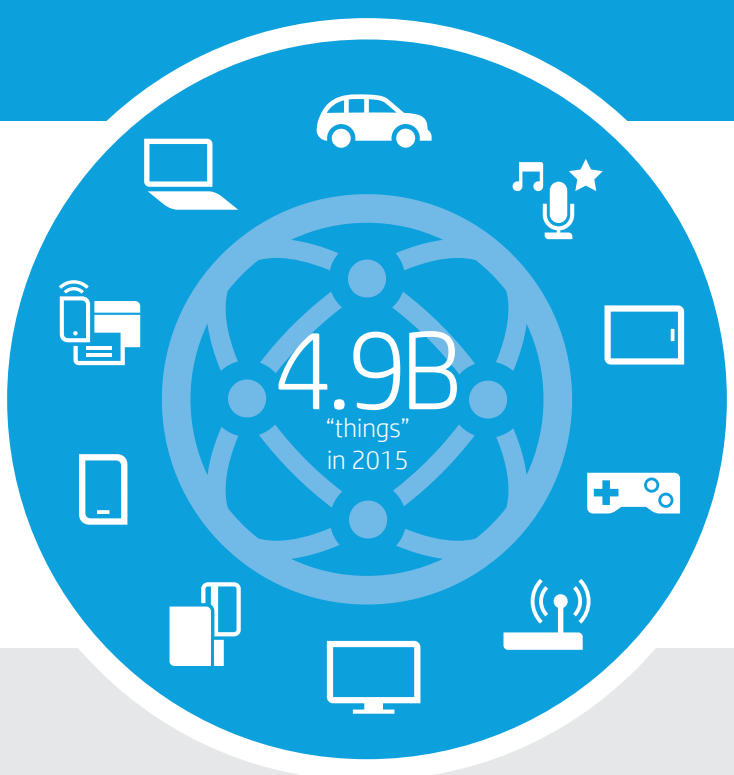
The home security Internet of Things paradox

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.



It's a huge issue.

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]

Deficiencies include:

- Authentication
- Authorization
- Cloud interfaces
- Mobile interfaces
- Privacy

100%
of home security systems tested were
VULNERABLE
to account harvesting

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

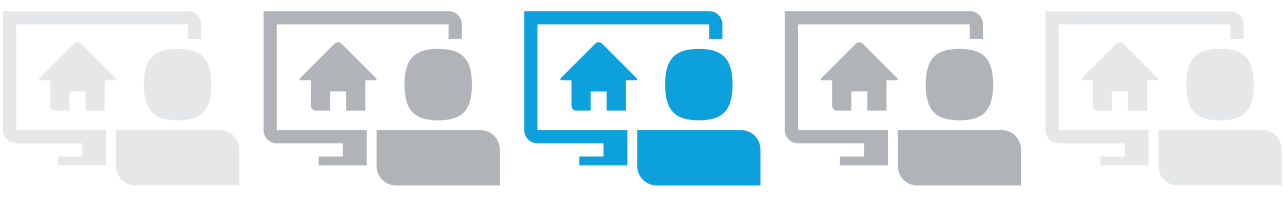
Lack of account lockout mechanism: The failure to lock out an account after a certain number of failed access attempts

Account harvesting is exacerbated when video access is granted to additional users such as family members or neighbors.

Top 5 vulnerability categories identified[2]:

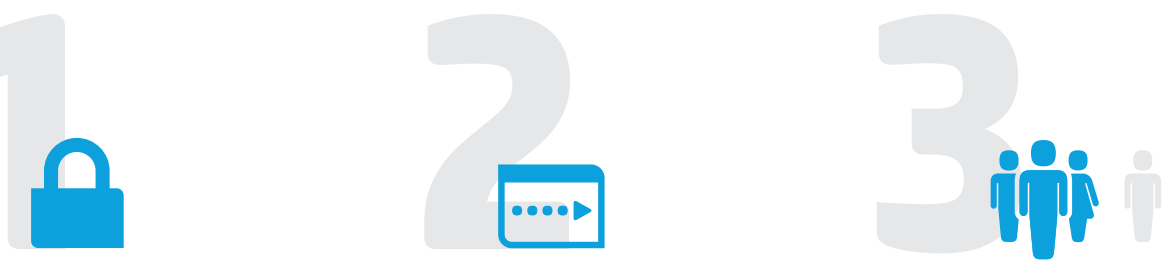
1. **Privacy** (100%)—raised privacy concerns regarding the collection of names, addresses, dates of birth, phone numbers, and even credit card numbers. Video image leaks are also an area of concern.
2. **Authorization** (100%)—an attacker can use vulnerabilities such as weak passwords, insecure password recovery mechanisms, and poorly protected credentials to gain access to a system.
3. **Insecure cloud** (70%)—cloud-based Web interfaces exhibit account-enumeration concerns.
4. **Insecure software/firmware** (60%)—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



Include security in feature considerations when evaluating potential IoT product purchases

Avoid using system defaults for user names and passwords whenever possible, and choose good passwords[3] when the option is available

Don't share account access with anyone outside your immediate family—and stress secure password practices with those who have access

The Federal Trade Commission (FTC) recommends that IoT device manufacturers incorporate security into the design of connected products.[4]

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**

[1]Gartner, Press Release, "Gartner Says 4.9 Billion Connected "Things" Will Be in Use in 2015" November 2014, http://www.gartner.com/newsroom/id/2905717.
[2]Open Web Application Security Project (OWASP) Internet of Things Top Ten Project
[3]SANS Institute Password Construction Guidelines (PDF)
[4]Security Is a Must for the Internet of Things, Terrell McSweeny, Commissioner, Federal Trade Commission