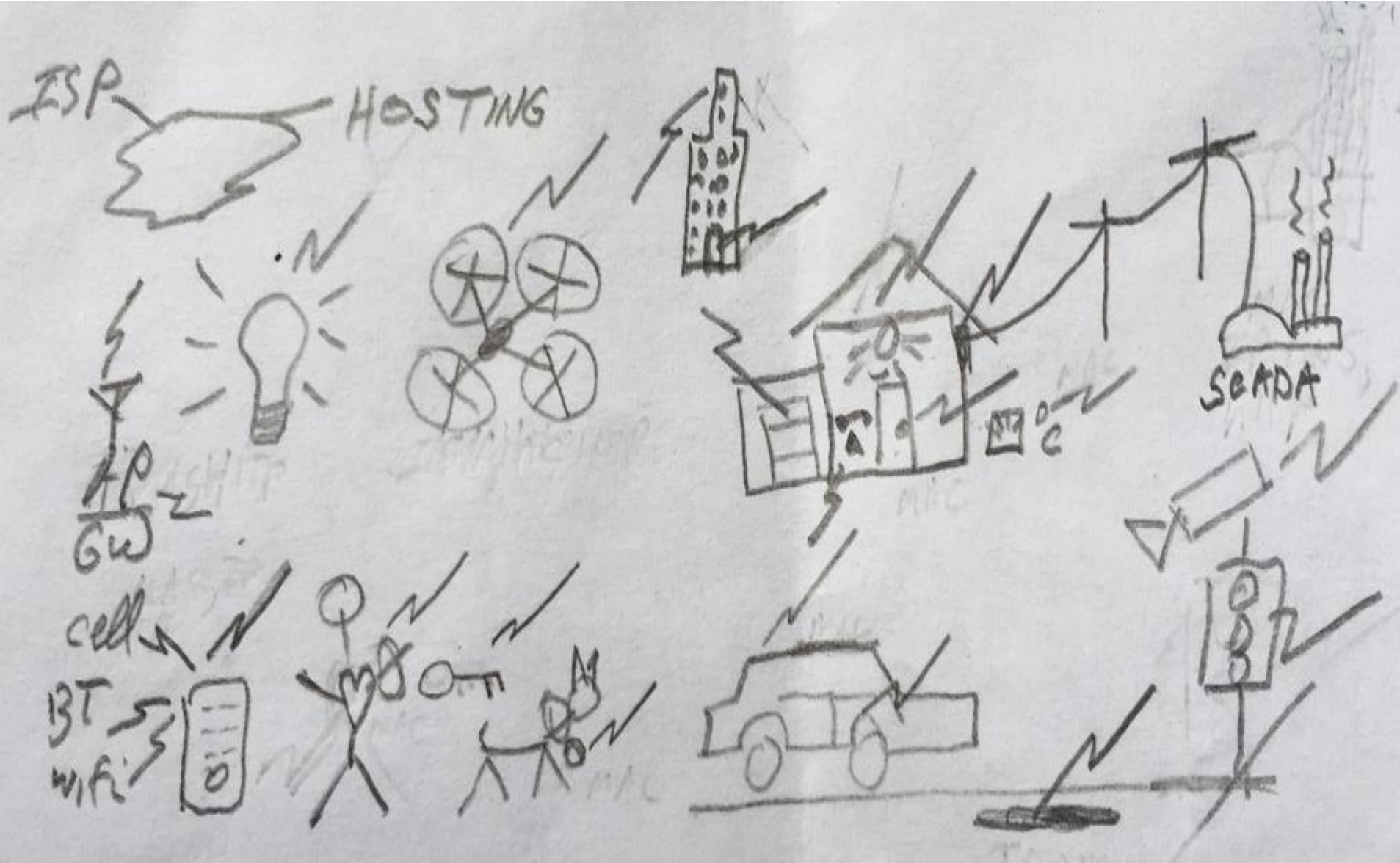




# Internet of Things and the Unique Identifier System

Fahd Batayneh | Regional Cybersecurity Summit | 31 OCT 2016

# What are we Talking About?



# And What's the Hype About?



# Simple View of IoT Dependencies

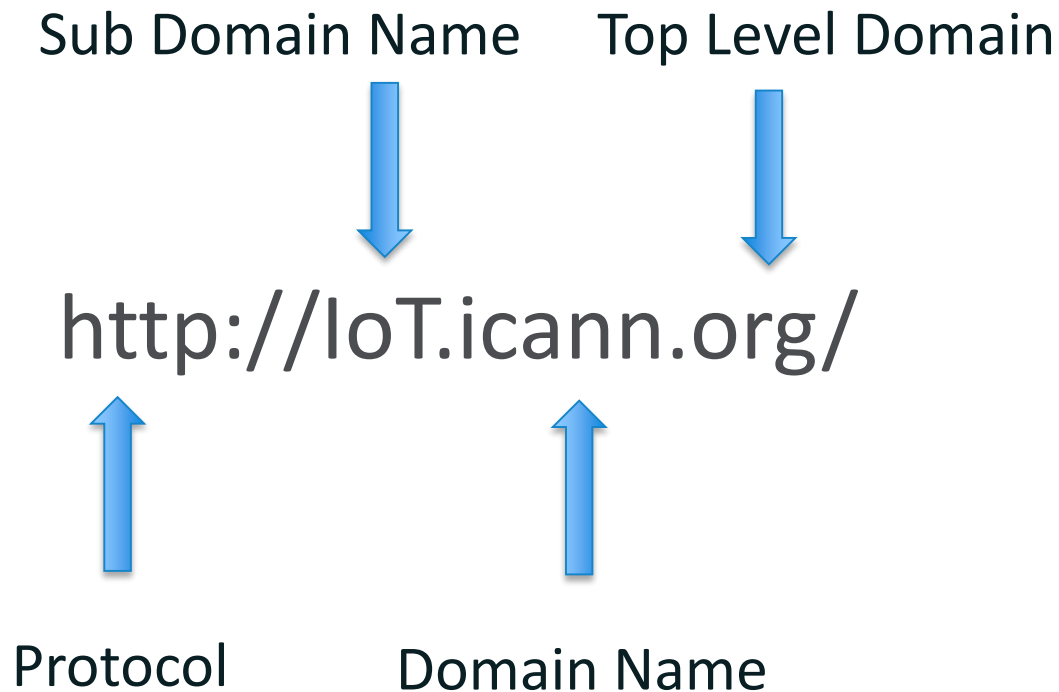
Economic/Societal Layer (IoT, Finance, Security...)

Logical Layer (Domain Names, IP Addresses...)

Physical Layer (Undersea cables, Satellite, IXPs...)

# Domain Names

- Remembering names is always easier than remembering number



# Security Online

- ◎ Cybersecurity is a key term today
- ◎ Billions of USD is lost yearly due to cybersecurity attacks

## WHEN DDoS ATTACKS THREATEN BUSINESS OPPORTUNITIES

### Cost per DDoS Attack

DDoS attacks cost small and mid-size businesses an average of \$52,000 per incident. For large enterprises, an average of \$440,000 is lost in business and IT spending.



CIO INSIGHT

## WHEN DDoS ATTACKS THREATEN BUSINESS OPPORTUNITIES

### Top Four Long-Term Cost of DDoS Attacks



CIO INSIGHT

# Security and the DNS

- ⦿ Is the DNS secure?
  - ⦿ DNS Spoofing - Diverts Internet traffic away from legitimate servers and towards fake ones
  - ⦿ Man in the Middle – Someone stands in-between you and the entity executing your transaction
- ⦿ Are there solutions?

**DNSSEC**

# DNSSEC Demystified





# ... cont. (DNSSEC Demystified)



# ... cont. (DNSSEC Demystified)



# Who Should Deploy DNSSEC?

**Registries** – registries must sign their zones and roll over their keys as part of routine maintenance

**DNS Providers** – will need to provide the ability for registrants to sign their domain names and generate the key they will provide to the zone through via their registrar

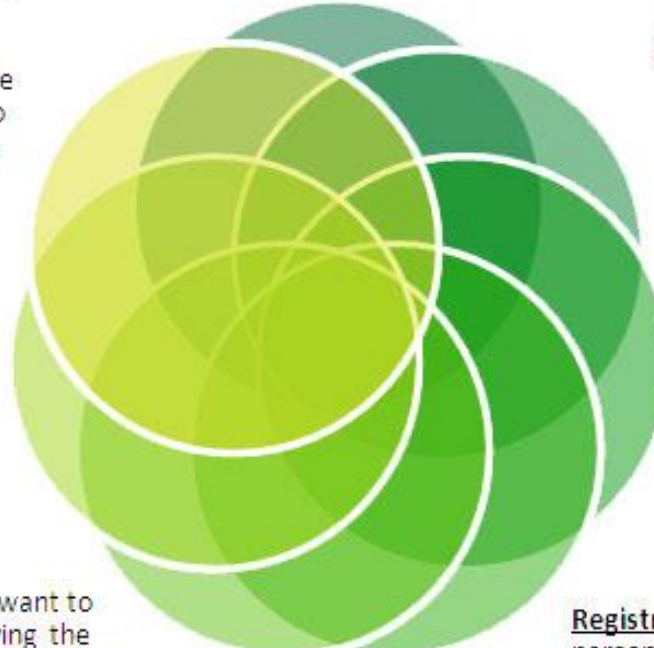
**ISP's** – must set their DO bits and ensure that their caching servers are configured for larger response sizes

**Hardware vendors** – may need to modify routers to accept larger packet sizes through port 53

**Registrars** – must prepare their account management interfaces to receive keys from their customers and pass them to the appropriate registry via EPP

**Browsers** – will want to consider modifying the browser interface to indicate the presence of DNSSEC as they have with https:// (padlock) and EV certs (green browser bar)

**Registrants** – who collect personal and/or financial information will want to generate a key for each of their names and submit to their DNS provider



Source - <https://www.neustar.biz/>

# And Who is Responsible for the DNS?!

- ⦿ The Internet Corporation for Assigned Names and Numbers (ICANN)
- ⦿ ICANN coordinates these unique identifiers across the world
- ⦿ ICANN **promotes competition** and **develops policy** on the Internet's unique identifiers
- ⦿ ICANN does not control content, it cannot stop spam, and it does not deal with access to the Internet
- ⦿ Has hub offices in Los Angeles (HQ), Istanbul, and Singapore
- ⦿ Has engagement centers in Montevideo, Washington DC, Brussels, Geneva, Beijing, and Seoul
- ⦿ Website at <http://www.icann.org/>

# Engage with ICANN



## Fahd Batayneh

Manager, Stakeholder Engagement, Middle East

Email: [fahd.batayneh@icann.org](mailto:fahd.batayneh@icann.org)

Website: <http://icann.org/>



[twitter.com/icann](https://twitter.com/icann)

[twitter.com/fahdbatayneh](https://twitter.com/fahdbatayneh)



[facebook.com/icannorg](https://facebook.com/icannorg)



[linkedin.com/company/icann](https://linkedin.com/company/icann)



[youtube.com/user/icannnews](https://youtube.com/user/icannnews)



[gplus.to/icann](https://gplus.to/icann)



[weibo.com/ICANNorg](https://weibo.com/ICANNorg)



[flickr.com/photos/icann](https://flickr.com/photos/icann)



[slideshare.net/icannpresentations](https://slideshare.net/icannpresentations)