



Seminar IT-Security

Going Dark & Parallelen zu den Crypto Wars

Benjamin
Institut für Informatik

20. Februar 2018

Introduction

- Retrospektive

- Wachstum im Bereich ITK

- Senate Bill 266 (1991)

Key-Escrow

- Clipper Chip

- Skipjack

- Law Enforcement Access

- Review

- Towards Clippers Demise

Software-Key-Escrow & Key-Recovery

U.S. Maßnahmen

Zusammenfassung

Diskussionsteil

Introduction

Retrospektive
Wachstum im Bereich ITK
Senate Bill 266 (1991)

Key-Escrow

Clipper Chip
Skipjack
Law Enforcement Access
Review
Towards Clippers Demise

Software-Key-Escrow & Key-Recovery

U.S. Maßnahmen

Zusammenfassung

Diskussionsteil

- ▶ Kryptografie ist Domäne staatlicher Institutionen – Militär, Geheimdienste etc.
- ▶ Kryptografische Algorithmen unterliegen CoCom
 - ▶ Exporteinschränkungen bzw. Exportverbot – „United States Munitions List“
 - ▶ Lizenzzwang kritischer Technologien
 - ▶ 1992 Software Publishers Association (SPA) erlaubt eingeschränkten Export
- ▶ Unterscheidung von Technologien für In-/Ausland
- ▶ Beeinflusst Entwicklung im ITK-Bereich
- ▶ D.h. Versionen entweder mit beschränkter oder keiner Kryptografie
 - ▶ s. Data Encryption Standard (DES), Secure Sockets Layer (SSL) in Netscape etc.

- ▶ Fall des Sowjetblocks & Ende des Kalten Krieges
 - ▶ → kein Ende der Beschränkung
- ▶ „neue“ Gefahren wurden Zielsicher ausgemacht
 - ▶ Fiese Terroristen/ Kriminelle & andere subversive Elemente

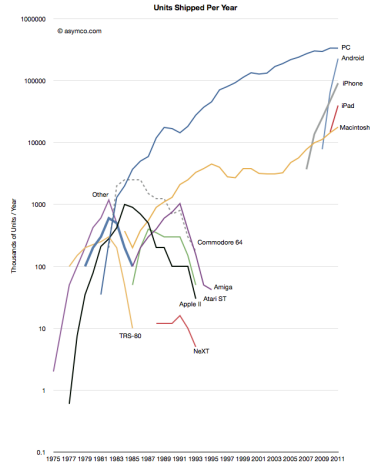


Abbildung: Absatz von Computern pro Jahr, übernommen von [Ded12]

It is the sense of Congress that providers of electronic communications services and manufacturers of electronic communications service equipment shall ensure that communications systems permit the government to obtain the plain text contents of voice, data, and other communications when appropriately authorized by law. ([Lev01])

Introduction

Retrospektive

Wachstum im Bereich ITK

Senate Bill 266 (1991)

Key-Escrow

Clipper Chip

Skipjack

Law Enforcement Access

Review

Towards Clippers Demise

Software-Key-Escrow & Key-Recovery

U.S. Maßnahmen

Zusammenfassung

Diskussionsteil

- ▶ Key-Escrow beschreibt Verfahren, bei dem zur Entschlüsselung notwendiger Schlüssel bei einer dritten (vertrauenswürdigen) Partei hinterlegt wird.
- ▶ D.h. in unserem Fall geben wir staatlichen Stellen einen „Zweitschlüssel“ mit Vertrauensvorschuss in die Hand.

Key-Escrow – Clipper Chip

- ▶ Krypto-Chipsatz entwickelt durch die National Security Agency (NSA)
- ▶ Ankündigung 1993 – Einstellung 1996
- ▶ Einsatzgebiet: Verschlüsselung von „voice and data messages“
- ▶ Soll staatlichen Stellen den Zugriff auf Daten ermöglichen – „built in backdoor“
- ▶ Jeder Chip ist ein Unikat – einzigartige Seriennummer (Unique-Identifizier (UID)) & geheimer Unique-Key (KU)



Abbildung: MYK-78 Clipper Chip, übernommen von [Goo09]

- ▶ Schlüsselaustausch via Diffie-Hellman
- ▶ Umsetzung des Key-Escrow durch Law Enforcement Access Field (LEAF)
- ▶ Verschlüsselungsalgorithmus für Payload: Skipjack
- ▶ Skipjack: Entwicklung der NSA – „classified SECRET“
 - ▶ Design aus den 1980igern – 1987 Beginn Entwicklungsphase [BDK⁺]
 - ▶ Symmetrischer 80-Bit-Key auf 64-Bit-Blöcken
 - ▶ Ähnlich dem DES-Algorithmus
 - ▶ Feistel-Chiffre
 - ▶ War durch Schlüsselgröße anderen Verfahren überlegen
 - ▶ Review war nur sehr beschränkt möglich – „Skipjack Review: Interim Report“ [Hof95, S. 119ff]
 - ▶ Freigabe („declassified“) durch NSA am 24.06.1998

► Nach Auguste Kerckhoffs – 1883

1. Das System muss im Wesentlichen (...) unentzifferbar sein.
2. **Das System darf keine Geheimhaltung erfordern (...).**
3. Es muss leicht übermittelbar sein und man muss sich die Schlüssel ohne schriftliche Aufzeichnung merken können (...).
4. Das System sollte mit telegraphischer Kommunikation kompatibel sein.
5. Das System muss transportabel sein und die Bedienung darf nicht mehr als eine Person erfordern.
6. Das System muss einfach anwendbar sein (...).

[Ker83]

1. Skipjack-Verschlüsselungsalgorithmus
2. 80-Bit-Family-Key (KF)
3. UID-Chip
4. 80-Bit-KU
 - ▶ erzeugt aus: 80-Bit-KU1 XOR KU2
5. Spezielle Kontrollsoftware

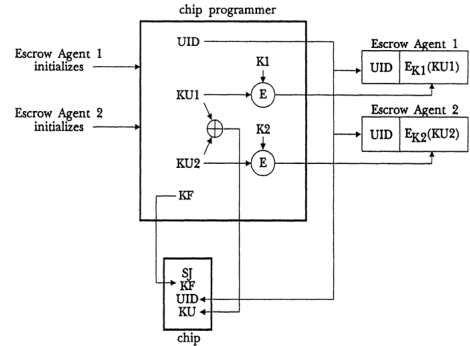


Abbildung: Initialisierung des Chips übernommen von [Hof95, S. 114]

- ▶ Voraussetzung: Key-Escrow-Fähiges System
- ▶ Handelt den geheimen Session-Key (KS) aus
- ▶ Nach Aushandlung des KS wird das LEAF aus KS & Initialization-Vector (IV) generiert
- ▶ Kontrollsoftware verschlüsselt KS durch KU
- ▶ Konkateniert verschlüsselten KS mit UID & Authentifizierer A
- ▶ Das wird alles nochmals mit dem KF verschlüsselt
- ▶ IV & LEAF werden an den Empfänger geschickt – Synchronisation & Validierung

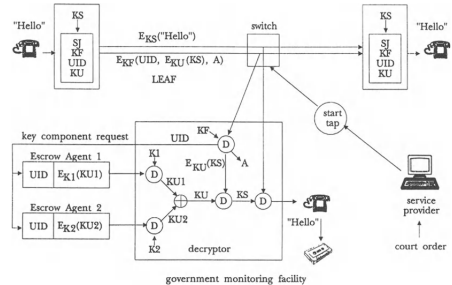


Abbildung: Initialisierung des Chips übernommen von [Hof95, S. 115]

- ▶ Ermöglicht staatlichen Institutionen Abhörmöglichkeit
- ▶ Nutzung an Bedingungen geknüpft:
 - ▶ Bestehende/Voraussehbare schwere Straftat
 - ▶ Abhörmaßnahme vielversprechend
 - ▶ Andere Untersuchungsmaßnahmen müssen Erfolglos/zu gefährlich gewesen sein
- ▶ Nur möglich durch richterliche Anordnung
- ▶ Entschlüsselung nur möglich, wenn beide Parteien Teilschlüssel zusammenfügen
- ▶ Mit Übertragung der verschlüsselten Schlüsselkomponenten wird Ablaufdatum übertragen
- ▶ Entschlüsselungsgerät vernichtet abgeleitete, abgelaufene Schlüssel „by design“

[Hof95, S. 116]

- ▶ Review durch Kryptologen – „Skipjack Review: Interim Report“ [Hof95, S. 119ff]
- ▶ Review unter Annahmen:
 - ▶ Risiko brechen von Skipjack durch Schlüsselraum absuchen ausgeschlossen/niedrig
 - ▶ Risiko brechen durch Short-Cut-Attacks gering
 - ▶ Stärke des kryptografisches Verfahrens unabhängig von der Geheimhaltung
- ▶ Bottom-Line: „Alles schick!“

- ▶ Clipper Chip wenig erfolgreich
- ▶ Wachsender Unmut
 - ▶ Datenschützern
 - ▶ Bürgerrechtlern
 - ▶ Verbrauchern
 - ▶ Akademia
 - ▶ Industrie
 - ▶ staatlichen Behörden (National Institute of Standards and Technology (NIST))
- ▶ Gegensteuern durch dubiose Artikel: „Don't Worry Be Happy: Why Clipper Is Good For You“ [Bak94]

- ▶ 1994 Matt Blaze „Protocol Failure in the Escrowed Encryption Standard“ [Bla94]
- ▶ Reverse-Engineering des Escrowed-Encryption-Standards (EES)
- ▶ Key-Recovery im LEAF möglich
- ▶ Brute-Force-Attack ermöglicht LEAF mit gleichen Hash-Wert, ergibt aber nicht die korrekten Schlüssel nach Escrow-Versuch
- ▶ Ermöglicht die Nutzung des (gute) Kryptografie Clipper Chips, ohne Key-Escrow
- ▶ 1995 Yair Frankel & Moti Yung veröffentlichen weitere Angriffsmöglichkeit – ebenfalls via LEAF, s. [FY95] et al.

Fahrplan

Introduction

- Retrospektive
- Wachstum im Bereich ITK
- Senate Bill 266 (1991)

Key-Escrow

- Clipper Chip
- Skipjack
- Law Enforcement Access
- Review
- Towards Clippers Demise

Software-Key-Escrow & Key-Recovery

U.S. Maßnahmen

Zusammenfassung

Diskussionsteil

- ▶ Versuch des Key-Escrows in Hardwareform gescheitert
- ▶ Erneuter Versuch – nun in Softwareform
- ▶ Firmiert unter dem Namen Software-Key-Escrow, Key-Recovery oder Commercial Key Escrow (CKE)
- ▶ Idee: Firmen sollen selbst Key-Escrow in Software implementieren
 - ▶ Flexibler & nutzbar in SW mit starker Krypto
 - ▶ Schlüssellänge auf 64 Bit begrenzt
 - ▶ Deal: Wenn IT-Branche auf Kuhhandel eingeht werden Krypto-Restriktionen gelockert

[WKB15, S. 8f]

Fahrplan

Introduction

- Retrospektive

- Wachstum im Bereich ITK

- Senate Bill 266 (1991)

Key-Escrow

- Clipper Chip

- Skipjack

- Law Enforcement Access

- Review

- Towards Clippers Demise

Software-Key-Escrow & Key-Recovery

U.S. Maßnahmen

Zusammenfassung

Diskussionsteil

- ▶ Stärkung der Kryptografie durch: Promotion of Commerce Online in the Digital Era (Pro-CODE)
- ▶ Security and Freedom Through Encryption (SAFE)
- ▶ 1997 Versuch die OECD zu beeinflussen Key-Escrow umzusetzen
 - ▶ Reaktion der OECD – Unterstützung von kryptografischen Verfahren [WKB15]
- ▶ Paper bekannter Krypto-Experten „The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption“[AAB⁺97] et al.
 - ... deployment of key-recovery-based encryption infrastructures to meet law enforcement's stated specifications will result in substantial sacrifices in security and greatly increased costs to the end user.*
- ▶ Bottom-Line: Komplexität extreme Hürde
- ▶ Übersteigt momentane Möglichkeiten, Kompetenzen in diesem Gebiet

- ▶ Rechtsstreit mit Bürgerrechtlern u.ä Organisationen
- ▶ Industrie & Wirtschaft kann auf Krypto-Markt durch Beschränkungen unzureichend Teilnehmen
- ▶ Beschränkung wirkt sich auf Softwareentwicklung aus etc.
- ▶ Rechtssicherheit nicht gegeben:
 - ▶ Bücher über Kryptografie – okay
 - ▶ konkrete Krypto-Algorithmen – okay
 - ▶ Sourcecode konkreter Algorithmen – okay
 - ▶ Binaries mit Krypto – geht gar nicht
 - ▶ Sourcecode veröffentlichen im Internet – ?
- ▶ 1996 Bill Clinton: Executive order 13026
- ▶ ... *the software shall not be considered or treated as 'technology'* ([oEA00])

Fahrplan

Introduction

- Retrospektive

- Wachstum im Bereich ITK

- Senate Bill 266 (1991)

Key-Escrow

- Clipper Chip

- Skipjack

- Law Enforcement Access

- Review

- Towards Clippers Demise

Software-Key-Escrow & Key-Recovery

U.S. Maßnahmen

Zusammenfassung

Diskussionsteil

- ▶ Versuch des Hardware-Key-Escrow gescheitert
- ▶ Software-Key-Escrow ebenfalls weitestgehend gescheitert
- ▶ Ablehnung von Restriktionen & Backdoors in großen Teilen der
 - ▶ Bevölkerung
 - ▶ Industrie
 - ▶ NGOs
 - ▶ ExpertenTM

Fahrplan

Introduction

- Retrospektive
- Wachstum im Bereich ITK
- Senate Bill 266 (1991)

Key-Escrow

- Clipper Chip
- Skipjack
- Law Enforcement Access
- Review
- Towards Clippers Demise





Software-Key-Escrow & Key-Recovery

U.S. Maßnahmen

Zusammenfassung

Diskussionsteil

- ▶ Nach Auflösung des Ostblocks – weiterhin Restriktionen gegenüber Kryptografie
- ▶ „Small Government“ – minimalistische Einschränkung durch den Staat in den U.S.A. durchaus populär

-  Hal Abelson, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Whitfield Diffie, John Gilmore, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller, and Bruce Schneier.
The risks of key recovery, key escrow, and trusted third-party encryption.
World Wide Web J., 2(3):241–257, June 1997.
-  Stewart Baker.
Don't worry be happy: Why clipper is good for you, 1994.
Letzter Aufruf: 19.11.2017.
-  E.F. Brickell, D.E. Denning, S.T. Kent, D.P. Maher, and W. Tuchman.
SKIPJACK Review Interim Report: The SKIPJACK Algorithm.
-  Matt Blaze.
Protocol failure in the escrowed encryption standard.
pages 59–67, 1994.



Horace Dediu.

The rise and fall of personal computing.

<http://www.asymco.com/2012/01/17/the-rise-and-fall-of-personal-computing/>, 2012.

Letzter Aufruf: 19.11.2017.



Yair Frankel and Moti Yung.

Escrow encryption systems revisited: Attacks, analysis and designs.

In Proceedings of the 15th Annual International Cryptology Conference on Advances in Cryptology, CRYPTO '95, pages 222–235, London, UK, UK, 1995. Springer-Verlag.



Travis Goodspeed.

Myk-78 "clipper chip" package markings.

https://commons.wikimedia.org/wiki/File:MYK-78_Clipper_chip_markings.jpg, 2009.

Letzter Aufruf: 19.11.2017.

Quellen III

-  Lance J. Hoffman, editor.
Building in Big Brother: The Cryptographic Policy Debate.
Springer-Verlag New York, Inc., New York, NY, USA, 1995.
-  Auguste Kerckhoffs.
La cryptographie militaire.
Journal des sciences militaires, IX:5–83, January 1883.
-  Steven Levy.
Crypto - How the Code Rebels Beat the Government—Saving Privacy in the Digital Age.
Penguin, New York, 2001.
-  Bureau of Export Administration.
Revised u.s. encryption export control regulations, 2000.
Letzter Aufruf: 19.11.2017.
-  Andi Wilson, Danielle Kehl, and Kevin Bankston.
Doomed to repeat history? lessons from the crypto wars of the 1990s.
2015.

DES Data Encryption Standard

LEAF Law Enforcement Access Field

KF Family-Key

NSA National Security Agency

SSL Secure Sockets Layer

SPA Software Publishers Association

UID Unique-Identifier

KU Unique-Key

KS Session-Key

IV Initialization-Vector

EES Escrowed-Encryption-Standards

NIST National Institute of Standards and Technology

CKE Commercial Key Escrow

SAFE Security and Freedom Through Encryption