PGP KEY 0x2440DE65

Prism, Tempora & Co

Wie NSA & GCHQ die Sicherheit im Netz systematisch unterminieren, warum nun Wirtschaftsspionage im Raum steht und wie man das Radar der Dienste mit einfachen Methoden unterfliegen kann

erich@moechel.com

Saarbrücken EDVGT 2013 09 27

Entzauberung mit Folgen

- Die NSA hat nicht nur ihre eigenen Methoden enttarnt, sondern die aller Geheimdienste
- Wissen ist nicht mehr aus der Welt zu schaffen
- Suche nach Schwachstellen hat erst begonnen
- Kryptografie wird weltweit hochgefahren
- Verdacht auf Wirtschaftsspionage erhärtet
- "Das wird der US-Wirtschaft schaden" – erste Äußerung von EU-Kommissarin Viviane Reding

Das Narrativ der NSA

- "Wir haben schon immer Kommunikationen abfangen und auswerten können" **=>**
- "Deswegen brauchen wir nun flächen-deckenden Zugang zu den Glasfasernetzen,"
- "Wir können aktuell vier von zehn Kommunikationen entschlüsseln" **=>**
- "Wir haben zu wenige Hintertüren . Der Pfusch mit manipulierten Zufallszahlen, elliptischen Kurven & gmail hinter der https-Verschlüsselung abgreifen, ist mühsam."

Mythen aus Maryland II

- "Wir haben strengste interne Sicherheitschecks unserer Systeme. Alles verläuft strikt legal." **=>**
- "Muss NSA Legal Counsel hindrehen. IF NOT:

  Software Probs, Trainingsdefizite. **=>**
- "Es wird explizit mehr Funding gebraucht."
- "Ohne unsere Vertragsfirmen geht nichts. " **=>**
- "Wo sonst könnten wir nach der NSA Vice Presidents werden als bei den Contractors?"

NSA hat Krypto nicht geknackt

- Faktorierung AES 256 et al Lichtjahre entfernt
- Deshalb werden Implementation und Peripherie starker Kryptografie attackiert, wo es geht.
- 0 Zufall: Pseudo Random Number Generators
- Bekannte Kurven bei Elliptic Curve Crypto Algorithmen kürzen reale Schlüssellänge
- Alle Methoden "extrem fragil" Kleine Korrekturen an den globalen Set-Ups können komplette NSA-Programme binnen kurzem killen.

Strategische Fragilität

- Globale NSA-Datenakquise wird schwieriger.
- "Trust us, wir fangen Terroristen " - LOL
- Analyse abgefangener Kommunikation wird durch neue, interne Vorgaben verlangsamt
- Politische und technische Gegenmaßnahmen werden Effekt zusammen vervielfachen
- NSA-Systeme werden noch wesentlich komplexer und teurer, bei sinkender Effizienz
- NSA-Überwachungsansatz geht von naiven Usern aus, die US-Cloudservices benutzen

Start blurring your profiles!

- Gesunde Paranoia hilft gegen Überwachung, wie Fieber grippale Erkrankungen killt.
- Welche Services nütze ich wie oft, welche sind essentiell, wie sind sie kombinierbar?
- Firefox mit Plugins aufrüsten. Noscript, Ghostery, Tor-Plugin. Javascript nur wenn nötig,Third Party Cookies deaktivieren.
- Gebet Google was Googles ist, aber kein Bit mehr. Die anderen Bits kriegt die Konkurrenz.

Praktische Browser-Multiphrenie

- Mit Chrome z.B. in erster Linie Google Services nutzen, plus Bankverkehr oder pr0n.
- Kreditkarte nur mit Firefox, für Browsing dazwischen noScxript und Tor-Plugin aufdrehen.
- Oder: Facebook und Amazon nur mit Safari. Firmenaccounts, Banking nur mit IE.
- Etwas weniger Bequemlichkeit bringt viel mehr Sicherheit gegen Profiling und Kriminelle.

Etwas Skalierung gefälllig?

- Thunderbird mit Enigmail Plugin für E-Mail, PGP-Schlüssel mit Ablaufdatum vershen
- Jabber mit OTR-Plugin für Chat
- Virtual Private Networks nutzen oder selbst eines einrichten, einfacher als man glaubt
- Ältere PCs mit Linux reaktivieren, alte Handys entsperren, Pre-Paid SIMs.
- Special Use Cases für Anwälte und andere Berufsgeheimnisträger,
- All das muss nicht 100 prozentig sein.

Über die De-Skalierung

- Jede Maßnahme addiert neue Identifiers, mehr Schattenprofile, vervielfacht den Aufwand
- Verschlüsselte Alltagsmails helfen, die neuen Datencenter in Utah und Ft.Meade zu füllen
- Jede einfache Gegenmaßnahme bedingt mehrfache non-triviale Konter der NSA
- **Diese NSA-Systeme skalieren unter dieser Belastung nonlinear negativ**

Datatrolling the NSA

- **//TS NO MORE // SNCI // ALLFORN // CC Clearance required for attendants!**
- **CODE RESTRAINT / IN CAMERA**

erich.moechel.com
/munications

http//:fm4.ORF.at/erichmoechel

pgp key 0x2440DE65

fingerprint

A564 1457 71C3 E907 6D78 429E 76F3 C66E 2440 DE65

OTR signature, https upload

http://moechel.com/kontakt.html

kontaqt my second grade cousin

harkank@jabber.ccc.de @harkank