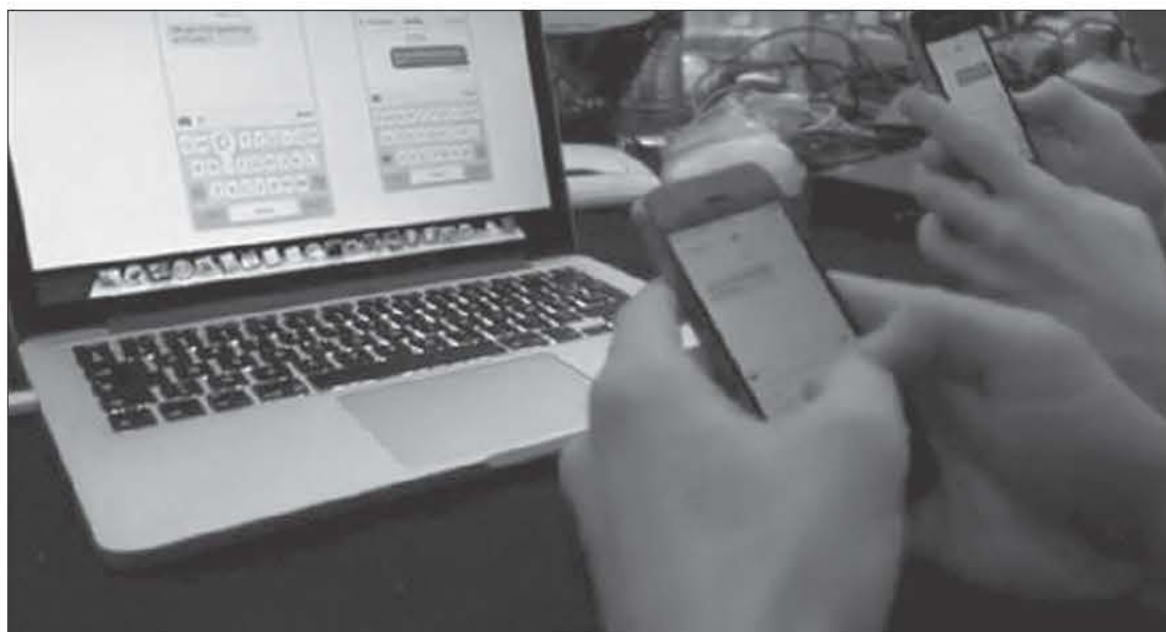


Την μέθοδο με την οποία η Apple θα μπορούσε να διαβάσει τα κρυπτογραφημένα σύντομα μηνύματα που διακινούνται από την δική της υπηρεσία άμεσης ανταλλαγής μηνυμάτων iMessage μεταξύ χρηστών υπολογιστών με Mac OS X, καθώς και χρηστών iPhone και iPad με iOS, έδειξαν χάκερ στο συνέδριο Hack In a Box που διεξάγεται αυτές τις ημέρες στην Μαλαισία.

Οι ερευνητές έδειξαν δημοσίως πώς μπορεί να παρεμβληθεί τρίτος στην επικοινωνία μέσω iMessage, ώστε να αλλάξει το περιεχόμενο του μηνύματος πριν φτάσει στον προορισμό του. Ο παραλήπτης δεν έχει τρόπο να υποψιαστεί ότι κάποιος άλλος υποδύεται τον αποστολέα του παραραγαμένου μηνύματος.

Ωστόσο, οι «Pod2G» και «GG» επεσήμαναν ότι το εγχείρημα δεν απευθύνεται σε αρχάριους. Το επίπεδο τεχνογνωσίας απαιτείται να είναι εξαιρετικό υψηλό.

Τον Ιούνιο, το όνομα της Apple ήταν ανάμεσα στις επτά επιχειρήσεις επικοινωνιών του Διαδικτύου -μαζί με την Google, το Facebook, την Microsoft και το Yahoo κ.ά- που φέρονται να επιτρέπουν στις μυστικές υπηρεσίες των ΗΠΑ -και συγκεκριμένα στην NSA- την πρόσβαση στο περιεχόμενο μηνυμάτων των μελών τους. Με αφορμή την, αν μη τι άλλο, γενναία αποκάλυψη του Έντουαρτ Σνόουντεν, η Apple σε επίσημη ανακοίνωσή της στις 16 Ιουνίου



«ΑΡΚΕΙ ΝΑ ΕΧΕΙ ΤΟ ΚΙΝΗΤΡΟ»

Η Apple θα μπορούσε να διαβάσει μηνύματα iMessage, αποδεικνύουν χάκερ

του 2013 τόνιζε πως τα μηνύματα μέσω iMessage (και Facetime) προστατεύονται από κρυπτογράφηση από άκρο σε άκρο, έτσι ώστε κανείς πλην του αποστολέα και του παραλήπτη να μην μπορεί να τα διαβάσει. Οι χάκερ ανέλαβαν την πρόκληση να θέσουν σε δοκιμασία τον ισχυρισμό της Apple ότι δεν μπορεί να διαβάσει

τα μηνύματα που ανταλλάσσονται μέσω iMessage καθώς, πρόκειται για κρυπτογράφηση από άκρο σε άκρο. Το white paper που δημοσιεύουν οι ερευνητές αποδεικνύει το αντίθετο, ότι δηλαδή είναι τεχνικά εφικτό.

Οι χάκερ έδειξαν ότι για την επέμβαση ο επιτιθέμενος θα πρέπει να αποκτήσει φυσική πρόσ-

βαση στην συσκευή, αρκεί όμως μια μόνο φορά για να το επιτύχει. Αρκεί να έχει το χρόνο να εγκαταστήσει πλαστά πιστοποιητικά στην συσκευή και να παραπέμψει σε ξένους διακομιστές που «μιμούνται» τους server της Apple -το κενό ασφαλείας εντοπίστηκε στο λεγόμενο certificate pinning, μια μέθοδο που λέει στον browser

ποια πιστοποιητικά να εμπιστευτεί και από ποια domain.

Τέλος, οι χάκερ ανέβασαν στο αποθετήριο GitHub ένα εργαλείο iMITMProtect με το οποίο οι κατάλληλα καταρτισμένοι χρήστες μπορούν να κλείσουν το κενό ασφαλείας και να προστατευτούν.

Το ZDNet ήταν στην Κουάλα Λαμπόρ και κατέγραψε σε βίντεο την επιτυχημένη μεσολάβηση τρίτου κατά την επικοινωνία δύο χρηστών iPhone.

Πάντως, η είδηση έφτασε στο Κουπερτίνο και η εταιρεία απάντησε στο All Things Digital λέγοντας πως η «θεωρητική» αυτή προσέγγιση προϋποθέτει ότι η Apple έχει την πρόθεση ή σχέδια να επέμβει στο σύστημά της, κάτι το οποίο δεν συμβαίνει. Δηλαδή, το εγχείρημα της Apple είναι ότι ανέπτυξε ένα σύστημα για να αντιμετωπίζει τις επιθέσεις μη εξουσιοδοτημένης παρέμβασης στο σύστημα επικοινωνίας, όχι για να τις εξαπολύει η ίδια. Έτσι, ο χρήστης καλείται να εμπιστευτεί την Apple. Στο white paper των χάκερ αναφέρεται ότι η Apple θα μπορούσε να το κάνει, εάν έχει την απαιτούμενη εισαγγελική εντολή (ενώ είναι γνωστό ότι οι εταιρείες που εμπλέκονται στο σκάνδαλο PRISM επιχειρούν να ξεπεράσουν τα νομικά εμπόδια που δεν τους επιτρέπουν να αποκαλύπτουν υπό ποιες συνθήκες είναι αναγκασμένες να υποκύπτουν στα αιτήματα των μυστικών υπηρεσιών).

Ο Κόσμος

ΕΝΗΜΕΡΩΝΕΙ ΚΑΙ ΕΓΧΩΝΕΙ

ΚΑΘΕ ΤΡΙΤΗ, ΤΕΤΑΡΤΗ, ΠΕΜΠΤΗ ΚΑΙ ΠΑΡΑΣΚΕΥΗ
503-507 Marrickville Rd, Dulwich Hill NSW 2203
ABN: 69 145 864 071 Phone: (02) 9568 3766, Fax: 9569 9344
www.kosmos.com.au • e-mail: kosmos@kosmos.com.au

PUBLISHER
HELLENIC NEWS PTY LTD
ΕΚΔΟΤΕΣ

Σπύρος Χαραλάμπους
ΑΡΧΙΣΥΝΤΑΚΤΗΣ
Γιώργος Χατζηβασιλίας
ΑΡΘΡΟΓΡΑΦΟΙ

Σάββας Λιμνατίτης, Δέσποινα Μπακά,
Γιώργος Τσερδάνης, Γιώργος Χατζηβασιλίας
ΑΡΧΙΣΥΝΤΑΞΙΑ ΑΘΛΗΤΙΚΩΝ
Γιώργος Σταυρουλάκης - sportseditor@gmail.com
ΔΙΑΦΗΜΙΣΤΙΚΟ

Βασιλική Τομαρά - sales@kosmos.com.au
ΜΕΤΑΦΡΑΣΕΙΣ

Γιάννης Δραμιτινός
ΗΛΕΚΤΡΟΝΙΚΗ ΣΕΛΙΔΟΠΟΙΗΣΗ
Γιάννης Γεωργιάδης, Σάββας Λιμνατίτης

PRINTED BY: Spotpress
WEBSITE: Platyrachos Publishing

εορτολόγιο Ιακώβου του Αδελφοθέου, Ιγνατίου Κων/λεως

Σίδνεϊ
20°C - 32°C

Μεμονομένες βροχοπτώσεις το πρωί, κυρίως ηλιοφάνεια το απόγευμα.
Άνεμοι: ΔΒΔ με 21 Km/h
Υγρασία: 29% - 60%

ΕΛΛΗΝΙΚΕΣ ΥΠΗΡΕΣΙΕΣ ΣΙΔΝΕΪ-ΚΑΜΠΕΡΑ

Ιερά Αρχιεπισκοπή: 02 9690 6100
Ελληνική Κοινότητα: 02 9740 6022
Κυπριακή Κοινότητα: 02 9557 1256
Ελληνική Πρεσβεία: 02 6273 3011
Κυπριακή Πρεσβεία: 02 6281 0832
Ελληνικό Προξενείο: 02 9264 1768
email: grgencon.sid@mfa.gr
Γραφείο Τύπου: 02 9267 0966
email: gpressbureau@tpg.com.au
Γραφείο Εκπαίδευσης: 02 9283 3800
ΣΑΕ Ωκεανίας: 02 9558 3744
Γραφείο ΕΟΤ: 02 9241 1663

NSW Lotteries

Thu 17/Oct/13, Draw 909
Winning Numbers: 30 4 19 12 13 8
Powerball: 2
Division 1: Jackpotted
0 Winners, Jackpotted to Draw 910
Next Draw: Thu 24/Oct/13, Draw 910



Mon 21/Oct/13, Draw 3288
Winning Numbers: 10 33 42 40 30 28
Supplementaries: 16 17
Division 1: \$1,000,000.00
1 Winner, of \$1,000,000.00
Next Draw: Wed 23/Oct/13, Draw 3289



DelphiBank

ΣΑΣ ΠΡΟΣΦΕΡΕΙ ΤΙΣ ΤΙΜΕΣ ΣΥΝΑΛΛΑΓΜΑΤΟΣ

COUNTRY	CURRENCY	ABBREVIATION	BANK BUYS	BANK SELLS
United States	Dollar	USD	1.0093	0.9318
Europe	Euro	EUR	0.7560	0.6715
United Kingdom	Pound	GBP	0.6343	0.5644

149 Forest Rd, Hurstville, Tel: 8567 1111 • 204 Burwood Rd, Burwood, Tel: 9745 0400
192 B Maroubra Rd, Maroubra, Tel: 8347 7100 • 276 Marrickville Rd, Marrickville, Tel: 8226 5888