

CFP

Author: Bruno Goncalves de Oliveira, bruno@bsdmail.com, +55 43 99726819

Hacking from the Restroom

One man enters in a company, asks for going to the restroom, from there, he takes his cellphone attacks the systems and got administrator privileges, a new Hollywood movie? Yes, until this presentation. A lot of papers are released showing techniques for hacking smartphones/pdas, if we can hack them, why not hack with them? It's a fu***** computer! The increase of softwares for mobile systems (Symbian, Windows Mobile, iPhone OS, Blackberry), increased the chance for making this real and the imagination helps a lot. This presentation has the goal to demonstrate that a smartphone is also swiss knife for hacking and not just for talking, no new attack just a new way for doing that.

Detailed Outline:

Goal

- Making a mobile device as a hacking tool

Why?

- It's a computer
 - Not just hack them, hack with them
- Too many smartphones on market
 - low prices
 - geek stuffs rules
- Mobile OS much more complex
 - symbian rox ;)
 - a lot of softwares availables
 - too many *mobile*Sotres
- Many conectivity resources
 - IR, Bluetooth, WLAN(1), UMTS, HSPDA
- SDKs available for developing
 - Symbian (C/C++, Python, other more?)
- Discrete
 - Hack with no attention
 - End-user doesn't know the power of smartphones
 - You can hack besides the iT manager
- Softwares already done (great!)
 - Apache + MySQL + PHP
 - Python

How? With Demo!

Client-Side Attacks = Apache, SMB + Social Engineer

Server-Side Attacks = Just a shell to attack

Reverse Tunnel = Hacking from the Restroom! ;D

Bio:

Bruno Gonçalves de Oliveira, computer engineer, security analyst at Altatech -Londrina/Parana/Brazil, holds some certifications, develops techniques to attack systems for profit == fun, does security structure analysis, applies defense tactics with softwares, hardwares and trainings. applies pentest for investment directions on info security and to assessment in a real world of actives in iT environment. And still researches about network security for acting in his current work/job, these works became talks at security cons like H2HC IV, YSTS 2.0, ToorCon X and already accepted for YSTS 3.0