RSAConference2018
San Francisco | April 16 – 20 | Moscone Center

NOW MATTERS

SESSION ID: TV-R05

IOT ARCHAEOLOGY: DIG SECURITY LESSONS

Chad Childers

Vehicle & Mobility Cyber Security
Ford Motor Company

History

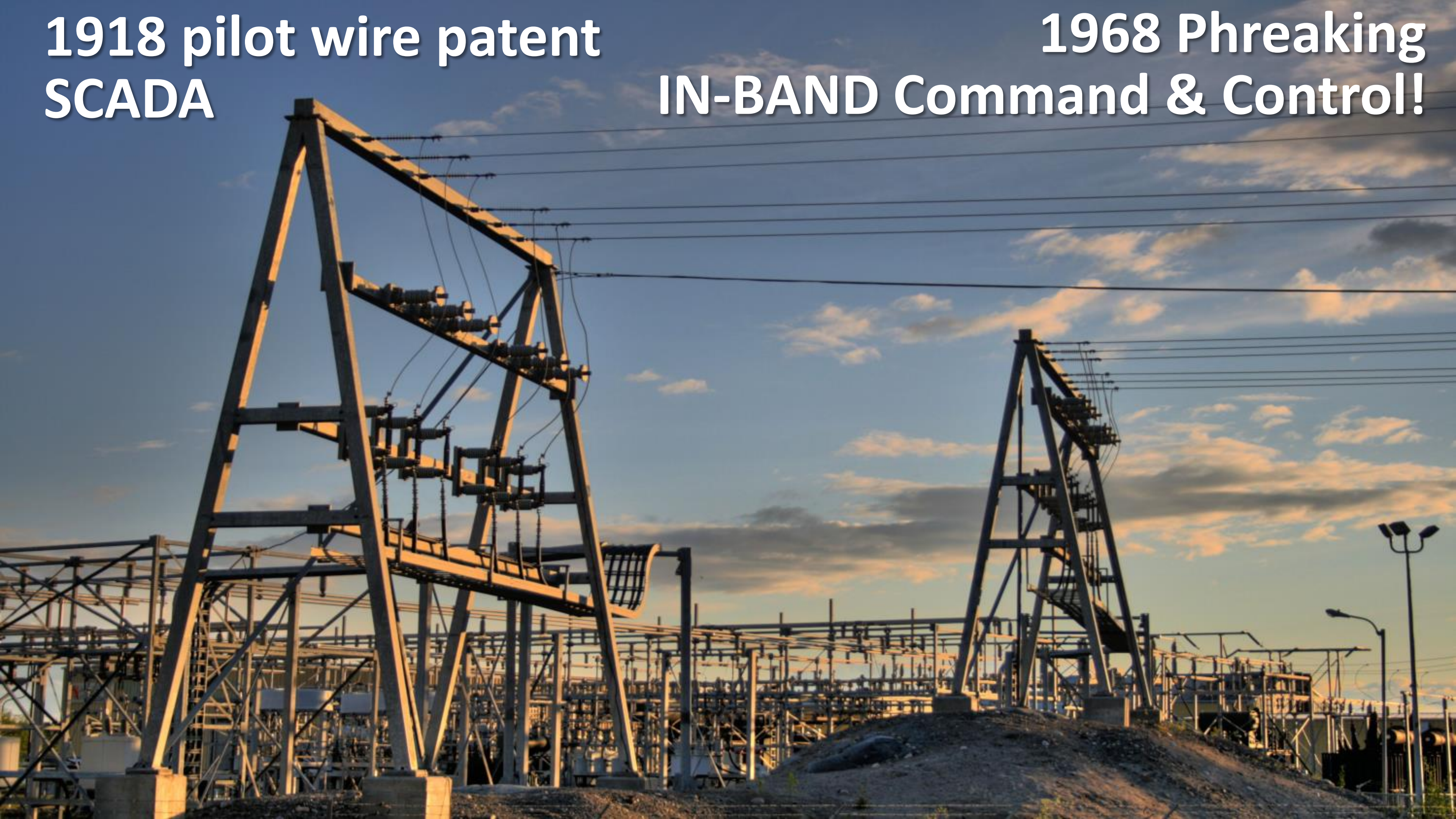
- The first connected device turns 100 years old this year
- More connected devices than people for the first time
- Those who cannot remember the past are condemned to repeat it. - George Santayana

1204 - Siege of Chateau Galliard

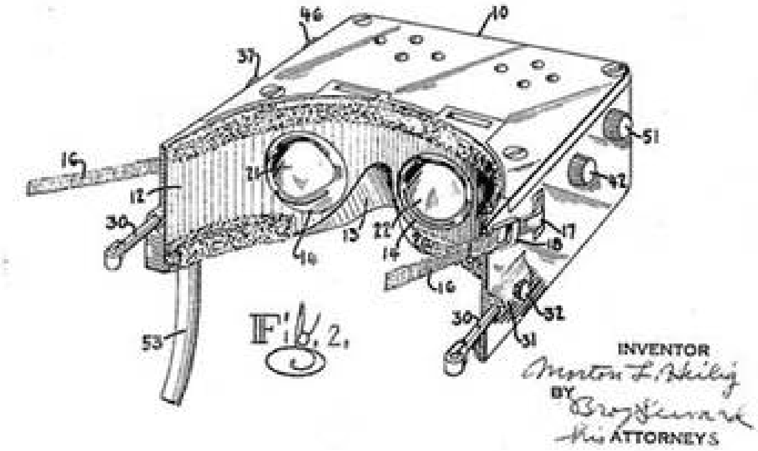
unguarded toilet chute
OUTBOUND ONLY!

1918 pilot wire patent
SCADA

1968 Phreaking
IN-BAND Command & Control!



Wearables

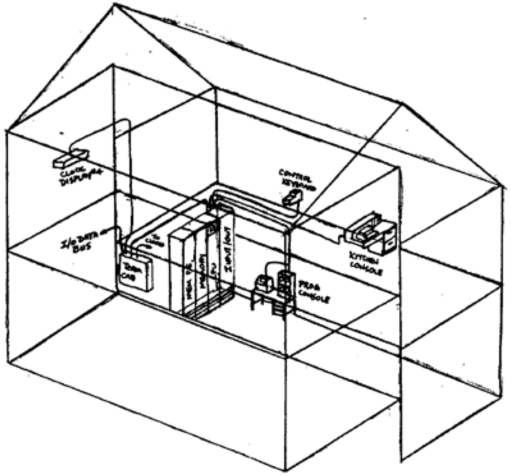


1957 HMD

1960 pacemaker
2007 fitbit

PRIVACY

1966 Home Automation



ECHO- IV SYSTEM DIAGRAM

CYBERTUB

Ypsilanti computer geek goes for a float on the Internet

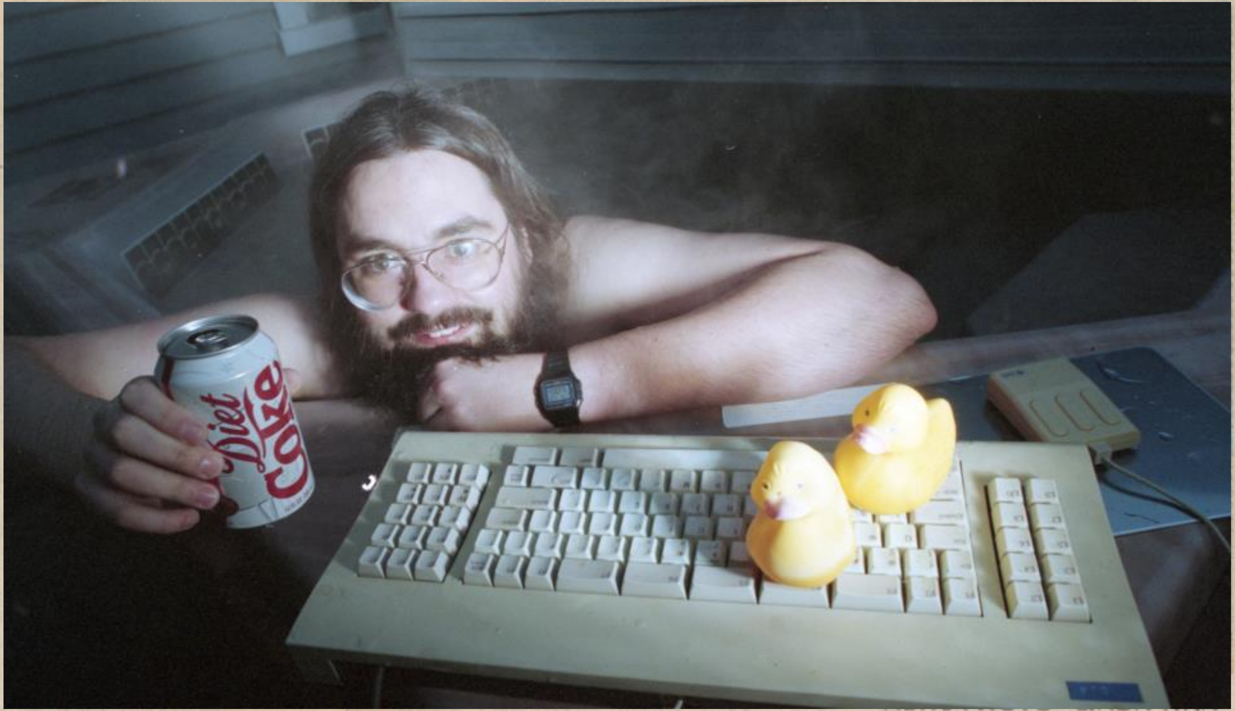
■ Users check out refrigerator, sample hot tub.

By JO COLLINS MATHIS
NEWS STAFF REPORTER

We know, we know. You don't spend a lot of time wondering about the temperature of Paul Haas' hot tub or the Diet Coke in his refrigerator.

But if you did, and if you were connected to Internet – the worldwide computer network – you could punch in a few keys and have the facts on your screen. It would read something like this:

Tub Status as of Wed Jan 18 14:29 EST 1995

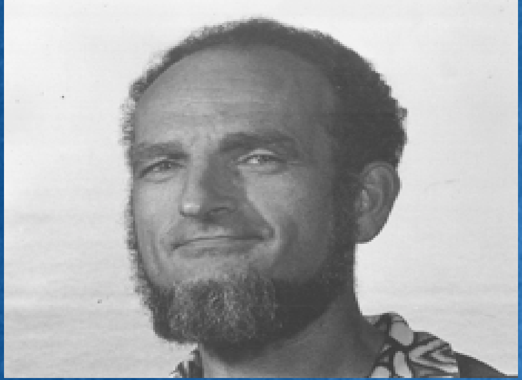


Self-described 'computer geek' Paul Haas of Ypsilanti.

Vending machines

Stanford
ARTIFICIAL
INTELLIGENCE

- 1974 SAIL Prancing Pony food & drink
  - charge accounts, email bills
  - double or nothing betting



Mobility

1976 SRI Packet Radio Van

1980 RFID key card parking

1994 GPS

REPLAY

CLASS-BREAK

PRIVACY

7 Common Attack Themes

OUTBOUND ONLY

Toilet chute and Mirai webcam botnet. Devices should not accept inbound traffic or peer to peer. Effective controls can be implemented at carrier or network layer. Use Shodan.

IN-BAND COMMAND & CONTROL

Phreaks. IoT has untrusted paths, don’t assume they are secure.

Don’t assume complexity/expense will last.

Sign updates, encrypt sensitive data.

REPLAY

RFID – MITM attacks are easy over WiFi, Bluetooth

7 Common Attack Themes

UNINTENDED

Morris worm and SQL Slammer – first incident is often on commodity technology, not targeted. Shodan search before you choose. Don't assume that suppliers secure it or it is fit for your purpose, do your own threat model.

UNTRUSTED SUPPLIER

Attacks on Bluetooth stack, chipset, SSL library, cloud, any common component that is used across a variety of devices can result in intentional or unintentional breach. Vulnerability management and updates.

7 Common Attack Themes

PRIVACY

Consider privacy issues early, do a threat model. Turn off features that are not needed, don't collect data that there isn't a business requirement for. Encrypt. Obfuscate or hash IDs, don't use name or other obvious key.

CLASS BREAK

Attackers with physical access to a device will find a way to elevate privilege. Crucial to assure that compromise of one device cannot be parlayed into compromise of a whole class or generation of devices. Require unique keys.

Get the basics right

- PRIVACY - Never collect or share more data than needed
- IoT is IN-BAND, UNTRUSTED, and vulnerable to REPLAY
  - Sign OTA updates
  - Encrypt
  - Use 2 factor authentication
  - Never assume commodity technology or cloud is secure
- CLASS BREAK
  - Use unique keys and credentials
- Threat model and plan an agile defense
- Remember anything is possible

I’ve got news for Mr. Santayana:
we’re doomed to repeat the past no matter what.
That’s what it is to be alive.
- Kurt Vonnegut

Apply what you have learned

- Right now
  - Identify and secure devices that accept inbound traffic
- Within three months
  - Start threat modeling to identify risks and mitigations
  - Identify agile security incident response plans
- The brass ring
  - Design systems for the greater good - security, safety, and empowerment