Report z konference 27c3 (CCC) - den čtvrtý

Vložil/a wwwnick [1], 6 Leden, 2011 - 21:40

- Hacking [2]
- Konference [3]

Poslední den byl víc pokojný a kratší než předešlé dny, a témata přednášek tomu odpovídaly.

Annalee Newitz představila svoji vizi, jak bude vypadat žurnalistika v roce 2050 a jak se změní pracovní náplň a prostředky. V dnešní době se mluví o krizi v žurnalistice a potřebě změny. Tak jak je každá profese postupně transformována vlivem pokroku, tak i žurnalistika se změní. Jedna z budoucích pracovních pozic bude „journalism hacker“, člověk který bude hledat, analyzovat a reportovat novinky za pomocí vlastních programů. Další z povolání bude „data-mining analyst“ jenž se bude specializovat na filtrování a zpracovávání velkého množství dat. „Crowd enginner“ bude víc zaměřený na získávání fakta a názory lidí, editování a moderování diskuzí a analýzy komentářů. S příchodem nových technologii se mění i profese a pracovní nástroje, které lidé používají.

Jeroen Massar z laboratoří IBM představil sběr dat v prostředí Internetu. Pakety tečou přes více autonomních systémů a cesta mezi zdrojem a cílem může být asymetrická a nevíme, která síť zachytává pakety, ať už z legislativních, statistických nebo jiných důvodů. Pro implementaci můžeme mít na fibre switchi mirror port který kopíruje celý provoz z jiného portu. Nevýhodou tohoto řešení je složitá analýza. Pro zjednodušení bylo vyvinuto několik síťových protokolů, které mají usnadnit sběr dat. Je zde netflow protokol, který vyvinula firma CISCO. Tento protokol byl v pozdějších verzích vylepšený a standardizovaný jako IPFIX protokol. Netflow protokol sbírá jen některé údaje z procházejících paketů. Množství údajů je různé podle verze protokolu. Další protokol, jenž se používá je sFlow. Tento protokol sbírá jen vzorky z komunikace (1 paket z 4000) a je alternativa k Netflow verze 5 protokolu. Pro další sledování provozu se používá systém pasivního DNS kdy se odposlouchávají DNS dotazy a odpovědi. Spojením dat z těchto zdrojů můžeme začít vytvářet

digitální profil uživatelů. Každý používá pravidelně jen určitou množinu služeb a mimo to každý generuje pravidelný provoz, jenž se skládá z aktualizací aplikací, antivirů a jiný automatický provoz. I při změně ip adresy nebo poskytovatele se nemění naše návyky. Pro větší anonymitu je potřeba snižovat rozdíl v chování uživatelů nebo kompletně maskovat provoz pomocí tunelování přes vlastní infrastrukturu v rámci internetu (firemní a soukromé VPN přesměrovávající provoz do anonymizačních služeb, a jiné způsoby). Pro statistickou analýzu existuje „Anophera tool“, jenž sbírá a analyzuje data, které obdrží od směrovačů přes Netflow/show/IPFIX protokol.

V době konce této přednášky se pomalu začínalo s balením věcí a definitivní konec celého kongresu nastal, když v nejnižším patře, kde po celou dobu kongresu byla tma a jediný zdroj světla tam představovaly monitory, se rozsvítily světla.
I letošní kongres dostál svému jménu, přestavily se zajímavé projekty, výzkumy, implementace a myšlenky, a už nyní se můžeme těšit na příští ročník.

URL článku:
https://security-portal.cz/clanky/report-z-konference-27c3-ccc-den-%C4%8Dtvrt%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