The home security Internet of Things paradox
Is home security really secure?

HP reveals that the Internet of Things (IoT) is far from secure. According to an ongoing HP IoT study series, home security systems are not nearly as secure as you may think—or as they should be.

Deficiencies include:
- Authentication
- Authorization
- Cloud interfaces
- Mobile interfaces
- Privacy

Unrestricted account enumeration: The ability to determine whether a specific account is valid on a system
Weak password policy: The lack of a policy and/or the presence of a weak policy
Lack of account lockout mechanism: The failure to lock out an account after a certain number of failed access attempts

Top 5 vulnerability categories identified:
1. Privacy (100%): related privacy concerns regarding the collection of names, addresses, dates of birth, phone numbers, and even credit card numbers. Video image leaks are also an area of concern.
2. Authorization (100%): an attacker can use vulnerabilities such as weak passwords, insecure password recovery mechanisms, and poorly protected credentials to gain access to a system.
3. Insecure cloud (90%): cloud-based Web interfaces exhibit account-enumeration concerns.
4. Insecure software/firmware (70%): did not include obvious update capabilities.
5. Insecure mobile (50%): have enumeration concerns with their mobile application interface.

Are you the only one monitoring your home?
If video streaming is available through a cloud-based Web or mobile application interface, then video can be viewed by an Internet-based attacker from hacked accounts anywhere in the world.

Three actions to mitigate risk

1. Include security in feature considerations when evaluating potential IoT products or services. Avoid using system defaults for user names and passwords whenever possible, and always choose good passwords when the option is available.
2. Don’t share account access with anyone outside your immediate family. Remind others on your household about this security issue.
3. The Federal Trade Commission (FTC) recommends that IoT device manufacturers incorporate security into the design of connected products.

HP Fortify on Demand
Solutions like HP Fortify on Demand enable organizations to test the security of software quickly, accurately, affordably, and without any software to install or manage—eliminating the immediate risk in legacy applications and the systemic risk in application development.

Read the full report: hp.com/go/fortifyresearch/iot2

Gartner, Inc. forecasts that 4.9 billion connected things will be in use in 2015, up 30 percent from 2014, and will reach 25 billion by 2020.1


Open Web Application Security Project (OWASP) Internet of Things Top Ten Project

2Open Web Application Security Project (OWASP) Internet of Things Top Ten Project
3SANS Institute Password Construction Guidelines (PDF)
4Security Is a Must for the Internet of Things, Terrell McSweeny, Commissioner, Federal Trade Commission