
E-Commerce, Electronic Security, and Requirements

23 February 2011
Lecture 1

Course Topic: Security!

- Threats and Security Requirements
- Foundations of Modern Cryptography
- Encryption and Randomness
- Hash Functions
- Authentication
- Public/Private Key Pairs
- Shared Secrets
- Decentralized Cryptography
- Key Management
- Certificates
- Network Security
- Internet Security
- Trust Management
- Electronic Banking
- Secure Payments
- Credit Card Transactions
- Telephone and Cellular Payments
- Micropayments
- Money Transfers
- Privacy Protection
- Digital Cash
- Content Protection
- Trusted Third Party Services: Digital Safes, Notaries, Agents

Course Topic: Security!

- What you won't learn:
 - How to hack into a misconfigured Apache web server
 - How to write viruses
 - Why Windows and Outlook have so many bugs
 - How to properly write a routing table for a firewall
- Our goal is to gain an understanding of the tools and techniques of modern digital communication security

Books for the course

- Listed on the syllabus
 - Ross Anderson. *Security Engineering: A Guide for Building Dependable Systems*. Wiley, 2nd edition, 2008.
 - Warwick Ford and Michael S. Baum. *Secure Electronic Commerce*. Prentice-Hall, 2nd edition, 2001.
 - Matt Bishop. *Computer Security: Art and Science*. Addison-Wesley. 2003.
 - Alfred J. Menzes, Paul C. van Oorschot, and Scott A. Vanstone. *Handbook of Applied Cryptography*. CRC Press, 1996.
- Anderson and Menzes, et al. are available for free online (legally)

And now we begin...

Topics for today

- Introduction
- What is E-Commerce?
 - Versus paper based commerce
- Source: Ford and Baum 1, Anderson 1

Introduction

- E-Commerce and Internet Security
 - Closely related
 - Why?

Security for E-Commerce means:

- Ensuring software we use doesn't have **flaws**
- Making sure the protocols we use for communication keep things **secret**
- Keeping **hackers and active attackers** out of our systems
- Keeping **passive attackers** from discovering business or trade secrets
- Keeping **accurate** business records or electronic transactions
- Producing **enforceable** contracts and agreements electronically
- Enabling electronic commerce transactions to be treated with the **same level of trust** associated with paper transactions

E-* vs. Traditional

Traditional business practices and commerce are **well understood**

- They are centuries old

E-Commerce is **much newer**

- Wide deployment didn't come until the 1970s and 1980s

E-* vs. Traditional

We can divide the business goals of E-Commerce security into two types:

- Efforts to give electronic commerce transactions the **same force** as their paper or traditional equivalents
- Efforts to give electronic commerce a **stronger** level of security than their paper or traditional equivalents
 - Usually because the threats are (or seem) stronger against electronic methods

E-* = Traditional

Example: Joining a club

Traditional – Sign a contract

- Member agrees to **payment** for a given time period
- Club defines the **benefits** for a given period of time
- Club maintains the **paper record** and records payment
- Member gets a **membership card** to prove his rights to the benefits

Electronic methods – What do we do?

- What is the **contract** that the club provides the person?
- How does the person **sign** on the contract?
- How does the club **receive payment**?
- How does the club issue the **membership card** to the person?

E-* = Traditional - Repudiation

Important question: What happens if the member or club later deny that the transaction took place?

Stand before a judge/arbiter and:

Traditional

- Produce the contract and signatures
- Produce payment stubs
- Produce membership card

Electronic methods

- Can we verify the contract? (What is the contract?)
- Can we verify the identity of the member?
- Can the member prove anything with his e-membership card?

E-* > Traditional

Example: Club Monthly Bill

Traditional:

- Send a **statement** to each member at the end of the month
- Details member's **transactions** and account balance

Weaknesses:

- What stops an attacker from **intercepting** the statement?
- An attacker can intercept it, **read it**, and send it along
- An attacker could **destroy** it
- An attacker could open the statement, **modify** it, and send the false one to the member (Tamper proof? Tamper evident?)
- The attacker could create a **false** statement and send it to the member

E-* > Traditional

Example: Club Monthly Bill

Electronic Methods:

- Create a protocol to overcome those vulnerabilities
- Perhaps use cryptography, secure communication, digital signatures

-
- Why don't we worry about them in traditional methods?
 - Culture
 - Laws
 - Probability of attack (Who would choose me?)
 - Ease of attack
 - With electronic methods, the dangers are (or seem) much worse
 - Automated attacks!

Example: Passports

What is a passport?

- A physical document with a picture and printed information
- It is stamped on entry (and sometimes on exit)

Repudiation?

- Show the physical document

Attacks?

- Tear out pages, Forge stamps, Forge the document

What about an electronic passport?

- How do you verify it?
- How do you stamp it?
- How would you resolve repudiation?



Our goals - again

- Better understand what tools we can use
- Better understand how they work (and don't work) together
- Learn about recent advances in security techniques
 - Also learn about historical ones for some perspective

So far

- Introduction
- What is E-Commerce?
 - Versus paper based commerce
- What is computer security?
 - Definitions

What is E-Commerce?

- Any transaction where at least one of the steps is conducted using an electronic or digital mechanism
- Why does it matter?
 - New modes of business interactions
 - Ease of communications
 - Lowering global barriers

E-Commerce Upsides

- Productivity advances
 - Communicate faster
 - Work faster and more easily
- Expanded and better-focused markets
 - Regional, National, International reach
- Cost reduction
 - Less paper, storage, management of physical documents
- Quality Gains
- Improve Customer Appeal
 - If 1% of people would buy your product – you can reach 1% of a whole country online
- Improved employee satisfaction
 - Less busy work and paperwork, more interesting stuff
- New partnerships based on better information sharing
 - Know your potential partners better
- New business opportunities
 - Online business is worth billions

E-Commerce Downsides

- Direct financial loss resulting from fraud (הונָאָה)
 - How much fraud?
- Exposure of intellectual property (קְנִיין רוֹחֵינִי)
- Damage to relations with customers or business partners
- Unforeseen costs

E-Commerce vs Paper Commerce

Security is not new

- People have been lying, cheating, and stealing for a long time

The applications and forms are new

There have been attempts at defining correspondences between electronic transactions and paper ones

- Most have failed

E-Commerce vs Paper Commerce

- Paper has some inherent security features
 - Ink embeds in paper fibers in a known manner
 - Signatures are understood and detectibly unique and can be personalized based on how the person's hand writes
 - Printing on paper has known effects and properties
 - Time stamps can be stamped on a document
 - Copying, modification, and deleting from documents is obvious
- Electronic means have known weaknesses:
 - Everything breaks down into bit which in turn are differentials in electrical voltage across some magnetic medium
 - There is nothing inherent in a 1 or 0 which tells you what it means
 - The bits can be copied around easily and normally undetected
 - They can be modified, read, copied, and understood by most anyone

E-Commerce vs Paper Commerce

- Negotiable (סְחָיָר) documents are especially difficult
- Think about cash
 - We know what a 20 shekel bill looks like
 - If I give it to you – it's an obvious, irrevocable act
 - What about an electronic 20 shekel bill?
 - If I send it to you by email – what's to stop me from keeping a copy and using it?
- We must find new concepts and safeguards to make e-commerce documents and actions secure and *understandable*
 - Otherwise we will get nowhere

Questions for thought

- Why are there no digital passports?
 - Why do I need to show a paper Israeli passport when I want to reenter Israel at נתבג?
- Why do I need to carry a רשיון נהיגה?
 - When a police officer stops me, why does he ask to see one?
 - Why does he ask to see the car's registration?
- Why don't we use finger prints for signatures and contracts?
- Why will your stock broker not take buy or sell order by email?
 - Although he will take them by telephone or by written letter.

Conclusion

- Introduction
- What is E-Commerce?
 - Versus paper based commerce
- What is computer security?
 - Definitions