Report z konference 27c3 (CCC) - den třetí

Vložil/a wwwnick [1], 3 Leden, 2011 - 13:17

- Hacking [2]
- Konference [3]

Třetí den, se nesl v duchu přednášek ale i demonstrace.
Příznivci herních konzolí netrpělivě očekávají přednášku ohledně postupu v prolomení ochran na PS3. Sál je plný a vzrušení stoupá, když jsou rekapitulovány dosavadní pokroky a exploity pro PS3. Následně tým, který si říká „Fail 0verflow“, představuje metody jak prolomit ochranu na PS3 a chyby v implementaci které SONY udělalo. Sony nevhodně implementovalo funkci k tvorbě ECDSA signatury, kdy nepoužili náhodné číslo ale konstantu, tako chyba pomohla k prolomení privátního klíče, pomocí kterého se podepisují binárky. Tato chyba vedla k finálnímu prolomení ochrany u PS3.

Foto: console hacking

Následovala přednáška o možnostech geolokace Android zařízení. Klasicky k geolokaci můžeme použít GPS nebo wifi (pokud známe polohy AP) anebo GSM sítě, konkrétně jednotlivé BTSky pokud známe jejich polohy. Existuje několik projektů, které si daly za cíl zmapovat polohy BTS. Jedna databáze obsahující tyto údaje je vlastněna společnosti Google, avšak není veřejně přístupná. Existuje důvěrné API, na jehož reverse-engineeringu se pracuje. Toto API je použito v android google maps. Analýzou se zjistilo, že je použit binární protokol, který se tuneluje přes http. Google gears také používá toto API, ale je implementováno pomocí JSON komunikace a je v dokumentaci označené jako zastaralé. Odpověď obsahuje zeměpisnou šířku, délku a plnou adresu. Toto můžeme zneužít k sledování, kde se pohybuje vlastník zařízení. V log souborech na android zařízeních najdeme identifikaci BTS, které zařízení vidí. Tyto logy jsou reprezentovány charakterovými zařízení v /dev/log. K stažení dat je potřeba fyzický přístup k zařízení nebo malware aplikaci. Aplikace musí mít

přístup k logům nebo vestavěným mechanizmům pro lokalizaci. V situaci, kdy aplikace má jen přistup k logům, musí útočník pro zpětný transfer dat použít tento postup: v aplikaci zapsat dané data do systemého logu a vyvolat spadnutí aplikace, aby uživatel pomocí nahlášení chyb v aplikaci přenesl data do google databáze. Útočník si pak jednoduše stáhne data k sobě. Další možnosti je aby aplikace běžela mimo sandbox. Pro infikování zařízení stačí, aby uživatel stáhnul libovolnou aplikaci, a útočník pomocí MITM útoku podvrhne malware. Renaud Lifchitz, jenž se tomuto výzkumu věnuje, během přednášky několikrát upozornil, že situace ohledně zabezpečení je mnohem horší na iPhone telefonech.

Foto: Renaud Lifchitz

Další přednáška „Running your own GSM stack on a phone„ se týkala okrajově GSM sítí, Harald Welte a Steve Markgraf prezentovali jejich implementaci vlastního open source GSM stacku na mobilních telefonech. Všeobecně se věci okolo GSM považují za uzavřené k malé skupině lidí, přesto specifikace GSM/3G jsou veřejně dostupné. Dokumentace k GSM chipsetům je slabá a dostupná jen vybraným lidem a společnostem. Implementace využívá existujících mobilů, pro které se dá v limitované podobě sehnat dokumentace. Projekt používá kód z OpenBSC a aktuální stav už umožňuje vytvoření a udržení hovoru a A5/1 + A5/2 šifrování. Dokončení tohoto projektu bude dalším ze základních kamenů pro větší možnost nezávislého výzkumu bezpečnosti v GSM sítích.


ccc
© Jan Klepek

Tento den byl také v symbolu demonstrace proti sběru a uchování dat.


AK VORRAT
© Jan Klepek


GG
SO
VORRAT

URL článku:
https://security-portal.cz/clanky/report-z-konference-27c3-ccc-den-t%C5%99et%C3%AD

Odkazy:
[1] https://security-portal.cz/users/wwwnick
[2] https://security-portal.cz/category/tagy/hacking
[3] https://security-portal.cz/category/tagy/konference