



Smart cars: Enhancing security and privacy through innovative technologies

Dimitris Gritzalis

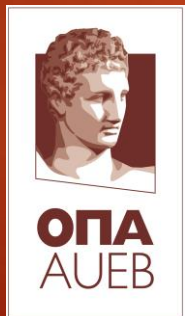
October 2014



5^ο Φεστιβάλ Βιομηχανικής Πληροφορικής
Καβάλα, Οκτώβρης 2014



Έξυπνα αυτοκίνητα: Καινοτομίες για περισσότερη ασφάλεια και ιδιωτικότητα



Καθηγητής Δημήτρης Γκρίτζαλης

Εργαστήριο Ασφάλειας Πληροφοριών & Προστασίας Κρίσιμων Υποδομών

(INFOSEC Laboratory, www.infosec.aueb.gr)

Τμήμα Πληροφορικής, Οικονομικό Πανεπιστήμιο Αθηνών

Πίνακας περιεχομένων

- Έξυπνα αυτοκίνητα
- Τεχνολογική εξέλιξη
- Κίνητρα αξιοποίησης δεδομένων
- Παράγοντες επικινδυνότητας
 - Διάσπαση προσοχής
 - Ζητήματα ιδιωτικότητας
 - Hacking
- Διαχείριση επικινδυνότητας έξυπνων αυτοκινήτων
- Μερικά βασικά συμπεράσματα

Smart car: Δεν εννοούμε αυτό...



Smart car: Εννοούμε αυτό!



Έξυπνα αυτοκίνητα

- ❑ Το αυτοκίνητο μετατρέπεται ταχέως σε έναν κινούμενο κόμβο παραγωγής - λήψης - μετάδοσης - επεξεργασίας δεδομένων
- ❑ Το έξυπνο αυτοκίνητο αποτελείται από ένα δίκτυο εξελιγμένων εφαρμογών, συνδεδεμένων μεταξύ τους, αλλά και με το Internet
 - Καταγραφή/αναφορά θεμάτων θαλάμου επιβατών και χρήσης του αυτοκινήτου
 - Διαχείριση λειτουργιών οχήματος (πέδηση, στάθμευση, αλλαγή πορείας κλπ.)
 - Ενσωματωμένο σύστημα πλοήγησης, επικοινωνίας, ενημέρωσης και ψυχαγωγίας

Τεχνολογική εξέλιξη

- ❑ Χρήση πληθώρας (~50) Ηλεκτρονικών Μονάδων Ελέγχου (ECU)
- ❑ Ως το 2017, ποσοστό >60% των νέων οχημάτων σε όλο τον κόσμο αναμένεται να έχουν δυνατότητες συνδεσιμότητας [1]
- ❑ Ενσωμάτωση λογισμικού, όπως:
 - Λειτουργικό σύστημα iOS (Apple) για ενσωμάτωση των συσκευών (iPhone, iPad) του οδηγού και των επιβατών στο όχημα
 - Λειτουργικό σύστημα Android, που επιτρέπει στον οδηγό πρόσβαση σε δεδομένα κίνησης, χαρτών, ψυχαγωγίας κλπ. (πχ. μέσω Google)
 - Google: Το ίδιο το αυτοκίνητο γίνεται μια συνδεδεμένη συσκευή Android

Τεχνολογική εξέλιξη

- ❑ **Wearables:** Συσκευές όπως γυαλιά ή ρολόγια που φοράει ο οδηγός για τη λήψη ή μετάδοση πληροφορίας
 - Παροχή τέτοιων συσκευών στους οδηγούς (BMW, Mercedes, Hyundai κ.ά.)
 - Αύξηση των επιπέδων και της έντασης της αλληλεπίδρασης οχήματος-οδηγού
- ❑ **Διασύνδεση:** Επικοινωνία με οχήματα και υποδομές μεταφορών
 - Στόχος η ανάπτυξη ενός πλήρους διασυνδεδεμένου συστήματος μεταφορών που θα αποτελείται από μια πλατφόρμα από τεχνολογίες, διεπαφές και διαδικασίες
 - Σκοπός οι ασφαλείς, σταθερές, διαλειτουργικές και αξιόπιστες λειτουργίες, που θα ελαχιστοποιούν τον κίνδυνο προβλημάτων στις μεταφορές [2]

Κίνητρα αξιοποίησης δεδομένων



Δυνατότητα εντοπισμού μορφότυπων οδήγησης και επιβολής ενεργειών εποπτείας του οδηγού από ασφαλιστικές εταιρείες και κυβερνητικούς ή ιδιωτικούς φορείς για την αντιμετώπιση μη ασφαλών συμπεριφορών



Παρακολούθηση στόλου οχημάτων, καθώς και μορφότυπων οδήγησης και δρομολόγησης για μείωση του κόστους καυσίμων, συντήρησης και ασφαλίσεων



Αποθάρρυνση των υπαλλήλων-οδηγών ενός οργανισμού από τη χρήση των οχημάτων του οργανισμού για προσωπικούς σκοπούς



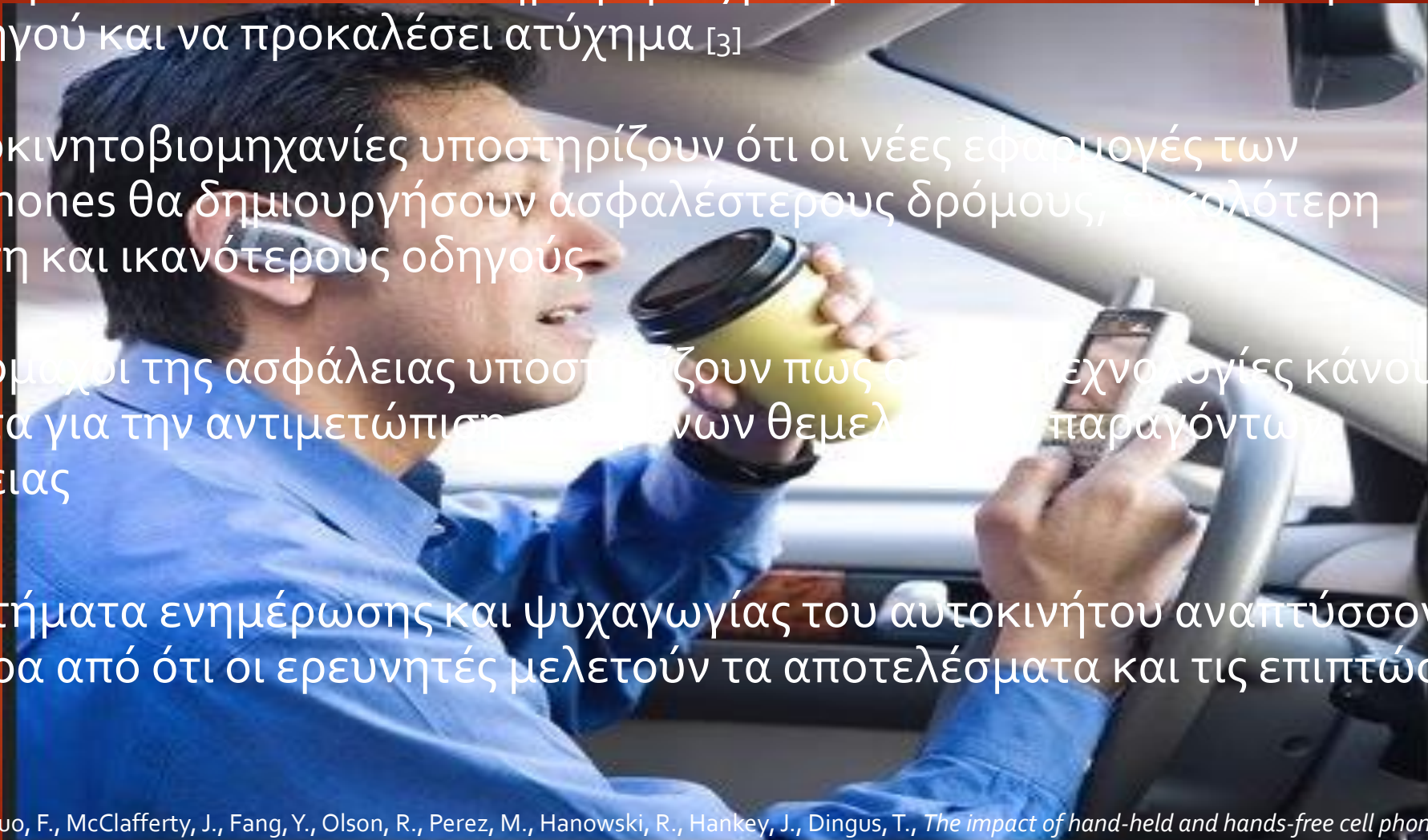
Τα δεδομένα του οχήματος μπορούν να διατεθούν στους ασφαλιστικούς φορείς για τη βελτίωση των χρεώσεων των ασφαλιστικών καλύψεων



Η τεχνολογία μπορεί να συμβάλλει αποφασιστικά στον εντοπισμό και την ανάκτηση κλεμμένων οχημάτων

Διάσπαση της προσοχής του οδηγού

- ❑ Ένα περιβάλλον πλούσιο σε πληροφορίες μπορεί να αποσπάσει την προσοχή του οδηγού και να προκαλέσει ατύχημα [3]
- ❑ Οι αυτοκινητοβιομηχανίες υποστηρίζουν ότι οι νέες εφαρμογές των smartphones θα δημιουργήσουν ασφαλέστερους δρόμους, καλύτερη οδήγηση και ικανότερους οδηγούς
- ❑ Οι υπέρμαχοι της ασφάλειας υποστηρίζουν πως οι τεχνολογίες κάνουν ελάχιστα για την αντιμετώπιση των ανων θεμελιωδών παραγόντων ασφάλειας
- ❑ Τα συστήματα ενημέρωσης και ψυχαγωγίας του αυτοκινήτου αναπτύσσονται ταχύτερα από ότι οι ερευνητές μελετούν τα αποτελέσματα και τις επιπτώσεις τους



Διάσπαση της προσοχής του οδηγού

- ❑ Εθνική Υπηρεσία Οδικής Ασφάλειας (NHTSA): Κατευθυντήριες γραμμές «για την ενθάρρυνση των κατασκευαστών αυτοκινήτων να περιορίσουν τον κίνδυνο διάσπασης της προσοχής του οδηγού από τις ηλεκτρονικές συσκευές του οχήματος»



Οι οδηγοί που εμπλέκονται, ταυτόχρονα, σε πολλαπλές δραστηριότητες έχουν μειωμένη αντίδραση, συνεπώς αυξάνεται ο κίνδυνος ατυχήματος [4]



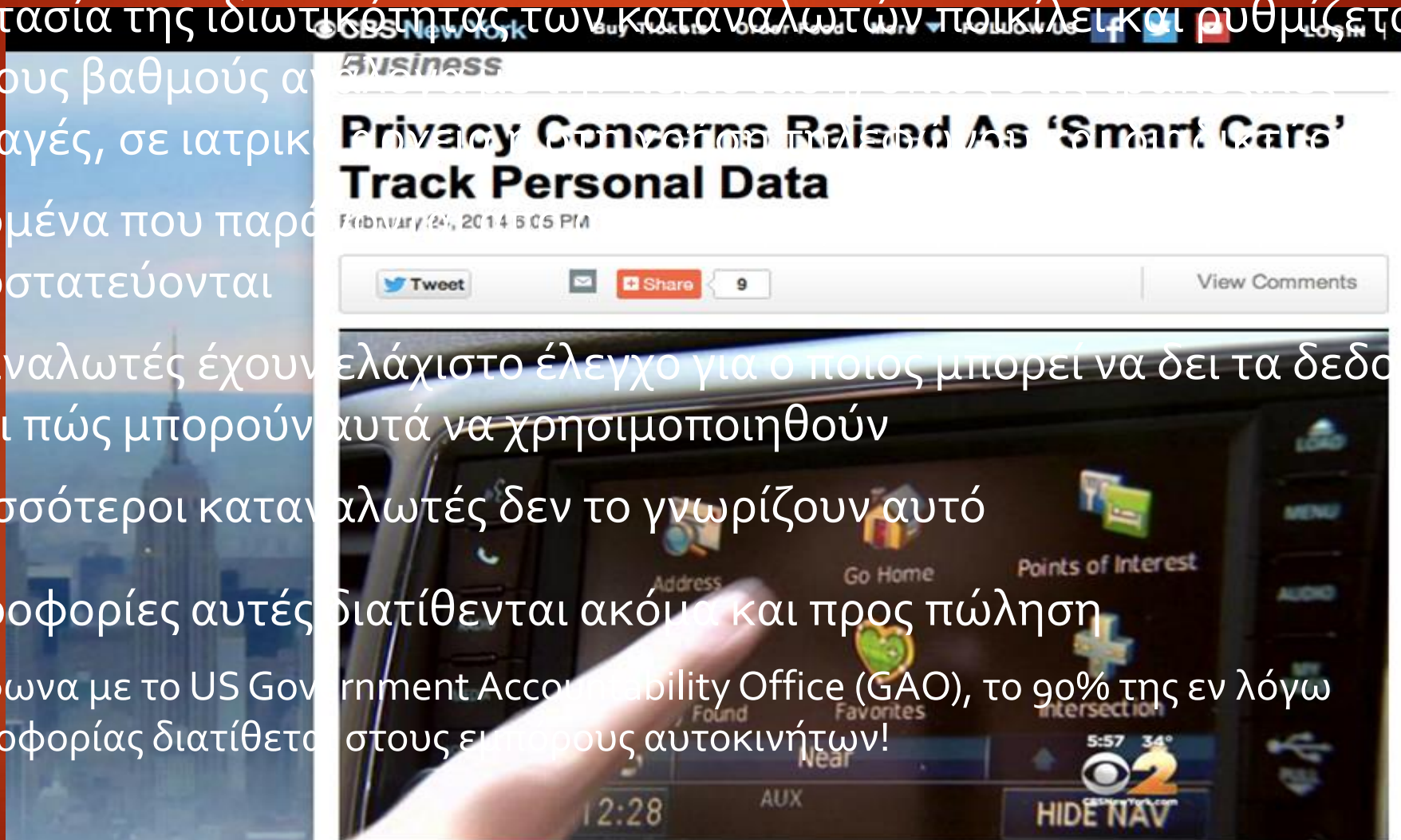
Οι κίνδυνοι διάσπασης της προσοχής του οδηγού οφείλονταν κυρίως σε οπτικούς και κινητικούς περισπασμούς. Οι ΤΠΕ μπορούν να τους μειώσουν [5]

[4] American Automobile Association & University of Utah, Think You Know All About Distracted Driving? Think Again, USA 2013.

[5] Virginia Tech Transportation Institute, New VTTI study results continue to highlight the dangers of distracted driving, USA 2013.

Ζητήματα Ιδιωτικότητας

- ❑ Η προστασία της ιδιωτικότητας των καταναλωτών ποικίλει και ρυθμίζεται σε διάφορους βαθμούς ανάλογα με τις συναλλαγές, σε ιατρικές και ασφαλιστικές.
- ❑ Τα δεδομένα που παράγονται από τις συναλλαγές δεν προστατεύονται.
- ❑ Οι καταναλωτές έχουν ελάχιστο έλεγχο για οποιος μπορεί να δει τα δεδομένα τους και πώς μπορούν αυτά να χρησιμοποιηθούν.
- ❑ Οι περισσότεροι καταναλωτές δεν το γνωρίζουν αυτό.
- ❑ Οι πληροφορίες αυτές διατίθενται ακόμα και προς πώληση.
 - Σύμφωνα με το US Government Accountability Office (GAO), το 90% της εν λόγω πληροφορίας διατίθεται στους εμπόρους αυτοκινήτων!



Ζητήματα Ιδιωτικότητας

- ❑ Τα δεδομένα που καταγράφονται από συστήματα των έξυπνων αυτοκινήτων δεν αφορούν μόνο την οδηγική συμπεριφορά [6]
- ❑ “Δεν είναι μόνο τα γενικά στοιχεία, γνωρίζουν πόσοι άνθρωποι ψωνίζουν σε αυτό το κατάστημα. Γνωρίζουν ότι είσαι εσύ, ξέρουν πού είναι κάθε άτομο την κάθε στιγμή και τι έκανε. Τα αυτοκίνητα είναι πλέον σε θέση να εντοπίζουν που ψωνίζουμε, που τρώμε και πού πάμε διακοπές” (Γερουσιαστής *Charles Schumer*, USA)
- ❑ Τα δεδομένα αυτά μοιάζουν με στοιχεία πιστωτικών καρτών και μπορούν να συμβάλλουν στη διαμόρφωση μορφότυπων καταναλωτή (για στοχευμένη διαφήμιση)
- ❑ Τα δεδομένα αυτά είναι άκρως διεισδυτικά, καθώς μπορεί να έχουν επίδραση σε ποσοστά ασφάλισης, ιατρικούς λογαριασμούς κλπ.

Ζητήματα Ιδιωτικότητας

- ❑ Αριθμός ασφαλιστικών εταιρειών εγκαθιστά συσκευές τηλεματικής που επιτρέπουν στην εταιρεία να εντοπίζει τους προσεκτικούς οδηγούς και να τους ανταμείβει με χαμηλότερα ασφάλιστρα
- ❑ Η εταιρεία Progressive, ηγέτης στο χώρο της τηλεματικής ασφάλισης, προέβη στην κατάργηση της καταγραφής των τοποθεσιών του οχήματος και στην αφαίρεση των συσκευών μετά από 6 μήνες [7]
- ❑ Οι ηλεκτρονικές συσκευές καταγραφής δεδομένων (EDR), γνωστά και ως «μαύρα κουτιά» (συγκεντρώνουν τα κρίσιμα στοιχεία που οδηγούν σε ένα ατύχημα) ενσωματώνονται πλέον στο 96% των νέων αυτοκινήτων
- ❑ Τα EDR συνεισφέρουν στο σχεδιασμό ασφαλέστερων αυτοκινήτων, παρέχοντας κρίσιμες πληροφορίες σχετικά με τα ατυχήματα. Ωστόσο, τα δεδομένα αυτά χρησιμοποιούνται και από δικηγόρους σε δίκες που αφορούν οδηγούς

Hacking

Αυτοκίνητο	Εύρος Επίθεσης	Αρχιτεκτονική Δικτύου	Απομακρυσμένη Πρόσβαση
2014 Jeep Cherokee	++	++	++
2015 Cadillac Escalade	++	+	+
2014 Ford Fusion	++	-	++
2014 Dodge Ram 3500	++	++	--
2014 BMW X3	++	--	++
2014 Chrysler 300	++	-	++
2014 Audi 8	++	--	+
2014 Honda Accord LX	-	+	+
2010 Range Rover Sport	-	--	-
2006 Toyota Prius	-	--	--



είναι πιο εύκολο να hacking [8]

είναι πιο δύσκολο hacking

Εύρος Επίθεσης: Πε παρακολούθησης πί

Αρχιτεκτονική Δικτ

Απομακρυσμένη Πρ ασύρματες εντολές.

of researchers has revealed the specific vehicles that are at the greatest risk.

Chris Valasek and Charlie Miller studied the schematics for a range of cars from the 2006 Range Rover Sport to this year's BMW 3 Series.

The 2014 Jeep Cherokee and 2015 Cadillac Escalade were the most vulnerable of the cars studied, while the 2006 Ford Fusion and 2010 Range Rover Sport were listed as two of the most secure.

Scroll down for video

Fi, συστημάτων

τιμόνι και τα φρένα.

θούν χρησιμοποιώντας

[8] Zurich Report: Smart Cars and Connected Vehicles, Privacy, Security and Safety Considerations.

Hacking



Η πληροφορία που παράγεται από ένα όχημα και μεταδίδεται μέσω του Internet μπορεί να υποκλαπεί, προς όφελος πληθώρας ενδιαφερόμενων



Οι ηλεκτρονικές μονάδες ελέγχου (ECU) βελτιώνουν τις επιδόσεις του οχήματος, αλλά είναι ευάλωτες σε hacking



CAESS (Κέντρο Ασφάλειας Ενσωματωμένων Συστημάτων Αυτοκινητοβιομηχανίας): «Με σύνδεση ειδικής συσκευής στη θύρα OBD-II στο χειριστήριο του αυτοκινήτου, μπορούν να ελεγχθούν όλα τα ζωτικά συστήματα του οχήματος»



CAESS: «Ο έλεγχος ενός οχήματος από απόσταση είναι δυνατός μέσω ειδικών συσκευών»



CAESS: «Είναι δυνατή η μόλυνση ενός οχήματος με ιομορφικό λογισμικό ενσωματωμένο σε MP3 αρχείο, με κώδικα που μεταδίδεται μέσω ασύρματης σύνδεσης»

Hacking

- ❑ CAESS: «Ο διαχωρισμός μεταξύ πληροφοριών διασκέδασης-ενημέρωσης και πληροφοριών ασφάλειας του οχήματος είναι αναγκαίος» (η τάση, όμως, είναι προς την κατεύθυνση μεγαλύτερης ολοκλήρωσης)
- ❑ Υπηρεσία Προηγμένων Αμυντικών Έργων Έρευνας (DARPA): Ερευνά τις τρωτότητες της ασφάλειας των συστημάτων των έξυπνων αυτοκινήτων
- ❑ TrendMicro: «Το οργανωμένο έγκλημα διαθέτει την αναγκαία τεχνογνωσία για να ελέγξει ένα όχημα μόνο με τη χρήση ενός φορητού υπολογιστή»
- ❑ Όσο τα οχήματα ενσωματώνονται στο Internet of Things, τόσο αυξάνεται η ευκολία να τα ελέγχει κάποιος από απόσταση

Διαχείριση επικινδυνότητας έξυπνων οχημάτων



Οι απλοί ιδιοκτήτες οχημάτων δεν μπορούν να λάβουν παρά προφυλάξεις «κοινής λογικής», όπως θα έκαναν με το PC ή το κινητό τους τηλέφωνο



Οι ιδιοκτήτες εμπορικών στόλων αυτοκινήτων πρέπει να σχεδιάσουν και να εφαρμόσουν μια συνολική στρατηγική ασφάλειας τους



Οι κατασκευαστές οχημάτων και οι εταιρείες παροχής τεχνολογίας και υπηρεσιών μετάδοσης, συλλογής και επεξεργασίας δεδομένων πρέπει να αναπτύξουν ισχυρά συστήματα, διαδικασίες και πολιτικές ασφάλειας

Μερικά βασικά συμπεράσματα

- ✓ Τα έξυπνα οχήματα θα αποτελέσουν, σύντομα, **κινούμενους κόμβους** παραγωγής, λήψης, μετάδοσης και επεξεργασίας δεδομένων
- ✓ Τα έξυπνα αυτοκίνητα μπορούν να λειτουργήσουν προς όφελος των **οδηγών**, των **επιβατών**, αλλά και της ενίσχυσης της **οδικής ασφάλειας**



Ανακύπτουν ζητήματα φυσικής **ασφάλειας** λόγω της ενδεχόμενης διάσπασης της προσοχής του οδηγού



Ανακύπτουν ζητήματα **ιδιωτικότητας** του οδηγού και των επιβαινόντων, λόγω της ανεπαρκούς προστασίας των δεδομένων που παράγονται στα οχήματα



Ανακύπτουν προβλήματα **φυσικής ασφάλειας** του οχήματος και **ασφάλειας των δεδομένων** των επιβαινόντων σε περίπτωση hacking των συστημάτων του οχήματος

- ✓ Προκύπτει ανάγκη συμπλήρωσης του **θεσμικού πλαισίου** που διέπει την προστασία των (προσωπικών και μη) δεδομένων που παράγονται στα έξυπνα οχήματα

References

1. Dötzer F., "Privacy issues in vehicular ad hoc networks", in *Privacy enhancing technologies*, pp. 197-209, Springer, 2006.
2. Hubaux J., Capkun S., Luo J., "The security and privacy of smart vehicles", *IEEE Security & Privacy Magazine*, pp. 49-55, 2004.
3. Gavrila D., "Smart Cars for Safe Driving", in *IEEE International Conference on Intelligent Computer Communication and Processing*, Keynote Lecture, 2012.
4. Gritzalis D., Kandias M., Stavrou V., Mitrou L., "The Social Media in the History of Information: Privacy violations and security mechanisms", in *Proc. of the History of Information Conference*, pp. 283-310, Law Library Publications, 2014.
5. Kandias M., Virvilis N., Gritzalis D., "The Insider Threat in Cloud Computing", in *Proc. of the 6th International Workshop on Critical Infrastructure Security*, pp. 93-103, Springer (LNCS 6983), Switzerland, 2011.
6. Kandias M., Stavrou V., Bozovic N., Mitrou L., Gritzalis D., "Can we trust this user? Predicting insider's attitude via YouTube usage profiling", in *Proc. of 10th IEEE International Conference on Autonomic and Trusted Computing*, pp. 347-354, IEEE Press, Italy, 2013.
7. Kandias M., Galbogini K., Mitrou L., Gritzalis D., "Insiders trapped in the mirror reveal themselves in social media", in *Proc. of the 7th International Conference on Network and System Security*, pp. 220-235, Springer (LNCS 7873), Spain, 2013.
8. Kotzanikolaou P., Theoharidou M., Gritzalis D., "Interdependencies between Critical Infrastructures: Analyzing the Risk of Cascading Effects", in *Proc. of the 6th International Workshop on Critical Infrastructure Security*, pp. 107-118, Springer (LNCS 6983), Switzerland, 2011.
9. Lekkas D., Gritzalis D., "e-Passports as a means towards a globally interoperable Public Key Infrastructure", *Journal of Computer Security*, Vol. 18, No. 3, pp. 379-396, 2010.
10. Mitrou L., Gritzalis D., Katsikas S., Quirchmayr G., "Electronic voting: Constitutional and legal requirements, and their technical implications", in *Secure Electronic Voting*, pp. 43-60, Springer, 2003.
11. Mylonas A., Meletiadias V., Mitrou L., Gritzalis D., "Smartphone sensor data as digital evidence", *Computers & Security*, Vol. 38, pp. 51-75, 2013.
12. Mylonas A., Tsoumas B., Dritsas S., Gritzalis D., "Smartphone security evaluation: The malware attack case", in *Proc. of the 8th International Conference on Security and Cryptography*, pp. 25-36, SciTek-Press, Spain, 2011.
13. 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.
14. Popa R., Balakrishnan H., Blumberg A., "VPriv: Protecting Privacy in Location-Based Vehicular Services", in *Proc. of the USENIX Security Symposium*, pp. 335-350, 2009.
15. Rass S., Fuchs S., Schaffer M., Kyamakya K., "How to protect privacy in floating car data systems", in *Proc. of the 5th ACM International Workshop on VehiculAr Inter-NETworking*, pp. 17-22, ACM, 2009.
16. Sun J., Wu Z., Pan G., "Context-aware smart car: from model to prototype", *Journal of Zhejiang University*, Vol. 10, No. 7, pp. 1049-1059, 2009.
17. Spirakis P., Katsikas S., Gritzalis D., Allegre F., et al., "SECURENET: A network-oriented intelligent intrusion prevention and detection system", *Network Security Journal*, Vol. 1, No. 1, pp. 22-39, 1994.
18. The Daily Mail, "The 20 most hackable cars revealed", August 8, 2014.
19. Theoharidou M., Tsalis N., Gritzalis D., "Smart Home Solutions for Healthcare: Privacy in Ubiquitous Computing Infrastructures", *Handbook of Smart Homes, Health Care and Well-Being*, Springer, 2014.
20. 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.
21. Virvilis N., Gritzalis D., "The Big Four - What we did wrong in protecting critical ICT infrastructures from Advanced Persistent Threat detection?", in *Proc. of the 8th International Conference on Availability, Reliability & Security*, pp. 248-254, IEEE, Germany, 2013.
22. Wang F., Zeng D., Yang L., "Smart cars on smart roads: an IEEE intelligent transportation systems society update", *IEEE Pervasive Computing*, Vol. 5, No. 4, pp. 68-69, 2006.