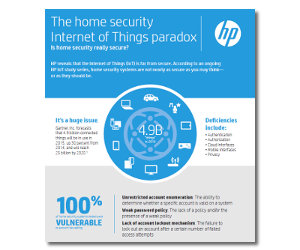
As I wondered which electronic device in my home could make me most vulnerable to hacking (for me it would be an electronic doggy door) the instantly terrifying thought I had was, "What if it's the home security system itself." Disbelief ensued when I discovered an article posted just two weeks ago on the website: Dark Matters, Superior Attack Intelligence. They reported on the ongoing research projects at Hewlett-Packard Enterprises. Ultimately, they found, "10/10 systems were vulnerable to account harvesting via the cloud interface." Their research explores the safeguards that come standard in home security systems to include: password strength (weak passwords are accepted instead of being rejected) and "lock out defense" (some will not execute the system to lock down when being tampered with). But perhaps most shocking, HP reports that 7/10 of security systems failed to utilize authentication "protocols." This is to say that the system didn't even verify they were using their own, safe, server. Even Twitter does that. Remember? You pay for that service with the ~50 characters remaining after your allotted 140 character tweet. Read the article here: <http://darkmatters.norsecorp.com/2015/02/11/connected-home-security-systems-proven-extremely-insecure/>

[](https://camo.githubusercontent.com/2ba8e872ec11e15b889d6d67e0611a5d2fb902e7/687474703a2f2f7777772e636570726f2e636f6d2f696d616765732f75706c6f6164732f68705f696e666f5f70672e6a7067)