Digital Money in Speedos

James Leslie Keedy
Eislebener Str. 20, 28329 Germany
email: keedy@jlkeedy.net
formerly Professor/Honorary Professor at the University of Newcastle, NSW; Monash University, Melbourne, the Technical University of Darmstadt, the University of Bremen and the University of Ulm

Abstract

We are all familiar with the idea that representations of money can appear in files, but in this paper the idea that money itself can stored in files and can be directly used to pay bills, etc. is proposed. This idea is new and raises even more difficult questions regarding the security of computers than those raised by simply storing information about money (e.g. in bank accounts on conventional computers). The paper illustrates how this can be achieved securely in Speedos. It assumes knowledge of the basic Speedos mechanisms, which can be obtained from the Speedos website[1].

Keywords

Capabilities, partitioned segmentation, capability systems, addressing registers, money pockets, inflation, inflation-free banking, fractional reserve banking.

1 Background

The concept described in this paper arose while I was working on a book which is provisionally called "Lateral Thinking in Society" [1], in a chapter called "Reorganising Banking". The ideas there are at least as unconventional as my ideas about computing. One of the aims of that chapter was to eliminate inflation, and it turned out that through ideas explained in this paper it is also possible to eliminate the need for private banks. In order to understand this it is first necessary to understand how Speedos protection functions.

2 Protecting Capabilities

Speedos is a design for a very secure computer system [2]. Its security is based on the use of capabilities. It is therefore important that the capabilities themselves are safely protected.

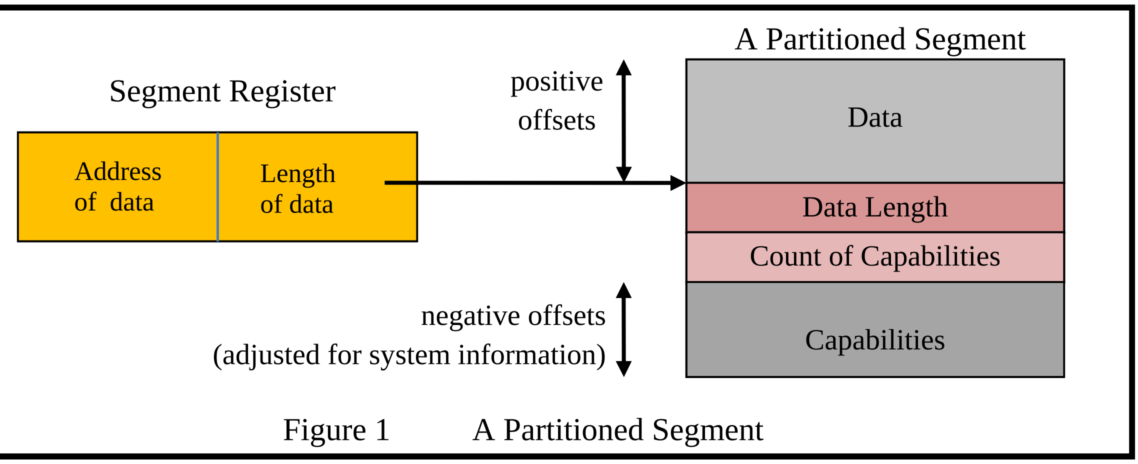

Figure 1 A Partitioned Segment

The technique used to protect capabilities in Speedos is known as partitioned segmentation, which was first suggested by Anita K. Jones [3]. The basic idea is shown in Figure 1. A Segment Register (which can only be set by the kernel) points to a segment in the virtual memory, see Figure 2.

[1] see https://www.speedos-security.org/

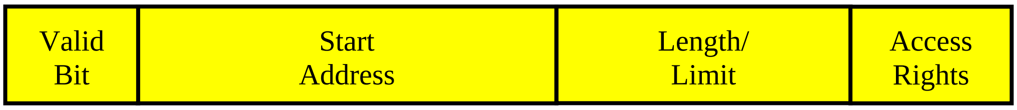

Figure 2: A Speedos Segment Register

A user program can use the normal instructions of the CPU to address data in association with positive offsets from the segment registers.

Beneath the data is a red tape area which can only be accessed by the kernel. This provides a fuller picture of the segment. The kernel also provides 'kernel instructions' which allow capabilities to be addressed securely by the owner of the segment. In the simple case envisaged by Jones the user program can select a capability by number.

In Speedos there are two levels of capabilities (for addressing segments and for addressing modules). Figure 3 shows how the partitioned segment technique is extended in Speedos to protect both segment capabilities and module capabilities. The latter are needed to access information-hiding modules (see [4]).

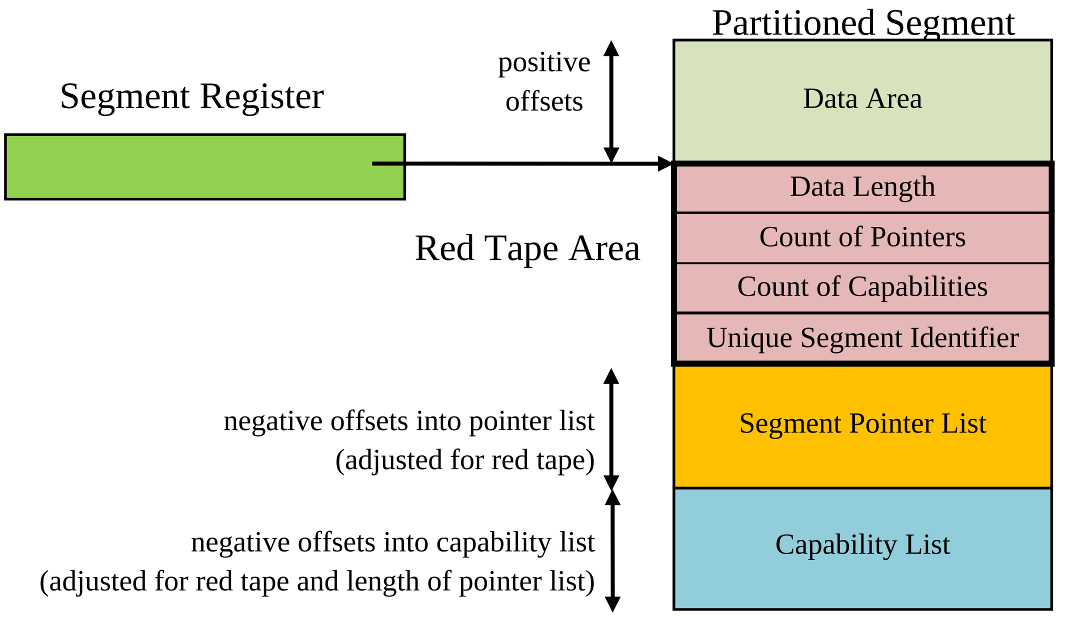
Partitioned Segment
Segment Register
positive offsets
Data Area
Data Length
Count of Pointers
Count of Capabilities
Unique Segment Identifier
Red Tape Area
negative offsets into pointer list (adjusted for red tape)
Segment Pointer List
negative offsets into capability list (adjusted for red tape and length of pointer list)
Capability List

Figure 3: SPEEDOS Partitioned Segments

They have four basic areas: a data area, a red tape area, a segment pointer list and a capability list. The Unique Segment Identifier is a further protection measure which need not be discussed here.

3 Implementing Secure Money

If it were considered appropriate to implement real money on computers, the next step would be to add an additional area in partitioned segments to allow money to be securely stored. Such an area is shown in Figure 4. This extends the red tape area by adding a field which contains a count of Money Pockets. Money Pockets are protected data structures which can only be accessed and modified by the kernel, via kernel instructions (analogous to capabilities).

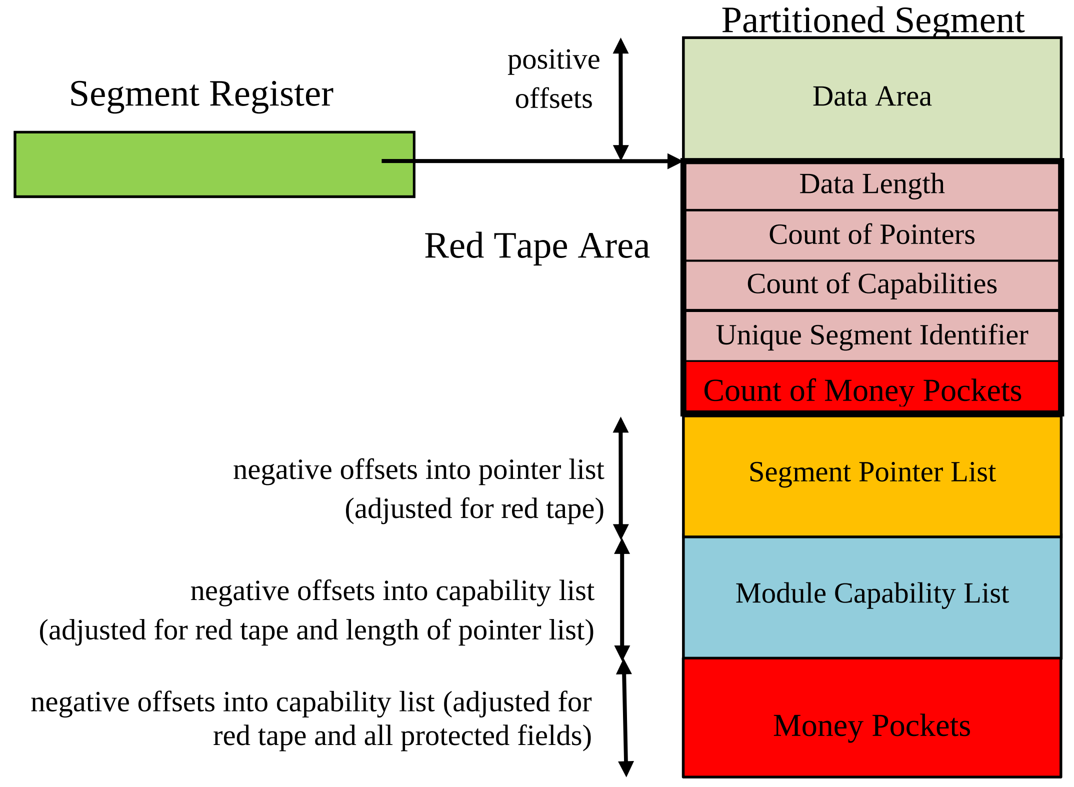
Partitioned Segment
Segment Register
positive offsets
Data Area
Data Length
Count of Pointers
Count of Capabilities
Unique Segment Identifier
Count of Money Pockets
Red Tape Area
negative offsets into pointer list (adjusted for red tape)
Segment Pointer List
negative offsets into capability list (adjusted for red tape and length of pointer list)
Module Capability List
negative offsets into capability list (adjusted for red tape and all protected fields)
Money Pockets

Figure 4: Storing real money in a SPEEDOS Computer

4 Kernel Instructions for Managing Money

Only two basic operations are needed by normal users in a Speedos computer system[2] in order to manage their Money Pockets. Here they are.

a) **Move X currency units from Money Pocket A to Money Pocket B**

This first operation allows the owner of digital money stored in a particular Money Pocket to move the (positive) number of currency units specified in a parameter X to another Money Pocket. This might be used for example to move money between different Money Pockets of its owner, but also to move money to Money Pockets of another user (e.g. to pay for goods which the user has bought from him).

A *normal* memory move operation in a computer system is in fact usually implemented as a *copy* operation, i.e. after moving information from location A to location B, A and B will contain the same information. But in the case of moving money from one Money Pocket to another the move operation is definitely *not* a copy operation, but is instead what I will call a *money move*.

By a money move I mean a move which reduces the amount of money stored in Money Pocket A by a specified number of currency units and increases the amount of money stored in Money Pocket B by the same amount.

Before a money move operation is carried out by the system kernel it checks that all the following conditions are met:

[2] "In a Speedos computer system" includes devices such as Speedos smart phones and other hand-held devices.

i) Both location A and location B must be Money Pockets.

ii) The amount of money held in A before the money move operation is carried out must be greater than or equal to the value indicated in the parameter X (which specifies the amount of money to be moved and must be a *positive* number of currency units).

iii) The invocation of these operations is restricted to persons or computer programs authorised to do so.

Here is the second operation which can be applied to a Money Pocket.

b) Write into data location C the number of currency units stored in Money Pocket A.

The purpose of the second operation on digital money is to allow a user to check the amount of digital money in one of his Money Pockets and to store the result in a normal data location of the computer. It is equivalent to opening your wallet so that you can see how much money it contains, then writing the result onto a piece of paper. This does *not* change or in any way affect the money stored in the Money Pocket.

This second computer instruction operates like a normal computer copy operation in the sense that on completion of the instruction the source location A is *not* changed, i.e. the amount of money held in Money Pocket A has neither increased nor decreased, and the location is still secure. But as a result of this operation a representation of the amount of money stored in Money Pocket A now appears as data (i.e. not the commodity money) in a normal data format in data location C. The result in C is *not* digital money but is merely a representation of money, as in current banking and accounting systems. As in current systems this money representation (not the money itself) provides the information needed for accounting, etc. Thus anything which current systems can do can also be achieved in the system being proposed. (The reverse is not true!)

Operations of type b) require location A to be a Money Pocket and location C to be a normal data location. Both are checked as part of the operation.

5 Handling Remote Money Pockets

The situation will often arise that a Speedos user wishes to make a payment to a Retailer. The simplest way to do this would be for the payer, who is presumably on the premises of the payee, to have a device which holds a Money Pocket containing enough money to make the required payment, e.g. a smartphone or a USB stick. Retailers will have a device which is able to access the Money Pocket to make a money move, and print a receipt, just as they have devices in current systems (adapted to Speedos).

Transferring money between normal users via the very simple and straightforward banking system which I envisage (without private banks) could be achieved via on-line banking, as is discussed in the next section but it would also be worth considering the manufacture of a simple device which makes money moves between two USB sticks available.

6 Banking Philosophy and Money Operations

If only these two operations were available, the following question would arise: How does real money get into the system? The answer to this question is crucial, since it depends on how money is created and regulated in the system. My preference is that money cannot arbitrarily be created, with the beneficial consequence that inflation cannot arise!

6.1 Inflation-free Banking

Inflation is now rife because US President Nixon, fearing in 1971 that the U.S. no longer had enough gold to cover all the dollars in circulation, suspended the convertibility of dollars into gold, which by 1973 caused the collapse of the Bretton Woods Agreement on currency exchange. We all suffer from this unfortunate decision. It opened the way for fiat money (the printing of banknotes not backed by gold). Thanks to the greed of bankers and others this has led to many disasters, including the rise of superrich multi-billionaires, the lack of funding for democratic governments, the increasing impoverishment of the working classes and even of the middle classes, which we are now beginning to witness. This has all happened because fiat money has no stable anchor. Gold previously provided this stable anchor because the amount of gold has scarcely increased over the centuries. Such a stable anchor can best be achieved for a computer-based currency by not allowing the amount of digital currency to be increased. The result would be that genuine inflation[3] would instantly cease, without all the almost endless pseudo-science which surrounds it today. Why then do we have inflation? The answer is that both private bankers and central bankers profit enormously from inflation. How they do this is explained in chapter 6 of [1].

Nevertheless a fixed amount (the 'money supply') must be set up before the system can begin. This can be set by the following additional operation.

c) Unrestricted move Y currency units from data location A to Money Pocket B

This is the inverse of the operation b). It is a very dangerous operation because, in banking parlance, it creates money out of thin air. My very strong conviction is that it should be used only once, by a very honest and controlled central banking authority, to kick-start the system.

Such a 'use once' arrangement might be organised in the code of the kernel instruction, e.g. by setting a global flag in the kernel's private data to indicate that the operation has already been carried out. Thereafter we have an inflation-free currency!

Quite surprisingly, this system is not only inflation-free, but it can also form the basis of a remarkably simple banking system which eliminates the need for private (commercial) banks and simplifies the work of a central bank. This is explained in more detail in chapter 6 of [1].

6.2 Conventional Banking and Fractional Reserve Banking

Like other business institutions private banks exist to make a profit. They make their profits primarily by maintaining accounts for their business customers and for their individual private customers. In chapters 6 and 7 of [5], Rothbard describes the origins of private banks and how there were separate but very interesting backgrounds for loan banking and for deposit banking. However, we leave these distinctions aside, because they are scarcely relevant to modern day banking. More relevant is a decision made by Lord Cottenham in the British House of Lords in 1848. He determined as follows:

"Money, when paid into a bank, ceases altogether to be the money of the principal; it is then the money of the banker, who is bound to an equivalent by paying a similar sum to that deposited with him when he is asked for it.… The money placed in the custody of a banker is, to all intents and purposes, the money of the banker, to do with it as he pleases; he is guilty of no breach of trust in employing it; he is not answerable to the principal if he puts it into jeopardy, if he engages in a hazardous speculation; he is not bound to keep it or deal with it as the property of his principal; but he is, of course, answerable for the amount, because he has contracted."

This disastrous judgement remains the legal situation in Western Europe and in the USA. It opened up the way for bankers legally to introduce *fractional reserve banking*, which, in the opinion of Rothbard [5] is best viewed as a form of legal counterfeiting. Instead of limiting the loans which they make to the amount of their reserves (assets), with fractional reserve banking bankers issue loans well in excess of the amounts deposited with them.

The bankers rely on the expectation that not all depositors will want to redeem their de-

[3] Rising prices are not necessarily a good indicator of inflation, since prices are also subject to the law of supply and demand (see [5, 6, 1].

posits together.

Suppose for example that a banker receives a deposit of $50,000 but issues a loan to Smith for $130,000 then the fraction in reserve, against which demands can be met, is 5/13. The money ("receipts") now in circulation has been increased by $80,000 to $130,000.

Where does the new money come from? In modern banking it is simply the result of the central bank printing more notes, i.e. creating money out of thin air! Thus the practice of fractional reserve banking is clearly fraudulent (though legal) and inflationary (by increasing the overall money supply). Modern commercial banks which take advantage of fractional reserve banking can (with the help of the central bank and within limits set by the latter) simply create money (just like counterfeiters). The profits from this accrue to the owners of the bank (or its partners or shareholders), and the cost to the general public is inflation and therefore devaluation of their income and/or savings. This is unfair on all, but especially on those with fixed incomes such as pensioners and recipients of social welfare payments!

Allowing fractional reserve banking implies that banks are not subject to the same rules as other companies. If a normal company does not at all times have sufficient assets to cover its liabilities when these fall due, then it is insolvent. Not so the commercial banks. Their liabilities (i.e. money on deposit to them) are due on demand, but if all their depositors request the redemption of their deposits at the same time, the bank would under normal rules be insolvent, which in fact means that they are technically in a permanent state of insolvency, because this can happen at any time as a result of the practice of fractional reserve banking.

The boom and bust business cycle, which has brought great personal distress to many individuals and bankruptcy to many companies (e.g. the Wall Street crash of 1929 and more recently the Global Financial Crisis of 2007-2008), has its roots in the practice of fractional reserve banking, because this makes bank credits subject not only to expansion but also to contraction.

When a loan is repaid the extra money created to allow the loan must be destroyed. This implies that the money supply contracts and so has a deflationary effect on prices and can eventually lead to a recession. If for example, in an excessive boom, depositors become nervous and begin to request the redemption of their deposits, banks which have over-issued loans will have to recall these in an attempt to satisfy the requests of their depositors, which can result in a recessionary bust. In other words the natural successor of an inflationary boom which gets out of control is a recessionary bust.

According to Investopedia[4], on 26th March 2020 the US (privately owned) central bank, the Federal Reserve, "reduced reserve requirements of all depositary institutions to zero. Instead, banks are now paid a specific interest rate on their reserve balance to encourage holding reserves". This in no way prevents the fundamental risks created by fractional reserve banking.

This apparent diversion on fractional reserve banking should hopefully make clear to all that private banking, which is almost universally used in the USA and Europe, is a costly luxury. Nevertheless, if society wishes to continue along this route of supporting private banks my proposal for implementing digital money is still possible. To achieve this requires only that the third operation "Unrestricted move Y currency units from data location A to Money Pocket B" will be frequently used by central banks to "create money out of thin air" and a further operation will be necessary to destroy money, as follows:

d) Destroy all currency units in Money Pocket C

This operation reduces the amount of currency in Money Pocket C to zero currency units.

[4] see https://www.investopedia.com/terms/f/fractionalreservebanking.asp

7 Conclusion

It has been shown how Speedos could support a digital currency by using some basic kernel instructions which are themselves protected via the partitioned segmentation scheme (the scheme which Speedos also uses to protect capabilities [4]). To support conventional banking four such basic operations are required, but the scheme can be used to support an inflation-free currency.

Since the ideas in this paper are somewhat speculative they are not part of the basic Speedos proposal as described on the Speedos website (https://www.speedos-security.org/), but have been added to illustrate the flexibility of Speedos and its potential for the future.

Funding: This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

References

[1] J. L. Keedy, Lateral Thinking in Society, https://www.jlkeedy.net/, 2024.

[2] J. L. Keedy, Making Computers Secure, Speedos Website, https://www.speedos-security.org/, 2021.

[3] A. K. Jones, “Capability Architecture Revisited,” *ACM Operating Systems Review*, vol. 14, no. 3, pp. 33-35, 1980.

[4] J. L. Keedy, “S-RISC: Adding Security to RISC Computers,” SPEEDOS Website (https://www.speedos-security.org/), 2023.

[5] M. N. Rothbard, The Mystery of Banking, Auburn, Alabama: Ludwig von Mises Institute, 2nd Edition, 2008.

[6] S. Forbes, N. Lewis and E. Ames, Inflation - What it is, Why it's bad, and How to fix it, New York, London: Encounter Books, 2022.