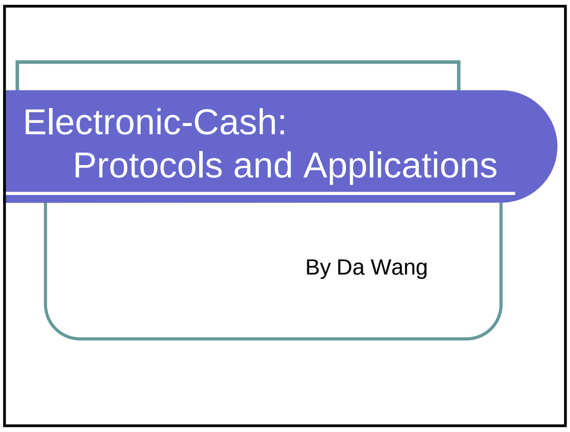
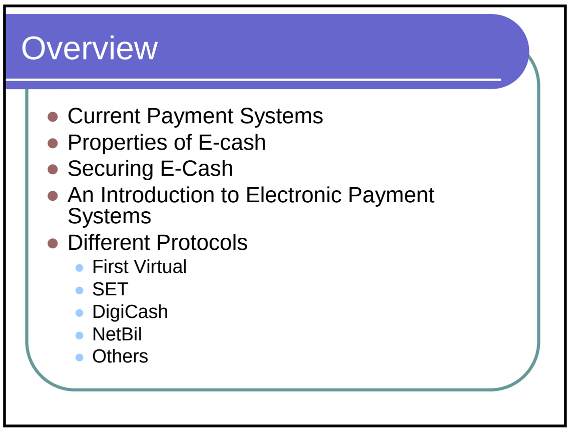


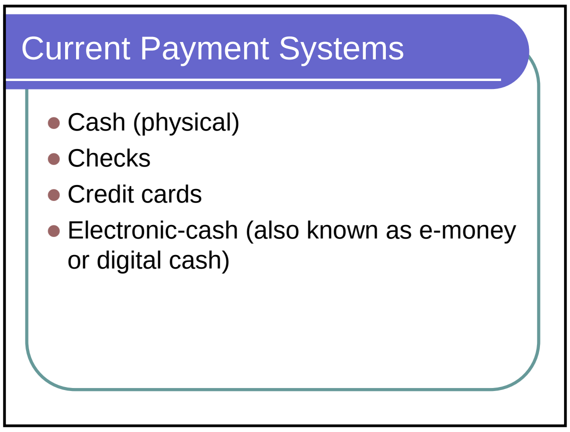
Electronic-Cash: Protocols and Applications

By Da Wang



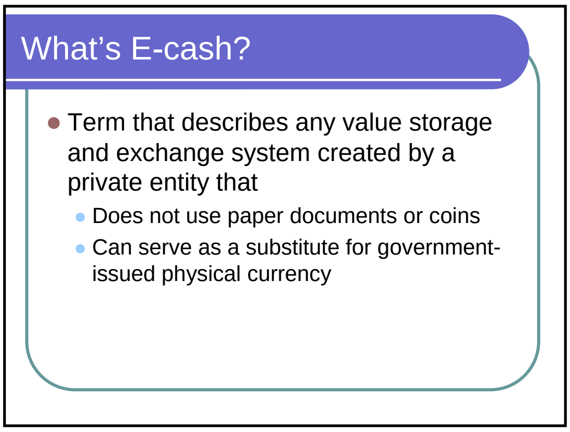
Overview

- Current Payment Systems
- Properties of E-cash
- Securing E-Cash
- An Introduction to Electronic Payment Systems
- Different Protocols
  - First Virtual
  - SET
  - DigiCash
  - NetBil
  - Others



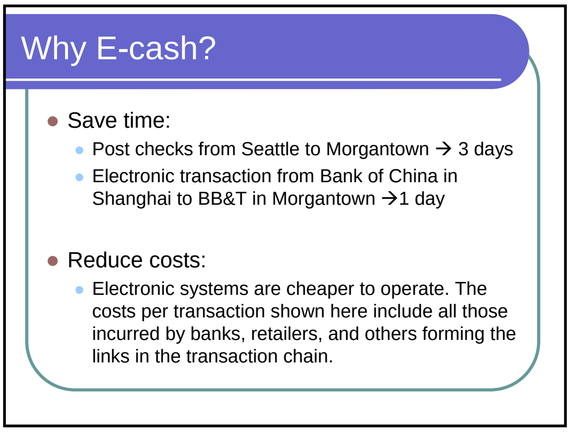
Current Payment Systems

- Cash (physical)
- Checks
- Credit cards
- Electronic-cash (also known as e-money or digital cash)



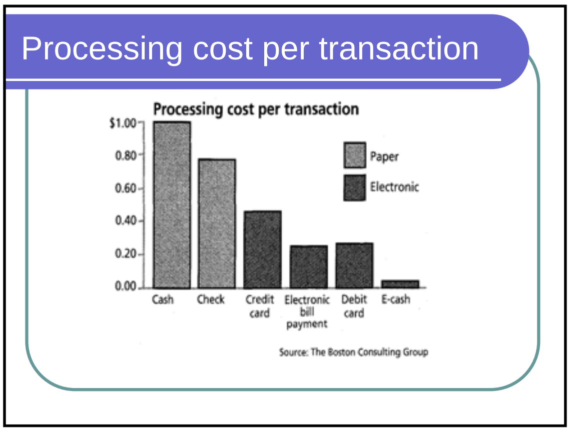
What's E-cash?

- Term that describes any value storage and exchange system created by a private entity that
  - Does not use paper documents or coins
  - Can serve as a substitute for government-issued physical currency



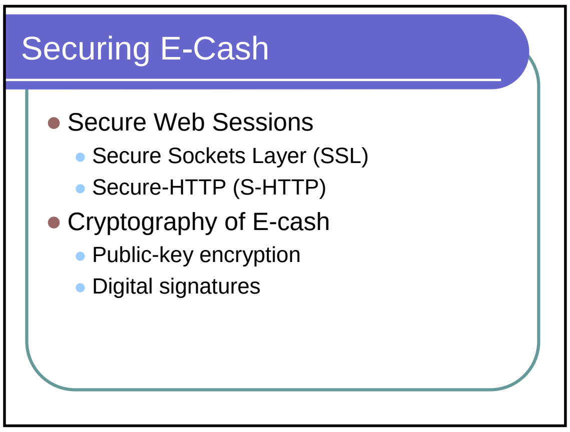
Why E-cash?

- Save time:
  - Post checks from Seattle to Morgantown → 3 days
  - Electronic transaction from Bank of China in Shanghai to BB&T in Morgantown →1 day
- Reduce costs:
  - Electronic systems are cheaper to operate. The costs per transaction shown here include all those incurred by banks, retailers, and others forming the links in the transaction chain.



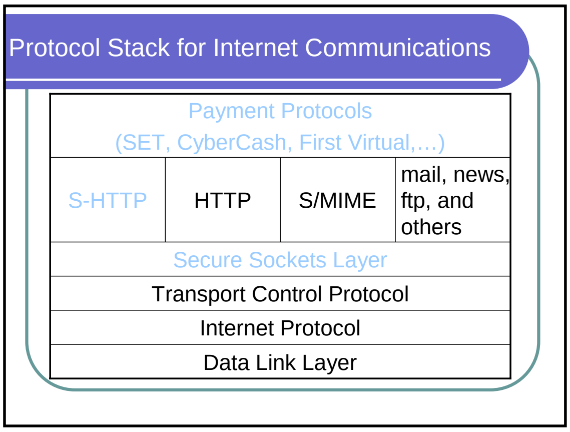
Processing cost per transaction

Source: The Boston Consulting Group



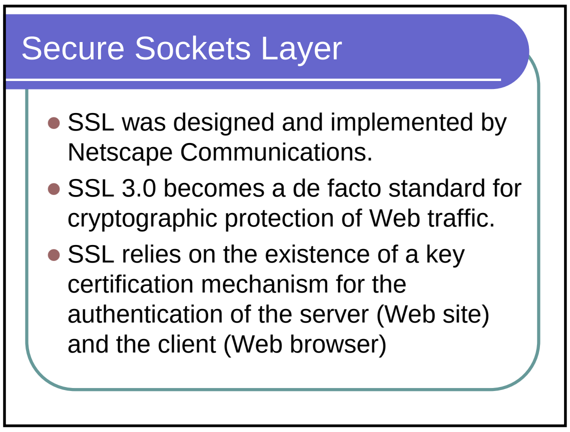
Securing E-Cash

- Secure Web Sessions
  - Secure Sockets Layer (SSL)
  - Secure-HTTP (S-HTTP)
- Cryptography of E-cash
  - Public-key encryption
  - Digital signatures



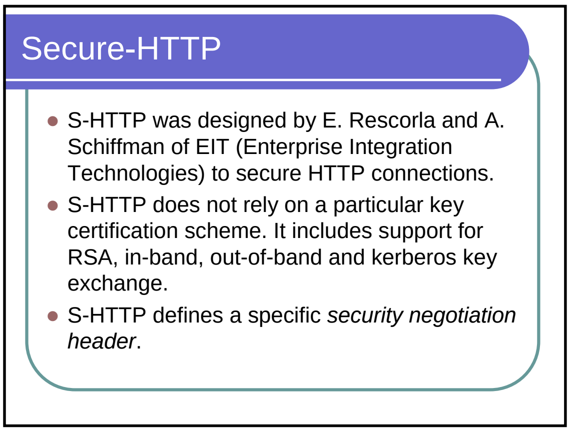
Protocol Stack for Internet Communications

Payment Protocols (SET, CyberCash, First Virtual,…)			
S-HTTP	HTTP	S/MIME	mail, news, ftp, and others
Secure Sockets Layer			
Transport Control Protocol			
Internet Protocol			
Data Link Layer			



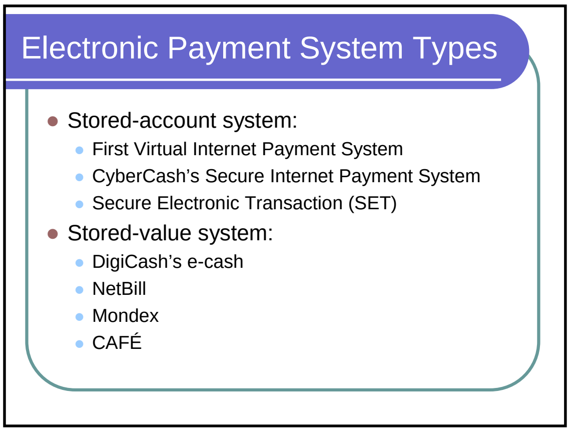
Secure Sockets Layer

- SSL was designed and implemented by Netscape Communications.
- SSL 3.0 becomes a de facto standard for cryptographic protection of Web traffic.
- SSL relies on the existence of a key certification mechanism for the authentication of the server (Web site) and the client (Web browser)



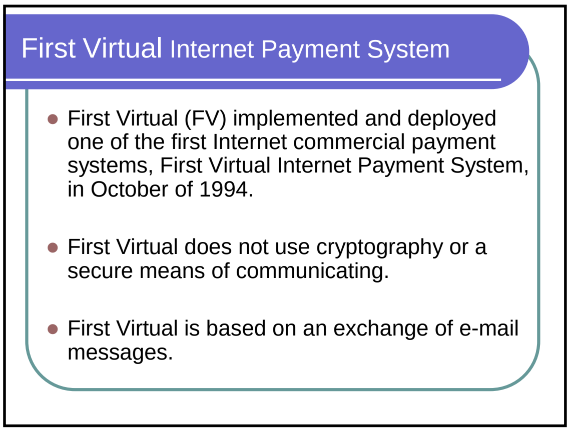
Secure-HTTP

- S-HTTP was designed by E. Rescorla and A. Schiffman of EIT (Enterprise Integration Technologies) to secure HTTP connections.
- S-HTTP does not rely on a particular key certification scheme. It includes support for RSA, in-band, out-of-band and kerberos key exchange.
- S-HTTP defines a specific *security negotiation header*.



Electronic Payment System Types

- Stored-account system:
  - First Virtual Internet Payment System
  - CyberCash's Secure Internet Payment System
  - Secure Electronic Transaction (SET)
- Stored-value system:
  - DigiCash's e-cash
  - NetBill
  - Mondex
  - CAFÉ



First Virtual Internet Payment System

- First Virtual (FV) implemented and deployed one of the first Internet commercial payment systems, First Virtual Internet Payment System, in October of 1994.
- First Virtual does not use cryptography or a secure means of communicating.
- First Virtual is based on an exchange of e-mail messages.

Transaction Steps of First Virtual 1

- First Virtual (FV) serves as a broker to credit card transactions between consumers and merchants.
  - 1.Consumer establishes an account with FV, and the account is secured with a credit card.
  - 2.Consumer is assigned a VirtualPIN.
  - 3.Consumer applies an order by e-mailing a participating FV merchant.
  - 4.The merchant requests the consumer's VirtualPIN and checks whether it is valid.
  - 5.The merchant initiates a payment transaction by sending e-mail to FV.
  - 6.FV contact the purchaser by e-mail to confirm the purchase.

Transaction Steps of First Virtual 2

- 7.Consumer confirms sale by sending a YES response back to FV.
- 8.FV sends a transaction result message to the merchant, indicating whether the buyer accepted the charges.
- 9.After a waiting period (91 days after buyer's credit card has been charged) , the amount of the sale minus transaction fees are directly deposited into the merchant's account.
  - Merchant assumes all risk!

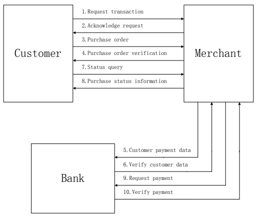
Pros and Cons

- Advantages:
  - The protocol is simple.
  - Neither buyer nor seller needs to install any software in order to use the system.
  - First Virtual has very low processing fees compared to other Internet payment schemes or even straight credit card processing.
- Disadvantages:
  - Merchant assumes all risk!
  - The content of the Web Session or e-mail may be captured and interpreted by network sniffers.

Secure Electronic Transaction

- Secure Electronic Transaction (SET) is an emerging *standard* for secure credit card payments over the Internet.

SET Transaction Steps



Source: LJ. Camp, “Privacy & Reliability in Internet Commerce”, PhD thesis, Carnegie Mellon University, 1996

DigiCash’s E-Cash

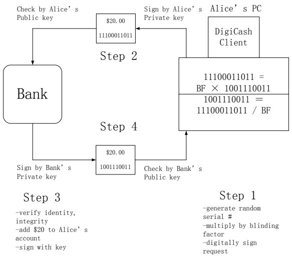
- Digital Payment System E-Cash (DigiCash for short) was invented by David Chaum in 1993.
- DigiCash is a stored-value cryptographic coin system that facilitates Internet-based commerce using software that runs on personal computers.
- The value of DigiCash is represented by cryptographic tokens that can be withdrawn from bank accounts, deposited in bank accounts, or transferred to another people.

Unique Property

- DigiCash is unique in its implementation of electronic cash because it has attempted to preserve the anonymity and un-traceability associated with cash transactions
  - DigiCash uses “Blind Signatures” for untraceable payments.

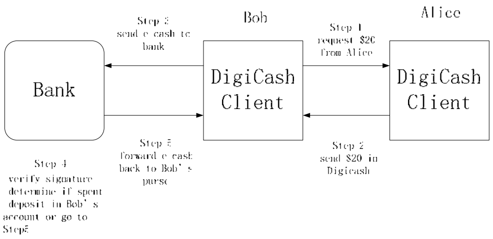
DigiCash Payment Protocol 1

- The DigiCash payment protocol and blinding can be illustrated by pictures:


Check by Alice’ s Public key
$20.00
11100011011
Sign by Alice’ s Private key
Alice’ s PC
DigiCash Client
Step 2
Bank
11100011011 = BF × 1001110011
1001110011 = 11100011011 / BF
Step 4
$20.00
1001110011
Sign by Bank’ s Private key
Check by Bank’ s Public key
Step 3
-verify identity, integrity
-add $20 to Alice’ s account
-sign with key
Step 1
-generate random serial #
-multiply by blinding factor
-digitally sign request

DigiCash e-cash withdrawal

DigiCash Payment Protocol 2



Spending e-cash

Pros and Cons

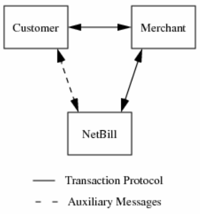
- Advantages:
  - It allows realization of untraceable payments system which offers increased personal privacy.
- Disadvantages:
  - Traceability of transactions may be lowered, resulting in a higher potential for undetected fraud.

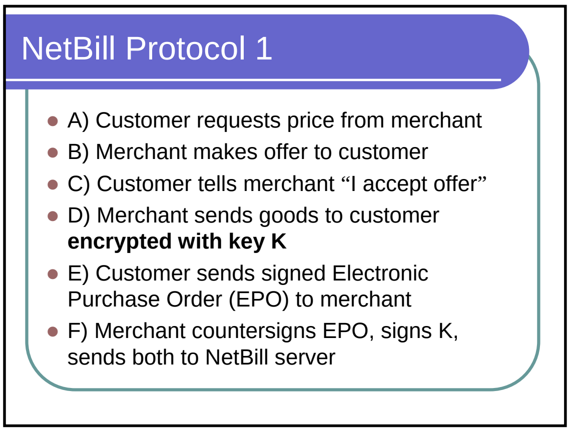
NetBill

- NetBill is a system for micropayments for information goods on the internet, which is developed by J.D. Tygar, Benjamin Cox, and Marvin Sirbu of Carnegie Mellon University.
- Micropayment system: NetBill acts as an aggregator to combine many small transactions into larger conventional transactions, amortizing conventional overhead fees.

Transaction Model

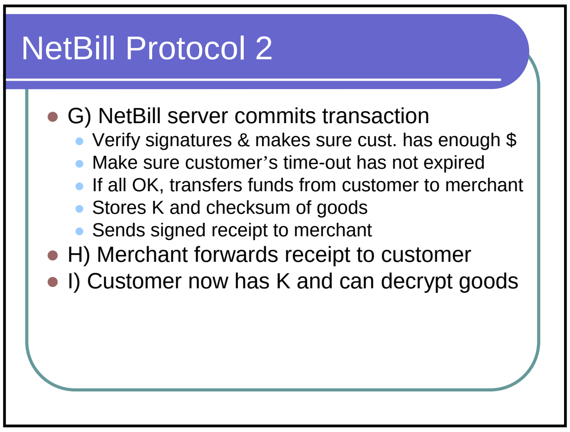
- Parties participating in a NetBill Transaction:
  - Customer
  - Merchant
  - NetBill
- NetBill account can be replenished from a bank or credit card.





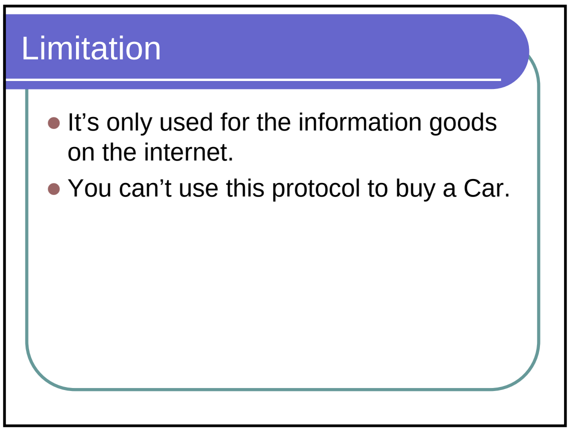
NetBill Protocol 1

- A) Customer requests price from merchant
- B) Merchant makes offer to customer
- C) Customer tells merchant “I accept offer”
- D) Merchant sends goods to customer **encrypted with key K**
- E) Customer sends signed Electronic Purchase Order (EPO) to merchant
- F) Merchant countersigns EPO, signs K, sends both to NetBill server



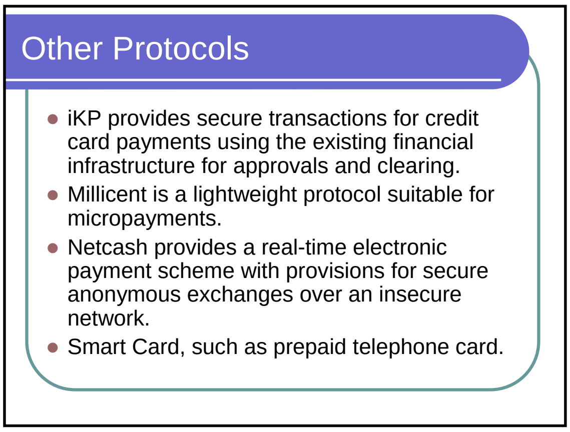
NetBill Protocol 2

- G) NetBill server commits transaction
  - Verify signatures & makes sure cust. has enough $
  - Make sure customer’s time-out has not expired
  - If all OK, transfers funds from customer to merchant
  - Stores K and checksum of goods
  - Sends signed receipt to merchant
- H) Merchant forwards receipt to customer
- I) Customer now has K and can decrypt goods



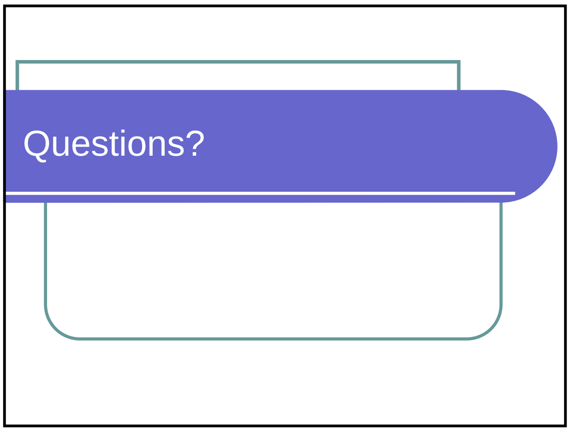
Limitation

- It’s only used for the information goods on the internet.
- You can’t use this protocol to buy a Car.



Other Protocols

- iKP provides secure transactions for credit card payments using the existing financial infrastructure for approvals and clearing.
- Millicent is a lightweight protocol suitable for micropayments.
- Netcash provides a real-time electronic payment scheme with provisions for secure anonymous exchanges over an insecure network.
- Smart Card, such as prepaid telephone card.



Questions?