SHA-1

Google Chrome warnt bald vor SHA-1

Hanno Böck

2014-09-14

- Rückblick Geschichte von MD5
- 1996: Erste theoretische Angriffe
- 2004: Praktische Kollissionsangriffe
- 2008: Erzeugung einer gefälschten Sub-CA mittels MD5-Schwäche
- 2011: Browser schaffen MD5-Support ab
- 2012: Flame-Virus nutzte unbekannte MD5-Schwäche für Angriff auf Microsoft Code-Signing

- Zeitleiste SHA-1
- 2004/2005: Immer bessere theoretische Angriffe, von finanzkräftigem Angreifer durchführbar
- 2011: CA/Browser-Forum Richtlinien zur Abschaffung von SHA-1
- 2013: NIST empfiehlt SHA-1 mehr zu benutzen (und hält sich selbst nicht dran)
- 2013: Microsoft kündigt Abschaffung für 2017 an
- 2014: CAs ignorieren alles und nutzen weiter SHA-1

- Chrome wird in verschiedenen Eskalationsstufen vor SHA-1-signierten Zertifikaten warnen, die über 2016/2017 hinaus gültig sind
- Opera will mitziehen, Microsoft wird wohl an 2017-Plan festhalten
- SHA-256 nutzen (SHA-512 ist kompatibilitätstechnisch problematischer und SHA-3 ist noch nicht fertig)
- Testen: `https://shaaaaaaaaaaaaa.com/`

- Bemerkenswerte Entwicklung: Browserhersteller macht Druck auf CAs, so dass diese sich nicht mehr alles erlauben können
- Bisher galt das ungeschriebene Gesetz dass kein Browserhersteller sich traut, bei HTTPS mehr Security zu enforcen, wenn dadurch irgendetwas potentiell bricht
- Und CAs konnten sich fast alles erlauben
- Macht Hoffnung. TLS/HTTPS/X.509 ist im Moment eine große Baustelle (siehe auch mein Talk Easterhegg), aber mit TLS 1.3, Key Pinning, Certificate Transparency etc. stehen einige Technologien in den Startlöchern, die die größten Probleme reparieren würden

- Fragen?
- `https://hboeck.de/`
- PGP: BBB51E42
- Fingerprint: FE73 757F A60E 4E21 B937 579F A588 0072 BBB5 1E42