Lehrstuhl für Sicherheit in der Informatik
Prof. Dr. Claudia Eckert

Fraunhofer AISEC

*Abschlussarbeit (Bachelor/Master) in Kooperation mit Fraunhofer AISEC, Garching*

# AntiPatterns bei der Anwendung von Crypto-Primitiven am Beispiel von Ransomware

## Motivation und Aufgabenstellung

Für die Gewährleistung von IT Schutzzielen, wie z.B. Vertraulichkeit, Integrität oder Authentizität, müssen meist kryptographische Verfahren eingesetzt und diese oft in Software implementiert werden. Bei der Realisierung der kryptographischen Verfahren treten dann typische Implementierungsprobleme auf, wie z.B. das sichere Speichern kryptographischer Schlüssel.

In dieser Abschlussarbeit soll am Anwendungsbeispiel von „Crypto-Trojanern“ (engl. Ransomware), wie bspw. Locky[1] oder Wannacry[2] untersucht werden, welche typischen Fehler bei der Anwendung und Umsetzung von kryptographischen Primitiven gemacht wurden.

Dafür ist zunächst eine Übersicht der verschiedenen Varianten von Ransomware zu erarbeiten. Darauf aufbauend sind die Implementierungsschwächen zu identifzieren, welche ausgenutzt werden konnten, um die Verschlüsselung einzelner Varianten auszuhebeln. Diese Schwächen sind in Kategorien zu unterscheiden und AntiPatterns zu identifizieren. Die erarbeiteten Erkenntnisse sind als Transferleistung für anderen Domänen aufzubreiten.

## Anforderungen

- Gutes Grundlagenwissen im Bereich IT Sicherheit und Public/Private Key Verfahren
- Praktische Erfahrung in der Anwendung und Implementierung kryptographischer Primitiven
- Grundkenntnisse in Binary Exploitation und Reverse Engineering hilfreich
- Implementierungen sollen plattformunabhängig erfolgen (bspw. Golang oder Python).

## Kontakt

**Norbert Wiedermann**
Telefon: +49 89 322-9986-141
E-Mail: norbert.wiedermann@aisec.fraunhofer.de

**Sven Plaga**
Telefon: +49 89 322-9986-134
E-Mail: sven.plaga@aisec.fraunhofer.de

Fraunhofer Research Institution for Applied and Integrated Security (AISEC)
Department Product Protection and Industrial Security
Parkring 4, 85748 Garching (near Munich), Germany
https://www.aisec.fraunhofer.de

[1] https://heise.de/-3111774
[2] https://heise.de/-3713235