Computer Security & Electronic Payment System
Term Paper

The Study of E-payment System Using Smart Card

2001.6.14

[Members]

2001060	Shin Heung-soon
2001057	Song Jae-il
2001084	Lee Mi-sung
2001122	Cheung Jae-ho

Contents

1. Introduction
   1) The background of project
   2) The purpose of project
2. The Smart Card
   1) Definition of smart card
   2) The type of smart card
   3) Application
   4) Major players
   5) The advantages of smart card
   6) The problems of commercialization
3. Approach developing the smart card to desirable one; three aspects
   1) Market appealing
   2) Security solution
      2.1) Physical security
      2.2) Protocol security
      2.3) Authentication security
4. Conclusion and comment
5. References

1. Introduction

1) The background of project

Forrester Research estimated that in 2003, the size of e-commerce (B2B, B2C) would be $3.2tril, which is 5% of total worldwide sales amount and Louis Gerstner, the CEO of IBM, forecasted that the size of e-commerce in Korea would be increased from $2.4mi in 1998 to $50mil in 2001. So the importance of e-commerce would be raised. In this moment, the one of the significant factor that affects on the development of e-commerce is electronic payment system.

The electronic payment system in e-commerce should provide strong security to protect personal information as well as data during transactions so that the electronic payment system should be needed powerful security system. What will be the ideal electronic payment system?

Nowadays, the most popular one may be the payment system using smart card, which is mentioned that it has strong security tool in it.

Even though the smart card got the good reputation about security, there is no perfect payment system around the world that satisfies all the requirement of security system. However, it is important subject for us to find out the way of developing the secure payment system using smart card.

2) The purpose of project

In this project, we would like to study how to make ideal payment system using smart card and try to present the way of developing more secure and convenient payment system from the point of various aspects.

2. The Smart card

1) The definition of smart card

A smart card is a credit-card sized plastic card embedded with an integrated circuit chip that makes it "smart". This marriage between a convenient plastic card and a microprocessor allows an immense amount of information to be stored, accessed and processed either online or offline. Smart cards can store several hundred times more data than a conventional card with a magnetic stripe. The information or application stored in the IC chip is transferred through an electronic module that interconnects with a terminal or a card reader.

2) The type of smart card

2.1) Contact card: The smart card that is operated by physical contact between smart card reader and chip of smart card.
It is used for authentication and digital signature.
2.2) Contactless card: A contactless smart card has an antenna coil that communicates with a receiving antenna to transfer information.
It is fit in application such as bus card or distribution, which has limit in transaction time.
2.3) Hybrid card: The contact card and contactless card are physically independent within one card. The application of Hardware support

(independent memory) and software support (independent OS) is not efficient. The production cost is high.

2.4) Combi card: The card mutually shares the common part of contact card and contactless card and has independent part respectively. It results in integration effect of heterogeneous application through sharing of internal source. If the sharing memory part is damaged, the function of contact and contactless card would be paralyzed.

3) Application

3.1) Wire and wireless communication: For GSM applications the Smart card, also called the SIM card (Subscriber Identity Module), consists of a dedicated microcontroller, various memory blocks and I/O integrated into a single chip, with its associated software. This chip is required to:

Execute authentication algorithms with key storage in order to identify the user, store data for various services such as abbreviated number dialing and short messages, and Store programs for certain applications and services.

The concept of a removable SIM adds mobility, flexibility for handset personalization and overall security to the subscriber. In addition, the availability of large non-volatile memories provides an evolution path towards new services and features that can be loaded OTA (Over The Air) into the SIM after the card has been issued.

3.2) E-commerce: The optimum means of payment and security. Store the data and information safely. Payment system

3.3) Financial Sector: Electronic cash, electronic purse, debit card etc.

3.4) Transportation: Automatic collecting toll system that perceives traffic information through the antenna in a tollgate or at a terminal and communicates between the antenna and OBU(On Board Uint) installed in a car in order to collect toll. It will save time of collecting toll, relieve the traffic congestion up to 30%, reduce fuel costs and preserving environments by relieving the traffic congestion, supply advanced customer service by cashless payment system, reducing management costs of collecting toll and optimize traffic management.

4) Major players

There are several major players in smart card market such as;
VISA(SET specification) : http://www.visa.com
Gemplus : http://www.gemplus.com
Bull : http://www.cp8.bull.net
Schlumberger : http://www.1.slb.com/smartcards
Siemens : http://www.sci.siemens.com
HP (alliance HP ? Informix : imagine card):
http://www-europe.hp.com/alliance
IBM smart card solution: http://www-3.ibm.com/pvc
Mondex solution : http://www.mondex.com
Recently Microsoft starts to enter the smart card market aggressively.

5) The advantages of Smart card

Compared to conventional data transmission devices such as magnetic-stripe cards, smart cards offer enhanced security, convenience and economic benefits. In addition, smart card-based systems are highly configurable to suit individual needs. Finally, the multifunctionality as payment, application and networking devices renders a smart card as a perfect user interface in a mobile, networked economy.

Security

Smart cards incorporate encryption and authentication technologies that can implement issuer's and user's requirements for the highest degree of security. Using encryption, contents and data can be securely transferred via wired and wireless networks. Coupled with biometric authentication methods which rely on personal physical attributes, smart cards are used in distributing government welfare payments in order to reduce frauds and abuse. Health care cards allow doctors to access and manage patient's medical records and insurance information without compromising privacy.

Personalized network access cards allow safer and easier management of diverse networks without a significant costs for access control.

Convenience

One use of the old fashioned memory cards is to replace various identification cards. Smart cards will combine paper, plastic and magnetic cards used for identification, automatic teller machines, copiers, toll collection, pay phones, health care and welfare administration. Universities, firms and governments rely on smart identification cards since they can contain more detailed data and enable many services to be integrated. Health care cards, for example, reduce document processing costs by allowing immediate access to personalized patient information stored in smart cards. Most other smart card uses combine identification function with specialized purposes as in military PX cards, government's Electronic Benefit Transfer cards, and university ID cards that are also used to pay for food and photocopies.

Economic Benefits

Smart cards reduce transaction costs by eliminating paper and paper handling costs in hospitals and government benefit payment programs. Contact and contactless toll payment cards streamline toll collection procedures, reducing labor costs as well as delays caused by manual systems. Maintenance costs for vending machines, petroleum dispensers, parking meters and public phones are lowered while revenues could increase, about 30% in some estimates, due to the convenience of the smart card payment systems in these machines.

Customization

A smart card contains all the data needed to personalize networking, Web connection, payments and other applications. Using a smart card, one can establish a personalized network connection anywhere in the world using a phone center or an information kiosk. Web servers will verify the user's identity and present a customized Web page, an e-mail connection and other authorized services based on the data read from a smart card.

Personal settings for electronic appliances, including computers, will be stored in smart cards rather than in the appliances themselves. Phone numbers are stored in smart cards instead of phones. While appliances become generic tools, users only carry a smart card as the ultimate networking and personal computing device.

Multifunctionality

The processing power of a smart card makes it ideal to mix multiple functions. For example, government benefit cards will also allow users access to other benefit programs such as health care clinics and job training programs. A college identification card can be used to pay for food, phone calls and photocopies, to access campus networks and to register classes. By integrating many functions, governments and colleges can manage and improve their operations at lower costs and offer innovative services.

6) The problems of commercialization

Even though there are several advantages of smart card, it has not been appealed in the market. These problems can be found from the case of Manhattan and New York project 'tested in last year.

First, there were no reliable alternatives for increasing the rate of using smart card. Especially there wasn t any motivation for forcing people to use smart card as electronic cash reasonably.

Secondly, the range of payment was very limited so people never had an interest using smart card in practice. For example, Visa cash and Mondex were used in general member store but could not be used in other public place such as public phone, bus, subway, taxi, which needed micropayment.

Thirdly, the smart card as an IC card could not performed the multifunction but just store the value of cash. Therefore, there were no combinations such as bonus program or debit function etc.

Fourthly, the technical instability would let the people ignore the smart card as payment system. The store experienced frequent system down, maintenance and repairing so that users felt inconvenient and it did not appealed to market.

As we can see the smart card payment system and some problems as above, from now on we will study how to resolve the problems and represent the way how to make ideal smart card payment system appeal to the market from the various aspects.

3. Approach developing the smart card to desirable one; three aspects

1) Market appealing

Smart card marketing strategy

Why are consumers so unimpressed on smart card?

The problem is not that consumers dislike the idea of smart card. Of course 2,400 North America surveyed last summer by smart card forum, a trade group, more than three quarters clamed that they would like to have one. But those "very" or "extremely" interested in smart cards were most eager for a card to carry vital medical and car-related information. Fewer than half wanted a smart card they could use to buy things.

Electronic money has thus turned out to be a solution in search of a problem. It was supposed to appeal to harry commuters wanting to buy paper and cup of coffee without fumbling for coins. All cash machine cards issued in Belgium include a chip that functions as an electronic purse.

And card's main use is not to shop, but to feed parking meters, Laundromats and pay telephones. Much the same is true in Finland, and New York.

To move electronic money beyond the Laundromats means finding ways to make consumers wants it. So we should have our eyes on versatile versions of electronic pursues.

Successful case of smart card

When American Express kick-started the smart-card trend in the U.S. with its Blue card in September 1999, it came as quite a surprise. The company rolled out a national ad campaign and special offers to get people to sign up. By the end of 2000, AmEx had issued 4 million cards; twice the number it had anticipated, according to research firm Brittain Associates. And fully half of the cardholders were new customers.

That Blue card caught on so quickly is something of a feat, given that, as smart cards go, it's pretty dumb. Encoded with an electronic wallet and not much else, the 16KB chip is so limited that it's little more than a design element.

But what an element, AmEx's marketing gurus plopped an enormous hologram in the center of the card, imbuing it with gauzy future-tech mystique. Call it the coolness factor. How could anyone hip and tech-savvy not carry Blue? They also made the card's chip-based online security feature a selling point, capitalizing on consumers' fears about online purchasing. And the company gave away free smart-card readers - a brilliant marketing strategy that was remarkably cost-effective. Only 8 percent of Blue cardholders actually order a smart-card reader, according to Brittain Associates. What really drew consumers, though, were some of the best terms in the industry: no interest for the first six months and no annual fee.

What would lure consumers to these new cards?

First of all, their exceptional marketing strategy was a best roll to contribute to lure consumers. And they tied it in with other benefits and other marketing that gives people a reason besides the chip to get the card. May be consumers could feel that they get something shiny and new that your neighbor doesn't have by getting blue card with a beautiful design and new technology is applied. Consumers love Blue for its beauty and its interest rate, not its factions. And a good thing, too.

Designing to accept combine smart card with loyalty program

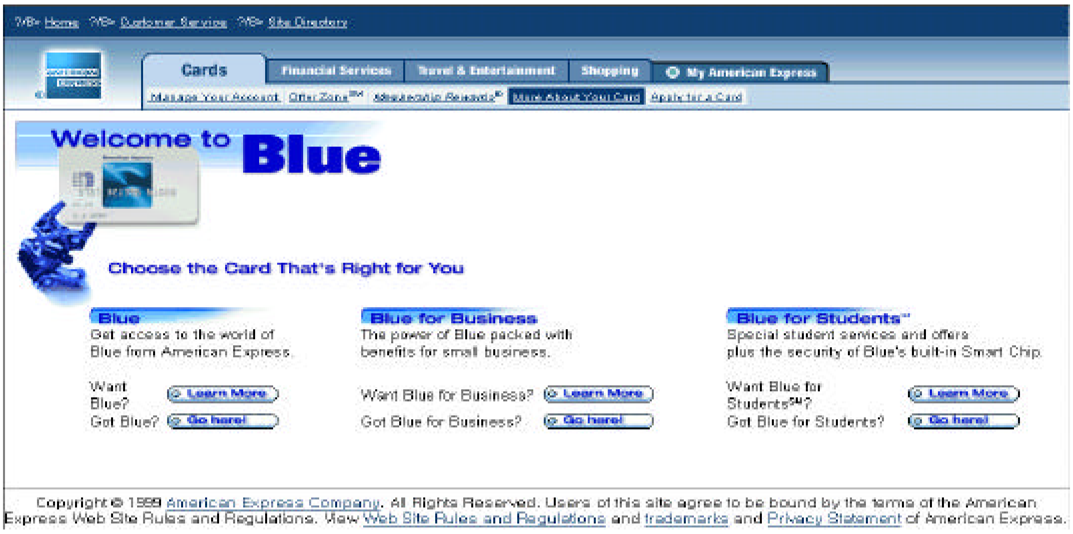
Consumer's cash card will record the fact that you have purchased 9burgers meals from big bite, so when consumer order the tenth consumer will get it free.
Discount coupons for online shopping; a program that tracks frequent-flyer miles, a program that holds airline- ticket and boarding-pass information. And when the smart card is slipped into a card reader, a small device attached to a PC, the cardholder can install new applications and delete old ones - a handy option, for instance, if corporate travel office ditches the Hilton in favor of the Marriott.

Amex's target market segmentation's strategy and on-line service through web-site
They targeted not those who would use as traditional credit card but also on-line shopper by providing point-of-sale terminals worldwide.
Customers can register on American Express' Web site for a software data-management and storage application known as an online wallet. Customers need only enter information - such as name, account number and shipping address - into the wallet once. When they want to buy something online, they just click open the wallet and hit the "complete purchase" button, according to the company.

In order to prevent unauthorized access to an American Express online wallet, customers could be offered free smartcard readers that can be connected to their PCs. The smart chip in the Blue card stores a digital certificate unique to each cardholder. When the card is placed in the reader, the cardholder enters his or her personal identification number, the digital certificate is read by the reader, and the online wallet can be unlocked.

Blue has its own web site where cardholders can check their current account status in terms of charges to their cards and pay their bills online. Cardholders can also download their card statements from the site into Intuit 's Quicken accountancy software or to Microsoft's Money application.

The Blue Web site additionally offers preview information on upcoming concerts and performers, and cardholders can hook up to free simulcast of concerts for which American Express is an advertiser. For example, on Tuesday, Eric Clapton, Chrissie Hynde, Sarah McLachlan, Stevie Nicks and Sheryl Crow will perform in Central Park in New York, at an American Express-backed concert to celebrate Blue's debut.



Choose the Card That's Right for You

Blue
Get access to the world of Blue from American Express.
Want Blue?
Got Blue?

Blue for Business
The power of Blue packed with benefits for small business.
Want Blue for Business?
Got Blue for Business?

Blue for Students℠
Special student services and offers plus the security of Blue's built-in Smart Chip.
Want Blue for Students℠?
Got Blue for Students?

Copyright © 1999 American Express Company. All Rights Reserved. Users of this site agree to be bound by the terms of the American Express Web Site Rules and Regulations. View Web Site Rules and Regulations and trademarks and Privacy Statement of American Express.

Amex 's website for customer service

Approach to improve lack of perception

If people begin to use smart cards in a business environment for applications such as computer security, building access and small purchases, then they will see how easy they are to use and will want to use them outside the office as well.

Businesses could use smart cards for a variety of functions. For example, one emerging use is to secure computer log-ons using smart cards in conjunction with a fingerprint identification system. The user carries a smart card that contains personal information, such as an authentication key. But in order to prove that the holder of the card is indeed the right user, the card would also store fingerprint information that could be matched to a scan of a fingerprint taken via a small hardware device. Once logged on, the user could send and receive information that would be automatically encrypted and authenticated using information stored on the smart card.

Another use that many companies have expressed interest in is the ability to use smart cards to store personal configurations of desktop applications, as well as security features, so that users can access their own information on a home server when traveling. The person would simply insert the smart card into a reader on any PC connected to the Internet, and get automatic access to their data on the server. For example, a smart card could hold information allowing a user to access address books, e-mail or documents stored on a server.

While the smart card is appealed to market, the most important thing is how to make much more secure payment system. In the next aspect, we are going to cover the security enhancement method at three parts; physical security, protocol security, authentication security.

2) Security Solution

2.1) Physical security; How To Make Tamper-Resistant Smartcard Processors

Tamper resistance is of importance in electronic payment system where the security of an entire system collapses as soon as a few cards are compromised
We describe techniques for extracting protected software and data from smartcard processors. This includes manual microprobing, laser cutting, focused ion-beam manipulation, glitch attacks, and power analysis. . We give ways that make such attacks considerably more difficult

① Tampering Techniques

We can distinguish four major attack categories:

- Microprobing techniques can be used to access the chip surface directly, thus we can observe, manipulate, and interfere with the integrated circuit.

- Software attacks use the normal communication interface of the processor and exploit security vulnerabilities found in the protocols, cryptographic algorithms, or their implementation.
- Eavesdropping techniques monitor, with high time resolution, the analog characteristics of all supply and interface connections and any other electromagnetic radiation produced by the processor during normal operation.
- Fault generation techniques use abnormal environmental conditions to generate malfunctions in the processor that provide additional access.

The design of most non-invasive attacks requires detailed knowledge of both the processor and software. On the other hand, invasive microprobing attacks require very little initial knowledge and usually work with a similar set of techniques on a wide range of products. Attacks therefore often start with invasive reverse engineering, the results of which then help to develop cheaper and faster non-invasive attacks.

② Tamper Resistance versus Tamper Evidence

I. Invasive attacks(violate tamper resistance requirement)

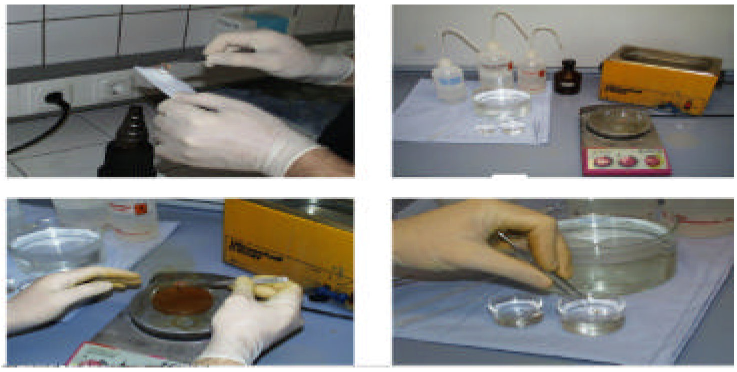
Microprobing, FIB editing, Layout reconstruction
Require between hours and weeks in a specialized laboratory, therefore the owner of the card is likely to notice the attack and can revoke certificates for keys that might be lost.

II. Non- invasive attacks (violate in addition tamper- evidence requirement)

Glitch attacks, Power analysis, Software vulnerabilities
Can be performed within a few seconds inside a Trojan terminal in a Mafia- owned shop, therefore card owner will not notice that card secrets have been stolen and will not revoke keys.

A. Details of Invasive Attacks

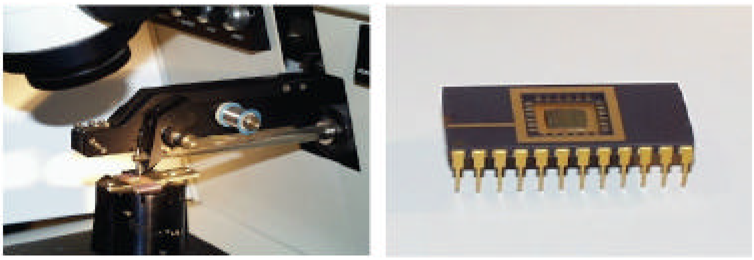
Depackaging of Smartcards



Preparation 1: Depackaging of the processor

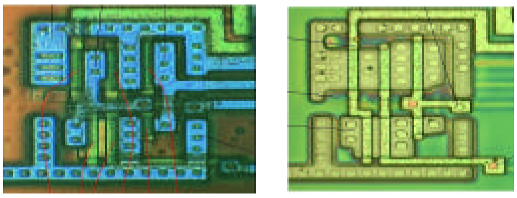
1) Heat up card plastic, bend it, and remove chip module

2) Dissolve package in 60 ℃ fuming nitric acid, then wash in acetone, deionized water, and finally isopropanol. The etching should be carried out under very dry conditions.



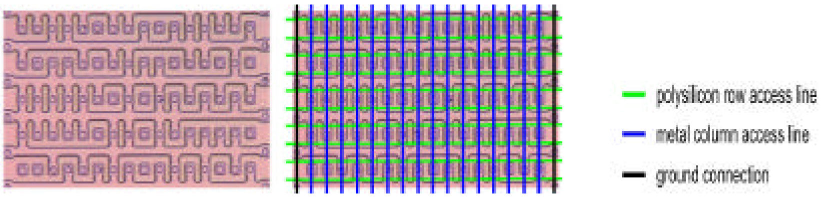
Preparation 2: Bonding into a Test Package

A manual bonding station establishes reliable contacts to the supply, communication, and test pads of the microprocessor using ultrasonic welding of a fine aluminium wire.



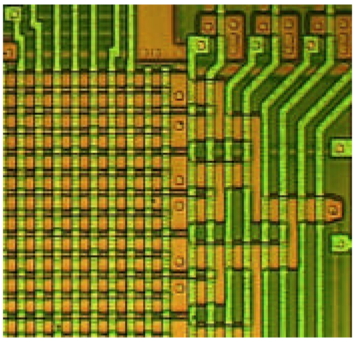
Optical Reverse - Engineering of VLSI Circuits

Confocal microscopes represent the different chip layers in different colors. In the right image, the metal interconnects have been removed with hydrofluoric acid. Both images together can be read almost as easily as a circuit diagram.

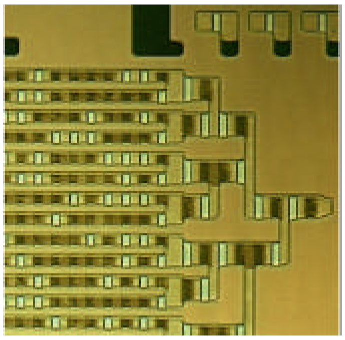


Optical Access to Diffusion Layer ROM Content

After all covering layers including the surrounding field oxide have been removed with hydrofluoric acid, the shape of the now visible diffusion areas will reveal the ROM content (here 16x10 bits).



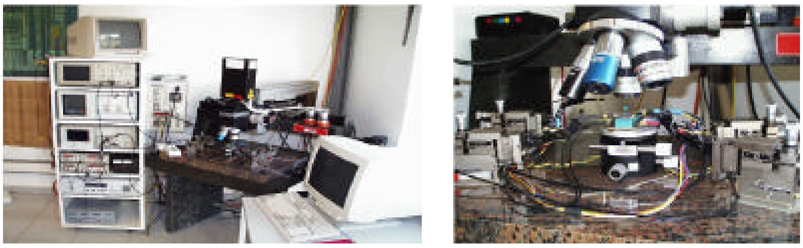
View of ROM with polysilicon intact



Diffusion layer after crystallographic etch

Optical Reconstruction of Ion Implantation ROM Content

This type of ROM does not reveal the bit pattern in the shape of the diffusion areas, but a crystallographic staining technique (Dash etchand) that etches doped regions faster
than undoped regions will still show the ROM bits.

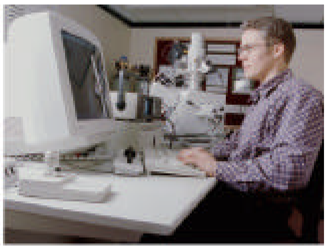


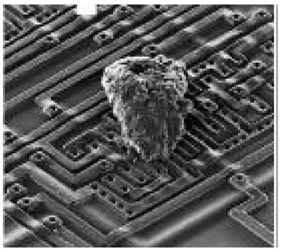
Access to CPU Bus via Laser Depassivation and Microprobing

A complete microprobing station consisting of a micro-scope (Mitutoyo FS-60), laser cutter (New Wave QuikLaze), four micropositioners (Karl Suss), CCD camera, PC with DSP card for card protocol interface handling and data acquisition, oscilloscope, pattern generator, power supply, logic analyzer, etc.

Microprobing Access to All Memory Locations

Passively monitoring and recording all memory- bus accesses might not be sufficient to attack all applications. Carefully designed smartcard software makes it difficult to trigger memory accesses to all secrets in a laboratory.





Focused Ion Beam Workstations for IC Modification

Focused ion- beam machines make high- resolution images of chip structures and allow us to both remove and deposit materials (metal and insulators) with 0.01 µm resolution. Gallium ions are accelerated with 30 kV and process gases like iodine or an organic compound are injected near the target location.

B. Details of Non- invasive attacks

B-1. Analog Circuit Characteristics Allow Non- Invasive Attacks

Delays vary along various signal paths (RC and gate count)

Static current consumption extremely small

Significant short- circuit when SRAM cell changes state

Brief short- circuit when CMOS gate changes state

Flip- flops sample input during a short interval and compare it with the supply voltage levels

Careful security reviews must usually include detailed analog VLSI simulations. Smartcard security cannot be achieved by studying only a digital abstraction of the processor design.

Smartcard processors are particularly vulnerable to non-invasive attacks, because the attacker has full control over the power and clock supply lines. Larger security modules can be equipped with backup batteries, electromagnetic shielding, low-pass filters, and autonomous clock signal generators to reduce many of the risks to which smartcard processors are particularly exposed

B-2. Glitch Attacks

In a glitch attack, we deliberately generate a mal-function that causes one or more flipflops to adopt the wrong state. The aim is usually to replace a single critical machine instruction with an almost arbitrary other one. Glitches can also aim to corrupt data values as they are transferred between registers and memory. Of the many fault-induction attack techniques on smartcards, glitch attacks are the ones most useful in practical attacks

We are currently aware of three techniques for creating fairly reliable malfunctions that affect only a very small number of machine cycles in smartcard processors: clock signal transients, power supply transients, and external electrical field transients

B-3. Current Analysis

Using a 10-15 Ωresistor in the power supply, we can measure with an analog/digital converter the fluctuations in the current consumed by the card.

Drivers on the address and data bus often consist of up to a dozen parallel inverters per bit, each driving a large capacitive load. They cause a significant power-supply short circuit during any transition. Changing a single bus line from 0 to 1 or vice versa can contribute in the order of 0.5-1 mA to the total current at the right time after the clock edge, such that a 12-bit ADC is sufficient to estimate the number

of bus bits that change at a time
SRAM write operations often generate the strongest signals. By averaging the current measurements of many repeated identical transactions, we can even identify smaller signals that are not transmitted over the bus. Signals such as carry bit states are of special interest, because many cryptographic key scheduling algorithms use shift operations that single out individual key bits in the carry flag. Even if the status bit changes cannot be measured directly, they often cause changes in the instruction sequencer or microcode execution, which then cause a clear change in the power consumption

③ Countermeasures

(i) *Randomized Clock Signal*

Many non-invasive techniques require the attacker to predict the time at which a certain instruction is executed. A strictly deterministic processor that executes the same instruction c clock cycles after each reset if provided with the same input at every cycle-makes this easy. Predictable processor behavior also simplifies the use of protocol reaction times as a covert channel
The obvious countermeasure is to insert random- time delays between any observable reaction and critical operations that might be subject to an at- tack. If the serial port were the only observable channel, then a few random delay routine calls con- trolled by a hardware noise source would seem sufficient. However, since attackers can use cross-correlation techniques to determine in real-time from the current fluctuations the currently executed instruction sequence, almost every instruction be- comes an observable reaction, and a few localized delays will not suffice.
We therefore strongly recommend introducing timing randomness at the clock-cycle level. A random bit-sequence generator that is operated with the external clock signal should be used to generate an internal clock signal. This will effectively reduce the clock frequency by a factor of four, but most smartcards anyway reduce internally the 3.5 MHz provided for contact cards and the 13 MHz provided for contact-less cards.

Hardware random bit generators (usually the amplified thermal noise of transistors) are not always 8.good at producing uniform output statistics at high bit rates, therefore their output should be smoothed with an additional simple pseudo-random bit generator.

The probability that n clock cycles have been executed by a card with a randomized clock signal after c clock cycles have been applied can be described as a binomial distribution: So for instance after we have sent 1000 clock cycles to the smartcard, we can be fairly sure that between 200 and 300 of them have been executed. This distribution can be used to verify that safety margins for timing-critical algorithms such as the timely delivery of a pay-TV control word are met with sufficiently high probability

Only the clock signals of circuitry such as the serial port and timer need to be supplied directly with the external clock signal, all other processor parts can be driven from the randomized clock

A lack of switching transients during the inactive periods of the random clock could allow the attacker to reconstruct the internal clock signal from the consumed current. It is therefore essential that the processor show a characteristic current activity even during the delay phases of the random clock. This can be accomplished by driving the bus with random values or by causing the microcode to perform a write access to an unused RAM location while the processor is inactive.

(ii) Randomized Multithreading

To introduce even more non-determinism into the execution of algorithms, it is conceivable to design a multithreaded processor architecture that schedules the processor by hardware between two or more threads of execution randomly at a per- instruction level. Such a processor would have multiple copies of all registers (accumulator, program counter, instruction register, etc.), and the combinatorial logic would be used in a randomly alternating way to progress the execution state of the threads represented by these respective register sets.

The simple 8-bit microcontrollers of smartcards do not feature pipelines and caches and the entire state is defined only by a very small number of registers that can relatively easily be duplicated. The only other necessary addition would be new machine instructions to fork off the other thread(s) and to synchronize and terminate them. Multithreaded applications could interleave some of the many independent cryptographic operations needed in security protocols. For the remaining time, the auxiliary threads could just perform random encryptions in order to generate a realistic current pattern during the delay periods of the main application

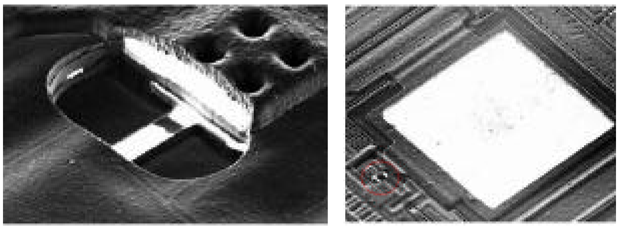
(iii) Robust Low-frequency Sensor

Bus-observation by e-beam testing becomes much easier when the processor can be clocked with only a few kilohertz, and therefore a low-frequency alarm is commonly found on smartcard processors. How- ever, simple high-pass or low-pass RC elements are not sufficient, because by carefully varying the duty cycle of the clock signal, we can often prevent the activation of such detectors. A good low-frequency sensor must trigger if no clock edge has been seen for longer than some specified time limit (e.g., 0.5 μs)

In this case, the processor must not only be reset immediately, but all bus lines and registers also have to be grounded quickly, as otherwise the values on them would remain visible sufficiently long for a voltage-contrast scan.

Laser cutting or FIB editing the RC element can quite easily disable even such carefully designed low-frequency detectors. To prevent such simple tampering, we suggest that an intrinsic self-test be built into the detector. Any attempt to tamper with the sensor should result in the malfunction of the en- tire processor. We have designed such a circuit that tests the sensor during a required step in the nor- mal reset sequence. External resets are not directly forwarded to the internal reset lines, but only cause an additional fr equency divider to reduce the clock signal. This then activates the low-frequency detector, which then activates the internal reset lines, which finally deactivate the divider. The processor has now passed the sensor test and can start normal operation. The processor is designed such that it will not run after a power up without a proper internal reset. A large number of FIB edits would be necessary to make the processor operational without the frequency sensor being active

Other sensor defenses against invasive attacks should equally be embedded into the normal operation of the processor, or merely merely destroying their signal or power supply connections will easily circumvent them.



Blown polysilicon fuse near test pad (Motorola)

(iv) Destruction of Test Circuitry

Microcontroller production has a yield of typically around 95%, so each chip has to be thoroughly tested after production. Test engineers like microprobing attackers have to get full access to a complex circuit with a small number of probing needles. They add special test circuitry to each chip, which is usually a parallel/serial converter for direct access to many bus and control lines. This test logic is accessible via small probing pads or multiplexed via the normal I/O pads. On normal microcontrollers, the test circuitry remains fully intact after the test. In smartcard processors, it is common practice to blow polysilicon fuses that disable access to these test circuits. However, attackers have been able to reconnect these with microprobes or FIB editing, and then simply used the test logic to dump the en- tire memory content

Therefore, it is essential that any test circuitry is not only slightly disabled but also structurally destroyed by the manufacturer. One approach is to place the test interface for chip n onto the area of chip n + 1 on the wafer, such that cutting the wafer into dies severs all its parallel connections. A wafer saw usually removes a 80-200 µm wide area that often only contains a few process control transistors. Locating essential parts of the test logic in these cut areas would eliminate any possibility that even substantial FIB edits could reactivate it

(v) Restricted Program Counter

Abusing the program counter as an address pat- tern generator significantly simplifies reading out the entire memory via microprobing or e-beam testing.

Separate watchdog counters that reset the processor if no jump, call, or return instruction is executed for a number of cycles would either require many transistors or are too easily disabled.

Instead, we recommend simply not providing a program counter that can run over the entire address space. A 16-bit program counter can easily be replaced with the combination of a say 7-bit off- set counter O and a 16-bit segment register S, such that the accessed address is S + O. Instead of over-flowing, the offset counter resets the processor after reaching its maximum value. Every jump, call, or re- turn instruction writes the destination address into S and resets O to zero. The processor will now be completely unable to execute more than 127 bytes of machine code without a jump, and no simple FIB edit will change this. A simple machine-code postprocessor must be used by the programmer to insert jumps to the next address wherever unconditional branches are more than 127 bytes apart

With the program counter now being unavailable, attackers will next try to increase the number of iterations in software loops that read data arrays from memory to get access to all bytes. This can for instance be achieved with a microprobe that performs a glitch attack directly on a bus-line. Programmers who want to use 16-bit counters in loops should keep this in mind

(vi) Top-layer Sensor Meshes

Additional metallization layers that form a sensor mesh above the actual circuit and that do not carry any critical signals remain one of the more effective annoyances to microprobing attackers. They are found in a few smartcard CPUs such as the ST16SF48A or in some battery-buffered SRAM security processors such as the DS5002FPM and DS1954.

A sensor mesh in which all paths are continuously monitored for interruptions and short-circuits while power is available prevents laser cutter or selective etching access to the bus lines. Mesh alarms should immediately trigger a countermeasure such as zeroizing the non-volatile memory. In addition, such meshes make the preparation of lower layers more difficult, because since the etch progresses unevenly through them, their pattern remains visible in the layers below and therefore they complicate automatic layout reconstruction. Finally, a mesh on top of a polished oxide layer hides lower layers, which makes navigation on the chip surface for probing and FIB editing more tedious

The implementations of sensor meshes in fielded products however show a number of quite surprising design flaws that significantly reduce the protection. The most significant flaw is that a mesh breach will only set a ag in a status register and that zeroization of the memory is left completely to the application software. We noted in Section 2.1.4 that a common read-out technique involves severely disabling the instruction decoder; therefore software checks for invasive attacks are of little use

A well-designed mesh can make attacks by manual microprobing alone rather difficult, and more sophisticated FIB editing procedures will be required to bypass it. Several techniques can be applied here

The resolution of FIB drilling is much smaller than the mesh line spacing, therefore it is no problem to establish contact through three or more metal layers and make deeply buried signals accessible for microprobing via a platinum or tungsten pad on top of the passivation layer. Alternatively, it is also possible to etch a larger window into the mesh and then reconnect the loose ends with FIB metal deposits around it

④ Summary and Conclusions

Invasive techniques break all currently available smartcards and have led to continued conditional access smartcard piracy since 1994.

Non- invasive attacks (glitching, current analysis) are the main concern only in tamper- evidence applications (banking, signatures), because microprobing is generally the far easier and more universal type of attack.

Examples for lowest cost countermeasures that are not yet implemented widely or in effective ways:

tamper- resistant sensors
top- layer sensor mesh
randomized clock

instruction multi- threading
constant- current regulators
destruction of test circuits
loosely coupled clock PLL

Smartcard form probably unsuitable for strong tamper- resistance requirements (conditional access, copy protection), better use battery-backed SRAM

Extremely careful engineering might lead to high tamper- evidence assurance for smartcards one day (for banking, authentication, digital signatures)

2.2) Protocol security; SET

① Introduction of SET

There is no question that electronic commerce, as exemplified by the popularity of the Internet, is going to have an enormous impact on the financial services industry. No financial institution will be left unaffected by the explosion of electronic commerce.

The most common Internet common Internet payment method for the B2C E-commerce is credit cards. However, while customers are sending credit information such as name, card number, and expiration date, these information can be exposed to some intruders. Thus, security is becoming the concern of customers as well as buyers. In buyers case, they also want to make sure that no one change the orders and that they are connected to the one they intend to connect, not an imposer.

The Internet is changing the way we access and purchase information, communicate and pay for services, and acquire and pay for goods. Financial services such as bill payment, brokerage, insurance, and home banking are now or soon will be available over the Net.

Nowadays, most companies are providing security and privacy using Secure Socket Layer (SSL). However, this protocol does not provide customers all the protection they could have.

Thus, VISA and MasterCard have jointly developed a more secure protocol called Secure Electronic Transaction (SET). In SET protocol, a special software mechanism called ‘digital wallet’ is adopted to provide a certificate which offers theoretically perfect protocol. However, SET did not propagate as fast as most people expected because of its complexity, slow response time and the need to install the digital wallet in the customer’s computer. Only 1 percent of electronic businesses plans to migrate to SET by 1999.

Then a question arise. Is SET a failure? The answer seems to be YES at this moment.

But, MasterCard say that the digital wallet would be distributed as embedded software in the next version of Windows, the most popular operating system. In addition, situations will be quite different when smart cards that stores the certificates are released and applied to the market with cheaper, better and faster solutions for SET.

② How SET works?

The fundamental principle that guided SET architects was to secure bank card transactions over the Internet without modifying existing banking circuits for authorization and remote collection.

To allow the scheme to work on a worldwide level, it is necessary to have following participants playing a different role in the Protocol. Thus, interoperability between these entities are very critical.

Card holder : Consumers or corporate purchasers who interact with merchants with personal computers. A cardholder uses a payment card that has been issued by an Issuer. The payment card account information must be kept in secret by SET protocol.

Issuer : A financial institution that establishes an account for a cardholder and issues the payment card. The Issuer guarantees payment for authorized transactions using the payment card in accordance with payment card brand regulations and local legislation.

Merchant : A merchant offers goods for sale or provides services in exchange for payment. A merchant that accepts payment cards must have a relationship with an Acquirer.

Acquirer : A financial institution that establishes an account with a merchant and processes payment card authorizations and payments.

Payment gateway : A device operated by an Acquirer or a designated third party that processes merchant payment messages, including payment instructions from cardholders. It also plays a role of managing the border between the Internet and the network of bank cards.

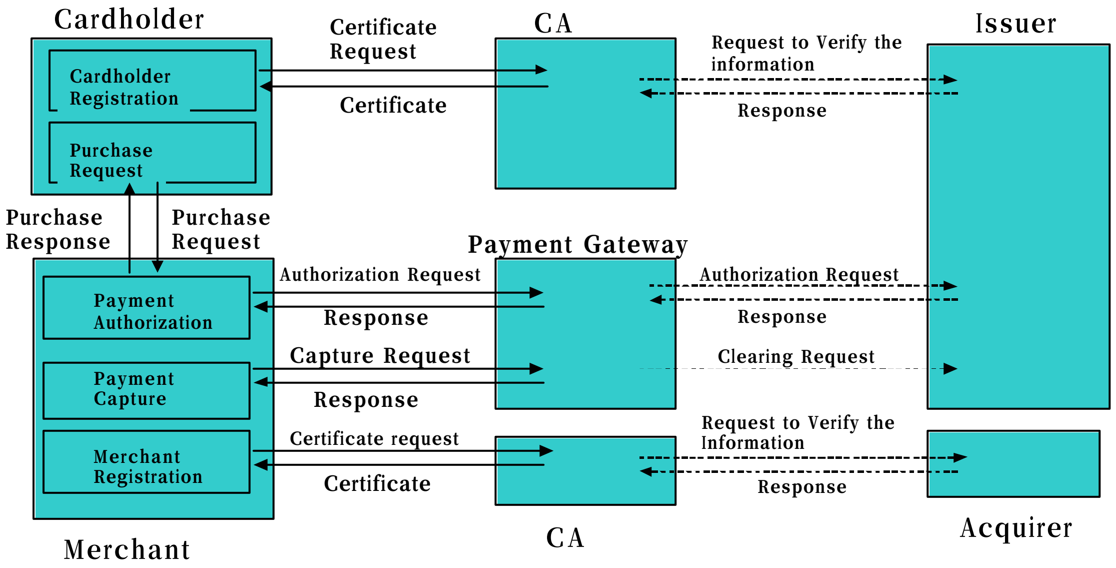
Certificate Authority (CA) : A trusted third party organization or company that issues digital certificates. The CA is responsible for guaranteeing that the individuals or organizations granted these unique certificates are, in fact, who they claim to be. Digital certificate create a trust chain throughout the transaction, verifying cardholder and merchant validity, a process unparalleled by other Internet security solutions.

All transactions between these participants should also be made on the following security requirements and transaction interoperability.

1. Confidentiality of payment information and order information transmitted along with the payment information.
2. Integrity of all transmitted data.
3. Authentication certifying that a cardholder is a legitimate user of a payment card account.
4. Authentication certifying that a merchant can accept payment card transactions through its relationship with an acquiring financial institution.
5. Best security practices and system design techniques protecting all legitimate parties in an electronic commerce transaction.
6. Protocol that neither depends on transport security mechanisms nor prevents their use.
7. Interoperability among software and network providers.

Now, let's take a look at how each secure transaction proceeds satisfying the security requirements.

Use of SET Protocol



< MAIN MESSAGES IN SET >

As shown in the picture above, SET is a transaction oriented protocol and functions in the REQUEST/RESPOND mode. And this SET transactions provide the following services and procedures.

1) Registration of the cardholders and the merchants with the certification authority
2) Delivery of certificates to cardholders and merchants
3) Authentication, confidentiality and integrity of the purchase transactions
4) Payment authorization for each transactions.
5) Payment capture to initiate the request for the financial clearance on behalf of the merchant.

③ SET PROTOCOL IN SMART CARD.

The considerable efforts are spent to adapt the SET protocol to smart card. For example, EMV(EuroPay, MasterCard, Visa) specifications, have built on the ISO standards to define multi-application Smart cards. At the EMV Executive Meeting, (September 1-2 1998, Purchase, New York) EuroPay International, MasterCard International and Visa International (EMV) agreed upon a minimum set of data elements to be used in the authorization messages and in the clearing messages for EMV Chip card transactions.

In addition, joint operation model of SSL and SET care also built to reduce the computational loads that SET imposes on client and merchant system. The new proposed architecture aims at simplifying the certification procedure to reduce the cost of cryptographic process while still protecting the financial data of the client.

While a software called 'digital wallet' that resides on the user's computer is responsible for carrying and retrieving the credentials that are stored on the user's computer in SET protocol, the C-SET architecture allows the SET certificates to be stored in the smart card. Also, the cardholder must enter a confidential code in a secure card reader to authorize a payment.

Thus, in this C-SET architecture, the different system support must be implemented as follows.

1) The secure card reader or Pin-pad reader is required to resemble calculator with a keyboard and a screen, and include software and a cryptographic module. Since the card holder enters the PIN Number, the reader must be tamper resistant and must not store any secrets.
2) C-SET registration server is needed to award C-SET certificates to the participants.
3) C-SET software distribution server is required to assure the download or the distribution of the secure software and its installation. This approach allows the automatic integration of other applications as they become available, or as new multi-application cards of the EMV type become available.

The main differences between SET and C-SET architecture comes from its certification procedures of them. These are ;

1) The cardholder is asked to insert its card and enter the PIN code during registration, which verifies the end to end authentication procedure.
2) The certificate is written on the smart card and not on the hard disk of the user's computer as in SET.
3) A-Pin-pad reader of an accredited brand and model is necessary to complete the cardholders certification.

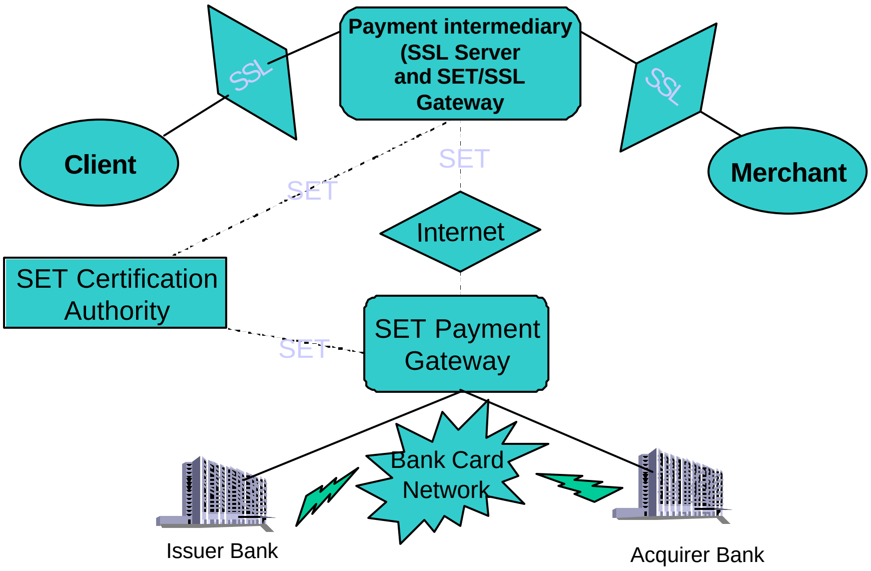
④ Effort to make better performing SET protocol.

Looking at server performance as a static situation is clearly the wrong thing to do since supporting technologies and new models are continuously being introduced. In this part, several expected improvement in performance will be introduced.

I. HYBRID SSL/SET ARCHITECTURE

This part introduces the hybrid payment architecture that combines the security advantages of SET with the simplicity of SSL in card transactions.

HYBRID SSL/SET ARCHITECTURE



The picture above presents the hybrid SET/SSL model. The payment intermediary is introduced playing a roles of SSL server with respect to the client and the merchant, Web host for the merchant, and SSL certification authority for both.

The use of payment intermediary reduces by an order of magnitude the cryptographic load on both the client and the merchant because SSL requires less computational demand than SET due to the off-load that client and merchant get from SET procedures. That is to say, the authentications process needed for each transaction in SET adding delays and computational cost can be significantly reduced.

The main drawback of this hybrid SET/SSL is that the client does not have the control over the certificate that was issued in his or her name because it is stored by the intermediary.

Nevertheless, this hybrid architecture seems to be useful for the small businesses or these who deal with small amounts due to the low cost and ease of the registration. In addition, the intermediary will be able to settle arbitrate disputes providing that all traces of the communications with the time-stemp. This is possible since all merchants and clients are supposed to go through the intermediary for every transactions.

Using this hybrid architecture, it is possible to reduce the computational load and accomplish the better performance on payment.

II. Symmetric multiprocessing (SMP) CPU scaling

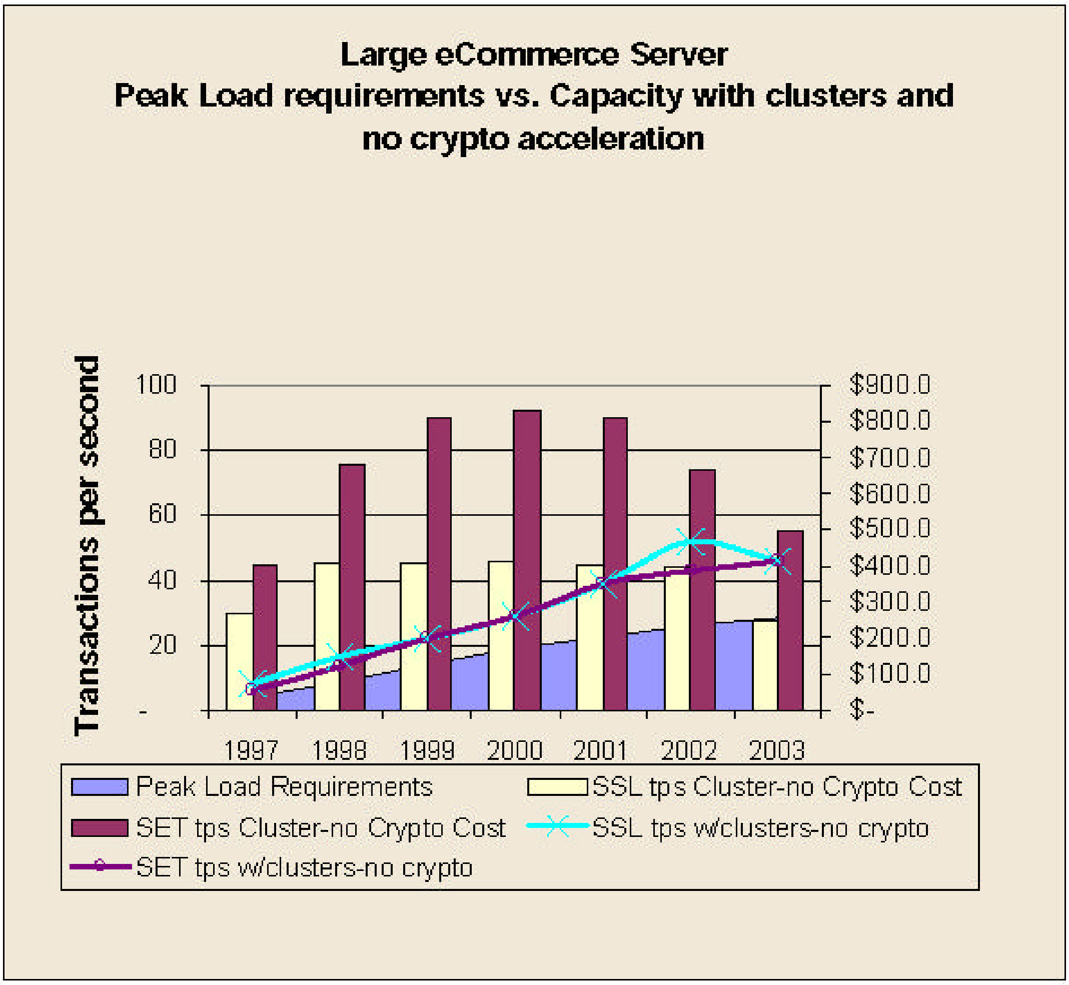
It is possible that the operating system(OS) dedicates individual processors to support cryptography as more processors are added to a system. The OS allocates individual CPU functionality to application and other processes, especially in Symmetric multiprocessing system.

III. Clustering

It is also very important to support failure handling mechanism of the system in order to improve the performance of the system as well as protocol. In order to achieve this

goal, the application load is shared between mutiple mutiprocessor CPUs, linked together into a cluster in most large sites. In case of an equipment failure, the other systems in the cluster will absorb the load until the failing system can be brought back online. In these environments, the additional systems provide the ability to spread the transaction load over multiple systems in the same cluster.

Picture > Cost of performance with clustered systems



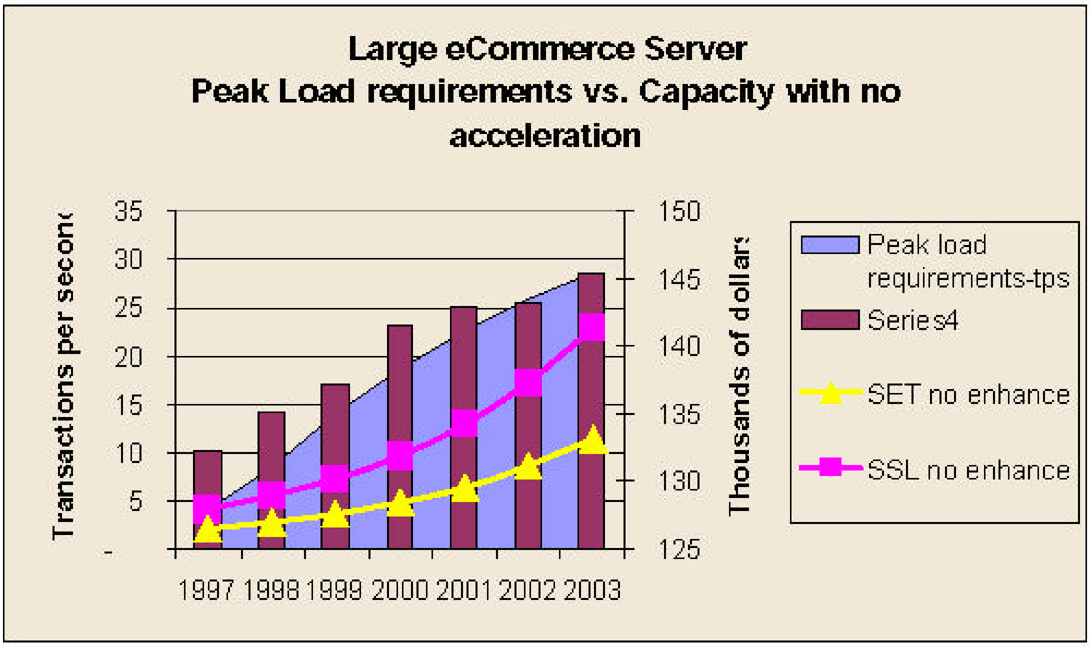
Source: GartnerGroup

This picture shows, on the left axis, the performance that can be achieved with SSL and SET by using a set of systems clustered together, and, on the right axis, the cost difference of SET over SSL in enhancing performance this way. Each configuration requires at least a 2-system cluster for SSL and a 6-system cluster for SET in 1999 through 2001.

IV. Cryptographic accelerators

New device called cryptographic accelerators are introduced in the market to improve the performance of arithmetic computation. Cryptographic accelerators means ‘special-purpose dedicated hardware units’designed to support off-load cryptographic operations from the CPU. Unlike 32-bit CPUs, which are inefficient at 1024-bit arithmetic, the processors in cryptographic accelerator hardware are designed specifically for long number arithmetic. The correct analogy is to think of cryptographic
accelerators like the graphics accelerators used in nearly every PC today. Graphics accelerators perform high-speed functions that offload the CPU and result in a system with substantially increased overall performance. Similarly, in systems with a substantial cryptographic load, cryptographic accelerators offload the CPU for much better overall system performance. Now, let's take a look at the picture below.
This picture shows the unaccelerated performance of our large e-commerce server configuration, supporting either SET or SSL, against the anticipated peak demand.

Picture > Performance without acceleration.



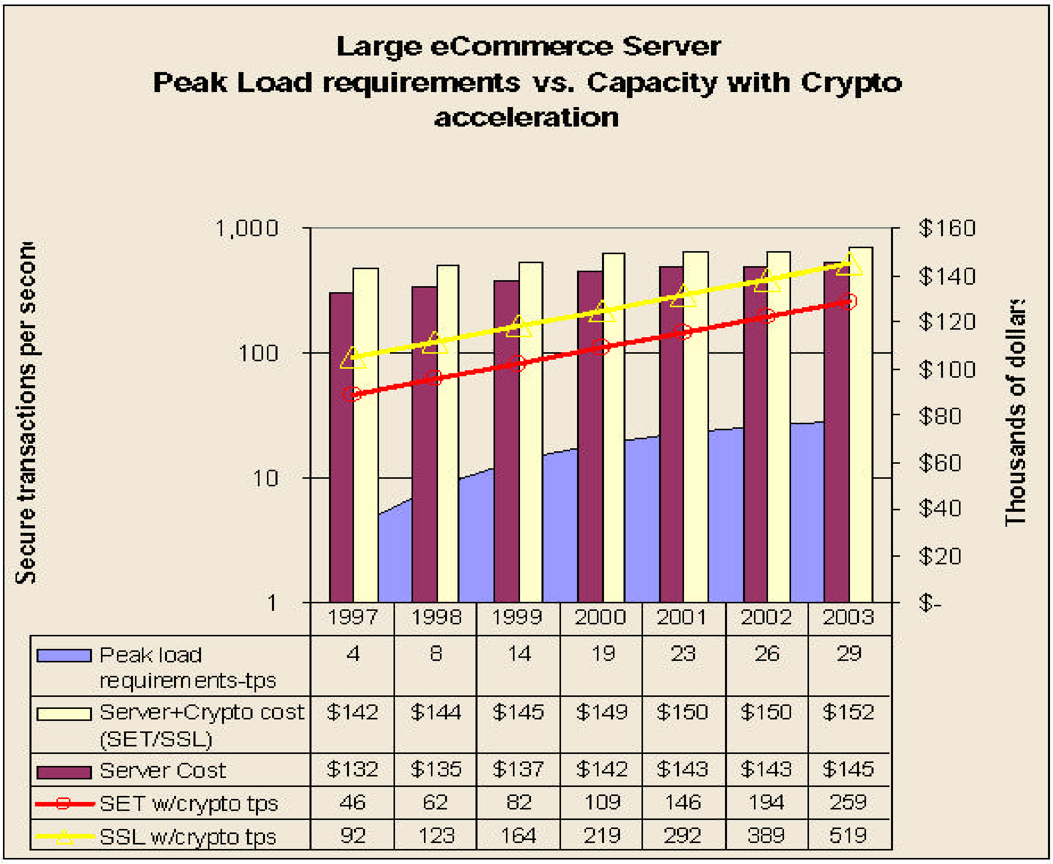
Source: GartnerGroup

The incline in the lines tells the increase in the server’s performance over time due to processor improvements (Moore’s law). Clearly, the server is unable to meet the demands of the applications it is running and support cryptographic operations at the same time. Cryptography based on either SET or SSL is too much of a load for the server. This server is a 16 CPU system costing in excess of $100,000 and it is unable to sustain the required load, we need to add additional resources.

In the next section we show the effect of adding a high-end cryptographic accelerator, costing in the neighborhood of $10,000 (although we expect this price to decline over time), but still a small portion of the price of the base system. For smaller configurations, lower performance and less expensive accelerators are available.

Now, then let’s take another picture below.
This picture shows the capacity of the same server with a single cryptographic accelerator. Note that this chart has a log scale on the left hand axis.

Picture > Capacity with Cryptographic Acceleration



	1997	1998	1999	2000	2001	2002	2003
🟦 Peak load requirements-tps	4	8	14	19	23	26	29
□ Server+Crypto cost (SET/SSL)	$142	$144	$145	$149	$150	$150	$152
■ Server Cost	$132	$135	$137	$142	$143	$143	$145
—o— SET w/crypto tps	46	62	82	109	146	194	259
—△— SSL w/crypto tps	92	123	164	219	292	389	519

Source: GartnerGroup

Now, it is clear to see that the server is fully capable of handling anticipated peak loads with both SET and SSL protocols with the addition of an accelerator. In addition, the capacity of both SET and SSL now exceeds the peak load requirements by a comfortable margin, reducing the risk of server overloading. Comparisons on the right hand axis show the cost of the server with the cost of the cryptographic graphic accelerator versus the cost of the server alone. Note that the difference is small for a substantial increase in performance.

V. Elliptical curve cryptography (ECC)

ECC is an encryption algorithm that provides equivalent security with a much smaller key size. In order to understand the how this can be achieved, it is better to see slightly more details about advantages in details.

The advantages of ECC in a constrained environment are ;

1. Shorter keys - 161-bit ECC is about 1024-bit RSA/DSA.
2. Shorter signatures ? 322-bit ECC is about 1024-bit RSA.

3. Shorter certificates ? 256-byte RSA or 168-byte DSA is about 62-byte ECC.
4. Simple generation of key pair, given a valid set of domain parameters.
5. Bullet certificate ? implicit certificate from one CA, 21-byte ECC.
6. ECSM ? combined message encryption and signature.

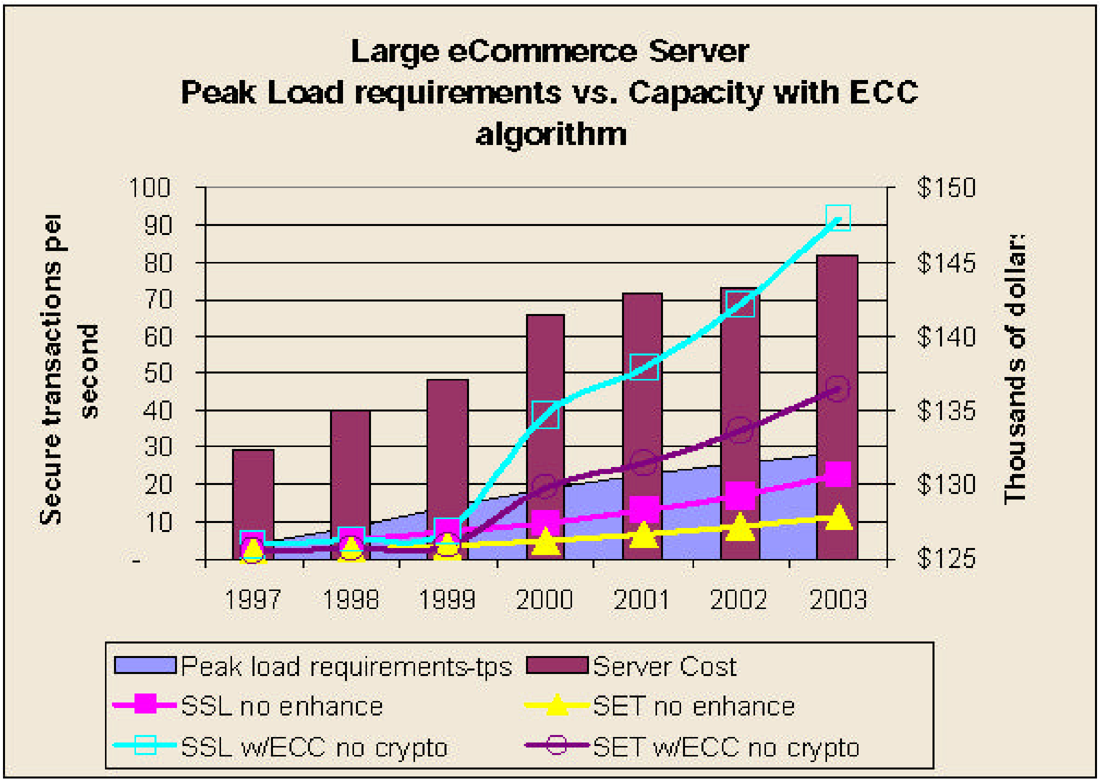
The Advantages of ECC in a high-security environment include the following:

1. Easy to achieve the security attribute of forward secrecy.
2. Simple mapping of symmetric key size to appropriate ECC key size.
3. Reasonable ECC key sizes to protect larger AES key sizes.
4. Proven equivalence between the ECDLP and the ECDHP.
5. Improved ECC public key performance via helper fields in a certificate with no additional risk.
6. A single-bit error in a signature calculation does not reveal ECC private key.
7. ECC private key is an ideal secret, a random number of a certain size.
8. ECC private key is resilient to partial key exposure, leaking information about the private key reduces the key space by the amount of information leaked.
9. ECC public key validation is ideal, validation is offline and is 100% (successful validation shows that an associated private key can logically exist, yet gives no information about the value of the associated private key).
10. Straightforward generation of a multi-party ECC private key.
11. Simple generation of a valid ECC public key where it can be publicly audited that no one knows the associated private key without doing an honest attack.
12. Straightforward detection of a "chilling" attack on random number generator.
13. Future resilient to the discovery of a new special-purpose attack on ECC.
14. Future resilient as a component (with RSA) of a two-algorithm signature that addresses fears of an advance in a general-purpose attack leading to catastrophic algorithm failure.

As you can see, the effect of adopting ECC is the greatly increase speed. However, this technology has not been widely deployed, and as such is not as well proven as the other technologies included here. Where we include the effects of ECC, we are assuming that it becomes widely available in 2000. Note that this date is subject to substantial variation. Availability of ECC is by no means assured. In contrast, hardware cryptographic accelerators are available today, and work effectively with today's cryptographic standards at a cost that is a small portion of the overall system cost.

Now, let's take a look at the effect of ECC algorithm with a picture.
This picture shows the effect of an assumed introduction of ECC in 2000.

Picture > The effect of ECC algorithm.



Source: GartnerGroup

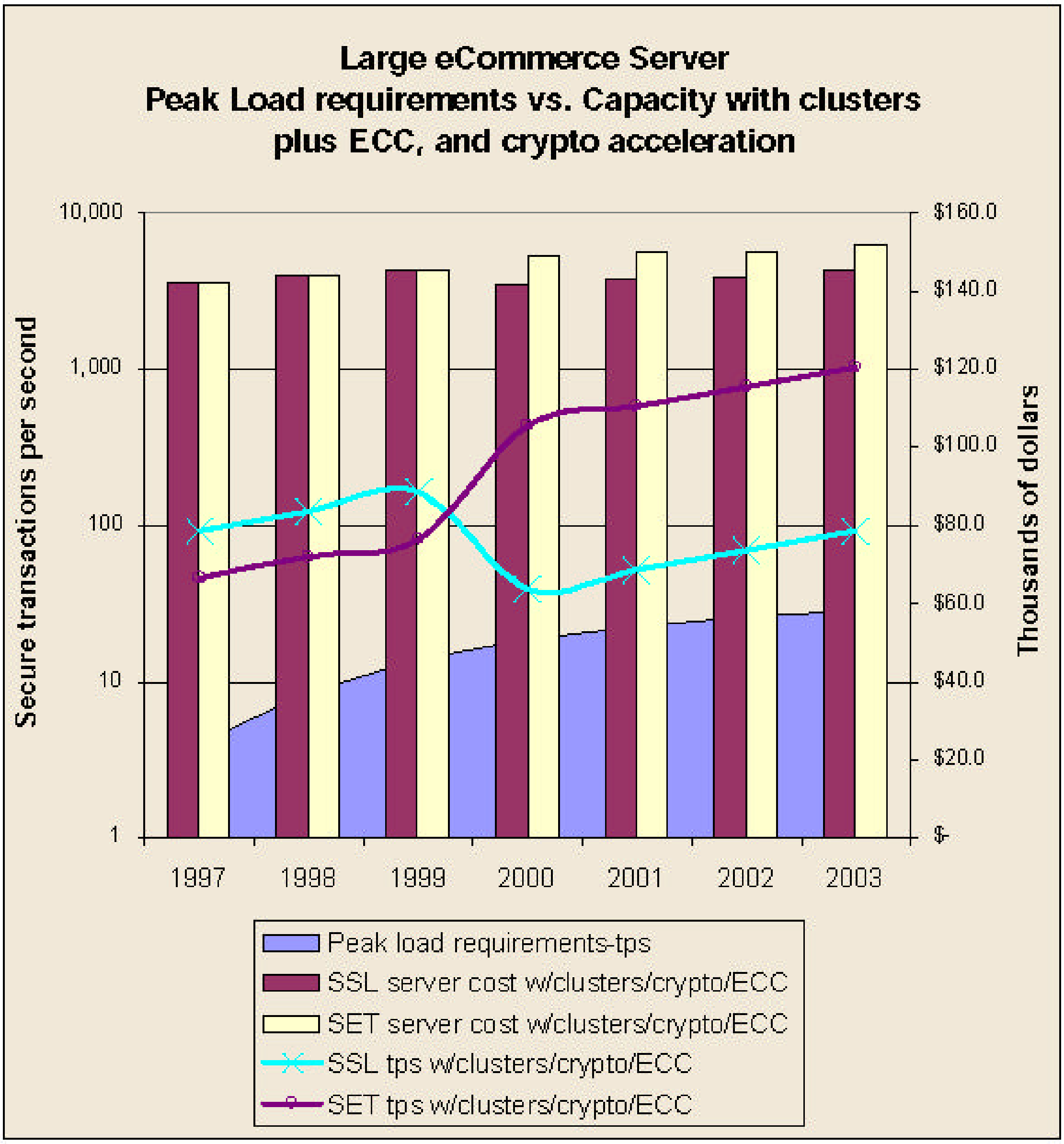
Note that servers is now able to handle the necessary load with very little margins, while provides servers based on SSL with significant peak margin. The reason is that ECC can provide about a 400 percent performance improvement on the conservative assumption. One very significant point is that there was no extra cost over the existing server, a change in the software as ECC's vendors claim a substantially better ratio of 1,000 percent.

VI. Performance improvement in overall.

As shown above, new architecture is being introduced and more powerful computing devices and algorithms are being continuously improved.

By using such mechanisms introduced, very significant improvement can be accomplished shortening the period of market penetration of SET protocol.

Now, the picture below shows the combined effect of ECC, clustered systems if needed, and the use of cryptographic accelerators on the costs to support SET over SSL.



Source: GartnerGroup

As you can see, the performance has been significantly improved.

In addition to the technologies introduced above, new encryption technology called ‘random key stream (RKS)’ is able to provide significant performance advantages.
If what the developer claims turns out to be true, it will certainly have a role in the secure server market. However, the technology will not be in effect until it is evaluated and deployed. Now, this technology has received some criticism

regarding the possibility of deployment.

2.3) Authentication security; Biometric

To make more secure payment system using smart card, we suggest combining biometrics method into smart card with strong cryptosystem.

The oldest and most widely accepted biometric is the fingerprint. The tip of every finger has a characteristic called ``friction ridges". While generally similar, no two-friction ridges are exactly the same. By imaging the ridges of the fingertips, we get the fingerprint.

Most implementations of fingerprint biometrics create a template from the original image, which is a fraction of the size of the original fingerprint image. This template can be used only to compare the fingerprint against other templates, and it cannot be used to recreate the original image. Template implementations of biometrics fit well with smart cards for two reasons. First, they usually range from 100 to 600 bytes in size and can easily fit on a smart card. Second, you don't have to worry about an attacker reproducing your fingerprints from your templates and using them to impersonate you. Biometrics can aid authentication. Here is a rough outline of the procedure for authenticating yourself to a computer application:

1. Insert your smart card into a reader. The smart card contains your cryptographic keys and biometric fingerprint data.
2. Enter your shared-secret PIN (or password), in order to unlock the digital representation of your fingerprint. In the trade, this is known as the minutia data.
3. Place your finger on the scanner. The scanned fingerprint is compared to the fingerprint data on the smart card.
4. If the data matches, the smart-card fingerprint data is converted into a number and combined with the smart-card secret PIN (retrieved in Step 2) and used as a symmetric cryptographic key to decrypt the private key.
5. A nonce (random number) is passed from the computer application to the smart card.
6. The private key on the smart card is used to encrypt the nonce and pass

it back to the application.
7. The application verifies that a certified public key obtained from the network-based directory service or from the card does, in fact, decrypt the encrypted message from the card and reveals the same nonce that was originally passed to the card.

This process irrefutably authenticates the person presenting the card as the same person to whom the cryptographic keys belong and provides the necessary tight binding between the cryptographic key storage and the authorized user of the cryptographic keys.

4. Conclusion and comment

So far we look at the advantages and vulnerability of smart card and present how to improve security system at various aspects in order for the smart card to be appealed in market.

The most important thing is to make most secure payment system as well as convenient system for users. To fit these purpose, we suggest the new model of smart card in three aspects of security such as physical security, protocol security and authentication security.

The new model consists of physically well designed suitable for its purpose and technology and temper-resisted card. It also contains SET protocol, it may use version 2.0 which can provide smart card but for reducing the transaction time, it should need elliptic curve cryptosystem and for more secure authentication, add biometric technology to smart card.

As a matter of fact, there is any fantastic electronic payment system using smart card that satisfies all the requirement of payment system.

In this paper, we would like to put worthwhile meaning to suggest the new ideal model of payment system using smart card that fit to be appealed in the market.

5. Reference

✍✍Electronic Commerce, A managerial Perspective by Efraim Turban, Jae Lee, David King, H. Michael Chung

✍✍Protocols for Secure Electronic Commerce by Mostafa Hashem Sherif. Series Edifor in Chief : Saba Zamir.

✍✍암호이론과 보안 (대영사) 박창섭 저.

✍✍SET Comparative Performance Analysis by Chris Le Tocq Steve Young (Gartner Consulting ś White paper)

✍✍www.SetCo.org The consortium of SET

✍✍Design Principles for Tamper-Resistant Smartcard Processors ;
Oliver Kommerling(Advanced Digital Security Research) and Markus G. (Kuhn University of Cambridge Computer Laboratory)

✍✍http://www2.linuxjournal.com/lj-issues/issue59/3013.html

✍✍http://www.smartcard.ust.hk/smartcards/main.htm

✍✍http://home.hkstar.com/~alanchan/papers/smartCardSecurity/

✍✍Smart Cards; Enabling Smart Commerce in the Digital Age, CREC/KPMG WHITE PAPER, May 1998, KPMG and center for research in Electronic Commerce, The University of Texas, Austin by Soon-Yong Choi and Andrew B. Whinston

✍✍www.thestandard.com

✍✍www.techweb.com