Ko se država znajde v temi

Razmah šifriranja komunikacij med običajnimi uporabniki

Matej Kovačič
matej.kovacic@ijs.si

9. konferenca kazenskega prava in kriminologije, 2016

Tehnologija in nadzor

V preteklosti je država tradicionalno imela praktično vedno dostop do komunikacij posameznikov.

- Prisluškovanje in elektronski nadzor sta postali eni najpomembnejših orodij v boju proti kriminalu.
- Nadzor komunikacij je mogoče tudi zlorabiti.

Tehnologija je pogosto zasnovana za (lažji) nadzor.

Po drugi strani pa tehnologija posameznikom omogoča, da se izognejo nadzorovanju...

Poskusi omejevanja kriptografije

Pritiski na raziskovalce iz področja kriptografije v ZDA:

- omejevanja predavanj na znanstvenih in strokovnih konferencah,
- finančni pritiski preko dodeljevanja raziskovalnih sredstev,
- Invention Secrecy Act (1951) - omejevanje patentiranja
- omejevanje izvoza (domača zakonodaja in mednarodni sporazumi),
- vsiljevanje šibkih kriptografskih standardov.

Vendar pa...

Sam obstoj močne kriptografije za represivne in obveščevalne organe ni tako problematičen, saj obstoj tehnologij zaščite še ne pomeni, da bodo posamezniki te tehnologije tudi **zares uporabljali**.

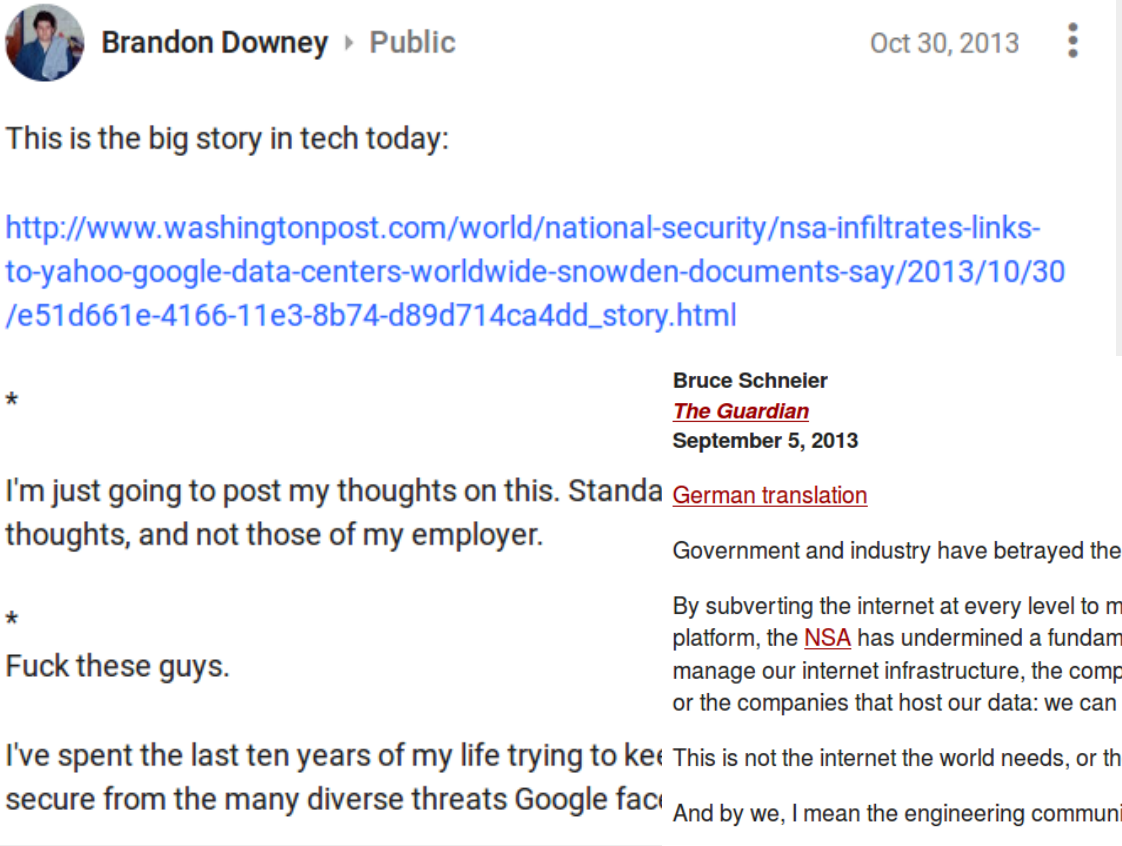
Kvalitetna tehnologija za zaščito komunikacij je bila **sicer javno dostopna**, vendar pa **ni bila implementirana** med najbolj razširjene komercialne rešitve.

Če pa že, je bila **zapletena** za uporabo, uporabniki pa so ob poplavi ranljivih in namerno okvarjenih rešitev težko ločili zrnje od plev.

Uporaba je bila zato omejena na peščico navdušencev, oziroma dostopna omejenemu krogu uporabnikov.

Junij 2013

Snowden…



Brandon Downey ▸ Public Oct 30, 2013

This is the big story in tech today:

http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html

*

I'm just going to post my thoughts on this. Standa
thoughts, and not those of my employer.

*

Fuck these guys.

I've spent the last ten years of my life trying to ke
secure from the many diverse threats Google fac

Bruce Schneier
The Guardian
September 5, 2013

German translation

Government and industry have betrayed the internet, and us.

By subverting the internet at every level to make it a vast, multi-layered and robust surveillance platform, the NSA has undermined a fundamental social contract. The companies that build and manage our internet infrastructure, the companies that create and sell us our hardware and software, or the companies that host our data: we can no longer trust them to be ethical internet stewards.

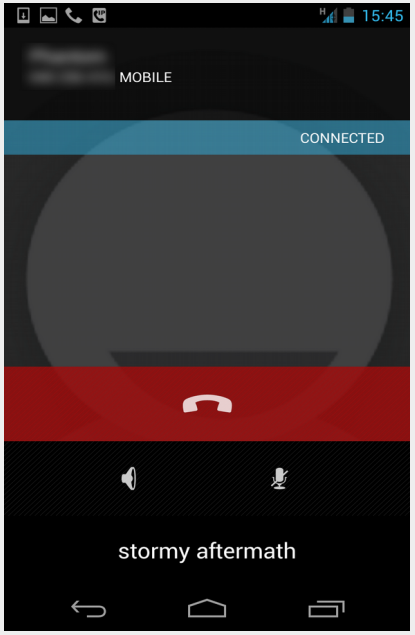
This is not the internet the world needs, or the internet its creators envisioned. We need to take it back.

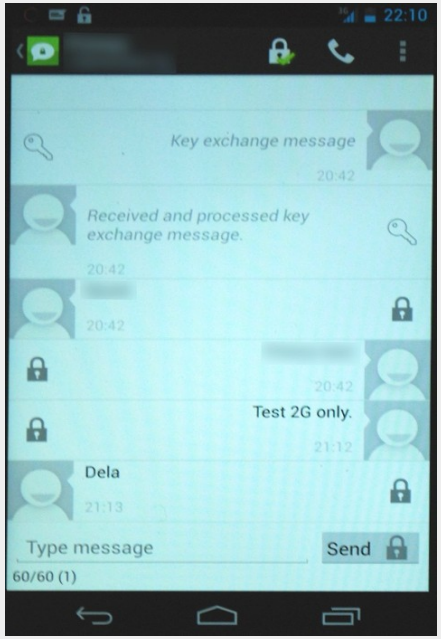
And by we, I mean the engineering community.

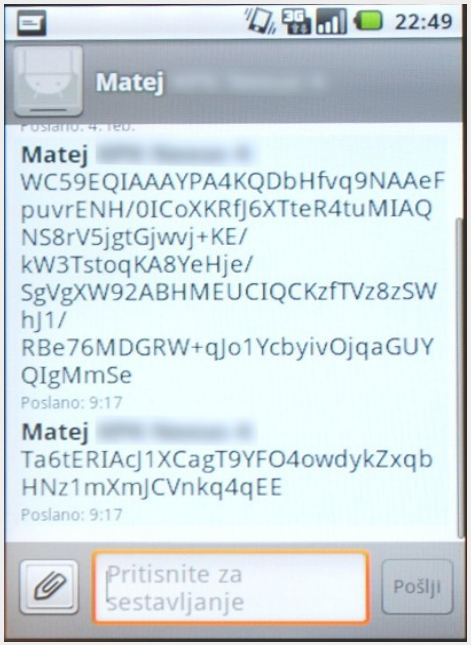
Yes, this is primarily a political problem, a policy matter that requires political intervention.

But this is also an engineering problem, and there are several things engineers can—and should—do.

Od koncepta do praktične implementacije







Rešitve Open Whisper Systems

Tehnična raven:

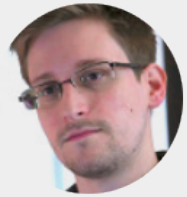
- algoritmi za močno šifriranje,
- poudarjena zaupnost,
- preverjanje napadov s posrednikom,
- »end-to-end« šifriranje,
- komunikacija poteka preko podatkovne povezave,
- komunikacija je lahko asinhrona,
- šifrirana podatkovna shramba sporočil in ključev.

Tehnična rešitev dejansko onemogoča prisluškovanje tako na komunikacijski povezavi, kot tudi pri »operaterju« sistema. Zagotavlja tudi določeno stopnjo anonimnosti.

Rešitve Open Whisper Systems

Uporabniška raven:

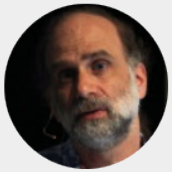
- enostavnost za uporabo,
- rešitev je brezplačna,



> Use anything by Open Whisper Systems.
>
> — **Edward Snowden**, Whistleblower and privacy advocate

> After reading the code, I literally discovered a line of drool running down my face. It's really nice.
>
> — **Matt Green**, Cryptographer, Johns Hopkins University

- programska koda aplikacije je prosto dostopna,
- prestala je več neodvisnih varnostnih testiranj.



> I am regularly impressed with the thought and care put into both the security and the usability of this app. It's my first choice for an encrypted conversation.
>
> — **Bruce Schneier**, internationally renowned security technologist

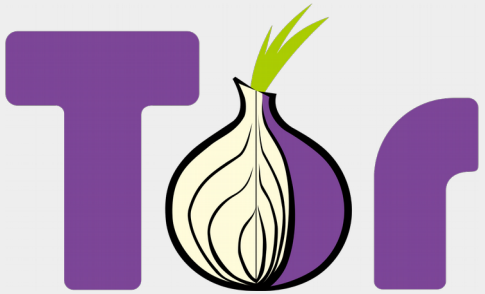
> Signal is the most scalable encryption tool we have. It is free and peer reviewed. I encourage people to use it everyday.
>
> — **Laura Poitras**, Oscar winning filmmaker and journalist

Prometni podatki?

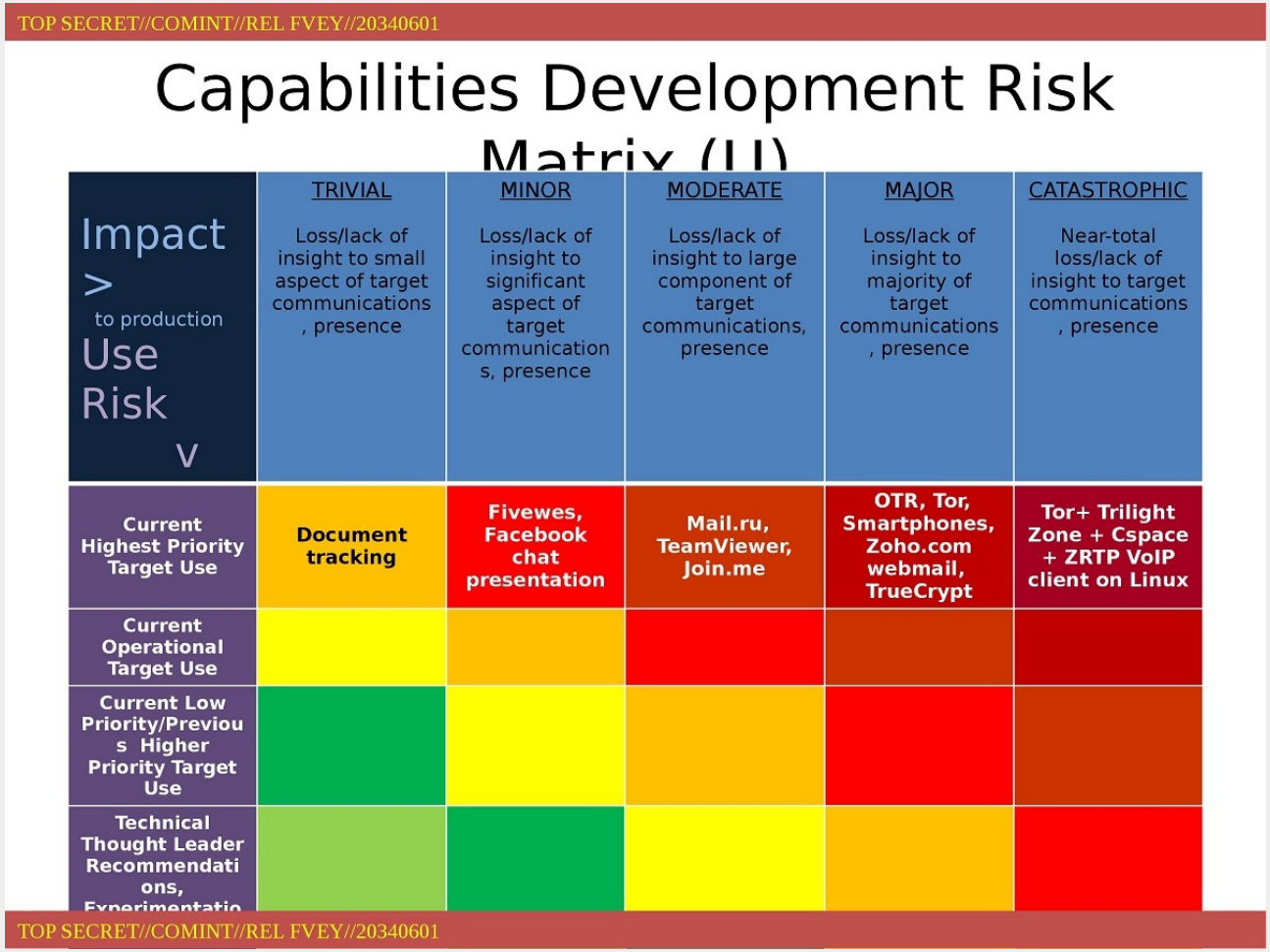
Prisluškovanje tehnično ni mogoče, kaj pa prometni podatki?

Attachment A

Account	Information
[redacted]	N/A
[redacted]	Last connection date: [redacted] Unix millis Account created: [redacted] Unix millis



Posledice za SIGINT



Things become "catastrophic" for the NSA at level five - when, for example, a subject uses a combination of Tor, another anonymization service, the instant messaging system CSpace and a system for Internet telephony (voice over IP) called ZRTP. This type of combination results in a "near-total loss/lack of insight to target communications, presence," the NSA document states. (Der Spiegel)

Signal protokol

Fundacija Open Whisper Systems leta 2013 razvije kriptografski protokol Signal.

Trenutna implementacija protokola:

- ***Facebook Messenger*** (julij 2015) – mesečno ima okrog milijardo aktivnih uporabnikov,
- ***WhatsApp*** (april 2016) – preko milijardo registriranih uporabnikov,
- ***Google Alo*** (september 2016) – od oktobra 2016 Google aplikacijo privzeto namešča na svoje mobilne telefone ***Pixel***,
- ***Viber*** (maj 2015) – delna implementacija – preko 100 milijonov mesečnih aktivnih uporabnikov.

Odziv države?

Nadzor se bo pomaknil še globlje v polje obveščevalne dejavnosti:

- izrabe varnostnih ranljivosti,
- podtikanje zlonamerne programske kode.

Prestrezanje pri viru.

Bundestrojaner/Staatstrojaner.

Napad preko IMSI lovilca.

Odziv države?

United States District Court,
S.D. New York.
UNITED STATES of America,
v.
John TOMERO, et al., Defendants.
No. S2 06 Crim. 0008(LAK).
Nov. 27, 2006.

MEMORANDUM OPINION

LEWIS A. KAPLAN, District Judge.

…

The government applied for a "roving bug," that is, the interception of Ardito's conversations at locations that were "not practical" to specify, as authorized by 18 U.S.C. § 2518(11)(a). Judge Jones granted the application, authorizing continued interception at the four restaurants and the installation of a listening device in Ardito's cellular telephone. The device functioned whether the phone was powered on or off, intercepting conversations within its range wherever it happened to be.

...

Toda, nadzor postaja čedalje bolj drag...

V zadnjih letih je informacijska varnost postala pomembna.

Programska koda se preverja za varnostnimi ranljivostmi.

Implementacija šifrirnih rešitev na vseh področjih.

Zakonodaja od podjetij zahteva, da osebne podatke in svoje sisteme varujejo na ustrezen način.

Proizvajalci so pričeli uporabnike čedalje bolj aktivno motivirati k nalaganju varnostnih posodobitev oz. jim le-te nalagajo samodejno.

Toda...

»Imamo eno infrastrukturo. Ne moremo si izbrati sveta, kjer ZDA lahko vohunijo, Kitajska pa ne more. Izberemo si lahko svet, kjer vsakdo lahko vohuni ali pa svet, kjer nihče ne more vohuniti. Lahko smo varni pred vsemi ali pa ranljivi do vseh.«

– Bruce Schneier

Vprašanja?