SHARE:

Join Our Email List

# The KIT — Knowledge & Information Technology

No. 179 - 1 November 2016

**Was this forwarded to you?**


**In This Issue**



## Consulting Services

- IT Strategy
- Enterprise Architecture Roadmap
- Business Process Modeling & Analysis
- Enterprise Software Selection
- IT Innovation Briefings
- IT Due Diligence
- Executive IT Seminars
- Cloud Computing
- Security Maturity
- Software Process
- Knowledge Strategy
- Technical Communities
- Knowledge Capture
- Taxonomy development
- Enterprise Social Media

## Contact Us:

## Fighting an Army of IoT Devices

It's not really funny to write "I told you so." Readers of the KIT knows that we have pointed out for a couple of years the vulnerabilities of Internet of Things devices: weak or unchanged passwords, lack of authentication capabilities, and more. The "Krebs incident" (see the last issue) and the attack on the Dyn servers on Oct. 21, both using connected home devices like DVRs and security cameras as proxies to perform mass denial-of-service attacks against targets, show that IoT security issues are very real. So far, no one has been injured and no physical infrastructure has been destroyed, but it is only a matter of time until it happens. It is even possible that it has happened already, and that the victims are keeping quiet about it to avoid hurting their reputation or incurring lawsuits.

A manufacturer of cameras, Xiongmai, has already recalled its devices used in the Dyn attack because they can be installed without changing the default factory password. The battle lines are being drawn between regulators, lawyers smelling big liability lawsuits, companies blaming the users for their carelessness, and users who don't quite know whom to blame or remain blithely unaware that their home devices were already used in an attack.

The genie won't be put back into the bottle. The IoT is here to stay and expand. But serious efforts are needed at all levels to prevent the takeover of devices to turn them into attack bots, to disable them, or to cause them to cause damage. This multi-pronged effort includes device authentication, code vulnerability elimination, defense in depth with layers of intrusion barriers, and in some cases (especially in an industrial context) not connecting to the Internet devices that don't need to be, or at least not using common but insecure protocols.

## Cloud Hosting in Europe

An article about data residency in the last issue mentioned that Microsoft, Amazon and Google are reacting to data movement restrictions out of Europe by building data centers within the EU. Our article hastily said that European companies had failed to capitalize on the opportunity to develop market share against the three US giants.

Two readers, Alain-Michael Diamant-Berger and Jean-Noël Bahar, wrote back to point out that OVH, based in the north of France but currently embarking on an aggressive international expansion plan, is a thriving European hosting and cloud company. 2014 revenues were €240 million, and the company's ambition is to reach €1 billion in 2020. We appreciate being informed of OVH's performance. Still, these are fairly modest numbers compared to the US gorillas. Amazon's cloud services grossed $2.9 billion in just the *second quarter*, and will approach $12 billion for the entire year. And Microsoft's Azure and Office 365 services have a combined goal of $20 million by 2018. And before you object that OVH may be a young upstart that hasn't had the time to grow, the company was founded in 1999.

Data residency issues give OVH a great selling point in Europe, but Amazon and Microsoft are now attacking that market with their much bigger checkbooks and experience, while OVH seems to disperse its efforts by opening multiple data centers around the world. It's going to be interesting to watch that battle unfold.

IT & Knowledge Management

www.cebe-itkm.com
info@cebe-itkm.com

+1 281 460 3595
Twitter: @cbaudoin

**Archive:**
**Previous KIT Issues**

**Forward this issue to colleagues and friends: use the "forward email" link below at left, rather than "Forward" in your email software, to preserve your privacy, give the recipient more options (their own unsubscribe link, etc.) and to give us better click-through data. Thanks!**

## Engineering Systems of Systems

IoT systems can be the most complex "systems of systems" we've had to deal with so far (which, by the way, should reinforce our concern for safety and security). Absent well-developed standards, it is important to apply to the design of such systems the best approaches, including Model-Based Systems Engineering (MBSE).

In this OMG/BrightTalk webinar on November 8 (just to distract you from another important event happening in the U.S. on the same day), Graham Bleakley of IBM and Matthew Hause of PTC will discuss MBSE and the use of the Systems Engineering Modeling Language (SysML).

## Uncertainty Modeling -- Request for Information

The Object Management Group's Analysis & Design Task Force has issued a Request for Information (RFI) on "uncertainty modeling." Responses are due in February 2017. The RFI asks for use cases for the explicit modeling of uncertainty, comments on what existing standards should have uncertainty modeling integrated into them, and how respondents would like to see this concept implemented (e.g., as a UML profile).

Anyone may respond, including non-OMG members. While the second and third topics require some knowledge of UML and other standards, the use case question is very accessible by application domain experts, whom we encourage to read the RFI (the "meat" of the document, sections 2.1 and 2.2, occupies only three pages) and submit their input.

## Seen Recently...

*"Greater than 75% of companies struggle with using, interpreting, integrating, or employing #BigData"*

-- Daniel Newman, @danielnewmanUV

*"One primary reason: There's simply too much data. One of the reasons #ai will be a key solution: Endless capacity to analyze #bigdata"*

-- Response by David Hinchcliffe, @dhinchcliffe
(#ai hashtag refers to artificial intelligence)