Report z konference 27c3 (CCC) - den první

Vložil/a wwwnick [1], 31 Prosinec, 2010 - 10:57

- Hacking [2]
- Programming [3]

Každý rok se koná v Berliner Congress Center (BCC) kongress pořádaný Chaos Computer Club, v tomto roce s pořadovým číslem 27.
Jedná se o 4denní konferenci na témata blízká k IT/GSM bezpečnosti, vědě, společnosti a hackerské kultůře.

Hned první přednáška se zabývala nedostatečně probíraným problémem jménem Anti-Counterfeiting Trade Agreement (ACTA) a boji proti pirátům. Jérémie Zimmermann zrekapituloval, z pohledu hudebního průmyslu, francouzský zákon o legalizaci odpojení obviněných "pirátů" od internetu bez pravocmeného odsouzení soudem, který byl následně změněn, aby se zachovala presumce neviny.

Čímž se zrušila očekávaná "rychlá" možnost odpojit piráta od internetu a tak hudební průmysl změnil taktiku a v UK vyzkoušel jiný postup, zjednodušeně namočit a přinutit k spolupraci ISP. I přesto že tento zákon je již částečně schválený, se připravuje další past pro svobodu výměny informací a to v podobě dohody ACTA. ACTA, která byla vytvářena tajně, aby v lidech vyvolala pocit strachu, a která si prošla stádii od spekulace, přes první neoficiální leak na Wikileaks až množství dalších úniků, má vynutit dodržování práv k duševnímu vlastnictví. V polovině příštího roku se čeká potvrzení nebo zamítnutí této dohody ze strany EU. Mezi aktuální zbraně zastánců této dohody patří tvrzení, že sdílení informaci je nemorální, kdežto zbraně kritiků této dohody vyzdvihují sdílení informací jako jeden z klíčových prostředků k vývoji kultury lidstva.

foto: Jérémie Zimmermann

foto: Jérémie Zimmermann

Další přednášky, které mne zaujaly, se věnovaly bezpečnosti mobilů.
Collin Mulliner a Nico Golde představili výzkum věnující se laboratornímu testování firmware mobilů na implementaci SMS/MMS služeb. Jedním z výsledků je python knihovna pro generování různých druhů SMS/MMS zpráv. Následně testovali, jak si s tim poradí firmware různých mobilů od různých výrobců. Výsledky nebyly až tak překvapivé, mezi odhalenými chybami se vyskytoval samovolný restart telefonu po přijetí upravené SMS/MMS zprávy, odpojení od sítě operátora až po situace ve kterých došlo k situaci, při které firmware odmítl všechny (i korektní) následné SMS/MMS zprávy. Při některých situacích kdy mobil přijal SMS, která ho přinutila k restartu dřív, než mohl odeslat zpět potvrzení o přijetí SMS, vedla k trvalému vyřazení telefonu z provozu na základě opakovaného posílání SMS od operátora. Tyto útoky, použitelné i ve velkém měřítku, můžou vést k cíleným útokům na skupinu uživatelů, operátora nebo výrobce. Útočník musí buď použit několik mobilů, SMS operátorů, botnetu z chytrých mobilů nebo přímého přístupu do sítě SS7,útoky můžou dosáhnout zhoršení jména značky, používají se také k vydírání, k organizovanému zločinu nebo testování kolik síť operátora vydrží. Obránce zde naráží na několik zásadních problemů, které ztěžují řešení situace, ať už výrobce ignorujícího tyto chyby, nedostatečné vydávání oprav firmware, modifikované verze firmware od operátorů anebo na základní nedostatek informaci o dostupnosti opravy mezi uživateli. Můžeme ale filtrovat SMS zprávy přímo u operátora, ale filtrační software se na tyto účely nepoužívá,

z důvodů neexistence centrální databáze chyb a případně snadnému obcházeni filtru.

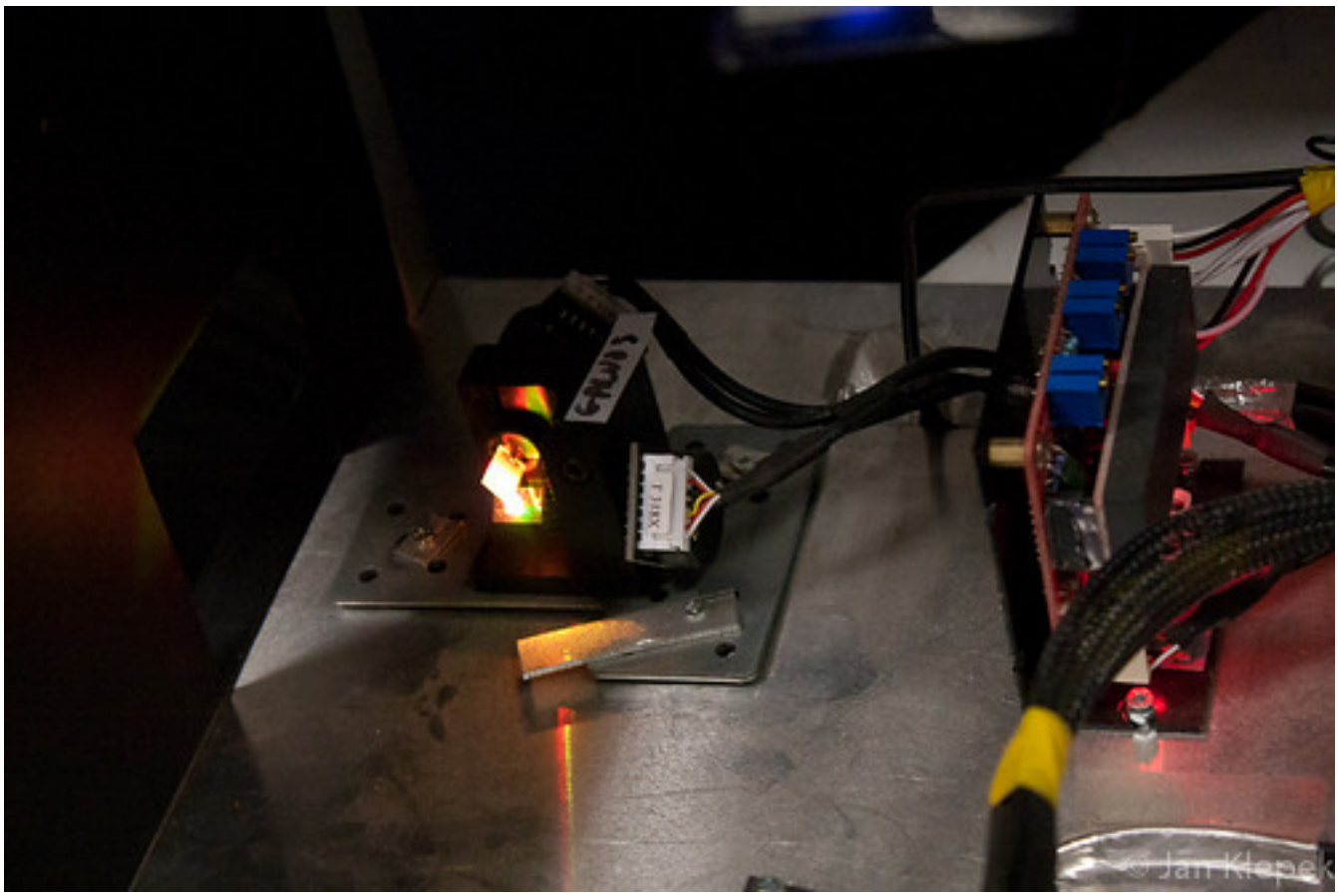
Ilja van Sprundel představoval výzkum v oblasti bezpečnosti chytrých mobilů. Jeho výzkum se zabývá iPhone a BlackBerry telefony. Jako první možný entrypoint se považuje implementace SMS/MMS funkcí, následně se nabízí možnost exploitování samotných aplikací a pokud by selhalo i to, jako třetí vstupní brána se může použít implementace komunikačních protokolů, ať už přes známé chyby v IRDA stacku (jenž už dnes málokterý telefon podporuje a které ani nejsou opravené), přes wifi a bluetooth až po útoky přes baseband (GSM/UMTS) stack.

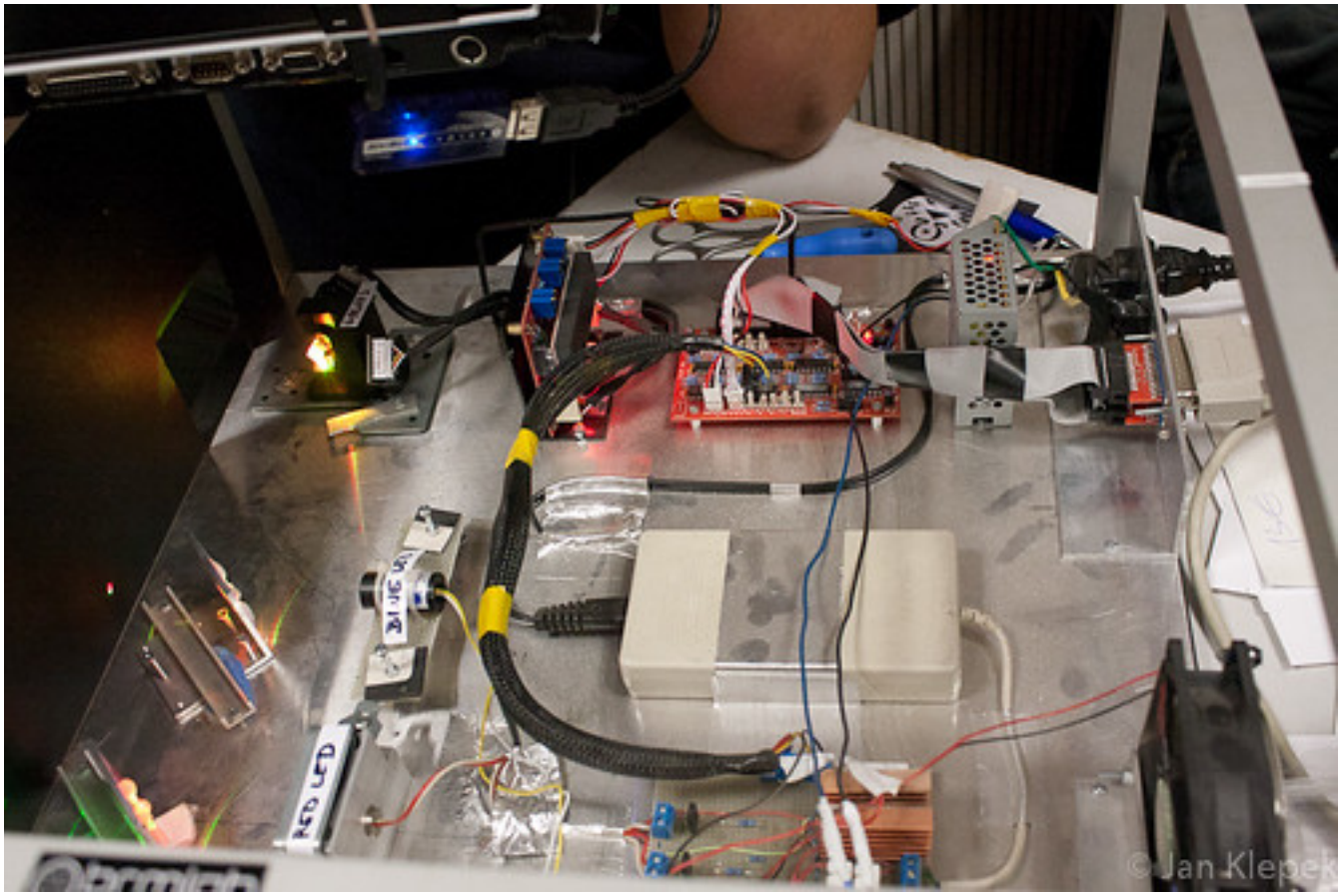
Závěr mého dne pak představovala přednáška o 'Data Retention in the EU five years after the Directive',

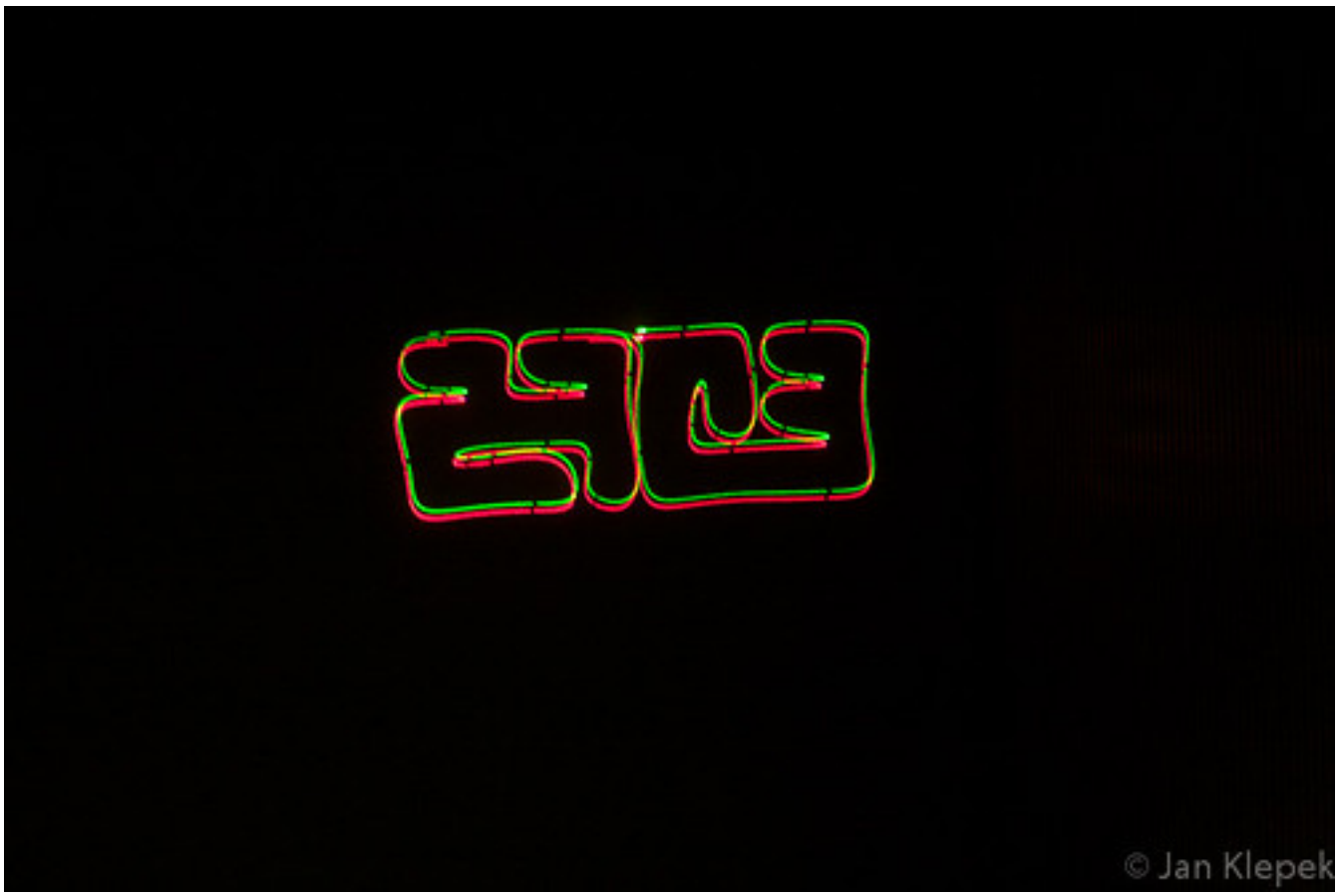
foto: (z leva: Patrick Breyer, Katarzyna Szymielewicz, Ralf Bendrath, Axel Arnbak)

jde o direktivu, která byla schválena v roce 2006 (Directive 2006/24/EC) a která je nyní revidována aby se zvážilo, jestli tato direktiva splnila svůj účel nebo je potřeba novelizace. Už během adaptace této direktivy do právního systému jednotlivých členů docházelo k protestům a německý soud v roce 2010 konstatoval, že implementace tohoto zákona je v rozporu s lidskými právy, což znamenalo zrušení zákona v Německu. Důvodem vzniku této direktivy byla pomoc USA s bojem proti terorizmu, na základě žádosti z USA. S použitím takto získaných dat lze na 90% určit, kdo jsou vaši přátelé a kolegové a s pravděpodobnosti 90% se dá předpovědět, jestli se s daným člověkem potkáte v příštích 12 hodinách. Existence této direktivy z ní vytváří odrazový můstek pro přijetí dalších opatření na sběr údajů o lidech, existuje návrh na rozšíření sběru dat o vyhledávání na vyhledávačích. Rumunský soud zrušil zákon implementující tuto direktivu s poznámkou "it could lead to destroy of democracy on the ground of defending it". Zajímavostí je, že implementace této direktivy nesdílejí jediný společný bod. Výzkum provedený na zjištění efektivity tohoto nařízení nezjistil signifikantní vliv na objasněnost IT zločinů, avšak vedlo to k zvýšenému použití anonymizačních služeb. V přehledu objasněnosti IT zločinů jde vidět sestupnou trendenci před i po zavedení zakonů o uchování dat. Zaznamenány byly i krádeže a prodej uchovávaných dat na černý trh. Nyní je čas zatlačit na politiky a vynutit si zrušení tohoto zákona a ochránit nás před velkým bratrem.

V rámci projektů prezentovaných na 27c3 se představil i náš Brmlab [4] s svým laserovým projektorem.


© Jan Klepek


© Jan Klepek



URL článku: https://security-portal.cz/clanky/report-z-konference-27c3-ccc-den-prvn%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/programming
[4] http://brmlab.cz/