

# Course ISE 328: Communication and E-Commerce Security

## Recitation 1 Exercise

Michael J. May

March 2, 2010

### 1 Review of Concepts

There were some important terms and concepts introduced today in class, let's review their definitions (many of these come from the dictionary):

1. Active Attacker

- A person or entity which attempts to take positive actions to interfere with a system, steal or modify its data, or otherwise disturb the system

2. Passive Attacker

- A person or entity which attempts to listen to the communications in a system without modifying them

3. Contract

- An agreement between two or more parties for the doing or not doing of something specified.

4. Repudiation

- to disavow or reject an obligation (as a debt) or duty (as performance under a contract)
- to reject with denial

5. Non-repudiation

- The prevention of the ability to repudiate

6. Negotiable

- transferable by delivery, with or without endorsement, according to the circumstances, the title passing to the transferee.

7. Authentication

- to prove or serve to prove that (something) is genuine; especially : to prove that (an item of evidence) is genuine for the purpose of establishing admissibility

8. Integrity

- a sound, unimpaired, or perfect condition

## 9. Fault Tolerance

- The ability of a system or component to continue normal operation despite the presence of hardware or software faults. This often involves some degree of redundancy.
- The number of faults a system or component can withstand before normal operation is impaired.

## 10. Covertness

- The quality of being undetectable or secret

# 2 Traditional versus Electronic

Let's consider some examples of communication and contract properties and how they can be supported in traditional and electronic situations

## 2.1 Scenario 1: Starting a Mortgage with a Bank

You want to buy a house with the help of a mortgage from a bank. The mortgage will be large (say 1,000,000 Shekels). The house will then have a lien from the bank until you pay off the mortgage.

Your obligations:

- Pay the bank a monthly amount to repay the loan amount
- In case you stop paying the mortgage, give the house to the bank.

The bank's obligations:

- Provide the 1,000,000 shekels loan
- Accept payments and credit your account when they are received

Requirements:

- Integrity:
  - The amount of the loan can't be changed
  - The house can be uniquely identified and can't be changed
  - The borrower can be uniquely identified and can't be changed
  - The bank can be uniquely identified and can't be changed
  - The payment dates and amounts can't be changed
- Non-Repudiation:
  - The borrower shouldn't be able to deny that he borrowed the money
  - The bank shouldn't be able to deny that they lent the money (why)?
  - The bank shouldn't be able to deny the terms of the loan (amount, payment schedule).

### 2.1.1 Accomplishing These Goals: Traditional

A traditional method of accomplishing the above requirements is:

- The bank and borrower write a contract specifying the terms of the mortgage
- The house is identified using some
- The borrowed signs the contract
- The bank manager or banker signs the contract
- The bank gives a photocopy of the signed contract to the borrower

## Attacks on this arrangement

1. The bank later claims that the terms of the contract were different:

- The mortgage was actually for 2,000,000 shekels
- The mortgage was for a different house owned by the borrower
- The mortgage was to be paid off in 10 years, not 25 years
- The payments were to be sent to account X, not account Y

Solutions:

- The bank must provide the judge a copy of the contract with the signature of the borrower on it. Assuming the signature can't be forged or transferred, the bank will not be able to do so
- The borrower provides his copy of the contract with the terms as he claims to the judge. The signatures from the bank manager will be used to authenticate his version.

2. The borrower later claims that the terms of the contract were different (similar to above)

Solution:

- The borrower must provide his copy of the contract (which will have the unchanged terms) to the judge
- The bank provides its copy of the contract to the judge

3. The borrower denies the mortgage ever occurred.

Solution:

- The bank must provide the judge a copy of the contract with the signature of the borrower on it and evidence to *authenticate* the signature

4. The bank (falsely) attributes the mortgage to someone else

Solution:

- The bank must provide the judge a copy of the contract with the signature of the borrower on it and evidence to *authenticate* the signature

5. The borrower breaks into the bank and steals their copy of the mortgage contract. He then denies that the mortgage took place.

Solution: Backups and copies of the bank's contract

6. The bank breaks into the borrower's house, steals his copy of the contract, and then claims the terms were different.

Solution:

- The bank must provide the judge a copy of the contract with the signature of the borrower on it. Assuming the signature can't be forged or transferred, the bank will not be able to do so

7. The bank forges a borrower's signature on a mortgage contract and claims that he owes the amount in the contract.

Solution:

- The bank must provide the judge with a copy of the contract with the signature on it and authenticate it.

### **2.1.2 Accomplishing These Goals: Electronic**

How can we get a similar level of security using purely electronic means?

What do we need?

- A digital signature mechanism
- A way of attributing a digital signature to a person
- A way to prevent modification of a signed digital object
- A way to prove that a digital stream represents a string of characters and numbers