SHARE:

Join Our Email List

The KIT — Knowledge & Information Technology

No. 221 - 1 August 2018

Was this forwarded to you?

join our mailing list

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:

Cloud Service Agreements -- What Matters?

One of the first actions of the OMG Cloud Working Group, which succeeds the Cloud Standards Customer Council as we announced in the previous issue, will be to revise two guides last published in 2015: our Practical Guide to Cloud Services Agreements and our white paper on Public Cloud Service Agreements: What to Expect and What to Negotiate.

This is your opportunity to participate! Of course, we're looking for volunteers to help update the papers. But even if you just want to share your input about what works (or doesn't) in the contracts and SLAs offered by your cloud providers, and you want to let us to the editing work, we'll be happy to take your contributions! Please contact Claude Baudoin.

Too Hot on the Beach?

If you don't know what to do in August, here are four ACM conferences that may still have some last-minute spaces (and/or interesting exhibits) -- and take place in interesting locations too. Take your pick:

- SIGGRAPH, the premier computer graphics conference in the world, is in Vancouver, BC, Canada, August 12-16. This will be the 45th edition of this conference.
- SIGKDD, the Conference on Knowledge Discovery and Data Mining, takes place in London, August 19-23.
- SIGCOMM, the conference of the ACM SIG on Data Communications, will be in Budapest on August 20-25. Jennifer Rexford, an excellent Princeton University professor of computer science, will give the keynote address.
- The ACM Symposium on Document Engineering (modeling, detection, storage and visualization of documents) will be in Halifax, Nova Scotia, on August 28-31.

Software Component Transparency

On July 19, the National Telecommunications and Information Administration (NTIA) held a "multistakeholder" meeting in Washington, DC, to kick off a new initiative to improve the security of software by tracing the provenance of its components. Here are some of the points the speakers discussed:

- The notion of Software Bill of Materials (SBOM) is understood, but standards such as SWID (software ID) and SPDX (Software Package Data Exchange) are not sufficient.
- If package P uses component C, which contains vulnerability V, it is not certain that P suffers from V. It is possible that there is no execution path of P that would cause C to execute the vulnerable code. This argument was mostly used by vendors who are trying to avoid the costs of systematic testing and removal of known vulnerabilities. The user community was rather unimpressed by this attitude.

cébé
IT & Knowledge Management

www.cebe-itkm.com
info@cebe-itkm.com
+1 415 870 ITKM
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!

- Vendors are also opposed to letting the public know that their software contains components that harbor vulnerabilities. Someone responded that the food industry has not been killed by the mandate to disclose the list of ingredients on each package, therefore we should be able to do the same for software.
- The National Vulnerability Database (NVD) maintained by NIST does not contain about 30% of the vulnerabilities that have been identified.
- There is a great risk that people will keep talking and will not actually do anything (remember that this is a government-led effort...).

The event concluded with the formation of several working groups:

- Scope and goals -- how large is the problem, and at what level of granularity does the tracking needs to be (components, line of code, ...)?
- Case studies -- understanding the costs and benefits and engaging more stakeholders.
- Standards review -- feasibility of using or improving on existing standards.
- A pilot, prototype, or proof-of-concept (people could not agree on the word) for medical device software, an area where the consequences of inheriting unsafe code can be life-threatening. This was seen as a way out to avoid the "all talk, no action" problem.

Seen Recently...

"In order to design for the future, you have to believe that future is possible."

-- Sandy Speicher, Managing Director of IDEO's education practice
and a strategic adviser to the K-12 Lab Network at the Stanford d.school

"The greatest obstacle to discovery is not ignorance -- it is the illusion of knowledge."

-- Daniel J. Boorstin, historian