Electronic Payment Systems (ECOM6016)

COURSE DESCRIPTION AND SYLLABUS

February 21 - March 9, 2014

Course Description

Electronic payments are the life blood of eCommerce. Electronic payments are expanding rapidly but also changing because of the pervasive use of tablets and smartphones, whose use is not confined to consumer transactions. This course covers a wide variety of electronic payment mechanisms that are used to make more than 10^16 HKD in payments worldwide each year. The course is designed to stimulate creative thinking about the use of new technologies in the movement of money, from small peer-to-peer transactions through the largest interbank payments. Even though everyone is familiar with money on a day-to-day basis, very few people, even those in the financial services industries, understand how money actually moves. Think about it: how does a bank pay another bank? How does the money actually move?

Payments are complex because they usually involve at least five parties -- in addition to the buyer and seller there are also the buyer's bank, the seller's bank and the country's central bank, and this does not even include service providers who transmit payment data and aggregate transactions. The buyer and seller must communicate with each other concerning the transaction, then instructions must be transmitted to the buyer's bank, which then takes action at the central bank to cause money to appear in the seller's account in the seller's bank. When different currencies are involved, the central banks of two countries are involved (except in HK in certain special cases, which is one way HK's financial system is unique).

Every payment system must provide for secure communication of payment orders. The course covers banking systems, epayment security, foreign exchange, Internet banking, wireless payments, stored-value cards, micropayments, peer-to-peer payments, large-scale B2B payments and the future of money. Particular attention is given to the Hong Kong and Mainland China banking systems.

Learning Outcomes

Upon completion of the course, you should understand the different forms of electronic money, how money moves through the world's banking systems, how security is achieved in payment systems, how electronic banking works and the unique role of Hong Kong payment systems in world commerce. After taking this course, you should be able to select and even design an appropriate payment method to fit a particular business model even as underlying technologies, such as mobile platforms, undergo rapid change.

Instructor

Michael I. Shamos is Distinguished Career Professor in the School of Computer Science at CMU, Visiting Professor at the University of Hong Kong, Director of the Universal Library and Director of the Master of Science in eBusiness Technology degree program at Carnegie Mellon University in Pittsburgh, Pennsylvania. He is a member of the Bars of the Commonwealth of Pennsylvania, the U.S. Supreme Court and the United States Patent and Trademark Office.

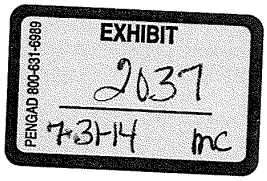
Email: shamos@cs.cmu.edu

Textbook (Required)

Protocols for Secure Electronic Commerce, by M. H. Sherif, Second Edition, ISBN 0849315093.

Other Recommended Books (Optional)

Two other worthwhile books on electronic payment system are:



Payment Systems: From the Salt Mines to the Board Room, by Rambure and Nacamuli. ISBN 978-0-230-20250-4. This is a high-level overview of money movement, including details of the U.S. and Honk Kong payments systems, Also includes material on SWIFT and electronic invoice presentment.

Payment Technologies for E-Commerce, by Weidong Kou, ISBN 3540440070. Prof. Kou is a faculty member at HKU and has compiled a number of papers in this book, including his own, concerning epayment security, mobile payment, digital cash and micropayments. This was the course textbook in 2011.

Readings (Required)

Assigned readings for a particular lecture are to be completed before the lecture. Some of the readings are quite long and detailed. In such cases you should familiarize yourself with the material generally and delve deeply only into the topics listed in the syllabus.

Course Format

10 three-hour lectures, readings, one homework assignment and an open-book final exam. The basis for the course is the lectures and the reading assignments provide important background information. No textbook exists that presents all the necessary course material. Attendance counts for 10% of the grade; the homework assignment counts for 30% of the grade; and the open-book final exam counts for 60% of the grade.

Course Syllabus

Lecture 1 - **INTRODUCTION TO MONEY AND BANKING** (Thursday, February 21, 2014, 6:45 p.m.) This lecture explores the fundamental nature of money, ways it can be made electronic, how it is transferred and the commercial and central banks play in the process. Payment for goods and services usually involve four parties, not two: the buyer, the seller, the buyer's bank and the seller's bank. Money moves between banks; goods and services move between buyer and seller. Parties communicate payment orders to their banks, and the banks actually move the money through the central bank that issued the currency involved. Therefore, almost all systems that result in money movement rely on payment orders, which can easily be made electronic.

Topics: money and its properties. Fiduciary v. scriptural money. Token v. notational money. Cash and "real money." World banking system, the role of central and commercial banks. Mechanisms of money transfer: giro, cheques, electronic funds transfer. How foreign exchange works.

Readings : Sherif Ch. 1, Sherif Ch. 2.1 - 2.4, Article by Camp, Sirbu and Tygar, Token and Notational Money in Electronic Commerce, World Payments Report 2010 (very useful for statistics)

Lecture 2 - **AUTOMATED CLEARING AND SETTLEMENT SYSTEMS** (Sunday, February 23, 2014. 9:30 a.m.) - About 100 billion payments are made in the world each day, amounting to more than 50 TRILLION (HK) dollars per day. Handling this volume requires banks to use sophisticated and rapid methods for transmitting and processing payment orders. "Clearing" means determining the net effect of multiple payment orders so that each one need not result in an individual payment. "Settlement" means depositing funds in a bank account so money can be used. The world's payment volume requires automated systems for clearing and settlement, as well as systems for communicating payment orders reliably, of which SWIFT is the leader.

Topics: Real-time gross settlement; net settlement. The automated clearing house, ATM networks. The Hong Kong and U.S. banking systems. Fedwire, CHIPS and SWIFT.

Readings : Sherif Ch. 2.8, Sherif Ch. 12, Payment Systems in Hong Kong, Hong Kong Financial Infrastructure, The Inefficiencies of Cross-Border Payments (VISA)
Optional reading (long): Presentment Models and Payment Options (NACHA)

Lecture 3 - **EPAYMENT SECURITY AND DIGITAL SIGNATURES** (Sunday, February 23, 2014, 2:00 p.m.) - Payment orders are useless if they cannot be communicated securely and privately. In particular, a financial institution must be sure that it is receiving a legitimate, authorized order, than no eavesdropper is able to see it, that the identity of the sender can be determined, and that the order has not been altered in transit. We examine

a collection of security mechanisms that achieve these goals and their specific use in electronic payment systems. A critical objective of this lecture is an explanation of exactly how public-key cryptography works since it is an important technological basis of online banking and electronic commerce in general. We are also obliged to review traditional symmetric encryption because public-key cryptography relies on it.

Cryptographic methods, hash functions, trapdoor functions, DES and AES (Rijndael). Public-key methods: RSA, Diffie-Hellman key exchange, El Gamal encryption. Digital signatures.

Readings : Sherif Ch. 3.1 - 3.6, 3.15, 3.18, 3.25, 3.26.
Optional reading: Understanding Cryptography -- Hash Functions (Paar & Pelzl), Understanding Cryptography -- DES (Paar & Pelzl), Understanding Cryptography -- Digital Signatures (Paar & Pelzl)

Lecture 4 - **CREDIT CARD PROTOCOLS** (Tuesday, February 25, 2014, 6:45 p.m.) - The purpose of a digital certificate is very simple: to associate a public key with a particular individual or organization. Digital certificates address a fundamental problem in electronic commerce, that of authenticating the identity of a remote party (someone not physically present and who therefore cannot be asked to sign his name or show an ID card). If the individual knows the private key corresponding to that public key, then it is often a good inference that he is who he says he is. Digital certificates an essential adjunct to digital signatures. Unfortunately, the implementation and administration associated with digital certificates is not simple, but must be managed carefully and involves a good deal more structure (e.g. certification chains and revocation lists) than may be obvious. It is also important to know when digital certificates are not a good solution to the authentication problem. Most consumer ecommerce uses credit cards as a payment mechanism. Having any merchant in the world be able to obtain a credit authorization from a credit-issuing bank in a few seconds requires a vast international communications network and interoperating protocols. This lecture deals with various aspects of credit-card processing, including SSL/TLS, the primary method used for secure Internet ordering.

Topics: Digital certificates, certification chains. The public-key infrastructure. Digital identity documents and remote authentication. The SSL/TLS Protocol, cipher suites, credit card networks, Secure Electronic Transactions (SET), Visa 3D-Secure.

Readings : Sherif Ch. 5 (omit appendix), Sherif Ch. 7.1, 7.2, Sherif Ch. 8.3, Digital Signatures, Certificates and Electronic Commerce (Gladman et al.)
Optional reading: Introduction to SSL, Everything You Always Wanted to Know About CC's (Joe Ziegler)..

Lecture 5 - **SMART AND STORED-VALUE CARDS, OCTOPUS** (Friday, February 28, 2014, 6:45 p.m.) - Numerous payment methods involve the use of wallet-sized cards that incorporate a processor (smart-cards). Some of these, like Octopus, also contain a representation of monetary value that decreases as the card is used. Clearly a good deal of security is required in such cards; otherwise, cardholders could essentially manufacture arbitrary amounts of money. We will look at the structure and applications of smart cards, specifically how they are used in making payments. An important objective is to explain how Octopus really works and how all the Octopus-accepting vendors receive payment for the goods and services they render.

Topics: Smart card architecture and security, RFID cards, PIN verification. Visa Smart Debit and Credit. Gift card technology and the expanding gift card market. Octopus.

Readings : Sherif Ch. 13, Security Analysis of the Octopus System.

Lecture 6 - **MICROPAYMENTS** (Sunday, March 2, 2014, 2:00 p.m.) - The objective of micropayment systems is to replace cash, which is expensive to make, transport and protect. There are different micropayment value ranges: large micropayments are typically in an amount similar to consumer cash payments. Small micropayments may have value below the smallest unit of a country's currency, and can be used, for example, to pay for online information. The cost of a credit card transaction may exceed the total value of a micropayment. Therefore, we cannot use credit card systems to process them. But if a micropayment is to be cheaper to process, then some aspect of credit card processing must be given up, typically security. The emphasis in micropayment systems is on very low processing cost, which requires system having a very different architectures than the ones previously discussed. The ultimate in inexpensive micropayment are statistical systems, in which only a small fraction of payments are actually processed. There is no analog of such a method in traditional banking, and students often find it hard to imagine, although we will see that the underlying concept is quite

simple.

Topics: Characteristics of micropayment systems: brokers, scrip systems such as Payword and MicroMint. Statistical micropayment schemes: Peppercoin, MR1 and MR2.

Readings : Sherif Ch.10.5, 10,6, Comparing and contrasting micropayment models for E-commerce systems, Micropayments Revisited (Rivest & Micali).

Lecture 7 - **MOBILE PAYMENTS, DIGITAL WALLETS** (Tuesday, March 4, 2014, 6:45 p.m.) - Because of the world uptake of smartphones, mobile payment is the hottest current topic in electronic banking. Fundamentally, there is no real difference between mobile payments and card-based payment -- they both involve authentication and communication of payment orders. However, because a telephone connection is present in a mobile payment, various additional services and functions can be performed that are not available in card systems.

Topics: Wireless payments, digital wallets, the Google wallet. Obopay.

Readings: Guidobaldi, Mobile Proximity Payment, Mobile Payments in Asia Pacific (KPMG), Security of Proximity Mobile Payments (Smart Card Alliance).
Optional reading: Mobile Contactless Technology Backgrounder (DeviceFidelity)

Lecture 8 - **PAYPAL, BANKING IN MAINLAND CHINA** (Friday, March 7, 2014, 6:45 p.m.) - This lecture has two distinct components: (1) PayPal, a peer-to-peer payment system; and (2) payments in mainland China. Peer-to-peer payments are those that do not involve a bank and therefore do not require use of a country's banking system. Without bank accounts, how can money actually be transferred? PayPal is the premier example of a peer-to-peer system, and we will look at it in detail. After dealing with peer-to-peer systems, we will examine electronic payments in mainland China, which are increasing at a very rapid rate, especially with the rollout of China's "Super Online Bank" in 2010. China has more bank branches than any country in the world except India. It requires a huge infrastructure to move money efficiently in such a large banking system.

Topics: Peer-to-peer payments: PayPal. The Mainland banking structure. China National Advanced Payment System (CNAPS), China Domestic Foreign Currency Payment System (CDFCPS).

Readings : Payment Systems of China, Payment Systems in China (in English and Chinese)
Optional reading: China's Payment Systems (Peoples Bank of China -- VERY LONG, 20MB FILE)

Lecture 9 - **ELECTRONIC CASH, VIRTUAL MONEY SYSTEMS** (Sunday, March 9, 2014, 9:30 a.m) - One of the early promises of electronic commerce was the possibility of purely electronic currency, basically the communication of money by sending bitstrings which themselves have value, as opposed to sending payment orders which by themselves have no value. In fact, electronic cash is feasible, but presents a number of problems which have not been effectively solved. In particular, because a copy of string is identical to the original, it is possible for a person to spend the same string more than once, and this must be prevented. The popularity of social networks has given rise to virtual money systems, which are a practical alternative to electronic cash, at least for small-value payments, and exist outside the world's banking systems. These include a variety of systems used in social gaming, in which tokens are awarded that can be used for more play or that can be redeemed for goods.

Topics: Foundations of electronic cash: anonymity, untraceability, double-spending prevention, virtual currencies, Bitcoin.

Readings : Sherif Ch. 11, Tanaka, Possible Economic Consequences of Digital Cash, Bitcoin Primer (Koss & Koss), Introduction to BitCoin Mining (Sterry)
Optional reading: Bitcoin: A Peer-to-Peer Electronic Cash System (Nakamoto)

Lecture 10 - **ELECTRONIC INVOICE PRESENTMENT AND PAYMENT** (Sunday, March 9, 2014, 2:00 p.m.) - Commercial payments are almost always made in response to a bill or invoice. Accounting controls require levels of approval and documentation of all payments in order to prevent fraud and abuse. The preparation, sending, receipt and handling of invoices is very expensive, but can be made cheaper by removing paper from the process

and rendering invoices electronically. This gives rise to Electronic Invoice Presentment and Payment (EIPP), sometimes called Electronic Bill Presentment and Payment (EBPP) or Electronic Statement Delivery (ESD). These are sophisticated systems that involve the use of various service providers and intermediaries to deliver invoices and process payments. A future objective is to eliminate invoices entirely because they are costly and result in payment delays. An example of an invoice-free system is Scan-Based Trading (SBT), which is now being utilized by large retailers.

Topics: Electronic statement delivery, EIPP providers: biller service providers, customer service providers. Thick vs. thin consolidation. Reconciliation. Bill data mining. B2B integration. Invoice elimination: scan-based trading (SBT).

Readings : Electronic Bill Presentment and Payment (FISERVE), Business-to-Business EIPP (NACHA), EBPP Business Practices