

ROLES AND RESPONSIBILITIES IN ETHICAL BANKING

P.Devika Rani

Lecturer, Dept of Computer Science, K.B.N College, Vijayawada
devikaranipn@gmail.com

Abstract— It is the objective of this paper to give an introduction to the notion of what is often described as “ethical, sustainable, social, alternative, development or solidarity” banking and finance. The common bond and specificity of this type of financial institutions is that they are characterized by values driven impulses and practices at the core of their business while values are poorly developed in the field of mainstream commercial banking and finance. This paper is giving an overview of the principal, roles& responses of managers and bank differences, modern pioneers in this field and is putting them in a context, describing the nature of their initiatives and procedure of hacking of a credit card. This article highlights roles, responsible of banks and ethical hacking such as social banking, ethical banking, green banking, global banking, rural banking, and agricultural banking, which help in achieving sustainable development of banking and finance. For this purpose, we have gone through a series of development that are taking place in current business scenario. This paper is divided in four parts. First part discuss introduction of Ethical Banking Industry in world. Second part ethical banking principles that bank should follow third part explains about roles and responsibilities of banks and managers banking and its development. It also discusses concept of Banks. Fourth part highlights some types of hacking and a hacking procedure of credit card system Social and Ethical issues related to Banking.

Keywords-Banking industry, social and ethical banking, unethical behaviour banking, banking hacking, roles and responsibilities

I. INTRODUCTION

An Ethical bank, also known as a social, alternative, civic, or sustainable bank, is a bank concerned with the social and environmental impacts of its investments and loans.

What's the difference?

In many ways an ethical bank is exactly the same as any other bank.

It offers similar products and services, from bank accounts and credit cards to mortgages, but it differs in the way it utilises customers' money.

All ethical banks have a specific policy concerning what is and what is not an acceptable way to use a customer's money.

The most ethical banking's are:



List of Ethical Banks

* Triodos Bank, Zeist, The Netherlands (also based in the UK, Belgium, Germany and Spain) * Co-operative Bank, United Kingdom * Reliance Bank, United Kingdom * Shore Bank, USA * RSF Social Finance, San Francisco and New York, USA * hared Interest, based in the United Kingdom, investing throughout the developing and developed world * Wainwright Bank, USA * Cultura Bank, Norway * GLS bank, Germany * Ethic Bank, Germany * MagNet Community Bank, Hungary * JAK members bank, Sweden, interest-free bank * Citizens Bank, Canada * CrÃ©ditcoopÃ©ratif and NEF, France * The Alternative Bank Schweiz, Switzerland * BancaEtica, Italy

Positive screening.

In principle, the term “banking” refers to services like deposit taking and payment services. But in practice, the financial services offered by these ethical banks go beyond mere banking to include investment and insurance services. Increasingly, traditional banks are beginning to offer ethical Products as well. Ethical banks offer customers the ability to open an account and lodge their savings as a basic or time deposit. With basic deposits, customers are able to withdraw their money at any time; with time deposits, they are restricted from withdrawing their funds before a certain date. Most ethical banks have developed special saving products that seek to promote sustainable development.

For example, customers may let the interest on their savings be (partially) transferred to environmental or human rights NGOs, or to a specific environmental project. Ethical banks in turn use the deposits at their bank to make loans to

households and companies, like any other bank. However, in contrast to regular banks, the borrowers are usually screened on sustainability indicators. For example, some ethical banks particularly grant mortgage loans to properties that provide an “ecological payback,”

Ethical Banking

As mentioned before, "ethical banking" is a fairly broad term. This allows financial institutions to decide for themselves what sort of policies they wish to pursue and which principles they are willing to follow. Those principles and policies are often written down in policy documents that are available to the public and their clients. But while the banks may have policy differences, they do tend to share some common characteristics. They include:

Community involvement: The bank takes an active interest in its community's welfare and takes steps to improve it. Among other things, this can include funding affordable housing projects, providing scholarships for students in local high schools, sponsoring community events and holding seminars to educate members of the community about their services.

Sustainable practices: The bank makes an effort to apply environmentally-friendly practices whenever possible, as well as to support clients who practice those policies.

Client screenings: The bank screens its clients in order to avoid doing business with individuals, organizations and corporate entities with a history of unethical and immoral practices. For example, it may avoid doing business with a company that has a history of using child labour.

Consistent internal and external ethics: Simply put, the bank practices what it preaches. If a bank applies the same ethical centres to its internal operations as it does to its external operations. For example, if a bank is not going to do business with a company that does not offer its employees' health insurance, it cannot refuse to offer health insurance its own employees.

Examples of unethical behaviour. The implementation of institutional reforms makes it possible for the economies in transition to reduce unethical behaviour to the lowest possible level. In practice, more attention is paid to investigating the cause of impairment of ethical principles, particularly in the business world. An ethical principle is impaired if an individual undertakes the activities which do not conform to his/her standards, in order to achieve success

II. ETHICAL BANKING PRINCIPLES

Banking is no ordinary business. Banks are “special” business units which, as financial intermediaries, borrow money from savers to on-lend for productive ventures. Thus, the underlying is one of the riskiest things in the world — money and money alone.

Banks run on public trust which, in turn, is a function of ethical principles and moral values they follow. The world is witness to numerous bank failures, small and large, which could not withstand the rigour of public trust. The ethical principles that banks follow ought to be of a higher order than those followed by any other businesses.

Depositors:

A depositor saves his hard-earned money in a bank, first and foremost, for ‘safety’ and then ‘return’. By ‘safety’ we do not mean from theft or burglary alone but also safety of the intrinsic value of money. For example, if a depositor puts Rs. 100 in his bank, he will definitely get back his nominal Rs. 100 plus some interest after the contractual period.

However, economically speaking, does the value of money, in real terms, remain same over time? No. Due to inflation its real value erodes. Hence, the first ethical principle that a bank should follow with respect to its depositors is to protect the ‘real’ value of money by providing an interest rate which would eventually neutralise the impact of inflation and give a positive ‘real’ return over the contractual period.

Are Indian banks doing this at present? The answer is an unequivocal ‘no’. Recently, an RBI Deputy Governor proposed inflation-indexed bonds as a hedge against inflation. Why not inflation-indexed deposits?

The second ethical question is the protection of small depositors' money from bank failures. In our country, up to Rs. 1 lakh is insured by the DI&CGC (Deposit Insurance and Credit Guarantee Corporation).

The limit, which was revised in May 1993, has remained stubbornly static despite rise in per capita income and inflation.

Net Interest Margin:

Our bankers are ‘programmed’ to be obsessed with targets. To achieve the ‘agreed’ level of profits, they artificially keep deposit rates low and lending rates high so that NIM is maximised. Is it ethical to penalise both depositors and borrowers like this?

The RBI Governor D. Subbarao in his speech “Five Frontier Issues in Indian Banking” at BANCON 2010 had argued for “a balanced approach to bring down NIM...” Sub-PLR Lending

Until July 1, 2010, banks had got into the unfair practice of sub-PLR lending to certain borrowers. Fortunately, the RBI constituted a Working Group on BPLR (Chairman: Shri Deepak Mohanty) and Base Rate system came into being. Since then the administration of lending rates has become transparent, an essential quality expected from entities like banks at all levels.

Customer Service:

Ethics should dominate customer service rendered by banks. Business etiquette should be an integral part of ethical customer service. Bankers need to be trained in this line. Fundamentally, banks should not differentiate customer service rendered to a small customer and a large customer.

Whether it is a depositor, borrower or simple service seeker there should not be any hidden charges cropping up from time to time because of the 'fine-print'.

Accounting, disclosures:

Banks' balance-sheets and profit and loss accounts along with other statutory disclosures must reflect the true scenario of banks. Data purity and integrity are of paramount importance for banks from the viewpoint of all stakeholders. Corporate governance holds the key here.

Employees:

If employees are demoralised by unethical policies relating to their service conditions, their frustration would be reflected in a bank's businesses, howsoever ethical it may be to its customers

III. ROLE OF ETHICS IN BANKING

Ontologies based on the concept of good as opposed to evil helps us define the banking business from the point of view of ethics. The idea of awareness or conscience of the need for banking products or services inevitably comes to mind. This simplified parallel leads us to the conclusion that full awareness of and the related ethics about the importance of banking products and services is imminent to all economies, regardless of

Their economic development. Principle of mutual trust is of special importance for successful functioning of the business system. Important and valuable deals are very often contracted over the phone, in the absence of witnesses, while the relationship between the participants is dominated by the inviolable principle of mutual trust.

Internet is developed. By using encryption systems and digital certificates it is possible to

realize four basic functions of the transaction security, such as: confidentiality, authentication, integrity and incontestability. The efficiency of such measures should be proved by more extensive use of electronic money. In banking operations, the key cause of ethical principles' erosion lies in using illegal banking transactions for the purpose of acquiring wealth. All banks are obliged to take a proper care of who

they work with and to proceed with all required measures for preventing such cases. Therefore, they are obliged to abide by international laws and codes. A growing concern due to the erosion of trust has prompted the governments of many countries to re-consider their approach to ethical codes. For example, the UK introduced the code of public conduct in 1994. Likewise, the ethical standards for bank officials should be clear

The bank managers should possess the following qualities:

- Human values, which is a duty of every individual, a prerequisite for proper life. It involves a correct cooperation with other persons,

- Unselfishness, implies that the bearers of managerial functions should bring in conformity their conduct with the bank's business policy. They should not adopt and implement decisions in order to derive financial or material benefits for themselves, their

families or friends. In exercising their duties they should demonstrate professionalism.

- Integrity, the bank's managers should be very cautious in providing financial services to their clients, so as to avoid clients' influence upon the conduct of their activities;

- Objectiveness, impartialness, equitability and an ambition to set even-handed criteria and goals of ethical behaviour.
- responsibility for all their acts and decisions;

- Honesty in terms of resolving any conflict of interests which may arise;

- Headers hip, bearers of managerial functions in a bank should promote and support these principles guided by personal example. Likewise, the clients should be interviewed in order to determine the level of their satisfaction. In case of an inadequate behaviour of subordinate officers, the managers.

- Principle of mutual benefit and interest means that none of the partners in a business relationship should feel cheated;

- Principle of good intentions is very important for business ethics and moral behaviour. This principle means that there is no intention to treat the business partner in an immoral way, whether it refers to deception, theft or some other undesirable way of treating a business partner;

- Principle of business compromise and business tolerance refers to the harmonization of the conflicting interests of participants in the business process;

- Principle of ethical improvement of business behaviour represents the business partner's readiness to accept the mistake that has been made as a result of his own actions.

He should admit the mistakes and respond in an appropriate way;

- Principle of DE monopolization of one's own position, because monopolistic behaviour on the market does not contain any ethical market value

- Principle of conflict between one's own interests refers to the inability to relate common to personal interests, with simultaneous adherence to the same ethical values. The isolation of ethical principles in banking occurs when the lenders take too much risk, trying to find a loophole that

allows them to approve more loans. Strict adherence to the law and regulations in the field of banking makes it possible to grant loans to all the qualified clients in a fair way. When it comes to general standards, the bank must take into account the following.

- The bank must avoid a high concentration of loans in one industrial branch, sector or field, with the exception of specialized institutions that have this as their core activity;
- Clients who want to obtain a loan should maintain a certain amount of financial re-sources as a precondition for loan security;

- Loan approval refers to a strictly formal procedure in terms of purpose, source, price, terms and the method of payment;

- All loan applications must be accompanied by financial reports of the debtor for the previous year and Loans are granted with an amortization payment schedule. Having in mind the negative effects of credit risks on the bank's operations, and the macro system's interest in the rational use of loans for the purpose of avoiding inflation trends, the bank should have a restrictive attitude towards loan applications that could be used to finance new risky investments, and thus avoid possible inflation tendencies. The theoretical assumption that banks with higher capitalization rates and a better liability structure can enter long-term credit arrangements with a higher risk level has been empirically proven. It stems from the above that each bank should respect the general and the specific principles in formulating its credit policy. Since banks are trying to optimize their micro economy, they perform a significant macroeconomic function through their activity. The bank's non-objectivity is most evident when it comes to establishing accurate information about the character of the debtor. Based on its subjective evaluation, the bank makes conclusions about the debtor. This indicator is most obvious when it comes to personal loans, and less obvious when it comes to corporate loans.

IV. HACKING IN ETHICAL BANKS

A. Phishing: We have discussed phishing on this website a lot of times in tutorials like how to hack Gmail accounts password or hacking Facebook accounts and others too. But for new Guys I explain what is Phishing. Phishing is a technique to hack password and login details of a particular website using Phish pages. Now what are Phish pages? Phish Pages are simply the fake pages that look like the original webpage. The only difference between phish page and original page is the Address bar link (for normal user) and redirection post and get method (inside source for advanced users). How to identify a fake link? Just check the address bar URL for a fake page or Phish page it will be showing different URL than the original URL. Also if you want that everything is done automatically then install a Web security tool bar in your browser (AVG and Crawler web security tool bars are

good choices) as it detects the phishing automatically and do not allow you to visit Phishing Pages.

B. Trojan: Trojans are type of viruses that steal your information. It can be in many forms like Key loggers or RAT's (remote administration tools). What a key logger does is that it monitors all the keys that you have pressed from your physical keyboard and stores them in form of a log and sends these details to hackers. RAT's are advanced form of Keyloggers that remotely monitor all your activities where keylogger is simply a functionality. Using RAT hacker can connect to your system anonymously i.e. without your information when you are online. RAT's have a huge list of functionality and these are best type of hacking tools available in the market. Now How you will protect yourself from Keyloggers? Just keep your antivirus updated and install KeyScramber that encrypts your keystrokes. Now why I haven't mentioned RAT there is because once the RAT enters your system you cannot do anything other than formatting your system. So RAT's attack only can be prevented before they enter in your system. For preventing from RAT's Please do not download any software or cracks or keygens online. Also avoid downloading freewares from new websites use certified websites only like CNET, filehippo etc.. Also please avoid testing fake hack tools (recommended for hackers) because most hacking tools have keylogger and RAT's attached to them. Test it under secured conditions like on Virtual Users. Means install virtual operating system user Virtual PC or Virtual Box and then test them there.

C. Session Hijacking: Most of us use Wireless Networks to access the internet and data flow in form of packets and channels. And we know that Wireless are easier to hack as they have very weak encryption. So Hackers hack the wireless networks and using session Hijacking they take control of the internet data transfer and redirects the user from original path to their path. Means suppose you are visiting Google or Gmail or Facebook, then hacker when gets access then he can redirect you to any of the page and capture your account details. Packet sniffing is another way to hack the account information and credentials using the wireless networks where Hackers capture packets and decrypt this encrypted information to get the information in form of plain text. Now how you will prevent this? It's also pretty simple to prevent this, you need to hide your SSID and BSSID from being discovered by the other networks. Just leave the SSID or BSSID empty for that. Now hacker will not be able to discover your wireless router so he will not be able to hack it.

What really is attack?

The fatal flaw that enabled the sensitive information to be stolen is possible when an end-user is not properly educated on an easy to do and well-known SSL exploit – SSL MITM. The hackers take benefit of that to get access your sensitive data. As it's a great saying PREVENTION IS BETTER THAN CURE. So an properly educated end user is really the requirement so that he can block all loopholes in the system. I

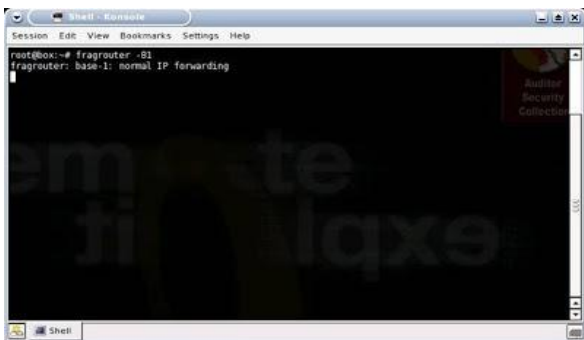
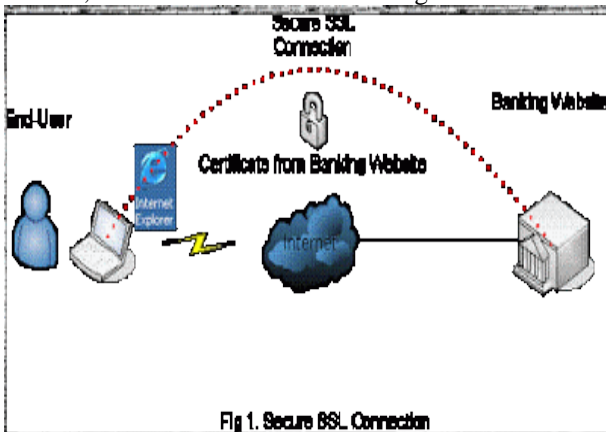
have already shared two articles with you about how to secure yourself. First one is Make your computer 100% hacker proof)

How the Hack works and How to do it?

First thing i will tell you hacking credit or debit cards is illegal and it will result in serious consequences like 10 years imprisonment and much more. This tutorial is for educational purposes only. I am explaining this tutorial is just to make you aware that how it works

How the hacker will do it?? suppose you are using a Wi-Fi connection to connect to internet. Now what hacker will do it will hack your Wi-Fi network and connect to it. He runs a series of utilities to redirect other user's data through his machine. He runs a number of other utilities to sniff the data, act as an SSL Certificate Server and to be the Man-the-Middle.

The following diagram shows a very simplified graphic of how your SSL Banking session should work under normal conditions, then how it would work during an attack:

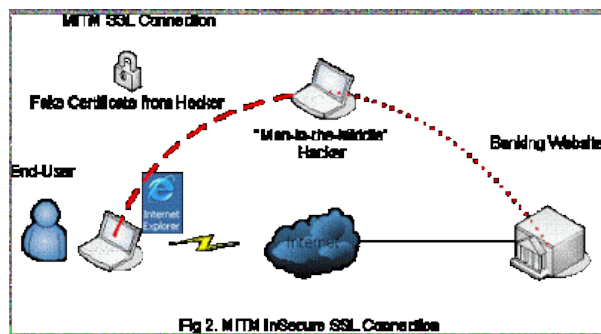
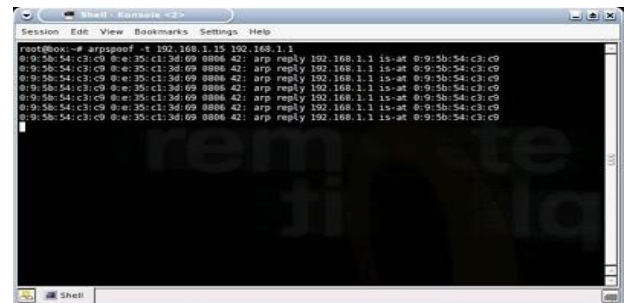


An important concept to grasp here is that a certificate is used to establish the secure SSL connection. This is a good thing, if you have a good certificate and are connecting directly to the website to which you intended to use. Then all your data is encrypted from your browser to the SSL website where the bank's website will use the information from the certificate it gave you to decrypt your data/credentials. If that is **truly** the case, then it is pretty darn hard for a hacker to decrypt the data/credentials being transmitted, even if he is able to sniff your data. This is a bad thing if you have a "Fake" certificate being sent from the hacker, and you are actually connecting to his machine, not directly to the bank's website. In this case, your credentials are being transmitted between your browser and the hacker's machine. The hacker is able to grab that traffic, and, because he gave you the certificate to encrypt the data/credentials, he can use that same certificate to decrypt your data/credentials.

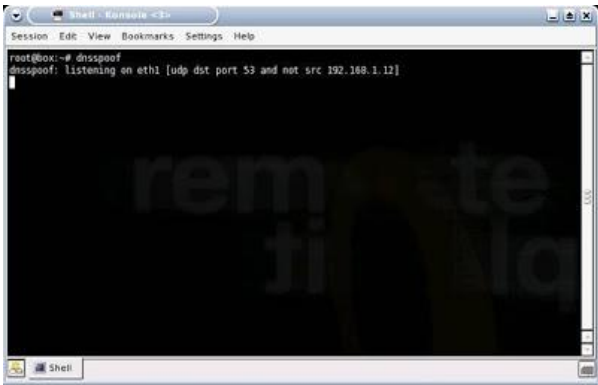
EXACT STEPS TO HACK CREDIT CARDS OR DEBIT CARDS

The first thing he would do is turn on Fragrouter, so that his machine can perform IP forwarding

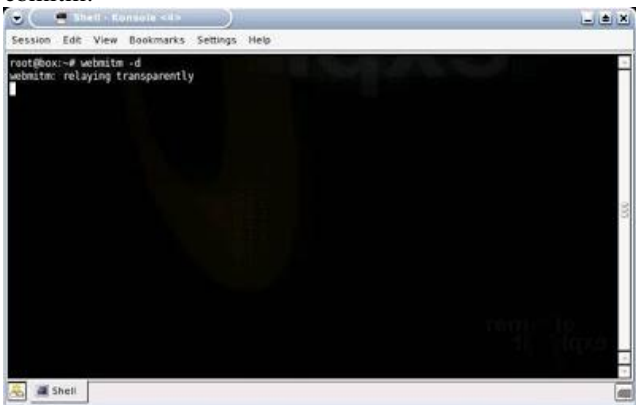
After that, he'll want to direct your Wi-Fi network traffic to his machine instead of your data traffic going directly to the Internet. This enables him to be the "Man-in-the-Middle" between your machine and the Internet. Using Arpspoof, a real easy way to do this, he determines your IP address is 192.168.1.15 and the Default Gateway of the Wi-Fi network is 192.168.1.1:



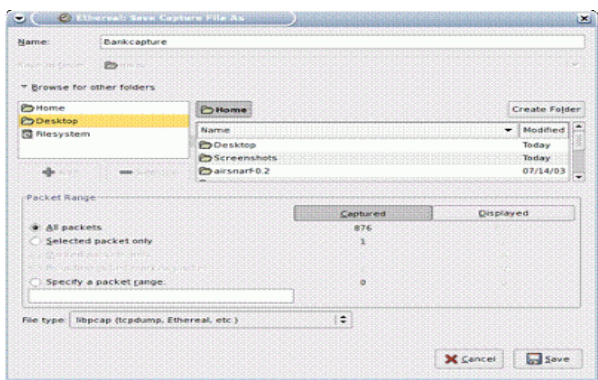
The next step is to enable DNS Spoofing via DNSSpoof:



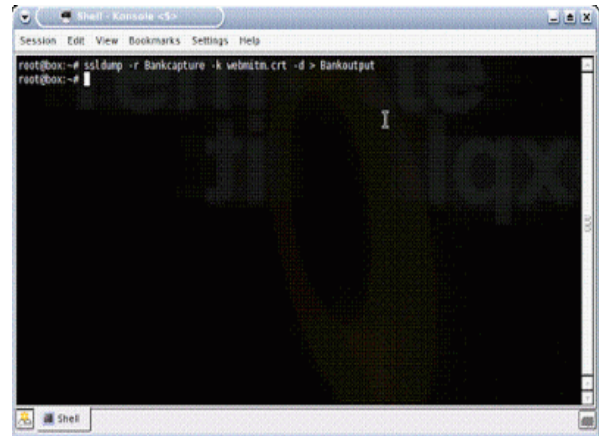
Since he will be replacing the Bank's or Online Store's valid certificate with his own fake one, he will need to turn on the utility to enable his system to be the Man-in-the-Middle for web sessions and to handle certificates. This is done via webmitm:



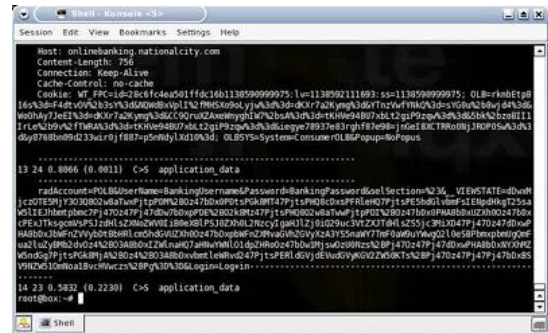
At this point, he is setup and ready to go, he now needs to begin actively sniffing your data passing through his machine including your login information and credit card info. He opts to do this with Ethereal, and then saves his capture:



He now has the data, but it is still encrypted with 128-bit SSL. No problem, since he has the key. What he simply needs to do now is decrypt the data using the certificate that he gave you. He does this with SSL Dump:



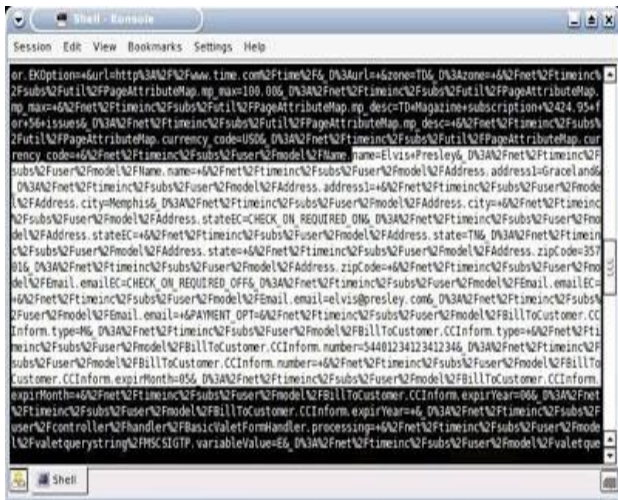
The data is now decrypted and he runs a Cat command to view the now decrypted SSL information. Note that the username is "Bank username" and the password is "Bank Password". Conveniently, this dumps also shows that the Banking site as National City. FYI, the better, more secure banking and online store websites will have you first connect to another, proceeding page via SSL, prior to connecting to the page where you enter the sensitive information such as bank login credentials or credit card numbers. The reason for this is to stop the MITM-type attack. How this helps is that if you were to access this preceding page first with a "fake" certificate and then proceeded to the next page where you were to enter the sensitive information, that page where you would enter the sensitive information would not display. That is because the page gathering the sensitive information would be expecting a valid certificate, which it would not receive because of the Man-in-the-Middle. While some online banks and stores do implement this extra step/page for security reasons, the real flaw in this attack is the uneducated end-user, as you'll soon see:



With this information, he can now log into your Online Banking Account with the same access and privileges as you. He could transfer money, view account data, etc.

Below is an example of a sniffed SSL credit card purchase/transaction. You can see that Elvis Presley was attempting to make a purchase with his credit card 5440123412341234 with an expiration date of 5/06 and the billing address of Graceland in Memphis, TN (He is alive!). If

this was your information, the hacker could easily make online purchases with your card.



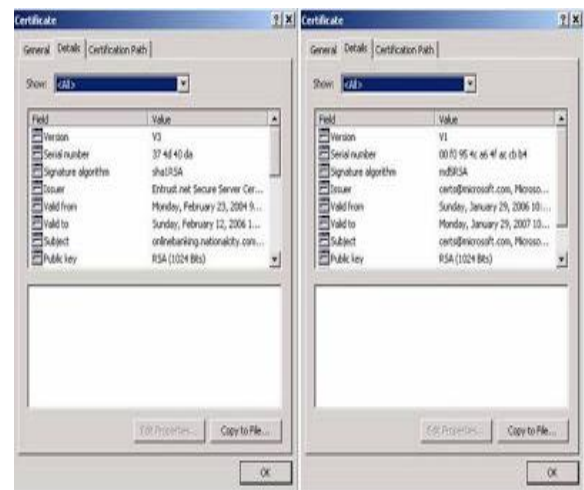
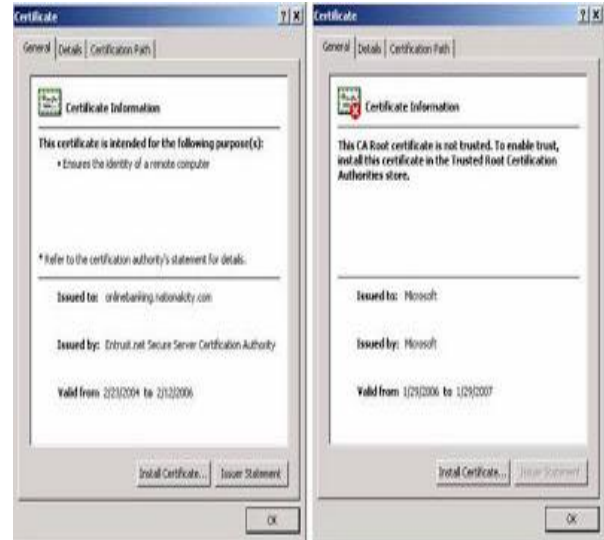
Also Real Bad News for SSL VPN Admins

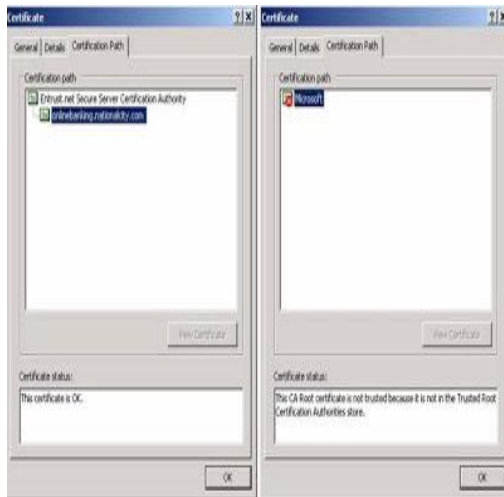
This type of attack could be particularly bad for corporations. The reason for this is that Corporate SSL VPN solutions are also vulnerable to this type of attack. Corporate SSL VPN solutions will often authenticate against Active Directory, the NT Domain, LDAP or some other centralized credentials data store. Sniffing the SSL VPN login then gives an attacker valid credentials to the corporate network and other systems.

What an End-User Needs To Know

There's a big step and end-user can take to prevent this from taking place. When the MITM Hacker uses the "bad" certificate instead of the "good", valid certificate, the end-user is actually alerted to this. The problem is that most end-users don't understand what this means and will unknowingly agree to use the fake certificate. Below is an example of the Security Alert an end-user would receive. Most uneducated end-users would simply click "Yes"... and this is the fatal flaw:

By clicking "Yes", they have set themselves up to be hacked. By clicking the "View Certificate" button, the end-user would easily see that there is a problem. Below are examples of the various certificate views/tabs that show a good certificate compared to the bad certificate:





interests of the Client have reported a much lower level of complaints.

VI. REFERENCES

- [1] <http://www.hackingloops.com/atom.xml?redirect=false>
- [2] http://www.social-banking.org/fileadmin/isb/Artikel_und_Studien/de_Clerck_Ethical_Banking.pdf
- [3] <http://www.hackingloops.com/2011/01/how-to-hack-credit-or-debit-cards.html#axzz3IdmR0IQs>
- [4] http://www.social-banking.org/fileadmin/isb/Artike_und_Studien/de_Clerck_Ethical_Banking.pdf
- [5] Global Alliance for Banking on Values: www.gabv.org
- [6] <http://www.ethicalconsumer.org/ethicalreports/bankingindustrysectorreport.aspx>
- [7] www.fsforum.org/Standards/Home.html.

How an End-User Can Prevent This

Again, the simple act of viewing the certificate and clicking “No” would have prevented this from happening.

Education is the key for an end-user. If you see this message, take the time to view the certificate. As you can see from the examples above, you can tell when something doesn't look right. If you can't tell, err on the side of caution and call your Online Bank or the online store.

Take the time to read and understand all security messages you receive. Don't just randomly click yes out of convenience.

How a Corporation Can Prevent This

Educate the end-user on the Security Alert and how to react to it.

Utilize One Time Passwords, such as RSA Tokens, to prevent the reuse of sniffed credentials.

When using SSL VPN, utilize mature products with advanced features, such as Juniper's Secure Application Manager or Network Connect functionality.

V. CONCLUSION:

The domination of ethical principles implies the elimination of criminal operation of commercial banks, i.e. less frauds, bribery, and corruption. Given that economy cannot successfully function in the absence of ethics and morals, the necessity of introducing ethical banking is frequently advocated. In the banking sector, the business ethics principles would be implemented. A lot of banks prioritise on honesty and thoroughness as well as the ability to communicate and avoid conflicts. Employees' sense of responsibility also holds a significant position. The survey has shown that the banks that focus more on fostering the motivation of their staff through different training courses and a well-structured system of incentives are usually able to attain better results. The banks that focus on working with their clients in order to identify and handle complaints with good will and in the best