Internet-of-Everything: No mercy for digital devices

Dimitris Gritzalis

March 2021

Στόχος μου η ζωή και όχι η ζωή μου στόχος!

Internet of Everything: No mercy for digital devices

18 ΑΝΟ
Στόχος μου η ζωή και όχι η ζωή μου στόχος!

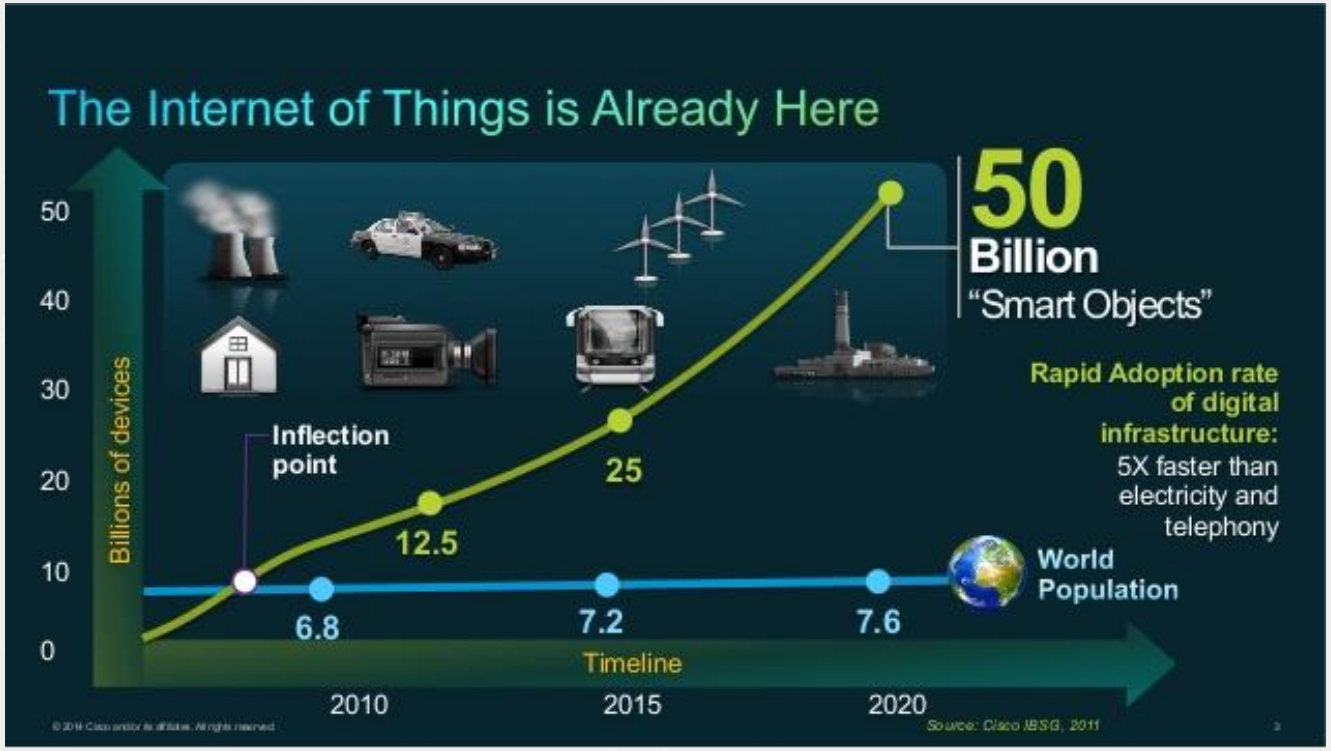
Διάλεξη, Μάρτης 2021

Dimitris Gritzalis

Professor of CyberSecurity & **Director**, M.Sc. Programme in Information Systems Security
Dept. of Informatics, Athens University of Economics & Business
dgrit@aueb.gr | www.infosec.aueb.gr

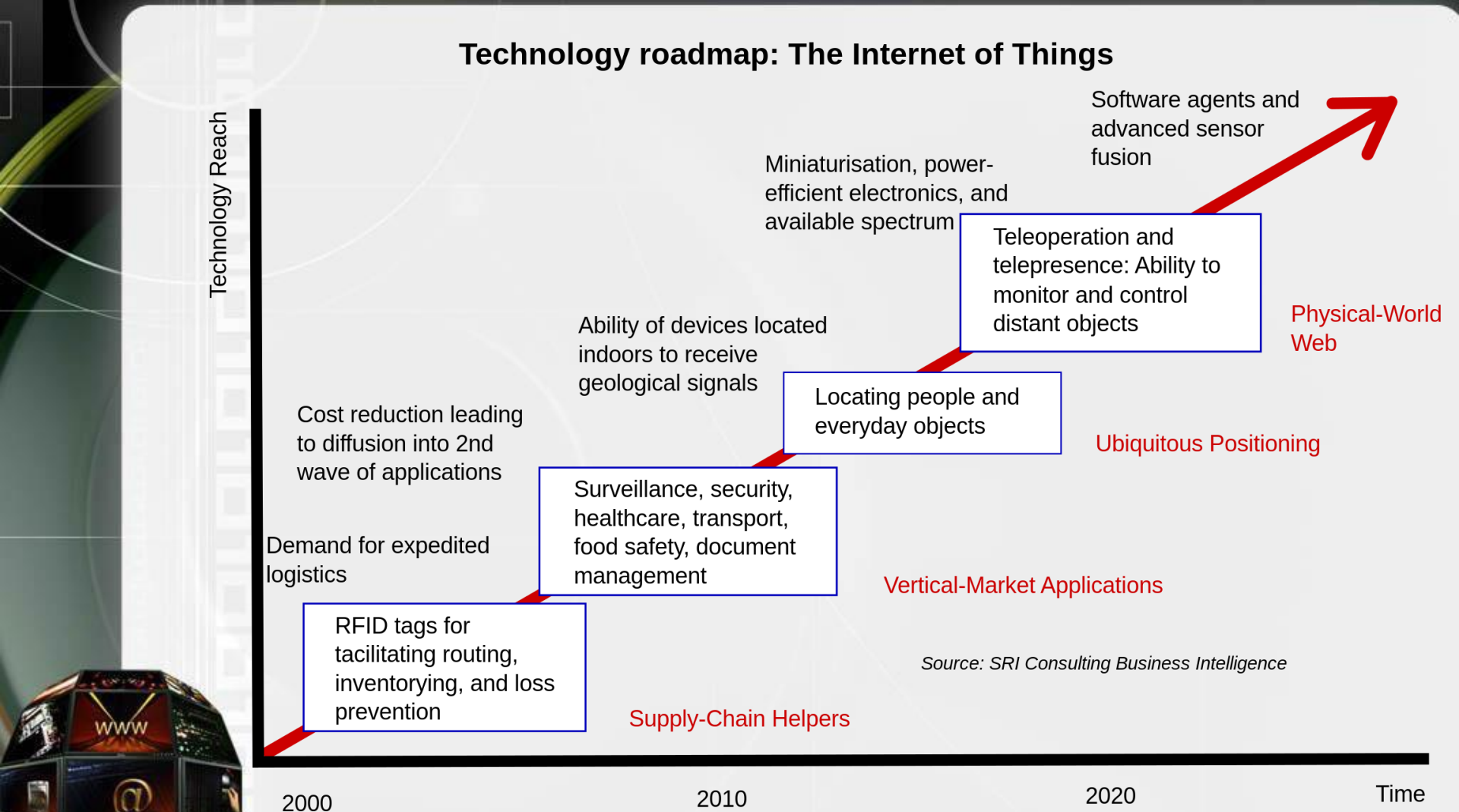
ΟΠΑ AUEB

Διαδίκτυο των ~~Αντικειμένων~~ Πάντων (Internet of ~~Things~~ Everything)



Το Διαδίκτυο των Αντικειμένων (Internet of Things) αποτελείται από διασυνδεδεμένες συσκευές, οχήματα, κτίρια και άλλα αντικείμενα - στα οποία είναι ενσωματωμένα ηλεκτρονικά, λογισμικό, αισθητήρες, ενεργοποιητές και δυνατότητες δικτυακής συνδεσιμότητας - που επιτρέπουν στα αντικείμενα αυτά να συλλέγουν και να ανταλλάσσουν δεδομένα. Το IoT είναι η υποδομή της Κοινωνίας της Πληροφορίας.

Internet of ~~Things~~ Everything



Κάποιες μη «συμβατικές» επιθέσεις

Επιχείρηση Aurora

Στόχος και θύμα οι ...παραδοσιακές μηχανές.

Εμφυτεύματα σε ανθρώπους

Επιθέσεις που μπορούν να προκαλέσουν το θάνατο!

Εκτυπωτής Laser

Δεδομένα που στέλνονται στον εκτυπωτή και ...διαρρέουν.

Κρυπτοσύστημα RSA

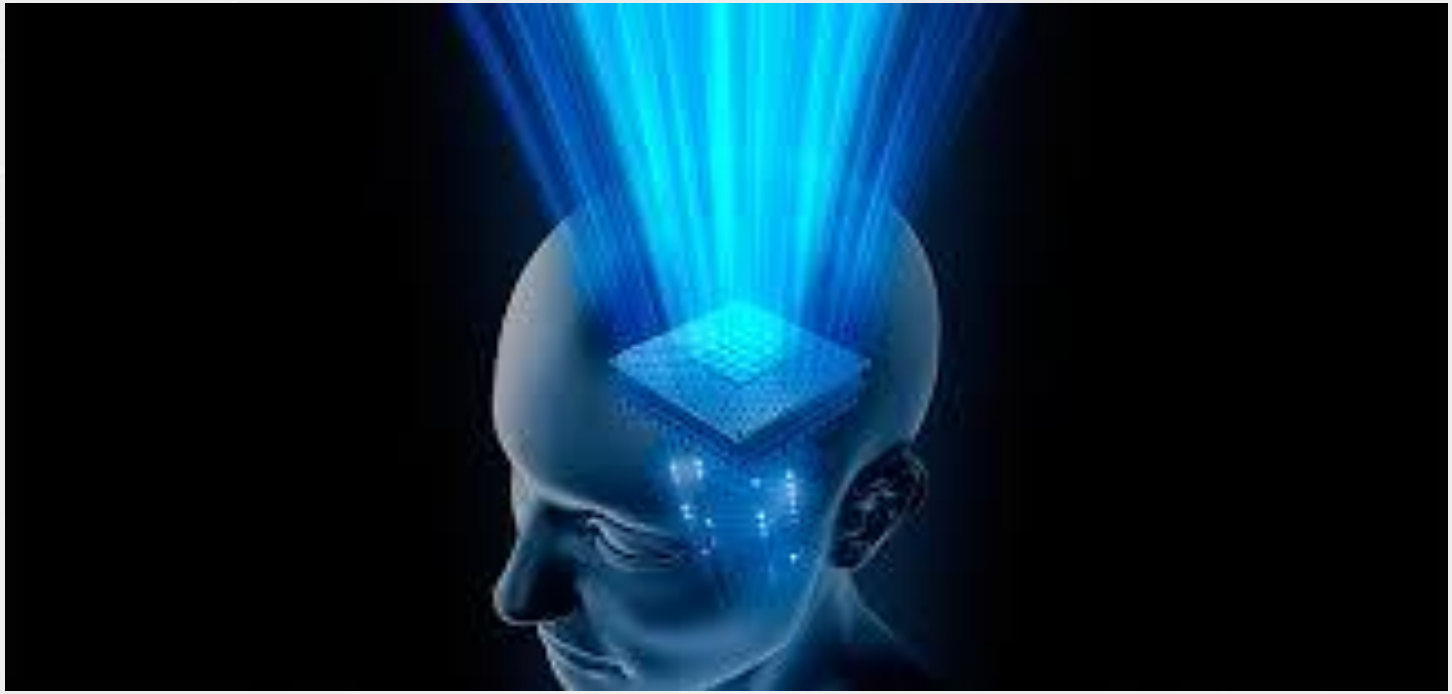
Το «Άγιο Δισκοπότηρο» των κρυπτοσυστημάτων; Όχι πια!

Κινητά τηλέφωνα

Αν ακούτε μουσική, κινδυνεύετε από ιομορφές...

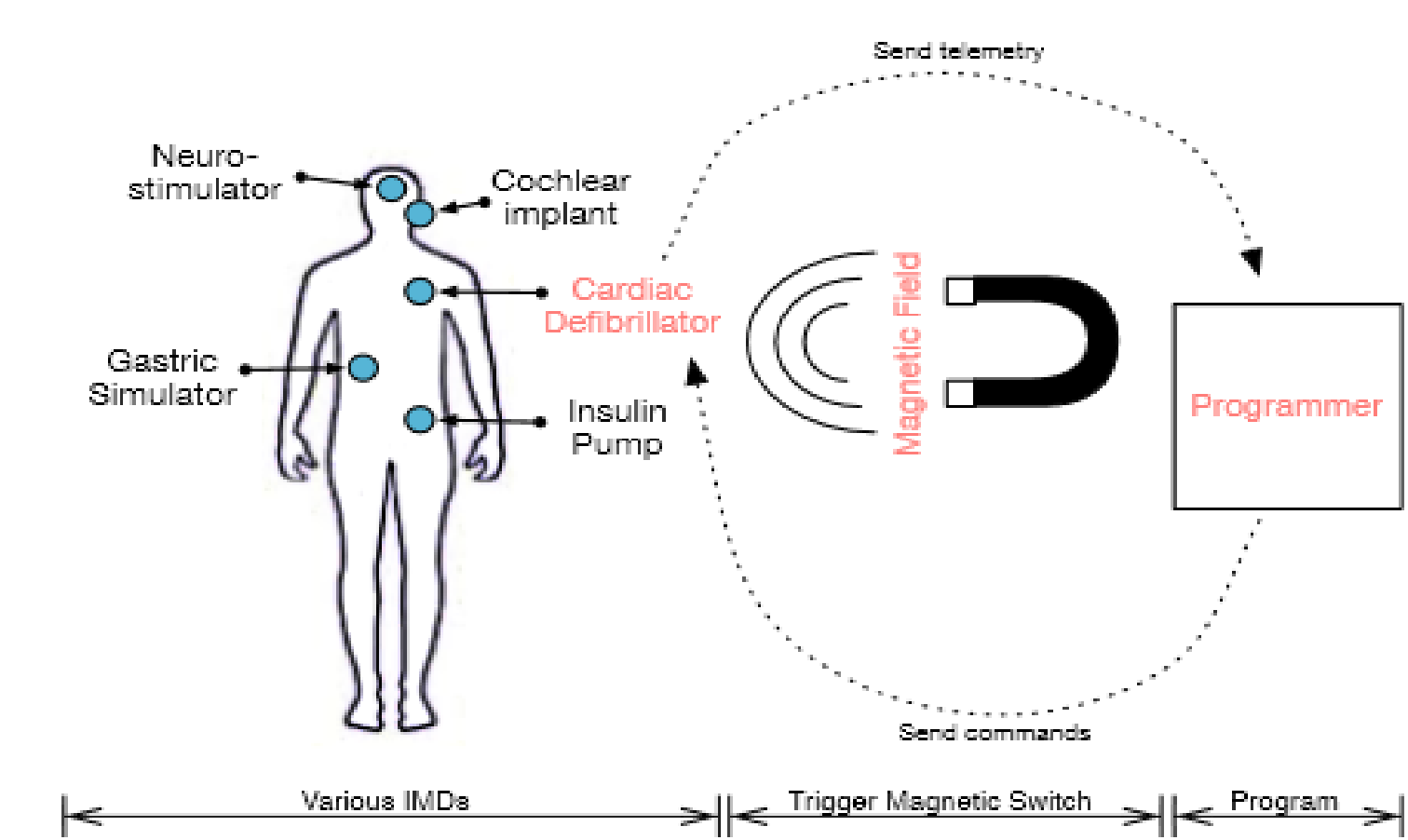
Επιχείρηση Aurora

Εμφυτεύματα σε ανθρώπους
(Implantable Medical Devices)



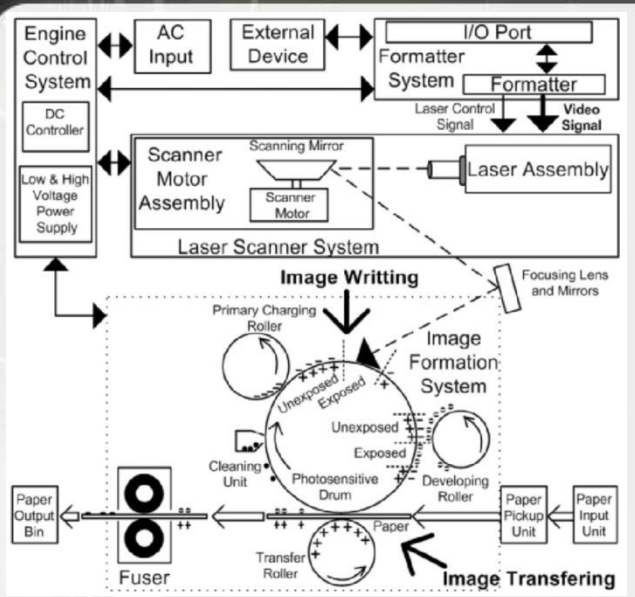
«Χακάροντας» εμφυτεύματα...

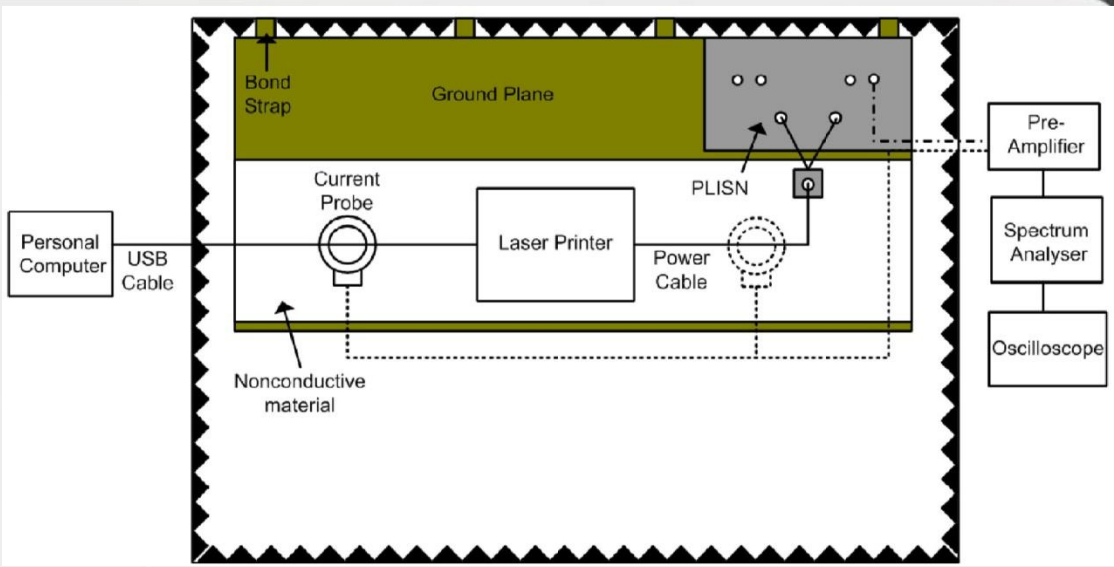
IMD: Implantable Medical Devices
ICD: Implantable Cardiac Defibrillator

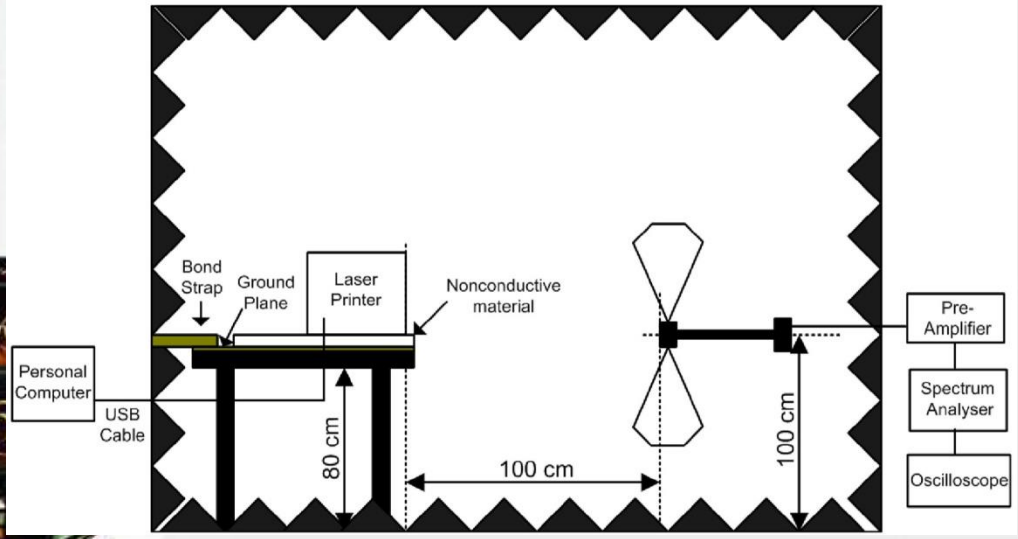


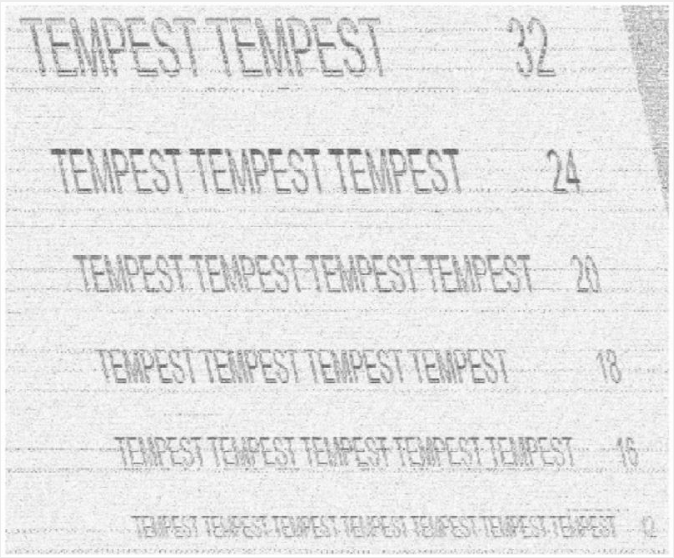
Ένας «αθώος» εκτυπωτής laser

«Χακάροντας» έναν εκτυπωτή laser









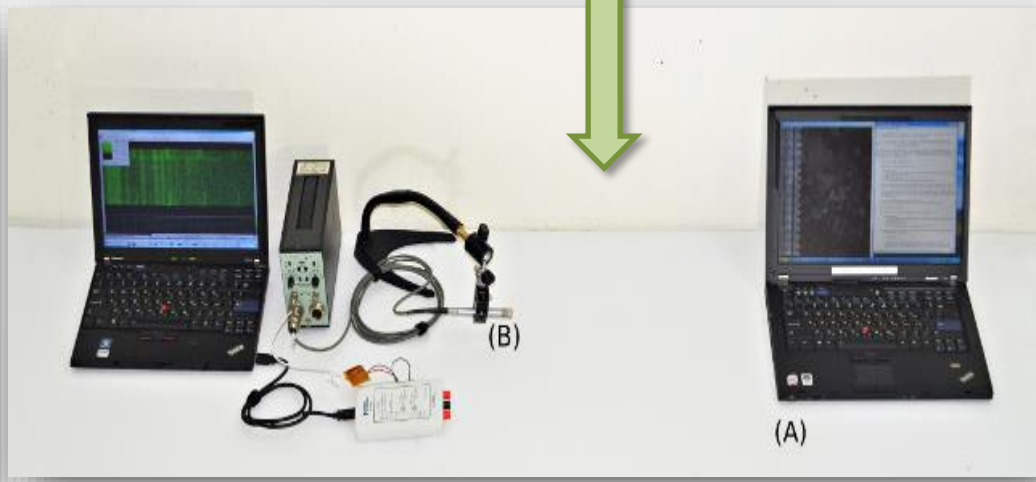
Το εμβληματικό κρυπτοσύστημα RSA

«Χακάροντας» το RSA

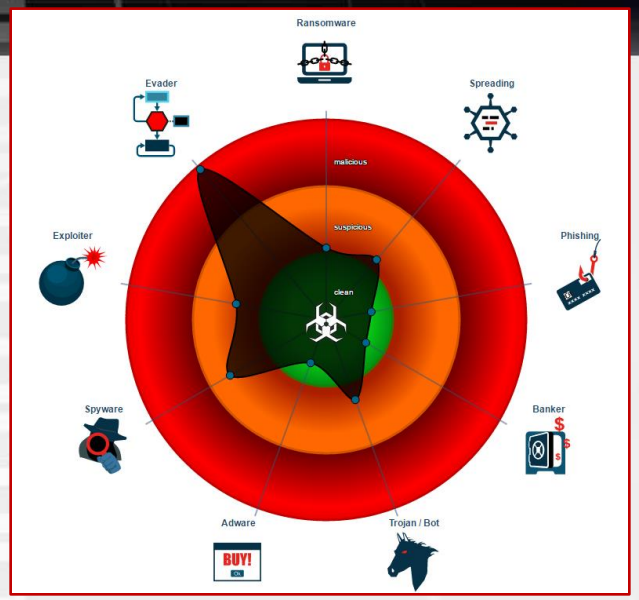
Η επίθεση με **κινητό τηλέφωνο** γίνεται με χρήση ενός *συνηθισμένου* τηλεφώνου, 30cm από ένα laptop

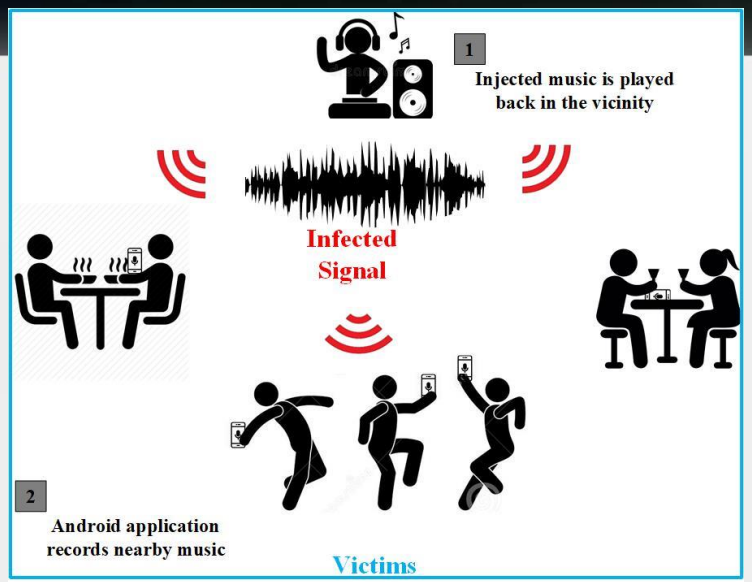
Η επίθεση με **ευαίσθητο μικρόφωνο** γίνεται με τοποθέτηση:

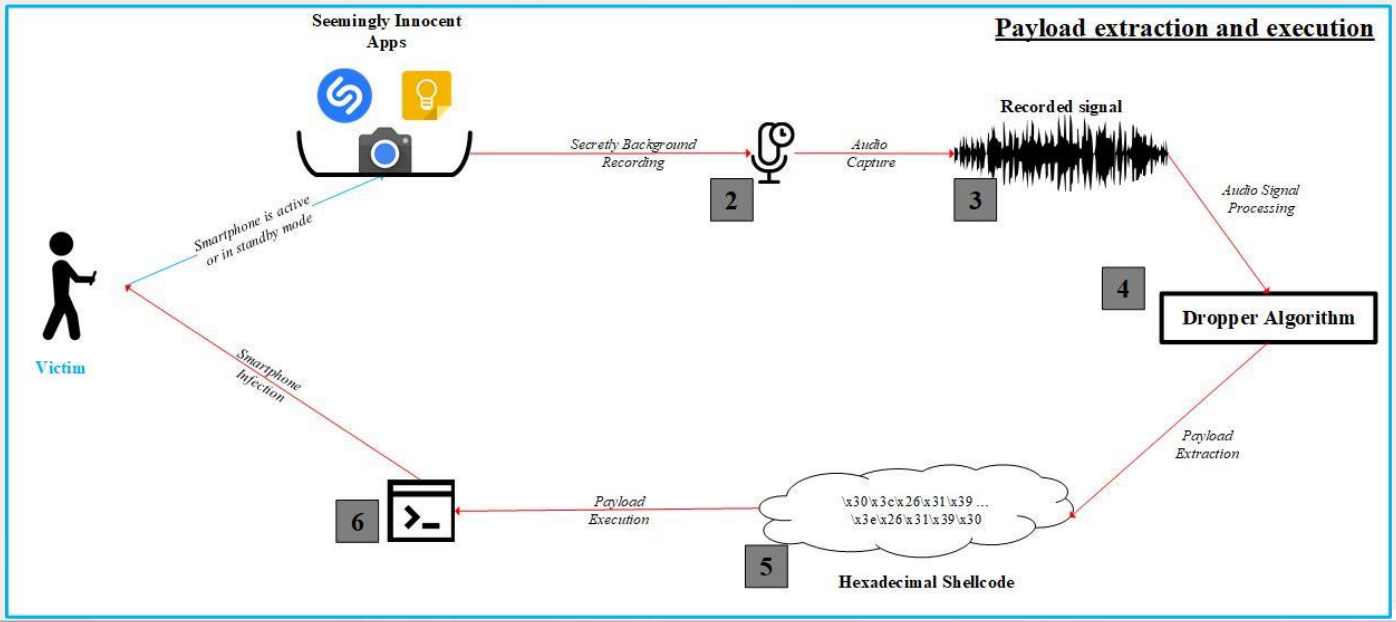
- *Παραβολικού* ευαίσθητου μικροφώνου 4m από το laptop
- *Απλού* ευαίσθητου μικροφώνου 1m από το laptop



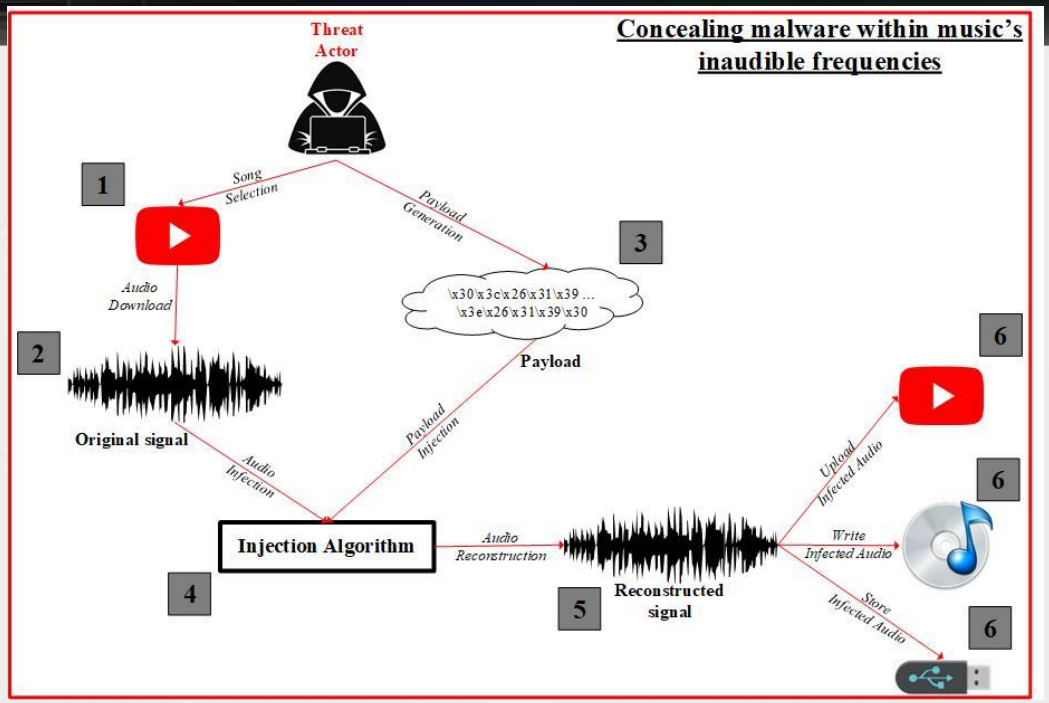
«Χακάροντας» κινητά μετά Μουσικής…

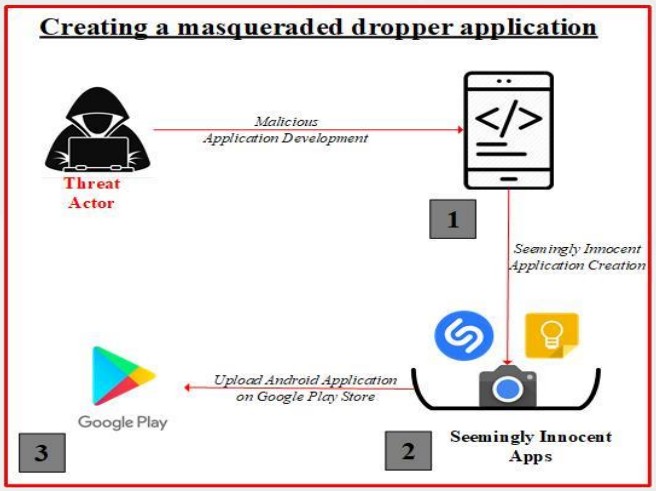


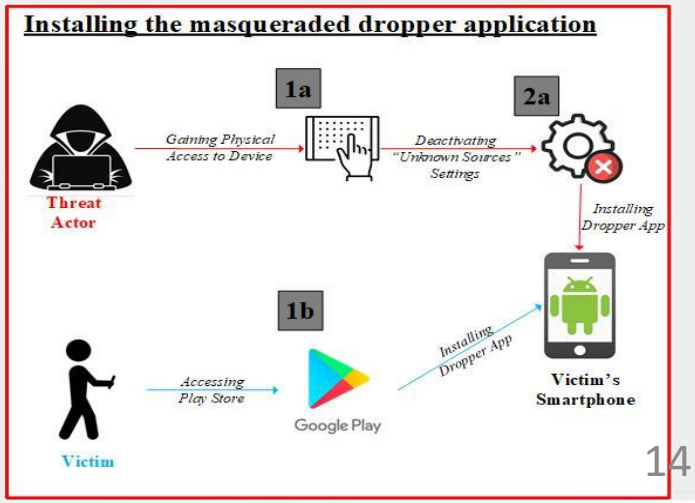




Από την ηχητική απόλαυση στη «μόλυνση»...







"Tears without action are irrelevant"

Κάθε ψηφιακή συσκευή μπορεί να «χακαριστεί»…

- ✓ **…με τον ένα ή τον άλλο τρόπο,**
- ✓ **...αργά ή γρήγορα,**
- ✓ **...απ' όσους έχουν κίνητρο και τεχνογνωσία.**

Ποιά είναι η προσωπική μας ευθύνη;

Ποιό είναι το προσωπικό μας καθήκον;

(...άκουσα κάτι για "δικαιώματα";)

References

1. Genkin D., Shamir A., Tromer E., “RSA key extraction via low-bandwidth acoustic cryptanalysis”, in *Advances in Cryptology* (CRYPTO 2014), pp. 444-461, Springer (LNCS 8616), 2014.
2. Mylonas, A., Dritsas, S., Tsoumas, B., Gritzalis, D., “Smartphone security evaluation: The malware attack case”, in *International Conference on Security and Cryptography*, pp. 25-36, IEEE, 2011.
3. Mylonas, A., Theoharidou, M., Gritzalis, D., “Assessing privacy risks in android: A user-centric approach”, in *International Workshop on Risk Assessment and Risk-driven Testing*, pp. 21-37, Springer, 2013.
4. Mylonas A., Tsalis N., Gritzalis D., "Hide and seek: On the disparity of browser security settings“, *9th Symposium on Usable Privacy and Security*, United Kingdom, 2013.
5. Rushanan M., Rubin A., Kune D., Swanson C., “SoK: Security and Privacy in Implantable Medical Devices and Body Area Networks”, in *Proc. of the 2014 IEEE Symposium on Security and Privacy*, pp. 524-539, IEEE Press, USA, 2014.
6. Stergiopoulos G., Gritzalis D., Anagnostopoulou A., Vasilellis E., “Dropping malware through sound injection: A comparative analysis on Android operating systems”, *Computers & Security*, vol. 105(102228), 2021.
7. Theoharidou, M., Kandias, M., Gritzalis, D., “Securing transportation-critical infrastructures: Trends and perspectives”, *7th IEEE Conference on Global Security, Safety and Sustainability*, pp. 171-178, Springer, 2012.
8. Ulaş C., Aşık U., Karadeniz C., “Analysis and reconstruction of laser printer information leakages in the media of electromagnetic radiation, power and signal lines”, *Computers & Security*, vol. 58, pp. 250-267, 2016.
9. 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.
10. 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.
11. 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*, pp. 248-254, IEEE, Germany, 2013.
12. Dritsas S., Tsoumas B., Dritsou V., Konstantopoulos P., Gritzalis D., “OntoSPIT: SPIT Management through Ontologies”, *Computer Communications*, vol. 32, no. 2, pp. 203-212, 2009.
13. Homeland Security News Wire**,** *“Wireless implantable medical devices vulnerable to hacking”***,** March 19, 2015 http://www.homelandsecuritynewswire.com/dr20150319-wireless-implantable-medical-devices-vulnerable-to-hacking