Das Fraunhofer-Institut für Naturwissenschaftlich-Technische Trendanalysen berichtet über neue Technologien

Cyber Reasoning Systems

Cyber-Angriffe nutzen vielfach Sicherheitslücken in Software aus, um ihre jeweiligen Ziele zu erreichen. Solche Sicherheitslücken sind dabei häufig das Ergebnis von unabsichtlichen Programmierfehlern. Cyber Reasoning Systems (CRS) sind IT-Systeme, die automatisiert, d. h. ohne menschliche Unterstützung, Sicherheitslücken in Software finden und diese anschließend beseitigen. CRS können dementsprechend als eine Form von automatisierter Cyber Defence angesehen werden. Mit der zunehmenden Vernetzung technischer Systeme könnten solche mit potenziell hoher Geschwindigkeit arbeitenden Abwehrmechanismen in Zukunft von erheblicher Bedeutung für deren sicheres Funktionieren sein. Heute befinden sich CRS allerdings im Wesentlichen noch im Forschungsstadium.

Generell nutzen Angreifer Sicherheitslücken in Software mithilfe eines geeigneten Programmcodes aus, eines sogenannten Exploits. In Abhängigkeit von der genauen Art der Sicherheitslücke kann mithilfe eines Exploits unter anderem ein System durch bestimmte Eingaben zum Absturz gebracht werden, sodass beispielsweise ein eventuell von diesem System angebotener Dienst nicht mehr verfügbar ist (Denial of Service). Außerdem können bestimmte Exploits verwendet werden, um Schadsoftware (Malicious Software = Malware) auszuführen.

CRS nutzen den Maschinencode einer Software, um auf dieser Grundlage eventuelle Sicherheitslücken zu entdecken. Software wird zwar durch einen Programmierer in Form eines sogenannten Quelltextes mithilfe einer geeigneten Programmiersprache erstellt. Dieser Quelltext kann allerdings durch einen Computer nicht direkt ausgeführt werden, sondern muss zuvor erst in den Maschinencode des jeweiligen Computers umgewandelt werden. Im Gegensatz zum Quelltext ist der Maschinencode jedoch nicht oder nur schwer für Menschen lesbar. CRS verwenden den Maschinencode, da unter anderem der Quelltext typischerweise nur dem jeweiligen Hersteller, nicht aber deren Anwendern zur Verfügung steht.

Das Auffinden von Sicherheitslücken erfolgt bei CRS mithilfe von geeigneten Methoden der Software-Analyse. Hierbei kann allgemein zwischen statischen und dynamischen Methoden unterschieden werden. Während die statische Software-Analyse eine Software untersucht, ohne diese dabei auszuführen, betrachtet die dynamische Software-Analyse die Software bei deren Ausführung. Ein wichtiger Ansatz zum Auffinden von Sicherheitslücken ist beispielsweise das sogenannte Fuzzing. Bei dieser dynamischen Methode wird das Verhalten einer Software bei verschiedenen, teilweise zufällig gewählten, Programmeingaben getestet, um auf diese Weise Fehler, wie z. B. Programmabstürze oder fehlerhafte Ausgaben, zu provozieren.

CRS sind generell für eine Vielzahl von IT-Systemen von großem Interesse. Dies gilt insbesondere vor dem Hintergrund der zunehmenden Verbreitung von miteinander vernetzten IT-Systemen. Diese Entwicklung kommt unter anderem im aktuellen Trend zum Internet der Dinge zum Ausdruck. Hierunter versteht man die Ausstattung von physischen Objekten mit Computertechnologie und deren, häufig drahtlose, Vernetzung untereinander. Hierzu zählen beispielsweise Objekte wie Haushaltsgeräte, am Körper getragene IT-Geräte (Wearables), medizinische Geräte, aber auch größere Objekte wie Fahrzeuge, Gebäude oder Industrieanlagen. Dies schließt auch Kritische Infrastrukturen wie die Energieversorgung oder Transport und Verkehr ein.

Aktuelle Geräte dieser Art weisen jedoch vielfach Sicherheitslücken auf. Das Risiko durch diese Sicherheitslücken wird dabei noch erheblich durch die potenziell sehr große Anzahl dieser Geräte verstärkt. Beispielsweise wurden kürzlich vermutlich mehrere Millionen Geräte aus dem Bereich des Internets der Dinge durch einen Angreifer mit Malware infiziert, der diese Geräte dadurch fernsteuern und auf diese Weise für einen Denial-of-Service-Angriff missbrauchen konnte. Weitere Bedrohungen können unter anderem durch Sensoren, wie z. B. Kameras, entstehen, die häufig in derartigen Geräten enthalten sind und die beispielsweise zu Spionagezwecken missbraucht werden können. Darüber hinaus können Cyber-Angriffe auch ernsthafte physische Auswirkungen zur Folge haben. Hierzu zählt beispielsweise das Verursachen von Verkehrsunfällen oder der Ausfall der Stromversorgung. Die potenziell große Menge und Vielfalt von Geräten im Internet der Dinge erfordert dabei einen automatisierten Ansatz für die Entdeckung von Sicherheitslücken.

Gegenwärtig erfolgt sowohl das Auffinden von Sicherheitslücken in Maschinencode als auch die notwendige Veränderung des Programmcodes zur Beseitigung der entdeckten Sicherheitslücken typischerweise noch nicht vollständig automatisiert, sondern überwiegend manuell und dementsprechend zeitaufwendig durch geeignete IT-Sicherheitsexperten. Der aktuelle technologische Stand von CRS lässt sich gut an den Ergebnissen eines von der US-amerikanischen DARPA (Defense Advanced Research Projects Agency) 2016 durchgeführten Wettbewerbs, der Cyber Grand Challenge, ablesen, bei dem erstmalig CRS gegeneinander antraten. Im Anschluss an die Cyber Grand Challenge nahm das Gewinnersystem noch an einem Wettbewerb mit menschlichen Gegnern teil und wurde dabei lediglich Letzter. Dies verdeutlicht, dass CRS zumindest augenblicklich entsprechenden IT-Sicherheitsexperten noch merklich unterlegen sind.

Daher ist wahrscheinlich erst langfristig mit tatsächlich praktisch einsetzbaren und mit all den derzeit angestrebten Fähigkeiten ausgestatteten CRS zu rechnen. Allerdings könnten eingeschränktere CRS wohl schon deutlich früher Bedeutung als Unterstützung von menschlichen IT-Sicherheitsexperten erlangen. Durch diesen kooperativen Ansatz lassen sich die jeweiligen Stärken von menschlichen Experten und automatisierten Systemen entsprechend kombinieren. Außerdem könnten CRS möglicherweise dazu beitragen, in Zukunft den aktuellen Mangel an Fachkräften auf dem Gebiet der Cyber Defence zu lindern. Allerdings könnten CRS zukünftig auch eine Bedrohung für die IT-Sicherheit darstellen, wenn solche Systeme offensiv zum Auffinden und Ausnutzen von Sicherheitslücken eingesetzt würden.

Dr. Klaus Ruhlig