Schutz der IIoT-Infrastruktur

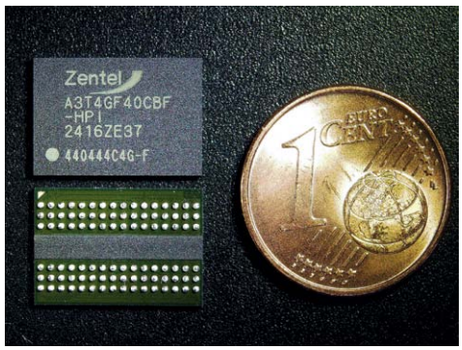
The Great DRAM-Firewall

Zentel hat kürzlich seinen Row-Hammer-immunisierten DDR3-DRAM-Chip mit integriertem Error-Correction-Code (ECC) für Automotive Grade 2 qualifiziert – nicht vorrangig für Autos, sondern um die eigenen Stromnetze vor feindlichen Cyberangriffen zu schützen.

Bilder: Zentel

Seit Verbreitung der dritten DDR-DRAM-Generation vor zehn Jahren wurde publik, dass DDR3-DRAMs in IoT-Systemen eine latente Schwachstelle und ein potenzielles Einfallstor über die Hardware darstellen für getarnte Cyberangriffe aus dem Internet mittels äußerst raffiniert manipulierter Websites – sogar vorbei an allen relevanten Schutzvorkehrungen auf Softwarebasis wie Firewalls, Antivirus-Apps oder Betriebssystem-Patches, und zwar ohne forensische Spuren im flüchtigen Hauptspeicher zu hinterlassen: »no smoking gun«.

Seitdem gibt es ein nicht enden wollendes Katz-und-Maus-Spiel zwischen der DRAM-Industrie und einer hochprofessionellen Hackerelite. Dazu zählen auch Professoren an der ETH-Zürich und deren Forschungsteams wie »SAFARI« um Prof. Onur Mutlu und die Computer-Security-Group um Prof. Kaveh Razavi. Erst kürzlich wurde die SAFARI-Publikation »RowPress: Amplifying Read Disturbance in Modern DRAM Chips« vom Fachjournal IEEE Micro zum Top-Pick des letzten Jahres gekürt. Darin wurde enthüllt, dass auch neuere DRAM-Generationen nicht gegen Row-Hammer-typische Angriffe gefeit sind, insbesondere wenn die Aktivierungsspanne für gezielt angegriffene Datenzeilen erheblich ausgedehnt wird. Im RowPress-Paper wird gezeigt, dass die Row-Hammer-anfälligen Zellen nicht mit den RowPress-anfälligen Zellen überlappen, daher ist dieser Effekt »Row-Hammer-ähnlich«.



Der Row-Hammer-geschützte 4-Gbit-DDR3L-DRAM-IC »A3T4GF40CBF-HP« mit integriertem Error-Correction-Code und proprietärem Bitflip-Overflow-Alarm für den Controller ist inzwischen in Automotive-Grade 2 erhältlich, um Stromnetze vor Cyberangriffen zu schützen.

Die DRAM-Industrie hatte vergeblich gehofft, durch Einführung eines erstmals mit dem DDR4-JEDEC-Standard möglichen Target-Row-Refresh (TRR) und »Hütchenspielertricks« – durch proprietäre Verschleierung der physischen Datenzeilen-Adressen – Cyberangriffe auszumanövrieren. Im Mai 2020 präsentierte das Forschungsteam »VUSec« unter maßgeblicher Mitwirkung von Kaveh Razavi an der Vrije Universiteit Amsterdam auf dem pandemiebedingt virtuell abgehaltenen »IEEE Symposium on Security and Privacy« das Paper »TRRespass: Exploiting the Many Sides of Target Row Refresh«, das bei DDR4-DRAMs der drei führenden Hersteller (mit 94 Prozent globaler Marktabdeckung) durch einen FPGA-basierten Fuzzing-Algorithmus das Versteckspiel umgehen konnte. Ebenso hat ein früheres Paper »RAMBleed: Reading Bits in Memory Without Accessing Them« die Fachwelt aufgerüttelt, indem es zeigte, dass man in DDR3-DRAMs aller Top-3-Hersteller einen eigentlich vom Betriebssys-

tem in versperrten Arbeitsspeicherbereichen versteckten RSA-2048-Entschlüsselungscode und Passwörter mit einem Row-Hammer-Zangenangriff auf mehr als eine Datenzeile fernauslesen – unter anderem auch in Smartphones – und mit den ausgespähten Administratorrechten ganze Netzwerke kapern konnte.

Letzte Nagelprobe für erste Row-Hammer-geschützte DDR3-DRAM-ICs

Inzwischen hatte Kubo Takashi, CTO von Zentel in Japan, 2-Gbit- und 4-Gbit-DDR3L-Chips mit einer neuartig integrierten Row-Hammer-Watchdog- und -Fangschaltung aus Zählerbaum- und SRAM-Strukturen entwickelt. Allerdings kamen sie für DDR4-DRAM-ICs mit ihren typischerweise höheren Speicherdichten nicht infrage. Denn wegen des ungleich höheren zusätzlichen Chipflächenbedarfs und einer entsprechend geringeren Waferausbeute würden sie so teuer, dass sie im gnadenlosen DRAM-Preiswettbewerb unverkäuflich würden. Zwar trifft dieser Kostennachteil auch auf geschützte DDR3L-ICs zu, aber in einem minder preiskritischen Rahmen. Immer noch gibt es viele ambitionierte IoT-Anwendungen selbst in Verbindung mit UHD-Displays oder entsprechend hochauflösenden Digitalkameras, für die DDR4-DRAMs mit ihren höheren Taktraten und Speicherdichten einen Overkill darstellen würden. Die Anforderung einer zusätzlichen Fangschaltung kam ursprünglich aus der HDD/SSD-Industrie zum Schutz des DRAM-Cache vor Datenkorruption oder Ausspähung. Auf Kubo Takshis industrielle Expertise stützte sich das ETH-COMSEC-Team um Prof. Kaveh Razavi unter anderem bei der Entwicklung eines ultimativ verschärften Testalgorithmus mit dem Arbeitstitel »Blacksmith: Scalable Rowhammering in the Frequency Domain«. Als beratender Unterstützer des Teams aus der industriellen DRAM-Chipdesign-Perspektive und Mitautor verschiedener Publikationen hatte er Zugriff auf den Testalgorithmus für DDR4-DIMM-Module und portierte den auf ein automatisches Test-Equipment für seine Row-Hammer-geschützten DDR3L-DRAM-ICs zu seiner Vergewisserung, dass die auch diesem final verschärften Row-Hammer-Test standhielten.

Das Hardware-Cybersecurity-Dilemma – zwei Seiten einer Medaille

Im Juni 2024 referierte Prof. Kaveh Razavi beim Cyb3r Spotlight Event in Oerlikon zum Stand der Hardware-Cybersecurity-Forschung mit seinem Vortrag »How I learned to stop worrying and love the insecure hardware« offenbar in Reminiszenz an Stanley Kubricks 60 Jahre alte Filmsatire »Dr. Strangelove or: How I Learned to Stop Worrying and Love the Bomb« in Anspielung auf das nukleare Vernichtungspatt im kalten Krieg. Zu seiner ausgefallenen Titelwahl berichtete er dem Publikum von einem Treffen mit Vertretern niederländischer Nachrichtendienste und deren Erklärung, dass man zwar nicht berechtigt sei, seine Hacking-Tools zur Ausspähung von Landsleuten anzuwenden, dafür aber andere Nationen mit Ermittlungshinweisen versorgen könne, etwa zu geplanten Terroranschlägen oder Kommunikation in Netzwerken der organisierten Kriminalität, was nun inzwischen verstärkt zu Razzien und Verhaftungen in anderen Ländern geführt hat. (ha)