Andrey Ruzhanskiy – Diplom
es gab insgesamt 15 Bewerber

Titel Abschlussarbeit:	Untersuchungen zur Durchsetzbarkeit des Schutzziels Verfügbarkeit in 5G-Netzen unter Berücksichtigung nicht-vertrauenswürdiger Hersteller von 5G-Komponenten
Kurzbeschreibung Abschlussarbeit:	Durch die Corona-Pandemie stieg die Präsenz des Internets im alltäglichen Leben und im Arbeitsumfeld enorm an. Diese sprunghafte Entwicklung der Digitalisierung führte zu einer Überlastung bestehender Netzwerke durch die vermehrte Nutzung von Streamingdiensten oder der weitgehenden Implementierung des Homeoffice. Auf diese Weise kam es besonders in den Anfangszeiten der Pandemie immer wieder zu Verbindungsabbrüchen oder Drosselungen, die zu Lasten der Wirtschaft, Wissenschaft und des allgemeinen sozialen Lebens gingen. Diese Störungen zeigen die Unzulänglichkeiten bestehender Netze und den Bedarf für neue Technologien und Möglichkeiten auf. Der vielversprechendste Ansatz ist dabei der in meiner Abschlussarbeit behandelte Mobilfunk der fünften Generation, kurz 5G. Um diese Innovation jedoch nicht zu gefährden, muss ein besonderer Fokus auf die Sicherheit dieser vielversprechenden Technologie gelegt werden, weshalb meine Arbeit genau diesen Aspekt untersucht. Dabei liegt das Hauptaugenmerk der Arbeit auf möglichen Bedrohungen, die die Verfügbarkeit einschränken. Insbesondere wird untersucht, welches Gefährdungspotenzial durch die Einbeziehung nicht vertrauenswürdiger Mobilfunkausrüster für 5G-Komponenten entsteht. Das Ziel meiner Arbeit war es, diese Bedrohungslage zu analysieren und ein Angreifermodell zu entwerfen, das diese nicht vertrauenswürdigen Hersteller am besten modelliert. Basierend darauf sollten alle 5G-Komponenten hinsichtlich ihrer Angriffseignung untersucht werden, um so mögliche Sicherheitslücken zu identifizieren. Insbesondere wurden dabei Schwachstellen der 5G-Infrastruktur aus den Spezifikationsdokumenten ermittelt und die daraus resultierenden Angriffe mittels frei verfügbarer Simulatoren getestet. Auf Grundlage dessen ist es mir gelungen, einzelne 5G-Komponenten hinsichtlich ihrer Angriffstauglichkeit zu bewerten. Dabei konnte ich bei der verwundbarsten Komponente zwölf erfolgreiche Angriffe gegen die 5G-Infrastruktur aufdecken, die die Verfügbarkeit eines 5G-Netzes je nach Art der Attacke unterschiedlich stark beeinträchtigen können. Die meisten dieser Angriffe konnten durch die Simulation eines 5G-Netzes erfolgreich evaluiert werden. Insgesamt zeigte sich das enorme Bedrohungspotential von nicht vertrauenswürdigen Herstellern, da die Angriffe unter anderem beliebige Nutzer

aus dem Netzwerk ausschließen und andere Komponenten in der 5G-Infrastruktur massiv überlasten konnten, was in einer digitalen Gesellschaft faktisch den Zusammenbruch kritischer Infrastruktur bedeuten würde. Auf weniger gravierenden Ebenen können die von mir gefundenen Angriffe weiterhin dazu genutzt werden, Mobilfunkbetreiber wirtschaftlich zu schädigen, beispielsweise durch einen mittels vorgetäuschter Überlastsituationen erzeugten zusätzlichen Stromverbrauch.
Die gegen solche Angriffe existierenden Schutzmechanismen erwiesen sich als nutzlos und konnten von mir sogar dazu missbraucht werden, die Schadwirkung möglicher Attacken zu vergrößern.

Durch die Ergebnisse meiner Arbeit konnte ich beweisen, dass die 5G-Netze gegenüber einem direkt in die Infrastruktur integrierten Angreifer machtlos sind. Durch geeignete Gegenmaßnahmen wie der Virtualisierung einzelner Komponenten konnte ich aufzeigen, dass das Bedrohungspotential minimiert werden kann.

Botschaft und Begründung der Bewerbung:

Die Stadt Dresden ist mit dem 5G Lab einer der in diesem Bereich bedeutendsten internationalen Forschungsstandorte. Die Technische Universität Dresden sowie eine Reihe von Industriepartnern setzen hier neue Maßstäbe für die Zukunft des mobilen Internets. Gleichzeitig kann Dresden als Landeshauptstadt Sachsens und Heimat des Silicon Saxony Hightech-Clusters von vielen der durch 5G ermöglichten technologischen Entwicklungen in der Industrie 4.0 zu profitieren. Der Standort Dresden wird für die Mobilfunkwelt immer lukrativer, was auch durch die Ansiedlung des Vodafone Research Centers unterstrichen wird.

Damit das volle Potential von 5G genutzt werden kann, ist es essentiell, dass die Sicherheit und Verfügbarkeit des Mobilfunknetzes gewährleistet ist. Dies muss insbesondere auch dann gelten, wenn den Herstellern der zum Ausbau des Netzes notwendigen Soft- und Hardware nicht - oder nur eingeschränkt - vertraut werden kann; ein Umstand, der vor einiger Zeit auch in den öffentlichen Medien für Aufmerksamkeit gesorgt hat. Nur so können der technische Vorsprung Dresdens erhalten und ausgebaut und das Leben der Bürgerinnen und Bürger durch innovative 5G-basierte Anwendungen in sicherheitskritischen Bereichen wie dem Gesundheitswesen, der Energieversorgung oder der Landwirtschaft verbessert werden.
Die vorliegende Arbeit leistet diesbezüglich einen wichtigen Beitrag indem sie Schwächen des 5G Standards aufzeigt, die böswillige Akteure ausnutzen könnten um sensible Informationen abzuhören, zu manipulieren oder Netzausfälle zu provozieren. Weiterhin zeigt sie auf, wie diese Probleme

durch Audit kritischer Software sowie Entkopplung (“Zero Trust”) und Virtualisierung verschiedener Komponenten des 5G-Netzwerkes gelöst werden können. Zusammenfassend wird damit der Grundstein für wichtige Diskussionen und technologische Weiterentwicklungen rund um das Thema 5G-Sicherheit gelegt

Nächste Ziele und Vorhaben:

Um wichtige Sicherheits-Probleme in der 5G Supply Chain einem breiteren Publikum näherzubringen, wurde meine Diplomarbeit zur Veröffentlichung für den 18. Deutschen IT-Sicherheitskongress eingereicht und befindet sich dort gerade in der Evaluierung.
Da ich noch viele Möglichkeiten für die Stärkung der Sicherheit im Mobilfunk sehe, sowohl für den 5G Standard als auch darüber hinaus, bin ich hochmotiviert, dieses Thema während meiner Promotion am Barkhausen Institut weiter zu verfolgen.
Gerade durch Innovationen im Bereich des Quantum Computings zeichnen sich hier auch insbesondere noch nie dagewesene Angriffsvektoren ab, denen es entgegenzutreten gilt. Daher ist es eines meiner Hauptziele, die 5G-Spezifikationen um Betrachtungen zur Post-Quantum Sicherheit zu erweitern. Ich hoffe, dass ich damit einen wesentlichen Beitrag zur Absicherung unserer digitalen und vernetzten Gesellschaft leisten kann.
Bereits während meines Studiums war ich zudem Mitautor in einer Studie des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zur Open Radio Access Network (ORAN) Technologie, die durch Entkopplung der Komponenten von 5G Mobilfunkmasten erhöhte Herstellerunabhängigkeit und Kostenreduktion verspricht. Insbesondere sollen dabei neue Innovationen wie maschinelles Lernen für die optimierte Netzabdeckung und Antennenausrichtung zum Einsatz kommen. Im Rahmen dieser Studie habe ich durch diesen Ansatz entstehende Sicherheitsrisiken analysiert und bewertet. Dies geschah in Kooperation mit dem in Dresden ansässigen Sicherheitsunternehmen secunet, das unter anderem an der Absicherung der Kommunikationsinfrastruktur des öffentlichen Dienstes arbeitet. Als Mitglied der ORAN-Alliance bringe ich mich auch weiterhin in dieses Thema ein, umso 5G unter sicherheitskritischen Aspekten zu verbessern.
Weiterhin konnte ich ebenfalls Mitglied des Europäischen Instituts für Telekommunikationsnormen (ETSI) werden, das den Standardisierungsprozess des Mobilfunks auf europäischer Ebene durchführt. Davon erhoffe ich mir, dass ich mein Wissen auch auf dieser Ebene einsetzen kann, um die Sicherheit und Souveränität der europäischen

Staatengemeinschaft im Bereich der Mobilfunktechnik zu fördern.