

Lecture 15 Security & Electronic Payment Systems

Boriana Koleva
bnk@cs.nott.ac.uk
C54

Overview

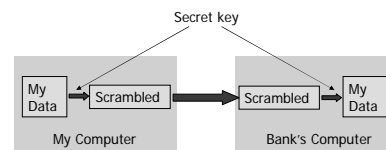
- Security Requirements and Solutions
 - Secret Key Encryption
 - Public Key Encryption
 - Digital Signatures
 - Digital Certificates
- Electronic Payment Methods
 - Electronic Fund Transfer (EFT)
 - Financial EDI
 - Credit Cards
 - Digital Cash
 - Online Stored Value Systems
 - Smart Cards

Security Requirements

- Confidentiality
- Authentication
- Integrity
- Nonrepudiation
- Availability

Secret Key Encryption (1)

- Encryption uses a single key (a unique data item)
- Both sender and receiver must have the same key

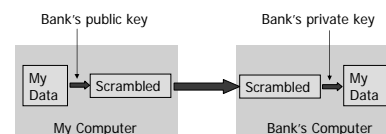


Secret Key Encryption (2)

- Secret key encryption can be very secure
 - security dependent upon size of key
- Data Encryption Standard (DES)
 - 56-bit DES is penetrable, but penetration would typically take years
- Problem
 - the key must be kept secret
 - there must be a secure means for transmitting the key between the sender and the recipient

Public Key Encryption (1)

- Encryption uses two different keys
 - Public and private keys
 - Public key is published, private is kept secret

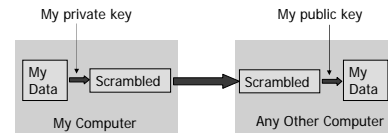


Public Key Encryption (2)

- Extremely secure
 - again security is dependent upon the size of keys
 - effectively impenetrable if the key is large enough
- Since the sender only requires the public key of the recipient, there is no problem with key delivery
- Rivest, Shamir & Adleman algorithm (RSA)
 - Widely used in e-commerce
 - Often used in conjunction with the faster DES

Digital Signatures (1)

- Used for authentication of senders
- Public key encryption in reverse
 - Anyone with the sender's public key can decrypt the message, but only if it was encrypted with the correct private key



Digital Signatures (2)

- Sender
 - Run document through hash function – message digest
 - Original message + digest encrypted with receiver's public key
 - Sender's private key used to encrypt the result again
 - Double encrypted messages sent over Internet
- Receiver
 - Uses sender's public key to authenticate the message
 - Uses own private key to decipher original message + digest
 - Applies hash function to the original message and compares result with received value in the message digest
 - confidentiality, authentication and integrity insured

Digital Certificates

- Issued by a certificate authority (CA)
 - trusted third party
 - VeriSign is the best known
- Certificates contain:
 - serial number
 - name of owner
 - public keys (for message receipt and signatures)
 - name of CA
 - CA's digital signature
 - other information (e.g. certificate type)
- Time-stamped certificates are often issued when a transaction occurs, and may be stored by the CA

Encryption for Electronic Payment

- Digital signature of the sender assures sender authentication and nonrepudiation
- Digital signature can be used to test data integrity
- Combined DES/RSA encryption is very secure - ensuring privacy
- Receiver's certificate assures receiver authentication and nonrepudiation
- Transaction certificates stored by CA provide third-party evidence of authentication and nonrepudiation

Security Schemes

- Security schemes are implemented by protocols
 - SSL (Secure Socket Layer)
 - SET (Secure Electronic Transaction)
- Secure-HTTP (S-HTTP) applies SSL used for HTTP communication
- SSL requires all communication is encrypted by RSA/DES, and integrity is confirmed
- S-HTTP is widely used for e-commerce web sites (e.g. for orders, credit card information etc.)
- S-HTTP requires an SSL compliant browser and server

SSL vs. SET

- SET (Secure Electronic Transfer) developed jointly by Visa, MasterCard & American Express
- SET is built on top of SSL, and is much more secure
 - Customer downloads and installs a "digital wallet"
 - The digital wallet contains the customers certificate
- SET is slower than S-HTTP
- SET is much more complex for the user
 - Very rarely used
 - Where SET is used, S-HTTP is offered as an alternative
- Wells Fargo have developed a smart card based certificate for use with SSL

Electronic Payment in E-commerce

- Business to Business Payments
 - small to very large sums
- Consumer Payments
 - small to medium sums
 - usually credit card transactions
- Micropayments (consumer)
 - very small sums
 - credit card transactions are much too expensive

Electronic Fund Transfer (EFT)

- Designed to transfer funds from one account to another
 - Customer instructs bank (e.g. using ATM)
 - Bank debits the customers account and submits payment notification to an automated clearing house
 - Clearing house submits payment notification to merchant's bank, which credits the merchant's account
- Traditionally this has used dedicated networks called VAM (Value Added Networks)
- The Internet may now be used in place of VAM
 - Internet banking
 - "Cyberbanks"
 - SSL is always used
 - Certificates are currently rarely used (this may change in the future)

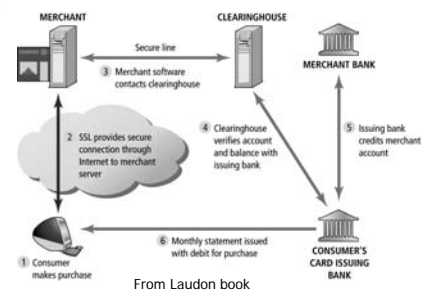
Financial EDI

- EDI (Electronic Data Interchange)
- The electronic interchange of standardised business documents between commercial partners
 - Orders
 - Bills
 - Credit approval
 - Shipping notices
 - Confirmations
 - Etc.
- Financial EDI extends this to incorporate EFT
- EDI is traditionally implemented on VAN, but is increasingly implemented on the Internet
- Financial EDI on the Internet uses SSL

Credit Card Payments

- Credit card payments are by far the most popular means of consumer electronic payment
- Conventionally credit card payment is only partially automated
 - Cardholder shows card to merchant
 - Merchant asks for approval from the credit card company
 - The bill is then considered paid by credit - the merchant keeping a sales slip
 - The merchant sells the slip to a bank, and pays a fee for the service
 - The bank requests that the credit card company reimburses the debt
 - The credit card company pays the bank, and bills the cardholder the same amount

Online Credit Card Transaction



Digital Cash – PayPal

- One of e-commerce's major success stories:
 - Went public in 2002; acquired by eBay October 2002 for \$1.5 billion
- An example of a "peer-to-peer" payment system
- Fills a niche that credit card companies avoided – individuals and small merchants
- Piggybacks on existing credit card and checking payment systems
- Weakness: suffers from relatively high levels of fraud
- Competitors include Western Union (MoneyZap), AOL (AOLQuickcash) and Citibank (C2it)

Smartcards

- Magnetic strips have been used to store personal ID numbers since the 1970's
- Smartcards (IC cards) are programmable devices with local storage that can store much more information
- These provide the ideal places to store certificates and encryption keys
- Rechargeable "electronic purse" or "Stored Value" cards
 - Examples
 - Mondex in UK
 - VisaCash in US
 - Electronic delivery vehicle for cash
 - Card is recharged from a bank account (effectively EFT)
 - Individual transactions are then effectively cash (i.e. no central communication, and no charge)
 - NB open (Mondex) vs. closed systems

Micropayments

- Making numerous very small charges for electronic goods or services
- Not feasible using credit cards or EFT - these are much too expensive
- Possible through:
 - Digital Cash
 - Smartcards (stored value systems)
 - Digital Accumulating Balance payment systems

Electronic Payment Summary

- Business to Consumer transactions
 - Credit card payment using SSL is currently the de facto standard
 - SET is not yet widely adopted, but may become so in the near future
 - Digital Cash is an alternative
- Business to Business transactions
 - Credit card fee system is too high for large transactions
 - EFT has been used for many years on dedicated VAN's
 - Increasingly the Internet is being used
 - Financial EDI is integrating all aspects of transactions
- Micropayment
 - Credit card or EFT fee system is prohibitive
 - Possible through Digital Cash, Smartcards and Digital Accumulating Balance payment systems