SHARE:

Join Our Email List

The KIT — Knowledge & Information Technology

No. 244 - 16 July 2019

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:

cébé
IT & Knowledge Management

A Standard Technical Debt Measure

The Consortium for IT Software Quality (CISQ) has developed a standard measure of software technical debt that can be derived from static inspection of source code. The Object Management Group (OMG) is publishing this under the name *Automated Source Code Technical Debt* (ASCTD), complementing a family of measures related to security, maintainability, reliability and more.

CISQ explains that "the cost to fix structural quality problems constitutes the principal of the debt, while the inefficiencies they cause, such as greater maintenance effort or excessive computing resources, represent interest on the debt." The new measure was developed by gathering input from software developers on the effort needed to fix various weaknesses, and multiplying this by a factor that represents aggravating factors such as the complexity and coupling of software components.

Knowledge Discovery and Data Mining

Too hot in August where you are? The ACM's Conference on Knowledge Discovery and Data Mining (KDD 2019) will take place in Anchorage, Alaska, on Aug. 4-8. The scope covers "data science, data mining, knowledge discovery, large-scale data analytics, and Big Data. The event includes workshops on topics ranging from AI of things to fashion to epidemiology. The opening keynote will be delivered by Peter Lee, Corporate Vice President, Microsoft Healthcare."

IoT Security

This topic almost merits a recurring slot, given the frequency at which we hear about vulnerabilities in mission-critical connected systems. This time, the news (courtesy of CNBC) is that "Medtronic is recalling some models of insulin pumps that are open to hacks, and the Food and Drug Administration warned consumers on Thursday [June 27] that they cannot be patched to fix the holes."

The article goes on to say that this is "a rare example of a medical device recall over a cybersecurity issue" -- we bet that this will not remain rare for long.

This incident (which potentially affects at least 4000 patients, possibly more) relates to a current software transparency initiative by the National Telecommunications and Information Administration (NTIA), part of the U.S. Department of Commerce. The goal of this effort is to develop recommendations for a "software bill of materials" standard that would provide traceability of which components (commercial as well as open-source) were incorporated into a product, potentially introducing vulnerabilities. The NTIA effort includes a proof of concept that happens to precisely be in the medical devices domain.

Chat Confidentiality and Retention

Gennie Gebhart, from the Electronic Frontier Foundation (EFF) wrote an op-ed for the New York Times entitled "What is All Your Slack Chats Were Leaked?" In a sense, she is being unfair to Slack, because she caught the company's disclosure in its filing with the Stock Exchange Commission that hostile nation-states present a particular risk of cyberspying, which is certainly true but is not explicitly mentioned by other companies that handle user messages. But her main point is that Slack (a) does not give users control over retention/deletion of messages, and (b) does not encrypt them end-to-end.

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!

When Ms. Gebhart mentioned her piece on Twitter, an interesting and passionate thread developed. Some people predictably focused on the product space and recommended alternatives such as KeybaseIO, RiotChat, xmpp with OMEMO, wire, ThreemaApp, signalapp and more. Others had the good sense to talk about adoption and change management issues. In response to a tweet saying, "I guess people just don't care enough about security," Mark Cataford replied: "I don't think that it's about not caring, I think it's about inertia: switching over from a tool like Slack would require efforts on your end, on your contacts end and on your organization's end, which is a tough sell unless you can really convey the criticality of doing so."

Seen Recently...

"Python came on the scene, I was like, 'Wow, this is making programming fun again'."

-- Barry Warsaw, recalling the excitement of discovering the language
invented by Guido van Rossum in 1994 and now widely used by data scientists