Mord und Intrigen in der Welt der Chip-Technologien

Mord und Intrigen in der Welt der Chip-Technologien

Eben noch hat Marc Jansen an seinem Schreibtisch in Hamburg eine Marktanalyse für Netzwerkchips erstellt, jetzt findet sich der Spezialist für Halbleitertechnologie plötzlich in einem undurchsichtigen Strudel aus Mord, Korruption und Intrigen wieder. Nach dem mysteriösen Tod eines renommierten amerikanischen Quanteninformatikers in Thailand sollen er und seine Partnerin Lana de Vries im Auftrag eines internationalen Konsortiums herausfinden, was es mit einer neuen Generation von Chips auf sich hat - der ermordete Wissenschaftler arbeitete angeblich an deren Herstellung. Noch ahnt Jansen nicht, auf was er sich da eingelassen hat.

Der Autor
Mit dem Roman "Die Nanolithografie" zeigt Autor Thomas Biehlig, dass sich berufliches Fachwissen und komplexe technologische Fragestellungen auf unterhaltsame Weise zu einer spannenden Thrillerhandlung verknüpfen lassen. Auf 560 Seiten zeichnet er einen Wettkampf internationaler Konzerne und dubioser Organisationen um Marktmacht und Technologieführerschaft in der Welt der Computerchips nach. Dabei liefert er sowohl Einblicke in aktuelle wissenschaftliche Erkenntnisse, als auch einen Ausblick auf mögliche technische Entwicklungen der Zukunft.

Das GLOSSAR zum Wissenschaftsthriller „Die Nanolithografie“

Quantencomputer
Ein Quantencomputer bzw. Quantenrechner ist ein Computer, dessen Funktion auf den Gesetzen der Quantenmechanik beruht. Im Unterschied zum Digitalrechner arbeitet er nicht auf der Basis der Gesetze der klassischen Physik bzw. Informatik, sondern auf der Basis quantenmechanischer Zustände, was wesentlich über die Regeln der klassischen Theorien hinausgeht. Die Verarbeitung dieser Zustände erfolgt nach quantenmechanischen Prinzipien, z.B. die sog. Quantenverschränkung.

Quantenverschränkung
Als Quantenverschränkung wird ein Effekt bezeichnet, der es zwei oder mehreren Teilchen scheinbar erlaubt, einander ohne Zeitverzögerung über beliebige räumliche Distanzen hinweg zu beeinflussen. Obwohl dieses Verhalten im Rahmen der Quantenphysik an sich weitgehend verstanden ist, widerspricht es unserer Intuition. Eine Möglichkeit, komplexe Verschränkungszustände zu erzeugen, ist, eine große Zahl von Photonen miteinander wechselwirken zu lassen. Sobald aber mehr als zwei oder drei Photonen im Spiel sind, wird es enorm schwierig. Die Quantentechnologie steht hier vor einer wirklich großen Herausforderung.

Qubit (QBit)
Qubits (oder QBits) bilden in der Quanteninformatik die Grundlage für Quantencomputer. Das Qubit spielt dabei die analoge Rolle zum klassischen Bit bei herkömmlichen Computern: Es dient als kleinstmögliche Speichereinheit.

Quantenpunkte
Ein Quantenpunkt ist eine nanoskopische Materialstruktur, meist aus Halbleitermaterial. Ladungsträger (z.B. Elektronen) in einem Quantenpunkt sind in ihrer Beweglichkeit in allen drei Raumrichtungen so weit eingeschränkt, dass ihre Energie nicht mehr kontinuierliche, sondern nur noch diskrete Werte (endlich, abzählbar) annehmen kann. Quantenpunkte verhalten sich also ähnlich wie Atome, jedoch kann ihre Form, Größe oder die Anzahl von Elektronen in ihnen beeinflusst werden. Dadurch lassen sich elektronische und optische Eigenschaften von Quantenpunkten maßschneidern. Eine Methode der Herstellung ist die Lithografie. Der Quantenpunkt wird mittels Elektronenstrahlen, Rasterkraftmikroskop oder ähnlichem auf ein Substrat „geschrieben“ und anschließend durch ein geeignetes Ätzverfahren freigelegt.

Quantenteleportation oder „Beamen“
Quantenteleportation ist die Übertragung von Quantenzuständen mithilfe einer sofortigen Zustandsänderung miteinander verschränkter Quantensysteme. Zur vollständigen Übertragung eines Quantenzustandes muss zusätzlich auch Information zwischen Sender und Empfänger auf einem klassischen Weg (also mit maximal Lichtgeschwindigkeit) ausgetauscht werden. Ein Team um den Wiener Physikprofessor Anton Zeilinger hat den Quantenzustand eines Photons von der Kanareninsel La Palma zum benachbarten Teneriffa teleportiert - über eine Strecke von 143 Kilometern. Das Interessante ist die Tatsache, dass damit die satellitenbasierte Quantenkommunikation in Reichweite kommt. Für das Teleportieren von Gegenständen oder gar Lebewesen ist die Technik übrigens nicht geeignet. Zwar ist es Forschern bereits gelungen, nicht nur die Eigenschaften von Lichtteilchen, sondern auch die von Atomen zu versenden. Doch das Beamen eines Menschen, so wie es in "Raumschiff Enterprise" vorkommt, dürfte bis auf Weiteres im Reich der Science-Fiction bleiben. Denn bekanntlich besteht ein Mensch aus einer ganzen Menge von Atomen, die obendrein am Zielort wieder in der ursprünglichen Anordnung ankommen sollten.

Nanolithografie/Nanoprägelithografie
Als Nanolithografie bezeichnet man Verfahren, die sich prinzipiell zur Erzeugung von Strukturen in der Größenordnung weniger Nanometer eignen. Dazu gehören beispielsweise die Elektronenstrahl- und Nanoprägelithografie. Sie werden dort eingesetzt, wo eine Strukturierung mithilfe konventioneller Fotolithografie nicht mehr möglich ist, und sollen diese daher künftig bei der Herstellung von integrierten Schaltkreisen ablösen. Nanoprägelithografie ist ein Nanolithografie-Verfahren zum kostengünstigen Herstellen von Nanostrukturen mittels eines nanostrukturierten Stempels. Anwendung findet die Nanoprägelithografie in der Herstellung elektronischer und opto-elektronischer Bauteile.
Die Nanoprägelithografie wird zur Herstellung von zwei- und dreidimensionalen organischen oder Halbleiter-Nanostrukturen für die Optik, Elektronik, Photonik sowie Biologie verwendet. Anwendungen in der Optik und Photonik sind optische Filter, Polarisatoren oder z.B. photonische

Schaltkreise. Quantendrähte und -punkte sind für optische Halbleiterelemente wie Laser oder Dioden von Interesse.

MRAM

Magnetoresistive Random Access Memory ist eine nichtflüchtige Speichertechnik, die seit den 1990er Jahren entwickelt wird.
Im Gegensatz zu herkömmlichen Speichertechniken, wie das DRAM oder SRAM, werden die Informationen nicht mit elektrischen, sondern mit magnetischen Ladungselementen gespeichert, das heißt, es wird die Eigenschaft bestimmter Materialien ausgenutzt, die ihren elektrischen Widerstand unter dem Einfluss magnetischer Felder ändern.
Der Vorteil der MRAM-Technik liegt darin, dass sie nichtflüchtig ist, das heißt, die Chips behalten ihre gespeicherten Daten auch nach dem Abschalten der Energieversorgung. Damit können elektronische Geräte, wie z. B. Computer, realisiert werden, die sofort nach dem Einschalten betriebsbereit sind und nicht erst die zum Betrieb notwendigen Daten von einem Festspeicher, etwa einer Festplatte, in den Arbeitsspeicher laden müssen. Im Gegensatz zu etablierten nichtflüchtigen Speichertechniken, wie Flash, können MRAMs wie herkömmlicher DRAM/SRAM praktisch unendlich oft beschrieben werden. MRAM soll so die Vorteile der verschiedenen etablierten Speichertechniken kombinieren und dadurch das Potential zum so genannten „Universal Memory“ aufweisen, der DRAM, SRAM und Flash ersetzen könnte.
Derzeit ist die Firma Everspin Technologies der einzige kommerzielle Anbieter von MRAM-Speicherchips. Fast alle anderen großen Speicherhersteller wie Samsung, Hynix etc. haben angekündigt, in die MRAM-Entwicklung und -Fertigung zu investieren.
Aufgrund des hohen Preises findet MRAMs in erster Linie Verwendung in industriellen Systemen, um kritische Datenverluste zu verhindern. Typische Applikationen sind speicherprogrammierbare Steuerungen (SPS), POS/Electronic Cash, GPS-Tracker oder als Cache in Serversystemen. Auch in der Luft- und Raumfahrt sind MRAMs aufgrund ihrer hohen Strahlungsfestigkeit vermehrt im Einsatz.

Bootkit-Virus

Ein Bootkit ist eine Sammlung von Softwarewerkzeugen oder Bootloadern, die nach dem Einbruch in ein Computersystem auf dem kompromittierten System installiert wird, um weitere Sicherheitsmechanismen des Betriebssystems zu deaktivieren. Ein Bootkit ist somit eine Mischung aus Bootsektorviren und Rootkits. Der Ansatz besagt, dass derjenige, der die Hardware bereits unter seiner Kontrolle hat, auch die Software unter seiner Kontrolle haben kann.

Rootkit

Ein Rootkit ist eine Sammlung von Softwarewerkzeugen, die nach dem Einbruch in ein Softwaresystem auf dem kompromittierten System installiert wird, um zukünftige Anmeldevorgänge des Eindringlings zu verbergen und Prozesse und Dateien zu verstecken.
Zweck eines Rootkits ist es, Schadprogramme („malware“) vor den Antivirenprogrammen und dem Benutzer durch Tarnung zu verbergen. Da eine hundertprozentige Erkennung von Rootkits unmöglich ist, ist die beste Methode zur Entfernung die vollständige Neuinstallation des Betriebssystems. Da sich bestimmte Rootkits im BIOS verstecken, bietet selbst diese Methode keine hundertprozentige Sicherheit über die Entfernung des Rootkits.
Die Grenze zwischen Rootkits und Trojanischen Pferden ist fließend, wobei ein Trojaner eine andere Vorgehensweise beim Infizieren eines Computersystems besitzt.

Backdoor

Backdoor (Hintertür) bezeichnet einen (oft vom Autor eingebauten) Teil einer Software, der es Benutzern ermöglicht, unter Umgehung der normalen Zugriffssicherung Zugang zum Computer oder einer sonst geschützten Funktion eines Computerprogramms zu erlangen.
Ein Beispiel sind Universalpasswörter für ein BIOS oder eine spezielle (meist durch einen Trojaner heimlich installierte) Software, die einen entsprechenden Fernzugriff auf den Computer ermöglicht. Backdoors vereinfachen dem Angreifer, auf bestehende oder bereits kompromittierte System zuzugreifen, indem beispielsweise eine Shell gestartet wird, oder wenn an einen bestimmten Netzwerkport eine Verbindungsanfrage gestellt wurde.

DDoS

Distributed Denial of Service (kurz DDoS; engl. für „ Verteilte Dienstblockade“) bezeichnet in der Informationstechnik die Nichtverfügbarkeit einer ganzen Anzahl von Systemen, die eigentlich verfügbar sein sollten. Obwohl es verschiedene Gründe für die Nichtverfügbarkeit geben kann, spricht man von DDoS in der Regel als die Folge einer Überlastung von Infrastruktursystemen. Dies kann durch unbeabsichtigte Überlastungen verursacht werden oder durch einen mutwilligen Angriff auf einen Server, einen Rechner oder sonstige Komponenten in einem Datennetz.
DoS-Angriffe wie SYN-Flooding oder der Smurf-Angriff belasten den Internetzugang, das Betriebssystem oder die Dienste eines Hosts mit einer größeren Anzahl Anfragen als diese verarbeiten können, woraufhin reguläre Anfragen nicht oder nur sehr langsam beantwortet werden. Beispiele sind WinNuke, die Land-Attacke, die Teardrop-Attacke oder der Ping of Death.
Denial-of-Service-Attacken werden mittlerweile von Cyber-Kriminellen zum Verkauf angeboten, etwa um Konkurrenten zu schädigen. Mutwillige DDoS-Angriffe werden oft mit Hilfe von Backdoor-Programmen oder Ähnlichem durchgeführt. Diese Backdoor-Programme werden in der Regel von Computerwürmern auf nicht ausreichend geschützten Rechnern installiert und versuchen selbstständig, weitere Rechner im Netzwerk zu infizieren, um so ein Botnetz aufzubauen. Je größer das Botnetz, desto wahrscheinlicher ist, dass der Angriff selbst gegen gut geschützte Systeme durchdringt.