IoT (Altice)
Manuel Ricardo, INESC TEC/Universidade do Porto
Pedro Diogo, Ubiwhere
Susana Sargento, Universidade de Aveiro/ IT

Relator: **Nuno Teixeira Castro,** ISOC-P

Relato

Na apresentação de abertura, o orador caracterizou diversas variáveis estruturantes do posicionamento da ISOC para a área da IoT, balizadas no relatório «*IoT trust framework v2.5*», da ISOC / OTA *Online Trust Alliance*. A apresentação abordou:

- O IoT numa visão integradora, como ecossistema integrando pequenos dispositivos, desde sensores, actuadores, computadores, etc., bem como serviços de software e soluções Cloud, em plataformas *full-stack* para colectar, trocar e processar dados;
- A capacidade de processamento e intervenção de sistemas IoT com vocação e adaptação dinâmica e cada vez mais autonómica e sem supervisão humana, no contexto da gestão das realidades ciber-físicas em que a IoT se insere e opera;
- Os desafios da evolução da situação atual (em que subsistem ambientes mais ou menos isolados de interconexão de coisas (numa IoT sem "I") e o contexto de uma verdadeira IoT interoperável, com expansão sustentável, confiável e segura;
- as oportunidades, ameaças, complexidades e desafios decorrentes, associadas à explosão esperada de implantação em escala de soluções IoT e a sua enorme diversidade e heterogeneidade.
- A necessidade de se refletir sobre a articulação e efetividade de quadros regulatórios, quer no plano da qualidade ou certificação de tecnologias, quer nas implicações societárias, com impacto nos aspetos de governança da IoT e Internet, bem como entrada progressiva da IoT na gestão de serviços sensíveis e infraestruturas críticas.

Painel

A composição do painel foi sumariamente apresentada pelo moderador, que resumiu a metodologia a seguir, baseada nos seguintes "teasers":

- *o estado da arte da realidade IoT;*
- *os principais obstáculos, como privacidade e a confiança, impacto ambiental, e a interoperabilidade dos protocolos de IoT;*
- *os impactos socioeconómicos;*
- *a governação da IoT.*

Do debate, feito por duas rondas, as principais ideias foram:

- Por um lado temos tecnologias de longo alcance, que operam tanto no plano licenciado como no não licenciado, que transmitem a longas distâncias mas a débitos baixos e com longos atrasos; esta condicionante não se conjuga com a necessidade de debitar ordens com muito pouco atraso nalgumas aplicações, nomeadamente para infra-estruturas críticas de energia, água, refinarias, entre outras.

- A cadência do débito da informação exprime a necessidade de maior largura de banda ou de alcance para aplicações críticas, desde que os protocolos de comunicação operem de forma suficientemente interdependente.
- Foi sugerida a consagração de um ecossistema robusto, passando da realidade presente de múltiplos pequenos ecossistemas, a um ecossistema com *standards* mais comuns.
- Com efeito, a normalização permitirá que os serviços inteligentes se destaquem, pela maximização da informação obtida por múltiplos elementos, vertendo-a num formato de dados inteligível, que possa ser trabalhado e utilizado por todos, potenciando os ganhos comuns.
- No plano dos obstáculos, contrastou-se a necessidade de identificadores que garantam uma maior rastreabilidade e confiança associada ao controlo da informação distribuída com a relação entre custo e capacidade da bateria 'versus' escalabilidade para milhares de milhões de equipamentos, com eventual alternativa de utilizar outro protocolo que não o IP.
- No plano da privacidade e da confiança foi identificado o problema principal: como se constrói uma cadeia de confiança? Será possível garantir que um dispositivo, uma 'coisa', mantenha a integridade inicial durante a expectativa temporal da sua utilização, e até que ponto se consegue garantir a segurança dos dados e das comunicações, sem que tal comporte custos acrescidos às organizações e aos utilizadores?
- Foi levantada a hipótese de no futuro se poder assistir à convergência da IoT com a *blockchain*. Mesmo reconhecendo a limitação actual de escalabilidade das blockchain num universo IoT, a *blockchain* poderá alvitrar uma maior segurança dos dados, garantindo ainda a privacidade destes, se, porventura, os *smart-hubs* vierem a operar como *nodes,* operando num plano intermédio.
- No que concerne ao impacto socioeconómico, foi referido o *digital twin*, no contexto de uma possível fábrica que venha a operar 24h/24h de forma completamente automatizada, e suas respectivas implicações sociais; foi salientada a falta de formação, mormente em telecomunicações.
- Foi também dado relevo à optimização operada pela digitalização. No plano das *smart-cities*, por exemplo, foram salientados os ganhos de eficiência com mecanismos, serviços e aplicações inteligentes que, em casos de recolha de lixo e do tráfego rodoviário, permitiram obter optimizações e eficiências na casa das dezenas percentuais.
- No final foi aberto ao público um espaço para colocação de questões, salientando-se o contraste entre a acuidade de leituras proporcionadas por um contador de eletricidade inteligente *versus* a possibilidade de *profiling* do cliente individual que esse mesmo contador poderá permitir.

Mensagens chave

- Crescimento exponencial de ´coisas' na rede, um mercado em franco crescimento, ainda deficientemente regulado e pouco consciente dos problemas de confiabilidade, segurança e privacidade, como critérios-chave para uma IoT de base sustentável e com equilíbrio de visões e interesses entre todos os intervenientes
- A fronteira a ultrapassar tem, necessariamente, de ser a interoperabilidade, para que a infraestrutura comunicacional seja mais eficiente e beneficie das melhores práticas de interoperabilidade ou *standards* de segurança de dados e comunicações, aos diversos níveis de intervenção da IoT: desde as tecnologias na periferia (*things / edge-IoT communication environments*) à sua convergência e integração em plataformas de serviços e soluções na Internet;
- Necessidade de articulação e promoção sinérgica de quadros de colaboração e de responsabilidades multi-stakeholder, que salvaguardem a expansão de uma IoT sustentável, antecipando a adopção progressiva em sectores críticos, cada vez mais exigentes do ponto de vista da confiabilidade, segurança e privacidade de dados e operações.
- O IPv6, (bem como suas repercussões nas áreas de IPSec e tecnologias relacionadas – ex., EDGE ou 6LowPan) bem como a normalização do encapsulamento de diferentes protocolos IoT data-link e encaminhamento IP) é vital para o desenvolvimento da IoT, podendo suavizar as dificuldades de interoperabilidade de protocolos de comunicação ao comportar mecanismos mais flexíveis na questão do endereçamento e encaminhamento seguros;
- É interessante seguir com atenção os esforços de normalização aberta no quadro dos standards de interoperabilidade e segurança IETF, em relação às iniciativas desenvolvidas para a IoT no quadro de protocolos do nível red, nível sessão e nível de suporte aplicação
- O *digital twin* e a digitalização da sociedade comportam riscos mas serão também um leque abrangente de possibilidades, para os quais será necessário antecipar reflexões e avaliações de impacto nos requisitos de siustentabiliddae, segurança e privacidade