# SMARTPHONE AND COMPUTER USB CONNECTIVITY-HACKING

## Εισαγωγή

Τα Smartphone περιέχουν προγραμματίσιμο hardware και λειτουργικό σύστημα που τους επιτρέπει να αλλάξουν τον τρόπο επικοινωνίας μεταξύ του hub και του host (της περιφερικής συσκευής-smart phone και του οικοδεσπότη-υπολογιστή). Γνωρίζοντας κάποιος όλες τις πληροφορίες μιας τέτοιας συσκευής μπορεί να υποκλέψει ότι δεδομένα θέλει. Η σύνδεση και το μέσω με το οποίο θα γίνει η υποκλοπή είναι το usb και αυτό γιατί θεωρείται αξιόπιστο και ακίνδυνο ενώ δεν υπάρχει κάποιος τρόπος ανίχνευσης του.

Μπορούν να γίνουν επιθέσεις με 3 διαφορετικούς τρόπους.

1) phone-to-computer
2) computer-to-phone
3) phone-to-phone

## Phone-to-computer

Κατά κύριο λόγο το πλεονέκτημα του κινητού είναι ότι έχει ανοιχτό λειτουργικό σύστημα (δηλαδή προγραμματίσιμο) και θεωρείται αξιόπιστη περιφερειακή συσκευή ώστε να συνδεθεί με τον υπολογιστή. Το δεύτερο είναι ότι εφόσον το συνδέσουμε αυτό τρέχει αυτόματα ότι περιεχόμενο είναι αποθηκευμένο στη μνήμη του. Τα περιεχόμενα, δηλαδή ο κώδικας, μπορούν να ελέγχουν είτε το ποντίκι είτε το πληκτρολόγιο (για να μπορέσει να ελεχθεί η συμπεριφορά του usb και να γίνει μια προσομοίωση του πληκτρολογίου προσθέτουμε στην λίστα των περιφερειακών που κάνει report to Smartphone στο pc ένα πληκτρολόγιο που έχουμε τα specification – χαρακτηριστικά- σαν μια περιφερειακή usb συσκευή). Αυτό γίνεται καθώς το usb έχει μία φυσική σύνδεση αλλά πολλές λογικές επιτρέποντας σε μία ή περισσότερες συσκευές να κάνουν multiplex πάνω από μία φυσική σύνδεση, έτσι το Smartphone μπορεί να έχει πολλές λογικές συνδέσεις χωρίς πρόβλημα και εφόσον οι συσκευές παραμένουν συνδεδεμένες. (Φυσικά πρέπει να προσομοιωθεί το ποντίκι ή το πληκτρολόγιο σαν μια επιπλέον λογική σύνδεση και αυτό επιτρέπεται όταν κάνεις register στο linux usb software hub που είναι προγραμματισμένο στον kernel) .

Το κινητό αποθηκεύει στην cd card ένα autorun.inf (το .inf προκύπτει από το information, είναι ένα plain text αρχείο που χρησιμοποιούν τα windows για να εγκαθιστούν software και drivers, η αρχιτεκτονική του inf είναι παρόμοια με του ini που θα δούμε παρακάτω, καθώς εκτελούν όμοιες λειτουργίες) και ένα calc.exe, οπότε την επόμενη φορά που ο χρήστης θέλει να μεταφέρει αρχεία το calc.exe θα εκτελεστεί by default. Μία από τις αρχικές λειτουργίες του προγράμματος που φτιάχνει ο υποκλοπέας είναι να εξετάζει και να αναγνωρίζει το λειτουργικό σύστημα κοιτάζοντας το urb. Το urb -usb requesting block- είναι μέρος του usb πρωτοκόλλου και διαφέρει μεταξύ λειτουργικών συστημάτων και διαφορετικών εκδόσεων, αυτές οι διαφορές είναι πολύ μικρές αλλά μας επιτρέπουν να ταυτοποιήσουμε το λειτουργικό και την έκδοση του. Συνδέοντας τις συσκευές έχουμε αναγνώριση των διαδρομών των πακέτων του υπολογιστή, εισχωρούμε σε αυτές ώστε να μπορούμε να υποκλέψουμε ότι θέλουμε ενώ ταυτόχρονα γίνεται κάποια φανερή μεταφορά

δεδομένων που έχει καθοριστεί από τους δύο χρήστες ώστε να μην καταλάβει ο διαχειριστής του υπολογιστή ότι κάτι δεν πάει καλά.

Ακόμα για τα iphone/ipod αυτή η διαδικασία είναι ακόμα ευκολότερη καθώς με την σύνδεση εγκαθίσταται το itunes που παίρνει τον έλεγχο όλων των πολυμέσων (εικόνες, τραγούδια, ταινίες) οπότε μπορούμε απευθείας να διαλέξουμε ότι θέλουμε να πάρουμε.

Computer-to-phone

Τα smart phone έχουν κλειδωμένα από κατασκευή τους το λογισμικό. Ο χρήστης που σκοπεύει να επιτεθεί το πρώτο πράγμα που κάνει είναι να δώσει εντολή να ξεκλειδωθεί το λογισμικό του κινητού. (Αν γίνει κάτι τέτοιο το κινητό χάνει την εγγύηση του καθώς αποδεσμεύεται από την εταιρία παραγωγής του. Ωστόσο ο χρήστης του κινητού δεν καταλαβαίνει κάτι καθώς δεν υπάρχει κάποια εμφανή διαφορά.) Συνεπώς το πρώτο βήμα για τον πλήρη έλεγχο του κινητού είναι η δημιουργία ενός μικρού προγράμματος –fastboot- ώστε όταν συνδεθούν οι συσκευές να πραγματοποιηθεί απευθείας το root (το ξεκλείδωμα του λογισμικού), ο χρήστης του κινητού όμως θα πρέπει να επιλέξει ένα "yes" για να ολοκληρωθεί η διαδικασία, οπότε ο προγραμματιστής φτιάχνει το πρόγραμμα έτσι ώστε οτιδήποτε πιέσουμε εκείνη την ώρα πάνω στο κινητό μας να θεωρηθεί σαν "yes".

Ακόμα πρέπει να έχουμε πληροφορίες για το kernel (είναι η καρδιά τόσο του λειτουργικού συστήματος, όσο και του μηχανήματός μας) και το ram-disk (is a block of RAM -primary storage or volatile memory- that a computer's software is treating as if the memory were a disk drive (secondary storage). του κινητού. Βρίσκουμε το αρχείο της ram-disk, εκεί μέσα περιέχεται ένα πρόγραμμα, το init.rc (συντομογραφία της λέξης *initialization-αρχικοποίηση*), αυτό αναλύει το αρχείο ram-disk που είναι η πρώτη διαδικασία για να βρούμε το λειτουργικό σύστημα. Εγκαθιστά ένα βασικό περιβάλλον για το σύστημα και ξεκινά κάποιες διαδικασίες με το deamon (αυτό είναι ένα πρόγραμμα που τρέχει χωρίς να φαίνεται και συνήθως δεν είναι στον έλεγχο του μόνιμου χρήστη), το πρόγραμμα init και το αρχείο init είναι πολύ σημαντικά για την εύρεση ολόκληρου του συστήματος. Αφού ολοκληρωθεί και αυτό ξεκινά μια adb σύνδεση από τον υπολογιστή προς το κινητό (Android Debug Bridge είναι ένα ευέλικτο εργαλείο γραμμής εντολών που επιτρέπει την επικοινωνία με ένα λογισμικό android, -αυτό το εργαλείο υπάρχει στο <sdk>/platform-tools/. Η εντολή που χρησιμοποιείται είναι η adb – d <serial number><command> ) και σε αυτό το σημείο είναι που εισέρχεται τελικά και το πρόγραμμα που μεταφέρει τα αρχεία που μας ενδιαφέρουν. Όταν λοιπόν ολοκληρωθούν και όλα τα παραπάνω, πρέπει να βγάλουμε το κακόβουλο πρόγραμμα που παίρνει τις πληροφορίες και αυτό το κάνουμε με την παρακάτω εντολή: adb push evilprog /system/xbin. Σε αυτό το σημείο γίνεται ένας πλήρης έλεγχος της συσκευής και ένα back-up σε όλες τις εφαρμογές ώστε να μην παρατηρήσει καμιά αλλαγή ο χρήστης του κινητού. Στο τέλος μπορεί να γίνει και un-root για να μην γίνει φανερό ότι κάτι έχει αλλάξει.

Ο χρόνος αυτής της διαδικασίας είναι περίπου 4 λεπτά και εξαρτάται από τις συσκευές αλλά και το μέγεθος του περιεχομένου που ενδιαφερόμαστε να πάρουμε. Τα προγράμματα δημιουργούνται σε c ώστε να μπορούν να τρέξουν οπουδήποτε. (Ο λόγος που επιλέγεται η c είναι γιατί οι αλλαγές στο κινητό γίνονται στο Linux kernel - που είναι γραμμένα σε c.)

Phone-to-phone

Στη συνέχεια έχουμε την υποκλοπή δεδομένων από ένα κινητό μέσω ενός άλλου κινητού. Η διαδικασία είναι εντελώς παρόμοια με την παραπάνω και έτσι δεν αναφερθούμε  λόγω και του περιορισμένου χρόνο.

Τρόποι αντιμετώπισης-Μελλοντικές επεκτάσεις

Το πρόβλημα είναι ότι το usb θεωρείται αξιόπιστο και μη ικανό να προκαλέσει ζημία στις συσκευές. Για να προστατευτούν οι συσκευές θα μπορούσαν να αναπτυχτούν μηχανισμοί όπως αυτοί που χρησιμοποιούνται στις συσκευές Bluetooth, ώστε να επιτρέπει ο εκάστοτε χρήστης να γίνει σύνδεση ή όχι. Αυτό θα αποτρέψει την σύνδεση αναξιόπιστων συσκευών που συνδέονται χωρίς οποιαδήποτε αλληλεπίδραση με τον χρήστη.
Τι στιγμή που εισέρχεται ένα ανεπιθύμητο πρόγραμμα είναι ακόμα πιο δύσκολο να το καταλάβουμε  γιατί ο χρήστης παίρνει τον πλήρη έλεγχο της συσκευής. Πιθανών να μπορούσαν να αναπτυχθούν κάποια φίλτρα και firewalls (μέχρι στιγμής δεν έχει γίνει κάτι τέτοιο) παρόμοια με αυτά που υπάρχουν για ελέγχους διαδικτύου. Θα μπορούσαν να ψάχνουν τα πακέτα που εισέρχονται στο usb και να τα κρίνουν κατάλληλα ή μη βάση κάποιων συγκεκριμένων κανόνων.