Carnegie Mellon University

STUDY OF THE INTERDEPENDENCIES WITHIN THE BANKING AND FINANCE INFRASTRUCTURE FOR SURVIVABILITY RESEARCH

A Thesis Submitted to the Information Networking Institute
in Partial Fulfillment of the Requirements

for the degree

MASTER OF SCIENCE
in
INFORMATION NETWORKING

by
Yen-Ming Chen

Pittsburgh, Pennsylvania

December, 1999

Carnegie Mellon University
Information Networking Institute

THESIS

SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF
Master of Science in Information Networking

Title Study of the Interdependencies within the Banking and Finance Infrastructure for Survivability Research

Presented by Yen-Ming Chen

Accepted by the Information Networking Institute.

Thesis Advisor	____________________ David Fisher	Date	______
Thesis Advisor	____________________ Howard Lipson	Date	______
INI Dept Chairman	____________________ Richard Stern	Date	______

Part I

Preliminaries

Contents

I Preliminaries i

1 Banking and Finance Infrastructure 1
- 1.1 Survivability 2
- 1.2 Target 2
  - 1.2.1 Federal Reserve 2
  - 1.2.2 Payment Systems 3

2 Analysis Methods 4
- 2.1 Formal Method 4
- 2.2 StarLogo 5
- 2.3 Markov Chain 5
- 2.4 EASEL 6
  - 2.4.1 Emergent Algorithms 6
  - 2.4.2 Language 7
  - 2.4.3 The simulator 7
- 2.5 Methodology for this paper 7
- 2.6 Rest of this paper 7

II Payment Systems 9

3 Cash Payment System 10
- 3.1 Introduction 11
- 3.2 Flow 11
  - 3.2.1 Bank to the Fed 12
  - 3.2.2 Fed to BEP 12
- 3.3 Statistics 12
- 3.4 Analysis 14
  - 3.4.1 Public 14
  - 3.4.2 Cash 16
  - 3.4.3 Banks 17
  - 3.4.4 Federal Reserve 18

3.4.5 BEP/Mint . . . 20
3.5 Scenarios . . . 21
3.5.1 Counterfeiting . . . 21
3.5.2 Money laundering . . . 21
3.6 Discussion . . . 21

4 Check Payment System **22**
4.1 Introduction . . . 23
4.2 Flow . . . 23
4.3 Statistics . . . 23
4.4 Analysis . . . 25
4.4.1 Actors . . . 25
4.4.2 The Public . . . 25
4.4.3 Collecting Bank . . . 25
4.4.4 Paying bank . . . 26
4.4.5 Correspondant Bank . . . 27
4.4.6 Federal Reserve . . . 28
4.4.7 Check . . . 28
4.5 Scenario . . . 29
4.5.1 Return items . . . 29
4.5.2 Check fraud . . . 29

5 Automated Clearing Houses **30**
5.1 Introduction . . . 31
5.2 Flow . . . 31
5.3 Statistics . . . 32
5.4 Analysis . . . 33
5.4.1 The Public . . . 33
5.4.2 Sending Bank . . . 33
5.4.3 ACH . . . 34
5.4.4 Federal Reserve . . . 35
5.5 Scenarios . . . 35
5.5.1 Credit Risk . . . 35

III Result **36**

6 Simulation **37**
6.1 Design . . . 38
6.1.1 Actors and Property . . . 38
6.1.2 Interdependencies . . . 43
6.2 Analysis . . . 44

6.2.1 Well-defined 44
6.2.2 Completeness 44
6.2.3 Correctness 44
6.3 Survivability requirements 45
6.3.1 Recognize 45
6.3.2 Resist 45
6.3.3 Recover 45
6.3.4 Evolve 46

7 Conclusion **47**
7.1 Conclusion 47
7.2 Future Work 48

List of Figures

3.1 Flow chart of Cash circulation 11

4.1 Flow chart of Check Process System 24

5.1 Flow chart of Automated Clearing House 31

6.1 Layers in the banking and finance infrastructure 39

List of Tables

3.1 Standard units for currency deposits 13
3.2 Standard units for coin deposits 13
3.3 Expectation mean time for bill circulation 13

4.1 1996 Interbank Check Collection Market[1] 24

5.1 Cap Multiple Matrix[2] 32

Abstract

The banking and finance infrastructure is one of the most critical infrastructures in the country. This infrastructure is crucial to the country in terms of economic development, confidence of residents, and the ability to support the growth of the nation. To preserve the public's confidence in this infrastructure, we need to examine its survivability. Survivability is the ability of a system to fulfill its mission, in a timely manner, in the presence of attacks, accidents, and failures. One approach to investigating the survivability of the banking and finance system is to design a simulation for the infrastructure. The simulation can help people to better understand the infrastructure by being able to run scenarios of simulated cyber-attacks against the infrastructure and to view the results.

We discussed several ways for analyzing survivability, including simulation tools. Then we introduce the tool we chose, EASEL (the Emergent Algorithms Simulation Environment and Language), and the concept of Emergent Algorithms. From the perspective of simulation, we study three payment systems in the infrastructure and present the result as the list of actors, neighbors, functions, and the algorithms which actors perform. Then we illustrate the interdependencies we found among the three payment systems.

After we understand the three payment systems, and illustrate the interdependencies among them, we discuss the relationships between the interdependencies and the survivability requirements for the infrastructure. We will also discuss some advantages and disadvantages about using EASEL to design the simulation and describe the payment systems.

Acknowledgment

I would like to thank my parents for sponsoring me to study in Carnegie Mellon University. And thanks to Prof. Jeannette Wing, who pointed me to Dr. Tom Longstaff in CERT, who introduced me to my advisors, Dr. David Fisher and Dr. Howard Lipson.

Also thanks to my thesis advisors, Dr. David Fisher and Dr. Howard Lipson for giving me advice on my thesis, and making the thesis work possible.

Finally thanks to all the INI people, Ben Bennington, Richard Stern, Susan Jones, Lisa Currin, and all the MS10 students.

Chapter 1

Banking and Finance Infrastructure

Contents

1.1 Survivability **2**

1.2 Target **2**

1.2.1 Federal Reserve 2

1.2.2 Payment Systems 3

The Banking and finance infrastructure is one of the most critical infrastructures in the United State. 'Critical' means that this infrastructure is important to the country in terms of economic development, confidence of residents and the ability to support the growth of the nation. The reason for examining the survivability of a critical infrastructure is to preserve the public's confidence in the nation's ability to provide essential services for everyone ([3]). Banking and finance is a basic infrastructure that all business, organizations, and individuals depend on. Because of the importance of the banking and finance infrastructure, we want to investigate the survivability of this infrastructure, which is exposed to cyber-attacks, accidents and failures to study how to protect this important infrastructure.

For such a purpose, we need to be able to simulate this infrastructure, and this simulation should be a good projection from the real infrastructure to the virtual computer world. In such a simulation, we should be able to study and possibly explore this infrastructure in detail, and do experiments in the simulation for the improvement of the infrastructure. Also we can examine a proposed monetary policy by deploying it first in the simulation model such that we can better understand what is the possible impact for some policy in the economy or structure of the infrastructure itself.

Simulating the banking and finance infrastructure is made more complicated because such a system lacks central control, individual participants have only a partial understanding of the whole system and the system is very dynamic with constantly changing and unpredictable participants. To build such a simulation, we first present the definition of survivability and some of its properties. We then describe three payment systems as the target for our study. Next we examine the currently available options we can use to: 1. analyze a system or an infrastructure, 2. study some subsystems in the infrastructure, 3. understand the interdependencies within the infrastructure. The reason for using our simulation approach will be illustrated later in this section.

1.1 Survivability

For every critical infrastructure, there is at least a mission for this infrastructure to fulfill. And there is the possibility for natural disasters ,intended attack ,failures or accidents taking place in the critical infrastructure. Together they make the definition of the term "Survivability"[4]:

The capability of a system to fulfill its mission, in a timely manner, in the presence of attacks, failures, or accidents.

For a system to be survivable, it has to have the following properties:

Resistance the system should be able to resist disaster, attack, or intrusion.

Recognition the system should be able to detect, and recognize whether there is a disaster or attack, also the extent of damage or compromise.

Recover the system should be able to recover from the harm caused by disaster, attack or intrusion.

Adaption and Evolution the system should be able to evolve from the accident caused by any disaster, attack or intrusion.

To compare the concept of survivability with the traditional security, we would say that survivability focus on different properties of a system than security. In security, it is protection oriented, which means that people trying to protect their information, machine or physical property through security. As survivability, it is mission oriented, which means that people are trying to get their job done in time no matter what happens to the system.

1.2 Target

1.2.1 Federal Reserve

We focus on building the simulation model for various payment system services which is provided or under supervision of the Federal Reserve. The Federal Reserve Banks are the central banks of the United States, they play an important role in the nation and also to the world economy. The missions of the Federal Reserve fall into the four categories[5]:

Monetary Policy The federal reserve has to maintain the stability of the nation's economic, therefore it has to conduct the monetary policy to achieve the goal.

Supervision The federal reserve has to supervise and regulate other banking institutions to protect consumers in the nation.

Financial Services The federal reserve provides several financial services to other banking institutions, such as these payment systems we are discussing in this paper.

Risk Management The federal reserve has to keep the nation's economic system stable. So it has to manage the risk in the financial market to maintain stability.

The most important service which the Federal Reserve provides to the people is the payment systems, because it is related to everyone's daily life. We will introduce the payment systems in section 1.2.2. Then we pick three systems inside the payment systems and study them. Among these three payment systems, Cash payment systems is the most detailed one we study into. Because that cash, or currency note, is the first way human being used to represent "value". Even for people who are trying to develop electronic cash, they still working so hard to preserve properties of cash to the electronic cash. The other payment systems like check, or ACH can be another form of cash.

1.2.2 Payment Systems

All the payment systems play an important role in our daily life. It is also the most important services provided by the federal reserve. Although there are more and more private financial service providers nowadays, but the federal reserve still owns large part of the market. Therefore building such simulation can help the manager understand some possible result caused by risk, realize how a policy or regulation could effect the system, or change the infrastructure to fit the survivability requirements.

The main reason we choose the payment systems is that such systems are critical for million of people and also used by people on a daily basis. And the role that played by the Federal Reserve Banks is particular important. That is because the Federal Reserve acts like a central banking and finance service provider for this country, which makes it the critical actor in the whole infrastructure.

We choose three payment system, and they are cash payment system, check payment system and automated clearing houses. These three system are the most widely used by people all over the country even the rest of the world too. With initial study on these systems, we can further expand such simulation into other electronic payment system such that the simulation could provide a reliable reference to examine the survivability of the system before it is widely deployed.

Chapter 2

Analysis Methods

Contents

2.1 Formal Method **4**
2.2 StarLogo **5**
2.3 Markov Chain **5**
2.4 EASEL **6**
2.4.1 Emergent Algorithms 6
2.4.2 Language 7
2.4.3 The simulator 7
2.5 Methodology for this paper **7**
2.6 Rest of this paper **7**

In this section, we want to talk about why we choose to use EASEL for analyzing our targets, and introduce related methods which can be applied on analyzing the survivability of an infrastructure or a system for comparison. We will talk about Formal Method, StarLogo, Markov Chain, and our tool, EASEL. Then we will introduce the concept of EASEL and the underlying concept, Emergent Algorithms, in the end of this chapter.

2.1 Formal Method

Most of the current approaches being used to analyze a system or an infrastructure would be using formal method. Which means "Methods that use ideas and techniques from mathematical or formal logic to specify and reason about computational systems"[6] the person wants to use formal method for analysis has to transform the whole system into formal specification (e.g. a set of symbols), formal logic and then deduct the result from the specification and the logic with deduction rules. After you can construct your system by these symbols and logics, you need to validate and verify your proof of your theorems.

The problem with this approach is mainly about that it is really hard for people to 'formalize' a system or an infrastructure, not to mention how hard to prove the system is secure from a set of axioms. And since it is a theorem system built on top of some axioms, then it might become pretty troublesome if there is something wrong with the axioms. So the cost of time and the complexity to build such a model is the main problems with this approach. We also think that formal method can not reach the completeness due to the "Incompleteness Theory" by Gödel. Which we will describe in later sections.

Scalability and complexity are probably the biggest problem for formal methods. For an unbounded system like the banking and finance infrastructure, it is almost impossible to use formal methods to analyze it, because it is too large and too complicated.

Besides the problems, formal method is good for examine the security of a system, especially if this system involved a strict model, e.g. Bell LaPadula and Biba model. Then using formal method to analyze seems to be the only formal way. But a model built according to formal method may not be used to examine other properties of a system, it is hard to model that too. We will talk about more in this aspect when we introduce the concept of survivability.

2.2 StarLogo

StarLogo[7] is developed in MIT Media Lab as a simulation environment for some biological or social system, e.g. Life in a pond, or traffic jam in New York City. It provides a easy-to-use and user friendly interface. It assumes that there are imaginative turtles controlled by the users (using Common Lisp) to simulate a decentralized system. StarLogo is pretty easy to use, and good for educational purposes.

The problems with StarLogo are the scalability, global visibility and centralized control. StarLogo can not perform well if we are going to use it to simulate a large system. And the idea behind the StarLogo system is very like the system we are going to use, but the concept of centralized control and global visibility are still implicitly embedded.

2.3 Markov Chain

In [8], we saw Markov Chain was used for analyzing the reliability of the payment systems. Markov Chain is being used to determine the probability distribution of incidents, so to estimate the downtime of a server, and its backup server. Such an analysis is not near to reality due to two reasons: 1. they assumed the communication lines are always operational in [8]. 2. the main assumption in the Markov Chain is the failure times for the individual system components are independent random variables following exponential distributions, which totally ignores the interactions among different system components and behavior of human attackers. Using Markov Chain can not examine the policy or risk of the payment system, it might only be a good tool for estimating time of certain events happen in the payment systems. Therefore we need a better tool to simulate the payment systems.

2.4 EASEL

EASEL stands for "Emergent Algorithm Simulation Environment and Language"[9]. It is developed to simulate an unbounded system and examine its security and survivability. An unbounded system here means that a loosely coupled system without central control and global visibility. To understand how we can use EASEL to build the simulation of an infrastructure and examine its security or survivability, we need to understand Emergent Algorithms first.

2.4.1 Emergent Algorithms

Emergent Algorithms were inspired from some biological and social system in which each participant performs a simple local action involving interactions with other participants but without complete knowledge of either who else is participating or their roles[9].

There are some important elements in EASEL that we should keep in mind while designing our simulation.

Unbounded System

When we talk about unbounded system, we mean a system which has no centralized control scheme. In biology system, we see flocks of birds flying without central commander. In social system, we see the economy develops without (despite) being controlled by the government or other organizations centrally. In computer network, the Internet will be the best example, where no one has central control of the whole Internet.

The next property of an unbounded system is "No global visibility", which means no one element in the system can see the whole system clearly. This property is complimented to the last one. For example, there is no single one router on the Internet have all the routing information about the whole Internet.

The last property we want to mention here is "Emergent properties". It means a property which does not exist on a single element in the system, but while every element works together as part of the system, there will be some property emerging on the system's scale. For example, with only power lines you can do nothing, but with a power generator, the power lines will serve as the transmission media of electricity to every house and they together construct the whole power system.

Actor

An actor could be any active entity in a simulation[9]. It can be a program, simulation, processor with multiple threads, a machine, a human being, or any object in the real system. There are some default special types for special kind of actors, which includes an observer, facilitator, and a processor.

Neighbor

A neighbor of an actor is another actor that interacts with the former. The definition of a neighbor can be described in geometrical distance (e.g. within 2 meters), in the line of sight or relationship (e.g. employee and employer). With the concept of actor and neighbor in mind, the interaction between them comes up naturally. Such interaction, or say, interdependency, is another important element for building the simulation in EASEL.

2.4.2 Language

EASEL is a language with strong user defined types, boundary checking, and structure language with a syntax similar to Algol, Ada, and Pascal. Compared to some methods described above, we think that using EASEL is easier and faster to develop a simulation for a critical infrastructure, while it is more flexible than using StarLogo.

2.4.3 The simulator

The EASEL simulator is targeted to be able to simulate a loosely coupled multiprocessing model on a uniprocessor platform[9]. It is implemented in C on PowerPC Macintosh platform. The implementation of this simulator is not finished yet. A public beta version is scheduled to be released in year 2001.

2.5 Methodology for this paper

We study this topic by understanding how the system works in the first place. We referred to Operating Circular and FedPoints in the Federal Reserve Banks. We also read papers related to such kind of research. After understood how the payment systems work, we try to apply the concept of Emergent Algorithms on analyzing the payment systems, looking for actors, their neighbors and the interdependencies. Because the EASEL simulator is a separated project from this thesis and it is not finished yet, therefore we can only use algorithms to describe the simulation we are going to design.

2.6 Rest of this paper

After introduction to our goal, the banking and finance infrastructure, in Chapter 1,then we describe the three systems we choose as target systems in Section 1.2. Brief introduction of the concepts about Formal Method in Section 2.1, StarLogo in Section 2.2, Markov Chain in Section 2.3, Survivability in Section1.1 and EASEL in Section 2.4 as the end of Part I.

In Part II, we will go into details about each payment system we choose, and we will discuss how we build the simulation for the cash payment system in Chapter 3. Check payment system are discussed in Chapter 4, while automated clearing houses are discussed in Chapter 5. Then we will present the architecture we built for designing the simulation as 6 in Part III . We will present the conclusion and future work in section 7 and section 7.2 as the end of this thesis.

In every chapter of payment systems, we will first introduce the mission of this system and its functions. Then we will show the flow of the system in graphic and text. In the analysis part, we will distinguish the actors, their properties, neighbors, functions and possible interactions. We will also present some possible risk scenarios and how we can express them in our simulation.

Part II

Payment Systems

Chapter 3

Cash Payment System

Contents

3.1 Introduction **11**

3.2 Flow **11**

3.2.1 Bank to the Fed 12

3.2.2 Fed to BEP 12

3.3 Statistics **12**

3.4 Analysis **14**

3.4.1 Public 14

3.4.2 Cash 16

3.4.3 Banks 17

3.4.4 Federal Reserve 18

3.4.5 BEP/Mint 20

3.5 Scenarios **21**

3.5.1 Counterfeiting 21

3.5.2 Money laundering 21

3.6 Discussion **21**

3.1 Introduction

Cash, notes of currency , printed by The Bureau of Engraving and Printing (BEP), is the most common way so far for people to exchange valuables. There are 500 billion US dollars in circulation all over the world now. Major circulation of US currency is outside of US.

The mission of the cash payment system is to keep the circulation of the cash stable and meet the demands of the public. Federal Reserve acts as the distributor of new cash notes, while it obtains those new cash from the Department of Treasury.

3.2 Flow

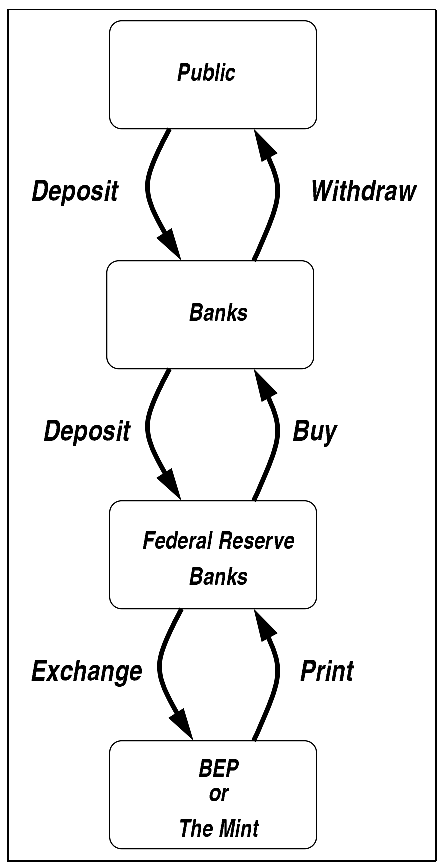

Figure 3.1: Flow chart of Cash circulation

In this flow chart of cash circulation, the public can deposit or withdraw money from local banks. Then the local banks can either go to bigger banks, or directly to the regional Federal Reserve to deposit the extra cash when the demand decreases, or buy new cash when the demand from the public rises.

The Federal Reserve Banks will examine all the notes sent by local banks. They will then destroy those 'unfit' notes, and require the amount of new money from BEP or the Mint by exchanging some collaterals equals to the value of money.

The general flow chart of the cash circulation procedures are illustrated in Figure 3.1. And in the following sections, we will list all the procedure for the cash circulation in more detail.

3.2.1 Bank to the Fed

A bank can require for obtaining cash service from its regional Federal Reserve Bank, which includes order and deposit.There are several requirements for a bank to obtain cash services from the Federal Reserve listed here:

1. Have an account on the books of a Federal Reserve Bank
2. Have access to a communications system designated by the Federal Reserve. The bank has to maintain the confidentiality and security of any access control features.
3. Have arranged for armored carrier transportation for the cash. USPS with prior approval can be an alternative.

The frequency for each bank to order/deposit currency/coin is once per week. But the Federal Reserve Bank reserves the right to reduce orders, refuse deposits, reverse credit or return deposits. Returns are at the bank's risk and expense.

The bank can make the order of currency through Fedline system or a telephone order system. If these two systems are not available, a FAX order is possible.

Cross Shipping

This term means if a bank deposit fit currency with your Federal Reserve Bank, the bank may not order currency of the same denomination from the Federal Reserve within five business days. Such practice should be eliminated or minimized at the depositing institution level.

Deposits of Currency

The currency has to be bundled according to denomination. A bundle should consists of 1,000 notes of the same denomination in ten equal straps. The bank is responsible for checking the currency beforehand.

3.2.2 Fed to BEP

The Federal Reserve Bank should ask currency or coin from BEP according to its policy and the demands of local banks. BEP would be responsible for producing currency and coins, also design of the security mechanism on the currency.

3.3 Statistics

In table 3.3, we list the expectation life of a bill in circulation of the cash system.

Denomination	Standard Strap (100 notes) Dollar Amount	Standard Bundle (1,000 notes in 10 straps) Dollar Amount	Standard ABA Color Code
$1	$100	$1,000	Blue
$2	$200	$2,000	Green
$5	$500	$5,000	Red
$10	$1,000	$10,000	Yellow
$20	$2,000	$20,000	Violet
$50	$5,000	$50,000	Brown
$100	$10,000	$100,000	Mustard

Table 3.1: Standard units for currency deposits

Denomination	Standard Unit Dollar Amount	Standard ABA Color Code
Pennies	$50	Red
Nickels	$200	Blue
Dimes	$1,000	Green
Quarters	$1,000	Orange
Halves	$1,000	Buff
Eisenhower	$1,000	Gray
Susan B. Anthony	$1,000	Gray

Table 3.2: Standard units for coin deposits

Denomination of Bill	Life Expectancy (Years)
$1	1.5
$5	2
$10	3
$20	4
$50	9
$100	9

Table 3.3: Expectation mean time for bill circulation

- About 500 billion US dollars are in circulation. Major part of them are outside the United States [10].
- Each business day, the Federal Reserve Bank of New York process 12 million notes [11].
- Each business day, the Federal Reserve Bank of New York destroys 5 million notes [11].
- In 1997, BEP produced 9 billion notes, worth 95 billion dollars [11]. 48% are 1 dollar bill.
- Cash is used for roughly 75 percent of retail payment transactions in the United States[1].

3.4 Analysis

After understanding the procedures of the Cash circulation, we can begin to make abstractions from the system, and form our simulation. We will focus on each entity in the system and on the function each of them performs. The most important of all will be on the impact of each function performed, and the 'neighborhood' relationship among all the entities in the system.

3.4.1 Public

The public here means an individual, corporation, or a business who has the chance to help the cash circulation but does not provide any financial service as a bank does. The public only performs two functions: deposit and withdraw. The public will only perform these functions to a bank. Therefore the neighborhood of a person will be someone he knows, and the bank he has account(s) in. We should also try to put a property on one person which we will name it "willingness to withdraw/deposit money", or "will" in short. Which will be used to measure a person's willingness to withdraw/deposit money from/to a bank.

Properties

- will - which describes how likely one person will withdraw/deposit money from/to the bank.
- wallet - the amount of cash one person holds in his wallet

Functions

- spend
- withdraw
- deposit

Neighborhood

- The public
- Local bank(s) with his account(s)

Interdependencies

- withdraw decrease the amount of money in an account of a local bank.
- deposit increase the amount of money in an account of a local bank.

Algorithm

The public spend cash according to their will and if they do not have enough money, they will withdraw from their bank accounts. The amount of money been spent, deposited, and withdrawed is decided randomly with some bound conditions.

We assume that using random number can simulate will of the public. Therefore we put will as a random integer between 1 to 3, where 1 means to spend, 2 means to deposit, and 3 means to withdraw money.

We use '.' to represent the structure member of a special data structure. And '[]' as element in an array. Capital letters would mean constants.

```
will = random( 1 .. 3 );
if ( will == SPEND ) {
  if ( wallet < money )
    withdraw ( bank, account, money );
    for ( i = 0 .. num_cash ) {
      num_cash[i].location = new_location;
      num_cash[i].bundle = no;
    }
    spend (money);
    wallet = wallet - money;
}

if ( will == DEPOSIT ) {
  money = random( 1 .. wallet );
  deposit ( bank, account, money );
  for ( i = 0 .. num_cash ) {
    num_cash[i].location = bank;
    num_cash[i].bundle = no;
  }
  wallet = wallet - money;
}

if ( will == WITHDRAW ) {
  money = random( 1 .. account_balance );
  withdraw ( bank, account, money );
```

```
  for ( i = 0 .. num_cash ) {
    num_cash[i].location = wallet;
    num_cash[i].bundle = no;
  }
  wallet = wallet + money;
}
```

3.4.2 Cash

Cash here means the currency, notes, or coins. They can be in good condition, worn out or even a counterfeit ones. A bundle of cash should be simulated too. Therefore cash should have the following properties:

Properties

- age - how old is it. This value increases with the simulation time by day.
- value - the face value of a currency or a coin.
- status - it should include good, usable, or bad (should be exchanged for a new one). The currency note will be good in the first week, usable and bad until the average life of currency note as Table 3.3.
- bundle - is it in a bundle of cash to be transfered to somewhere?
- location - where is it now.
- type - the currency note can be either real, recorded, or fake.

Neighborhood

A currency note or coin should be able to be seen by any other actors around it (them). That includes a person, a bank, Federal Reserve, or BEP.

Interdependencies

The cash can be deposit or withdraw by the public from local banks, which might change its status (e.g. good into worn out).

And the BEP would create new currency notes/coins as demanded.

Algorithm

For cash, we can only assign value to each of the properties, it does not perform any functions by itself.

```
cash.age = 0;
cash.value = value;
cash.status = good;
cash.type = real;
cash.bundle = yes;
cash.location = BEP;
```

3.4.3 Banks

Local banks will provide accounts for the public to deposit their money and withdraw from. Depending on the size of the bank, a bank might have an account in regional Federal Reserve. Then the bank can obtain new cash from Federal Reserve and deposit the excess.

Smaller banks do not have accounts in the Federal Reserves, so they have to deposit the excess and buy new cash from larger local banks.

Properties

- number of accounts and their balance
- amount of cash in the bank

Functions

- send excess money to the Federal Reserve
- require cash service from Federal Reserve
- open new account for customer
- close account for customer
- calculate the balance for each account according to its transactions

Neighborhood

A local bank should be seen by Federal Reserve, and its customers. We assume no one else is supposed to be able to access any information in the bank.

Interdependencies

- balance of each account will be changed by the account owner
- the total reserve in the bank will be changed according to the demand by its customer

Algorithm

According to the functions, the reserve in the bank will be changed according to the customer's activity. And the bank will ask for cash service from the Federal Reserve once per week.

```
if ( customer_withdraw ) {
  verify ( account, pin );
  account.balance = account.balance - money_withdraw;
  reserve = reserve - money_withdraw;
}
if ( customer_deposit ) {
  for ( i = 0 .. num_cash ) {
    if ( check ( num_cash[i].type ) != FAKE ) {
      account.balance = account.balance + money_deposit;
      reserve = reserve + money_deposit;
    }
    else { call_police(); }
  }
}
while ( once_every_week ) {
  if ( reserve > default_reserve ) {
    send ( reserve - default_reserve , federal_reserve );
    reserve = default_reserve;
  }
  if ( reserve < default_reserve ) {
    request ( default_reserve - reserve , federal_reserve );
    reserve = default_reserve;
  }
}
```

3.4.4 Federal Reserve

Federal Reserve plays a role of controlling the distribution of new cash and destroy of unfit cash. It can require new cash being printed from BEP or made by the Mint, if the request is for coins. The Federal Reserve would keep a reserve as a buffer for fulfilling the requests from local banks.

Properties

- reserve - Federal Reserve prepares some cash for emergency or daily distribution.
- location - which Federal Reserve is this

Functions

- destroy currency notes
- distribute currency notes/coins
- verify currency

Neighborhood

- other Federal Reserve
- local banks which have accounts in it

Interdependencies

- Reserve in the Federal Reserve is changed according to the activities by its customers (other banks).

Algorithm

```
while ( receive_request ( bank_id , request ) ) {
  if ( request.type == withdraw ) {
    if ( cash_reserve < request.amount ) {
      withdraw_bep ( request.amount , request.cash_type );
      cash_reserve = cash_request.amount;
    }
    bundle ( request.amount );
    send ( bank_id );
    debt_account ( bank_id , request.amount );
  }
  if ( request.type == deposit ) {
    if ( verify ( request.cash ) == fail ) {
      return_cash ( bank_id ) && sue ( bank_id );
    }
    else {
      deposit ( request.amount, bank_account );
      cash_reserve = cash_reserve + request.amount;
      credit_account ( bank_id , request.amount );
    }
  }
}

if ( cash_reserve < cash_threshold ) {
```

```
  withdraw_bep ( amount , type_cash );
  cash_reserve = cash_reserve + amount;
}
if ( cash.status == OLD || BROKEN ) {
  destroy ( amount, type_cash );
  withdraw_bep ( amount, type_cash );
}
```

3.4.5 BEP/Mint

The role played by BEP or Mint is only making new cash for the demand from the Federal Reserve. The security features on the currency is designed by BEP.

Functions

The main functions BEP will perform are:

- create currency notes/coins
- destroy coins[1]

Neighborhood

There should be no direct access from the public and local banks to the BEP. Only the Federal Reserve should have the access right to make transaction with BEP.

Interdependencies

- The cash reserve in the federal reserve will be changed by the production of the new currency notes or coins.

Algorithm

The BEP is only responsible for producing money and destroy money.

```
while ( request = accept_request ( fed_bank_id ) ) {
  if ( request.type == withdraw ) {
    produce ( request.amount , request.currency );
    send ( request.amount , request.currency , fed_bank_id );
  }
  if ( request.type == exchange ) {
    destroy ( request.amount , request.currency );
    produce ( request.amount , request.currency );
    send ( request.amount , request.currency , fed_bank_id );
```

[1] Federal Reserve destroys the currency notes directly

```
  }
}
```

3.5 Scenarios

3.5.1 Counterfeiting

By counterfeiting money we mean that the attacker produces currency note, or cash which looks or feels like the real one, but is not.

Algorithm

The counterfeiting is just a process to produce fake money and use it.

```
cash.age      = 0;
cash.value    = value;
cash.type     = fake;
cash.location = wallet;
```

3.5.2 Money laundering

When some currency notes are being recorded by police, for example, the gangster will try to deposit those notes into a bank, and get new cash from the bank. That is the money laundering scenario.

Algorithm

```
cash.type = recorded;
cash.location = wallet;

deposit ( bank_id , account , cash );
withdraw ( bank_id , account , cash );
```

3.6 Discussion

We did not provide detail about how the communication system is being used for cash services between the Federal Reserve and a local bank. We think that we can simply put a factor for the failure of the communication in the simulation.

Chapter 4

Check Payment System

Contents

4.1 Introduction **23**
4.2 Flow **23**
4.3 Statistics **23**
4.4 Analysis **25**
4.4.1 Actors 25
4.4.2 The Public 25
4.4.3 Collecting Bank 25
4.4.4 Paying bank 26
4.4.5 Correspondant Bank 27
4.4.6 Federal Reserve 28
4.4.7 Check 28
4.5 Scenario **29**
4.5.1 Return items 29
4.5.2 Check fraud 29

4.1 Introduction

Around 60 billion checks are written by Americans a year, worth a total value about 75 trillion[1]. And the number of checks total every year is still growing in a rate at 2 percent per year. The role of Federal Reserve Banks in the Check Payment System is mainly providing interbank check collection services to any check collecting and check paying banks.

Except Federal Reserve, there are lots of local/regional check collecting banks for regional check collection and clearing. But the Federal Reserve still handles about 35 percent of the interbank check collection in 1996[1].

4.2 Flow

A scenario from [12]:

A check is sent from the withdrawing bank, it goes to the Federal Reserve check processing site, and goes through the Interdistrict Transportation System to another Federal Reserve check processing site, then to the depositing bank. We can use figure 4.1 to illustrate a more general situation:

In Figure 4.1, the public can deposit a check into the collecting bank, if the paying bank is the same as the collecting bank (it is called a 'on-us' check), then the check will be settled in this bank. If the paying bank is another bank, then the collecting bank will transfer the check to some intermediary banks (clearing houses, correspondant bank, bankers' bank, or Federal Reserve), then to the paying bank. Then the account in the collecting bank should be credited by the amount of the check while the account in the paying bank should be debted accordingly.

4.3 Statistics

- The Federal Reserve accounted for about one-third of the estimated 45 billion interbank checks collected in the United States[1].
- The Federal Reserve had a 35 - 37 percent market share of the Interbank check collection in 1996[1].
- The Federal Reserve Banks currently present 13 percent of their total check volume electronically, which constitutes over 2 billion checks a year for more than 2,000 depository institutions.
- About 30 to 35 percent of checks written in the United States are "on-us" checks[1].

The check collection market distribution:

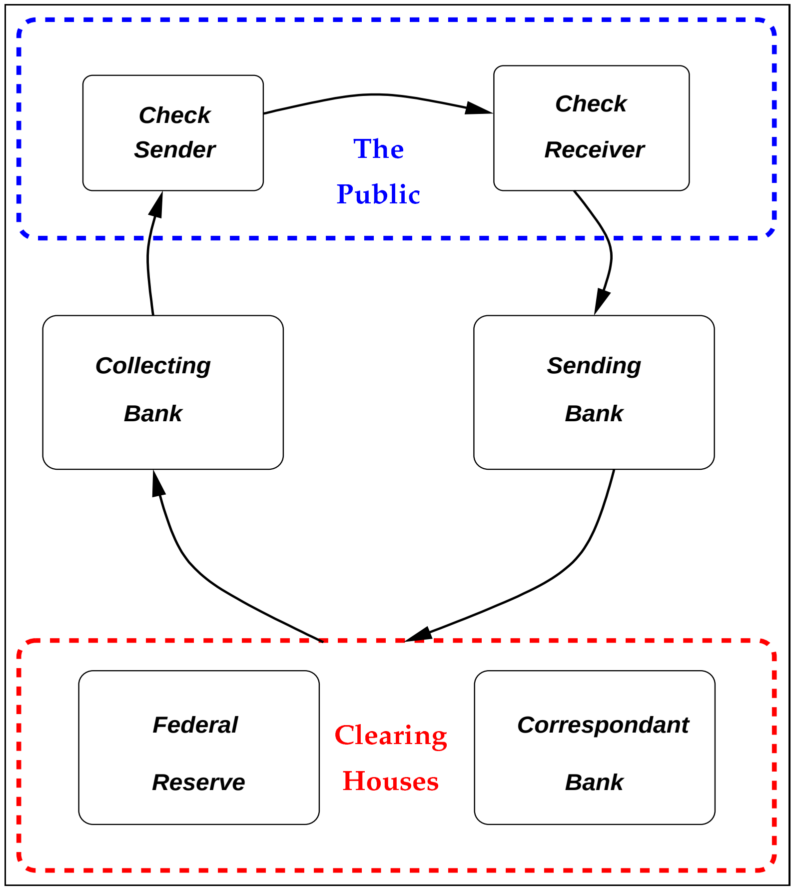

Figure 4.1: Flow chart of Check Process System

Check Collection channel	Standard Unit Dollar AmountVolume (billions of checks)	Market share (percent)
Clearinghouse	10 - 11	23 - 24
Direct Presentment	6	14
Correspondent Banks	10 - 11	24 - 25
Bankers' Banks	less than 1	1
Third-party Service Providers	less than 1	1
Federal Reserve Banks	16	35 - 37
Total	42 - 45	100

Table 4.1: 1996 Interbank Check Collection Market[1]

4.4 Analysis

4.4.1 Actors

We identify the actors in this system as the following:

The Public It includes the sender of the check and the receiver of the check.

Collecting Bank The bank where the check is first deposited.

Paying Bank The bank where the check is drawn.

Correspondant Bank The intermediary bank responsible for check collection among a few banks within a region. It can be a clearing houst or bankers' bank.

Federal Reserve It provides check collection services, including check processing and transfering.

We will try to find the properties of each actor in our simulation.

4.4.2 The Public

In the check payment system, there are the sender of a check and the receiver of a check. The sender and the receiver can be either an individual, or a company.

Property

- account - The sender must has an account in a local bank so he can open a check to the receiver. The receiver is not required to have a bank account.

Function

- Send a check
- Receive a check

Neighbor

- The public
- Local bank (Collecting or Sending)

4.4.3 Collecting Bank

A normal collecting bank should have an account for the public to deposit the check they get into their bank accounts or cash the check[1].

[1] If you present proper ID, then you can cash a check without holding a bank account.

Property

- Account holder
- Account balance
- Account number
- Amount of the check
- Number of the check
- image of the check
- Name
- Routing number

Neighborhood

- The paying bank
- The public
- The correspondant bank
- The federal reserve

Function

- transfer the check
- present the check
- credit the account
- process the returned check

4.4.4 Paying bank

The paying bank is the bank where the check is drawn on. Under some circumstances, it is possible to cash the check without[12].

Property

- Account holder
- Account balance
- Account number
- Name
- Routing number

Neighborhood

- The collecting bank
- The correspondant bank
- The federal reserve

Function

- Debt the account
- Examine the check
- Return the check
- Transfer credit

4.4.5 Correspondant Bank

A correspondant bank is a intermediary bank between the collecting and paying banks. Therefore, the check is exchanged through the intermdeiary bank if it is not an "on-us" check. A correspondant bank can be a clearing house, or bankers' bank.

Property

- Name
- Routing number

Neighborhood

- Collecting bank
- Paying bank
- Federal Reserve

Functions

- Return check
- Process check
- Verify check
- Credit the collecting bank account
- Debt the paying bank account
- Charge check processing fee

4.4.6 Federal Reserve

Property

- Bank account
- Account balance

Neighbor

- Collecting bank
- Paying Bank
- Correspondant bank

Functions

- Immediate credit
- Deferred credit
- Return check
- Verify check
- Charge check processing fee

4.4.7 Check

We think that check should be one of the actor, because there are many properties which can be altered or created by the public, the attacker or the bank. These interdependencies make the check proper for being one of the actors here.

Property

- Amount
- Pay to the order to
- Account
- Signature
- Geneuine
- Memo
- Image
- Bank
- Type (True or False)

Neighbor

- Collecting bank
- Paying bank
- Correspondant bank
- Federal Reserve
- The public

4.5 Scenario

We considered some scenarios related to risk assessment of the check payment system[13]. And there are two major categories of scenarios we are currently considering:

4.5.1 Return items

The check could be returned for the following reasons:

Not enough funds in the paying bank's account This situation can be expressed as that the balance of the account in the paying bank is less than the amount of the check. So the paying bank has to reject the payment and return the check.

A stop payment order has been issued This situation can be expressed as the account in the paying bank has been issued a 'stop-payment' flag, so the paying bank will reject and return the check.

A fraudulent check The check has been verified and labeled to be a fraudulent check, so either the collecting bank, correspondant bank or the paying bank can return the check.

The paying bank failed The paying bank failed to make the payment of this check. That means the paying bank has to be labeled as failed to make the payment.

4.5.2 Check fraud

Check kiting Writing checks on two or more banks to fraudulently obtain interest-free unauthorized loans.

Forgery Forge the signature on a check. The signature on the check should be labeled as forged.

Altered checks Some information on the check is altered. The information on the check should be labeled altered.

Counterfeit checks The check should be labeled counterfeit.

Paperhanging The account on this check is already closed.

Chapter 5

Automated Clearing Houses

Contents

5.1 Introduction **31**

5.2 Flow **31**

5.3 Statistics **32**

5.4 Analysis **33**

5.4.1 The Public 33

5.4.2 Sending Bank 33

5.4.3 ACH 34

5.4.4 Federal Reserve 35

5.5 Scenarios **35**

5.5.1 Credit Risk 35

5.1 Introduction

The Automated Clearing Houses are built to use electronic ways to avoid using paper check for routinely payments, e.g. salaries, consumer and corporate bill payments, interest and dividends, and Social Security.

The system is mainly for handling funds transfer. It consists of an infrastructure of data processing and communications hardware and software. The mission of the infrastructure is to deliver and settle large volumes of electronic payment transactions and related information.

5.2 Flow

The automated clearing house contains banks, servicing reserve banks, federal reserve and the public. We illustrate the whole ACH system as the following example and figure 5.1:

A company can activate a direct deposit from its depository institution to its employees, say, for their payrolls. So the company can initiate this transaction from the sending bank ,which holds an account for this company, to all of the company's employees' bank accounts. After the sending bank authenticates itself to the ACH, it can begin to send the credit items (the amount of payroll) to the ACH, then the ACH will send those credit to each of the employee's accounts.

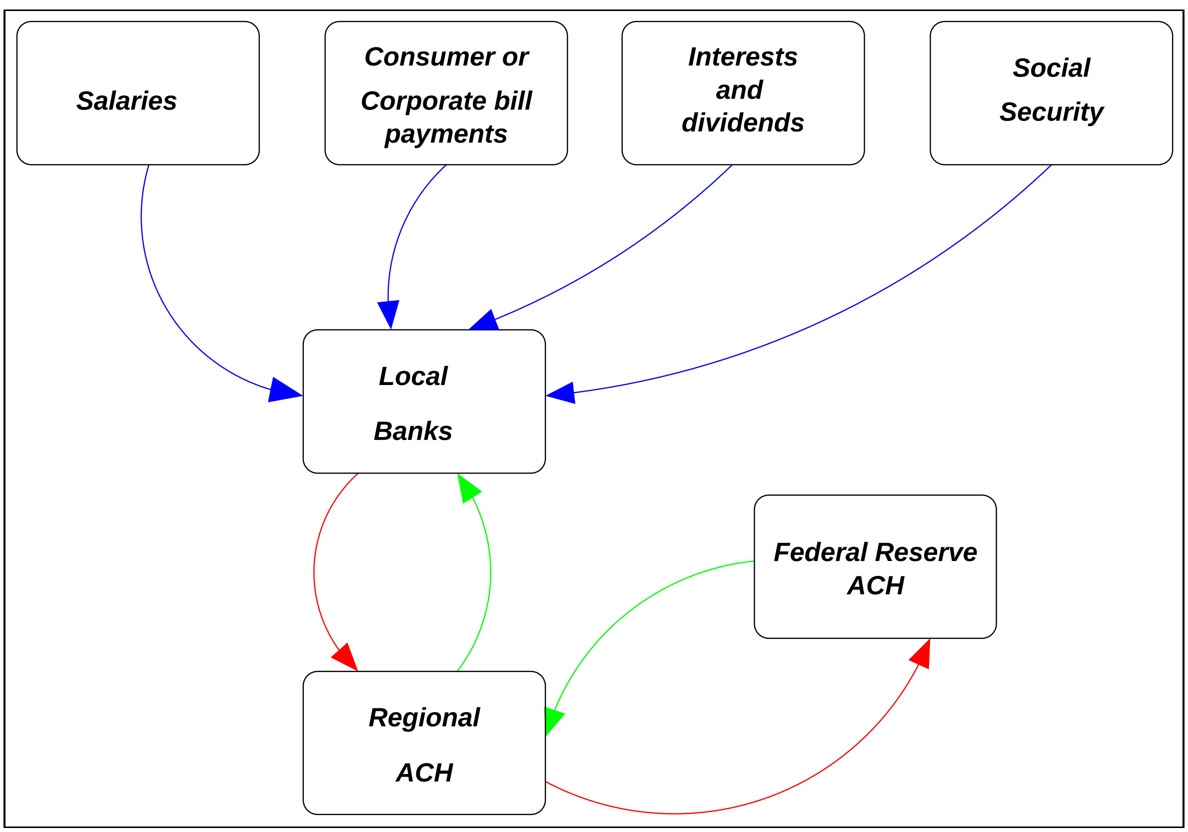

Figure 5.1: Flow chart of Automated Clearing House

There are some posting transaction rules related to ACH should be listed here[2]. These rules are used mainly for daylight overdraft[1] measurement.

- Post at 8:30 a.m. Eastern Time:
  - Government and commercial ACH credit transactions
  - Treasury Electronic Federal Tax Payment Systems (EFTPS) investments from ACH credit transactions
- Post at 11:00 a.m. Eastern Time:
  - Government and Commercial ACH debit transactions
  - EFTPS investments from ACH debit transactions
- Post at 5:00 p.m. Eastern Time:
  - Same-day ACH transactions

5.3 Statistics

- In 1997 over 3.4 billion payments with a total value of more than $10.7 trillion were processed by ACHs through the Federal Reserve System.
- ACH payments represent only less than 5 percent of non-cash transactions in the United States[1].
- Except Federal Reserve, there are other three commercial providers process and transmit ACH transactions.
- Federal Reserve is accounting for 80 percent of commercial interbank ACH transactions in 1996.

Cap Categories	Cap Multiples	
	Single Day	Two-Week Average
Zero	0	0
Exempt-from-filing[2]	$10 million/0.20	$10 million/0.20
De minimis	0.40	0.40
Average	1.125	0.75
Above average	1.875	1.125
High	2.25	1.50

Table 5.1: Cap Multiple Matrix[2]

[1] A negative position in an institution's Federal Reserve account at any time during the business day.

5.4 Analysis

We first identify the actors in the ACH payment system as follows:

- The public
- Sending Bank
- Receiving Bank
- ACH
- Federal Reserve

And we will describe each of the actors in the following sections.

5.4.1 The Public

The public here could be an individual, a company, or any legal subject which can create an account in the bank and initiate an ACH transaction. For example, an individual can allow a company (e.g. his/her insurance company) to deduce certain amount of money from his account periodically and automatically. This can be also done through ACH.

Property

- Account in bank (sending or receiving)

Neighborhood

- Sending bank or receiving bank
- The public

Functions

- Initiate a transaction

5.4.2 Sending Bank

The sending bank is the bank where the company or the payment originator has an account in. So when the payment originator activates a payment to other payment receivers (e.g. a company wants to activate the payrolls to its employees), the sending bank would send the credit/debt item with the account information in the receiving bank to the ACH or the Federal Reserve to be processed.

Property

- A routing number for identifying the sending bank.
- An account for the customer

Neighborhood

- The public
- Regional ACH
- Federal Reserve

Functions

- Send information (e.g. credit, or debt)
- Receive information (Acknowledgment from ACH)
- Detect account balance
- Authenticate

5.4.3 ACH

ACH provides hardware and software for processing the credit and debt sent from the sending bank to the settlement accounts in the receiving bank. Sometimes the ACH may have to send the information to another ACH if there is no direct connection between the first ACH and the receiving bank.

Property

We list some rules regarding to the process of ACH items here as the property of an ACH.

Neighborhood

- Other ACH
- Sending bank
- Receiving bank
- Federal Reserve

Functions

- Authenticate the sending bank
- Credit an account
- Debt an account
- Transfer to another ACH or Federal Reserve
- Transfer to receiving bank

- Process return item
- Process overdraft

5.4.4 Federal Reserve

One of the roles of Federal Reserve is to provide ACH service . They provide hardware and software for clearing and settlement. And banks can choose to use the Federal Reserve ACH services or they can use other commercial ACHs.

Neighborhood

- Sending bank
- Receiving bank
- Other ACH

Functions

- Authenticate the sending bank
- Credit an account
- Debt an account
- Transfer to another ACH or Federal Reserve
- Transfer to receiving bank
- Process return item
- Process overdraft

5.5 Scenarios

We will illustrate some scenarios related to risk management in the following sections. These scenarios will be used to examine or verify the simulation we are going to build.

5.5.1 Credit Risk

The settlement account in ACH might not be able to settled due to some credit risk, e.g. not enough fund in the originating account.

Part III

Result

Chapter 6

Simulation

Contents

6.1 Design **38**
6.1.1 Actors and Property 38
6.1.2 Interdependencies 43
6.2 Analysis **44**
6.2.1 Well-defined 44
6.2.2 Completeness 44
6.2.3 Correctness 44
6.3 Survivability requirements **45**
6.3.1 Recognize 45
6.3.2 Resist 45
6.3.3 Recover 45
6.3.4 Evolve 46

6.1 Design

After understand three payment systems, we are going to design our simulation for these three payment systems. We do not want to design three simulations (one for each of the payment systems) since they are related to each other. Therefore we will design one simulation for all three payment systems.

After the analysis in the former three chapters, we can separate the infrastructure into 4 different layers and one special role according to their functions as in figure 6.1 These four layers and the special role are:

The Public This layer means the actors which perform the behaviors including producing value, making transaction initiatives, sending and receiving value.

Local Banks The actors in this layer are the banks which hold accounts for customers but can not perform any clearing functions.

Inter-Banks The actors in this layer do not deal with the Public layer directly. They deal with the Local Banks layer and hold accounts for these banks so they can process transactions between two different local banks.

Government Organizations The actors in this layer are not involved into the transactions. They create currency notes (i.e. cash), and make regulations for the other layers.

The Attacker This is a special actor. Because the attacker can perform various attack from different layers

.

The steps we are going to use is first to identify the actors in the system according to the analysis we did for three payment system. And extract the properties and functions from each payment system.

6.1.1 Actors and Property

After the analysis and study of the payment systems, we conclude to claim we identified the following actors. Their properties will be describe together from three different payment systems.

- The public
- The bank
- ACH
- Federal Reserve
- The attacker

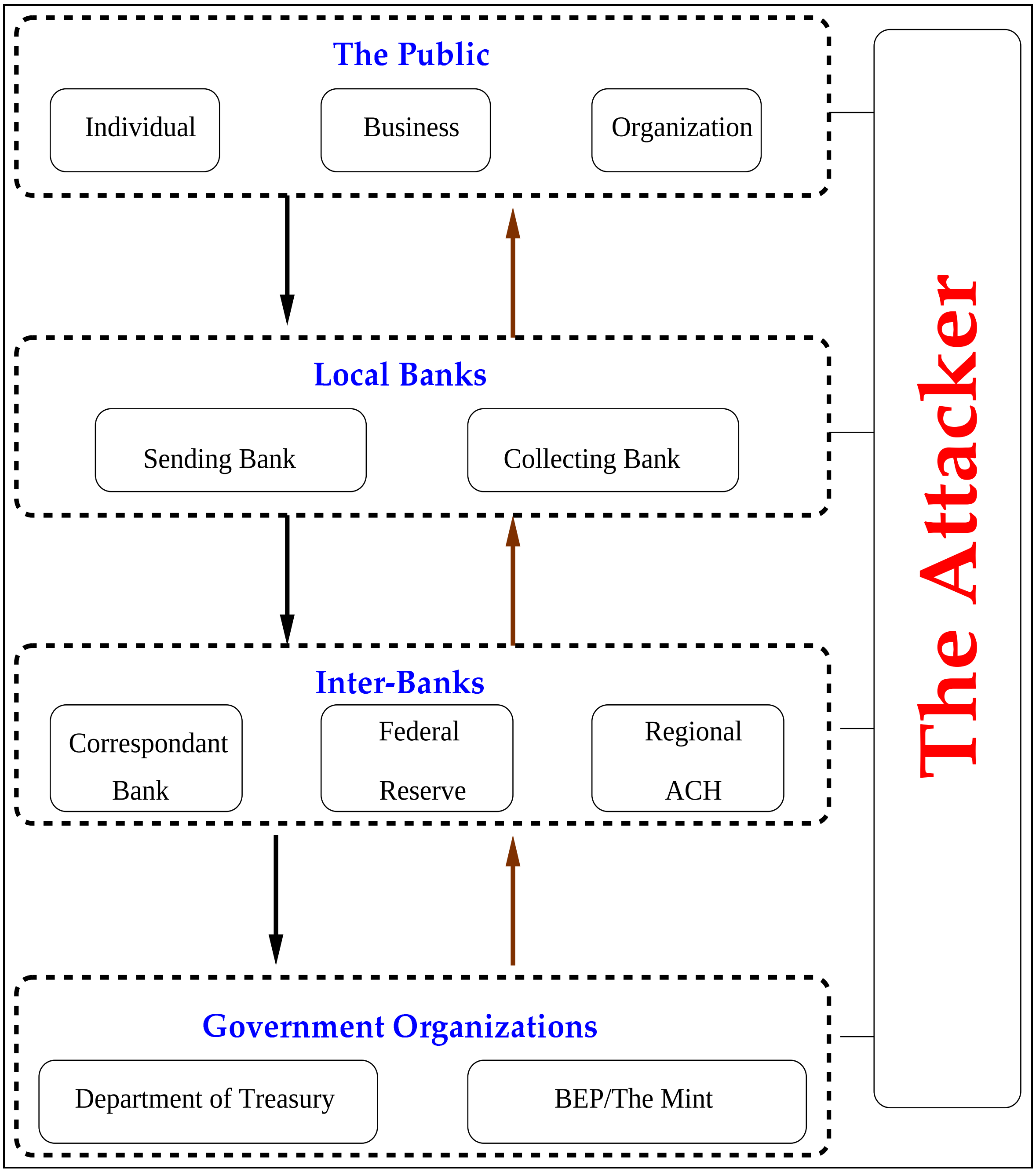

Figure 6.1: Layers in the banking and finance infrastructure

The public

The public represents an individual or a company who has access to use cash, check or being able to initiate an ACH transaction.

Property

- Account in bank (sending or receiving)
- will - which describes how likely one person will withdraw/deposit money from/to the bank.

Neighbor

- The public
- The bank

Function

- withdraw
- deposit
- Initiate a transaction

The Bank

Property

- number of accounts and their balance
- amount of cash in the bank
- A routing number for identifying the sending bank.
- An account for the customer
- Account holder
- Account balance
- Account number
- Amount of the check
- Number of the check
- image of the check
- Name
- Routing number

Neighbor

- The public
- Regional ACH
- The paying bank
- The correspondent bank
- The federal reserve
- The collecting bank

Function

- send excess money to the Federal Reserve
- require cash service from Federal Reserve
- open new account for customer
- close account for customer
- calculate the balance for each account according to its transactions
- Debt the account
- Examine the check
- Return the check
- Transfer credit
- Send information (e.g. credit, or debt)
- Receive information (Acknowledgment from ACH)
- Detect account balance
- Authenticate

ACH

Neighbor

- Other ACH
- Sending bank
- Receiving bank
- Federal Reserve

Function

- Authenticate the sending bank
- Credit an account
- Debt an account
- Transfer to another ACH or Federal Reserve
- Transfer to receiving bank
- Process return item
- Process overdraft

Federal Reserve

Property

- Bank account
- Account balance
- reserve - Federal Reserve prepares some cash for emergency or daily distribution.
- location - which Federal Reserve is this

Neighbor

- Collecting bank
- Paying Bank
- Correspondent bank
- other Federal Reserve
- local banks which have accounts in it
- Sending bank
- Receiving bank
- Other ACH

Function

- destroy currency notes
- distribute currency notes/coins
- verify currency
- Authenticate the sending bank
- Credit an account
- Debt an account
- Transfer to another ACH or Federal Reserve
- Transfer to receiving bank
- Process return item
- Process overdraft
- Immediate credit
- Deferred credit
- Return check
- Verify check
- Charge check processing fee

The attacker

The attacker is the actor which can act almost every action a normal actor can perform in a payment system. For example, if the attacker is going to use fake money, then he can create fake money and use it in the market or probably deposit it into the bank.

6.1.2 Interdependencies

After studying all these payment systems, we found that the accounts are the connection between our different actors in the payment systems. If we treat money as flow of water, then the account is like the hub which will control the direction and hold the water for a certain amount of time. The account keeps track of the money.

From the history aspect, people used to use books to keep the account. No one uses books to keep records nowadays. With the use of computer, the possibility for Salami attack (gathering roundoff numbers in computer to become one large amount of money) becomes larger. Because the computer can handle the number more precise than the real money can handle.

Among the three payment systems we studied, we found that the cash payment system is the final system which continues to work even when the other two (check and ACH) do not work. Because the currency notes represent value, while no one will be willing to exchange checks for goods when the check payment system could not properly work, not to mention the ACH, which is almost all electronic. So we can claim that other payment systems are based upon cash circulation. Cash does not depend on other payment systems to work. And we consider it to be more survivable.

For newer payment systems like electronic payment systems, credit cards and probably digital cash payment systems, we think that the architecture of our simulation continues to fit it pretty well. The reason is that these new payment systems are not changing the fundamental architecture of the original payment systems. These new payment systems are just turning the actors into electronic machines. There will still be the public who spends money, the bank responsible for processing the transactions. The role of Federal Reserve and other commercial service provider might change, and using the simulation should be the best way to study the possible results before policy deployment.

6.2 Analysis

We would like to discuss the issue of completeness for projecting the real system onto a simulation. The method we use here for EASEL is to analyze the system into actors, neighbors, and the interactions between them. For simulating our target, payment systems in banking and finance infrastructure, we treat the infrastructure as a flow of value (information). For a piece of value to flow in the system, there must be a sender and receiver, while the flow of value might change sender or receiver, which might also cause some chain reaction to the whole system. And we would like to categorize our discussion into following sections:

6.2.1 Well-defined

When we say a simulation is well-defined we mean that a simulation can represent every relationship in the real system. In our case, we use actors to represent the sender or receiver of the information, and the properties of an actor could be changed according to the information being passed around.

The criteria to judge whether a simulation is well-defined could be measuring the actions performed by the real system and comparing it with the simulation.

6.2.2 Completeness

Completeness means that the simulation is able to produce every possible result in the real system. Due to the "Incompleteness Theorem" by Gödel, there must be a statement in an axiom system within which can not be either proved or disproved. The simulation is always built upon some assumptions and axioms, therefore we claim that there is always some statement which a simulation can not simulate. The same claim applies to formal methods.

6.2.3 Correctness

Correctness means that with the equivalent input condition in both the simulation and the real system, they should produce equivalent results. In our simulation, we can feed real data into the simulation so we can verify the correctness of our simulation. Using scenarios to test the simulation is another way to measure this property.

6.3 Survivability requirements

In this section we want to discuss the interdependencies and the survivability requirements for the banking and finance infrastructure.

6.3.1 Recognize

From the point of recognizing disaster or possible intrusions, the payment systems in the banking and finance infrastructure needs to recognize mainly the fraud and operation error. And there are some limits to the current system.

For example, the recognition of fake currency notes is usually being done in the merchant or the bank. The normal public has knowledge to recognize part of the fake cash, but some of the fake cash is hard to be distinguished from the real one.

A fake check will not be recognized until the sending bank or the collecting bank process it. Problems with a checking account are recognized during the settlement. Using the electronic check process can only shorten the time for handling daylight overdraft.

6.3.2 Resist

One strategy that some Intelligent Agencys use to disturb or destroy one country's economy is to make lots of fake money and put them into the cash circulation. When the amount of total money is too large, then the economy of a country will break down. We have no data to indicate how much fake money is currently in the circulation. But our simulation should help people to understand the possible threshold of breakdown.

Most of the bad checks or checking accounts are found. Though actions might be taken to reduce the loss, there are still some uncovered loss due to check fraud.

6.3.3 Recover

Once the banking and finance infrastructure is under attack, the fastest recovered payment system should be cash payment system. Because cash is distributed outside the bank. The value of cash is not totally dependent on banks, it also depends on the country. Without relying on the bank, people can still use the cash to exchange for goods. That is the reason why people would like to withdraw more money before the year 2000. The check or ACH payment system can not work without banks. In other words, they are dependent on the accounts in the banks. Therefore, a requirement for diversity (similar to that provided by the cash payment system) should be addressed while designing the payment systems of the future.

6.3.4 Evolve

One evolution of cash is the anti-counterfeiting measures on the new currency notes. The techniques that people use to counterfeit money is improving, so do the anti-counterfeiting measures.

We still think that diversity is the requirement for evolve. For example, when the banks go down, the cash system can still work in a different way, which means people will use the currency they still believe to have value to exchange for goods. That will fall back to the original way people trade with each other.

Chapter 7

Conclusion

Contents

7.1 Conclusion 47
7.2 Future Work 48

7.1 Conclusion

In our opinion, the concept of Emergent Algorithms is easy to understand and apply when designing a simulation of unbounded systems like the banking and finance infrastructure. There are no axioms to be built, no theorems to be proved (Formal Methods, in section 2.1) and no need to imagine turtles crawling around (StarLogo, in section 2.2). It is definitely easier and more pratical to use EASEL to apply the concept of Emergent Algorithms to design and implement the simulation. Implementing such a simulation will help people get better insights on how to build a survivable system.

The completeness of a simulation depends on the amount of detail given and thus full completeness is impossible to reach. As the amount of detail increases, other tools like formal methods become impractical to specify and analyze. For an EASEL simulation, the more details given, the more questions that can be answered by the simulation. The more details given to the simulation, the more closely we approximate the real world. Of course the most complete description and the only complete description of the world is the world itself. That involves some philosophical questions, which are out of the scope of this thesis. Beyond those philosophical questions, we should develop ways to evaluate how much detail is needed for a useful simulation. In this thesis, we use some special cases (e.g. counterfeiting money, fake signature or fake check) to evaluate whether our simulation can properly project the real infrastructure. Other methods should be explored, e.g. existing monetary policies. By using the concept of Emergent Algorithms and EASEL for simulation, we are trying to build an abstraction of the real system. We focus on the relationship and interactions among actors within the system. We contrast EASEL's practicality with formal methods, StarLogo, and Markov Chains. Simulations in EASEL appear to provide a firm foundation for developing emergent algorithms and developing intuitions about survivable systems.

For the survivability of the banking and finance infrastructure, we found the accounts in each bank form the interdependency within the infrastructure. Each payment system depends on the others by sharing the same account in different banks. The cash payment system is the most survivable, because the value of cash depends not only on the accounts in banks, and the amount of gold in the Federal Reserve vault, but also on the economy of a country, and on the confidence people have in the value it represents. When the other payment systems break down, the cash payment system can still be used. Thus the cash system's diverse sources makes it more survivable. Cash also adds diversity to the payment systems.

For electronic payment systems, we found that their survivability currently depends entirely on the stability of the automated systems. Unlike cash, which can still be used even if all the computers are down, electronic payments can fail completely.

7.2 Future Work

The most important future work is to implement the simulations we talk about in this paper in EASEL. Within the banking and finance infrastructure, there are other payment systems which need to be understood and simulated. In the meantime, some monetary policy proposals can be injected into the simulations for estimating possible effects. Interdependencies with other infrastructures should be explored too. For example, there are currently other students working on the power industry and the health information management systems. There also may be critical interdependencies between payment systems and the communications infrastructure.

Designing the simulation for the rest of the banking and finance infrastructure will require sorting out all the details of those systems and determining which parts are critical. A method for evaluating the details of those systems should be developed while building the simulation.

Bibliography

[1] Committee on the Federal Reserve in the Payments Mechanism. "The Federal Reserve in the Payments Mechanism". Jan. 1998. http://www.federalreserve.gov/boarddocs/press/General/1998/19980105/19980105.pdf.

[2] Federal Reserve System. "Overview of the Federal Reserve's Payments System Risk Policy". Technical report, Federal Reserve, May 1998. http://www.federalreserve.gov/PaymentSystems/PSR/overview.pdf.

[3] Transition Office of the President's Commission on Critical Infrastructure Protection and the Critical Infrastructure Assurance Office. "Preliminary Research and Development Roadmap for Protecting and Assuring Critical National Infrastructures". 1998.

[4] R. J. Ellison, D. A. Fisher, R. C. Linger, H. F. Lipson, T. A. Longstaff, and N. R. Mead. "Survivable Systems: An Emerging Discipline". In *Proceedings of the 11th Canadian Information Technology Security Symposium (CITSS)*, Ottawa, Ontario, May 1999. Communications Security Establishment, Government of Canada.

[5] Board of Governors of the Federal Reserver System, Washington DC. "The Federal Reserve System Purposes and Functions". 1994. http://www.bog.frb.fed.us/pf/pdf/frspurp.pdf.

[6] John Rushby. "Formal Methods and their Role in the Certification of Critical Systems". Technical Report CSL-95-1, Computer Science Laboratory, SRI International, Mar 1995.

[7] M. Resnick. "Computers and Exploratory Learning". In *New Paradigms for Computing, New Paradigms for Thinking*. Springer-Verlag, 1995.

[8] A. Burnetas, G. Reynolds, and J. B. Thomson. "Reliability Analysis of the Federal Reserve Automated Payments System". Working paper, Federal Reserve Financial Services Research Group, Mar. 1997. http://www.clev.frb.org/research/fsrg/fsrg0397.pdf.

[9] David A. Fisher. "Design and Implementation of EASEL, A Language for Simulating Highly Distributed Systems". Proceedings of MacHack 14, the 14th Annual Conference for Leading Edge Developers, June 1999.

[10] FedPoint. *"How Currency Gets into Circulation"*, chapter 1. Federal Reserve Bank New York. http://www.ny.frb.org/pihome/fedpoint/fed01.html.

[11] FedPoint. *"Currency Processing and Destruction"*, chapter 11. Federal Reserve Bank of New York. http://www.ny.frb.org/pihome/fedpoint/fed11.html.

[12] Federal Reserve Atlanta. "Check Booklet". http://www.frbatlanta.org/publica/brochure/check/check.htm.

[13] John C. Knight, M. C. Elder, J. Flinn, and P. Marx. "Summaries of Three Critical Infrastructure Applications". *Dept. of Computer Science, University of Virginia*.

[14] R. B. Avery, R. W. Bostic, P. S. Calem, and Glenn B. Canner. "Changes in the Distribution of Banking Offices". *Federal Reserve Bulletin*, September 1997.

[15] W. F. Treacy, and M. S. Carey. "Credit Risk Rating at Large U.S. Banks". *Federal Reserve Bulletin*, November 1998.

[16] J. C. Williams. "Simple Rules for Monetary Policy". Technical report, Board of Governors of Federal Reserve System, 1999.

[17] R. S. Demsetz, and P. E. Strahan. "Historical Patterns and Recent Changes in the Relationship between Bank Holding Company Size and Risk". *Federal Reserve Bank New York, Economic Policy Review*, July 1995.

[18] A. M. Gilbert, D. Hunt, K. C. Winch. "Creating an Integrated Payment System: The Evolution of Fedwire". *Federal Reserve Bank New York, Economic Policy Review*, July 1997.

[19] J. Jayaratne, and D. Morgan. "Information Problems and Deposit Constraints at Banks". Research Paper, November 1997. http://www.ny.frb.org/rmaghome/rsch_pap/9731.html.

[20] D. P. Morgan. "Judging The Risk of Banks: What Makes Banks Opaque?". Research paper, Federal Reserve Bank of New York, September 1997. http://www.ny.frb.org/rmaghome/rsch_pap/9805.htm.

[21] S. E. Black, and D. P. Morgan. "Risk and The Democratization of Credit Cards". Research paper, Federal Reserve Bank of New York, June 1998. http://www.ny.frb.org/rmaghome/rsch_pap/9815.htm.

[22] Euro-Currency Standing Committee. "On the use of information and risk management by international banks". Technical report, Bank for International Settlement, 1998.

[23] Federal Reserve System. "Modifiying Federal Reserve ACH Operations and Pricing Practices Relative to Private-Sector ACH Operations". Technical report, Federal Reserve System, 1999.

[24] Basle Committee on Banking Supervision. "Credit Risk Modelling: Current Practices and Applications". Technical report, Basle Committee on Banking Supervision, April 1999.

[25] Board of Governors of Federal Reserve System. "Report to the Congress on Funds Availability Schedules and Check Fraud at Depository Institutions". Technical report, Board of Governors of Federal Reserve System, October 1996.

[26] J. Wenninger, and D. Laster. "The Electronic Purse". *Federal Reserve Bank New York, Current Issue in Economics and Finance*, 1(1), April 1995.

[27] L. J. Radecki, J. Wenninger, and D. K. Orlow. "Bank Branches in Supermarkets". *Federal Reserve Bank New York, Current Issue in Economics and Finance*, 2(13), December 1996.

[28] Federal Reserve Bank of New York. "A day at the FED". http://www.ny.frb.org/pihome/addpub/dayatfed.pdf.

[29] Board of Governors of Federal Reserve System. "Report to the Congress: on the Application of the Electronic Fund Transfer Act to Electronic Stored-Value Products". Technical report, Board of Governors of Federal Reserve System, March 1997. Submitted to the Congress pursuant to section 2601 of the Economic Growth and Regulatory Paperwork Reduction Act of 1996.

[30] General Accounting Office. "Payments, Clearance, And Settlement. A Guide to the Systems, Risks, and Issues", June 1997.

[31] Federal Reserve Bank of New York. "The Key to the Gold Vault". http://www.ny.frb.org/pihome/addpub/goldvaul.pdf.

[32] J. A. Lopez. "Regulatory Evaluation of Value-at-Risk Models". Research Paper, Research and Market Analysis Group, Federal Reserve Bank of New York.

[33] Board of Governors of Federal Reserve System. "Report to the Congress: Concerning the Availability of Consumer Identifying Information and Financial Fraud". Technical report, Board of Governors of Federal Reserve System, March 1997.

[34] Basle Committee on Banking Supervision. "On the Use of Information and Risk Management by International Banks". Technical report, Basle Committee on Banking Supervision, October 1998.

[35] FedPoint. *"Automated Clearing Houses (ACH)"*, chapter 31. Federal Reserve Bank of New York. http://www.ny.frb.org/pihome/fedpoint/fed31.html.

[36] Federal Reserve Bank. *"Cash Services"*, chapter 2. Operating Circular. http://www.ny.frb.org/bankinfo/operating/oc2.pdf.

[37] Federal Reserve Bank. *"Collection of cash items and returned checks"*, chapter 3. Operating Circular. http://www.ny.frb.org/bankinfo/operating/oc3.pdf.

[38] Federal Reserve Bank. *"Automated Clearing House Items"*, chapter 4. Operating Circular. http://www.ny.frb.org/bankinfo/operating/oc4.pdf.

[39] R. J. Ellison, D. A. Fisher, R. C. Linger, H. F. Lipson, T. Longstaff, and N. R. Mead. "A Survivable Network Analysis Method". In *Position Papers for the 1998 Information Survivability Workshop*, Orlando, Florida, Oct 1998. IEEE Computer Society, 1998.

[40] Howard F. Lipson, and D. A. Fisher. "Survivability - A New Technical and Business Perspective on Security". In *Proceedings of the 1999 New Security Paradigms Workshop*. Association for Computing Machinery, 1999.

[41] R. J. Ellison, R. C. Linger, T. Longstaff, and N. R. Mead. "A Case Study in Survivable Network System Analysis". Technical Report CMU/SEI-98-TR-014, Software Engineering Institute, Sep 1998.

[42] David A. Fisher and H. F. Lipson. "Emergent Algorithms – A New Method for Enhancing Survivability in Unbounded Systems". Maui, HI, Jan 1999. Proceedings of 32nd Annual Hawaii International Conference On System Sciences (HICSS-32), IEEE Computer Society Press, Los Alamitos, CA, 1999.

[43] John C. Knight, M. C. Elder, A. C. Chapin, B. K. Combs, S. Geist, S. McCulloch, L. G. Nakano, and R. S. Sielken. "Topics in Survivable Systems". Technical Report CS-98-22, University of Virginia, Aug 1998.