

Security in the Internet of Things: A primer

G. Stergiopoulos, D. Mentzelioti
June 2017

**ΑΣΦΑΛΕΙΑ
ΣΤΟ
INTERNET OF
THINGS**

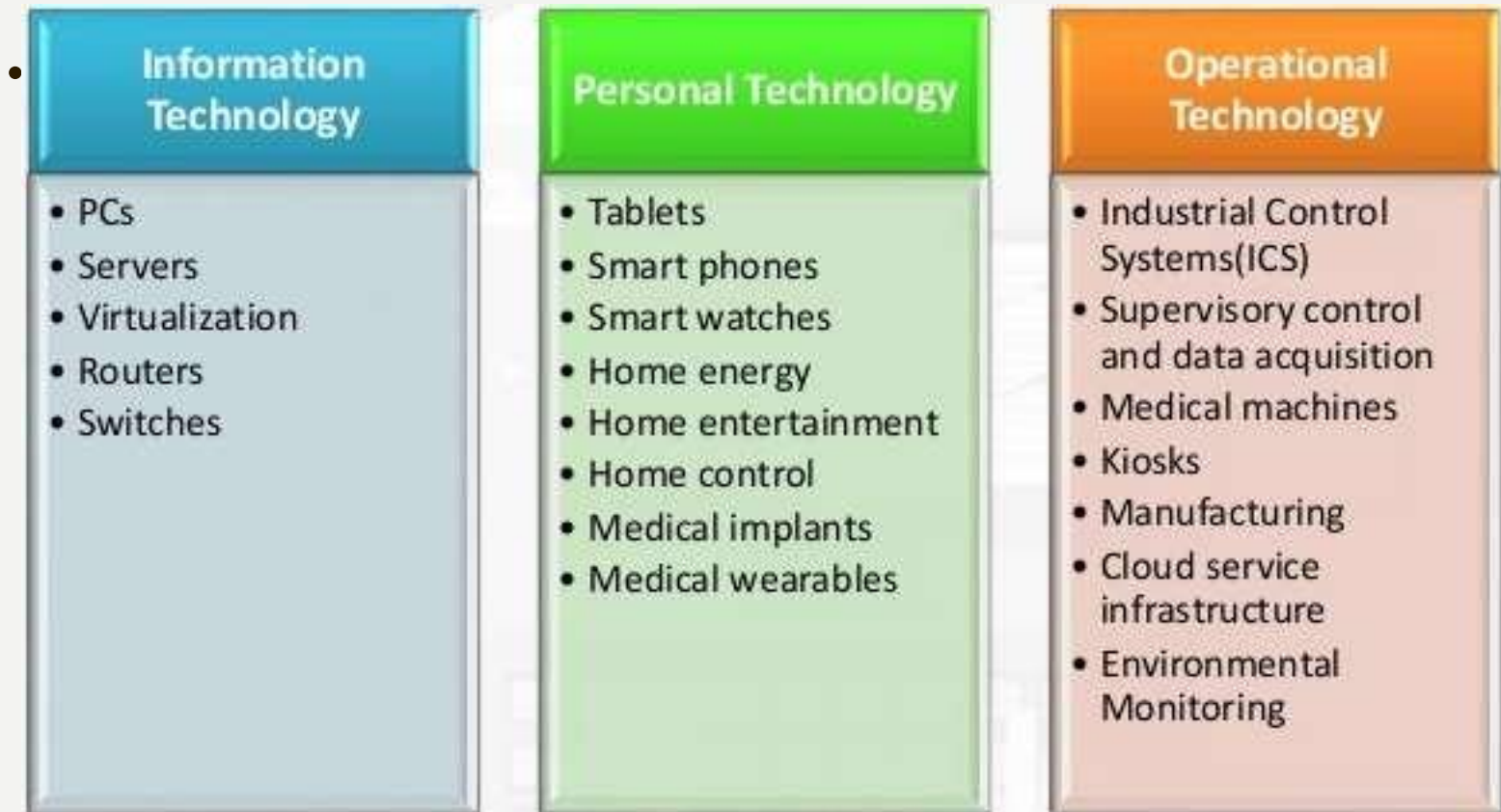
**INFOSEC LAB
ΟΙΚΟΝΟΜΙΚΟ
ΠΑΝΕΠΙΣΤΗΜΙΟ
ΑΘΗΝΩΝ**

2016 - 2017

ΘΕΜΑΤΑ ΣΥΖΗΤΗΣΗΣ

- Τι είναι αυτό το... πράγμα;
- Κύκλος ζωής ενός... πράγματος
- Χαρακτηριστικά και χρήση των έξυπνων συσκευών
- Χαρακτηριστικά και χρήση των κινητών συσκευών
- Τάσεις και απειλές
- Αρχές ασφάλειας
- Τεχνολογίες ασφάλειας και εμπορικές λύσεις

ΤΙ ΕΙΝΑΙ ΑΥΤΟ ΤΟ... ΠΡΑΓΜΑ;



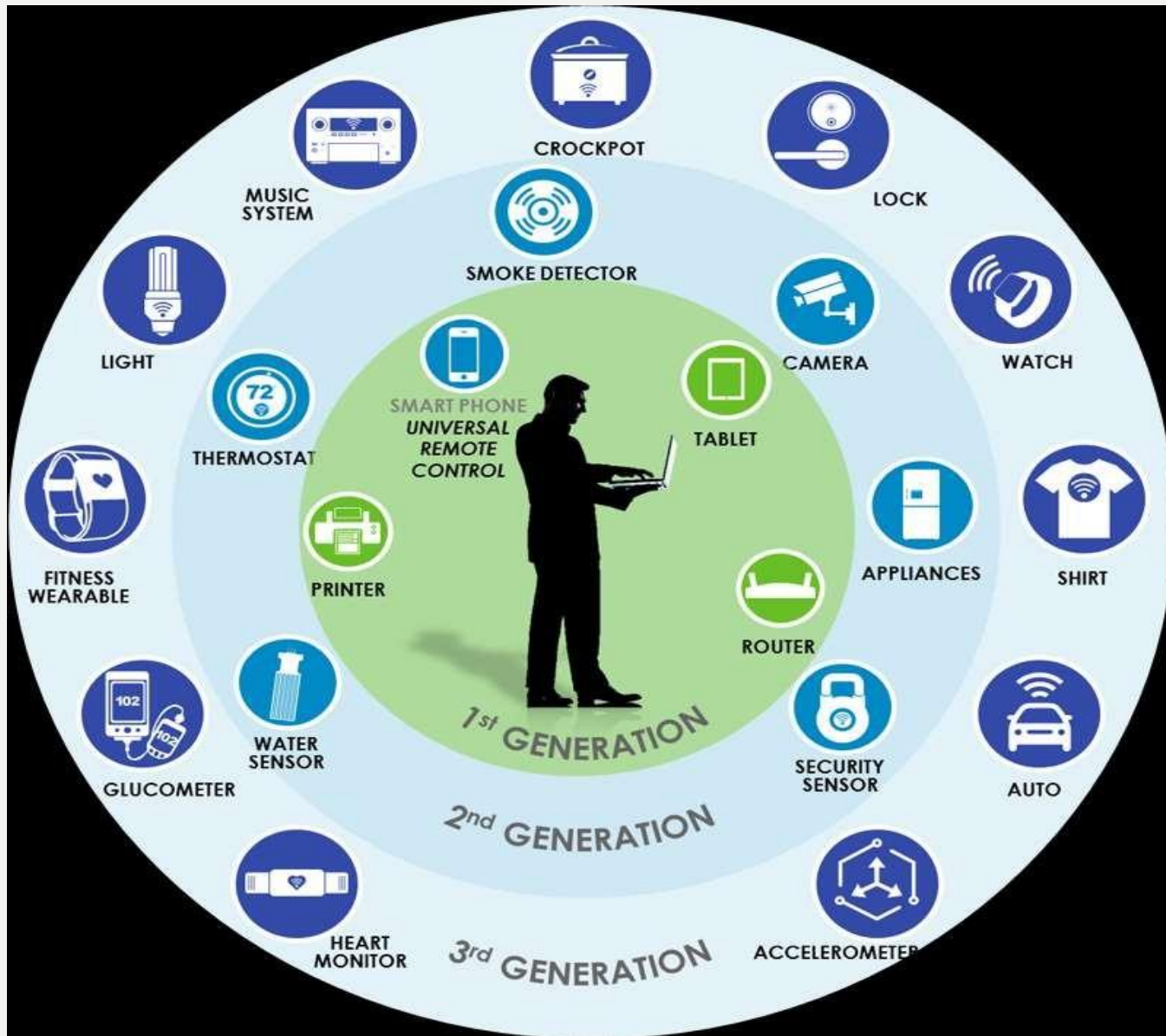
INTERNET OF THINGS - 1

- «Η διασύνδεση φυσικών μηχανών, αυτοκινήτων, κτηρίων η οποιουδήποτε άλλου αντικειμένου με ενσωματωμένο ψηφιακό σύστημα, λογισμικό, αισθητήρες και ικανότητα διασύνδεσης που επιτρέπει στα αντικείμενα αυτά να συγκεντρώσουν ή/και να ανταλλάξουν δεδομένα».

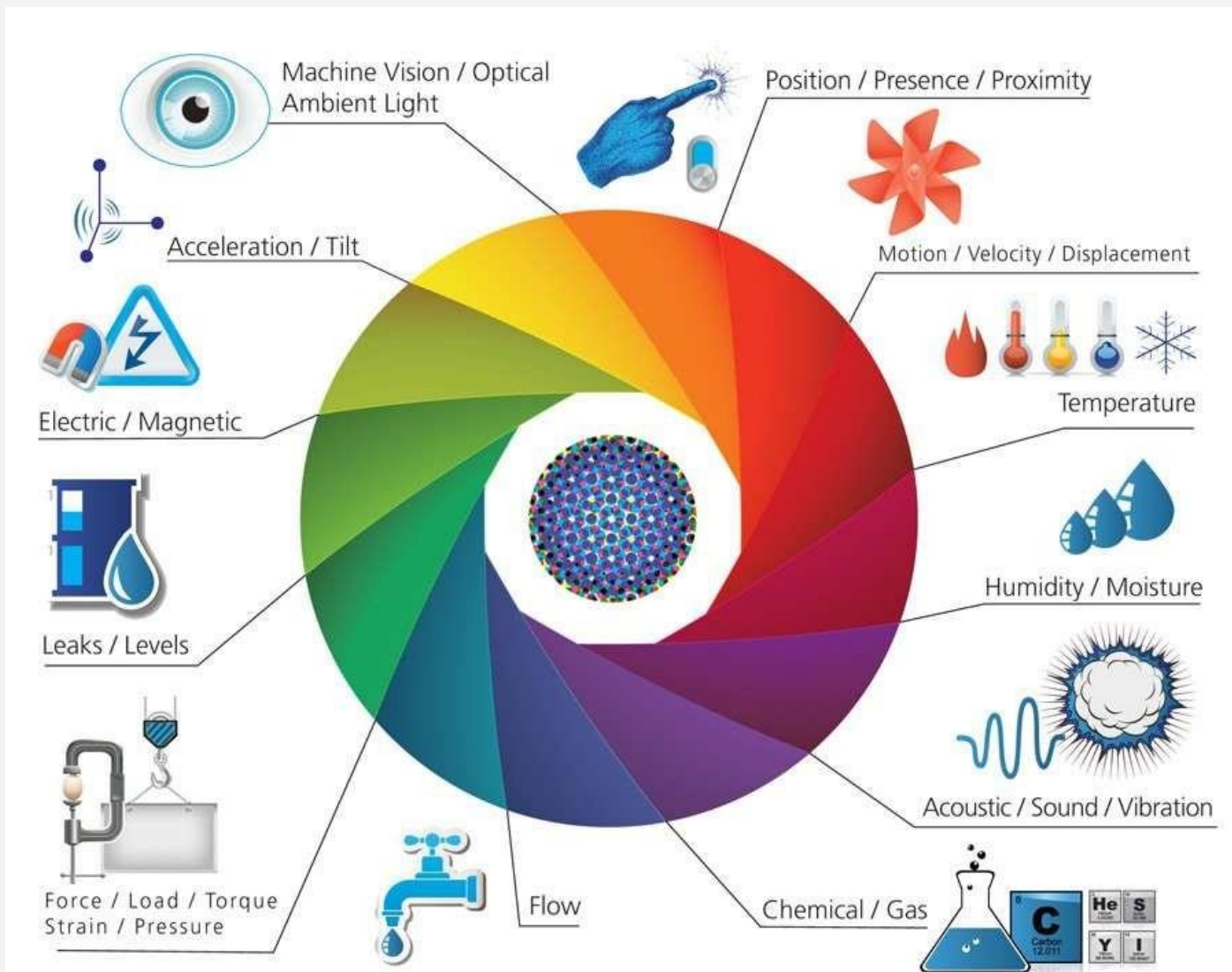
Vermesan, Ovidiu; Friess, Peter (2013)

ΠΡΑΓΜΑΤΑ, ΕΞΥΠΝΕΣ ΚΑΙ ΚΙΝΗΤΕΣ ΣΥΣΚΕΥΕΣ





ΑΙΣΘΗΤΗΡΕΣ



Internet of Things in Logistics, Columbus Region Logistics Council on the IoT, Jeff Risley, B2B Marketing.

INTERNET OF THINGS - 2

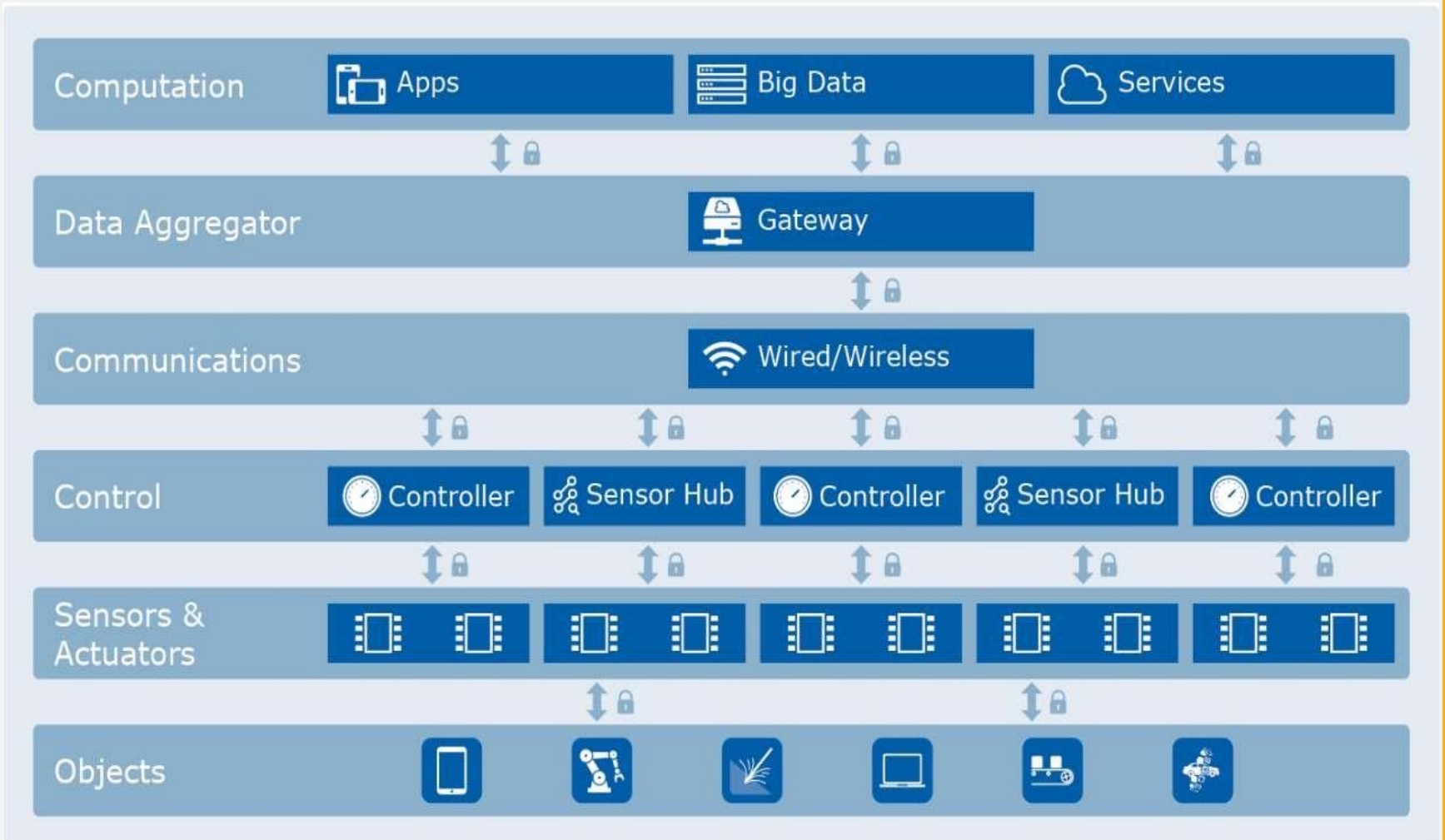
Τρία κύρια μέρη:

1. Τα "πράγματα" (αντικείμενα)
2. Τα δίκτυα επικοινωνιών που τα συνδέουν
3. Τα υπολογιστικά συστήματα τα οποία χρησιμοποιούν τα δεδομένα που ρέουν προς και από τα αντικείμενα.

INTERNET OF THINGS - 3

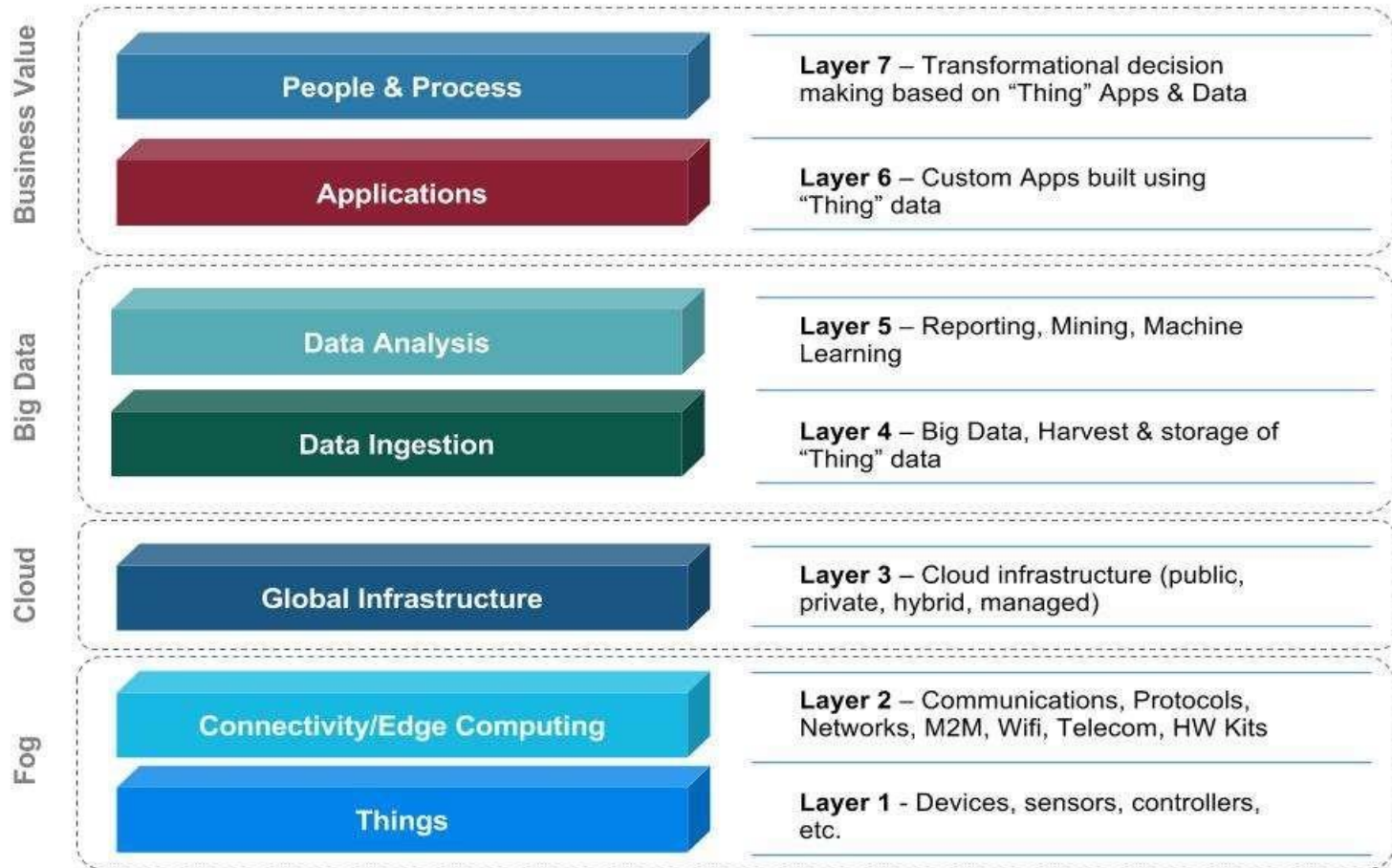
- **Δίκτυο συσκευών** μεταδίδει, διαμοιράζει και χρησιμοποιεί δεδομένα από φυσικό περιβάλλον για παροχή υπηρεσιών.
- **Αντικείμενα-πράγματα** μόνα ή συνδεδεμένα με άλλα αντικείμενα ή άτομα με μοναδικά αναγνωριστικά (identifiers)
- **Εφαρμογές** στο χώρο της υγείας, των μεταφορών, του περιβάλλοντος, της ενέργειας κλπ.
- Τα **δεδομένα** σχετικά με το **ποιοι είμαστε** και **τι κάνουμε**.

ΔΟΜΗ - INTERNET OF THINGS



ΤΑ ΕΠΙΠΕΔΑ ΤΟΥ ΙΟΤ

7 Layers of the Internet of Things (IoT)

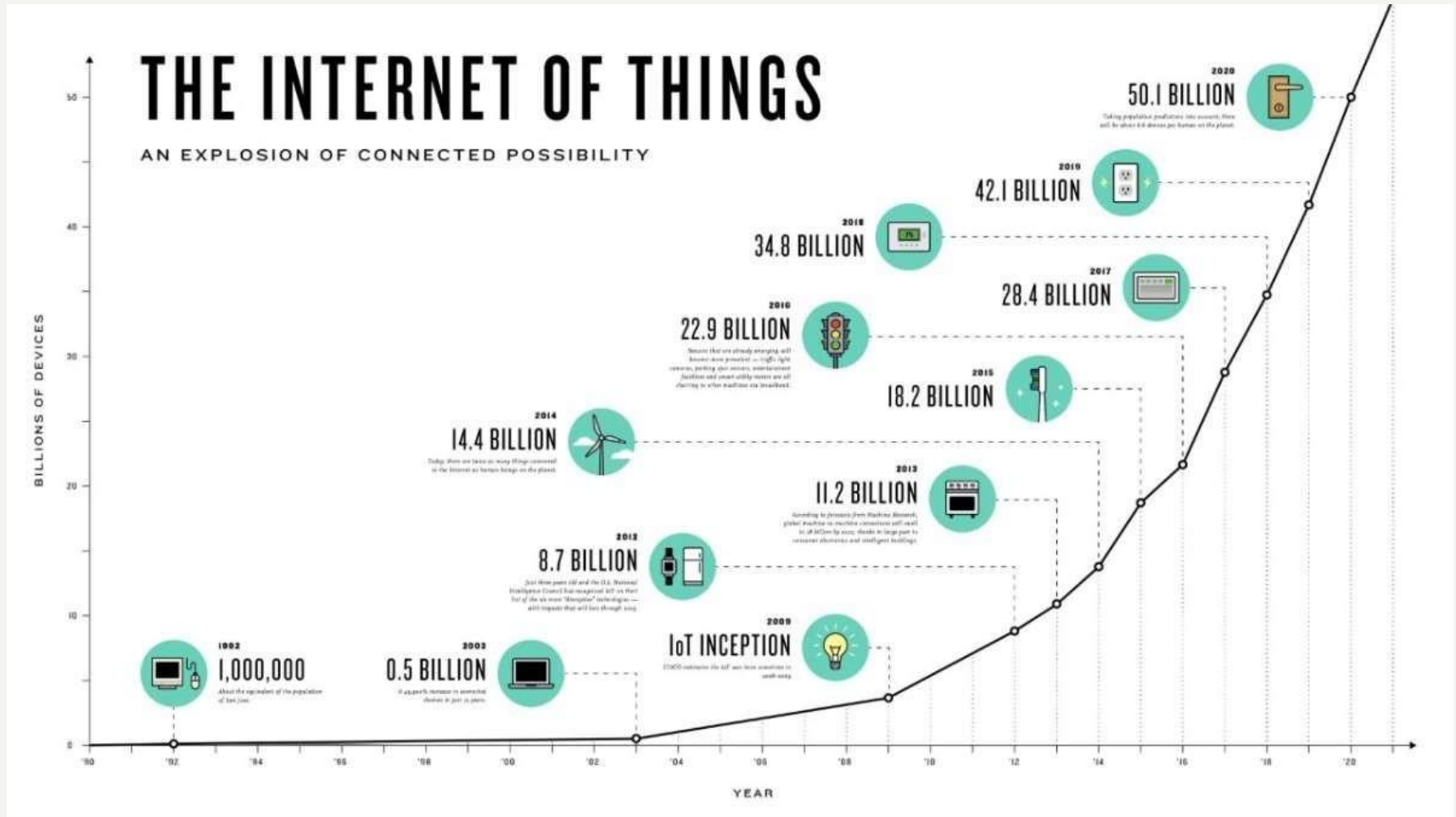


ΠΕΡΙΟΧΕΣ ΥΨΗΛΟΥ ΡΙΣΚΟΥ

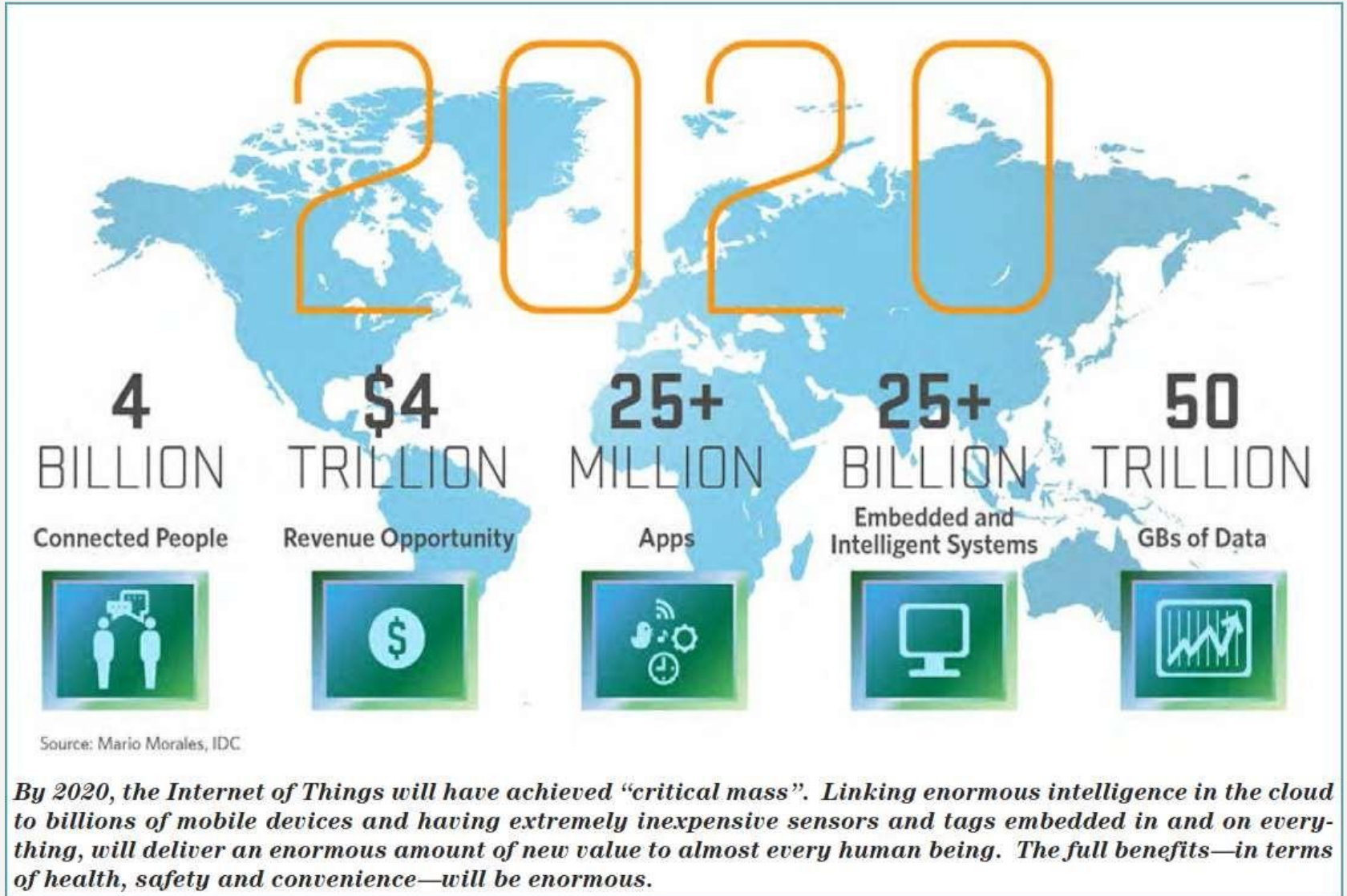
– Κρίσιμες περιοχές (Kaspersky Lab):

- **Desktops and laptops** συνδεδεμένα σε mobile δίκτυα αυξάνουν τον κίνδυνο προσβολής.
- **Bring Your Own Device (BYOD)** που χρήστες έχουν πρόσβαση σε ευαίσθητα δεδομένα από προσωπικές συσκευές, κινητά, tablets κτλ χωρίς τον απαραίτητο έλεγχο.
- Το μέγεθος του IoT μεγαλώνει εκθετικά και τόσο γρήγορα που είναι αδύνατον να επιβλέπονται όλες οι συσκευές ορθώς και πλήρως.

ΣΥΣΚΕΥΕΣ ΙΟΤ - 1



ΣΥΣΚΕΥΕΣ ΙΟΤ - 2



ΣΥΣΚΕΥΕΣ ΙΟΤ - 3



IoT Analytics – Quantifying the connected world

Applications

Overall popularity (and selected examples)

Scores

Rank	Application	Overall popularity (and selected examples)	Searches ¹	Tweets ²	LinkedIn Posts ³
1	Smart Home	Smart thermostat, Connected lights, Smart fridge, Smart doorlock 100%	61k	3.3k	430
2	Wearables	Smart watch, Activity tracker, Smart glasses 63%	33k	2.0k	320
3	Smart City	Smart parking, Smart waste management 34%	41k	0.5k	80
4	Smart grid	Smart metering 28%	41k	0.1k	60
5	Industrial internet	Remote asset control 25%	10k	1.7k	30
6	Connected car	Remote car control 19%	5k	1.2k	50
7	Connected Health	6%	2k	0.5k	5
8	Smart retail	2%	1k	0.2k	1
9	Smart supply chain	2%	0k	0.2k	0
10	Smart farming	1%	1k	0.0k	1

1. Monthly worldwide Google searches for the application 2. Monthly Tweets containing the application name and #IOT 3. Monthly LinkedIn Posts that include the application name. All metrics valid for Q4/2014.

Sources: Google, Twitter, LinkedIn, IoT Analytics

ΑΠΕΙΛΕΣ ΣΤΟ ΙΟΤ -1

– Top 7 Mobile Security Threats by Kaspersky Lab

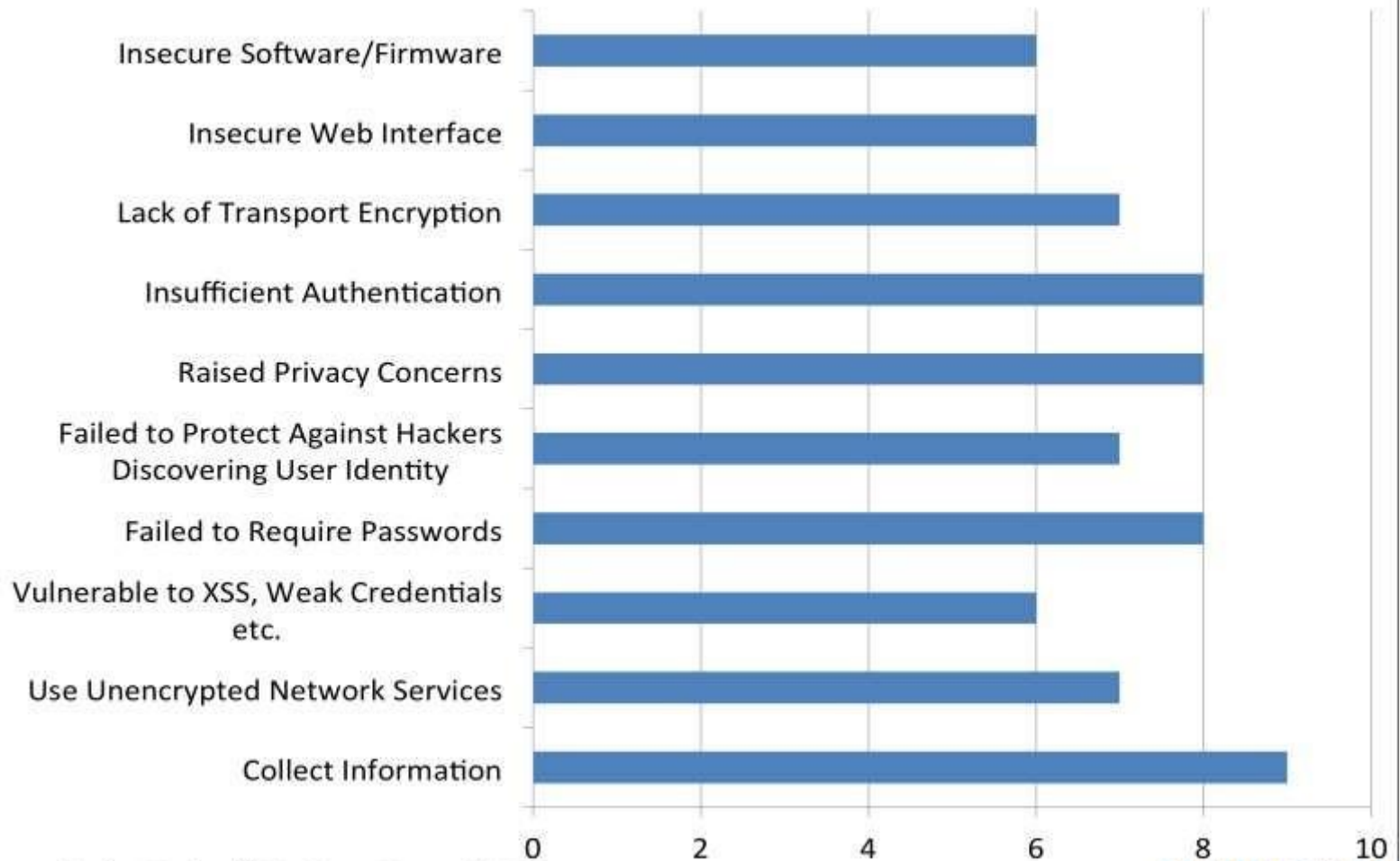
1. Data Leakage
2. Unsecured Wi-Fi
3. Network Spoofing
4. Phishing Attacks
5. Spyware
6. Broken Cryptography
7. Improper Session Handling

– Top επιθέσεις σε συσκευές ΙΟΤ

1. Default, εύκολα hardcoded συνθηματικά.
2. Firmware και OS δύσκολο να βελτιωθούν
3. Έλλειψη υποστήριξης από παραγωγό
4. Ευπαθή web interfaces (SQL injection, XSS)
5. Προγραμματιστικά λάθη (buffer overflow)
6. Clear text πρωτόκολλα
7. DoS / DDoS
8. Φυσική κλοπή ή tampering.

ΑΠΕΙΛΕΣ ΣΤΟ ΙΟΤ -2

Security Flaws Of Top 10 IoT Devices



Source: Hewlett Packard's Fortify on Demand, 2014

BI INTELLIGENCE

ΑΠΕΙΛΕΣ – CASE STUDIES

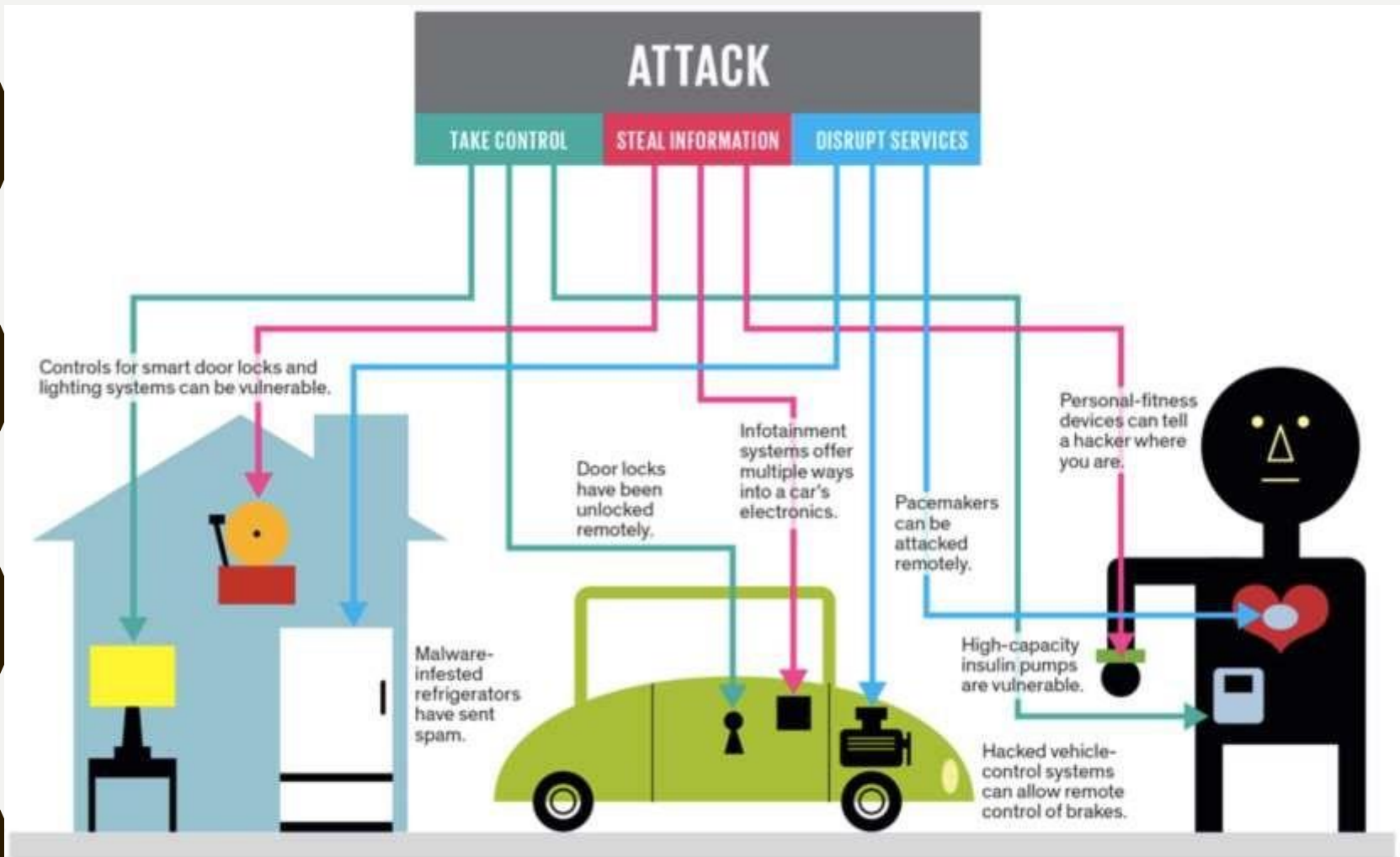


Illustration: J. D. King

CASE STUDY: TRANE

- Εντοπίστηκε διασυνδεδεμένος **θερμοστάτης** με ευπάθειες που επέτρεπαν πρόσβαση στο εσωτερικό δίκτυο (Cisco Talos group)
- Χρειάστηκε **12** μήνες για patch που διόρθωνε 2 ευπάθειες
- **21** μήνες για διόρθωση μίας ευπάθειας
- Ιδιοκτήτες συσκευών συχνά **αγνοούν** ότι υπάρχουν updates και δεν τα εγκαθιστούν.



IOT GONE MEDICAL



MRI Device Hacked to Access Patient Information

Researcher “able to hack into the hospital's network with ease – [and permission – with vulnerable medical devices listed on Shodan.](#)”-*International Business Times, Feb 2006*

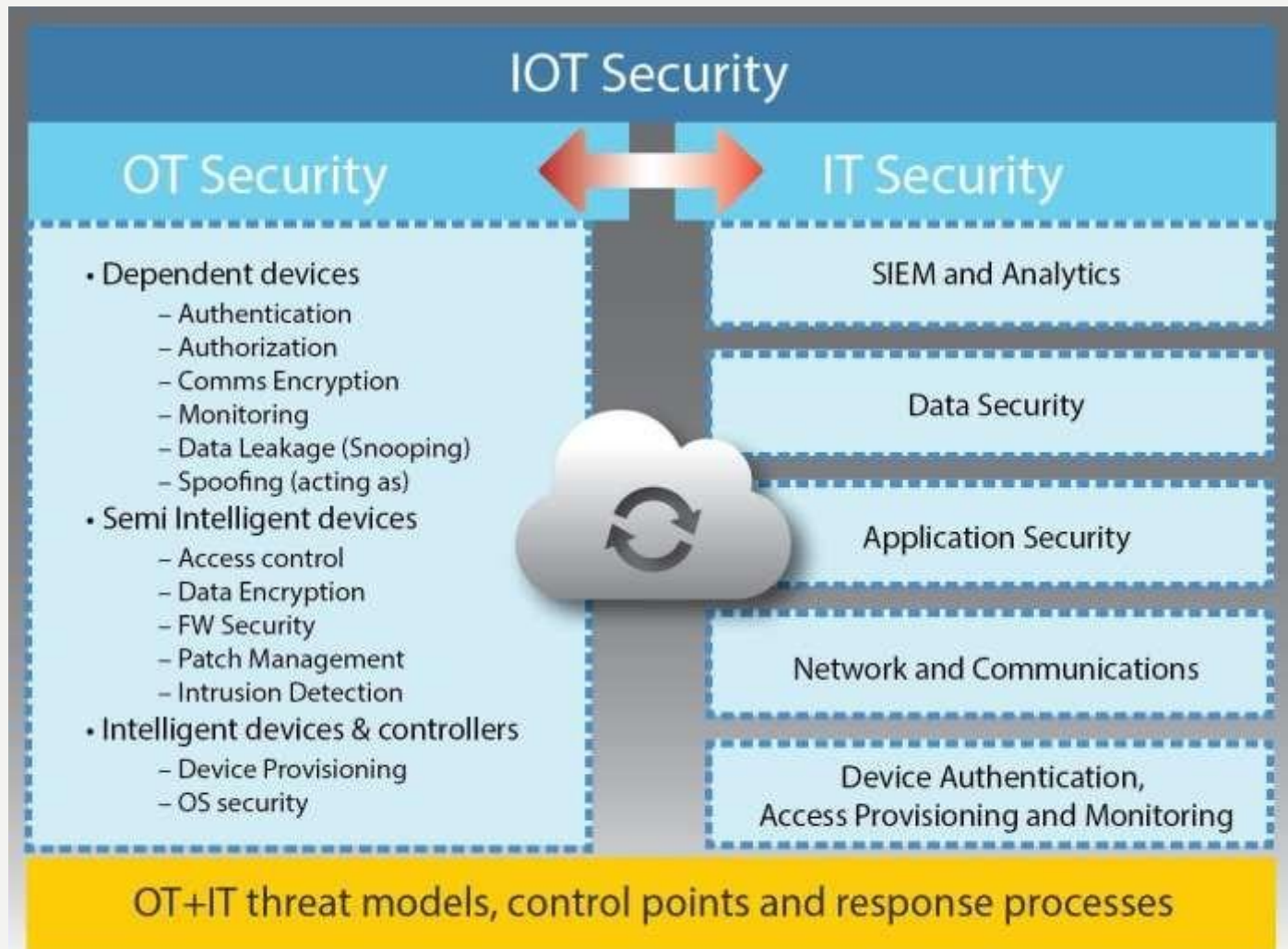
Infusion Pump Hacked to Administer Fatal Drug Dose

Security Professionals “showed how easy it is for hackers to take control of a hospital drug infusion pump by overwriting the device’s firmware with malicious software. The hack would allow someone to remotely administer a fatal drug dose.”

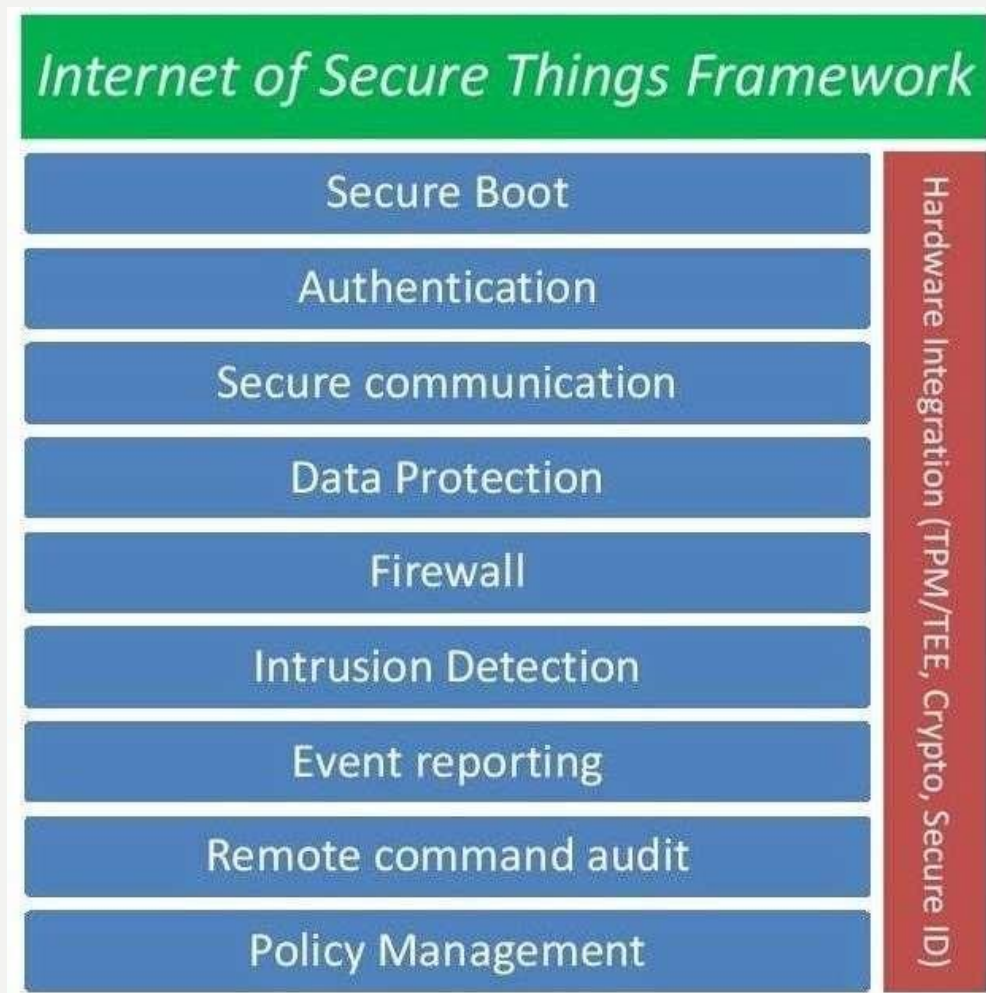
WIRED

Aug 12, 2015

ΑΡΧΕΣ ΑΣΦΑΛΕΙΑΣ ΙΟΤ



ΜΕΤΡΑ & ΤΕΧΝΟΛΟΓΙΕΣ ΑΣΦΑΛΕΙΑΣ



References

1. Pipyros K., Thraskias C., Mitrou L., Gritzalis D., Apostolopoulos T., "A new strategy for improving cyber-attacks evaluation in the context of Tallinn manual", *Computers & Security* (Special Issue), 2017.
2. Tsalis N., Mylonas A., Nisioti A., Gritzalis D., Katos V., "Exploring the protection of private browsing in desktop browsers", *Computers & Security*, Vol. 67, pp. 181-197, 2017.
3. Pipyros K., Mitrou L., Gritzalis D., Apostolopoulos T., "Cyberoperations and International Humanitarian Law: A review of obstacles in applying International Law rules in Cyber Warfare", *Information & Computer Security*, Vol. 24, No. 1, pp. 38-52, 2016.
4. Soupionis Y., Koutsiamanis A.-R., Efraimidis P., Gritzalis D., "A game-theoretic analysis of preventing spam over Internet Telephony with audio CAPTCHA-based authentication", *Journal of Computer Security*, Vol. 22, No. 3, pp. 383-413, 2014.
5. Mylonas A., Meletiadiis V., Mitrou L., Gritzalis D., "Smartphone sensor data as digital evidence", *Computers & Security* (Special Issue: Cybercrime in the Digital Economy), Vol. 38, pp. 51-75, October 2013.
6. Mylonas A., Kastania A., Gritzalis D., "Delegate the smartphone user? Security awareness in smartphone platforms", *Computers & Security*, Vol. 34, No. 3, pp. 47-66, May 2013.
7. Pipyros K., Thraskias C., Mitrou L., Gritzalis D., Apostolopoulos T., "Cyber-attacks evaluation using a simple additive weighting method on the basis of Schmitt's analysis", in *Proc. of the 10th Mediterranean Conference on Information Systems* (MCIS-2016), AISel, Cyprus, 2016.
8. Virvilis N., Tsalis N., Mylonas A., Gritzalis D., "Mobile devices: A phisher's paradise", in *Proc. of the 11th International Conference on Security and Cryptography*, pp. 79-87, ScitePress, Austria, 2014.
9. Pipyros K., Mitrou L., Gritzalis D., Apostolopoulos T., "A cyber attack evaluation methodology", in *Proc. of the 13th European Conference on Cyber Warfare and Security*, pp. 264-270, ACPI, Greece, 2014.
10. Pierrakakis K., Kandias M., Gritzali C., Gritzalis D., "3D Printing and its regulation dynamics: The world in front of a paradigm shift", in *Proc. of the 6th International Conference on Information Law and Ethics*, Law Library Publications, Greece, 2014.
11. Virvilis N., Gritzalis D., "Trusted Computing vs. Advanced Persistent Threats: Can a defender win this game?", in *Proc. of 10th IEEE International Conference on Autonomic and Trusted Computing*, pp. 396-403, IEEE Press, Italy, 2013.
12. Virvilis N., Gritzalis D., "The Big Four - What we did wrong in Advanced Persistent Threat detection?", in *Proc. of the 8th International Conference on Availability, Reliability & Security* (ARES-2013), pp. 248-254, IEEE, Germany, 2013.
13. http://www.internet-of-things-research.eu/pdf/Converging_Technologies_for_Smart_Environments_and_Integrated_Ecosystems_IERC_Book_Open_Access_2013.pdf
14. http://www.cisco.com/c/dam/en_us/solutions/trends/iot/introduction_to_IoT_november.pdf
15. <http://www.vs.inf.ethz.ch/publ/papers/Internet-of-things.pdf>
16. http://madsg.com/wp-content/uploads/2015/12/Designing_the_Internet_of_Things.pdf
17. <http://mattturck.com/wp-content/uploads/2016/03/Internet-of-Things-2016.png>