Hot Clicks: 50 Million Accounts Hit by Facebook Hack

If you had to log back in recently, you may have been impacted.

Amanda Ziadeh

Mon, 10/01/2018 - 15:51

Photo Credit: filistimlyanin/iStock

On Sept. 25, Facebook's engineering team found a security issue affecting 50 million accounts. Attackers exploited a vulnerability in Facebook's code that impacted the "View As" feature, which lets people see what their own profile looks like to others. Ultimately, this let the hackers steal Facebook access tokens which they could use to take over someone's account. Facebook's VP of Product Management Guy Rosen said 50 million accounts were "directly affected" and Facebook knows the vulnerability was used against people, as the attacks are capable of using the accounts as if they are the account holder. The attack is still

under investigation so it's hard to tell if and how the accounts were misused yet, but Facebook said it fixed the vulnerability and 90 million people were logged out of their accounts or Facebook apps as a result. [Mashable](#)

DARPA's New Challenge Asks More from Robots

The Defense Advanced Research Projects Agency's newest challenge, the Subterranean Challenge, is taking robotic design and control to the next level. It requires teams to have robots maneuver objects through three different environments: caves, an urban environment, and a maze of confined tunnes. The robots will be remote-controlled and will still need autonomous skills, like the ability to quickly map and explore unfamiliar environments even when conditions aren't great for communication or sensors. Teams will be able to use as many different types of robots as they want, but that expands the network and complexity of communication and coordination. And the robots will need advances in their form in order to maneuver around these environments, smart remote to balance autonomy and tele-operation, and the fusion of different sensors. Hopefully, these robots can eventually mitigate the safety risks for underground miners and explorers in situations like the recent rescue of the Thai soccer team trapped inside a cave. [MIT Technology Review](#)

US Space Command Treks On

Plans to establish a new combatant command, the U.S. Space Command, continues, as Chairman of the Joint Chiefs of Staff Gen. Joseph Dunford will schedule tabletop exercises this fall to explore its mission details and structure. In a recent memo, Dunford addressed concerns that the space force command would overlap Air Force Secretary Heather Wilson's proposal for a Space Force as a separate military department, the Department of the Space Force. Dunford said the language authorizing service-like responsibilities for the commander of the U.S. Space Command has been removed and if the secretary of the defense wants be commander of the Space Command in the future, changes can be made for a unified command plan. The memo also referenced concerns about acquisitions of space systems and ensuring they reside within the Space Force, and the Joint Staff seems to prefer modeling the Space Command after U.S. Special Operations Command — but perhaps not giving the Space Command the same level of

procurement powers as SOCOM. [Space News](#)

Humanoid Robot Can Install Your Drywall

Japan's Advanced Industrial Science and Technology institute built a humanoid robot called the HRP-5P that can instal drywall, amongst other common construction tasks, using environmental measurement, object detection and motion planning. In a video, HRP-5P uses small hooks to hold onto a wallboard and side it onto the floor, turn it vertically, walk it over to a joist and drill the wallboard into place. This is a very practical-use bot, which can eventually lead to robots building construction sites and assembling aircrafts and ships, and the researchers think the robot can replace an aging population, declining birth rate and manual shortages in the future. Replacing humans in construction could either be a blessing or curse for the 6 million U.S. contractors. [TechCrunch](#)

Voting Machines Can Still Get Hacked

Despite recent awareness of Russian interference in the 2016 U.S. presidential elections, new research suggests voting machines are still highly vulnerable to attacks. The report came out of DefCon's Voting VIllage event, which looked into seven active models of voting machines and vote counters. They found dozens of vulnerabilities, ranging from weak password protections to elaborate ways of remote access. These vulnerabilities weren't necessarily all new, but the ones they knew about were easy to find, reengineer and haven't been fixed in more than a decade of knowing about them, said one of the organizers of the Voting Village. Lots of the vulnerabilities were basic, tracing back to the manufacturers, and in some instances, require having physical access to the machines. Plus, the exploitable bugs accessible remotely would be hard to leverage, but not impossible.

And though election security researchers believe adversaries are more likely to focus on disinformation then changing votes, nation state actors aren't the only threats, and state and local officials don't have the funding needed to replace outdated equipment. [Wired](#)

[View printer friendly version](#)
[Facebook](#)
[space](#)