

# »Biologie ist total cool«

Professor Kay Hamacher simuliert nicht nur Proteine, sondern auch Cybersicherheits-Szenarien



Professor Kay Hamacher leitet seit 2012 das Fachgebiet „Computational Biology & Simulation“ am Fachbereich Biologie der Technischen Universität Darmstadt. Bereits seit 2011 ist Hamacher kooptierter Professor an den Fachbereichen Informatik und Physik der TU.

Physiker, Biologe, Informatiker, Big-Data-Spezialist – hinter all diesen Begriffen steckt Professor Kay Hamacher. Sein Spezialgebiet ist die mathematische und computerbasierte Biophysik (englisch Computational Biology), oder wie er es beschreibt: „Wir verbessern das Signal-Rausch-Verhältnis“.

Was da rauscht, ist die Evolution. „Im Genom werden Informationen von 100 Millionen Jahren Umweltstress gespeichert“, erklärt Hamacher. Da die Evolution ein zufälliger Prozess ist, ergeben nicht alle dieser Speichervorgänge auf den ersten Blick Sinn. Dennoch existieren in all dem zufälligen Rauschen auch Signale, eingeprengte Muster – zum Beispiel die fünf Finger an einer Hand. In seiner Forschung arbeitet Hamacher allerdings an etwas kleineren Bauteilen des menschlichen Körpers. „Wir sind im Proteinsimulationsbusiness“, fasst er es zusammen.

Er und sein Team aus Biologen und Informatikern arbeiten mit riesigen Datenbanken, um Proteine zu analysieren. Die besondere Schwierigkeit dabei ist, dass Proteine zwar eine chemische Formel haben, aber auch physikalische Objekte sind, die im 3D-Raum funktionieren müssen. Tun sie das nicht, können Erbkrankheiten die Ursache sein. Auch die Verschaltung einzelner Proteine kann fehlerhaft sein, zum Beispiel bei Krebs. „Dann müssen wir verstehen, an welcher Stelle man effektiv eingreifen kann, um es gar nicht erst zur falschen Verschaltung kommen zu lassen“, so Hamacher.

Um das herauszufinden gibt es zwei generelle Schritte, erläutert der Biologie-Professor das Hauptprinzip seiner Forschung: „Der erste Schritt ist die Mustererkennung, dafür analysieren wir die Daten, bis wir eine Hypothese finden. Wir behaupten: Es könnte ein Muster geben.“ Als nächstes wird diese Behauptung mit Simulationen untersucht, um zu beweisen, ob das Muster existiert und wenn ja, was es in unseren Genen codiert. Doch wo kommt im „Proteinsimulationsbusiness“ die Cybersicherheit ins Spiel? Hamacher arbeitet sogar an zwei



Botanischer Garten der TU Darmstadt, Sitz des Fachbereichs Biologie

Foto: Thomas Ott / TU Darmstadt

Sicherheitsthemen: zum einen der Schutz von Genomdaten (englisch Genomic Privacy) – zusammen mit Prof. Stefan Katzenbeisser will er dafür sorgen, dass es bei Genomdatenbanken nicht mehr entweder Datenschutz oder medizinischer Fortschritt heißen muss. Zum anderen „nutzen wir unsere Methodenkompetenz aus der Proteinsimulation, sodass wir damit Sicherheitsthemen bearbeiten können“. Viele Sicherheitsszenarien seien im Prinzip mit dem gleichen Vorgehen wie in der Biologie zu lösen: Muster erkennen – Hypothese bilden – Behauptung überprüfen – Aussage treffen.

Als Beispiel nennt Professor Hamacher eine Studie zu WikiLeaks, die er durchgeführt hat. „Dabei ging es um eine Theorie von Julian Assange: Ständige Informationslecks durch eine Plattform wie WikiLeaks stiften Unfrieden in Organisationen, zum Beispiel Terrorgruppen, solange bis sie sich selbst von innen zerstören.“ Salopp zusammengefasst heißt das: WikiLeaks als Friedensstifter. Doch wie kann man das überprüfen? Assanges Hypothese sei biologistischer Natur, so Hamacher. Er erläutert den Mechanismus: Durch Informationslecks entstehe in Organisationen ein kollektives internes Miss-

trauen. Das führe zu höheren Kosten, die Organisationsstruktur sei nicht mehr nachhaltig. „Das Prinzip funktioniert ab dann wie in der Biologie: Entzieht man Ressourcen, in diesem Fall Geld und Struktur, ist die Einheit ab einem gewissen Grad nicht mehr überlebensfähig.“

Auf dieser Grundlage simulierte Hamachers Forschungsteam die Wikileaks-Hypothese: Jede ‚böse‘ Organisation ist dabei eine kleine Einheit, die wie in der Natur mit begrenzten Ressourcen, wie Geld oder Personal, ausgestattet ist. Die Informationslecks werden in der Simulation als unterschiedlich starke Attacken dargestellt. „Kennt man die Größe eines Parameters nicht, werden einfach mehrere Simulationen mit allen möglichen Werten durchgeführt“, erklärt Hamacher das Prinzip der Simulation. Sind alle Werte eingegeben, rechnet ein moderner Multicore-PC einige Tage lang alle Möglichkeiten durch. Die Ergebnisse der Simulation werden dann dazu benutzt, die Hypothese zu bestätigen oder zu entkräften.

Im WikiLeaks-Fall kam der Biologie-Professor zu einem spannenden Ergebnis: „Es gibt Situationen, in denen eine Organisation auf Kosten einer anderen Organisation den Marktanteil vergrößert, indem sie ihr durch Leaks schadet. Assange hatte aber behauptet, dass beide Organisationen sich von innen zerstören und damit verschwinden. Das konnten wir so nicht bestätigen.“

Professor Hamacher wird auch in Zukunft den Hypothesen von Cybersicherheitsexperten auf den Zahn fühlen – und das mit den Prinzipien der Biologie. Von seinem Fachbereich schwärmt er jedenfalls: „Biologie ist total cool – es ist sowohl eine physikalische Wissenschaft als auch eine Informationswissenschaft.“ Das ist wohl eine Hypothese, die auch ohne Simulation als bewiesen werden kann.



Am Profildbereich CYSEC (Cybersecurity [at] TU Darmstadt) sind mehr als 30 Fachgebiete aus acht Fachbereichen beteiligt und forschen an zentralen Themen der Cybersicherheit und des Privatsphärenschutzes. International anerkannte Spitzenforschung in zahlreichen Bereichen der Cybersicherheit und die Ausbildung von Experten für IT-Sicherheit sind Kernkompetenzen von CYSEC. Technologietransfer über nationale und internationale Kooperationen mit außeruniversitären Forschungseinrichtungen und industriellen Partnern runden das Profil von CYSEC ab.

Ann-Kathrin Braun  
Wissenschaftskommunikation  
akbraun@cysec.tu-darmstadt.de  
06151 / 16-22662

## CRISP - IP1 Project - Scalable Privacy-Preserving Protocols

In diesem Projekt werden innovative Methoden entwickelt, die den Schutz der Privatsphäre gewährleisten, in Anwendungen integriert werden können und auch für große Datenmengen skalierbar sind. Die Effizienz und Skalierbarkeit bestimmter datenschutzrelevanter Protokolle soll verbessert werden, hierzu zählen etwa die Schnittmengen privater Datenmengen, das Abrufen privater Informationen und das sichere Rechnen auf der Basis von unbemerktem Speichern.

Von besonderer Bedeutung ist aufgrund unkontrollierbarer Bedrohungen in der Zukunft der Bereich der genomischen Privatsphäre, welcher von DNA-Sequenzdaten bis Omics-Daten in der Biomedizin reicht. Es sollen maßgeschneiderte Protokolle und Anpassungen bewährter Methoden für diesen wichtigen Bereich entwickelt werden.