Dr. Do und die Detektive
… und die netzweite Suche nach den Fehlern im Code

Dr. Quoc Huy Do arbeitet seit 2017 am Institut für Informationssicherheit der Universität Stuttgart daran, Hackern das Leben schwer zu machen. Zusammen mit seinen Kollegen am SEC fahndet der Vietnamese nach Sicherheitslücken in grundlegenden Web-Standards und -Protokollen.

Im Vergleich zu den Fluren im Institut für Informationssicherheit (SEC) der Universität Stuttgart mit ihren Sitzecken und verspiegelten Teeküchen erscheint das Büro von Dr. Quoc Huy Do geradezu spartanisch. Papierlos der Schreibtisch, Laptop, Flachbildschirm und eine Tasse Tee. Ein Foto seiner Familie ist sein einziges Zugeständnis ans Privatleben. Es scheint, als wolle der 36-Jährige alle Ablenkung von seiner Arbeit fernhalten, damit ihm nicht jene Fehler unterlaufen, die vielen Programmierern passieren: Sie schreiben versehentlich Sicherheitslücken in die Codes des Internets – und nichts motiviert einen Hacker mehr als so ein security hole. „Wir arbeiten hier sehr hart“, ist Dos freundlich lächelnde Zusammenfassung des Büroumfelds.

Dr. Do ist in dem Kräftespiel der Datenjäger und -sammler einer der Guten. Zusammen mit seinen Kollegen einer Arbeitsgruppe am SEC fahndet er nach Sicherheitslücken in grundlegenden Web-Standards und -Protokollen. Ob er eine Art Detektiv sei, der mit Ausdauer und präzisem Verstand nach Spuren möglicher Angriffspunkte suche? Do nickt, ja, das könne man so sagen.

Kein klassischer Tatort

Natürlich – und da fängt die Komplexität des Themas bereits an – ist das Internet nicht wie ein Tatort, an dem gründliche Ermittler Fingerabdrücke, Tatwaffen oder DNA-Material finden. Das Netz präsentiert sich uns zwar scheinbar physisch auf allerlei Bildschirmen, aber es ist in Wahrheit nicht greifbar. Und auch nicht unangreifbar. Im Gegenteil: Das Internet ist eine Art unkontrolliert wachsender Organismus, der sich in jede Dimension immer weiter ausdehnt. Dass dabei auch Lücken entstehen, Angriffspunkte für Hacker, liegt in der natürlichen Fehlbarkeit des Menschen begründet. „Nichts auf der Welt ist perfekt, auch kein Code“, sagt Dr. Do. Daher hat sich das Team um Institutsleiter Prof. Ralf Küsters ein Werkzeug zum Ziel gesetzt, das Web-Entwicklern mögliche Schwachstellen in ihren Codes schon aufzeigen soll, bevor sie damit online gehen. Eine Art unbestechlicher Prüfinstanz, die Fehler in den Codes auf logisch-mathematischer Basis aufspürt.

Auf dem Papier ist dieses Tool bereits skizziert – und schon da ist es ein hochkomplexes Projekt. Bis Ende des Jahres, so hofft Do, soll auch ein erster struktureller Rahmen des Test-Werkzeugs programmiert sein.

Verwurzelt in der Computerwissenschaft

Die Computerwissenschaft zieht sich schon seit Beginn seines Studiums durch Quoc Huy Dos Karriere. Und mit jedem weiteren Schritt drang der Vietnamese tiefer in die Materie vor, bis er nun in Stuttgart quasi an den Fundamenten des Internets angekommen ist.

In Vietnams Hauptstadt Hanoi geboren, studierte Do an der People's Security Academy zunächst die Grundlagen, im Masterstudium an der Vietnam National University in Hanoi – „die beste Universität in Vietnam“ – arbeitete er sich bereits in die Welt der Programm-Verifikation vor. Da war der Weg nach Stuttgart freilich noch nicht vorgezeichnet.

Für seine Promotion forschte Do an der Technischen Universität Darmstadt in der Arbeitsgruppe von Prof. Reiner Hähnle. „Dort arbeitete ich an Informationsfluss-Sicherheit“, erklärt Do. Das klingt für den Laien zwar ähnlich, der Forscher versichert jedoch, dass das „etwas völlig anderes“ war: „Wir programmierten ein Tool für Java-Entwickler, das prüft, ob die Software versteckte Informationsflüsse aufweist.“

Am Thema Sicherheit hatte sich Quoc Huy Do da allerdings schon festgebissen: „Nach meiner Promotion wollte ich weiter in diese Richtung arbeiten.“ Und in Stuttgart schien sich eine Gelegenheit aufzutun: Prof. Küsters hatte in Trier an einer umfassenden Sicherheitsanalyse des OAuth-2.0-Protokolls gearbeitet und war zu dieser Zeit gerade an die Stuttgarter Universität gewechselt.

Diese Forschung in einer frisch zusammengestellten Arbeitsgruppe fand Do faszinierend und bewarb sich. Und obwohl er zur gleichen Zeit auch andere Angebote hatte, entschied sich Do für Stuttgart. „Die Arbeitsatmosphäre und die enge Zusammenarbeit sind toll, außerdem ist Stuttgart eine schöne Stadt“, sagt der Post-Doktorand, der im September 2017 seine Stelle am SEC antrat.

Wohnte Do mit seiner Familie zunächst im Gästehaus der Universität, vermittelte das Welcome Center der Stadt Stuttgart bald Kontakte zu potenziellen Vermietern, half bei allerlei behördlichen Fragen („ein Alptraum“) und organisierte für die neu Angekommenen sogar eine Weihnachtsfeier. „Meine Kinder waren begeistert davon“, erzählt er. Mittlerweile hat die Familie nicht nur eine Wohnung gefunden – sie ist auch gewachsen: „Mein Sohn wurde bereits in Stuttgart geboren“, sagt Do. Die beiden Töchter gehen hier in den Kindergarten und in die Grundschule.

Foto: Universität Stuttgart/Max Kovalenko

Fan der Forschungsfreiheit

„Wissenschaftler zu werden, war anfangs gar nicht mein Plan“, sagt der Sicherheitsexperte. Heute fühlt sich der 36-Jährige sehr wohl in der universitären Forschungswelt. „Ich mag es, zu lernen und mich neuen Herausforderungen zu stellen. Genau dafür ist Wissenschaft eine tolle Möglichkeit.“ Auch wenn er bislang noch nie für ein Unternehmen gearbeitet habe, schätze er die Freiheit in der Forschung als höher ein. „Wir konzentrieren uns auf bestimmte Themen, während man in der Wirtschaft immer das Endprodukt im Blick haben muss.“

Im Kern des Projekts, an dem Quoc Huy Do mit seinen Kollegen arbeitet, steht mit OAuth 2.0 (Open Authorization) ein weit verbreitetes Protokoll zur Autorisierung und Authentifizierung im Netz. Dies soll eine sichere Autorisierung von Web-Diensten oder -Anwendungen gewährleisten, ohne dass Drittanbieter geheime Daten erhalten. In der Praxis wählt man sich über seine geheimen Zugangsdaten bei einem Anbieter ein und kann danach auch Dienste von Drittanbietern nutzen, ohne sich jedes Mal neu anmelden zu müssen.

In der Vergangenheit gab es bereits mehrere Hackerangriffe auf OAuth 2.0. Solche Attacken führen in der Regel zu eiligen Reparaturen an den Programmcodes. Das Werkzeug, an dem das SEC arbeitet, soll anhand der Muster erkannter Schwachstellen von OAuth dazu beitragen, potenzielle Einfallstore für Bösewichte bereits in einem frühen Stadium zu erkennen.

Dos Vertrag am Institut läuft noch bis September 2019, ob er danach weiter in Stuttgart arbeiten wird, weiß er noch nicht. Dass hingegen Sicherheit sein Thema bleiben wird – das ist sicher.

Jens Eber