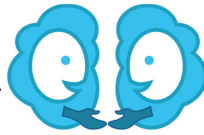


OmniShare

Daten in der Cloud teilen –
verschlüsselt, benutzerfreundlich, sicher

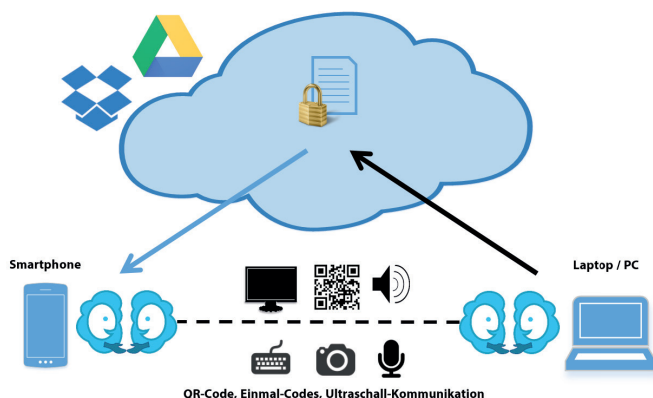


Die Cloud ist ein benutzerfreundliches und bequemes Speichermedium.

Allerdings sind die hinterlegten Daten leicht angreifbar, besonders weil die Cloud-Anbieter Zugriff darauf haben. Eine Lösung besteht darin, die Daten vor dem Hochladen zu verschlüsseln. Der Schlüssel muss jedoch auf allen Geräten, die Zugriff erhalten sollen, umständlich verteilt werden. Momentan umgehen Cloud-Services dieses Problem durch Passwörter, die jedoch oft nicht sicher genug gewählt sind, und daher nur eine begrenzte Sicherheit bieten.

Die preisgekrönte App OmniShare löst dieses Problem: starke Verschlüsselung schützt die Daten in der Cloud vor unerwünschtem Zugriff, gleichzeitig können die benötigten Schlüssel komfortabel, beispielsweise über QR-Codes, geteilt werden. So können mehrere Nutzer verschlüsselt auf die Daten zugreifen, und auf mehreren Geräten synchronisieren. OmniShare ist kompatibel mit weit verbreiteten Cloud-Services, wie Dropbox oder Google Drive.

OmniShare ist der Hauptgewinner des mit 20.000 Euro dotierten "Privacy via IT Security: Innovating Mobile Apps"-Wettbewerbs des MAPPING-Projekts, das von der EU gefördert wird. Die App ist für Android und Windows verfügbar und soll auch bald für iPhones zur Verfügung stehen.



Funktionsweise der App „OmniShare“: Daten verschlüsselt zwischen mehreren Geräten und Nutzern teilen.

HosTaGe & TraCINg



Die Bedrohung durch Cyber-Angriffe nimmt stetig zu. Um diesen Angriffen gezielt begegnen zu können, sind mehrere Schritte notwendig:

1) Ein allgemeines Bewusstsein der Bedrohungslage muss etabliert werden, 2) Angriffe müssen zeitnah erkannt werden und 3) detaillierte Informationen über Angriffe müssen Forschern zugänglich sein, um neue Schutzmechanismen entwickeln zu können.

Das Fachgebiet Telekooperation an der TU Darmstadt stellt sich diesen Herausforderungen mit zwei Anwendungen:

Das großflächige Projekt TraCINg sammelt durch gezielt platzierte Sensoren Information über Angriffe und Angriffsvorbereitungen. Diese Informationen können von Wissenschaftlern für weitere Forschung genutzt werden. Durch die Aggregation der Informationen, also auch den einfachen Web-Zugang, wird der breiten Öffentlichkeit die aktuelle Lage vermittelt.

Die App HosTaGe (Honeypot-To-Go) erlaubt es jedermann, die Bedrohungslage in drahtlosen Netzwerken zu analysieren (zu Hause, im Hotel, im Café). Hiermit wird gerade für Privatpersonen jene Hürde überwunden, die durch die Anschaffung, Installation und Betrieb traditioneller Sicherheits-Systeme entstehen würde. Weiterhin kann HosTaGe an Orten eingesetzt werden, die anderweitig wirtschaftlich oder technisch nicht zu erschließen sind, etwa drahtlose Kleinstnetze zur Vernetzung von Maschinen im industriellen Umfeld.

Beide Anwendungen sind darüber hinaus so verbunden, dass Synergien aus deren Kollaboration entstehen: So können etwa Erkenntnisse aus HosTaGe mit TraCINg so verschmolzen werden, dass Nutzer sich bereits vor dem Verbinden mit einem Hotel-WLAN über Bedrohungen aus der Vergangenheit informieren können.



M.Sc. Emmanouil Vasilomanolakis zeigt die Hackerangriffe auf die ausgelegten „Honeypots“ auf einer Weltkarte.

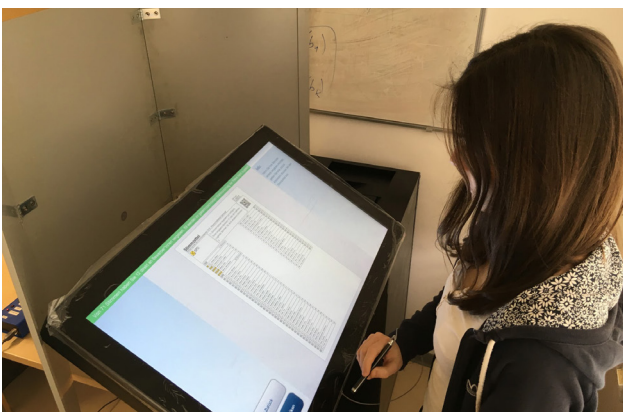
EasyVote



Wahlen unterscheiden sich nicht nur stark von Land zu Land, sogar in den Bundesländern gibt es verschiedene Arten von Wahlen. Einige haben sehr einfache Stimmzettel mit nur zwei Kandidaten oder einer Ja-/Nein-Frage, während andere Stimmzettel, zum Beispiel jene für einige Kommunalwahlen in Deutschland, mehr als 500 Kandidaten auflisten und außerdem dem Wähler eine kumulative Stimmabgabe, d.h. die Stimme auf mehrere Kandidaten aus unterschiedlichen Wahlvorschlägen zu verteilen und das Ausstreichen von Kandidaten, erlauben. Dies führt zu riesigen Stimmzetteln. Die Stimmen von Hand auszuzählen ist sehr fehleranfällig und zeitintensiv. Das Auszählen bei Kommunalwahlen in Deutschland dauert meistens zwischen vier und sechs Tagen. Dabei gibt es technische Unterstützung für das Auszählen, indem man alle Stimmzettel Stimme für Stimme eingibt, beziehungsweise abbildet. Auch die Stimmabgabe ist fehleranfällig, da Wähler unabsichtlich und ohne es zu merken ihre Stimme ungültig machen und abgeben können.

Um die aktuelle Situation zu verbessern, wurde das EasyVote Konzept entwickelt. Dieses Konzept soll hauptsächlich bei Wahlen mit komplexen Stimmzetteln angewandt werden, kann aber auch für jede andere Wahl verwendet werden.

Außerdem ist EasyVote das einzige Konzept eines Wahlsystems, das speziell auf die deutsche Rechtslage in Bezug auf die Benutzung von elektronischen Wahlen bei Kommunalwahlen in Hessen zugeschnitten ist.



Elektronische Stimmenabgabe mit dem „EasyVote“-Terminal.

Private Set Intersection

Gemeinsame Daten schnell, sicher und bequem finden und zugleich alle übrigen Informationen schützen



Viele Aktionen in der digitalen Welt verlangen vom Benutzer die Herausgabe seiner gesamten Daten. Oft möchte der Benutzer allerdings nicht, dass die Gesamtmenge seiner Daten einem Dritten offengelegt wird. Ein Beispiel hierfür sind mobile Nachrichten-Apps, die Zugriff auf das Adressbuch eines Benutzers benötigen, um die Kontakte zu finden, die diese Apps auch nutzen. Private Set Intersection (PSI) ist eine kryptographische Technik, die es ermöglicht, nur die gemeinsamen Kontaktdaten schnell, sicher und bequem herauszufiltern, ohne die restlichen Daten offenzulegen.

PSI ermöglicht somit einen nutzerkontrollierten Abgleich von Daten unter Schutz der Privatsphäre.



M.Sc. Michael Zohner präsentiert der Bundesministerin für Bildung und Forschung, Johanna Wanka, den „Private Set Intersection“-Demonstrator.