Einführung in die Informationssicherheit

Florian Mendel

Institute for Applied Information Processing and Communications (IAIK)
Graz University of Technology
Inffeldgasse 16a, A-8010 Graz, Austria

http://www.iaik.tugraz.at/

L3 – Electronic Payment Systems

Einführung in die Informationssicherheit

Übersicht

- Zahlungsarten und ihre Eigenschaften
- Etwas Kurioses: Anonymes elektronisches Bargeld (e-cash)
- Etwas weit Verbreitetes: Bankkarten-Systeme
- Etwas, das überarbeitet wurde: SET und Nachfolger
- Alternative Zahlungssysteme

Motivation: E-Shopping

We all like shopping, don’t we?

E-Shopping

1. Der Kunde surft auf den Online-Shop, browst nach Waren und legt die Waren in seinen Einkaufswagen
   - Internet Security, Accessibility, Availability
2. Der Kunde bestimmt ein Zahl- und Versandmethode
   - Internet Security
3. Die Waren werden geliefert, der Händler wird bezahlt.
   - Vertrauenswürdigkeit

Vorteile des E-Shopping

- Für den Kunden:
  - Muss sein Haus nicht verlassen um Sachen zu kaufen (Bequemlichkeit)
  - Muss sein Haus nicht verlassen um die Sachen abzuholen (Bequemlichkeit)
- Für den Händler:
  - Muss kein physisches Geschäft haben (Ersparnis)
  - Neue Möglichkeiten der Werbung und Möglichkeit Kundenprofile zu erstellen (Gewinn)

Kunden & E-Shopping

- Viele potentielle Kunden weigern sich online zu kaufen wegen
  - mangelndem Vertrauen für den Händler,
  - zu schwierigen Prozessen beim e-Shopping, oder
  - zu geringer Verlässlichkeit
- Es ist notwendig, dem Kunden ein besseres Gefühl für die Sicherheit eines Systems zu geben . . .

Sicherheitsaspekte

- Kunde:
  - Zahlungen kommen an
  - Zahlungsdetails bleiben geheim
  - Kundenprofil
- Händler:
  - Zahlungen kommen an
  - Die Services sind erreichbar

$\Rightarrow$ Unterschiedliche Parteien haben meistens unterschiedliche Sicherheitsanliegen . . .

Sichtheitsaspekte

- In den unterschiedlichen Schritten des e-Shoppings sind ebenfalls unterschiedliche Aspekte wichtig:
  1. Web shop - Erreichbarkeit (ausfallssicher)
  2. Zahlungsdetails (Kreditkarte) - Vertraulichkeit
  3. Zustellung - Verlässlichkeit
- Die Vorlesung kann sich klarerweise nur um Schritt 2 kümmern!

Zahlungsarten

- Direkte Zahlungsarten
  - Bargeld
  - Schecks
  - Bankkarten
- Kredit-Systeme
- Debit Systeme (Lastschrift-Systeme)
- Diese traditionellen Zahlungsarten können durch elektronische Zahlungsarten ersetzt werden

E-Money

- E-Money, E-Cash, E-Currency
  - Soll ungefähr die gleichen Eigenschaften haben wie echtes Bargeld
  - Das Vervielfältigen von Bargeld soll nicht möglich sein!!
- Micro-Payments
  - Transaktionen mit winzigen Beträgen
- Macro-Payments
  - Transaktionen mit mittleren Beträgen

Aspekte von (E)-Money

- Sicherheit
  - Anonymität vs. Verfolgbarkeit
  - Verbreitung von Verschlüsselung?
- Akzeptanz
  - Bequemlichkeit
  - Übertragbarkeit
  - Beständigkeit
  - Teilbarkeit (Wechselgeld?)
- Kosten
- Unabhängigkeit
- Sofortige Kontrolle

Andere Trade-Off

- On-line vs. Off-line
- Hardware vs. Software
- Transparenz vs. zu viel Infos

Das E-Cash System – DigiCash

DigiCash

- Ein Konzept für digitales Bargeld mit Hinblick auf die Anonymität des Nutzers
- Basiert auf Techniken die von David Chaum entwickelt wurden
  - Bedient sich mehrerer nicht-trivialer Methoden
  - Anonymität des Benutzers während des Geldausgebens
- Wir betrachten eine vereinfachte Version des Systems:
  - Alice: Der Kunde
  - Bob: Die Bank
  - Martin: Der Händlers

DigiCash

- Das System hat 3 Phasen:
  - Money Generation Phase
  - Money Spending Phase
  - Double-Spending Checking Phase
- Für alle 3 Phasen definiert das E-Cash System eine Reihe von Schritten (ein Protokoll)

E-cash (vereinfachte Version)

- Geld:
  - Geld (eine Münze) ist nur ein Character-String
- "Blinding" des Geldes:
  - Blinding bedeutet, die Münze in einen Umschlag zu geben
- Nur wenn Alice (der Kunde) das Geld selbst generiert, kann sie bei einer späteren Transaktion anonym bleiben:
  - Wir wollen nicht, dass die Bank (Bob) weiß, welche Münzen Alice gehören
  - Alice generiert die Münzen und Bob bestätigt die Münzen

Münze erzeugen (vereinfachte Version)

1. Alice erzeugt n Geld-Aufträge

2. Alice blindet alle n Geld-Aufträge und schickt diese an die Bank Bob

3. Bob lässt Alice zufällig $n - 1$ Geld-Aufträge öffnen und überprüft diese auf Korrektheit

4. Bob signiert den verbleibenden Geld-Auftrag und schickt ihn zurück an Alice. Diese “unblindet” den Auftrag und hat eine bestätigte Münze

Geld ausgeben und Doppelausgaben-Check

1. Alice gibt ihr Geld aus

2. Der Händler überprüft die Signatur der Bank

3. Der Händler bringt das Geld zur Bank

4. Die Bank überprüft die Signatur und die SN

5. Hat die Bank die SN schon in ihrer DB $\rightarrow$ doppelte Ausgabe!!

Analyse (vereinfachte Version)

- Geld erzeugen:
  - Alice hat nur eine geringe Chance, bei der Erzeugung zu betrügen, da Bob verlangt, dass $(n-1)$ Geld-Aufträge geöffnet werden.
- Geld ausgeben:
  - Der Händler überprüft die Gültigkeit einer Münze anhand der Signatur der Bank.
- Doppelausgaben:
  - Die Bank kann herausfinden, dass eine Münze doppelt ausgegeben wurde.
  - Die Bank weiß nicht, wer das versucht hat . . .

E-Cash

- Münze hat nicht nur eine Seriennummer, sondern zusätzlich einen identity string:
  - Wir werden sehen, dass das nichts an der Anonymität der Münze ändert
- Um sicher zu stellen, dass die Identitätsinformationen nicht nachträglich verändert werden, werden sogenannte (bit)-commitment Techniken benutzt

Commitment-Schema

- Sei h eine kryptographische Hashfunktion
- Angenommen, Alice will sich zu x committen
- Sie berechnet $y = h(x)$ und schickt y an Bob
- Wenn Alice zu einem späteren Zeitpunkt den Wert x offenlegen soll, schickt sie x und Bob kann überprüfen, dass $y = h(x)$
- Für eine kryptographisch starke Hashfunktion ist es für Alice praktisch unmöglich, ein weiteres x' zu finden, dass ihr Commitment bestätigt d.h. $y = h(x) = h(x')$
- Bob kennt jedoch bis zu diesem Zeitpunkt den Wert x nicht, da er nur $h(x)$ kennt.

E-Cash: Geld erzeugen

- Eine Münze besteht aus
  - einer Seriennummer,
  - Identitäts-String (n Paare):

$$I_1 = (L_1, R_1), I_2 = (L_2, R_2), \ldots, I_n = (L_n, R_n)$$

  - Jedes Paar erlaubt die Identifikation von Alice
- In dem Geldauftrag sind nur die jeweiligen Commitments enthalten!
- Die Geld-Blinding Phase bleibt wie vorher

E-Cash: Geld ausgeben

- Geld ausgeben (hat einen Schritt mehr):
  - Händler überprüft Signatur
  - Händer sendet (L,R)-Folge an Alice und erhält die zugehörigen Identitäts-String Hälften

E-Cash: Überprüfen von Doppelausgaben

- Die Bank checkt, ob die SN schon vorhanden ist
- Jetzt kann Bob aber herausfinden, wer betrogen hat:
  - Bob hat zu SN auch die Identitäts-Strings gespeichert (wenn der Händler die Münze einzahlen will)
  - Wenn diese Identitäts-Strings mit den gespeicherten übereinstimmen, dann will der Händler betrügen
  - Wenn nicht, dann will Alice betrügen

paysafecard

SET Secure Electronic Transaction™

PayPal™

Andere Zahlungssysteme

clickandbuy
SAFE AND SIMPLE ONLINE PAYMENT

MasterCard paypass™

QUICK

VISA payWave

Google wallet

Bankkarten

- Maestro und Quick sind unterschiedliche Systeme, nur Quick bietet einen gewissen Grad an Anonymität
- Ähnliche Systeme in anderen Ländern:
  - Proton in Belgien
  - Geldkarte in Deutschland
- Man erhält keine Informationen über Quick ohne ein NDA zu unterschreiben

Quick

- Quick aufladen:
  - Benötigt PIN
  - Benötigt online Verbindung zum zentralen System
  - Behebt den Geldbetrag vom Kundenkonto und zahlt es auf ein sogenanntes “Pool-Konto” von Europay ein.
- Terminal-Karte:
  - Sind in allen Quick-Terminals vorhanden
  - Erlaubt “offline” Zahlungen durch Authentizierung der Quickkarte gegenüber dem Terminal

Quick

- Quick Transaktionen:
  - Kunden und Terminalkarten können sich gegenseitig authentifizieren
  - Geld wird vom Kunden-Quick-Konto auf die Terminalkarte übertragen
- Geld einsammeln:
  - Daten des Terminals werden an Europay übertragen
  - Geld wird dann vom Pool-Konto von Europay auf das Händlerkonto überwiesen

Secure Electronic Transactions – SET

- Vorherrschendes System der Vergangenheit für Kreditkartentransaktionen
- SET wurde 1996 von Mastercard und VISA entwickelt
- Basieren auf PKI
- Erfordern die Installation einer elektronischen Geldbörse auf dem PC

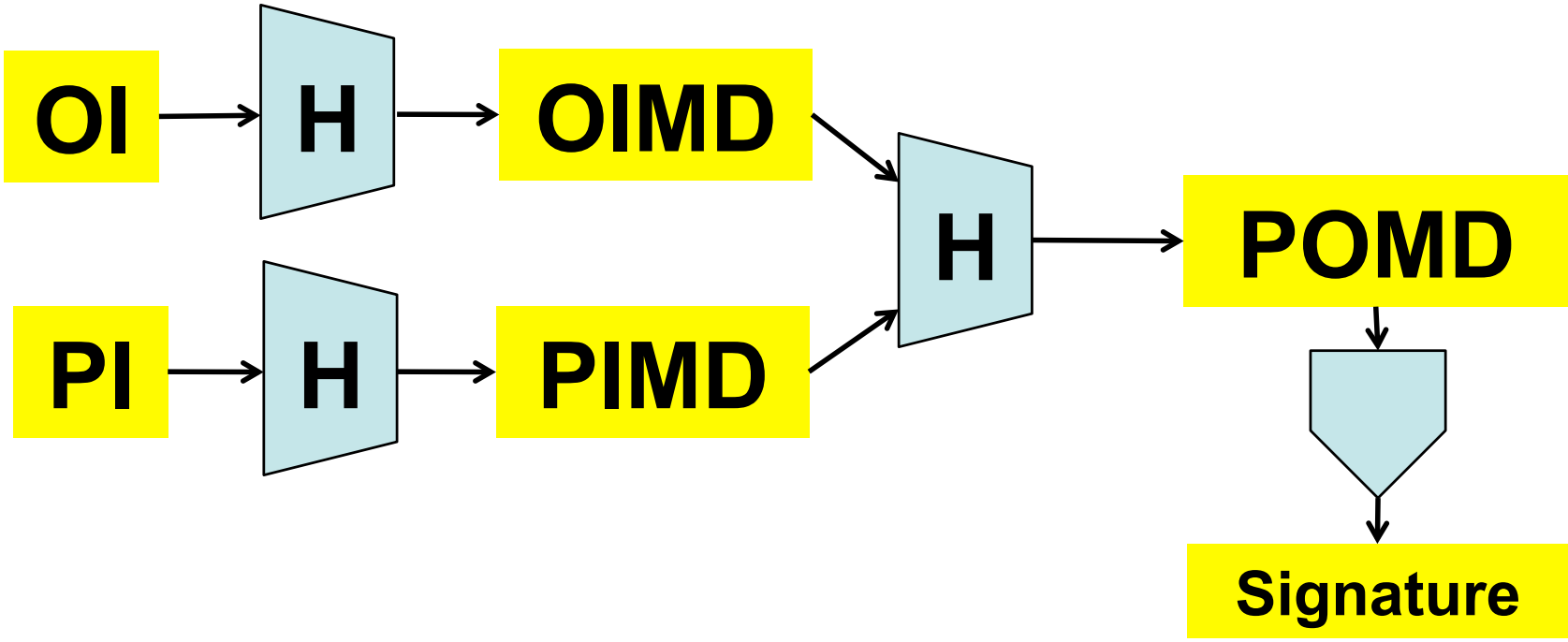
SET: Sichere Transaktionen

- Authentische Transaktionen
- Vertrauliche Transaktionen
- Privatsphäre der Kunden:
  - Händler sollen keine Kontodaten der Kunden wissen
  - Banken sollen nicht das Kaufverhalten der Kunden erfahren
  - Wird durch sogenannte duale Signaturen erreicht

SET: Duale Signaturen

- Erlaubt dem Kartenbesitzer die Abwicklung der Bestellung und Bezahlung in einer Nachricht
- Die Nachricht hat einen Zahlungsabschnitt und einen Bestellabschnitt
  - Der Händler kann den Zahlungsabschnitt nicht sehen
  - Der Bezahlungs-Gateway kann den Bestellabschnitt nicht sehen
  - Aber, beide Abschnitte sind aneinander gebunden

SET: Duale Signaturen



- Bank erhält: *PI*, *OIMD*, *signature*
- Händler erhält: *OI*, *PIMD*, *signature*

Wie funktioniert SET?

- Der Kunde sendet einen Purchase-Request:
  - Order: OI, duale Sig., SHA-1(PI)
  - Payment:

$$DES_k(PI, \text{duale Sig.}, \text{SHA-1}(OI)), \text{RSA-Enc}_{PK-Bank}(k)$$

  - Zertifikat des Kunden
- Händler:
  - Verifiziert Zertifikat und duale Signatur
  - Bearbeitet Bestellung und leitet Payment-Abschnitt weiter
- Bank:
  - Entschlüsselt alles und überprüft duale Sig.
  - Wenn ok $\Rightarrow$ Authorisiert Bestellung

Nachteile von SET

- Installation der Geldbörsen-Software am Kunden-PC
- PKI:
  - Kunde benötigt Schlüsselpaar und Zertifikat
  - Bank benötigt Schlüsselpaar und Zertifikat
  - Händler benötigt Schlüsselpaar und Zertifikat
- Der System-Aufbau war sehr langsam

3-D secure

- Nachfolger von SET
- Erscheint erfolgreicher zu sein

PayPal

- Begann in 1998
- Jeder mit einer mail-Adresse und einem Bankaccount kann so ein PayPal-Konto eröffnen
- PayPal wurde schnell groß:
  - 164 Millionen Accounts
  - 2002 von eBay übernommen

Wie funktioniert PayPal?

- Kunde und Händler muss ein PayPal-Konto haben
- Kontoeröffnung benötigt:
  - Kreditkarten/Kontoinformation
  - Gültige Mailadresse
- Geldüberweisung benötigt:
  - Name und mail-Adresse des Empfängers

Wie funktioniert PayPal?

- Wie man Geld erhält:
  - Man erhält eine Mail
  - Das Geld wird dem PayPal-Konto gutgeschrieben
- SSL/TLS-Verbindungen für die Sicherheit
  - CAPTCHA
  - Security Key (2007)

Probleme von PayPal

- Einige Webseiten zeigen User-Probleme mit PayPal:
  - `www.paypalsucks.com`
  - `www.paypalwarning.com/`
- Hängt oft mit der Eröffnung und Schließung von PayPal-Konten zusammen
  - Händler konnten für Kunden Konten anlegen, ohne dass deren Zustimmung nötig war
- Betrugsfälle durch Phishing

PaySafe Karte

- Ein österreichisches System
  - Das System wird in Wien gehostet
- Pre-paid Karten:
  - User können mit diesen Karten später anonym bezahlen
  - Unterschiedliche Kartenwerte (25-100 Euros)
- Einfach und benutzerfreundlich

Wie funktioniert die PaySafe Karte?

- Jede Karte hat einen 16-Ziffern PIN
- Im Web-Shop gibt der Kunde den PIN und den Betrag ein
  - Der PIN wird online auf Gültigkeit überprüft.
  - Der Betrag wird von dem Karten-Konto abgebucht
  - Alle Transaktionen werden durch SSL geschützt
- Der PIN ist “eindeutig” für jede Karte
- Wenn die Karten erzeugt werden, werden die PINs in das System übernommen, aber nicht aktiviert . . .
- Nur wenn die Karten an die Händler ausgeliefert werden, werden die PINs aktiv geschalten

FirstGate Click&Buy

- Ein deutsches System für Micro-Zahlungen
- Kunde registriert sich bei FirstGate:
  - Name, Adresse, e-mail-Adresse und Bankkonto
  - Alle Transaktionen werden durch SSL gesichert
- Händler verlinken ihre Inhalte zu Click&Buy:
  - Die Inhalte sind downloadbar, wenn der Preis bestätigt wird und der User sich durch Username/Passwort authentifiziert hat
- FirstGate sammelt diese Überweisungen und bucht monatlich die gesammelten Beträge vom Bankkonto des Kunden ab

NFC und Google Wallet

- Near Field Communication
- Google Wallet App kann Kreditkarten, Debitkarten, etc. speichern (“Your wallet in the cloud”)
- Pay-Pass (Mastercard) und payWave (Visa) Terminals
- Kann in den USA bereits an vielen Stellen genutzt werden

Zusammenfassung

- Es gibt eine Vielzahl von Anläufen für sicheres elektronisches Geld
- Die am besten durchdachten Ansätze scheiterten durch ihre Komplexität und Benutzerunfreundlichkeit
- Daher wurden andere Richtungen von den Unternehmen eingeschlagen
- Es scheint, dass Bequemlichkeit über Sicherheit gestellt wird

Vielen Dank für Ihre Aufmerksamkeit!