Universität Hamburg
Fachbereich Informatik

Das cMix-Verfahren

am Arbeitsbereich Sicherheit in Verteilten Systemen (SVS)

todo

10. Juni 2016

Inhaltsverzeichnis

Abstract / Einleitung

Das ist die Zusammenfassung

Und das die Einleitung

1 Übersicht Chaumsche Mixe

1.1 Funktionsprinzip

-> Verwendung onion routing?

1.2 Probleme

Das Problem ist

1.3 vorherige Ansätze

2 Das cMix Verfahren

2.1 Idee

Die grundsätzliche Idee des cMix Verfahrens ist es, Schlüsselberechnungen in Echzeit zu vermeiden. Hierdurch entsteht auf der einen Seite eine Steigerung der Effizienz von Mix-Netzen, d.h. bessere Performance, also weniger Verzörerte Kommunikation. Auf der anderen Seite wird hierdurch der Energiebedarf verringert, was z.B. zu längerer Akkulaufzeit eines Smartphones führen kann. Um dies zu erreichen werden vor der Kommunikation Schüssel berechechnet (precomputation) und zwischen dem Sender und den Mix-Nodes ausgetauscht. Diese werden dann als Seed für einen Pseudozufallsgenerator verwendet, um weitere (gleiche) Schlüssel zu erzeugen.

2.2 Funktionsprinzip

2.3 Sicherheitsanalyse

3 Schlussbemerkungen / Fazit

Thema: Privacy Enhancing Technologies zum Schutz von Kommunikationsbeziehungen

Bearbeiter: Eva Musterfrau, Heinz Mustermann

Datum: 10. Juni 2016

Literaturliste

David Chaum: Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. Communications of the ACM 24/2 (1981) 84–88.

David Chaum: The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability. Journal of Cryptology 1/1 (1988) 65–75.

David Goldschlag, Michael Reed, Paul Syverson: Onion Routing for Anonymous and Private Internet Connections. Communications of the ACM 42/2 (1999) 39–41.

Andreas Pfitzmann: Diensteintegrierende Kommunikationsnetze mit teilnehmerüberprüfbarem Datenschutz. IFB 234, Springer-Verlag, Berlin 1990.

Wei Wang, Mehul Motani, Vikram Srinivasan: Dependent link padding algorithms for low latency anonymity systems. Proc. 15th ACM conference on Computer and communications security. ACM, 2008, 323–332.