PRISM and an Agenda for European Network Security Research

Another Turn of the Wheel: Mainframe, Desktop, Cloud, Peer

Christian Grothoff

Technische Universität München

27.06.2013

Everybody Has Secrets

Everybody Has Secrets

- Business & Trade Secrets
- Political opinions
- Illegal activities

Everybody Has Secrets

- Business & Trade Secrets
- Political opinions
- Illegal activities

Everybody Has Secrets

- Business & Trade Secrets
- Political opinions
- Illegal activities

- Encryption: baseline
- Hide meta-data: state of the art
- Practice today?

Send everything to US in plaintext

- Guardian: “The PRISM program allows the intelligence services direct access to the companies servers.”
- Cooperating providers: Microsoft, Yahoo, Google, Facebook, PalTalk, YouTube, Skype, AOL, Apple

- Guardian: "The PRISM program allows the intelligence services direct access to the companies servers."
- Cooperating providers: Microsoft, Yahoo, Google, Facebook, PalTalk, YouTube, Skype, AOL, Apple
- Focus is on collection (storage!), not real-time evaluation
- Data collected: E-mails, instant messages, videos, photos, stored data (likely files), voice chats, file transfers, video conferences, log-in times, and social network profiles
- Tiny part of NSA: $20 M budget

- Guardian: “The PRISM program allows the intelligence services direct access to the companies servers.”
- Cooperating providers: Microsoft, Yahoo, Google, Facebook, PalTalk, YouTube, Skype, AOL, Apple
- Focus is on collection (storage!), not real-time evaluation
- Data collected: E-mails, instant messages, videos, photos, stored data (likely files), voice chats, file transfers, video conferences, log-in times, and social network profiles
- Tiny part of NSA: $20 M budget
- US discussion focuses on spying on US citizens and legality under US law

Frank Church (D-Idaho): “The NSA’s capability at any time could be turned around on the American people, and no American would have any privacy left, such is the capability to monitor everything: telephone conversations, telegrams, it doesn’t matter.”

TOP SECRET//SI//NOFORN

GAO

Global Access Operations

The mission never sleeps...

BOUNDLESSINFORMANT

Describing Mission Capabilities from Metadata Records

- NSA’s tool to track global surveillance data
- 2,392,343,446 records from the US
- 97,111,199,358 records worldwide
- This is for March 2013 alone

TOP SECRET//SI//NOFORN

GAO

Global Access Operations

The mission never sleeps...

BOUNDLESSINFORMANT

Describing Mission Capabilities from Metadata Records

- NSA's tool to track global surveillance data
- 2,392,343,446 records from the US
- 97,111,199,358 records worldwide
- This is for March 2013 alone
- Germany most surveilled country in Europe

TOP SECRET//SI//NOFORN

GAO

Global Access Operations

The mission never sleeps...

BOUNDLESSINFORMANT

Describing Mission Capabilities from Metadata Records

- NSA's tool to track global surveillance data
- 2,392,343,446 records from the US
- 97,111,199,358 records worldwide
- This is for March 2013 alone
- Germany most surveilled country in Europe
- "leverages FOSS technology"

Other Programs

- “The SIGAD Used Most in NSA Reporting” ⇒ there are more SIGINT tools
- Presentations list FARVIEW and BLARNEY
- Monitor fiber cables and infrastructure (IXPs?)
- “NSA collecting phone records of millions of Verizon customers daily” –Guardian

Other Programs

- "The SIGAD Used Most in NSA Reporting" ⇒ there are more SIGINT tools
- Presentations list FARVIEW and BLARNEY
- Monitor fiber cables and infrastructure (IXPs?)
- "NSA collecting phone records of millions of Verizon customers daily" –Guardian

We do not know all about PRISM. Repr. Sanches (D-Calif.), after learning more during a briefing, said there is … "significantly more than what is out in the media today (...) I believe it's the tip of the iceberg."

History: ECHELON

- SIGINT collection network of AU, CA, NZ, UK and US
- Baltimore Sun reported in 1995 that Airbus lost a $6 billion contract in 1994 after NSA reported that Airbus officials had been bribing officials to secure the contract.
- Used to facilitate Kenetech Windpower's espionage against Enercon in 1994-1996.

Former US listening station at Teufelsberg, Berlin.

Does it matter?

MPI estimated industrial espionage damage in 1988 at DM 8 billion.

So how does the EU react to learning about PRISM?

Does it matter?

MPI estimated industrial espionage damage in 1988 at DM 8 billion.

So how does the EU react to learning about PRISM?

"Direct access of US law enforcement to the data of EU citizens on servers of US companies should be excluded unless in clearly defined, exceptional and judicially reviewable situations."
–Viviane Reding, EC vice-president in response to PRISM

History: Irak War

Katharine Gun leaked memo from NSA agent Frank Koza in 2003 about an American effort to monitor the communications of six delegations to the United Nations who were undecided on authorizing the Iraq War and who were being fiercely courted by both sides:

> “As youve likely heard by now, the Agency is mounting a surge particularly directed at the UN Security Council (UNSC) members (minus US and GBR of course) for insights as to how to membership is reacting to the on-going debate RE: Iraq, plans to vote on any related resolutions, what related policies/negotiating positions they may be considering, alliances/dependencies, etc — the whole gamut of information that could give US policymakers an edge in obtaining results favorable to US goals or to head off surprises. In RT, that means a QRC surge effort to revive/create efforts against UNSC members Angola, Cameroon, Chile, Bulgaria and Guinea, as well as extra focus on Pakistan UN matters.”

The Utah Data Center at Bluffdale

NSA's lastest expansion (2013):

- 1-1.5 million square feet
- \$2 billion building, \$2 billin hardware
- 65 MW power consumption
  SuperMuc: < 3 MW, 155,656 cores, ≈ 3 Peta FLOPS

$\Rightarrow$ Likely able to store and process all communication

Not Just Monitoring

- US **controls** key Internet infrastructure:
  - Number resources (IANA)
  - Domain Name System (Root zone)
  - X.509 CAs and browser vendors

Technical Cooperation

Bloomberg reports:

- US companies provide internal information to US secret services
- Companies from software, banking, communications hardware providers, network security firms
- Including technical specifications and unpatched software vulnerabilities
- In return, these US companies are given access to intelligence information
- Partners include: Microsoft, Intel, McAfee

Political Solutions?

Ron Wyden (US Senate intelligence committe) asked James Clapper, director of national intelligence in March 2013:

“**Does the NSA collect any type of data at all on millions or hundreds of millions of Americans?**”

Clapper replied:

“**No, sir.**”.

The Enemy Within

"In February, The UK based research publication Statewatch reported that the EU had secretely agreed to set up an international telephone tapping network via a secret network of committees established under the "thrid pillar" of the Mastricht Treacty covering co-operation on law and order. (...) EU countries (...) should agree on international interception standards (...) to co-operate closely with the FBI (...). Network and service providers in the EU will be obliged to install tappable systems and to place under surveillance any person or group when served an interception order. These plans have never been referred to any European government for scrutiny (...) despite the clear civil liberties issues raised by such an unaccountable system. (...) The German government estimates that the mobile phone part of the package alone will cost 4 billion D-marks."

Scientific and Technological Options Assessment (STOA), "An Appraisal of Technologies of Political Control",

European Parliament, PE 166499, 6 January 1998.

Technical Solutions

Can we develop technologies to solve problems created by technology?

Technical Solutions

Can we develop technologies to solve problems created by technology?

- Hack back?

Technical Solutions

Can we develop technologies to solve problems created by technology?

- Hack back?
- Monitor them?

Technical Solutions

Can we develop technologies to solve problems created by technology?

- Hack back?
- Monitor them?
- Move data to European cloud?

Technical Solutions

Can we develop technologies to solve problems created by technology?

- Hack back?
- Monitor them?
- Move data to European cloud?
- Decentralize data and trust!

Decentralize Everything

- Encrypt everything end-to-end
- Decentralized PKI
- Decentralized data storage
- No servers
- No authorities

Decentralize Everything

- Encrypt everything end-to-end
- Decentralized PKI
- Decentralized data storage
- No servers
- No authorities

⇒ No jucy targets for APTs

Decentralized vs. Centralized

- Slower
- No economics of scale
- More complex
  - to use
  - to develop

Decentralized vs. Centralized

- Slower
- No economics of scale
- More complex
  - to use
  - to develop
- hard to secure
- hard to evolve

Decentralized vs. Centralized

- Slower
- No economics of scale
- More complex
  - to use
  - to develop
- hard to secure
- hard to evolve

- compromised