# Aufgabe 1: Digitales Vergessen

# Aufgabenteil a)

Die Idee hinter diesem Ansatz ist, dass der Schlüssel durch DNS-Caching abgeleitet wird. Dabei stellt jede Domain beziehungsweise jeder Resolver genau ein Bit des Schlüssel dar. Die daraus resultierende DNS-Infrastruktur definiert somit den *Ephemeral Key Storage*. Ein Bit nimmt den Wert **1** an, wenn der Resolver einen gecachten Eintrag vorweist. Der Wert **0** wird dann angenommen, wenn dieser Eintrag fehlen sollte.

Das Widerrufen der Schlüssel wird somit realisiert, dass jedem Eintrag im Resolver ein *Time-To-Live* (TTL) Wert mitgeliefert wird. Dieser Wert wird bei jedem Aufruf um den Wert 1 dekrementiert. Sollte die TTL den Wert 0 erreichen, wird der zugehörige Eintrag im Resolver entfernt. So erscheint als Bit des ursprünglichen Keys fälschlicherweise eine 0 an dieser Stelle. Der Schlüssel -und damit auch der verschlüsselte Inhalt- kann nun nicht mehr rekonstruiert werden.

## Aufgabenteil b)

Dieser Mechanismus schützt nur gegen einen *retrospective adversary*, da sowohl der Schlüssel, als auch der geschützte Inhalt, nach der Widerrufung nicht mehr wiederhergestellt werden kann.

Allerdings bietet dies keinen Schutz gegen Angreifer, welche vor der Wiederrufung in Kenntnis des Schlüssel gelangen, da der verschlüsselte Inhalt auch danach stets mit dem gleichen Schlüssel verschlüsselt ist. Somit kann der Inhalt auch nach der Widerrufung des Schlüssel mit eben diesen entschlüsselt und ausgelesen werden.

# Aufgabe 2: Grundlagen von Tor

## Aufgabenteil a)

Die Idee der *Onion Encryption* ist, dass der zu verschlüsselnde Inhalt mehrmals mit unterschiedlichen Schlüsseln verschlüsselt wird. Zudem passiert der zu verschlüsselnde Inhalt bei der Übertragung mehrere Knoten. Jeder Knoten besitzt dabei genau einen dieser Schlüssel. Der Schlüsselaustausch verläuft dabei iterativ.

Schickt der Client nun ein Datenpaket zum Server, wird dieses von ihm mit allen bekannten Schlüsseln verschlüsselt. Jeder Knoten entschlüsselt dabei schichtweise den Inhalt mit seinem individuellen Schlüssel.

Die Verschlüsselung verläuft analog auf umgekehrten Wege. Das Datenpaket vom Server wird bei jedem Knoten mit dessen Schlüssel jeweils einmal verschlüsselt. Der Client entschlüsselt das Gesamtpaket dann mit allen Schlüsseln.

## Aufgabenteil b)

Es ist besonders kritisch, dass die *Entry Guards* vertrauenswürdig sind, da diese die einzigen Knoten sind, welche Einsicht auf die niedrigste Schicht in der zuvor genannten *Onion Encryption* haben.

Sollte ein *Entry Guard* nicht vertrauenswürdig sein, kann dieser sowohl die Identität des Clients feststellen, als auch Nachrichten mitlesen oder verändern, welche nicht -beispielsweise mit TLS- gesichert werden.

## Aufgabenteil c)

Tor-Bridges sind Relays, welche nicht im Hauptverzeichnis von Tor gelistet sind. Da es keine öffentliche Liste dieser Bridges gibt, wird es Internet Service Providern (ISPs) erschwert sämtliche Relays zu blockieren. Dies hilft dabei Maßnahmen zu umgehen, welche beispielsweise von Regierungen getroffen werden, um den Tor Dienst in einem bestimmten Gebiet zu sperren. Der Durchführung von Zensur im Internet kann somit entgegengewirkt werden.

# Aufgabe 3: Traffic Analysis Attack

## Aufgabenteil a)

Bei der Traffic Analysis Attack wird der Datenverkehr von einem Angreifer an jedem Endpunkt der Verbindung mitgeschnitten. Der eigentliche Inhalt des Traffics ist zwar verschlüsselt, allerdings beinhalten mitgeschnittene Metadaten noch immer Informationen, welche Rückschlüsse auf die versendete Nachricht zulassen.

Aufgrund der Metadaten ist es möglich, Relationen zwischen Paketen/Verbindungen zu beobachten, welche die Identität des Senders offenbaren können. Dies folgt aus der Tatsache, dass die Metadaten die Unterscheidung verschiedener Paket Streams (Traces) ermöglichen, welche für nahezu jeden Nutzer verschieden sind.

Dieser Angriff wird auch Ende-zu-Ende Korrelationsangriff genannt.

## Aufgabenteil b)

Eine Gegenmaßnahme stellt das sogenannte *Mixing* dar. Beim Mixing werden Pakete im Datenverkehr zufällig für eine bestimmte Zeit zurückgehalten, bevor diese weiterverschickt werden. Dies hat den Vorteil, dass Relationen zwischen gesendetem und empfangendem Traffic zerstört werden. Allerdings beinhaltet diese Methode den Nachteil, dass eine langsamere Verbindung vorherrscht, da die Latenz künstlich erhöht wird.

Eine zweite Gegenmaßnahme stellt die Verwendung eines *Dummy Traffics* dar. Hierbei werden der Verbindung Dummy Pakete hinzugefügt, welche ebenfalls durch künstlich hinzugefügter Pakete mögliche Relationen beseitigen. Auch hier stellt sich eine sehr stark ausgelastete Bandbreite als Nachteil heraus.

## Aufgabenteil c)

Beim Website Fingerprinting wird zur Vorbereitung bestimmter Datenverkehr mitgeschnitten, welcher Website Requests beinhaltet. Anschließend wird der Datenverkehr des Opfers mitgeschnitten, um Ähnlichkeiten zwischen den von dem Nutzer gesendeten Daten und den Website Requests zu erhalten. Unterschieden wird hierbei mithilfe des jeweiligen Radio Network Temporary Identifier (RNTI).

Der Unterschied zum Ende-zu-Ende Korrelationsangriff besteht darin, dass hier nicht Metadaten miteinander verglichen werden, um die Identität des Nutzers zu ermitteln. Stattdessen werden gesendete Website Requests verglichen, um besuchte Websites eines Opfers zu identifizieren.