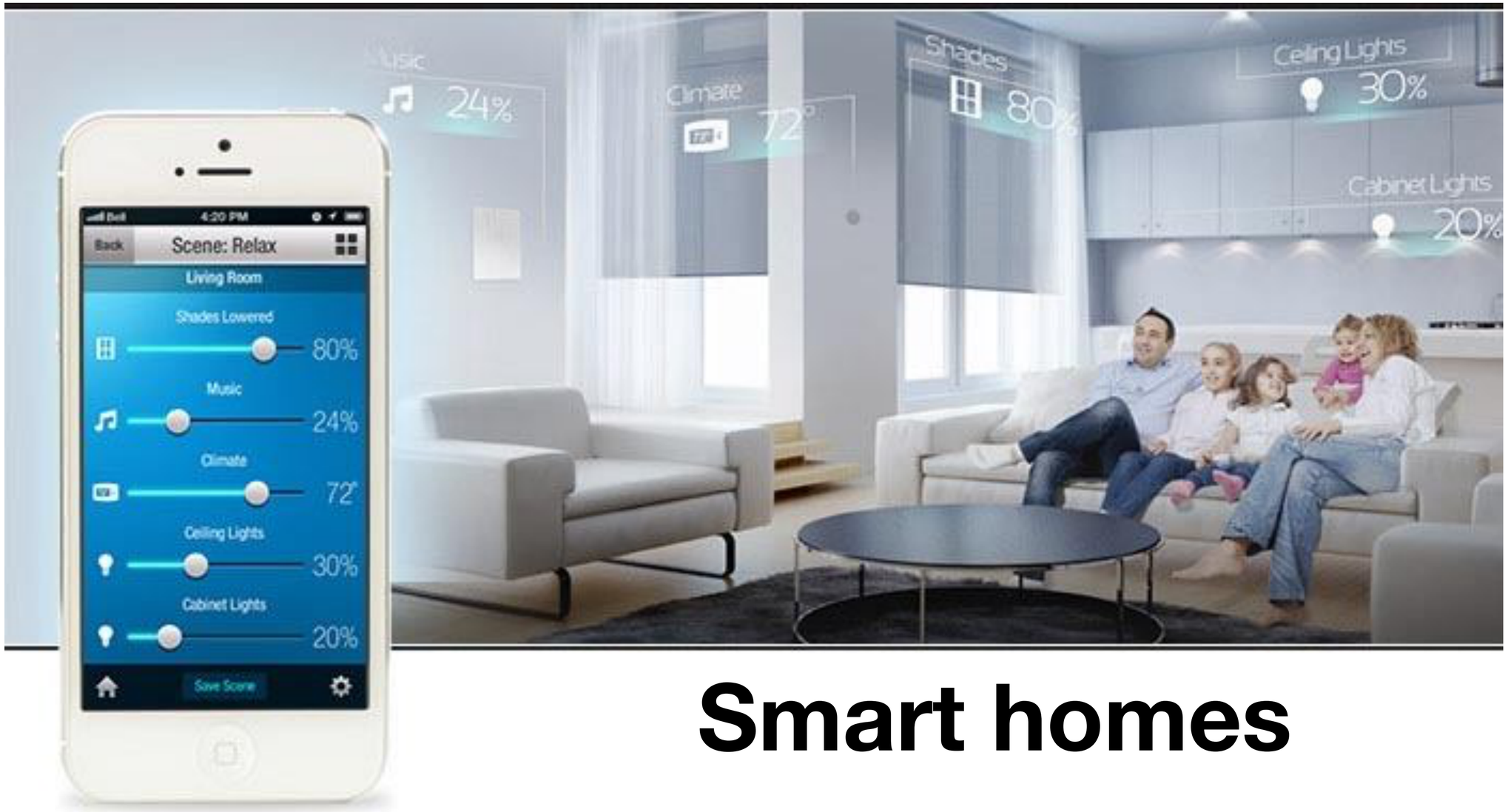
Challenges to ensuring human safety throughout the life-cycle of Smart Environments

David Kotz and Travis Peters
Dartmouth College
November 2017

SafeThings 2017
ACM Workshop on the Internet of Safe Things

Advent of Smart Environments



Smart homes

http://7ngbi4euja2hsxjw2esg0d13.wpengine.netdna-cdn.com/wp-content/uploads/sites/4/2017/03/smart-home-family-in-house-1.jpg

Smart buildings

http://alabamacontrols.com/wp-content/uploads/2013/06/Building-management.jpg

Smart offices

http://onesoundchoice.com/company-blog/cache/com_zoo/images/Christie-Brio_Main-Boardroom_Hi-Res_ec55f224830c302b49ee9af72f17153a.jpg

Smart malls

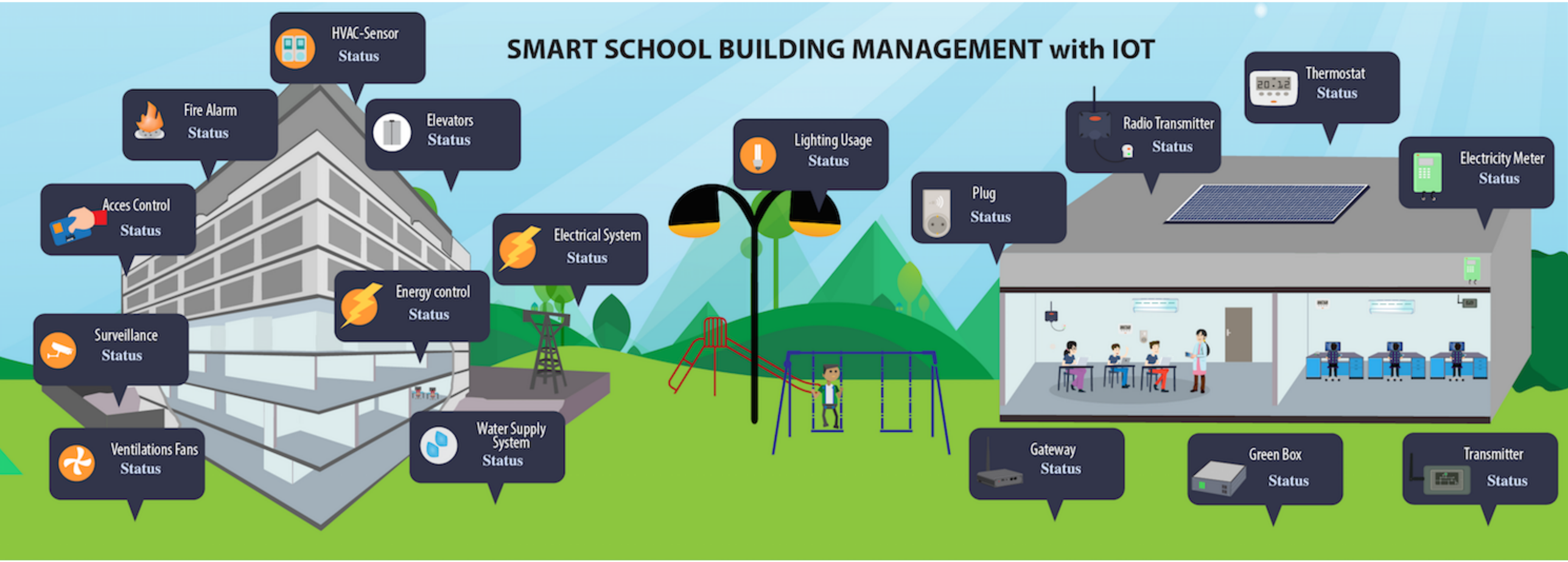
http://trolley.ae/image/data/old/Smart-Mall.jpg

https://t4.ftcdn.net/jpg/01/62/38/83/500_F_162388377_pQyFYRwEhJRnpzbLfEpEGBLuZfUrgreM.jpg

Smart schools

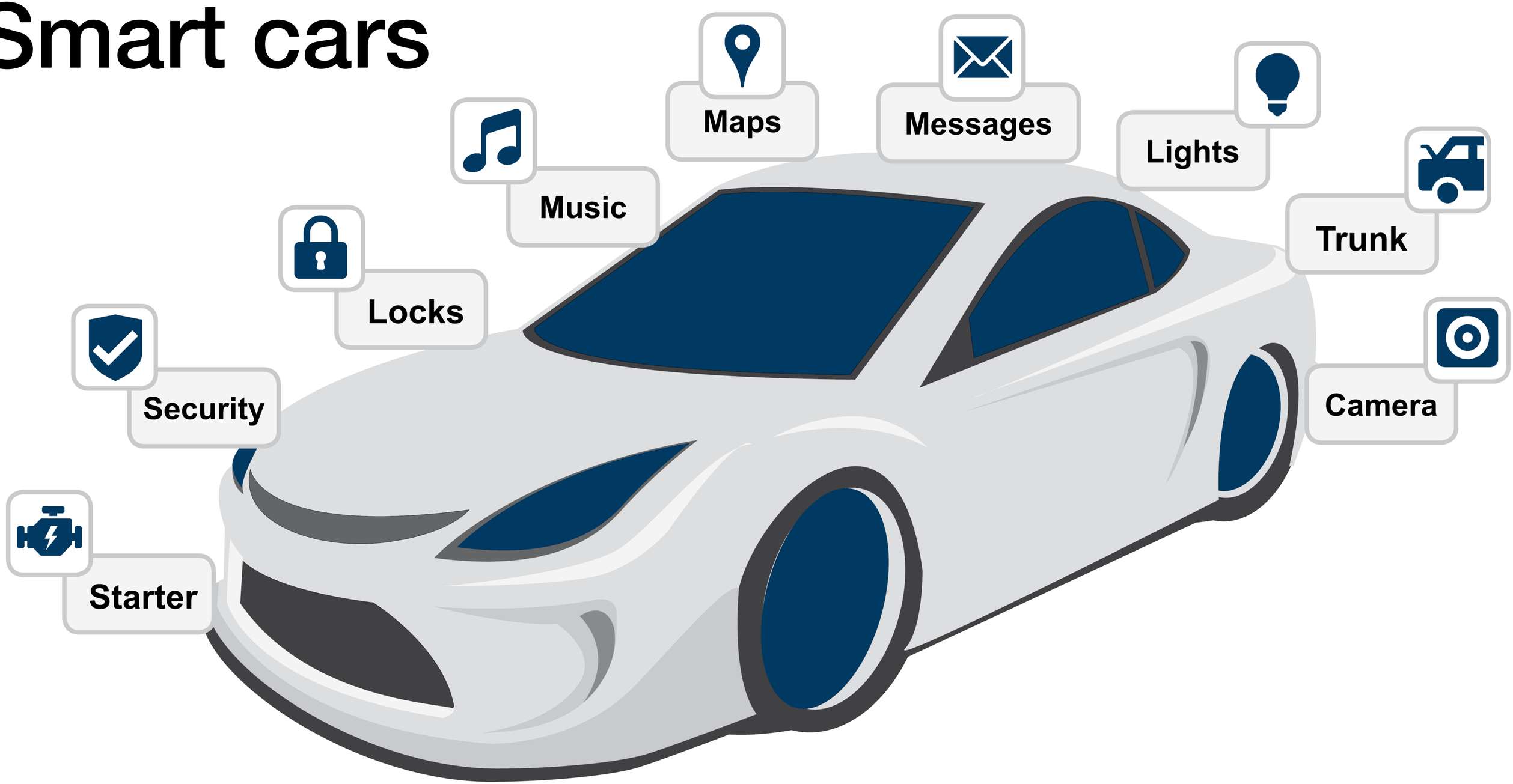
http://2.bp.blogspot.com/-rCst6A028ME/UYGfC72zuiI/AAAAAAAAABM/9xNjAgrv9SQ/s1600/overview_education_lead_3.jpg

Smart school buildings



http://www.cyberschool.id/sites/www.cyberschool.id/files/IOT_SMART%203.png

Smart cars



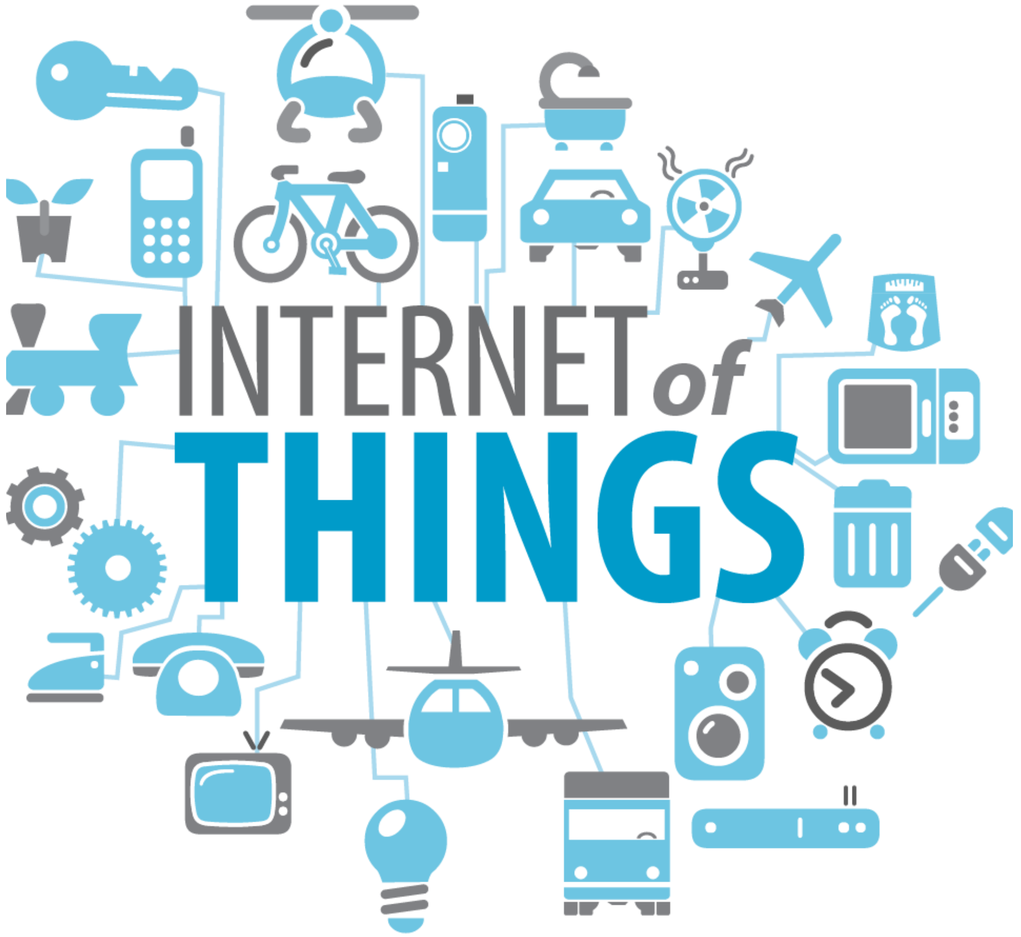
https://iot.do/wp-content/uploads/sites/2/2016/10/IotCar.png

Definitions

https://img.wikinut.com/img/25wulsha.lly79n-/jpeg/0/Definitions-matter.jpeg

Internet of Things

a vision in which a wide range of everyday objects become Smart Things through the inclusion of digital electronics and a network interface that allows them to communicate with other Things and, directly or indirectly, through the Internet with remote services.



https://www.industriaitaliana.it/wp-content/uploads/2016/05/IoT-2.png

Smart Things, Smart Environments

Smart Things

- may be able to sense, or affect, their environment
- may or may not have a human interface
- may be tiny (like hearing aid) or large (like refrigerator)
- may be stationary or mobile
- may be battery or line powered

Smart Environment is an environment where

- Things interact with the environment, with its human occupants, with each other, and with remote services, to accomplish one or more applications.

Things – and human occupants – may come and go from the environment, over short and long time scales.

Owners, Occupants, Operators

- An **owner** is a person or organization who legally owns the Thing or Environment
- but Things or Environments may have an **operator** distinct from owner
- An Environment has a dynamic set of **occupants** (people)
- Example: corporation **owns** a shopping mall, but independent contractor **operates** the building infrastructure; shopkeeper owns the displays inside her shop; shopper briefly **occupies** the shop, wearing personal Things.

Safety

- **Smart Environment is *safe* if it does not create undue risk of harm to persons, organizations, or infrastructure.**

- Smart Things, and the resulting Smart Environments, may create risk because of errors in design, implementation, or configuration, or due to mechanical or electrical failure.

  - Persons may suffer **physical harm**, **financial harm**, or **reputational harm**.

  - Organizations may suffer financial harm or reputational harm.

  - Infrastructure may suffer physical harm, which can cause financial harm to its owner.

  - Occupants may experience **logistical harm**.

  - Example: a school burns down but nobody is injured – the city must pay for a new school and the schoolchildren have no place for school.

Cyber threats

Our focus: **cyber-security** or **digital privacy** failures, which may cause

- physical harm to Things, Environments, or occupants, and thus financial harm to owners;

- reputational or financial harm to owner or occupants through exposure of personal information.

Security and privacy are necessary (but not sufficient) to safe Environments.

http://www.anseetec.com/wp-content/uploads/2016/11/smart-home-security-700.jpg

Adversary model

- **Remote third party** may seek to harm persons, Things, or Environments.
- **Thing manufacturer** may violate privacy of owners or occupants.
- **Thing owner** or **operator** may violate occupant privacy.
- **Occupants** may attack Things from greed or malicious intent.

Challenges

1. Things must be configured – securely
2. Things may have multiple owners
3. Occupants will move across Environments
4. Things will move across Environments
5. Things may transfer to a new owner
6. Environments may transfer to a new owner
7. Things must be discovered and identified
8. Things may fail – and must fail-safe
9. Thing vendors may change terms of service
10. Thing vendors may disappear
11. Things will be thrown away
12. Things will last longer than expected
13. Everyday people manage everyday Things

http://pinuji.net/wp-content/uploads/2014/06/challenges-ahead.jpg

Things must be configured – securely

configuring Things to

- connect to network(s)
- coordinate with other Things
- communicate with back-end services

and to securely

- install keys and credentials
- establish relationships among Things, Environments, and owners

WANDA

see thaw.org/wanda

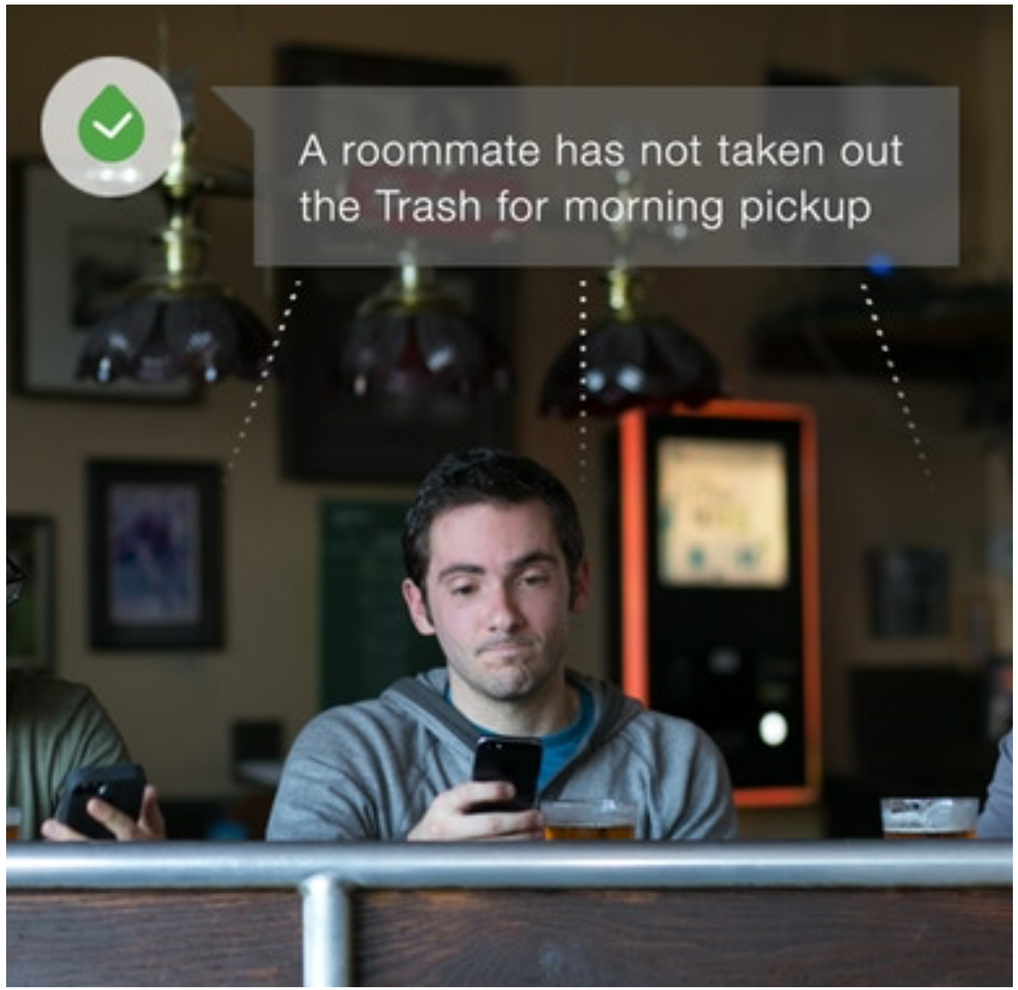
Things may have multiple owners

The common model (wrong):

- A homeowner buys, installs, and uses all the Things in her Smart Home.

The reality: multiple owners in one Environment

- e.g., landlord owns apartment building
- renter owns appliances
- roommates own personal Things
- guests bring in personal Things
- neighbors' networks overlap



https://ksr-ugc.imgix.net/assets/003/404/597/d4f0cc9a230bc11add6bdbae2fd3e64c_original.jpg?w=680&fit=max&v=1425848094&auto=format&q=92&s=9f5c6d270a879572f8e7c576d9d814b1

Occupants will move across Environments

8:10 am

Brush teeth

Jennifer brushes her teeth and showers in water pumped via underground pipes into her home. The water is monitored at the source for contaminants, and added fluoride helps to prevent cavities.

8:40 am

Drive to work

Jennifer wears a seatbelt, as required by law, to reduce auto injuries. Her car was manufactured according to automobile safety standards and is inspected annually for emissions levels to protect air quality.

9:15 am

Cross the street

Jennifer parks her car in a municipal lot, drops a birthday card for her brother in the mailbox, and crosses to her office building. She has to walk around some construction workers filling potholes.

9:25 am

Take elevator to office

To get to her office, Jennifer takes the elevator. It has been built to comply with safety regulations. Her building is reinforced to protect against injury during earthquakes, hurricanes, and other natural disasters.

11:00 am

Work on the Internet

In her office, Jennifer uses the Internet to communicate, get information, and conduct business. The Internet was first developed by researchers at the Department of Defense.

12:20 pm

Make ATM withdrawal

Jennifer's bank accounts are insured by the Federal Deposit Insurance Corporation, created by Congress to ensure that people do not lose their savings if their bank fails.

12:30 pm

Buy lunch

Jennifer buys a salad from her favorite deli. The local health department inspects the deli for cleanliness and makes sure employees practice hygienic food handling.

4:00 pm

Take son to park after school

Jennifer's 4-year-old son plays and learns at their local public preschool. Jennifer's county government maintains parks, pools, skating rinks, and more, keeping them clean, safe, and fun.

5:10 pm

Take mother to the doctor

Jennifer picks up her mother to get her a flu shot, as recommended by health officials, who coordinate flu vaccine development each year. Since she's over 65, she qualifies for Medicare to help pay her medical bills.

6:30 pm

Cook dinner

Jennifer and her husband prepare a meal. The variety of food products available to Americans has been expanded by new trade treaties. Food quality, safety, and labeling are monitored upon entry into the U.S.

7:30 pm

Put baby to bed

Their daughter wears flame-retardant pajamas, cuddles a teddy bear appropriate for a child her age, and sleeps in a safe crib, all thanks to consumer protection and safety regulations.

7:20 pm

Recycle trash

Jennifer sorts her garbage for curbside pickup. Her town provides sanitation services, such as garbage collection and sewerage systems, that protect public health and ensure a pleasant living environment.

A walk through the day of a typical American woman reveals an array of public investments that help us build capabilities, decrease risks, and increase resilience. The legacy of such investments is all around us—so much so that we tend to take them for granted.

Things may transfer to a new owner

Selling or gifting a used Thing to new owner…

Challenges:

- deleting sensitive data
- deleting keys and credentials
- and *verifying* these are done correctly.

https://ae01.alicdn.com/kf/HTB1UPYPSFXXXXb.XFXXq6xXFXXXO/Good-selling-Keyless-Entry-Replacement-font-b-Key-b-font-Case-for-Toyota-font-b-Smart.jpg

Environments may transfer to a new owner

Selling a smart home, or transferring rental property to new renters…

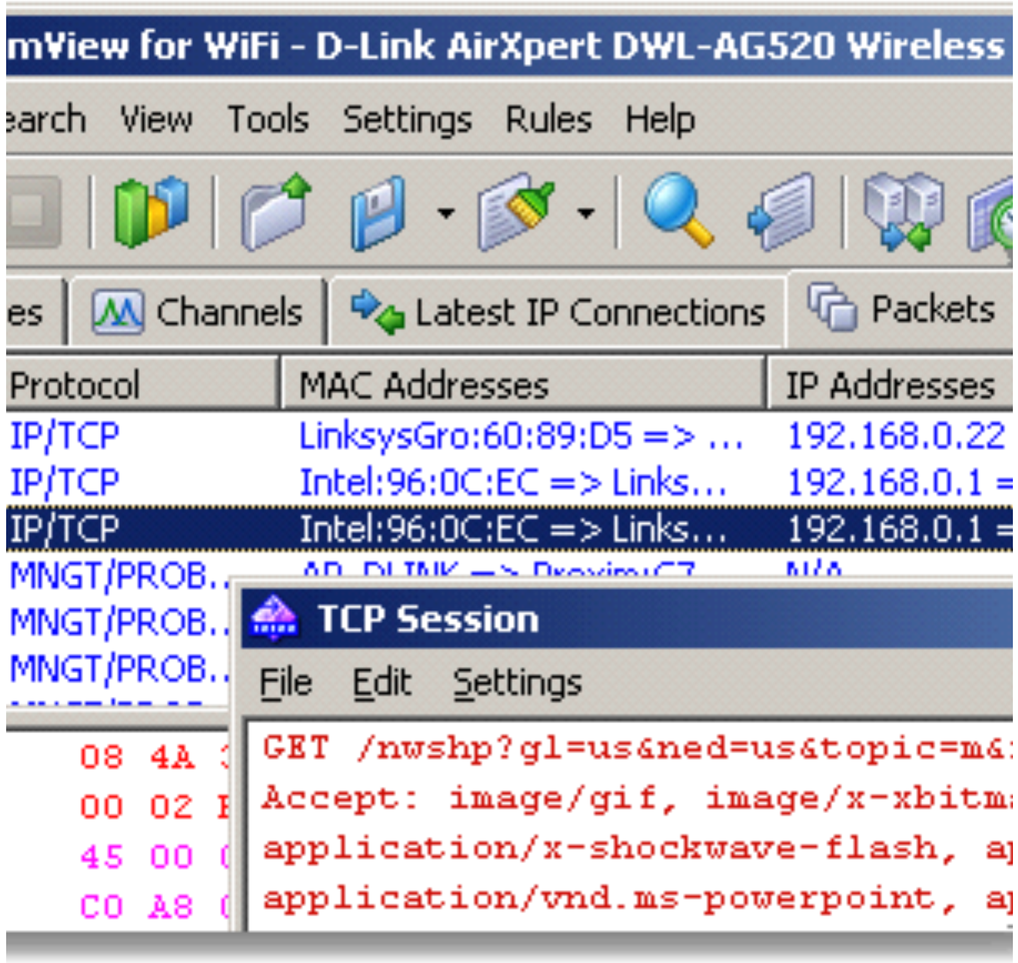
Challenges:

- de-authorizing prior owners and operators
- from Things and back-end services
- and *verifying* this is done correctly.

Things must be discovered and identified

Challenges:

- what Things are here?
- where are they?
- who owns them?
- who operates them?
- what terms of service apply?
- what privacy policies apply?
- which firmware is outdated?
- how do I find updates?



http://www.tamos.com/i/caclip1.png

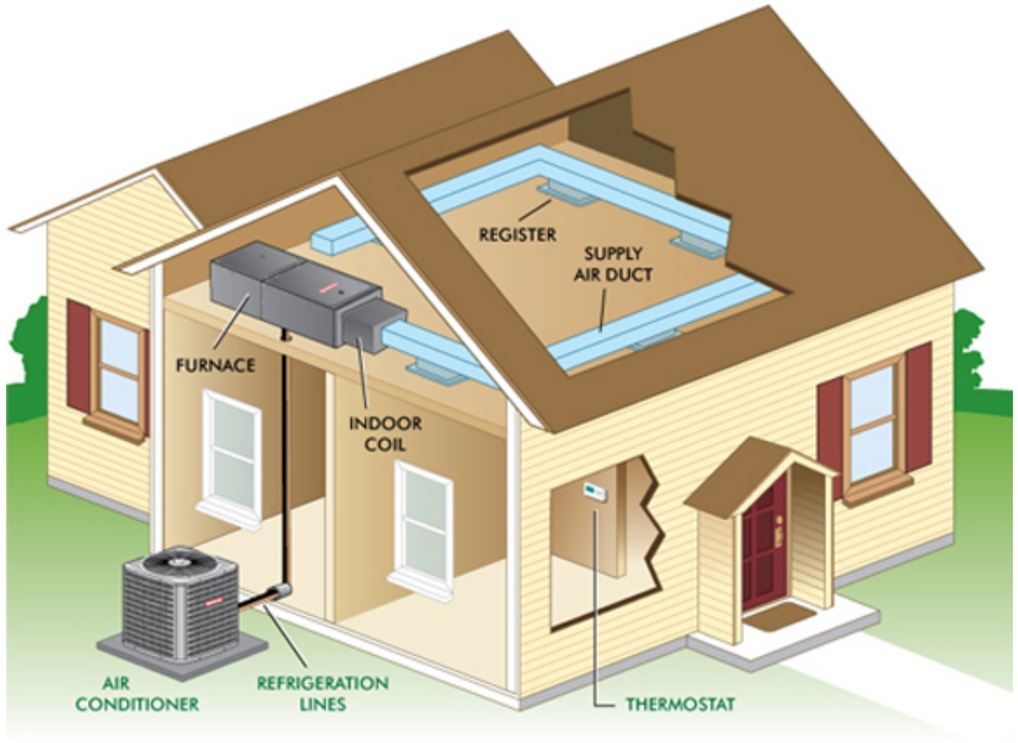
Things may fail – and must fail-safe

When under attack, fail-stop may not be a viable option:

turning off the furnace in mid-winter

disconnecting your glucose sensor

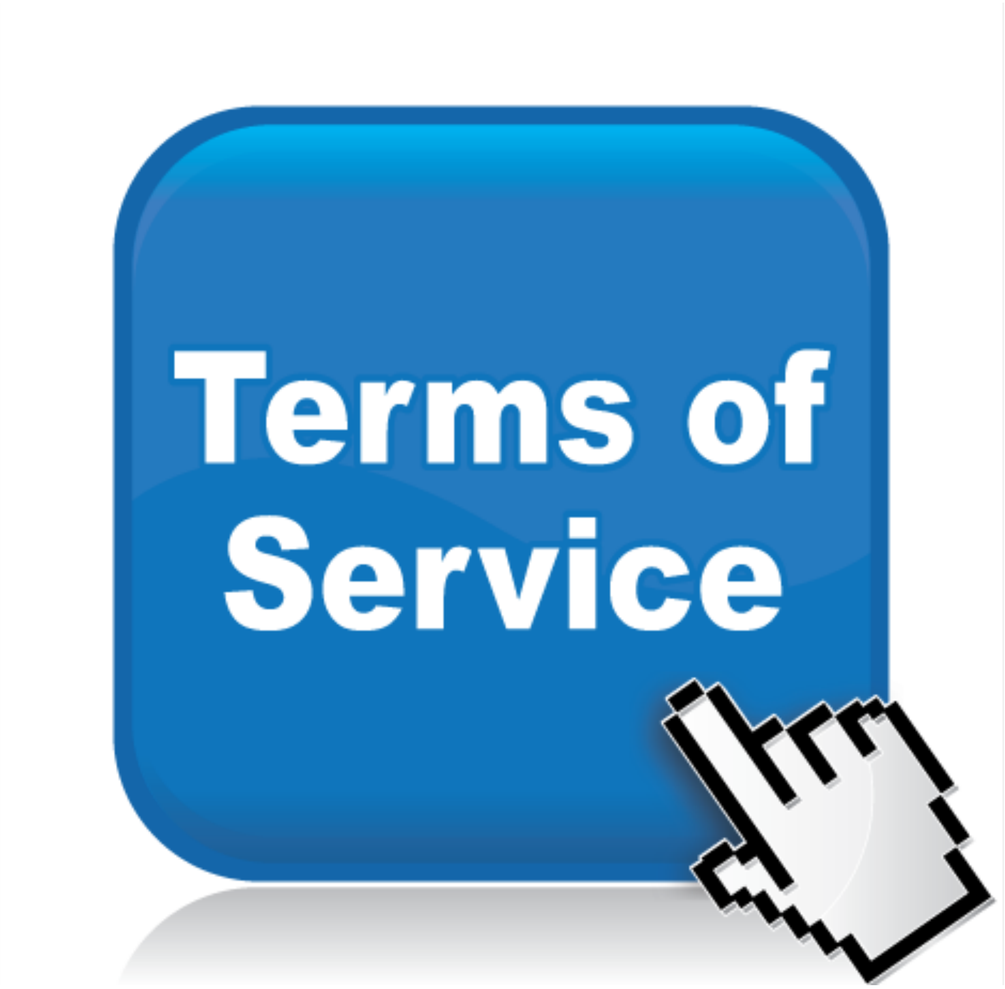
…



http://www.greenbuildingadvisor.com/sites/default/files/Furnace%20illustration%20from%20AHRI.jpg

Thing vendors may change terms of service

- How are owners, occupants notified when vendor or service changes privacy policy, or service policy?
- And what can they do about it?



http://generalstandards.co/wp-content/uploads/2014/07/Dollarphotoclub_58922791-480x460.png

Thing vendors may disappear

- What happens when vendors go out of business, or are sold to a new vendor?
- Do Things stop working?
- Will security updates continue?
- Will owners even know about it?

https://readcenter.org/wp-content/uploads/2017/09/out-of-business-www.imagesplitter.net_.jpeg

Things will be thrown away

Discarding an old Thing…

Challenges:

- deleting sensitive data
- deleting keys and credentials
- and *verifying* these are done correctly.

https://www.gearfuse.com/wp-content/uploads/2015/09/abc.png

Things will last longer than expected

- Today’s IT devices last 2-4 years
- Tomorrow’s Smart Things may be installed (and used) for 20-40 years…
- how to maintain them?
- how to keep track of them?
- how to find old things that don’t speak modern protocols?

http://the52weeks.com/wp-content/uploads/2012/06/IMG-20120606-00338.jpg

Everyday people manage everyday Things

Smart homes don’t come with a sysadmin!

Smart Things will be

- purchased
- installed
- configured
- used
- transferred
- destroyed

by everyday people, not tech-savvy people.

https://www.greatescapepublishing.com/wp-content/uploads/thephotographerslife/images/normal_110411_Everyday_People-5236-.jpg

Research questions

skip

https://s3.amazonaws.com/libapps/accounts/54020/images/Mindmap.JPG

Research questions

- Risk management – and prioritizing risk
- Multi-owner, multi-occupant environments
- Intermittent connectivity
- Platform security
- Secure embedded systems
- Common software infrastructure
- Mobility across environments
- Authenticated data sources
- Authenticated humans
- Discovery and management mechanisms
- Unknown lifetimes
- Secure de-provisioning and destruction
- Discovering, identifying, and attesting to Thing properties

skip

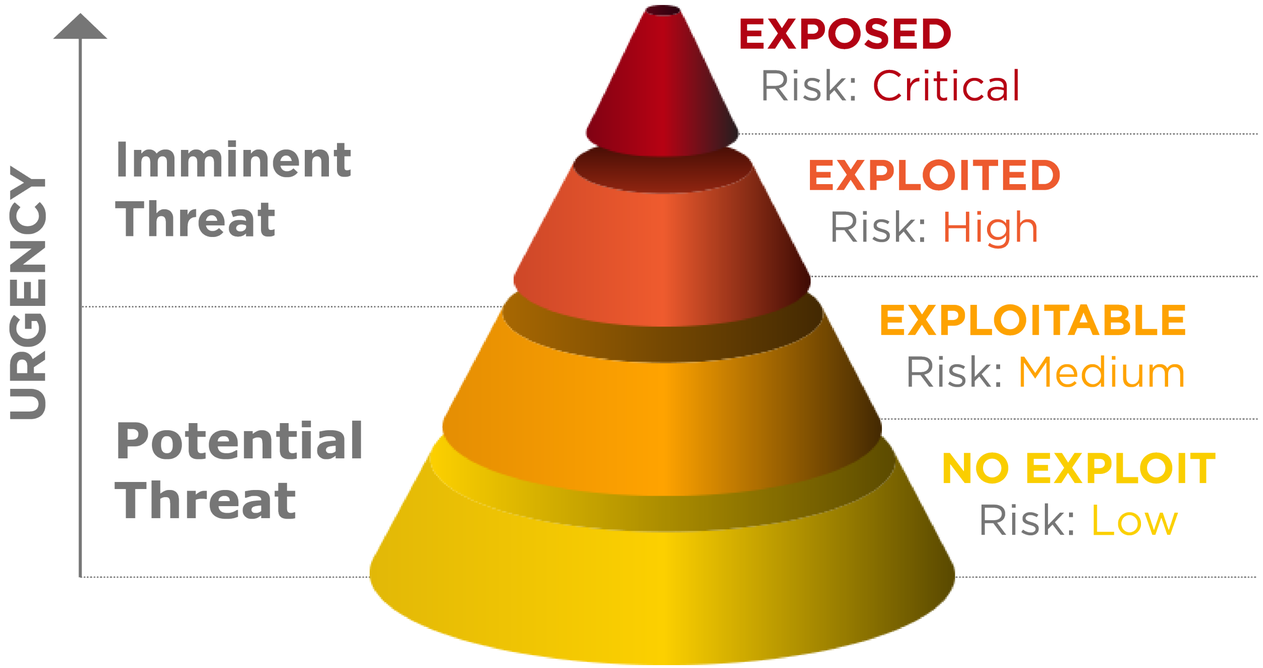
Risk management

- How can Smart Things and Smart Environments ensure safety properties even in the face of failure or attack?
- How are Smart Environment owners/ operators made aware of failed or compromised Things?

http://www.kweaus.com/uploads/60108/ufiles/Risk_Management.jpg

Prioritizing risk

- Can we develop a structured model for characterizing and grading the most important risks in a given application, allowing developers to focus design and implementation effort on the most substantial risks?
- Can such models help occupants or owners to assess and manage their own safety risks?

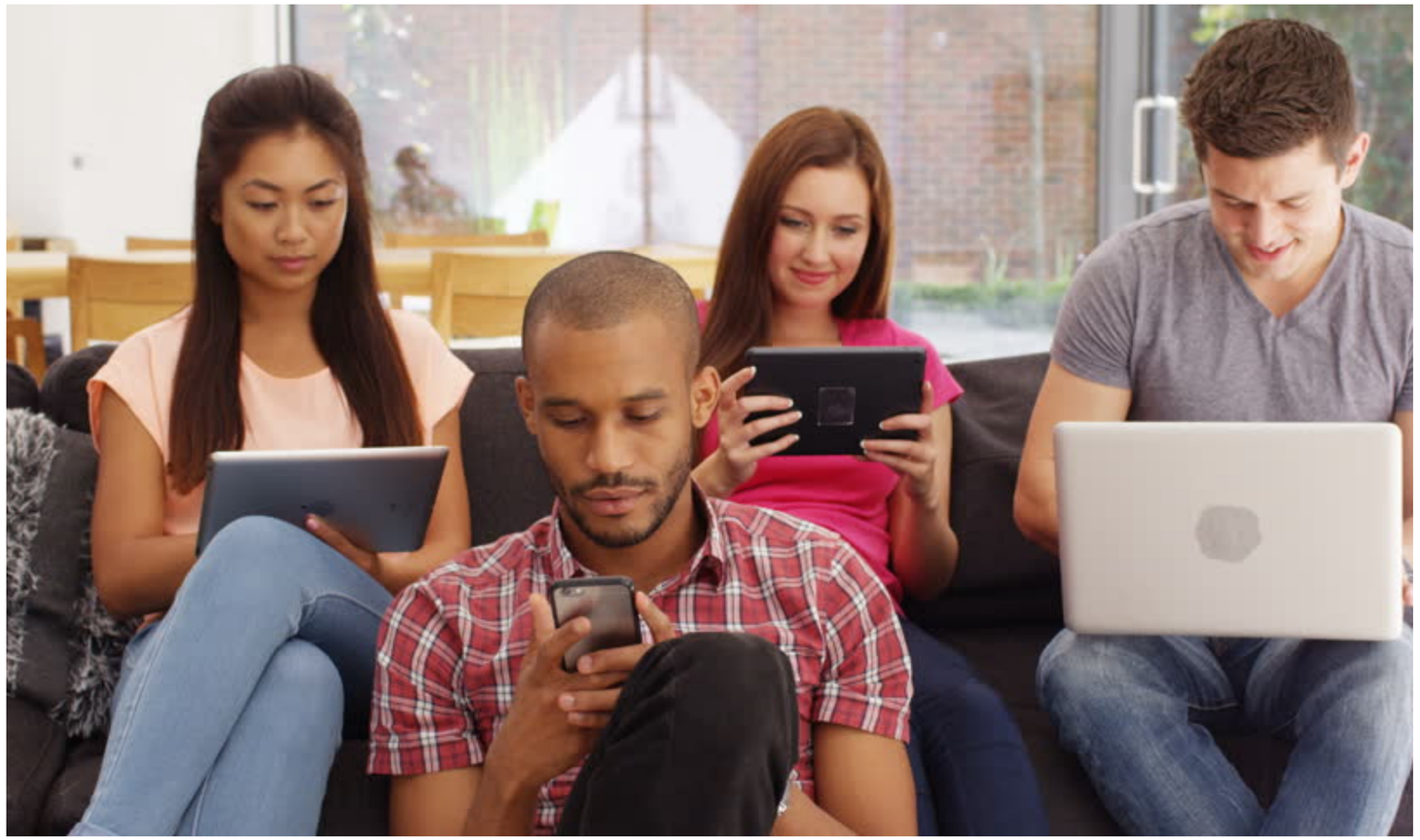


https://www.skyboxsecurity.com/sites/default/files/Vulnerability_Control-prioritization.png

Multi-owner, multi-occupant Environments

- What security architecture allows an Environment owner to manage a space with Things that are owned by unknown other persons, or for a Thing owner to manage its relationships with Things owned by others?

- How is a Thing (or Environment) securely and verifiably transferred to a new owner?



https://ak8.picdn.net/shutterstock/videos/24308258/thumb/1.jpg

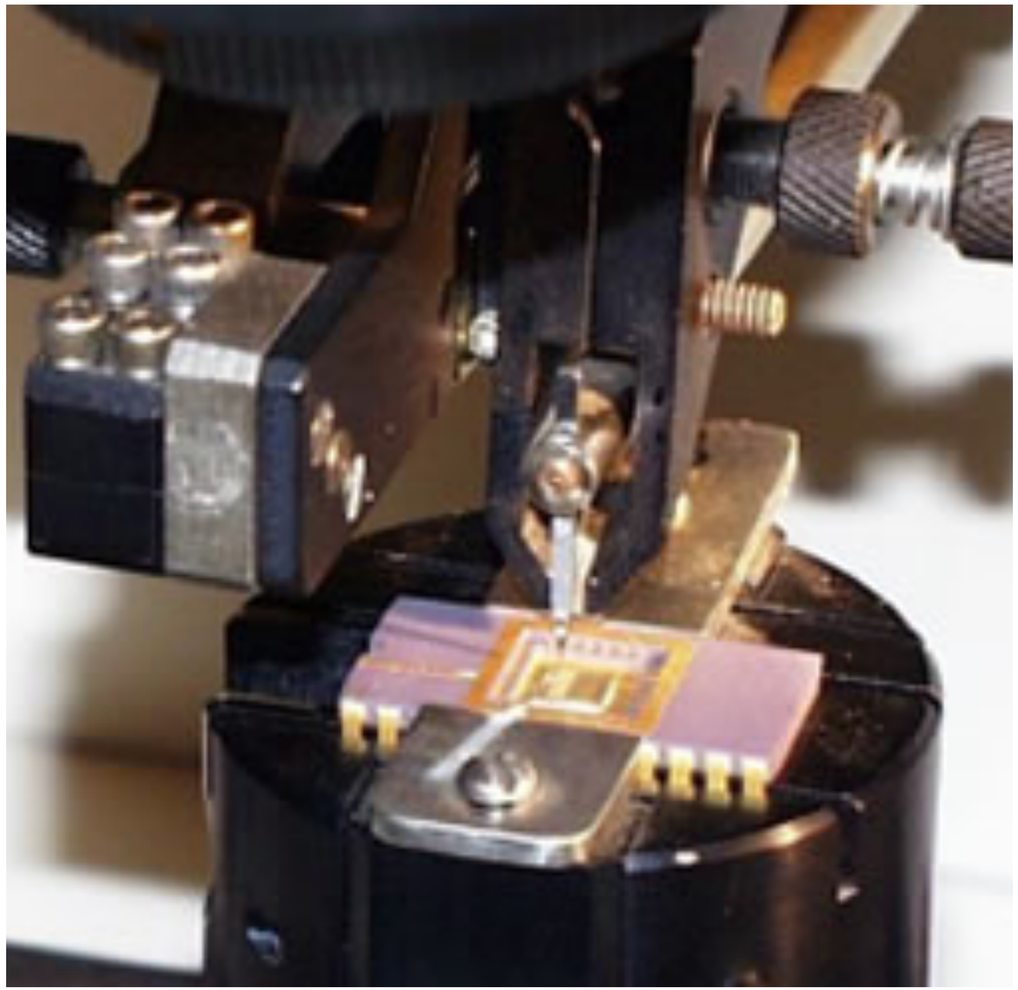
Intermittent connectivity

- How can we architect Smart Things and Environments to be robust to lapses in network connectivity, with an aim to mitigate harm to humans and Things?

http://www.ukiahwireless.com/wp-content/uploads/2016/07/TOWERA.png

Platform security

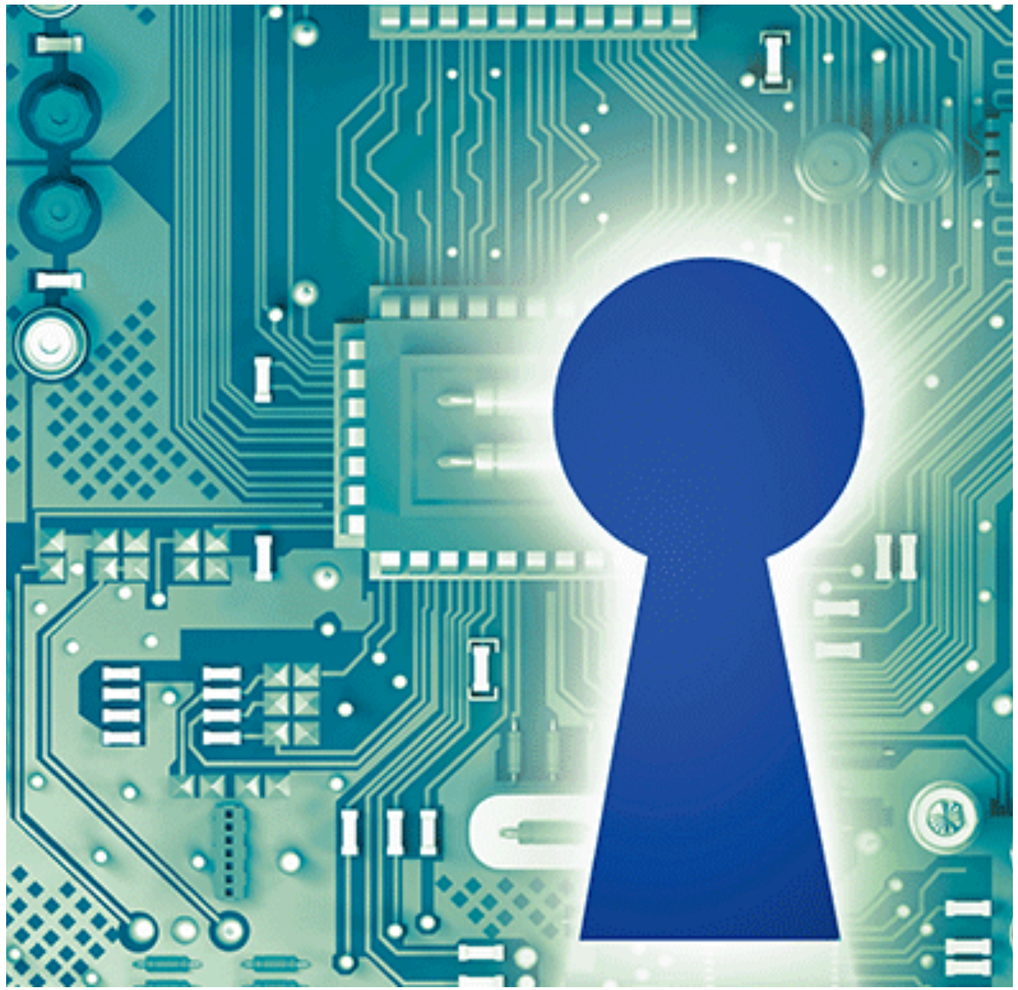
- How can we provide physical security for cryptographic material and computations, and a trustworthy platform for secure computation and remote attestation, in low-resource embedded devices?



http://www.mikahk.com/topics/images/A-M-2.jpg

Development of secure embedded systems

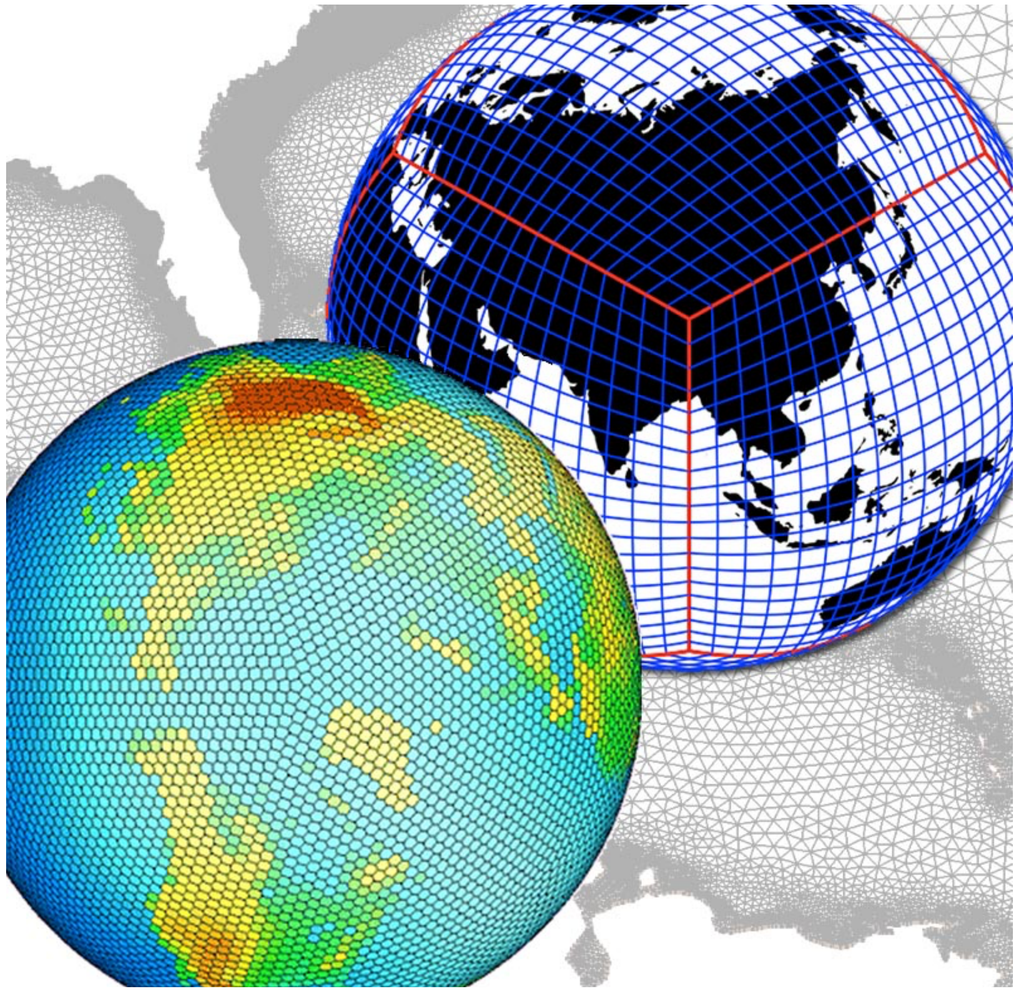
- What tools can assist programmers in developing secure software for embedded systems, and in particular, distributed systems of embedded Things?



https://cdn.wibu.com/fileadmin/images/Heroimages/Level_2/1/Level_1.5-Embedded-Security.png

Development of common software infrastructure

- The Internet of Things needs the development of common frameworks that could provide secure, robust, and usable mechanisms for Thing commissioning, deployment, management, and decommissioning.



http://cpo.noaa.gov/sites/cpo/News/2015/FFO_FY15/6_ESSModels.jpg

Mobility across Environments

- How, then, do we architect network protocols and management systems in support of frequent changes in the set of available Things – while maintaining safe and secure operation of the applications dependent on those Things?

http://www.hindustantimes.com/rf/image_size_640x362/HT/p2/2016/01/30/Pictures/smart-city-shutterstock-image_e206f2c6-c777-11e5-9c36-a121b4394ec6.jpg

Authenticated data sources

- How are data sources authenticated? Once authenticated, how are data sources continually verified as being correct and uncompromised?

http://cdn2.itpro.co.uk/sites/itpro/files/styles/article_main_wide_image/public/images/dir_220/it_photo_110107.jpg?itok=lCJmzYoF

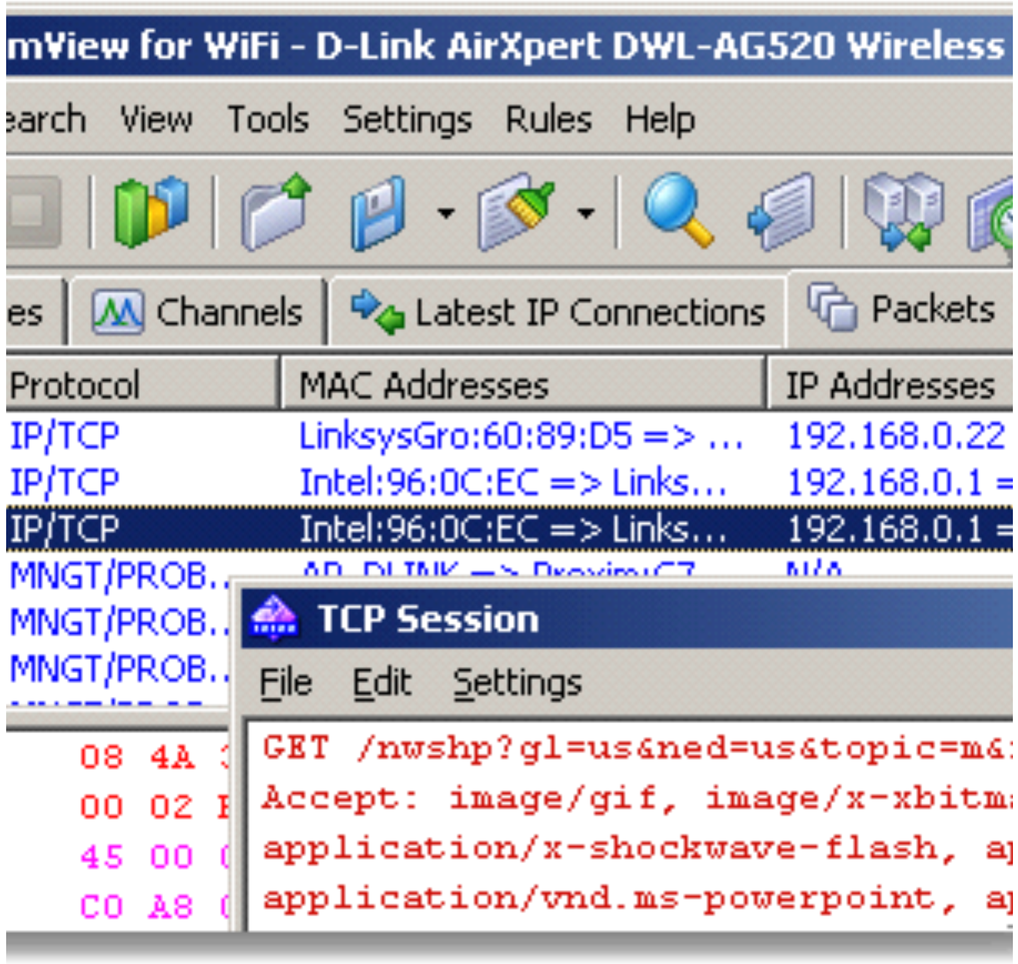
Authenticated humans

- How do Things identify and authenticate their user?
- How do Smart Environments identify and authenticate occupants, without raising privacy risks?
- How do Things verify authorization when sensitive actions are requested?
- How do owners and occupants delegate authority to others who assist in managing Smart Environments – without undue privacy risk?

http://c.asstatic.com/images/1228383_634547670001201250-1.jpg

Discovery and management mechanisms

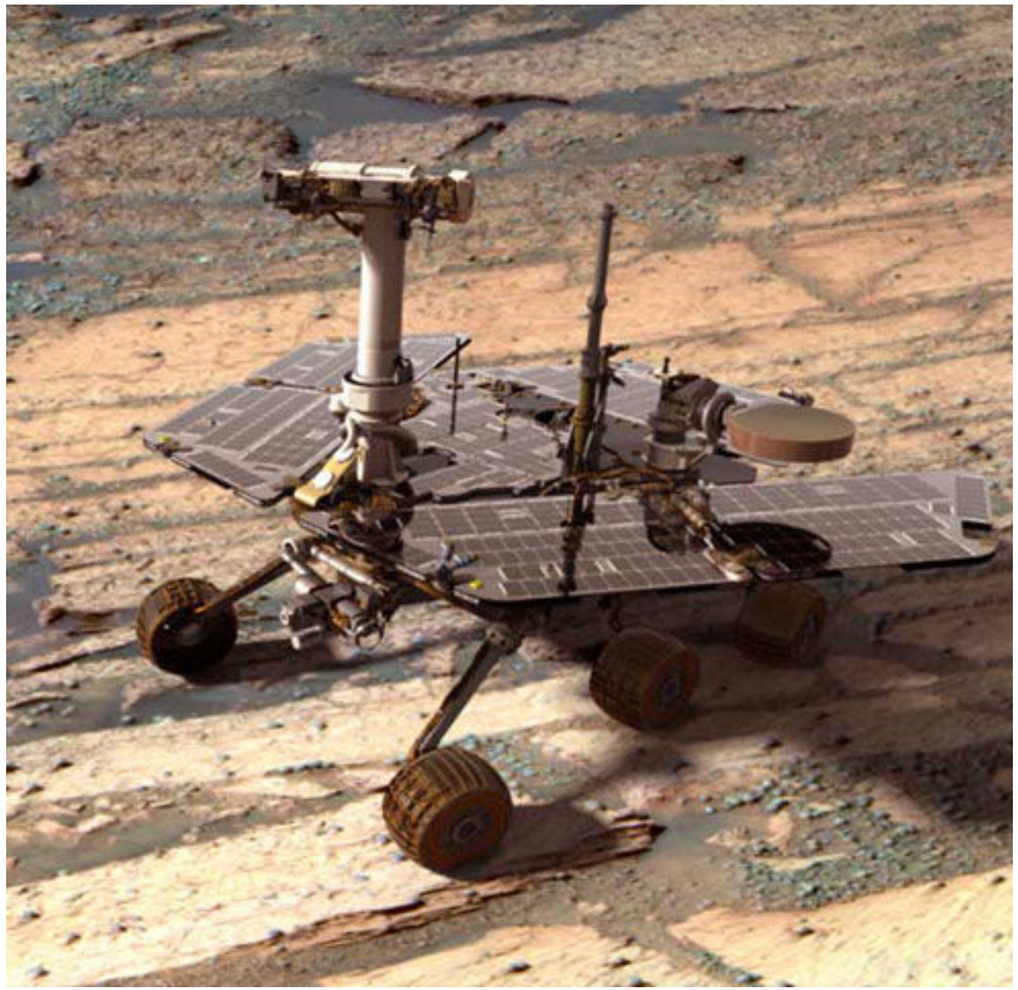
- How is a proper inventory for all Things in a Smart Environment maintained when some of those Things, perhaps malicious devices, choose to hide or falsify their identity?



http://www.tamos.com/i/caclip1.png

Unknown lifetimes

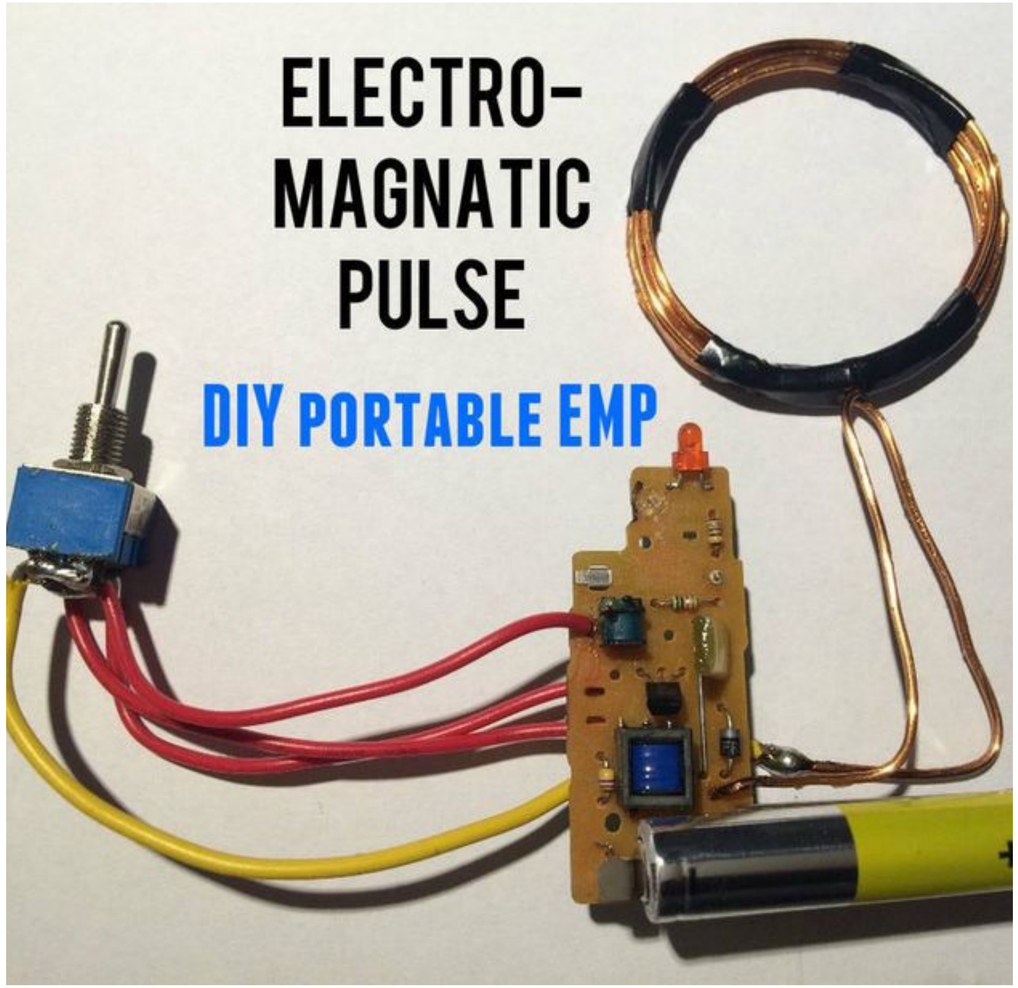
- What mechanism can help manage Things that outlive their intended lifetimes?



http://pop.h-cdn.co/assets/cm/15/05/640x480/54cb12a4eeb9a_-_opportunity-0613-de.jpg

Secure discovery and destruction of Things

- How does an owner discover all Things needing destruction, and verifiably erase all sensitive information from those Things before they are discarded?



https://i.pinimg.com/736x/b6/7b/f7/b67bf70a07b12dadfda075d4ecde7783--electronics-projects-arduino-projects.jpg

Attesting to safety properties

- How can users be assured that their Smart Things and Environments actually provide the safety and security properties they expect?
- What mechanism can Things use to attest their properties, and what interfaces enable normal humans to believe those attestations?

http://www.shreesaidocumentation.com/images/retwolayoutandwaitfortwomoretoday/MARRIAGE%20CERTIFICATE%20%20UAE%20EMBASSY%20ATTESTATION.jpg

FYI...

Dartmouth Computer Science

Recruiting **four** faculty this year

http://communications.dartmouth.edu/sites/communications.dartmouth.edu/files/styles/basic_article_slideshow/public/baker_2014-1212150008.jpg?itok=8nZqEAlR

Conclusion

For more information, see

- David.F.Kotz@Dartmouth.edu
- www.cs.Dartmouth.edu
- thaw.org
- amulet-project.org
- auracle-project.org

This research results from a research program at the Institute for Security, Technology, and Society at Dartmouth College, supported by the National Science Foundation under award number CNS-1329686. The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the sponsors.