wehr technik I/2016

G 4949 • 48. Jahrgang • € 14,50
ISSN 0043-2172

IWA & Enforce Tac

Sanitätsdienst

- Neuausrichtung der Führungsunterstützung der Luftwaffe
- Pioniersymposium in Ingolstadt
- Marine: Effektoren der Zukunft

Projekt APT-Sweeper: Wirksamer Schutz gegen gezielte Angriffe

Gegen Advanced Persistent Threats (APT) gibt es bis heute kein wirksames Mittel. Dabei verursachen diese professionell ausgeführten, gezielten Cyber-Angriffe große Schäden, bspw. können sensible Daten und Know-how unbemerkt abfließen, kritische Infrastrukturen sabotiert oder Firmen erpresst werden. Im Forschungsprojekt APT-Sweeper werden gegen diese Bedrohung neuartige Abwehrmaßnahmen entwickelt. Ansatzpunkt ist die Analyse von Meta-Informationen, durch die APT-Angriffe frühzeitig erkannt und abgewehrt werden können. Projektbeteiligte sind die Friedrich-Alexander-Universität Erlangen, die Georg-August-Universität Göttingen und der deutsche IT-Sicherheitsspezialist **genua gmbh**, als assoziierte Partner das Bundesamt für Sicherheit in der Informationstechnik und **Siemens**. Das Projekt APT-Sweeper läuft bis Juli 2017 und wird vom Bundesministerium für Bildung und Forschung gefördert.

Die APT-Angriffe unterscheiden sich deutlich von anderen Hacker-Attacken: Täter sind zumeist gut ausgestattete und kompetente staatliche Dienste oder kriminelle Organisationen, das Ziel ist ein bestimmtes IT-System in den Bereichen Wirtschaft, Forschung, Politik oder Militär. Durch eine sorgfältige Aufklärung wird der Angriff so angelegt, dass erkannte Sicherheitsmaßnahmen wie Virenscanner und Intrusion Detection-Systeme getäuscht oder umgangen werden. Ist das Ziel infiziert, wird der Angriff weiterhin mit großem Aufwand verheimlicht, um den erlangten Zugriff möglichst lange zu nutzen und somit maximalen Schaden anrichten zu können.

Die Meta-Daten verraten verdächtige Kommunikation: Im Projekt APT-Sweeper werden Verfahren entwickelt, um solche Angriffe bereits in der Anfangsphase erkennen zu können. Der Schlüssel dazu sind Meta-Informationen aus der Mail- und Web-Kommunikation. Denn um das Zielsystem zu erreichen, muss der Angreifer Malware in das anvisierte Netzwerk einschleusen. Dazu werden häufig E-Mails mit infizierten Anhängen und gefälschten Absenderadressen oder auch mit Malware versehene Webseiten eingesetzt, die von Mitarbeitern im Ziel-Netzwerk aufgerufen werden. Vergleicht man jetzt die Meta-Daten dieser Kommunikation mit zuvor angelegten Profilen, ergeben sich Abweichungen: Die E-Mail eines bekannten Absender wird erstmals von einem anderen Mail-Server versandt oder eine Website wird mit Flash ausgeliefert, die bisher stets ohne diesen Content auskam. Diese Indizien deuten auf eine APT-Attacke hin. Im Projekt APT-Sweeper werden Methoden erarbeitet, um Abweichungen von der gewohnten Kommunikation erkennen, bewerten und somit Angriffe abwehren zu können. Der IT-Sicherheitsspezialist genua beschäftigt sich in dem Projekt mit der Entwicklung von Indikatoren zur APT-Erkennung in Datenströmen.

IZT-Produkte ermöglichen Aufbau eines leistungsfähigen OTA-Kommunikationstestsystems

Die Fraunhofer Gesellschaft präsentierte ein OTA (Over-The Air)-System mit Wellenfeldsynthese für den Test und die Zertifizierung von GNSS (Global Navigation Satellite System)-Empfängern. Die Installation befindet sich am Prüfstand für mobile Satellitenkommunikation des **Fraunhofer-Instituts für Integrierte Schaltungen IIS** (FORTE). Das innovative und komplexe Testsystem basiert im Wesentlichen auf Hardware- und Software-Komponenten der **IZT GmbH** - wie leistungsfähigen HF-Empfängern und Signalgeneratoren. Der Testaufbau stellt einen neuen Ansatz für den Test von GNSS-Empfängern dar - im Gegensatz zu gängigen Conducted- oder Open-Field-Tests. Dabei werden die realen Verhältnisse unter steuerbaren und wiederholbaren Bedingungen realistisch emuliert. So ist ein praxisgerechter Vergleich von Empfängern und Algorithmen möglich. Das demonstrierte Testsystem ist außerdem kosteneffizient, flexibel und skalierbar.

Die neuesten Generationen mobiler Kommunikationssysteme, wie LTE, LTE-A, WIMAX oder WLAN nutzen meist mehrere Antennen für die Übertragung und den Empfang. Üblicherweise werden MIMO (Multiple Input Multiple Output) OTA-Testsysteme eingesetzt, um diese breitbandigen mobilen Kommunikationsgeräte zu evaluieren, zu testen und zu zertifizieren. Dabei müssen die Geräte in ihrem realen Umfeld getestet werden. Im Gegensatz zu Mobiltelefonen sind Satelliten-Empfänger (GNSS) wesentlich empfindlicher auf Störungen durch Interferenzen. Daher galt es ein Testsystem zu entwickeln, mit dem die Robustheit von GNSS-Empfängern gegenüber Interferenzen überprüft werden kann.

Über den Militärstandard hinaus – die Sicherung von militärischen Daten in einem rauen Umfeld

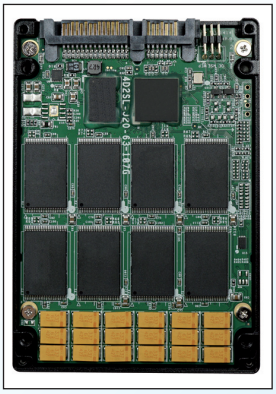
Wenn es um die Beschaffung von elektronischen Geräten geht, liegt es nahe, sich nach Produkten von bewährten Herstellern umzusehen, die nach militärischen Standards zertifiziert sind. Doch ist dies ausreichend? Gerade bei Produkten auf SSD-Basis kann dies mitunter zu Problemen führen. SSDs sind zwar aufgrund ihrer Stoß- und Vibrationsresistenz, ihrem niedrigen Stromverbrauch und ihren kompakten Abmessungen beim Militär äußerst gefragt, die Schwächen der Technologie sind dagegen oftmals noch nicht im Bewusstsein verankert. Dabei geht es bspw. um die Anfälligkeit für einen Datenverlust während eines Stromausfalls.

SSDs sind in der Lage, Daten in einer Umgebung zuverlässig zu speichern, in welchen herkömmliche Festplatten versagen. Dies trifft allerdings nur zu, solange die Stromversorgung gewährleistet ist. Der zum Einsatz kommende Flash-Speicher selbst ist ein nicht-flüchtiger Speicher. Dies bedeutet, dass die Daten unabhängig von der Stromzufuhr intakt bleiben. Nichtsdestotrotz nutzen fast alle modernen SSDs einen flüchtigen DRAM-Puffer um die Lebensdauer und die I/O-Performance zu steigern. Die Größe der temporär im DRAM-Puffer zwischengelagerten Daten kann dabei recht groß werden und darüber hinaus kritische Mapping-Informationen beinhalten. Sollte demnach ein Stromausfall im laufenden Betrieb auftreten, gehen sämtliche Daten im DRAM-Puffer verloren, die auch die Daten auf dem nicht-flüchtigen Flash-Speicher beeinflussen und dort für korrupte Dateien sorgen können.

Bei militärischen Einsatzzwecken in rauen Umgebungen ist die Stromzufuhr nicht immer gesichert. Infolgedessen müssen SSDs für schroffe, militärische Anwendungsszenarien, über die reine mechanische Stabilität hinausgehen und auch gegen einen Stromausfall gesichert werden.

Eine der besten Möglichkeiten SSDs gegen einen Datenverlust in Folge eines Stromausfalls zu sichern, ist die Integration einer Notfallstromquelle. Damit kann die SSD solange mit Strom versorgt werden, um die Daten aus dem flüchtigen DRAM-Puffer auf den nicht-flüchtigen Flashspeicher zu kopieren.

Stromausfallsicherungssysteme wie die iCell-Technologie von **Innodisk** setzen dabei bei der Firmware als auch bei der Hardware direkt an. Mittels Super-Kondensatoren und einem Schaltkreis zur Erkennung eines Stromausfalls kann im Notfall ein Datenverlust verhindert werden. Sobald ein Stromausfall registriert wird, aktiviert die Firmware des Laufwerks eine spezielle Power-Down-Sequenz, die alle Daten aus dem DRAM-Puffer auf den Flashspeicher kopiert. Während dieser Sequenz bezieht das Laufwerk den Strom über die verbauten Kondensatoren. Somit können Daten sicher und effektiv geschützt werden.



Flashspeicher mit iCell-Technologie von Innodisk zur Rettung von Daten bei Stromausfall. Hier Innen und Außenansicht. Die DRAM-lose Technologie ist ein weiterer Schutz gegen Energieverlust, geeignet für kleinere SSDs wie dieses SATA Disk On Flash Modul in Briefmarkengröße. Bei Stromausfall schützen die extra Kondensatoren (in gelb) und die firmware diese Innodisk SSD vor Datenverlust. (Grafik: Innodisk)

Abgesehen davon gibt es einen neuen Ansatz, die Problematik eines Stromausfalls zu lösen. Neuere Flash-basierte Laufwerke verzichten auf einen flüchtigen DRAM-Puffer. Um Leistungseinbußen zu verhindern, werden Performance-Optimierungen im Flashcontroller direkt vorgenommen. SSDs ohne DRAM-Puffer können zwar nicht so hohe Kapazitäten wie herkömmliche SSDs bieten, sind dafür aber aufgrund der fehlenden Notstromversorgung (Kondensatoren) kleiner. Durch den kleineren Formfaktor sind sie für viele spezielle militärische Anwendungsgebiete wie gemacht. Bspw. in UAVs und in der Luftfahrt können SSDs ohne DRAM-Puffer eine Möglichkeit bieten, Daten stabil und sicher zu speichern.