WG5
IoT security, privacy, policy

L Jean Camp <ljeanc@gmail.com>
Ivan Evtimov <ie5@cs.washington.edu>
Earlence Fernandes <earlenceferns@gmail.com>
Tadayoshi Kohno <yoshi@cs.washington.edu>
Philip Levis <pal@cs.stanford.edu>
Dan Lieberman <dan@tumbiri.com>
Lynette Millett <LMillett@nas.edu>
Thomas Pfenning <thomaspf@microsoft.com>
Dave Thaler <dthaler@microsoft.com>
Joshua Siegel <siegelj@gmail.com>
Stefan Thom <Stefan.Thom@microsoft.com>
Ron Zahavi <Ron.Zahavi@microsoft.com>

A Security Disaster

The Economist | World politics | Business & finance | Economics | Science & technology | Culture

Cyber-security

The internet of things (to be hacked)

Hooking up gadgets to the web promises huge benefits. But security must not be an afterthought

Jul 12th 2014 | From the print edition

Timekeeper Like 217 Tweet 594

How the Internet of Things Could Kill You

By Fahmida Y. Rashid JULY 18, 2014 7:30 AM - Source: Tom's Guide US | 5 COMMENTS

Hacking the Fridge: Internet of Things Has Security Vulnerabilities

JESS SCANLON | MORE ARTICLES
JUNE 28, 2014

Philips Hue LED smart lights hacked, home blacked out by security researcher

By Sal Cangeloso on August 15, 2013 at 11:45 am | 7 Comments

- HP conducted a security analysis of IoT devices[1]
  - 80% had privacy concerns
  - 80% had poor passwords
  - 70% lacked encryption
  - 60% had vulnerabilities in UI
  - 60% had insecure updates

[1] http://fortifyprotect.com/HP_IoT_Research_Study.pdf

The Internet of Things is something people trust, not fear.

trust, not fear

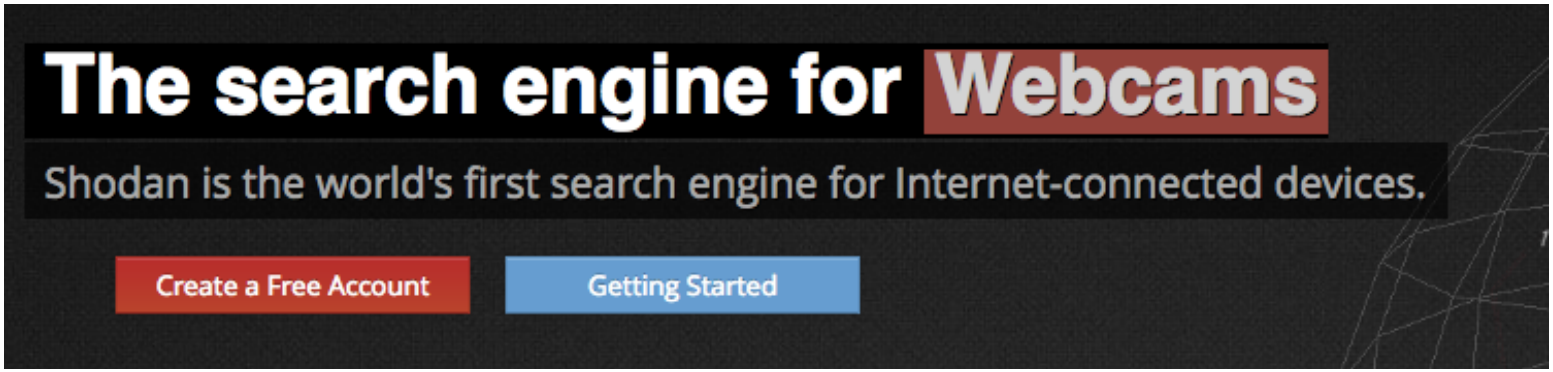
Three technical goals
towards achieving this vision.

1. The Internet of Things is not a significant threat to the broader Internet.

1. The Internet of Things is not a significant threat to the broader Internet.

2. The security of a smart object is greater than or equal to a dumb object.

2. The security of a smart object is greater than or equal to a dumb object.



Hotel ransomed by hackers as guests locked out of rooms

The Local
news.austria@thelocal.com

28 January 2017
10:42 CET+01:00

crime

3. The Internet of Things is not a significant threat to the physical world.

3. The Internet of Things is not a significant threat to the physical world.

German Steel Mill Meltdown: Rising Stakes in the Internet of Things

January 14, 2015 | By Pamela Cobb

Three Goals

- The IoT is not a significant threat to the broader Internet.
  - e.g., Mirai botnet
- The security of a smart object is as good or better than that of a dumb object.
  - E.g., shodan.io, Austrian hotel
- The IoT is not a significant threat to the physical world.
  - E.g., German steel mill, Jeep Cherokee, Austrian hotel

Projects towards vision

1. IoT security adopts the best practices in web and payment system security.
   - Low hanging fruit — new tools, frameworks, systems; successes from web security are valuable.

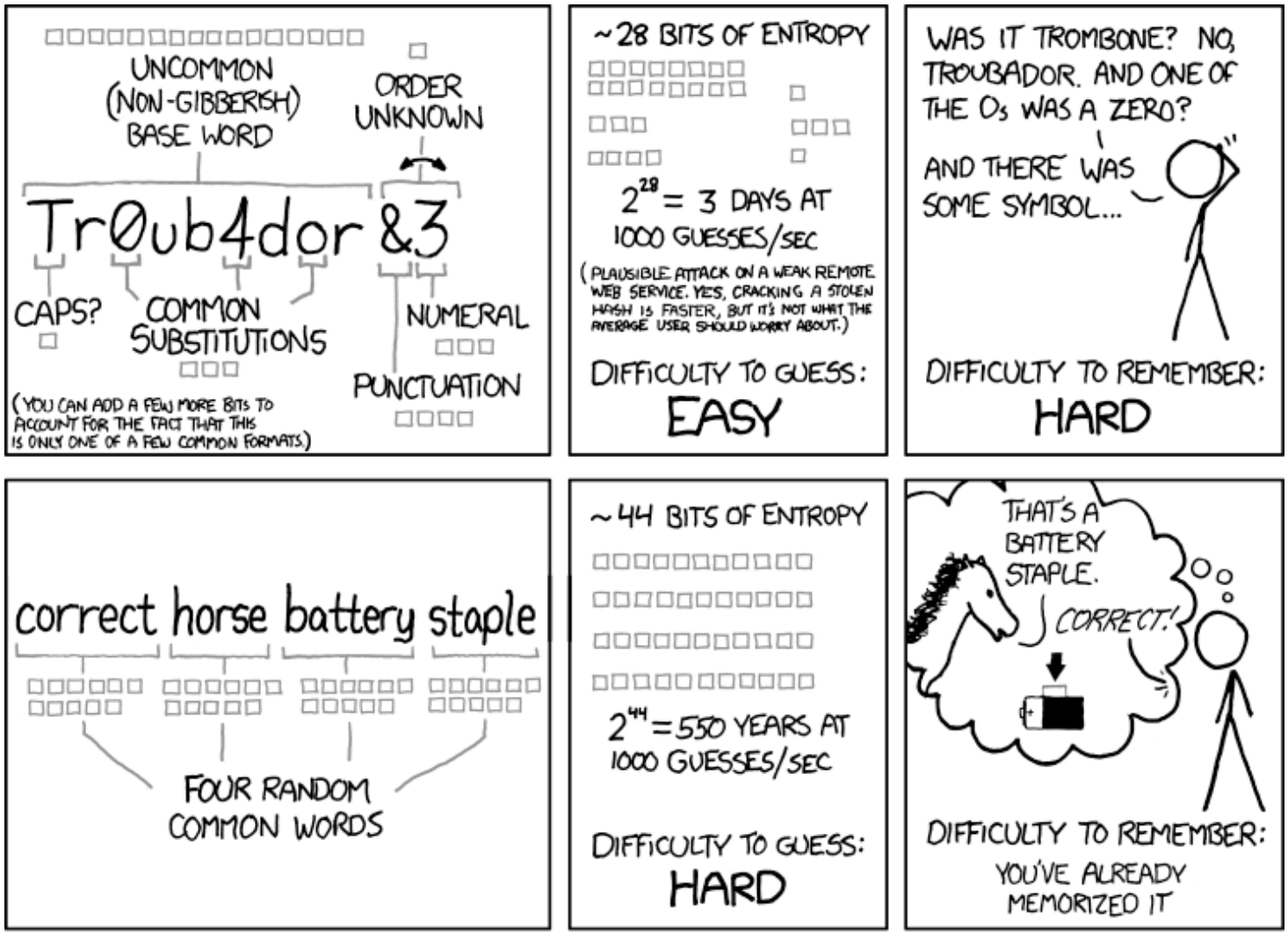
2. Communication transparency: owner can observe, filter, suppress their own IoT network traffic.
   - Visibility and control allow management and countermeasures.

Projects towards vision

3. Sound user authentication methods that embrace human factors.
   - Password policies today are a failure: security is less secure.

4. Master Chief: digital assistant for managing and monitoring security of your network.
   - Automate, provide a basis for trust, human-centric interactions and cognitive models.

Questions/Comments



THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

North stars (time machines?)

- A world without passwords: security policies are understandable by humans
- A world without botnets
- Owners of data have full control over it

What was discussed

- Hygiene: passwords, password policies, etc.
- in some point in the future, no botnets (systems security)
- transparency: owner can observe monitor and manage all data that a device collects (added: in an understandable way) (added: depending on the context)
- if cloud service is compromised, it doesn't compromise your data (homomorphic encryption under current model? but no need to constrain to current capability) [data in the cloud is somehow secure when the cloud is hacked]
- models for securing IoT - crypto and security primitives that are not only effective but are also understandable by humans [Security mechanisms that make intuitive effective interactions that allow users to understand threats]
- failsafe modes that protect life, notion of privacy. Notion of failing safely as the device is built.
- proof of non-repudiability [e.g.,: how do we design forensics in a world where people share passwords?]

State of Art

- Bad states of the art:
  - Passwords, including lots of default passwords
  - Shared credentials, reuse of credentials
  - Botnets
- Good states of the art:
  - Spreading computation across multiple servers to have to compromise all to compromise a system
  - Non-password-based pairing protocols
  - See presentations from earlier this week
    - Secure boot, language/OS protections, Trusted Execution Environments, etc.