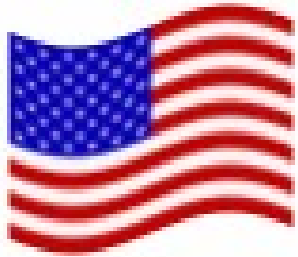


Staatliches Abhören – Wer, Wann, Was, Woraus?



Vortragender:
Alex Bihlmaier alex.bihlmaier@inf.fh-brs.de

Escrowed Encryption Standard

- April 1993, Clinton/Gore Administration
- Technik: NSA (Chip und symmetr. Verschl.)
- Gesetz: Implementierung in amerik. TK Geräte, Nutzung vorgeschrieben, Subvention
- Wettbewerb? Export von starker Krypto beschränkt

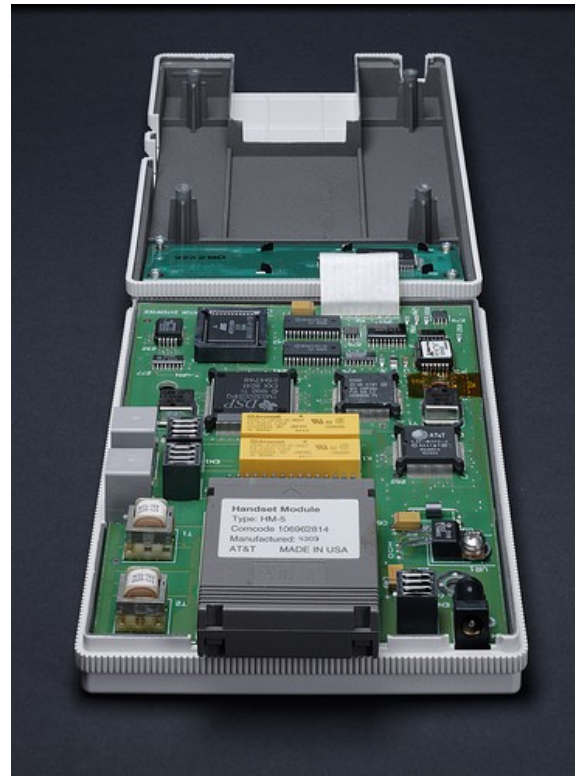
„Clipper-Chip“ -> Skipjack

- Verschlüsselungskomponente für Telefone, 1993 vorgestellt
- Entwicklung: NSA
- 1996 abgesetzt und verworfen
- 1998 Skipjack Algorithmus Public Domain



Das erste und einzige

- AT&T TSD-3600E Clipper Telefon
- US Regierung kauft kräftig ein... (\$ 1000 pro Gerät)
-Version ohne E am Ende war DES-basiert und hatte natürlich kein Backdoor



Schlüsselhinterlegung

- „key escrow“ - 2 Teile bei unterschiedlichen Behörden/Parteien
- Konkret:
- NIST & Department of Treasury
- EFF 1994: „key surrender“
- Vorgaben zur Schlüsselfreigabe schwammig; Dringende Fälle auch ohne richterliche Befugnis (-> BKA Gesetz?)

NIST



Patriot Act

- Oktober 2001 durch Bush in Kraft getreten, März 2006 dauerhaft verabschiedet
- Versch. Legalitäten im Bereich Personenfestsetzung, Einreise...etcpp.



Patriot Act

- Oktober 2001 durch Bush in Kraft getreten, März 2006 dauerhaft verabschiedet
- Versch. Legalitäten im Bereich Personenfestsetzung, Einreise...etcpp.
- Interessanter:
 - Wohnraumdurchsuchung ohne Mitwissen des Wohnraumbesitzers
 - Richter als Kontrollinstanz bei TK Überwachung weitgehend aufgehoben
 - CIA erhält Auftrag zur Inlandsermittlung



2001-???: Rasterüberwachung NSA

- Gesetzeswidrig von NSA (im Auftrag des Präsidenten); Abhörung von Telefonie/Internet von US Bürgern die mit vermuteten Terroristen kommunizieren ohne Gesetzesgrundlage oder Befugnisse
- Aktiv: Seit 2001
- Nach Aufdeckung durch New York Times: Präsident erklärte 2005 Teilaspekte für wahr
- Brisant: Whistleblower „Marc Klein“



2001-???: Rasterüberwachung NSA

- Nach 2008, aus „Marc Klein“ wird „Russel Tice“.
- <http://www.eff.org/deeplinks/2009/01/wistleblower-reveals-new-abuses-wiretapping-power>



FAA 2008 (FISA Amendments Act)

- US Gesetz, rückwirkende Immunität für TK Anbieter die am widerrechtlichen inländischen Abhörprogramm mitgewirkt haben
- Erlaubt: kommentarlose Einstellung von Verfahren gegen TK Anbieter
- Aktuell: Hepting ./ ATT

Deutschland: „Artikel 10 Gesetz“

- Artikel 10 Gesetz beschränkt Post und TK Geheimnis um staatliche Eingriffe, ohne Kenntnisnahme des Betroffenen, zu ermöglichen
- Wer: VS, MAD, BND (Überwachung durch PKG)
- Was: Abwehr von freiheitlichen Gefahren für die BRD & stationierte verbündete Truppen
- Wodurch: Überwachung TK & Brief/Postgeheimnis aufheben

