

RSA® Conference 2015

Abu Dhabi | 4–5 November | Emirates Palace

SESSION ID: SSC-W09

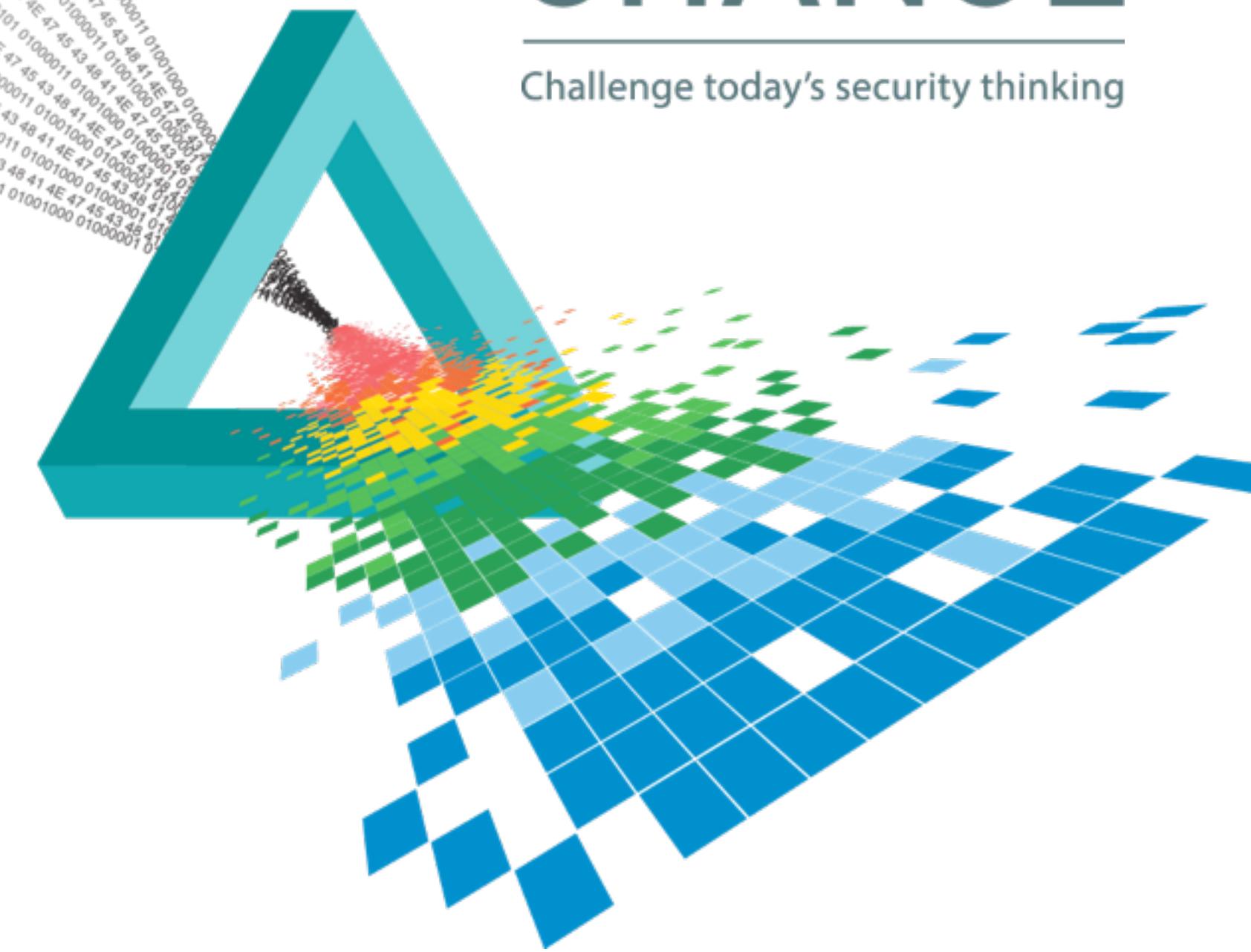
IoT: Securing the Smart City

Dave Lewis

Global Security Advocate
Akamai Technologies
@Gattaca

CHANGE

Challenge today's security thinking

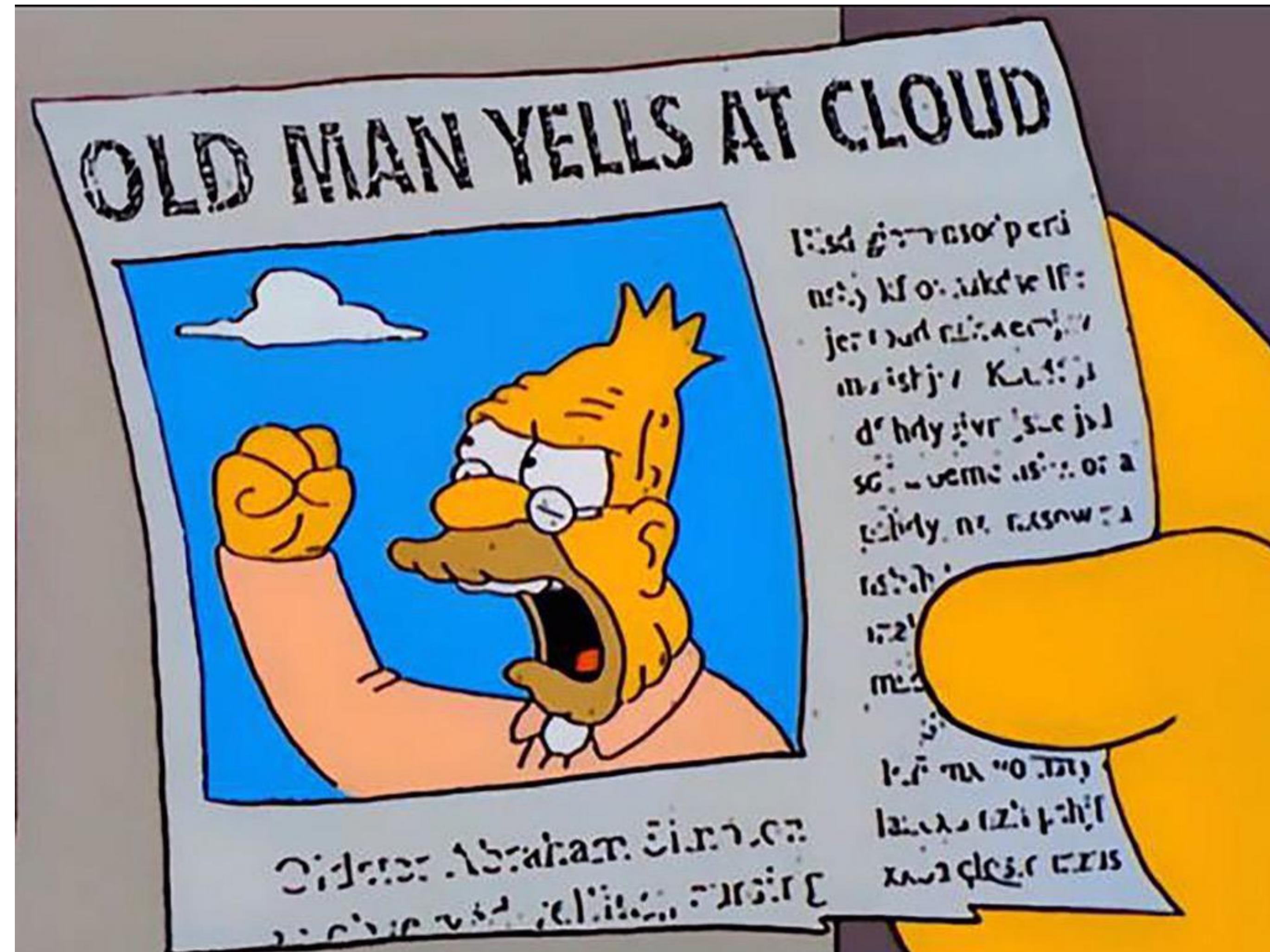


Whoami

- ◆ Over two decades in security
- ◆ Board of Directors (ISC)2
- ◆ CSO Online, Forbes, HuffPo
- ◆ Worked in power for 9 years
- ◆ liquidmatrix.org for 18 years
- ◆ Work for Akamai Technologies



I often feel like this...



Time To Seek Help

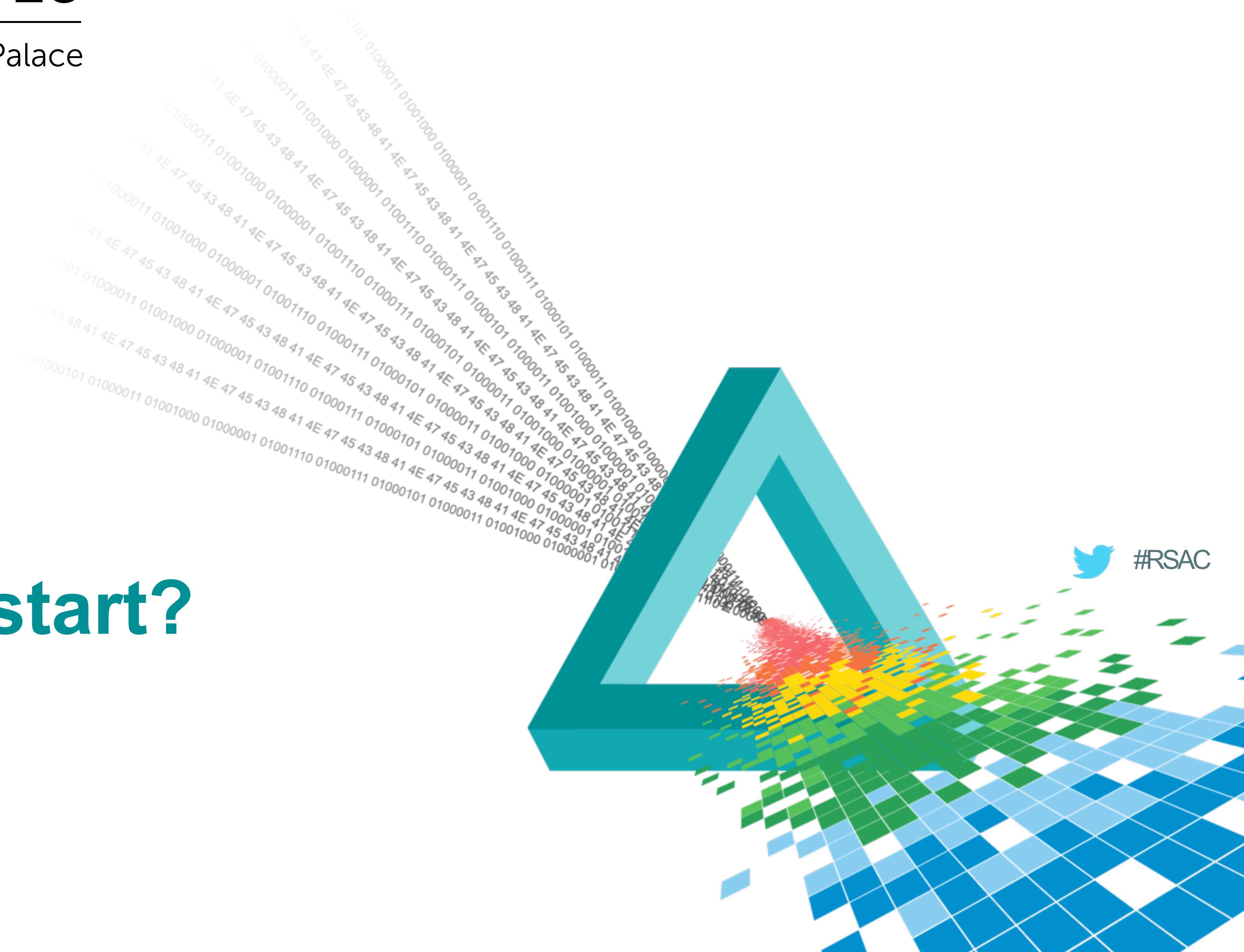
- ◆ IoT is here to stay
- ◆ Acceptance is necessary
- ◆ Need to not be afraid to ask for help
- ◆ Security needs to be integrated



RSA® Conference 2015

Abu Dhabi | 4–5 November | Emirates Palace

So, where do we start?



How Does This Apply To You?

- ◆ Overall Actions:
- ◆ Gain an understanding of your adversary
- ◆ Understand the security issues pertaining to IoT
- ◆ Specific Actions:
 - ◆ Review what are you doing for IoT risk reduction?
 - ◆ Have you assessed the risk to your environment?
 - ◆ Quantify the expected financial loss due to an outage?

Topics

- ◆ Define the nomenclature
- ◆ What is the attack surface
- ◆ Threat Agents
- ◆ Digital Supply Chain
- ◆ Third party vendors



Definition

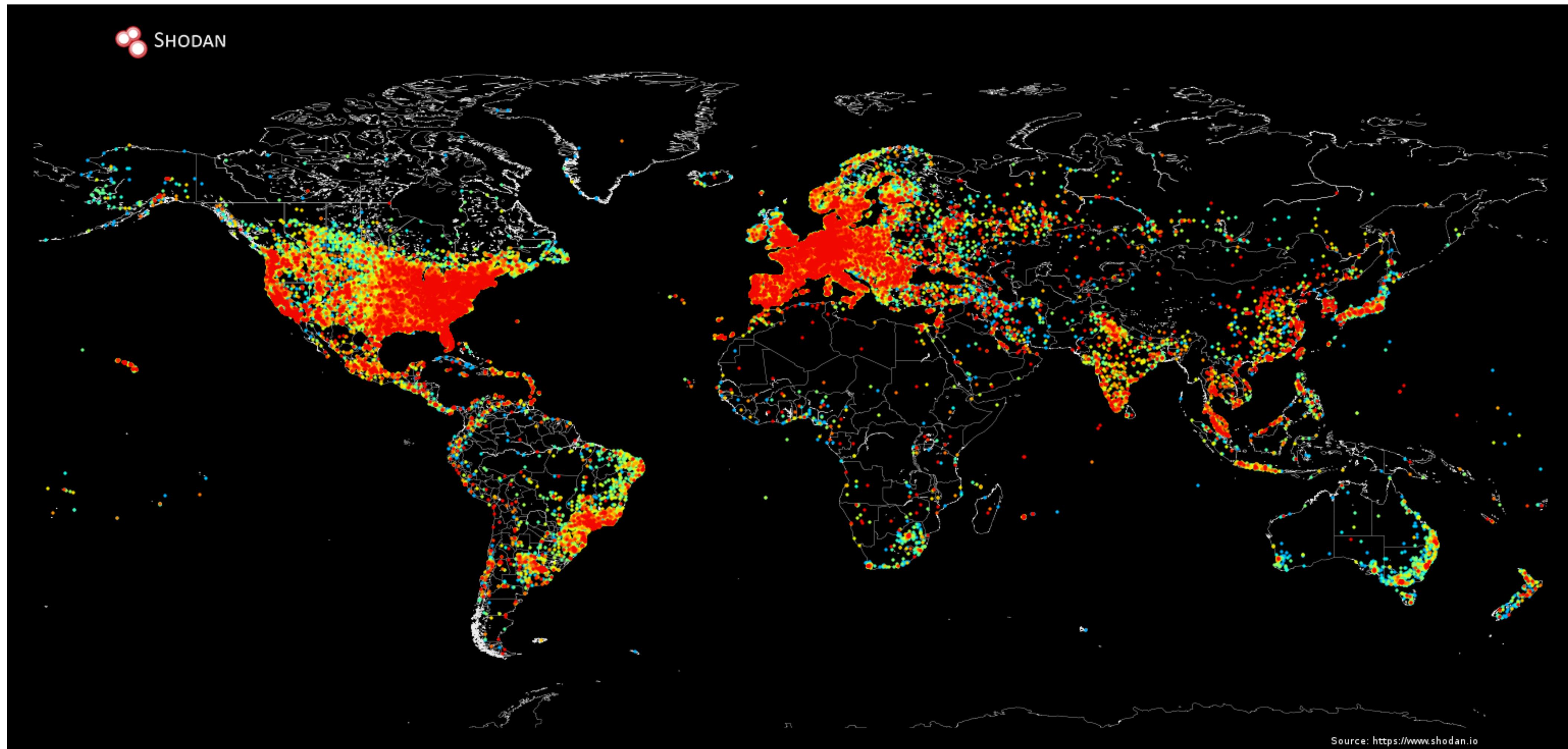
- ◆ IoT: The catch-all phrase
- ◆ Was RFID related
- ◆ Now, simply connected
- ◆ The data is everything
- ◆ There will be obstacles



Misconceptions

- ◆ What is the Internet of Things?
- ◆ 50 billion devices connected by 2020
- ◆ \$1.9 trillion in value by 2019
- ◆ We have to understand that it isn't just about the devices, network, or the clients
- ◆ The surface area is extensive to say the least
- ◆ We have to examine each aspect

Attack Surface



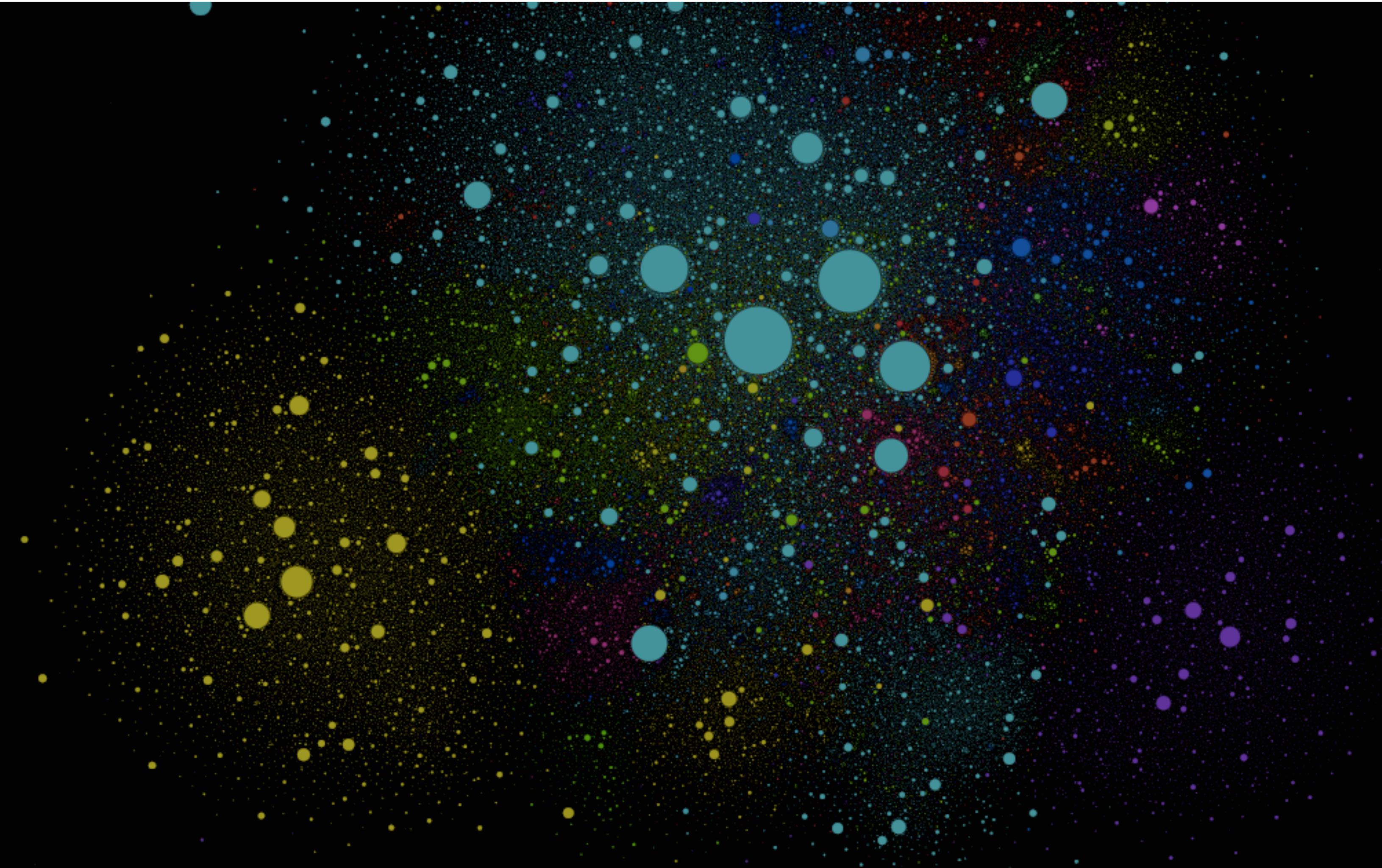
Target Rich Environment



What To Take Into Account

- ◆ The device (phone, wearable, tablet, PLC...or toaster)
- ◆ The cloud platform
- ◆ Applications
- ◆ Encryption
- ◆ Physical security
- ◆ Authentication

Digital Supply Chain



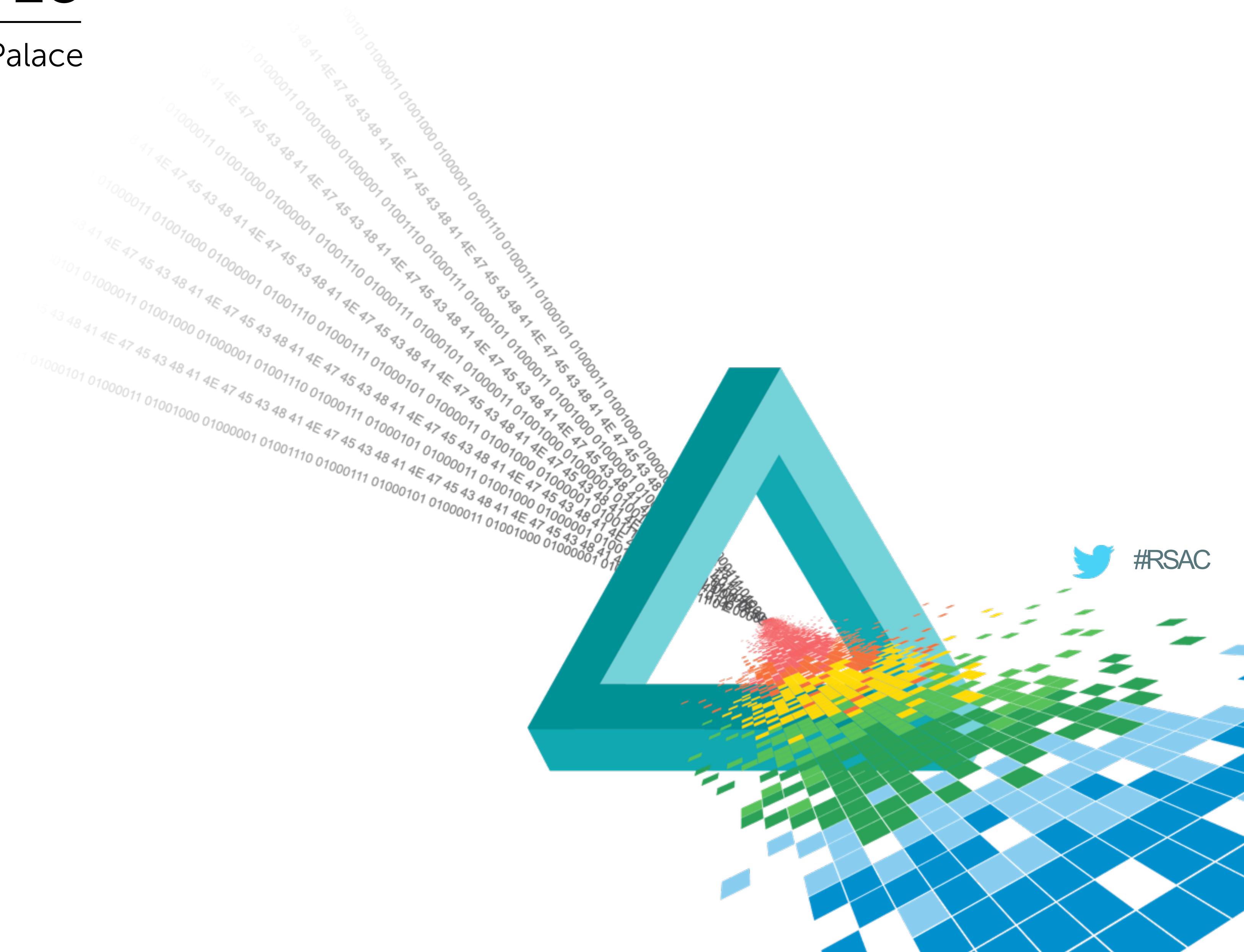
Third Party Vendors



RSA® Conference 2015

Abu Dhabi | 4–5 November | Emirates Palace

Threats



Threat Agents



Actors: Bored Kids





Actors: Hacktivists



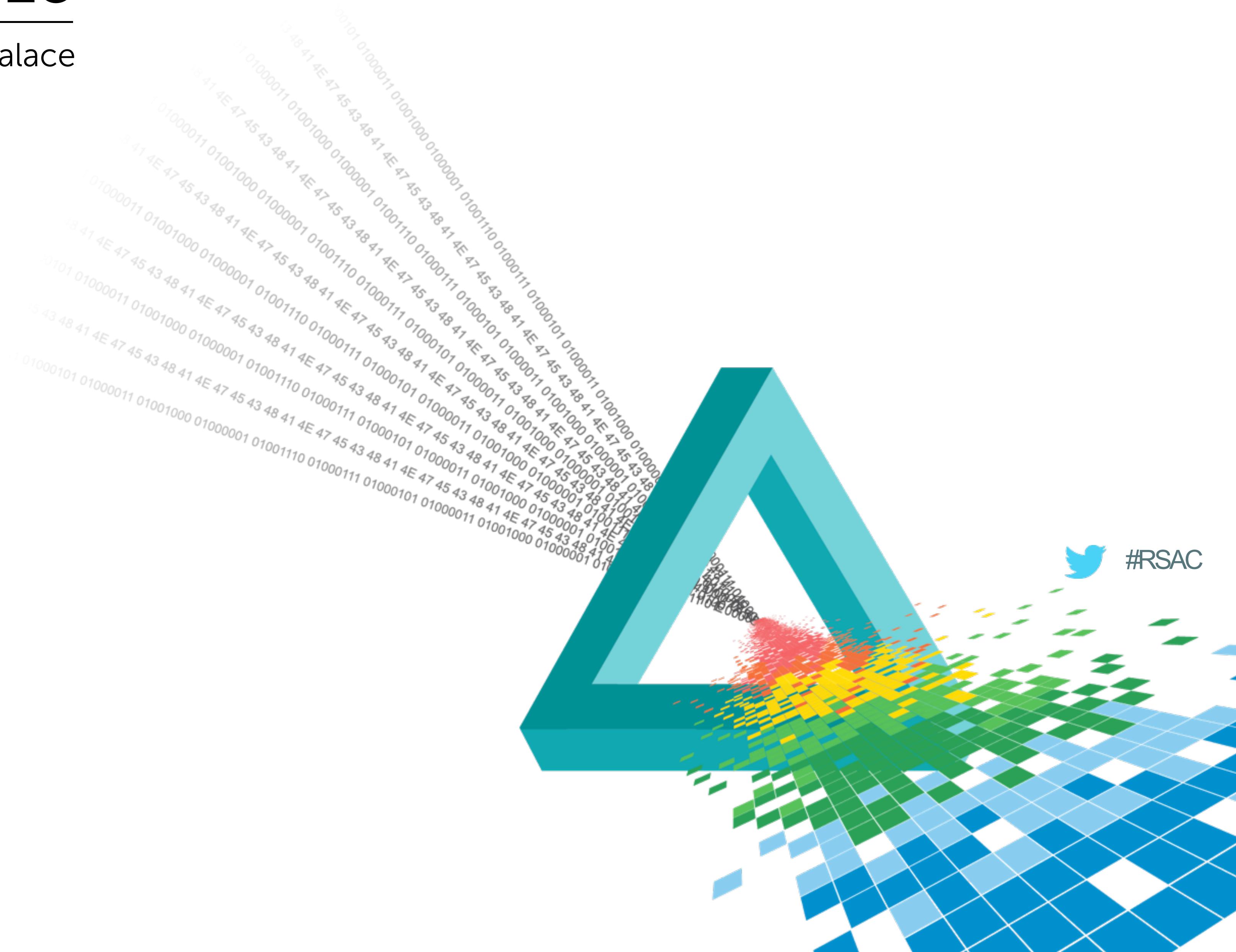
Actors: Nation States



RSA® Conference 2015

Abu Dhabi | 4–5 November | Emirates Palace

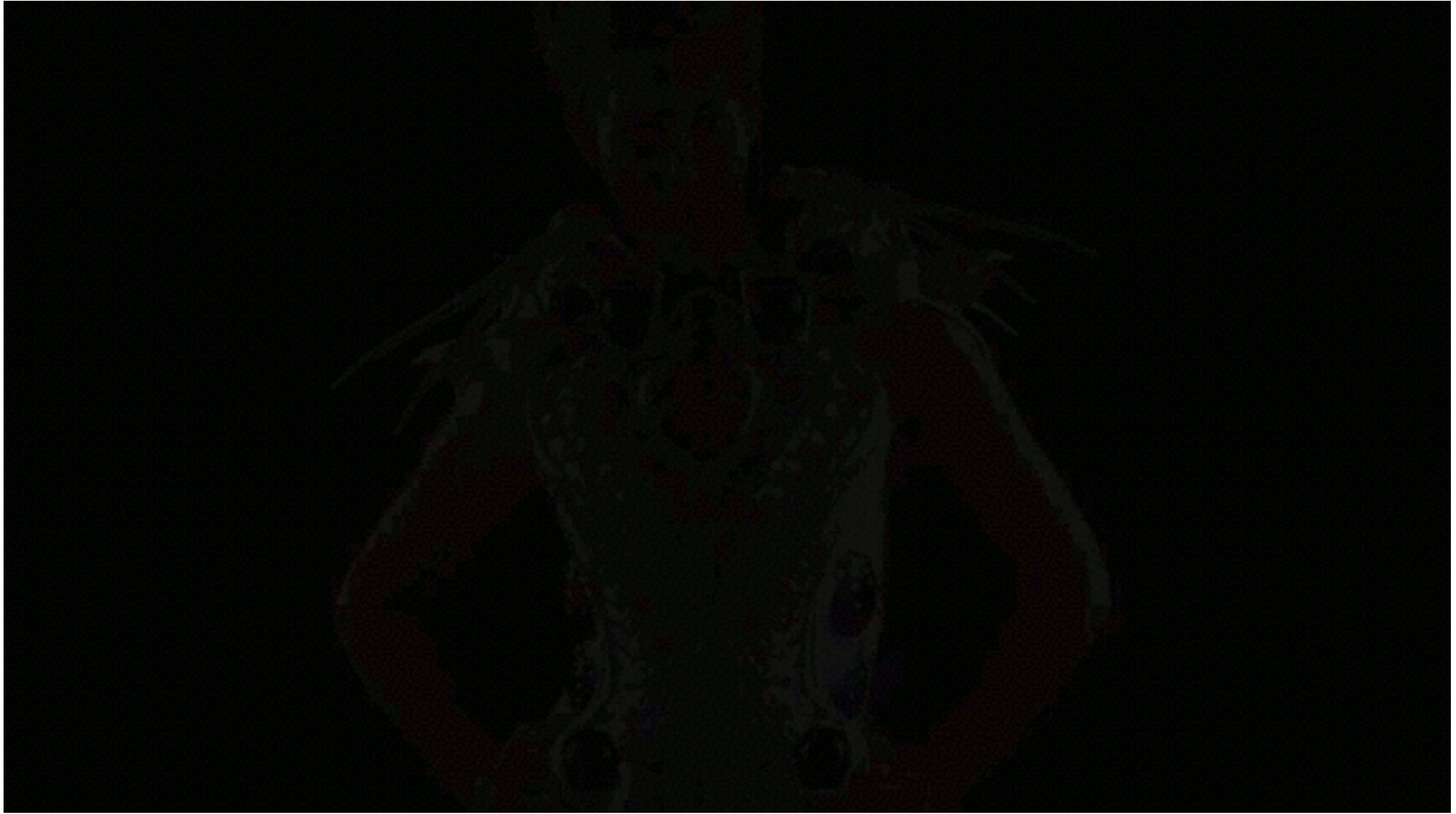
Wearables



Wearables



IoT: Personal Defense



Wearables: Security Issues



Wearable Botnets?

GIZMODO

[Log in / Sign up](#)

Hackers Can Wirelessly Upload Malware to a Fitbit in 10 Seconds



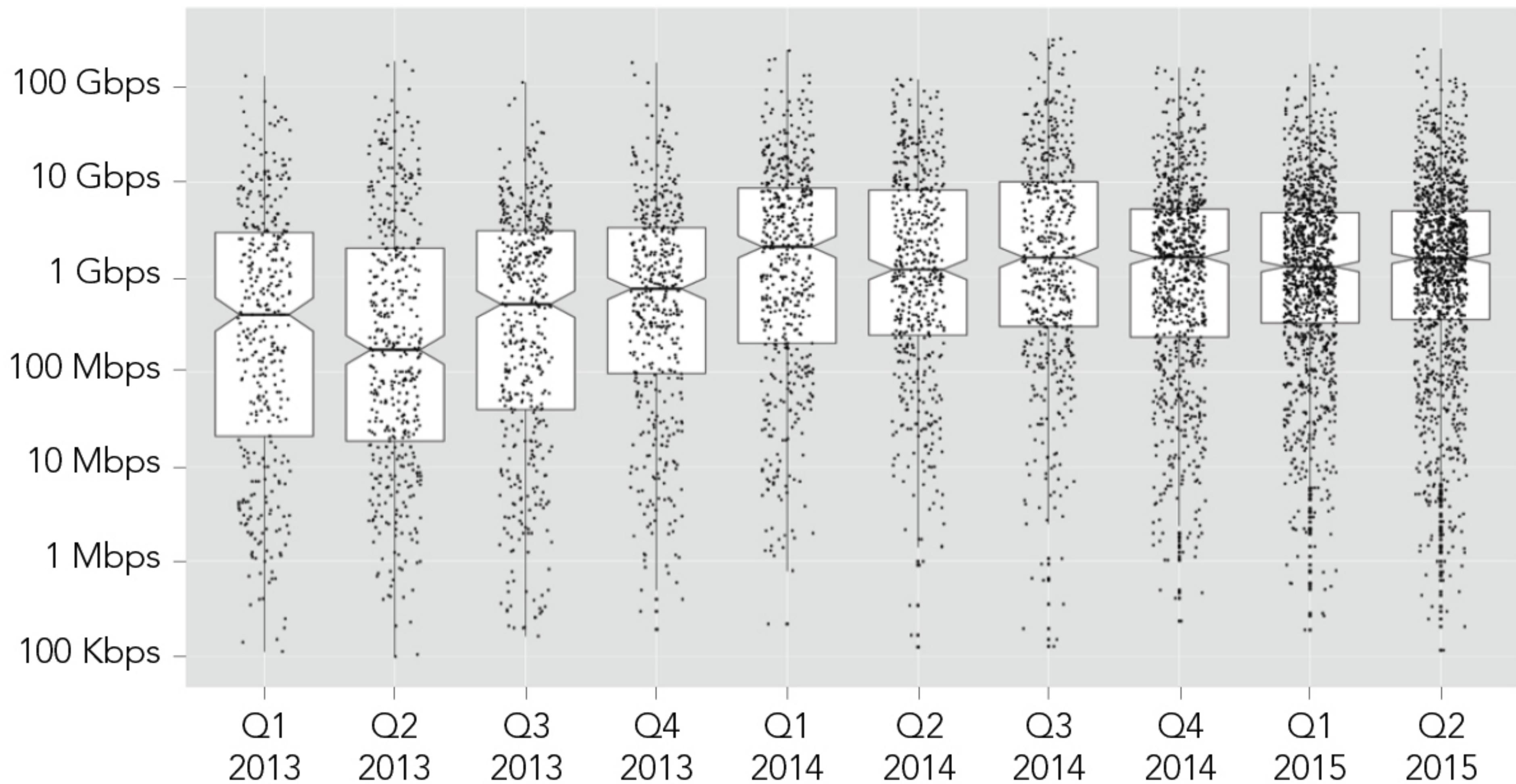
Adam Clark Estes

Filed to: SECURITY 10/21/15 5:05pm

6 ▾



DDoS Size as a Function of Time



LIFX Light Bulb Example

- ◆ Wirelessly connected
- ◆ Rudimentary issues
- ◆ Attackers could spoof
- ◆ Lengthy patch process
- ◆ Security costs time & money
- ◆ Level of security is suspect



What Is The Risk?

- ◆ The internet of things is a building block for cities
- ◆ Many companies offering products are start-ups and under pressure to get to market quickly.
- ◆ Shortcuts happen as a result
- ◆ Security often left in the wake.

TV Set Top Boxes



NEST



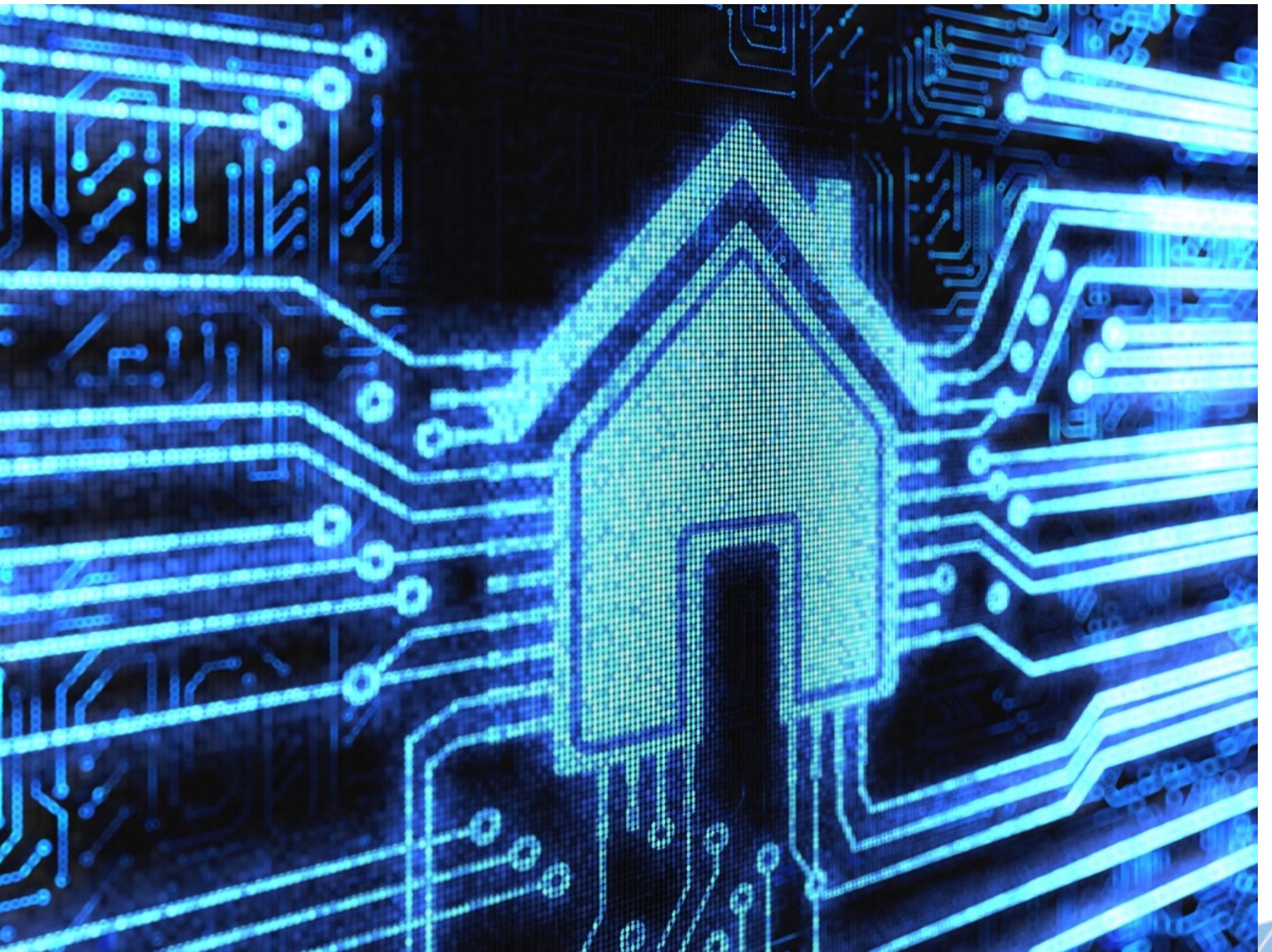
Central System Had Default Credentials



Credit: <https://www.flickr.com/photos/brandongrasley/8227882239/sizes/l>

Home Automation

- ◆ Toasters
- ◆ Refrigerators
- ◆ TVs
- ◆ Heating/Cooling



Internet Enabled Toaster

80
HTTP



HTTP/1.1 403 Forbidden
Date: Wed, 25 Mar 2015 10:49:35 GMT
Server: Hamilton Beach Toastation: 2 Slice Toaster and Oven
Content-Length: 202
Content-Type: text/html; charset=iso-8859-1

443
HTTPS



HTTP/1.1 403 Forbidden
Date: Thu, 02 Apr 2015 16:30:47 GMT
Server: Hamilton Beach Toastation: 2 Slice Toaster and Oven
Content-Length: 202
Content-Type: text/html; charset=iso-8859-1

Mobile Devices

- ◆ Android platform
- ◆ Apple iOS platform
- ◆ Deprecated systems
- ◆ Support for vulnerable services



Control Systems



Robot Vehicles

engadget[®]

REVIEWS

FEATURES

GUIDES

VIDEOS

GALLERIES

PUBLIC ACCESS GAMING

ENGADGET LIVE



Self-driving taxis will begin trials in Japan next year



by Daniel Cooper | @danielwcooper | October 1st 2015 At 12:49pm



Personal Robots: Pepper

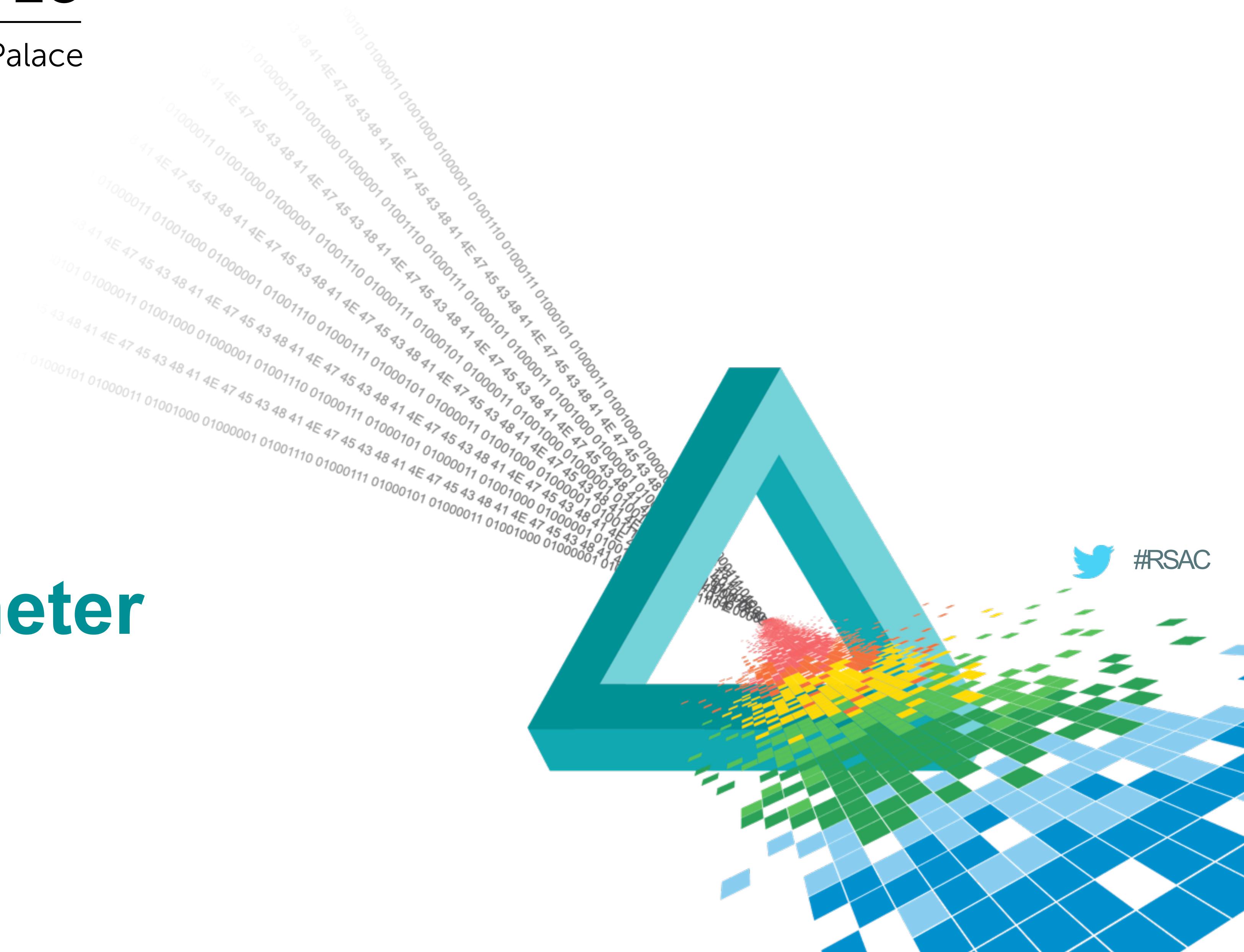
- ◆ “*SoftBank Robotics Corp., an international company based in Japan, put 1,000 personal robots, priced at \$1,600, on sale on Saturday. Within one minute, they were sold out. Customers also must pay a \$120 per month cloud connection fee and monthly insurance of \$80.*”
- ◆ ComputerWorld, June 22, 2015



RSA® Conference 2015

Abu Dhabi | 4–5 November | Emirates Palace

Data Is The Perimeter



Data Protection



Protecting The Surfeit Of Data

- ◆ Data at rest
- ◆ Data in motion
- ◆ Sheer volumes of data
- ◆ Storage



Privacy

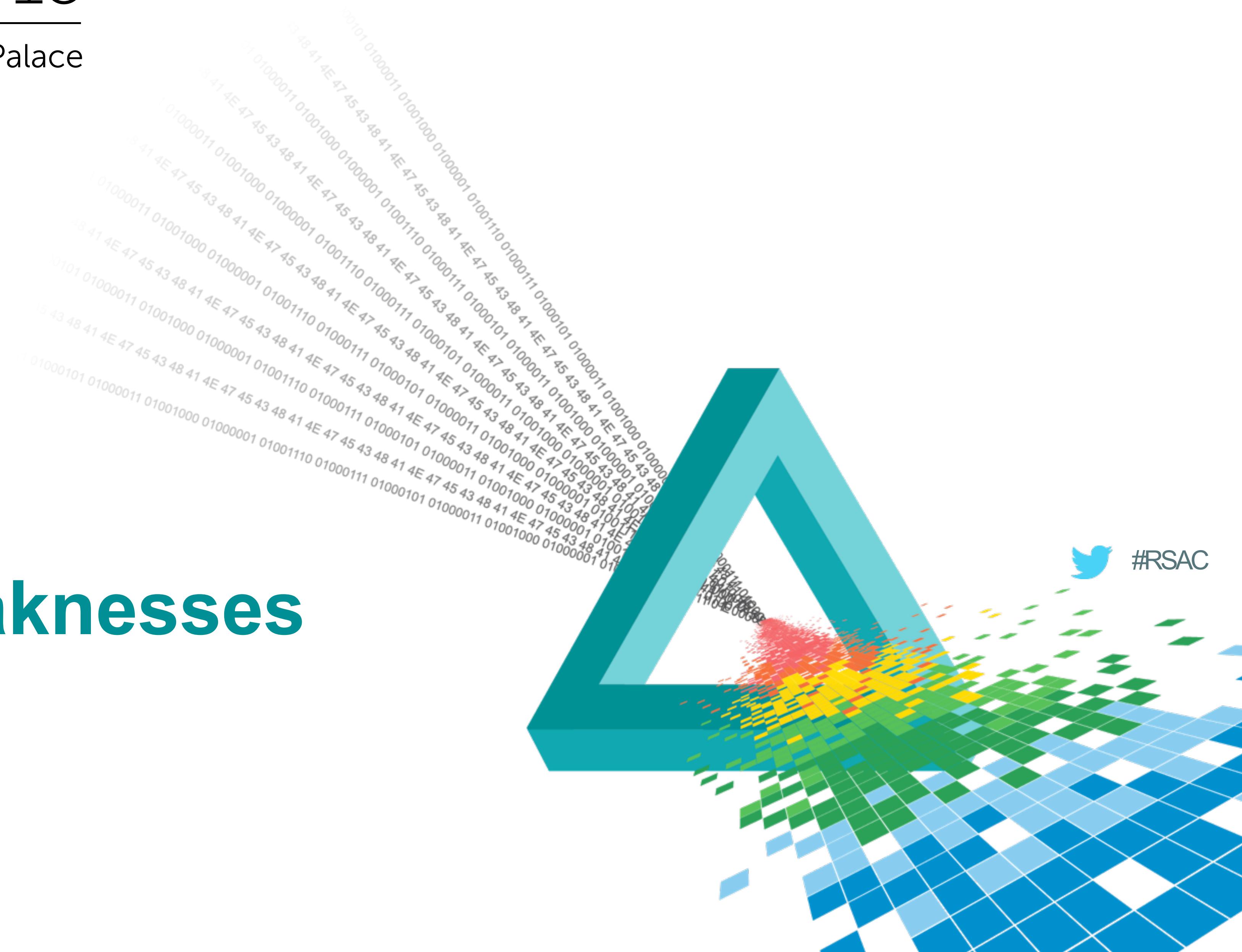
- ◆ Data security
- ◆ Healthcare information
- ◆ Financial Information
- ◆ In transit (TLS)
- ◆ Access control



RSA® Conference 2015

Abu Dhabi | 4–5 November | Emirates Palace

Exposures & Weaknesses



Time to Market

- ◆ Implausible project timelines
- ◆ The push to get products out
- ◆ Security gets sidestepped
- ◆ Mistakes happen



Web Interface

- ◆ Web vulnerability testing
- ◆ Default accounts
- ◆ SQL injection
- ◆ Session management
- ◆ Enumeration
- ◆ iFrames
- ◆ Resource exhaustion



How To Fix This?

- ◆ Actively testing applications for vulnerabilities
- ◆ Ensuring that there are no default username/passwords
- ◆ Ensure the application does not leak information
- ◆ Make sure that recovery mechanisms cannot be abused

Authentication

- ◆ Need to ensure that authentication mechanisms are resilient
- ◆ Limit the users/applications to only what they actually need.
- ◆ Ensure that there is key rotation in place
- ◆ Are you using multi factor authentication?
- ◆ Does the “root” account have active keys?

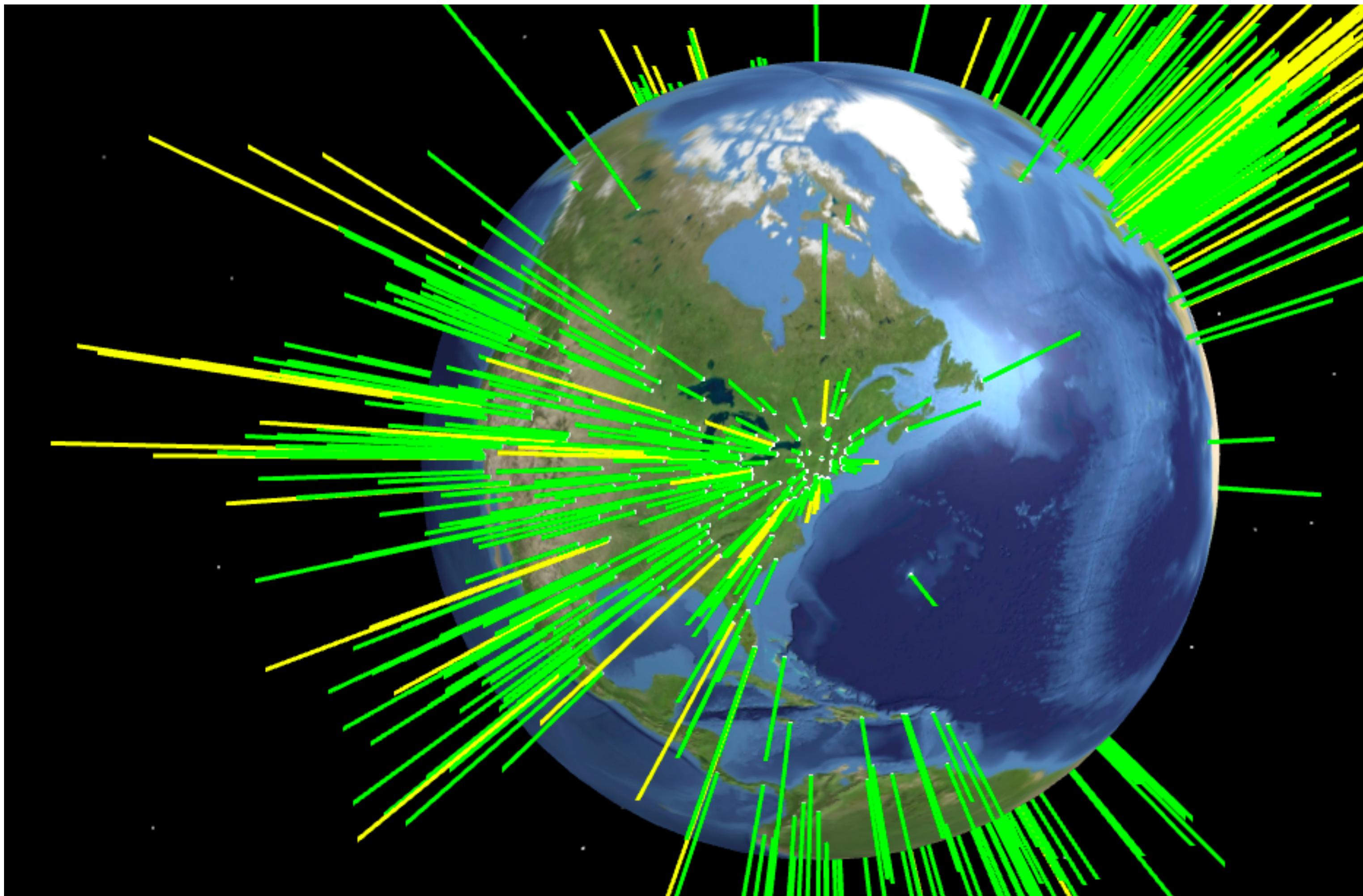
APIs



APIs

- ◆ Authentication: Identity of the requesting party
- ◆ Authentication: What access level is granted?
- ◆ Federation of credentials
- ◆ Protecting externally exposed APIs
- ◆ Scalable security to future proof IoT infrastructures

DNS: Internet Infrastructure

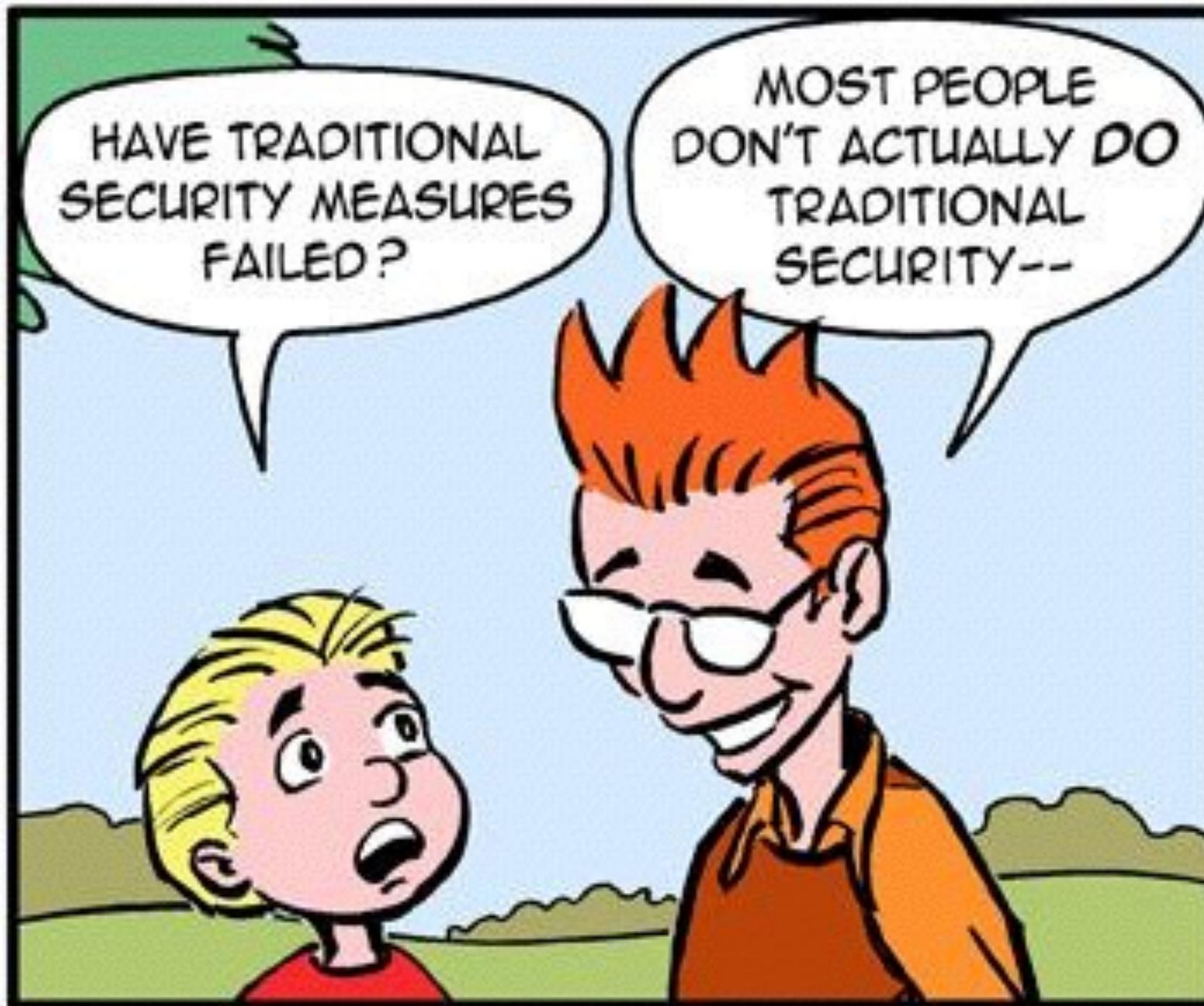


DNS Security

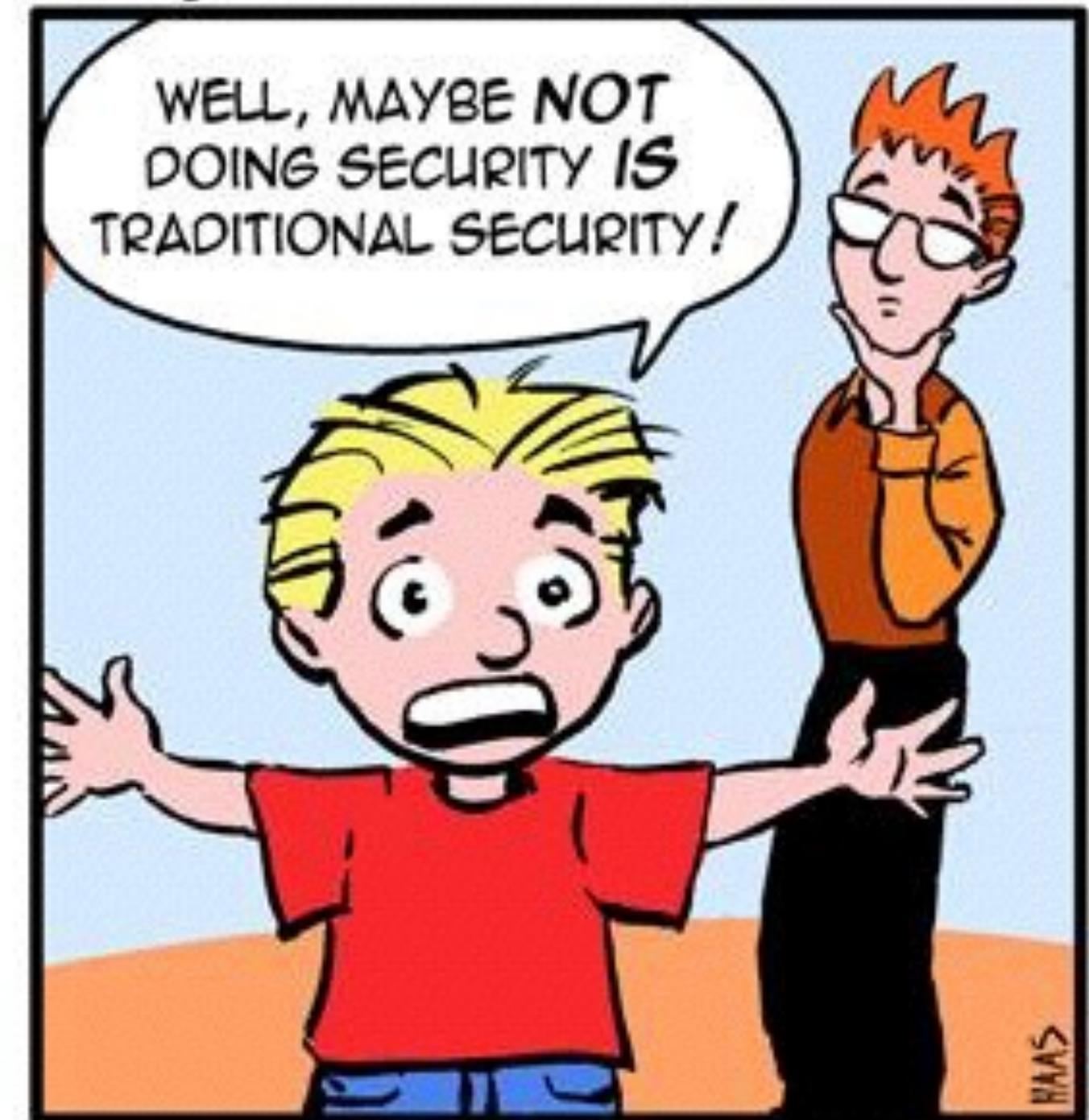
- ◆ DNS is the underpinnings of all things IoT
- ◆ Protect your DNS against amplification & reflection attacks
- ◆ Provide defense against resource utilization attacks
- ◆ Prevent DNS cache poisoning attacks
 - ◆ Attackers use this exploitation technique to redirect users from legitimate sites to malicious sites or to inform the DNS resolver to use a malicious name server that is providing information used for malicious activities.

Exposed Network Services

LITTLE BOBBY



by Robert M. Lee and Jeff Haas



Testing



PATCHING!!!!

- ◆ Security patches happen
- ◆ How will IoT devices have their patching managed?
- ◆ What mechanism are in place to ensure success?
- ◆ ...and to measure failure?

RSA® Conference 2015

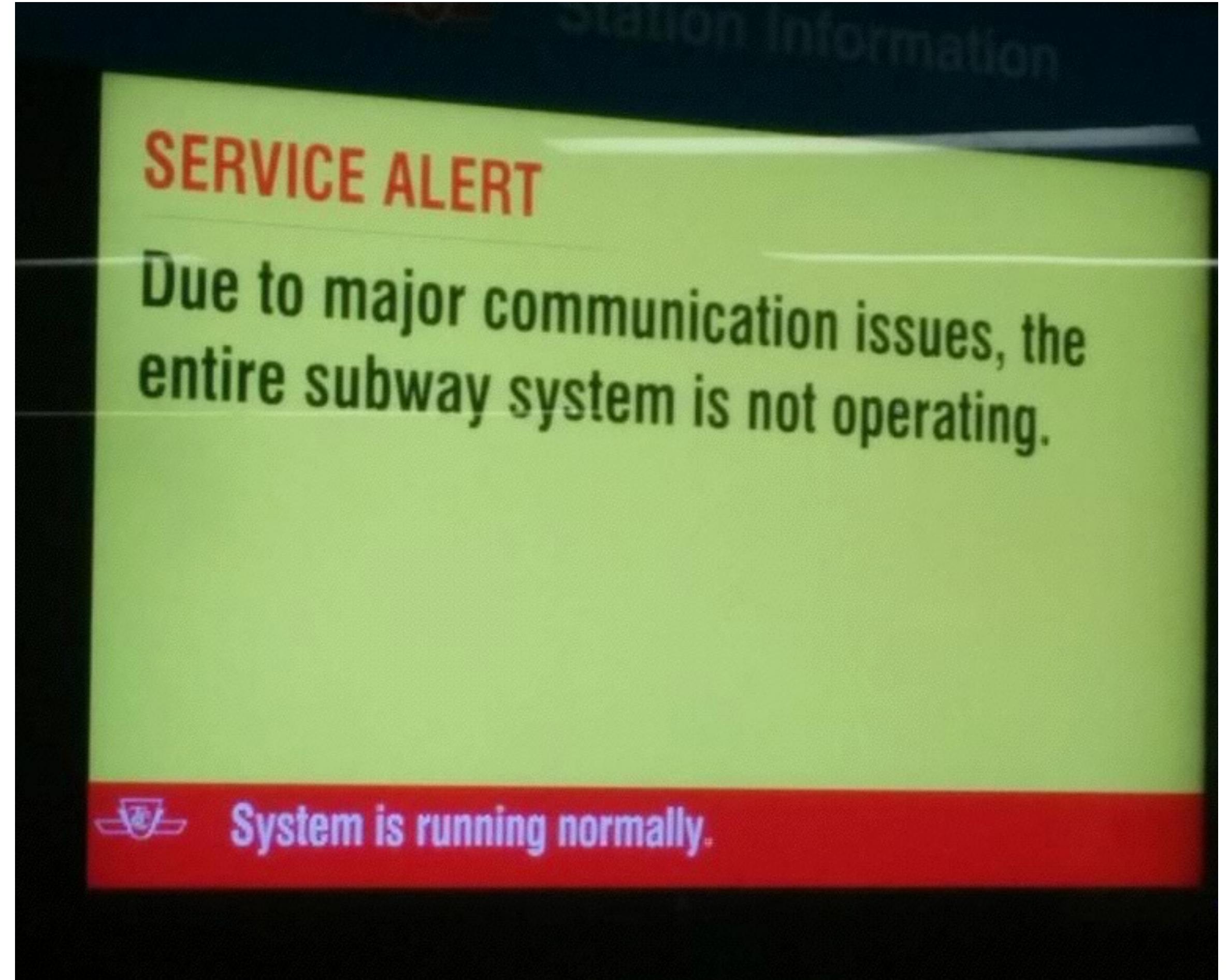
Abu Dhabi | 4–5 November | Emirates Palace

Elements of a Secure City



Security Elements Of The Smart City

- ◆ Power management
- ◆ Traffic flow
- ◆ Mass transit
- ◆ Security
- ◆ Communication methods



Connected City Streets

- ◆ Wireless traffic lights
- ◆ 3G connectivity
- ◆ Greater efficiency
- ◆ Subject to wireless security issues
- ◆ Lower congestion
- ◆ Security testing is necessary



Credit: https://upload.wikimedia.org/wikipedia/commons/8/87/Traffic_lights.jpg

Interconnecting Everything

- ◆ Ease of data interconnection
- ◆ Data for convenience
- ◆ More services available online
- ◆ Potential for errors increases
- ◆ Wider attack surface
- ◆ Chance for attackers to abuse



What Needs To Be Done?

- ◆ Cisco estimates 50 billion devices by 2020
- ◆ Gartner estimates 30 billion devices by 2020
- ◆ Rate of adoption ever increasing
- ◆ The attacks will increase
- ◆ How can patches be managed?
- ◆ Barriers to security need to be managed
- ◆ Security failures can lead to serious real-world consequences.

Questions?



<https://www.flickr.com/photos/jarbo/9379813470/sizes/l>

Thanks

- ◆ Dave Lewis
- ◆ Global Security Advocate
- ◆ Akamai Technologies
- ◆ dave@akamai.com
- ◆ Twitter: @Gattaca

