| Erstellt am: Montag | 05.05.2008 | 07:0(

Die Chip-Paranoia der US-Militärs
In Radaranlagen, Jets und anderem Equipment sind Millionen von nie völlig durchgetesteten ASIC- und FPGA-Bausteinen aus Fernost verbaut. Unter den Militärs steigt die Befürchtung, dass darunter "Hardware-Trojaner" sind, die über einen feindlichen Funkimpuls alle möglichen Systeme deaktivieren könnten.

Am Donnerstag lief in der Defense Advance Research Projects Agency [DARPA] des Pentagon ein neues Großprojekt an, Hunderte Millionen Dollar sind jährlich dafür budgetiert.

Die DARPA wurde beauftragt, eine "National Cyber Range" aufzubauen, also einen Übungsschießplatz für den vernetzten Krieg.

NSA-Hackerteams
Dabei sollen "groß dimensionierte heterogene Netzwerke" wie die "C4"-Kommandozentralen der Armee - "C4" bedeutet "Command, Control, Computer, Communications" - samt angeschlossenen Rechnern abgebildet werden, um Angriffe simulieren zu können.

In der vergangen Woche ging zudem eine Übung der National Security Agency über die Bühne, in der NSA-Hackerteams vier Tage lang die Netzwerke der Akademien von Army, Navy, Air Force und Coast Guard angriffen.

Der vernetzte Krieg
Wie der "Monterey Herald" berichtet, konnten die IT-Sicherheitstechniker der Naval Postgraduate School ihr Netz vier Tage lang gegen die angreifenden NSA-Kollegen verteidigen, aber eben nicht ganz.

99,4 Prozent Sicherheit erwiesen sich als zu wenig, denn die einzige erfolgreiche Attacke, die durchkam, brachte den Angreifern den Sieg.

Fremde Komponenten
Die Netzwerke sind dabei längst nicht die einzige Stelle, an der die Supermacht USA verwundbar ist.

Wie alle anderen Abnehmer aus dem Zivilbereich von Unterhaltungselektronik bis PC-Industrie lässt auch das Pentagon in allem nur denkbaren Gerät Abermillionen vor allem in Fernost produzierter elektronischer Komponenten verbauen.

Jets, FPGAs und ASICs
Die Produktionsstätten für FPGAs [Field Programmable Gate Arrays] und ASICs [Application Specific Integrated Circuits] sind seit den 70er Jahren sukzessive nach Fernost verlagert worden.

Und nun plagt die US-Militärs die zunehmende Sorge, dass unter diesen Chips auch solche sein könnten, die neben ihrer eigentlichen Funktion noch weitere Schaltungen enthalten, die höchst gefährlich sind.

Abschuss per Funksignal
Das Szenario: US-Kampfjets stürzen ab, sobald sie in Tiefflug übergangangen sind, weil die automatische Geländeabtastung plötzlich ausgefallen ist.

Dem vorausgegangen war ein kurzes feindliches Funksignal vom Boden, das vom "Terrain Following Radar" des Fliegers empfangen wurde.

Hardware und Hintertüren
"Natürlich ist es relativ einfach, Backdoors in Hardware unterzubringen, die Frage ist nur, wie man sie aktiviert, wenn man die Schaltung nicht kennt, in die der entsprechende Chip verbaut ist. Bei FPGAs müsste man so an allen Anschlusskontakten lauschen, da die Nutzschaltung ja erst durch die Programmierung entsteht", sagte der Computer-Forensiker Peter Franck am Sonntag zu ORF.at.

FPGAs
Da diese FPGAs, wie schon ihr Name sagt, "field programmable", also nachträglich umprogrammierbar sind, sieht Franck die Gefahr hier weniger in ab Fabrik eingebauten Hintertüren oder Abschaltfunktionen.

Auslöser der Gefahr könnten bei FPGAs weit eher Personen sein, die physischen Zugang zu militärischem Gerät haben. Ein beliebiges Beispiel wäre, ein FPGA, das in Funkgeräten zur Verschlüsselung benützt wird, nachträglich so zu modifizieren, dass der Schlüssel im Klartext mit übertragen wird.

"Mixed Mode"-ASICs
"Anders als bei FPGAs ist die genaue Funktion von ASIC-Bausteinen bereits bei deren Herstellung definiert, daher ist klar, welches Signal an welchem PIN zu erwarten ist. Hier lassen sich natürlich jede Menge Backdoor-Funktionen einbauen", sagt Franck.

"ASICs werden auf Grund ihrer Schnelligkeit häufig in der Signalverarbeitung eingesetzt. In Funkempfangsanlagen lässt sich eine 'Sonderfunktion' der Bausteine durch ein charakteristisches Eingangssignal triggern." Am ehesten sei das in "Mixed Mode"-ASICs - in analog-digitalen Hybridchips - möglich, wie sie in allen militärischen Radar- und Funkanalagen enthalten sind.

"Kill Switch"
Das könnte etwa dazu führen, dass bestimmte, in Waffensysteme integrierte Halbleiterbausteine sich plötzlich abschalten, wenn sie ein bestimmtes Funksignal empfangen.

Wie die renommierte US-Fachzeitschrift IEEE-Spectrum am Wochenende berichtete, hat das Problem auch bereits einen Namen: "Kill Switch". Einen derartigen Ausschalter in einem leistungsfähigen und entsprechend komplexen Halbleiter zu entdecken ist alles andere als einfach.

Einer von Millionen Transistoren
"Im Prinzip genügt für die Abschaltfunktion ein einziger von Millionen

Transistoren in einem Schaltkreis", sagt Franck, Signalerkennung und Verarbeitung seien mit etwas mehr rechnerischem Aufwand verbunden.

Diesen Zusatzmechanismus in einem ASIC zu verbergen sei relativ einfach, die Manipulation nachträglich zu entdecken sei hingegen äußerst schwierig.

Baupläne von Drittfirmen
Zudem würden von den Chipherstellern auch sehr häufig Baupläne von Drittfirmen integriert, sagt Franck: "Wird für ein ASIC eine bestimmte Komponente, sagen wir ein MPEG-Decoder für militärische Videoanwendungen, benötigt, so lizenziert man in der Regel eine existierende Schaltung und integriert sie in das Chipdesign. Das ist wesentlich billiger, als selbst einen Decoder zu entwickeln."

Technik-Globalisierung
Ein derartiger Chip eines koreanischen Herstellers für die Bordelektronik eines US-Kampfflugzeugs kann so Designelemente aus Drittsstaaten wie China und sogar Russland enthalten.

Da es auch für die US-Militärs beim heutigen Stand der Technik-Globalisierung schlichtweg nicht möglich ist, die benötigten Elektronikkomponenten ausschließlich in den USA fertigen zu lassen, wurde ein aufwendiges Programm zur nachträglichen Analyse installiert.

Das "TRUST in Integrated Circuits Program" der DARPA sieht die systematische Hardware-Analyse von ASICs und FPGAs vor, die in militärischem Equipment verbaut werden.

Seziert durch Ionenstrahlen
Dazu kommt eine Mixtur aus technischen und mathematischen Analyse- und Bearbeitungsmethoden der Hardware zum Einsatz: Beschuss mit Ionenstrahlen anhand von Daten aus dem Elektronenmikroskop, fortgeschrittene Mustererkennung und andere exotische Seziermethoden.

Im IEEE-Spectrum ist auch der jüngste bekanntgewordene Fall von spektakulärem Versagen der Elektronik eines militärischen Geräts zitiert.

Syriens russisches Radar
Beim Luftschlag der israelischen Armee gegen eine Atomanlage in Syrien vom September 2007 waren eher betagte israelische F-15 und F-16 ohne Tarnkappenfunktion in den syrischen Luftraum eingedrungen.

Warum das von den Russen gelieferte neue Radarsystem der Syrer nicht funktionierte, ist seitdem in Diskussion.

Die IEEE-Zeitschrift zitiert einen Insider des Rüstungsgeschäfts, der erwähnte, dass eine französische Rüstungsfirma zum Beispiel manipulierte Chips in ihr Gerät verbaue, um es ferngesteuert zu deaktivieren, falls es in feindliche Hände falle.

"Wer Waffen an andere Länder liefert, wird sicherstellen, dass sie nicht gegen die eigenen Interessen eingesetzt werden können, das ist nur logisch", sagt Franck, der 2003 im Rahmen

der UNO-Mission im Irak als Waffeninspektor irakische Militärcomputer nach Spuren von Massenvernichtungswaffen durchsuchte.

Das Hardware-Analyseprogramm der DARPA
IEEE-Spectrum-Artikel
Im Zivilberuf rettet Peter Franck Daten

Globalisierung und Netzwerkkrieg

Was den "netzwerkzentrierten" Krieg angeht - seit 1996 eine US-Militärdoktrin -, so zeigt sich die Globalisierung wie schon gewohnt manichäisch.

So werden im wohlhabenden Teil der Welt gerade Grundnahrungsmittel zu Treibstoff verarbeitet, was dazu beiträgt, dass unter dem nicht-motorisierten Großteil der Weltbevölkerung regional Hungersnöte ausbrechen.

Die Billiglohnländer des Fernen Ostens wiederum haben ihr Wachstum nicht zuletzt dem Umstand zu verdanken, dass dort seit mehr als zwei Jahrzehnten jene elektronischen Komponenten entworfen und produziert werden, die auch für den Netzwerkkrieg der Supermacht USA ein "Must-have" sind.

[futurezone | Erich Moechel]