

---

## - HIWI-Stelle /Bachelorarbeit -

### Ein Cross-Matching-Angriff auf Fingerprint-Fuzzy-Vault

---

#### CASED

Das Center for Advanced Security Research Darmstadt (CASED) bündelt die Kompetenzen der Technischen Universität Darmstadt, des Fraunhofer-Instituts für Sichere Informations-technologie und der Hochschule Darmstadt. In einer Kooperation von Informatikern, Ingenieuren, Physikern, Juristen und Betriebswirten sowie mit internationalen Forschungszentren und Industriepartnern, erforscht CASED zukunftsweisende IT-Sicherheitslösungen, entwickelt diese und bringt diese in die Anwendung und wirtschaftliche Verwertung. Mehr Informationen unter [www.cased.de](http://www.cased.de).

#### Hintergrund

Fingerabdruckerkennung ist das am weitesten verbreitete biometrische Verfahren und besitzt mehr als 50% Marktanteil. Minutien, welche die Verzweigung oder Endung der Fingerlinien beschreiben, sind standardisierte Features zur Beschreibung von Fingerabdrücken. Um die Privatsphäre der Benutzer zu schützen, wurde das Fuzzy-Vault-Verfahren entwickelt. Dieses Verfahren basiert auf dem Secret-Sharing-Protocol und versteckt tatsächliche Minutien in zwischen zahlreichen Streuungspunkten. Allerdings ist das Verfahren anfällig für einen Cross-Matching-Angriff, mit dem die tatsächlichen Minutien wiederhergestellt werden können, wenn mehrere Einträge der gleichen Person zur Verfügung stehen. Die Ziele dieser Arbeit sind, einen solchen Cross-Matching-Angriff zu implementieren und die Effizienz dieses Angriffes zu evaluieren.

#### Aufgaben

- Entwicklung eines Cross-Matching-Angriffs auf das Fingerprint-Fuzzy-Vault-Verfahren
- Evaluierung des entwickelten Angriffs

#### Voraussetzungen

- Interesse an Sicherheitsanalyse
- Kommunikationsbereitschaft und Teamfähigkeit
- Gute Kenntnisse in Statistik und Sicherheitsanalyse
- Kenntnisse in Matlab
- Sehr gute deutsche sowie gute englische Sprachkenntnisse

#### Starttermin

- Ab sofort

#### Kontakt

Dr. Xuebing Zhou  
[xuebing.zhou@cased.de](mailto:xuebing.zhou@cased.de)

CASED - Center for Advanced  
Security Research Darmstadt  
Mornewegstraße 32  
64293 Darmstadt

Tel. 06151 16 75181

