erich.moechel.com
/munications

# Die Crypto Wars - WikiLeaks 1.0

Die Methode, von Zensur bedrohte Dokumente durch Vervielfachung [Mirroring] zu immunisieren, ist fast so alt wie das Internet. Während der „Crypto Wars“ wurde gegen massiven Widerstand der Militärgeheimdienste so die Freigabe starker Verschlüsselungsprogramme für die Zivilgesellschaft durchgesetzt.

erich[at]moechel.com

Linz Kepler Salon 2011 01 24

# Abriss der Crypto Wars

- Bis 1970 war starke Verschlüsselung auschließlich in der Domäne der Militärs.
- 1976 Whitfield Diffie und Martin Hellman veröffentlichen Konzept für sichere Public Key Encryption.
- 1978 Ron Rivest, Adi Shamir und Len Adleman

  RSA-Methode zum Schlüsseltausch.
- 1978 – 1990 Stillstand, obwohl Konzepte, Methoden und Algorithmen bekannt waren.
- Die Cypherpunks formieren sich im Netz

# Die Anfänge von PGP

- 1991 Phil Zimmermann stellt Pretty Good Privacy ins Netz und erhält Besuch vom FBI
- 128 Bit Verschlüsselung, nur 40 Bit erlaubt
- Exportkontrollen, Kryptoprogramme werden in den USA als "Waffen" eingestuft.
- PGP-Quellcode vom MIT als Buch in einer scannerfreundlichen Version veröffentlicht.
- Die Cypherpunks sammeln sich auf der gleichnamigen Mailinglist.

# Geheimdienste als Treuhänder

- "Key-Escrow" und "Clipper Chip" – Pläne für Schlüsselhinterlegungspflicht
- 1994 Matt Blaze knackt den Clipper Chip. Gegen Zimmermann läuft Untersuchung
- 1995 EFF und ACLU: Kampaigns in den USA
- 1996 Gründung der Global Internet Liberty Campaign [GILC]. PGP hat bereits ein GUI
- Cypherpunks gründen Cryptome.org, Mutter aller WikiLeaks. "Samisdat Publishing"
- quintessenz veröffentlicht geheime Kryptographie-Empfehlungen der OECD

# PGP kommt nach Europa

- Banken und [IT]-Industrie fordern Freigabe starker Verschlüsselung für Webbrowser
- Netscape/IE dürfen nur 40 Bit verwenden, Knackzeit für NSA: Millisekunden
- PGP in Version 2.6. Norwegischer Klon 2.6.3 erscheint. PGP-Mirrors formieren sich
- US/UK Crypto Exportgesetze im Wassenaar Vertrag fortgeschrieben. 33 Staaten inkl. AT
- 1997 elf verschiedene "Flavours" von PGP
- Druck der Banken auf Regierungen steigt

# 1998 Krypto Showdown beginnt

- Wassenaar-Büro in 1010 Wien lokalisiert
- EFFs DES-Cracker knackt mittlerweile erlaubte 56 Bit DES Verschlüsselung
- PGP kommt in zwei Bänden nach NL. EU-Verkaufsstart kommerzielle Version.
- Electronic Frontiers Australia und quintessez koordinieren die GILC "Wassenaar Campain"
- Besuche im Wassenaar Office mit EFF/ACLU, zufällige Begegnungen mit interessanten Gesprächspartnern aus den USA

# Der Anfang vom Ende des Exportverbots

- Wassenaar Campaign [zwei Dutzend NGOs weltweit] wird von IT und Banken unterstützt.
- ECHELON Überwachungssystem von UK/USA kommt in die Medien. EU-Untersuchung beginnt
- 1999 Nachfolge-Campaign iCrypto organisiert weltweites Netz von PGP-Mirrors.
- PGP-Klon GnuPG für Linux- Betriebssysteme
- Deutschland, Frankreich heben Krypto-Exportverbote auf. Druck auf die USA wächst

# Crypto Wars: Hasta la victoria siempre!

- 2000 ECHELON Untersuchungsausschuss im EU-Parlament.
- Die USA geben auf, Exportkontrolle fällt
- Webbrowser werden durch starke Krypto erstmals sicher genug für Internetbanking.
- Firmen errichten weltweite, verschlüsselte VPNs, Industriespionage wird schwieriger.

erich.moechel.com
/munications

# Die Crypto Wars: Wikileaks 1.0

Freundlichen Dank für die Aufmerksamkeit!
Fragen?

http://moechel.com/kontakt

PGP Key ID 0x007DB429