# Hard-coded PIN vulnerability found in smart toilets

August 6 2013, by Nancy Owano


(Phys.org) —Security experts are warning us all over the place. The digital life used to be a cubicle and workstation. Now it's well, life. Everything is connected, and Internet is everywhere. That means criminal intruders along with pranksters can also broaden their reach from computer malware to home connections such as smart appliances and meters. Last week, there was one more proof that this was so: According to a warning by the information security firm Trustwave, a Satis-brand toilet by the Japan-based company Lixil can be controlled

remotely by an Android app.

According to Daniel Crowley a managing consultant with information security firm Trustwave SpiderLabs, the vulnerability could allow a prankster to outsmart the toilets. The firm posted a warning on August 1 that a luxury brand of toilets that carry a smartphone app for controlling the smart features of the toilet can be commandeered by an outside invader. These toilets can communicate with the phone app through Bluetooth and therein lies the problem.

The Satis smart toilet, said the advisory, is controlled using the app My Satis. This Android application has a hard-coded Bluetooth PIN of "0000" and any person using the application can control any Satis toilet by downloading the app and entering the "0000" PIN. An attacker could cause the toilet to flush repeatedly. This would in turn raise water usage and for those who pay water bills could see an increase in costs on their utility bills.

Attackers could also cause the unit to unexpectedly open and close the lid, activate the bidet or air-dry functions. Depending on age and mental status, these acts could not be so funny and could cause fear or general distress, even though the damage is not lethal. According to Trustwave, the manufacturer was notified about the vulnerability.

The Satis line of luxury toilets may cost anywhere from $2,385 to $4,657 depending on the model. They are loaded with features such as automated lids that open and close, heated seats with temperature control, sprays, music, and deodorizers. The line offers a bowel-movement tracker for those concerned with monitoring their health. At the end of last year, Lixil announced that in 2013 it was to add something even smarter, a series of toilets that can be controlled by smartphone.

They said that the My Satis Android app, which communicates with the toilet using Bluetooth, enables the user to operate its various functions using a handset.

News of the vulnerability has attracted many jokes and snarky metaphors. Apart from entertainment value, though, the story is worth noting because the security firm flagged a situation where a household fixture with a live connection to a smartphone can be exploited.

Interestingly, among the recent Black Hat 2013 presentations was one about "home invasion" where Crowley took part, and it had to do with network-connected devices used in homes posing security risks.

"Once upon a time, a compromise only meant your data was out of your control. Today, it can enable control over the physical world resulting in discomfort, covert audio/video surveillance, physical access or even personal harm," said the presentation notes.

**More information:** www.blackhat.com/us-13/briefings.html#Crowley www.trustwave.com/spiderlabs/a … ies/TWSL2013-020.txt