Report z konference 27c3 (CCC) - den druhý

Vložil/a wwwnick [1], 1 Leden, 2011 - 21:29

- Hacking [2]
- Konference [3]

Druhý den začínal v pomalejším rozjezdu. Jako první na řadu přišly lightning talks. V rámci krátkých přednášek na různá témata, kdy cílem prezentujících bylo představit svůj projekt během 4-5ti minut.

Dennis Lohr představil svůj DaPrim projekt (Data Privacy Management), který má zajistit pomocí TPM modulu a softwarových komponent přístup k zašifrovaným datům jen v případě že systém je v bezpečném stavu (tzn., nedošlo k změnám v systému od doby vytvoření databáze s daty), v jiném případě jsou data nedostupná.

Foto: Denis Lohr

Raffael Kéménczy představil svůj projekt Starfish celosvětové distribuované sítě tvořené uživateli. Jedná se o síť kde zodpovědnost a kontrola je ponechána přímo na uživatelích, což má vést zpět k neutralitě internetu a poskytnout dostatečné kapacity pro budoucí rozvoj.

Foto: Raffael Kéménczy

Arthur Lutz prezentoval projekt „FreedomBox“, který má podpořit větší svobodu na internetu. Jedna se o počítač běžící na Debianě využívající cloud pro aplikace a data. Mezi funkce, které každý box může poskytovat, patří: p2p dns, tor router, microblogging, voip, p2p storage a další. Další kroky vývoje mají vést k větší implementaci p2p do různých programů, lepšímu grafickému rozhraní a vytvoření balíčků pro debian.

Foto: Arthur Lutz

Projekty založené na platformě Arduino představil Mitch Altman, platforma má sloužit k tvorbě různých HW zařízení, z existujících open-source projektů kterých je více než 1000, jmenujme například tv-b-gone jenž umožňuje dálkové ovládání libovolné televize. Jedná se o platformu, která nemá být určena jen geekům ale i umělcům a ostatním.

Foto: Mitch Altman

Alternativu k ICANN kořenovým DNS serverům představil Jonatan Walck, jmenuje se Telecomix DNS. A jedná se o systém decentralizovaných DNS serverů, které mají odstranit single point of failure v podobě kořenových DNS serverů. A odstranit cenzůru, která může nastat na úrovni top-level domén.

Foto: Jonatan Walck

S nástrojem (NetS-X) pro výuku síťové bezpečnosti se nám představil Alexander Ott, jedná se o sandbox síť, která běží na reálných síťových prvcích a počítačích a není založena na virtualizaci pomocí automatů.

Foto: Alexander Ott

Jak už bývá tradicí v posledních pár letech, na kongresu jsou přednášky, které demonstrují, že lze věci dělat bezpečněji. Jedním z případů je i GSM síť která v posledních pár letech utrpěla zásahy do oblasti zabezpečení. Přednáška Wideband GSM sniffing dvojice Karsten Nohl a Sylvan Munaut dala zabezpečení v GSM další zásah.

Jejich výzkum se soustředí na lokalizaci a odposlech telefonu za pomocí levných nástrojů na zachycení a analýzu.

Lokalizace telefonního čísla je možné provést pomocí SS7 sítě, v které si operátoři navzájem důvěřují a to už je dneska zneužívané na SMS spam. HLR query v kombinaci s silent SMS nám pomůže určit lokalitu čísla až na úroveň BTSky. Následně pomocí reprogramování telefonního firmware můžeme přetvořit telefon, který bude plnit funkce od debuggeru našich vlastních hovorů až po sniffer na uplink+downlink provoz. Pro zašifrování hovoru mezi BTSkou a telefonem se používá A5/1 šifra s session klíčem. Tento klíč se nemění často, většinou jednou denně. Zachycená data, které na normálním PC za pomocí rainbow tabulek rozšifrujeme v řádu sekund, pak můžeme použít na rekonstrukci hovoru, nebo čtení poslaných a přijatých SMS. Pro zvýšení bezpečnosti se doporučuje měnit session key po každém hovoru nebo SMS. Dalo by se říct, že v aktuální době je možné s levnými nástroji odposlouchávat hovory. Jste si jisti, že váš rozhovor s klientem nebo rodinou někdo neodposlouchává?

Poslední přednáška byla o možnostech vysoko rychlostního a vysoce bezpečného internetu. Daniel J. Bernstein poukazuje na nebezpečnost technologie DNSSECu jako nástroje, který může být zneužit k DNS DDOS útokům s amplifikačním faktorem od 30 až po 90, se zvětšováním účinku při dalším rozšíření DNSSECu. Dále poukazuje na nedostatek řešení, které by komplexně zajišťovalo šifrování a autenticitu od nejnižší vrstvy (TCP/UDP pakety). Není dostatek výpočetní síly, aby všechny informace tekly přes HTTPS, aktuálně i Google přes HTTPS provoz pouští pouze text a žádnou grafiku (na https://google.com [4] nenajdete odkaz na mapy, náhled stranky, a další). Jako řešení tohoto problému by mělo být nasazeno šifrování UDP paketů za pomocí asymetrické kryptografie na bázi eliptických křivek, výsledný CurveCP protokol by zároveň obsahoval mechanizmy na dosažení spolehlivosti TCP protokolu. CurveCP protokol by používal veřejné klíče přímo z URL adres. Pro zvýšení komfortu pro uživatele by tyto adresy měly lehce pamatovatelné CNAME (např. www.twitter.com [5] by byl CNAME na pub123456780.twitter.com). Implementace se skládá z instalace nástroje, který bude u uživatele dělat http proxy, šifrovat provoz a na straně serveru zas naopak. Tímto sice obejdeme DNS caching, ale šlo by jen o 15% nárůst oproti stávající situaci, s tím že poskytovatelé DNS mají kapacity na zvládnutí nárůstu, kvůli dnešním DDOS hrozbám a došlo by k uvolnění kapacit, které jsou třeba pro HTTPS.

Uvidíme v budoucnu, kam půjdou kroky k zabezpečení internetu.

URL článku: https://security-portal.cz/clanky/report-z-konference-27c3-ccc-den-druh%C3%BD

Odkazy:
[1] https://security-portal.cz/users/wwwnick
[2] https://security-portal.cz/category/tagy/hacking
[3] https://security-portal.cz/category/tagy/konference
[4] https://google.com
[5] http://www.twitter.com