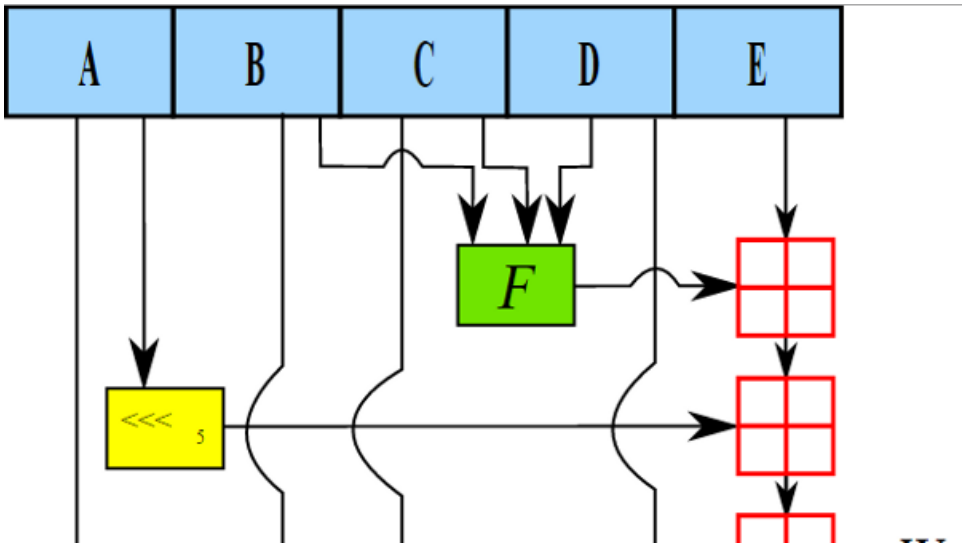
Todesstoß für SHA-1 steht bevor

16.10.2015 18:11 Uhr – Dennis Schirrmacher vorlesen



Ein erster praktikabler Angriff von Sicherheitsforschern auf SHA-1 verschärft die

Aussage, dass die Hashfunktion nicht mehr zum Einsatz kommen sollte.

Sicherheitsforscher haben die seit einem Jahrzehnt als unsicher geltende kryptologische Hashfunktion SHA-1 erfolgreich attackiert. Dafür haben sie ein 64-GPU-Cluster zehn Tage lang rechnen lassen. In einem ausführlichen Bericht erläutern sie ihre Vorgehensweise (PDF-Download).

Die sogenannte SHA-1-Kollision bricht den Sicherheitsforschern zufolge die Hashfunktion aber noch nicht komplett auf. Der Ansatz gebe aber einen Ausblick, wann es soweit sein könnte und die Sicherheitsforscher gehen von einer baldigen Kompromittierung aus. Frühere Berichte prophezeiten das für das Jahr 2017.

SHA-1 kostengünstiger und schneller knacken

Schon seit 2005 existieren theoretische Kollisionsattacken auf SHA-1, die die Sicherheitsforscher ausgebaut haben. Ihr Ansatz zeigt auf, dass Grafikkarten die Berechnungen besonders effizient stemmen können. Das geht nicht nur schneller als mit CPUs, sondern senkt auch die Kosten.

Aufgrund ihrer Erkenntnisse raten die Sicherheitsforscher dringlich dazu, SHA-1 zeitnah nicht mehr einzusetzen. Zudem sprechen sie sich gegen das Vorhaben des CA/Browser Forums aus, die Verteilung von SHA-1-Zertifikaten bis zum Ende des Jahres 2016 zu verlängern.

Der beteiligte Sicherheitsforscher Marc Stevens war auch Teil des Teams, das bereits MD5 den Todesstoß versetzt hat. Dabei nutzten die Forscher eine Kollision mit MD5, um sich selbst ein CA-Zertifikat zu erstellen, das von allen Browsern akzeptiert wurde. (des)

Kommentare lesen (83 Beiträge) « Vorige | Nächste »

Forum zum Thema: **Serversicherheit**

60 28

http://heise.de/-2849484 Drucken

Mehr zum Thema **Hash-Funktion Grafikkarten MD5**

Analysiert: Lego Mindstorms für Cyber-Angriffe missbraucht

In einer deutschen Forschungseinrichtung arbeiten auch Lego-Roboter im Dienste der Wissenschaft. Eines Tages entwickelten diese jedoch ein gefährliches Eigenleben. Mehr…

Router auf WPS-Lücken testen

Viele WLAN-Router weisen die sogenannte PixieDust-Lücke auf, über die sich Angreifer ganz einfach Zugang zu Ihrem Netz verschaffen können. Kommen Sie denen zuvor und testen Sie Ihr eigenes Funknetz. Mehr…

Analysiert: Google-Interna im Second-Hand-Shop

Ein in Deutschland gekaufter Gebraucht-Router hatte offenbar einen prominenten Vorbesitzer. Es lieferte den neuen Besitzern interessante und brisante Einblicke in die Infrastruktur von Google – einschließlich Zugangsdaten. Mehr…

Alle Artikel im Überblick...