SMARTPHONE AND COMPUTER USB CONNECTIVITY-HACKING

Τμήμα: Μηχανικών Πληροφορικής και τηλεπικοινωνιών

Ημερομηνία: 28/11/2012

Όνομα: Μπάτσου Ελευθερία

Επιβλέπων καθηγητής: Δρ. Μηνάς Δασυγένης

Διάλεξη 5 λεπτών για το μάθημα Αρχιτεκτονικής ΗΥ

Εισαγωγή

Usb: Universal Serial Bus

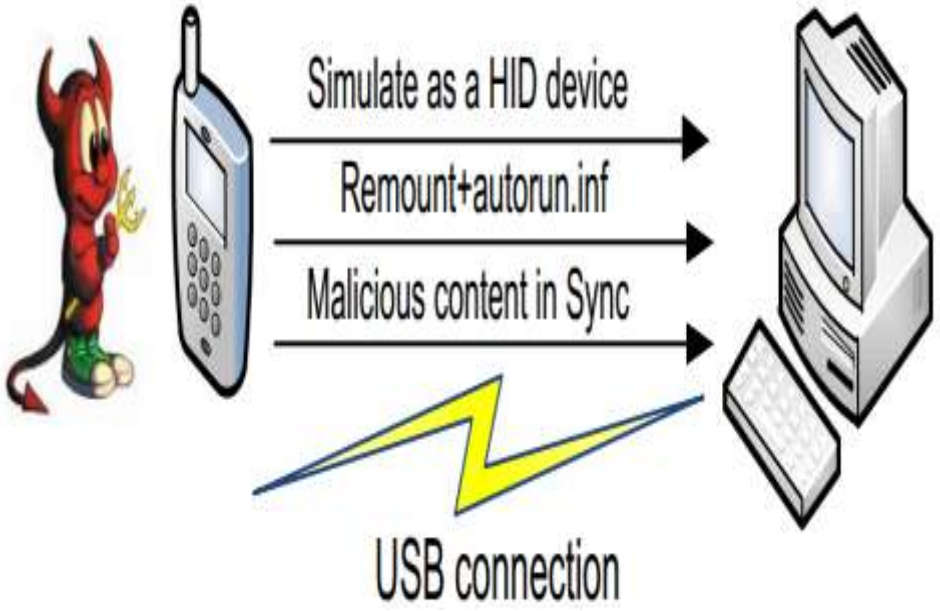
- **Smartphone**
- Προγραμματίσιμο hardware
- Λειτουργικό σύστημα
- **Επικοινωνία**
- Μεταξύ hub και host
- **Usb**
- Θεωρείται αξιόπιστο
- Ακίνδυνο
- Μη ανιχνεύσιμο

Μπορούν να γίνουν επιθέσεις με 3 διαφορετικούς τρόπους.

- phone-to-computer
- computer-to-phone
- phone-to-phone

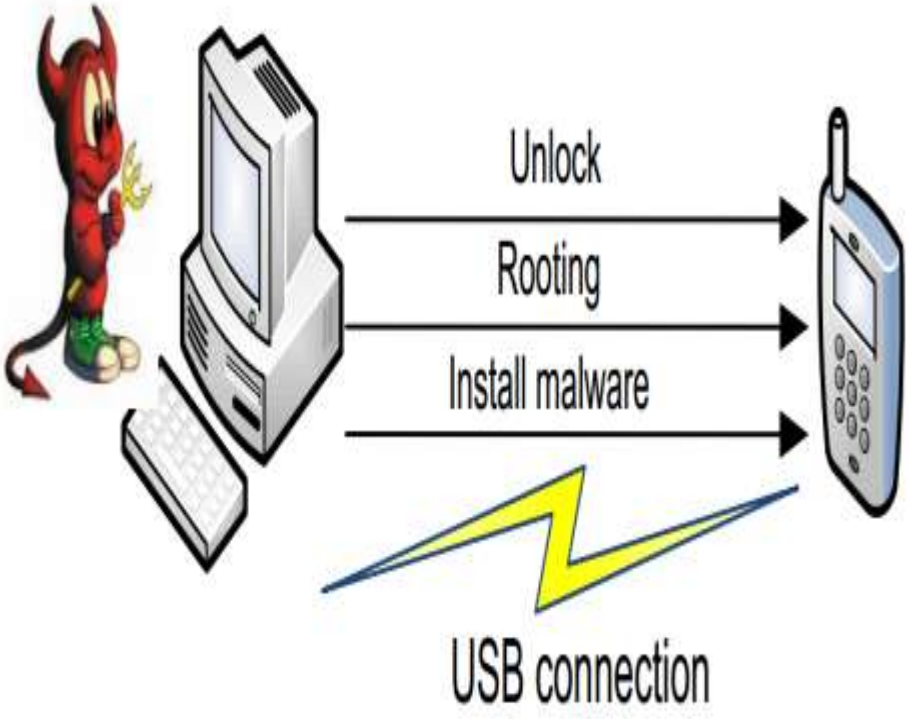
Phone-to-computer

- Τρέχει αυτόματα ότι περιεχόμενο είναι αποθηκευμένο στη μνήμη του.
- Αποθηκεύει στην cd κάρτα ένα autorun.inf και ένα calc.exe.
- Εξετάζει και αναγνωρίζει το λειτουργικό σύστημα του υπολογιστή κοιτάζοντας το urb (usb requesting block).



Computer-to-phone

- Root, ξεκλείδωμα λογισμικού του κινητού.
- Πληροφορίες για το kernel και το ram-disk.
- Περιέχεται ένα πρόγραμμα, το init.rc.
- Αναλύει αρχείο ram-disk.
- Εγκαθίσταται το deamon.
- Ξεκινά μια adb σύνδεση.
- Back-up στις εφαρμογές.



εντολές

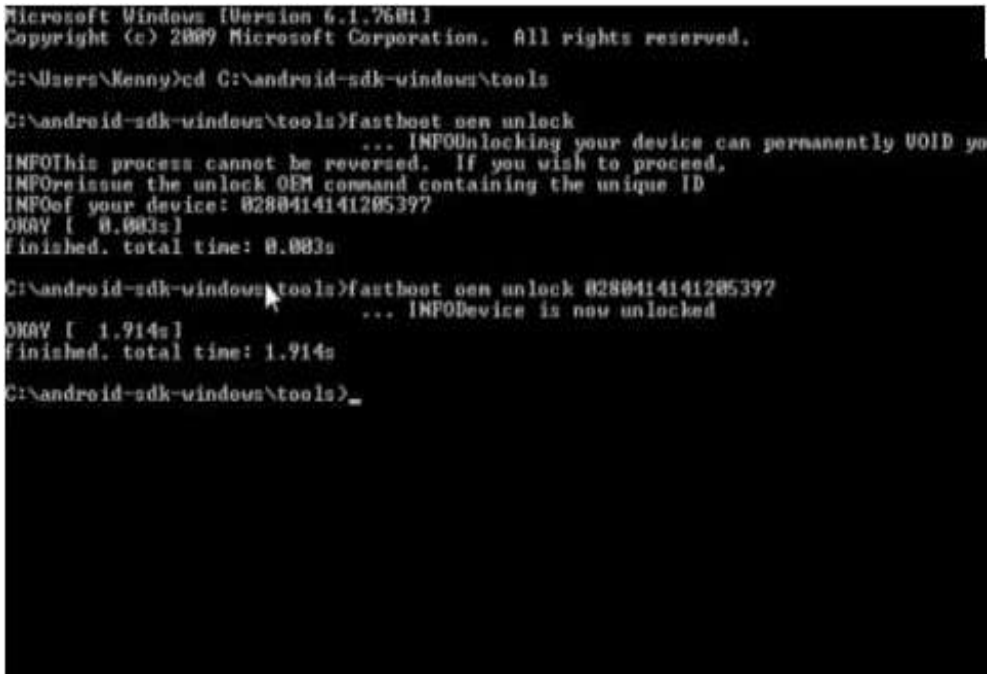
adb σύνδεση

υπάρχει στο <sdk>/platform-tools/

- Εντολή: adb – d <serial number><command>

- Για να αφαιρεθεί το πρ/μα
- adb push evilprog /system/xbin

Root –ξεκλείδωμα λογισμικού



Τρόποι αντιμετώπισης- Μελλοντικές επεκτάσεις

- θα μπορούσαν να αναπτυχτούν μηχανισμοί όπως αυτοί που χρησιμοποιούνται στις συσκευές Bluetooth, ώστε να επιτρέπει ο εκάστοτε χρήστης να συνδεθεί ή όχι.

- 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.

Βιβλιογραφία

Άρθρο:
Exploiting Smart-Phone USB Connectivity
For Fun And Profit

- http://www.gaw.ru/pdf/interface/usb/USB%203%200_english.pdf
- http://en.wikipedia.org/wiki/Init
- http://en.wikipedia.org/wiki/Daemon_(computing)
- http://developer.android.com/tools/help/adb.html
- http://en.wikipedia.org/wiki/INF_file
- http://www.msnbc.msn.com/id/44993238/ns/technology_and_science-security/t/phone-hack-logs-keystrokes-nearby-computers/#.ULRn1OTZajt

Εικόνες:
google images