COMP 3410 / 6341 – I.T. in Electronic Commerce

E-Trading

3. Electronic Payments

Roger Clarke

Xamax Consultancy, Canberra

Visiting Professor, A.N.U. and U.N.S.W.

http://www.rogerclarke.com/EC/ ...

ETIntro.html#L3, OhdsET3.ppt

ANU RSCS, 4 September 2012

E-Trading
Electronic Payments

Agenda

1. Pre-Electronic
   Early Electronic
2. Internet
   Mobile
3. Threats and Vulnerabilities
4. Who wears the Damage?

Some Important Payment Mechanisms Prior to the Internet Era c. 1995

Pre-Electronic

- Cash (Coins, 'Bank' Notes)
- Cheque
- Money Order
- Periodic Payment Authority
- Charge- or Credit-Card voucher using a Flick-Flack (from the 1960s)
- Card Not Present (CNP) Mail Order (MO..)

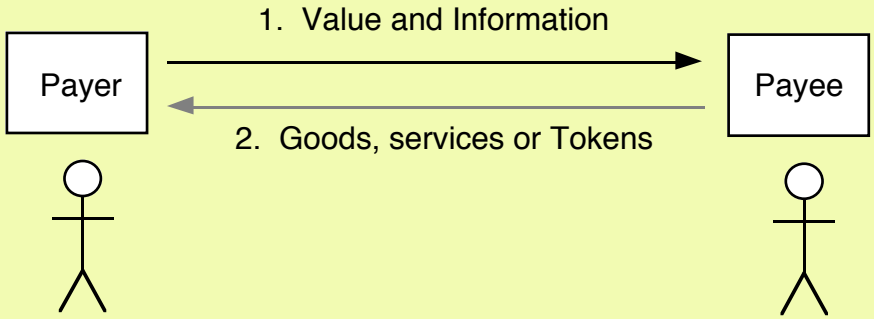
Some Important Payment Mechanisms Prior to the Internet Era c. 1995

Pre-Electronic

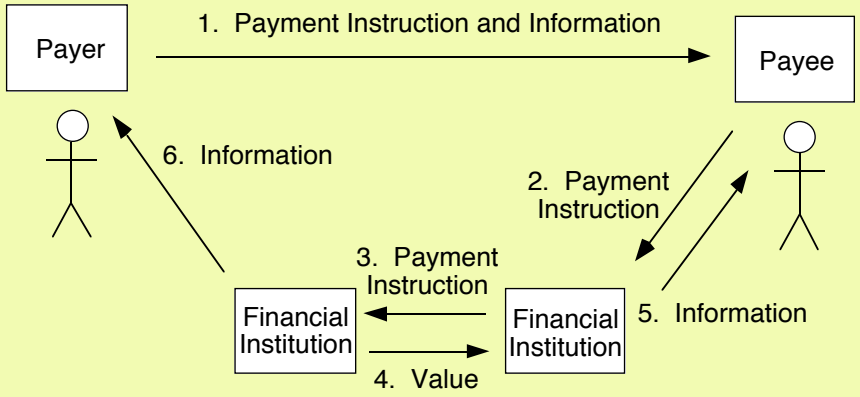
- Cash (Coins, 'Bank' Notes)
- Cheque
- Money Order
- Periodic Payment Authority
- Charge- or Credit-Card voucher using a Flick-Flack (from the 1960s)
- Card Not Present (CNP) Mail Order (MO..)

Early Electronic

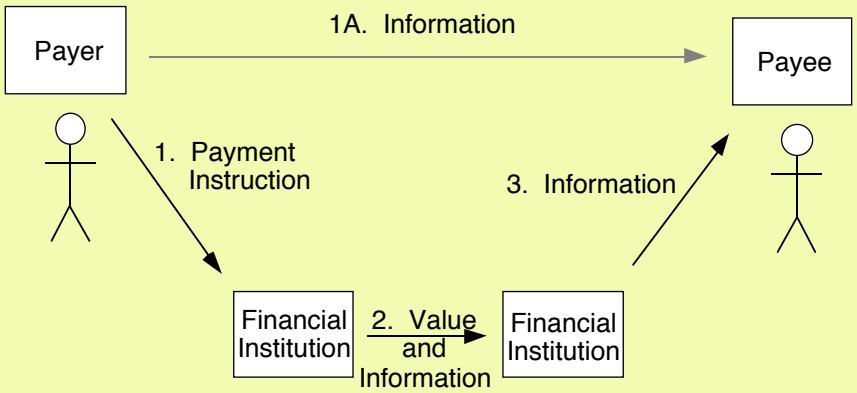
- Telegraphic Transfer (TT) (from the 1870s)
  Wired transfer
  Direct Credit
  Giro
- Card Not Present (CNP) Telephone Order (..TO)
- Telco Account
- Card voucher with EFTPOS (from the 1980s)



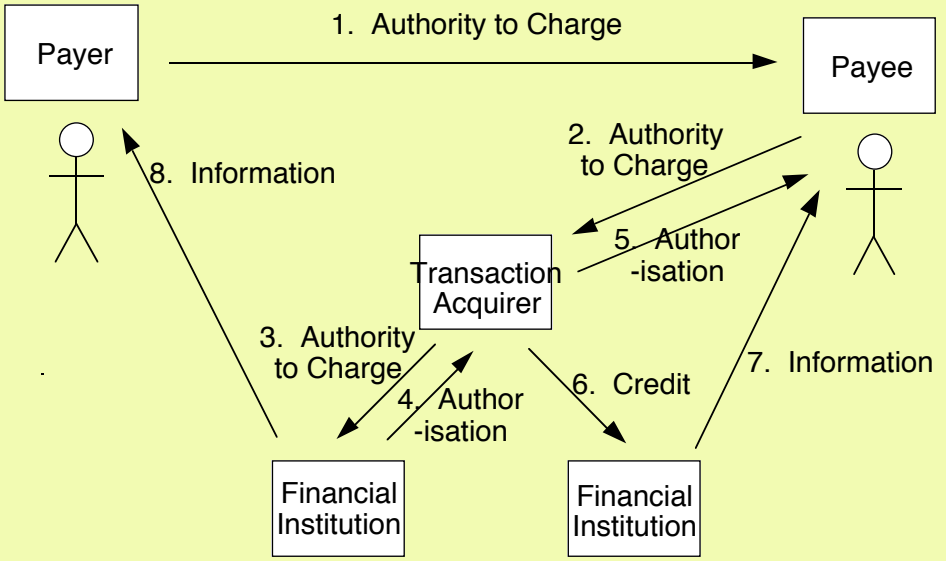
Payment by Cash



Payment by Cheque



Direct Credit
Giro, 'TT', Salary Payments



Credit Cards and Charge-Cards
(in 'Meatspace' Transactions)

The Security Profile of Meatspace Credit-Card Transactions

- Two-factor Authentication:
  - 'have a token'
  - 'know (a secret?)'
- Vulnerable to cloning, forgery, card&PIN-capture
- Relies on:
  - **card-holder retention of the card**
  - **production of the card at POS**
  - **performance of a signature facsimile or PIN**
  - consumer reconciliation of their accounts
  - self-insurance by merchants (banks issue 'charge-backs')

The Improved Security Profile of Meatspace Credit-Card Transactions with Contact-Based Chip-Card / EMV

- Two-factor Authentication:
  - 'have a token'
  - 'know (a secret?)'
- Vulnerable to **cloning**, **forgery**, card&PIN-capture
- Relies on:
  - **card-holder retention of the card**
  - **production of the card at POS**
  - **performance of a signature facsimile or PIN**
  - consumer reconciliation of their accounts
  - self-insurance by merchants (banks issue 'charge-backs')

The (In)Security Profile of Card-Not-Present (CNP/MOTO) Transactions

- Single-Factor Authentication:
  - 'have credit card details' not 'have the card'
  - no 'know a secret' factor
- Vulnerable to lying, cloning, forgery, carddetails-capture
- Relies on:
  - secrecy of credit-card details [??]
  - general levels of honesty
  - **consumer reconciliation of their accounts**
  - **self-insurance by merchants (banks issue 'charge-backs')**

The Very Slightly Improved (In)Security Profile of Card-Not-Present (CNP/MOTO) Transactions with Contact-Based Chip-Card / EMV

- Single-Factor Authentication:
  - 'have credit card details' not 'have the card'
  - no 'know a secret' factor
- Vulnerable to lying, **cloning**, **forgery**, carddetails-capture
- Relies on:
  - secrecy of credit-card details [??]
  - general levels of honesty
  - **consumer reconciliation of their accounts**
  - **self-insurance by merchants (banks issue 'charge-backs')**

2. Internet Payment Schemes

- **Credit-Cards**
  - Via Email, or http, or even https
  - Pre-stored / Intermediated
- **Electronic Value-Tokens**
  especially DigiCash's eCash
- **Electronic Payment Instructions**
  - Batch Direct Entry, e.g. FEDI
  - Online Direct Entry
    - Internet Banking
      initiated by Payer or Payee

(Additional) Credit-Card Insecurities

- Email (generally) and http are 'in clear', so **eavesdroppers can capture and exploit the data**
- SSL/TLS, e.g. https
  - protects against eavesdropping; but
  - is subject to masquerade
    because dig certs are all-but worthless

So **spoofing / phishing is a major exposure**

Payments in the Network Era
Initially Wired, Increasingly Unwired

Insecure Models

- EFTPOS – Cr Tx

Payments in the Network Era
Initially Wired, Increasingly Unwired

Insecure Models

- EFTPOS – Cr Tx

Highly Insecure Models

- Credit Card Tx
  over the Internet
  (CNP / MOTO)

Payments in the Network Era
Initially Wired, Increasingly Unwired

Insecure Models

- EFTPOS – Cr Tx

Highly Insecure Models

- Credit Card Tx over the Internet (CNP / MOTO)

'Secure' Models

- ATMs
- Direct Entry
- EFTPOS – Dr Tx (i.e. with PIN)
- Internet Banking (https & 2-factor)

Chips in Payment Schemes

From ... open magnetic-stripe data containing all the thief needs

... To data on a contact-chip, which hides data necessary to the Tx

Withheld in Australia 2000-2010
Still withheld in some countries

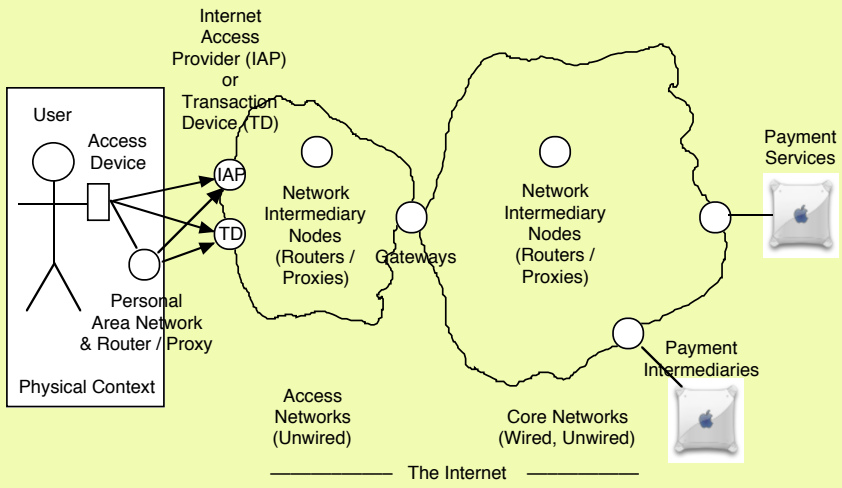
3. Mobile Payment Schemes

- **Stored-Value Cards** for low-value purchases

3. Mobile Payment Schemes

- **Stored-Value Cards** for low-value purchases
- **Credit-Card Transactions from Handhelds**
  CNP/MOTO living on the very edge

Credit-Card Transactions from Handhelds Technical Architecture



Threat Aspects – Third-Party, Within the System (Who else can get at you, where, and how?)

- Points-of-Payment Physical:
  - Observation
  - Coercion
- Points-of-Payment Electronic:
  - **Rogue Devices**
  - **Rogue Transactions**
  - **Keystroke Loggers**
  - **Private Key Reapers**
- Network Electronic
  - **Interception**
  - Decryption
  - **Man-in-the-Middle Attacks**
- Points-of-Processing
  - Rogue Employee
  - Rogue Company
  - **Error**

Threat Aspects – Third-Party, Within the Device

- Physical Intrusion
- Social Engineering
  - Confidence Tricks
  - **Phishing**
- Masquerade
- Abuse of Privilege
  - **Hardware**
  - **Software**
  - **Data**
- Electronic Intrusion
  - Interception
  - Cracking / 'Hacking'
    - Bugs
    - Trojans
    - Backdoors
    - Masquerade
  - Distributed Denial of Service (DDOS)
  - **Infiltration by Software with a Payload**
  - **...**

Threat Aspects – Third-Party, Within the Device Infiltration by Software with a Payload

Software (the 'Vector')

- Pre-Installed
- User-Installed
- **Virus**
- **Worm**
- ...

Payload

- Trojan:
  - **Spyware**
  - **Performative**
  - **Communicative**
  - Bot / Zombie
- Spyware:
  - Software Monitor
  - Adware
  - **Keystroke Logger**
  - ...

The Vulnerability Aspect

- The Environment
  - **Physical Surroundings**
  - Organisational Context
  - **Social Engineering**
- The Device
  - Hardware, Systems Software
  - Applications
  - **Server-Driven Apps (ActiveX, Java, AJAX)**
  - **The Device's Functions: Known, Unknown, Hidden**
  - **Software Installation**
  - **Software Activation**
- Communications
  - Transaction Partners
  - Data Transmission
- Intrusions
  - **Malware Vectors**
  - **Malware Payloads**
  - Hacking, incl. Backdoors, Botnets

Key Safeguards Required

- Two-Sided **Device Authentication**, i.e.
  - by Payee's Chip of Payer's Chip
  - **by Payer's Chip of Payee's Chip**
- **Notification to Payer** of:
  - Fact of Payment (e.g. Audio-Ack)
  - Amount of Payment
- At least one **Authenticator**
- Protection of the **Authenticator(s)**
- **A Voucher** (Physical and/or Electronic)
- Regular **Account Reconciliation** by Payers

3. Mobile Payment Schemes

- **Stored-Value Cards** for low-value purchases
- **Credit-Card Transactions from Handhelds**
  CNP/MOTO living on the very edge
- **Contactless Cards**
  - Contactless ETags for Toll-Roads
  - Tap-On-and-Off for Public Transport Tickets
  - Tap-and-Pay

Contactless Cards

Contactless Cards

- **eTags for Toll-Roads**
  Operate autonomously
  Limited audit-trail; difficult to challenge

RFID Tags for Road-Tolls

- Car requires a Tag
- Car drives through Control-Point
- Fee shown on a static or variable display
- Control-Point interacts with Tag
- Toll is deducted automatically
- Audio-acknowledgement of transaction
- Depends on blind consumer trust

Contactless Cards

- **eTags for Toll-Roads**
  Operate autonomously
  Limited audit-trail; difficult to challenge

- **Tap-On-and-Off – Public Transport Tickets**
  HK Octopus, London Oyster, ...
  Qld GoCard, ACT Myway?, Vic MyKi?, NSW???

Octopus Hong Kong Since Sep 1997

- To pay, wave an Octopus card within a few cm of the reader (even if it's in a wallet/purse)
- Audio-acknowledgement (beep)
- Display of tx amount and remaining balance
- On MTR and KCR transport, the tx amount is calculated from the entry and exit points

Contactless Cards

- **eTags for Toll-Roads**
  Operate autonomously
  Limited audit-trail; difficult to challenge
- **Tap-On-and-Off – Public Transport Tickets**
  HK Octopus, London Oyster, ...
  Qld GoCard, ACT Myway?, Vic MyKi?, NSW???
- **Tap-and-Pay** – Visa **PayWave**, MasterCard **PayPass**
  PIN-less up to c. $100, with no dockets necessary

Contactless Chip-Cards as Payment Devices

- RFID / NFC chip embedded in card
- Wireless operation, up to 5cm from a terminal
- Visa Paywave and MasterCard PayPass
- Up to $100 (cf. the promised $25)

Contactless Chip-Cards as Payment Devices

- RFID / NFC chip embedded in card
- Wireless operation, up to 5cm from a terminal
- Visa Paywave and MasterCard PayPass
- Up to $100 (cf. the promised $25)

- Presence of chip in card is not human-visible, but Logo / Brand may be visible
- No choice whether it's activated
- Operation of chip in card is not human-apparent
- No action required when within 5cm range, i.e. automatic payment
- No receipt becomes the norm
- Used as Cr-Card: Unauthenticated auto-lending
- Used as Dr-Card: PIN-less charge to bank account

Contactless Chip-Cards as Payment Devices
What Consumers Have To Do

- **Discover a suspect transaction**. But that's not easy, because:
  - statements must be reconciled, and within 30-60 days
  - the transaction-count is large, and the statements are long
  - for many valid transactions, no voucher is to hand
  - many entries don't contain the merchant's name
- **Discover how to complain**
- **Complain**
- **Convince** your financial institution to reverse the transaction

- Most bogus transactions will never be found
- Cheats will prosper and consumers will suffer
- Criminals will learn to use the system carefully, but often

E-Trading
Electronic Payments

Agenda

1. Pre-Electronic
   Early Electronic
2. Internet
   Mobile
3. Threats and Vulnerabilities
4. Who wears the Damage?

COMP 3410 / 6341 – I.T. in Electronic Commerce

E-Trading
3. Electronic Payments

Roger Clarke

Xamax Consultancy, Canberra
Visiting Professor, A.N.U. and U.N.S.W.

http://www.rogerclarke.com/EC/ ...
ETIntro.html#L3, OhdsET3.ppt

ANU RSCS, 4 September 2012

Japanese Osaifu-Keitai / Mobile Wallet

- Many Japanese mobile phones contain an extra chip, which uses RFID/NFC to communicate with payment-related devices
- Services include:
  - eMoney (Edy)
  - public transport (Mobile Suica)
  - credit card?
  - vending machines (Cmode)
  - (loyalty card, id card, ...) Don't lose it!!
- The chip is the Sony FeliCa (as in Octopus)
- Sony Viao PCs can interact with FeliCa

http://en.wikipedia.org/wiki/Japanese_mobile_phone_culture
http://en.wikipedia.org/wiki/Osaifu_Keitai

Visa MicroTag Trials
using Visa payWave Technology

- Intended to support 'instant purchase'
- Carried as a key-ring / key-chain
- Requires proximity (1-2 inches)
- Provides a visual indication when it operates
- No confirmation under a threshhold [US$ 25?]
- Not standards-based?
- No independent security testing?
- No public audit and certification?

http://arstechnica.com/news.ars/post/20070930-ready-or-mostly-not-here-come-more-contactless-payment-devices.html – 30 Sep 2007

UK Parking Payment

- Customer registers with RingGo
- RingGo stores (most of) their credit card details
- Customer uses their mobile phone to call a RingGo phone-number displayed in the car-park
- Customer keys the car-park's 4-digit code
- Customer chooses the duration of stay
- Customer keys remaining digits of credit-card
- RingGo processes a credit-card transaction, and makes data available on-line to traffic wardens
- Customer can access the transaction trail online
- [Still pre-paid, so still risk over-run!]

http://www.ringgo.co.uk/

Australian M-Payment

- No information about the security design
- Unclear risk allocation
- Unclear/incomplete privacy policy
- Unclear who's behind the company
- Unclear/incomplete terms of contract at:
  http://www.mhits.com.au/content/tabID__3340/Policy.aspx
- Unclear what regulatory regimes apply:
  - RBA/APRA (financial)
  - Ombudsman/ACCC/ASIC (consumer)

http://www.mhits.com.au/

PayPal

- Links an Account with the Intermediary to:
  - an existing bank account; and / or
  - an existing credit card

  (but may be becoming a card-issuer too)
- Passes on Payment Instructions sent from:
  - web-browser
  - touch-tone to IVR
  - SMS / text-messages

  (but imposes punitive terms and fees)

Drill-Down on Security Analysis

- **'The ATM Model'**
  - ATMs
  - Debit-Cards over EFTPOS
  - Internet Banking
  - Debit-Cards over the Internet
- **'The Credit-Card Model'**
  - Credit-Cards over EFTPOS
  - Credit-Cards over the Internet
  - Ready-SET-Don't Go
  - 3D-Secure?

ATMs

- 2-factor:
  - have card
  - know the PIN
- PIN keyed into secure PIN-pad, in a manner which makes it difficult to observe [?]
- Hash of PIN transmitted and compared
- So the 'know' part is protected from both physical and electronic observation

Debit-Cards over EFTPOS Networks Followed ATMs and the ATM Security Model

- 2-factor:
  - have card
  - know the PIN
- PIN keyed into secure PIN-pad, in a manner which makes it difficult to observe [?]
- Hash of PIN transmitted and compared
- So the 'know' part is protected from both physical and electronic observation

Internet Banking – Various Implementations

- 2-factor or 3-factor authentication, e.g.
  - know account details / login-id
  - know PIN
  - various third factors:
    - pre-registered IP-addresses only
    - know One-Time Password (OTP)
    - receive and key OTP sent at the time over another channel (e.g. SMS msg)
- Authenticator(s) keyed into insecure key-pad, in a manner which makes it difficult to observe
- So the 'know' part is protected from physical, and partly from electronic, observation

Debit Transactions over the Internet

- Customer is at a merchant's payment page
- **Customer is re-directed to a specialised version of their own bank's online-banking services**
- **Customer uses their own bank's Internet Banking service to authorise the transaction, including an encrypted channel (SSL/https)**
- Customer is redirected to the merchant
- Canada's scheme is called Interac Online: http://www.interaconline.com/
- This leverages on a well-trusted infrastructure, but requires careful interfacing from merchants

Credit-Cards over EFTPOS Networks
Did *NOT* Follow the ATM Security Model

- 2-factor:
  - have card
  - reproduce signature pre-recorded on-card
- No PIN
- Some improvement through stop-list being automated on-line rather than manual
- The primary purpose was not security, but the transfer of data-capture costs to merchants

Credit Card Tx over the Internet
Worse Yet – Applied the CNP/MOTO Model

- The 'have' factor is not 'have the card' but merely 'have credit card details'
- No second-factor such as 'know a secret'
- Relies on:
  - an encrypted channel (SSL/https)
  - secrecy of credit-card details [??]
  - general levels of honesty
  - consumers reconciling their accounts
  - self-insurance by merchants (banks issue 'charge-backs')

Ready – SET – Don't Go
Secure Electronic Transaction Processing for Internet Credit Cards

- Card-Holder states that he wishes to make a payment
- Merchant acknowledges
- **Card-Holder provides** payment amount, **digital certificate**
- Merchant requests an authorisation from the Payment-Processing Organisation (via a Payment Gateway / Acquirer)
- Existing EFTS networks process the authorisation
- Merchant receives authorisation
- Merchant sends capture request (to commit the transaction)
- Merchant receives confirmation the transaction is accepted
- Merchant sends Card-Holder confirmation

Credit-Card Transactions over the Internet 3-D Secure

- A Visa Initiative, but licensed to others:
  - Verified by Visa
  - MasterCard SecureCode
  - JCB J/Secure
- For merchants and financial institutions, specifies authentication and processing procedures
- Requires some form of **card-holder** authentication, at this stage generally keying of a **password/PIN**
- May require EMV-chip and smartcard reader

http://en.wikipedia.org/wiki/3-D_Secure
https://partnernetwork.visa.com/vpn/global/...
...retrieve_document.do?documentRetrievalId=118

Credit-Card Payments in the MCommerce Mobile / Handheld / Unwired Era

- Inherits weaknesses of MOTO / Internet
- Less visible payee, no 'footprint'
- Less visible process, perhaps invisible
- Less visible transaction data?
- Notification record / transaction voucher?
- Any improvement may depend on mobile devices incorporating a smartcard-reader

Debit-Card Payments in the MCommerce Mobile / Handheld / Wireless Era

- Less visible payee, no 'footprint'
- Less visible process, perhaps invisible
- Less visible transaction data?
- Notification record / transaction voucher?
- **Vulnerability of Authenticators when processed on mobile devices**
- **Transmission of PIN or hash w/- SSL?**