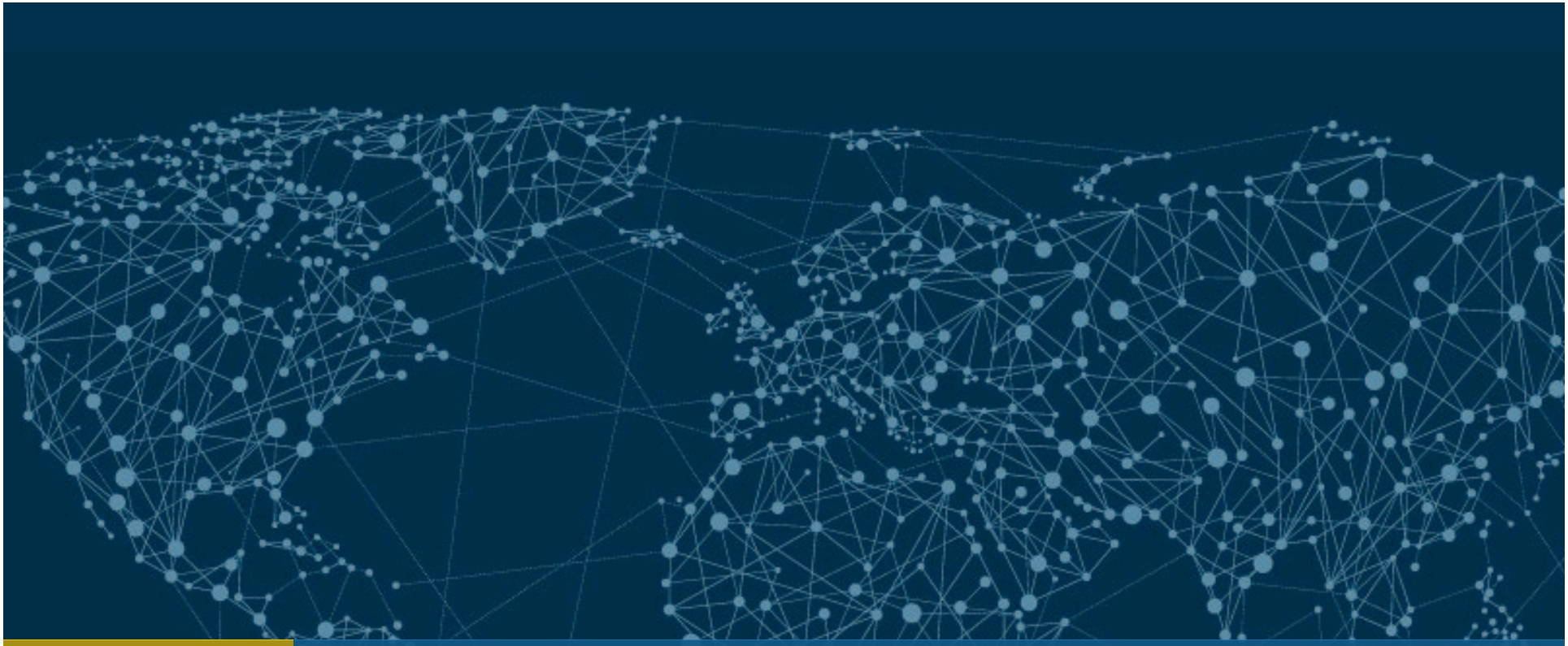


Security, Internet of Things, DNS and ICANN

ICANN Security Team |Kiev | November 29-30 2016

Agenda

What is the Internet of Things?

IOT device characteristics and challenges

Threat landscape

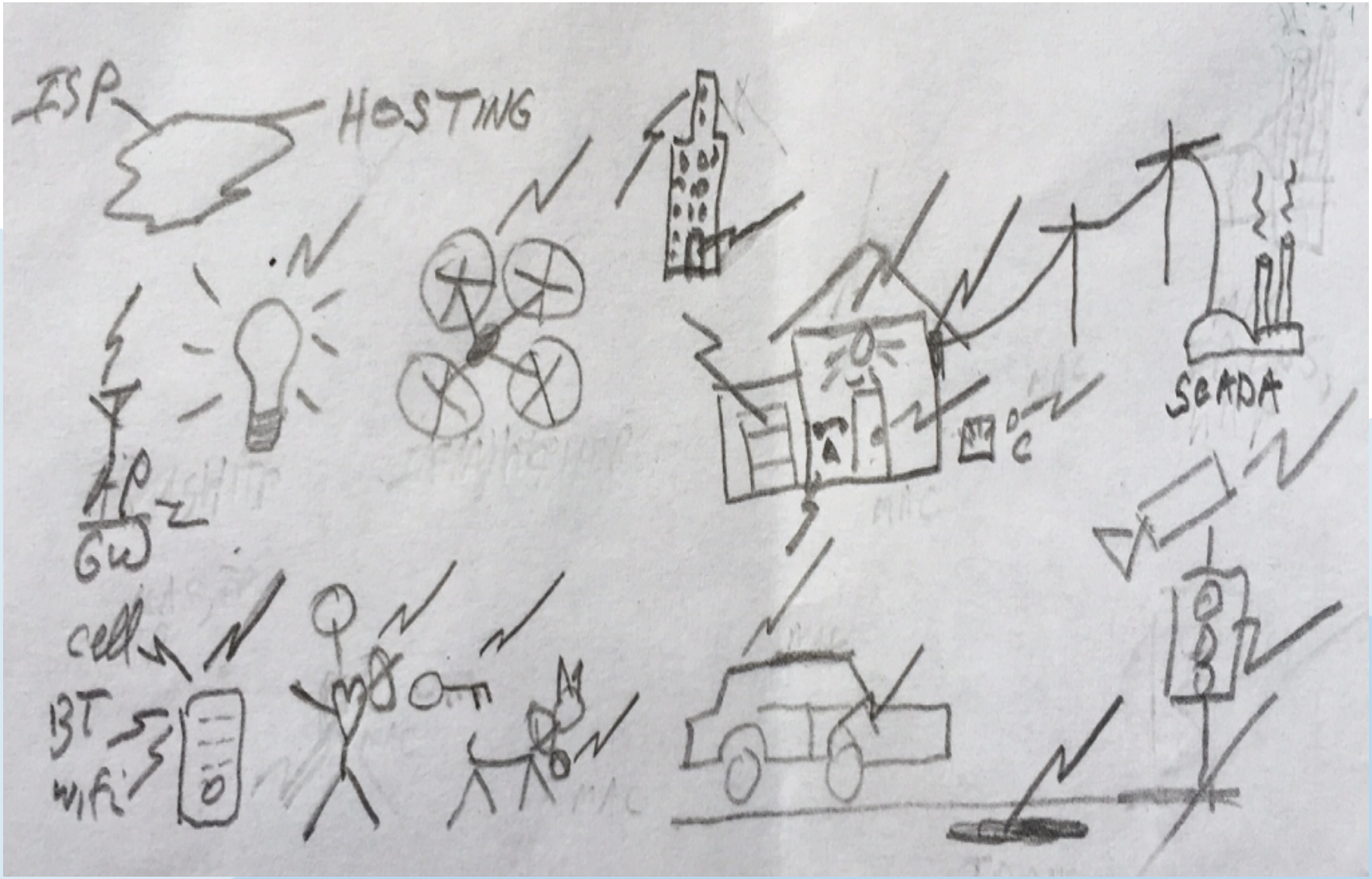
Is the past a prelude to the future?

What is the Internet of Things?

IoT (Internet of Things) is about connecting the next wave of devices to the Internet.

- A universe of devices that may be present in
  all aspects of lifestyle, health, or society
- These devices are locally and globally connected via Internet services

IoT on a Bar Napkin



Characteristics of IoT Devices

Very large to unimaginable number of devices

- "Things" encompasses virtually any thing that might be automated or expected to collect or report information

Devices are small or embedded in things or beings

- Initial wave have limited processor, memory, or power constraints

Machine to machine communication is typically more common than human to machine communication

Like all preceding waves, security and privacy are at odds with the desired pace to commoditize

Machine to Machine communications: The loss of the “human factor”

IOT will change communication patterns:

- Not limited to “eye-ball” bandwidth

➔ Potentially infinite aggregated bandwidth

- Not limited to human work/home/sleep patterns

➔ Changes to daily/weekly traffic patterns

Retail cost is a key driver

Impacts?

- Will we see new “streamlined” protocols?
- Custom operating systems?

We have been here before

- Remember WAP versus HTML markup in early mobile devices?

Race conditions:

- Pace of development or adoption of new protocols versus pace of device hardware improvements

Threat landscape

Devices may increasingly control traditionally human-directed activities at much larger scales than ever before

- Autonomous vehicles
- Aviation
- Package or other forms of delivery
- Residential or business environmental control systems

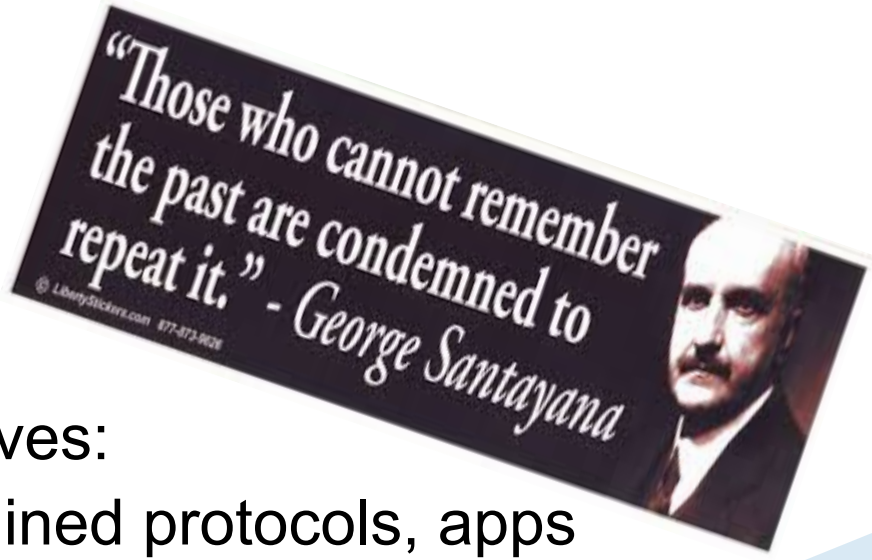
Devices may increasingly become “part of us”

- They may assist with human bio-functions
- They may store significant or critical health data

There may be no human to detect or respond to malfunction

- Things could break and go undetected until a security event

Past is Prelude…



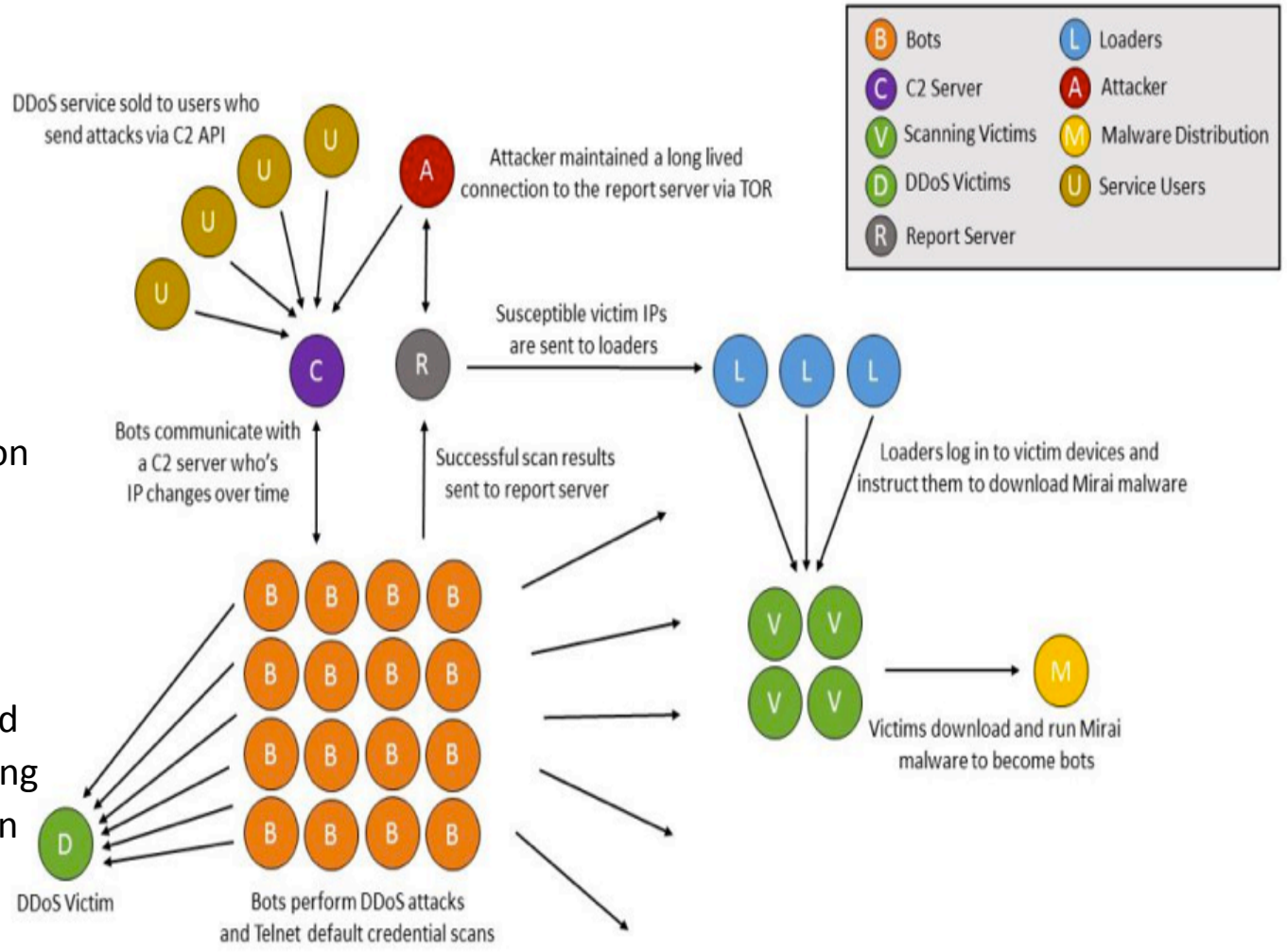
History shows that we introduce new attack vectors with new waves:

- New/custom OSs, streamlined protocols, apps
- Modifications to streamline general purpose operating systems
  - New generation of developers that are unfamiliar with historical vulnerabilities
- Inherited problems of lax configuration defaults

Some threats have been realized…

"Vulnerable IoT devices are subsumed into the Mirai botnet by continuous, automated scanning for and exploitation of well-known, hardcoded administrative credentials present in the relevant IoT devices. These vulnerable embedded systems are typically listening for inbound telnet access on TCP/23 and TCP/2323."

Roland Dobbins, Arbor Networks



http://blog.level3.com/security/grinch-stole-iot/
https://www.arbornetworks.com/blog/asert/mirai-iot-botnet-description-ddos-attack-mitigation/

What warning bells does Mirai ring for us all

Mirai encapsulates many IoT security issues

- A botnet is largely comprised of IoT devices
- The compromised devices use plain text channels that have long been regarded as unsecured and removed from use in current wave of products
- The default credentials for these services are known and shared
- The devices can be re-purposed for many kinds of attacks
- An IoT-populated botnet takes DDOS as a service to another level

Building IoT devices

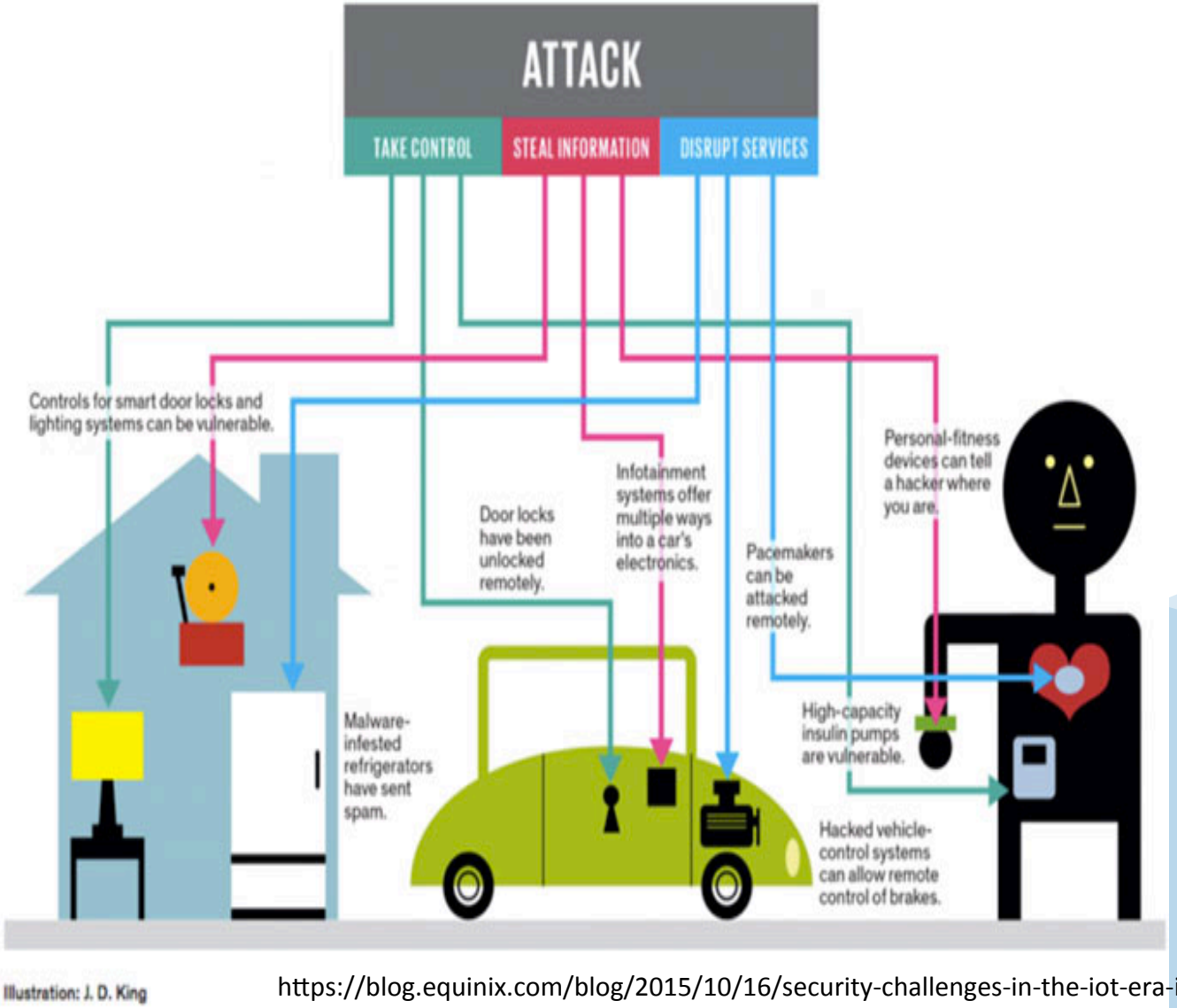
Re-purpose general purpose OSs or build a custom OS from scratch?

- Can you effectively and correctly prune services or binaries that attackers can exploit?

Or

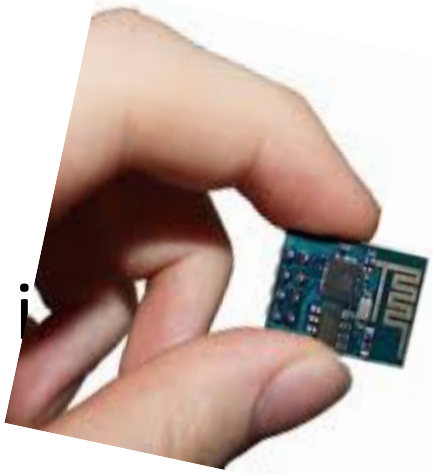
- Can you securely code a custom OS and improve the security baseline for IoT devices

Historically, lowest cost solution wins… and security?



https://blog.equinix.com/blog/2015/10/16/security-challenges-in-the-iot-era-internet-things-coming-together/

Building IoT devices



Build or re-purpose hardware?

- Use chips tailored to be just what i needed

Or use

- Mass-produced, high-capacity chipsets (that provide more capable attack delivery systems)

Once you build them…

How do you continue to secure them?

- History shows that commodity devices
  - Are not routinely upgraded or patched
  - Are not always managed according to best practices

Commodity devices also are saddled with the “shelf life” problem

- Units may occupy shelves in stores for months or years
- Multiple versions of firmware or software may be in the field
- Vendors may not offer consumer managable upgrade methods

Mirai suggests that IoT devices will follow same path

Retail cost objectives conflict with security objectives

Secure or confidential communication protocols may be incompatible with memory or CPU footprint. This affects

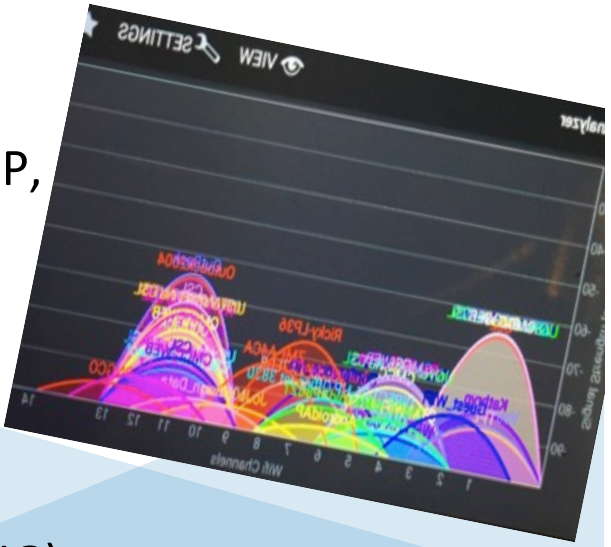
- Cost of device
- Development cost
- Desired time to market window of manufacturers

Persistently strong incentives to collect metadata or personal identifying information

- Cost of implementing authorization (e.g., data permissions)
- Incentives to provide data to third parties for fee
- *Is anyone considering data protection on devices?*

IoT by the numbers, identifiers, protocols

- Spectrum ..13.56MHz, 900MHz, 2.4/5GHz, 24GHz… (GOVTs/ITU)
- Modulation, Media Access Control, e.g. bluetooth, wifi, zigbee,.. (IG/ IEEE)
- MAC addresses, e.g., 00:20:68:12:BE:EF/ISDYNE (IEEE)
- Other numbers: ports: 80/HTTP, 443/HTTPS, 161/SNMP, OID/PEN: 1.3.6.1.4.1.2011/Huawei (IETF/ICANN)
- IPv4, IPv6: 199.7.83.42, 2001:500:9f::42 (RIR/ICANN)
- ASN: AS2706/Wharf TT… (RIR/ICANN)
- Domain Names: www.co.tt … (ICANN)
- HTTP, SMTP, SIP, XMPP, RTP, app specific… (IETF/ITU/IG)
- Security: SSL/TLS, RSA, ECC, AES, … (Academia/IG/IETF/GOVTs)



Very large quantity of devices
Next orders of magnitude

Tens of billions of smart devices by 2020

- Gartner, McKinsey, Cisco, Ericsson

Even if each sends small amounts of traffic...

Addressing considerations:

- NAT still? Forcing function to IPv6?
  - Most device communications are local to a home LAN
  - Traffic to the outside goes through a controler
  - Still, very different scale of NAT
- What about naming devices? Other identifiers?

DNSSEC and IoT

Security is a well known missing piece for IoT

Many IoT applications have physical world safety implications

- human harm, disruption of critical infrastructure service delivery

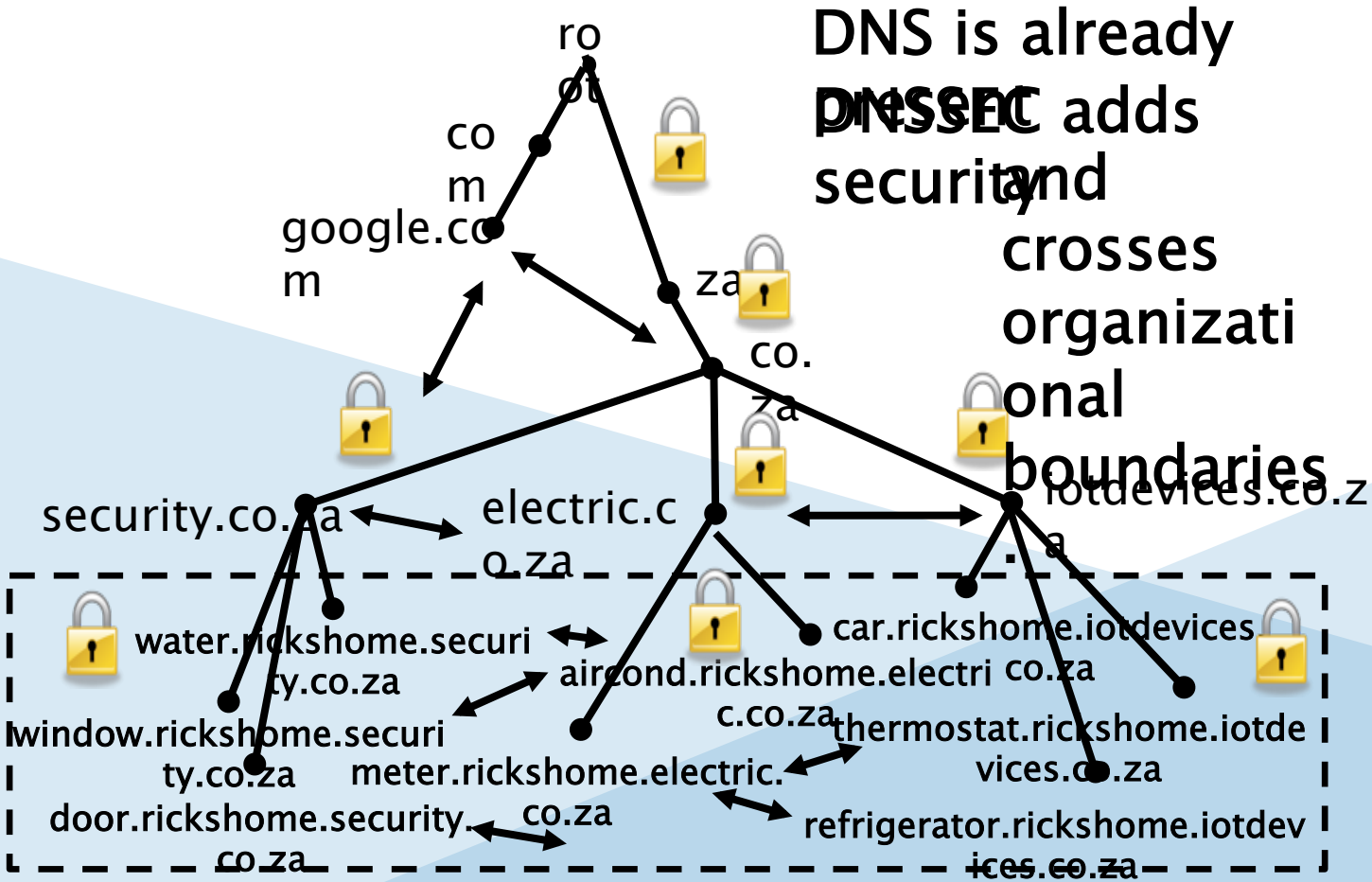
Can we use an existing infrastructure to enable a secure, global, cross-organizational, trans-national communication channel between devices?

- Specifically, can we use DNSSEC for key distribution necessary to secure channels and then securely bootstrap application specific security mechanisms?

Can DNS with DNSSEC solve this problem?

- For example, can we use DANE to publish public keys in the DNS, so that end user can validate keys using DNSSEC?

Can DNS provide a foundation for scalable security



Animated slide

Summary

The Internet of Things holds great promise

If we allow history to repeat,

➔ it can also pose a great threat

~~Is~~ Must the past (be) a prelude to the future?

➔ if not, who can influence the market and how?

Questions?

- Contacts:
  email: dave.piscitello@icann.org
  twitter: @securityskeptic
- web: securityskeptic.com
- company: icann.org
- ICANN Security Team:
  icann.org/resources/pages/security-2012-02-25-en