M1 : IOT (Internet of Things)

Gilles Menez

Université de Nice – Sophia-Antipolis
Département d'Informatique
email : menez@unice.fr
www : www.i3s.unice.fr/~menez

31 octobre 2022: V 1.0

Table des Matières (1)

Cours 1

Techno Schéma

MongoDB

https://docs.mongodb.com/
https://ibmcloud.developpez.com/tutoriels/apprendre-nodejs-mongodb/

Ethique

J'aime bien la définition Canadienne :

"L'éthique, quant à elle, n'est pas un ensemble de valeurs ni de principes en particulier. Il s'agit d'une réflexion argumentée en vue du bien-agir"

http:

//www.ethique.gouv.qc.ca/fr/ethique/quest-ce-que-lethique/quelle-est-la-difference-entre-ethique-et-morale.html

---

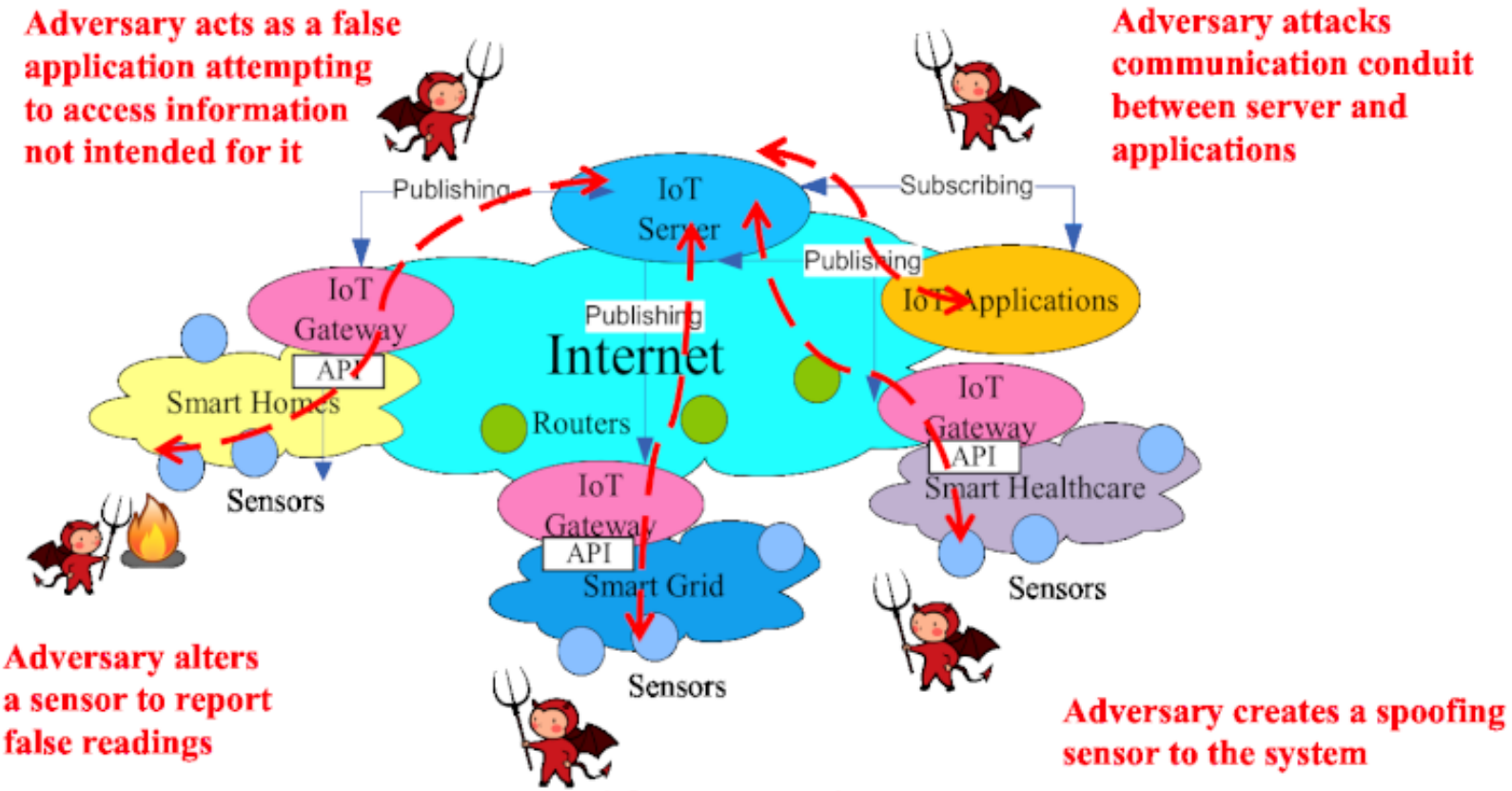
Dans un Internet, on adhère à la divulgation de "ses" données et on "espère" maîtriser cette divulgation.

Dans un IoT, on fait partie, facilement à notre insu, des données.

Maintenant regardons comment évolue Internet . . . et projetons cela sur l'IoT.

Un informaticien/citoyen/humain averti en vaut plusieurs et on comprend que la notion d'éthique accompagne le développement de l'IoT.

Sécurité



"A Security Framework for the Internet of Things in the Future Internet Architecture"
auteurs : Liu, Xiruo and Zhao, Meiyuan and Li, Sugang and Zhang, Feixiong and Trappe, W.

doi = 10.3390/fi9030027

http ://www.smartgrids-cre.fr/index.php ?p=objets-connectes-cybersecurite
Comme l'indique le tableau 1, ci-dessus, les caractéristiques techniques des objets connectés sont jusqu'à 1 million de fois inférieures à celles d'un équipement de bureau, ce qui a plusieurs conséquences en termes de gestion de ces objets :
un état des lieux difficile à établir et à maintenir à jour ; une absence d'information en temps réel ; la quasi-impossibilité à mettre en place des agents de surveillance locaux ; des coûts de remise en fonctionnement rédhibitoires dus à la dissémination des équipements.
Ces différentes conséquences rendent la gestion des risques associée à ces objets complexe et incertaine.
De plus en plus de systèmes critiques sont appelés à être pilotés, informés et guidés par des systèmes complexes et autonomes constitués en partie d'objets connectés, et ce dans de nombreux domaines tels que les transports (véhicules autonomes), la météo ou la gestion des flux au sein d'une collectivité (fluides, trafic).
Cette automatisation vise à accroître la sécurité et la fiabilité des systèmes et promet des gains d'efficacité à court terme.
Outre les difficultés intrinsèques que comportent de telles infrastructures,

celles-ci attireront certains « agresseurs » déterminés à prendre en otage leur propriétaire par différents moyens, comme l'usurpation, le détournement des informations ou le sabotage. Il s'agit donc, pour les gestionnaires de risques au sein des organisations concernées, de faire évoluer leur politique de sécurité des systèmes d'information afin d'assurer efficacement la gestion, la supervision et le respect de la conformité de ce type de parc d'objets connectés.

Before the IoT/big data nexus can deliver on its promise, there are a number of barriers to overcome. The main ones are summarised below. For the IoT to work, there must be a framework within which devices and applications can exchange data securely over wired or wireless networks. One player in this area is OneM2M, an umbrella orgainsation including seven standards bodies, five global ICT fora and over 200 companies (mostly from the telecoms and IT industries). In February this year, OneM2M issued Release 1, a set of 10 specifications covering requirements, architecture, API specifications, security solutions and mapping to common industry protocols (such as CoAP, MQTT and HTTP). "Release 1 utilises well-proven protocols to allow applications across industry segments to communicate with each other as never before – not only moving M2M forward but actually enabling the Internet of Things," said Dr Omar Elloumi, Head of M2M and Smart Grid Standards at Alcatel-Lucent and OneM2M Technical Plenary Chair, in a statement. OneM2M has also published a useful white paper that characterises the background to its mission thus : "The emerging need for interoperability across different industries and applications has necessitated a move away from an industry-specific approach to one that involves a common platform bringing together connected cars, healthcare, smart meters,

emergency services, local authority services and the many other stakeholders in the ecosystem".
Not surprisingly, given the scope and potential value of the IoT market, there are plenty of other standards bodies vying to get their ideas adopted. These include : the AllSeen Alliance, Google's The Physical Web, the Industrial Internet Consortium, the Open Interconnect Consortium and Thread.
According to IDC, "Within two years, 90% of all IT networks will have an IoT-based security breach, although many will be considered 'inconveniences'...Chief Information Security Officers (CISOs) will be forced to adopt new IoT policies". Progress on data standards (see above) will help here, but there's no doubt that security and privacy is a big worry with the IoT and big data – particularly when it comes to areas like healthcare or critical national infrastructure.
The IoT was certainly prominent in the security predictions for 2015 issued by analysts and other pundits at the beginning of the year. Here's a selection :
Your refrigerator is not an IT security threat. Industrial sensors are (Websense) Attacks on the Internet of Things will focus on smart home automation (Symantec) Internet of Things attacks move from

proof-of-concept to mainstream risks (Sophos) The gap between ICS/SCADA and real world security only grows bigger (Sophos) Technological diversity will save IoE/IoT devices from mass attacks but the same won't be true for the data they process (Trend Micro) A wearables health data breach will spur FTC action (Forrester)
It's not all doom and gloom, though. Two commentators foresaw security tightening around critical infrastructure in 2015, for example :
Critical infrastructure will see security improvements (Neohapsis) Greater focus on securing our critical infrastructure (Damballa)
Big data featured in the 2015 security predictions too, but not to such an extent : Rise of Salami attacks will leave a bad taste at the big data banquet (Varonis Systems) ; Machine learning will be a game-changer in the fight against cyber-crime (Symantec) ; and Big data will become a buzzword for the bad guys too (Neohapsis).
As OneM2M points out, security in the IoT is tricky because the multiple stakeholders will have different needs : "For a telecoms operator, security is about ensuring availability ; for a customer organisation, it's about protecting their data ; and for an M2M and IoT provider it's about ensuring uptime...The huge diversity of M2M and IoT device types, their different capabilities and the range of deployment scenarios makes

security a unique challenge for the M2M and IoT industry".

Network & data centre infrastructure

The vast amounts of data that will be generated by IoT devices will put enormous pressure on network and data centre infrastructure. IoT data flows will be primarily from sensors to applications, and will range between continuous and bursty depending on the type of application :

Conclusion

The Internet of Things (IoT) promises to have a big effect by adding a new dimension in the way people will interact with the surrounding things.

Les freins/risques au développement de l'IOT

- ✔ Les limites atteintes de IPv4 : Le nombre maximal d'adresses (2^{32}) est dépassé depuis Février 2010.
  - ➢ Il faut que IPv6 se déploie pour que l'IoT puisse réellement décoller.
- ✔ L'alimentation électrique des capteurs :

  Il faut que les capteurs deviennent autosuffisants : solaire, ou utilisation de nanogénérateurs (dans votre talon de chaussure ?)
- ✔ L'interopérabilité / Les normes :

  Nul doute que chacun va proposer sa solution propriétaire : par exemple amazon, google, free . . . pour le domaine domotique (déja bien développé : Domoticz, Jeedom . . .).

  L'enjeu c'est d'aboutir à une standardisation. Là encore c'est "comme pour les réseaux de données" avec OSI de l'ISO.

  Sauf qu'au final, Internet ne respecte pas ce modèle normatif :
  - ➢ C'est donc bien le plus fort qui a gagné . . . grâce à notamment à UNIX (vecteur de propagation) !
- ✔ La sécurité.

Inter opérabilité

By the Web ? WoT (Web of Things) ! ?