Secure, zero-touch Bootstrap for the Internet of Things

(IETF ANIMA BRSKI)

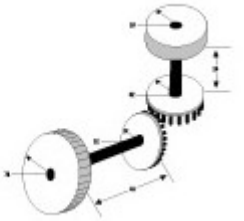
Michael Richardson
Sandelman Software Works

Who am I?

Xelerance Corp 2003-2007,2014-

Internet technologist, doing IP since 1988. “Garage Entrepreneur”

SANDELMAN SOFTWARE WORKS



1996-

SOLIDUM

(1998-2001)

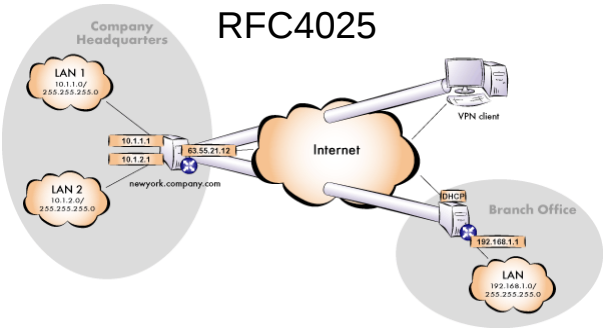
FreeS/WAN (2001-2004)

Linux FreeS/WAN

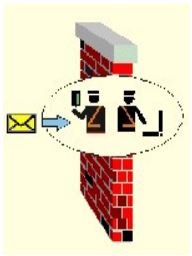
SIMtone CORPORATION

CENTRE DE RECHERCHE ET DÉVELOPPEMENT EXPÉRIMENTAL EN INFORMATIQUE LIBRE
CREDIL
CENTRE FOR RESEARCH AND EXPERIMENTAL DEVELOPMENT IN INFORMATICS LIBRE

RFC4322
RFC4025



#4 at Milkyway Networks (1994)



ROLL – RFC6550
2012-

6TiSCH

IETF standard security:IPsec/VPN

Outline of talk:

- What kind of IoT am I talking about?
- The challenge of network enrollment
- What is ANIMA, what's BRSKI, and BRSKI for IoT
- Questions and Conclusions

What is IoT?

- Internet
- Of
- Things

- Which things?

  Coke Machines?

  - https://www.cs.cmu.edu/~coke/

"The way that machines communicate with each other in order to improve automation and efficiency in daily tasks" (Kevin Aston 1999)

Connected Things

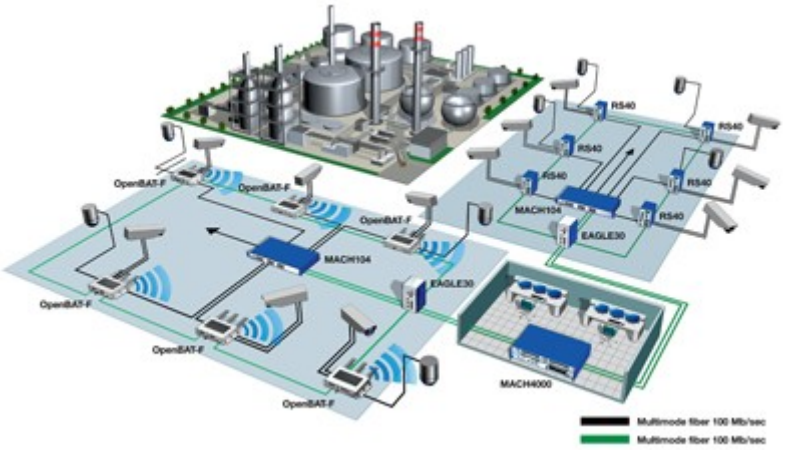
Web Connected Things

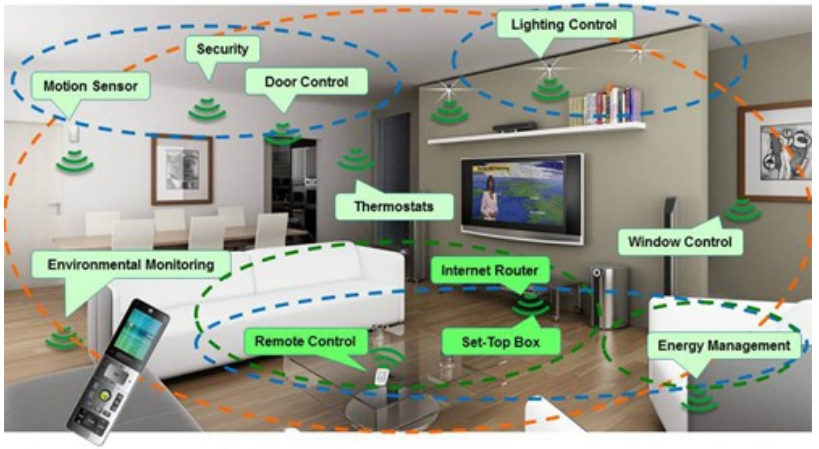
Data:

(coming soon) Powered by [e] enphase ENERGY

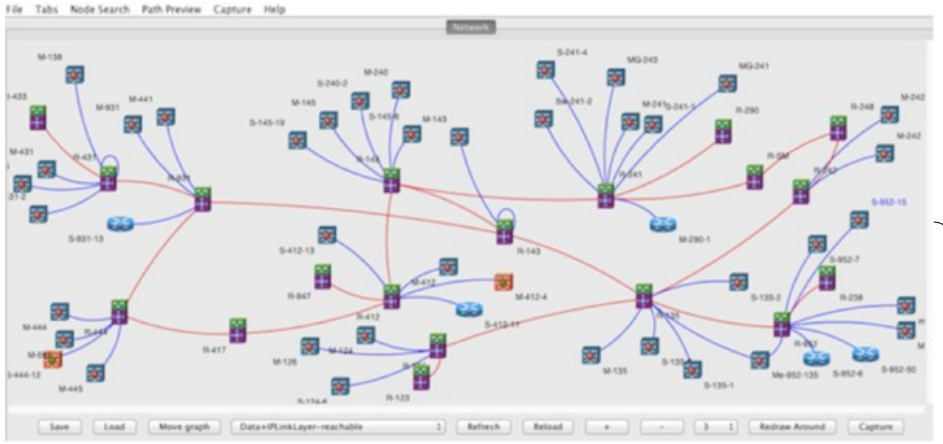
- Enphase - Public Installs map
- Enlighten Reference Installations
- Enphase Downloads
- Enphase API Licence
- Enphase Register for the Beta Program

Internet of Things





Autonomic Networking Integrated Model and Approach (anima)



1) Drop-ship new system
2) BRSKI connects new device to existing network
3) Configure system

Why do this? Profit!

- System unpacked and installed by remote hands
- Senior people do not waste time and expense travelling just to setup systems

- Consistent and repeatable, automated installations
- Out-of-band access replaced with secure, always up in-band VPN overlay (ACP)

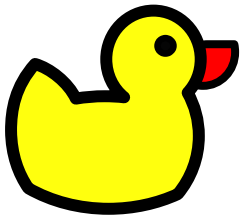
Legacy out-of-band access used to mean copper phone lines. The PSTN is gone, and what if you are the phone company?

Enterprise/ISP to IoT

Remote Hands
Become Home
Users

Some BRSKI terminology and icons!

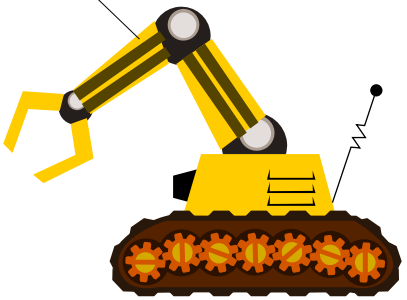
- Pledge



Stajano, F. and Ross Anderson,
"The resurrecting duckling: security issues for ad-hoc wireless networks", 1999,
https://www.cl.cam.ac.uk/~fms27/papers/1999-StajanoAnd-duckling.pdf
Wikipedia, "Wikipedia article: Imprinting", July 2015,
https://en.wikipedia.org/wiki/Imprinting_(psychology)
https://en.wikipedia.org/wiki/Animal_House

20yr Old Ross Anderson paper

- Manufacturer Authorized Signing Authority -> MASA.

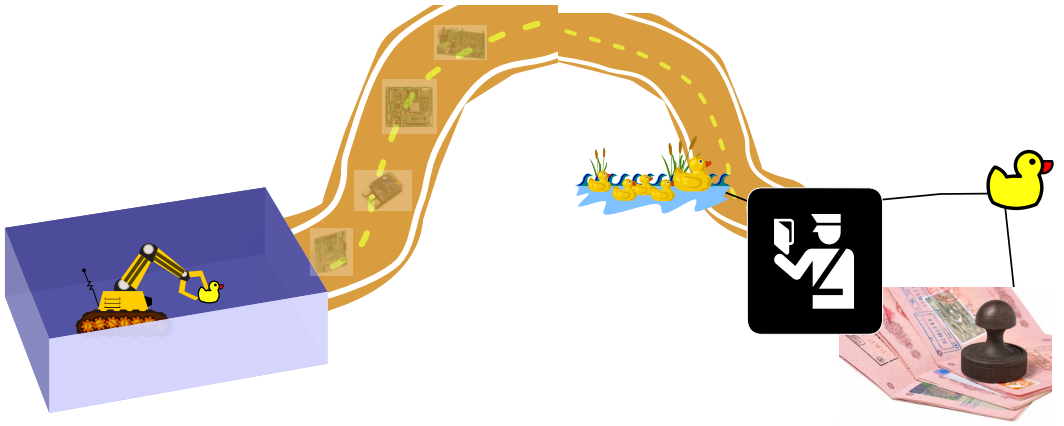


- Join Registrar/Coordinator
  - JRC
  - “Registrar”

- VOUCHER
  - RFC8366

A Day in The Life of the Pledge

- Device is provisioned with 802.1AR IDevID
  - Private key unique!
- MASA anchor installed
- When deployed, Pledge authenticates with IDevID
- Network authenticated itself with Voucher
- Pledge receives Domain-Specific LDevID via Enrollment over Secure Transport



Network Flow Two

MASA

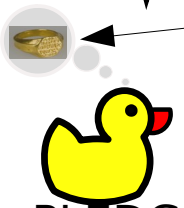
Registrar

New
Domain
Owner

A: this
is your
parent!

Q:
Is this
my new
mommy?

RFC8366



PLEDGE

A live voucher

JSON Format Of YANG Defined voucher


```
{"ietf-voucher:voucher":
    {
      "assertion":"logged",
      "created-on":"2017-10-12T13:54:31.439-
04:00",
      "serial-number":"00-D0-E5-F2-00-02",
      "nonce":"Dss99sBr3pNMOACe-LYY7w",
      "pinned-domain-cert":"MIIBr...Yrc3o="
    }
}
```


With CMS signature (signed by MASA) around it!

BRSKI status

- IETF document in final cross-area reviews
  - 43 issues, half minor,
  - Some out of scope for ANIMA
- Part of IETF 6TiSCH Zero-touch enrollment for Deterministic Industrial 802.15.4
- Fairhair Alliance (building automation) interop in Dublin Nov 27/28.
  - 3 device makers, 2 chip vendors
  - Integration by Thread n+1

Includes testing of Open source Reference code

New work

- BRSKI over EAP-TLS for WiFi enrollment
- MASA-less ideas
- Use in IETF DOTS WG being discussed

PUF?

Some costs of security

Essentially A part of Sales Channel (licensing!)

- Must individualize devices with IDevID.
  - (part of JTAG testing)
  - (outsource to TPM)
- Crypto operations in device
  - Moderate, need privacy in device anyway.
  - Secure Update for IoT (SUIT) needs it too!

Some new Complexity In devices

- Must operate MASA
  - Specifically designed to be outsourced.
  - Can control resell.
- Owner must operate Registar!
  - Core part of ANIMA NOC.
  - Not a problem for Industrial IoT
  - New issue for Home Owner. Plenty of home automation systems could take it up

SecureHome Gateway.ca Project!

PUF => https://en.wikipedia.org/wiki/Physical_unclonable_function

Summary and Questions

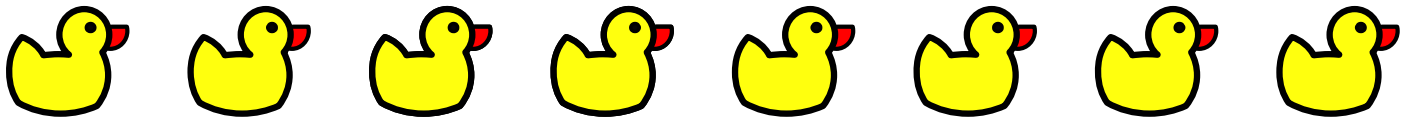
1) More links to talks at:

   http://www.sandelman.ca/SSW/ietf/brski-links/

2) draft-ietf-anima-bootstrapping-keyinfra

3) Reference code:

   https://minerva.sandelman.ca



Abstract:

This talk is about an IETF standard secure bootstraping system (BRSKI) developed in the ANIMA and 6TISCH Working Groups. The assumptions behind BRSKI are explained, along with an explanation of the moving parts required to build a successful system. The system described deals the questions:

- Who is this device?
- What is its identity?
- Is it mine?
- Do I want it?
- What are the chances it has been compromised?
- And for the device: Should I join this network?

The first document is RFC8366, with additional documents being published in late-2018.

Photo and Image Credits

- https://commons.wikimedia.org/wiki/File:Penrose_triangle.svg
- http://blog.stephenwolfram.com/2016/09/how-to-teach-computational-thinking/
- https://www.learntek.org/blog/common-problems-faced-business-analysts/
- https://productcoalition.com/oh-you-are-a-product-manager-what-things-should-i-do-to-improve-my-product-53f28add82b8
- http://dilbert.wikia.com/wiki/Pointy-Haired_Boss
- https://en.wikipedia.org/wiki/Necker_cube
- https://www.news18.com/news/buzz/elon-musk-tweets-that-twitter-locked-his-account-after-suspecting-hack-1917565.html
- https://www.50-best.com/funny_cat_pictures/pics/sideways_head.htm
- https://www.applefritter.com/node/21333
- https://hockeytrain.com/shop/accessories/edge-protect-post-protector/
- https://collectpeanuts.com/toys/games-puzzles/puzzles/milton-bradley/
- https://www.engineersrule.com/how-a-coke-machine-and-the-industrial-internet-of-things-can-give-birth-to-a-planetary-computer/
- https://www.ge.com/digital/blog/when-assets-need-optimized-proactive-maintenance
- http://www.salut.ru/ViewTopic.php?Id=647
- http://electricgeneratorhigataki.blogspot.com/2017/02/gas-turbine-electric-generator.html
- https://www.powerzone.com/resources/glossary/steampoweredgenerators
- http://www.libelium.com/smart_city_environmental_parameters_public_transportation_waspmote/
- https://www.meddeviceonline.com/doc/medtronic-launches-world-s-first-app-based-remote-monitoring-system-for-pacemakers-0001
- https://www.drewpritchard.co.uk/products/indian-marriage-elephant
- https://mydeejay.com/advice/wedding-planning-timeline-when-to-book-wedding-vendors-wedding-vendor-checklist/
- https://www.express.co.uk/travel/articles/764690/hotel-room-thermostat-secret

More Credits

- https://www.gentlemansgazette.com/signet-ring-primer/
- http://blog.tmcnet.com/blog/rich-tehrani/uploads/d-link-dgs-8000-right.jpg
- https://i.ytimg.com/vi/2zp7Nt7ZQOU/maxresdefault.jpg
- https://img.memecdn.com/grandma-won-a-iphone_o_1874239.jpg
- https://i.kinja-img.com/gawker-media/image/upload/s--qAHc1cG8--/c_fill,fl_progressive,g_center,h_900,q_80,w_1600/1933etzkox2zjgif.jpg
-