# Why the Security of USB Is Fundamentally Broken


Die Karte zeigt übrigens eine Reiseroute, die ich 1982 geplant hatte. Meine damalige Lebensabschnittsgefährtin wollte dann aber doch nicht durchs Darien Gap (awesome story!) marschieren. (Ja! Zu Fuß und per Boot und nicht per Jeep! Das geht!) Wir sind (leider) von Panama nach Kolumbien geflogen. Ich weiß nicht, ob ich da jemals noch hinkomme. Allein würde ich das nicht machen, aber eine Lebensabschnittsgefährtin müsste schon sehr tough sein.

Wired: „Why the Security of USB Is Fundamentally Broken“:
*Computer users pass around USB sticks like silicon business cards. Although we know they often carry malware infections, we depend on antivirus scans and the occasional reformatting to keep our thumbdrives from becoming the carrier for the next digital epidemic. But the security problems with USB devices run deeper than you think: Their risk isn’t just in what they carry, it’s built into the core of how they work.*

Das wäre ja noch schöner, wenn ich USD-Sticks fremder Leute an meine Rechner ließe. Autostart via USB – ohne meine jeweilige ausdrückliche Erlaubnis? Igitt. (Und natürlich ist unter Windows auch mein BIOS verrammelt und verriegelt.)

*All manner of USB devices from keyboards and mice to smartphones have firmware that can be reprogrammed—in addition to USB memory sticks, Nohl and Lell say they've also tested their attack on an Android handset plugged into a PC.*

Das Problem haben Karsten Nohl (Security Research Labs GmbH, Berlin, und Jakob Lell (Blog) aufgedeckt. Das Thema wird auch auf der Blackhat 2014 vorgestellt werden:

*This talk introduces a new form of malware that operates from controller chips inside USB devices. USB sticks, as an example, can be reprogrammed to spoof various other device types in order to take control of a computer, exfiltrate data, or spy on the user. We demonstrate a full system compromise from USB and a self-replicating USB virus not detectable with current defenses.*

Ich gehöre nicht zu den Leuten, die Artikel schreiben mit dem Tenor „das Ende ist nahe". Panikmache ist fehl am Platz. Das mag daran liegen, dass ich nicht für Geheimdienste arbeite, wie mir von einigen Verschwörungstheoretikern vom CCC seit meher als einem Jahrzehnt immer wieder unterstellt wird (vermutlich arbeiten gerade die für Geheimdienste). Die meisten Artikel in deutschen Medien über das obige Thema hinterlassen Laien mit dem Gefühl zurück: Die sind schon drin in meinem Computer, und man kann eh nichts tun. Das halte ich für kontroproduktiv, defätistisch und erst recht im Sinne der Dienste.

Ich sehe gerade, dass Heise etwas zum Thema berichtet. (Hätte ich mir denken können, ich bin über Bruce Schneider zur Wired gekommen.)

*Die Kommunikation zwischen PC und USB-Sticks setzt auf das altbewährte SCSI-Protokoll auf. Dabei implementieren die Controller-Chips der Sticks mehr oder weniger SCSI-konform zusätzliche Hersteller-spezifische Erweiterungen. Über die kann Software auf dem PC dann etwa die Firmware des Sticks*

*auslesen und auch einen neue, etwas modifizierte Firmware schreiben. Sicherheitsfunktionen, die dies irgendwie absichern würden, gibt es in der Regel nicht. (…) Um dann wiederum weitere Sticks zu infizieren, benötigt der Schadcode zwar Systemrechte, doch die lassen sich in der Regel ohne allzu großen Aufwand beschaffen – insbesondere, wenn man bereits „an der Tastatur sitzt.*

Also ich weiß nicht. Das ist ja alles logisch, aber funktioniert nur unter bestimmten Voraussetzungen. Wie will jemand zum Beispiel an mein System-Passwort kommen?

Der Heise-Artikel zeigt auch anschaulich, dass Antiviren-Software Schlangenöl ist. Quod erat demonstrandum.