MIT razvio novu tehnologiju za zaštitu osobnih podataka

Istraživači s američkog sveučilišta MIT nedavno su objavili kako su razvili novi enkripcijski sustav koji bi u budućnosti trebao spriječiti neželjeno "zavirivanje" u povjerljive i osobne podatke. Inicijalno nazvan **Mylar** – novi sistem omogućava programerima izradu web aplikacija koje će biti imune na napade.

Njegovi tvorci bili su potaknuti činjenicom da svatko tko ima pristup poslužitelju (bio to napadač, radoznali sysadmin ili vladin agent) može vidjeti i analizirati sve podatke pohranjene na njemu. Mylar omogućuje da su podaci na serverima kriptirani, a kriptirani i putuju do korisnika, te se dekriptiraju tek u korisnikovom pregledniku. Isto vrijedi i u obrnutom smjeru. Zanimljivo je da Mylar omogućuje pretraživanje podataka na serveru po ključnim riječima, iako su podaci kriptirani različitim korisničkim ključevima. Druga njegova prednost je u tome što omogućuje korisnicima da dijele ključeve i šifrirane podatke sigurno, čak i uz prisustvo aktivnih napadača. I konačno, Mylar omogućuje da je kod aplikacije na korisničkoj strani autentičan, čak i u slučaju da je na serverskoj strani maliciozan.

Prilagodba web aplikacija je jednostavna, zahtijeva dodavanje 35 redaka (u prosjeku), uz prihvatljivu potrošnju resursa i zanemarivu latenciju.

“Korisnici web aplikacija neće primijetiti nikakvu razliku u odnosu na aplikacije koje nemaju ugrađenu takvu vrstu zaštite, ali će istovremeno svi podaci biti enkriptirani pomoću zaporke prije nego se putem browsera pošalju dalje”, istaknuo je Raluca Popa, istraživač s MIT-a koji je dizajnirao Mylar. Dodaje kako je tehnologija prilično jednostavna - ako bilo koja vlada zatraži podatke o vama, poslužitelj nema mogućnost dati vaše podatke državnim agencijama u čitljivom tj. dekriptiranom obliku.

Ako smo zagolicali vašu radoznalost, skinite Mylar i poigrajte se s njim:

```
git clone -b public git://g.csail.mit.edu/mylar
```

ned, 2014-04-27 23:32 - Uredništvo**Vijesti:** Sigurnost [1]
Vote: 0

No votes yet

Source URL: https://sysportal.carnet.hr./node/1388

Links
[1] https://sysportal.carnet.hr./taxonomy/term/13