Intrusion Detection, Internet Law Enforcement and Insurance Coverage to Accelerate the Proliferation of Internet Business

Christopher Ting, Ong Tiang Hwee, Tan Yong Tai & Ng Pek Yong

DSO National Laboratories
20 Science Park Drive
Singapore 118230

Abstract

In this article, we propose a framework to accelerate the ubiquitous capitalization of Internet as a vehicle to merchandise goods and services. The motivation for proposing this framework derives from the fact that many consumers and small-to-medium-sized companies are still hesitant to use Internet to shop, trade and disclose sensitive information such as credit card numbers. While IT security technologies and products are widely available, there are still gaps that have to be filled in before Internet becomes a truly viable and profitable channel to do business.

The business model that we propose is anchored upon the trilogy of three elements, which are interwoven and indispensable. We believe that to do business over the cyberspace, IT security technologies need to be complemented by financial and law enforcement instruments. We propose and present the case that Intrusion Detection, Internet Law Enforcement and Insurance Coverage (I3) can fill the gaps, both from the technical as well as non-technical standpoints. Just like Command, Control and Communications (C3) are indispensable in any military operations, I3 are critical to creating a trusted environment for Internet Business.

The highlight of the I3 framework is an Agent-based Monitoring, Intrusion Detection And Response (AMIDAR) system. AMIDAR is proposed to *enable* the law enforcement agency to "police" the cyberspace effectively, so that both the virtual shop owners and the consumers feel secure to buy and sell on the Internet. For the insurance underwriters, AMIDAR forms the basis to gain insights into the residual risk, and to draw up realistic insurance policies that sell well. We also point out that risk assessment, automated systems configuration checking as well as computer forensics are the associated technologies to help make the I3 business model feasible. Another novelty is the shopping protocol. It is designed to raise the level of assurance to the proposed I3 framework against fraud. We hope that the I3 framework with the associated shopping protocol can turn the Internet into a market place.

1. Introduction

Evolving from a working prototype in the research labs and academia, Internet has gained its statute in reaching out to the mass in the early 90's. Although electronic transactions are not new and they have existed even before the arrival of Internet and web, only big corporations and government bodies can afford the resources to streamline their financial, tendering and other transactions with external business partners. Internet banking, Internet commerce, Internet retailing and so on are still at the rudimentary stage, at least in the context of Singapore.

Set in the Asian backdrop, Singaporean consumers are reluctant to disclose their credit card information over the insecure Internet. The entrepreneurs and retailers, especially those not in the IT-related businesses are also hesitant to exercise the option of using

Internet as a vehicle to launch a strategic dimension to their traditional business practices[◊]. Part of the reason stands from the fact that there is no security assurance; the liabilities are also ambiguous. Despite the availability of IT infrastructure, IT security products and consulting services, there is a prevalent sense of mystique and insecurity as far as Internet business is concerned.

In this paper, we propose a tripartite framework to address the issues of lack of assurance and confidence. It is hoped that the I3 framework of Intrusion Detection, Internet Law Enforcement and Insurance Coverage will catalyze the process of turning Internet into a vibrant market place.

2. Problem Formulation & Principal Considerations

If a small-sized business[♦] – take florist shop for instance – were to put up a web server to advertise the range of goods and the order information, would the shop owner end up loosing money? On a more positive note, what is the profit margin that he can expect from the sales that are attributed to the orders coming through the Internet? On the other hand, from the consumer's point of view, is there a mechanism to assure that his credit card information is well protected?

There are probably more issues that need to be considered, such as non-repudiation, claims of goods not received physically and not in good conditions and so on. However, these issues are common to ordering a piece of pizza over the telephone, or a watch by mail. As they are not specific to Internet business, we shall not discuss them in this paper.

Again, much as people still prefer reading hard-copied documents than their electronic versions, changing the habit of choosing merchandised objects with physical touch is not over-night. Having said that, it is up to the imagination of every money-making merchant to think of innovative and clever ways to allow the Internet shoppers to "examine" goods, say durians, through the web. Hence, we will not address the problem of habits here.

Suppose, a buy-and-sell (be it a flower, durian or stock option) via the Internet is accompanied by financial commitment in the form of credit or other types of electronic arrangement, what are the instruments needed to give confidence to both the suppliers and consumers? This is the problem that this paper is addressing.

From the consumer's point of view, he is worried that

C1

He loses his credit card information and other personal information

C2

[◊] It seems that Singaporeans are not the exception. The British poll shows that 69% of the British companies are hesitant to do business over the Internet [1].

[♦] In this paper, the I3 framework is restricted to the local context of Singapore. Although it is interesting, more meaningful and useful to conceive a framework that applies across national borders, the legal aspects are likely to become overwhelmingly complex and controversial to address in this conference adequately.

He is transacting with a spoofed web site

From the supplier's point of view, he is worried that

S1

He is liable to pay for the customer's claim that its web site is responsible for disclosing the personal information.

S2

His web server is broken into by hackers, who may alter the content of the web pages.

S3

His web server is crashed by denial-of-service attacks, and during the downtime, his business may potentially lose out to his competitors.

3. Intrusion Monitoring, Detection and Response

Before discussing the proposed I3 framework, a description of an Agent-based Monitoring, Intrusion Detection And Response (AMIDAR) system is in order. While there are many technical aspects of AMIDAR, we have selected to describe those that are relevant to this paper.

In our technological development project, we have rapid-prototyped an AMIDAR that provides the following security services:

- Monitor the IP packets travelling in the network to detect and respond to network-based attacks
- Monitor the log generated by the firewall to look for suspicious activities in the network
- Monitor the servers' log entries online to detect and respond to host-based attacks
- Monitor the behaviour of the router to detect and respond to attacks targeted at it

While there are many intrusion detection products in the market, as well as many advanced prototypes in the research labs all over the world, the AMIDAR is the first in being an integrated suite of intrusion detection and response capability.

In addition, AMIDAR is contemporary in the sense that it adopts the technology of software agents in building the prototype. From our experience, we find that the benefits that we have obtained in adopting the agent-based approach are as follows.

- Ease of installation and deployment
- Ease of administration
- Reliability and robustness in the communications of intrusion detection information to the administrator or the custodian of the information systems.

- Scalability
- Re-configurability
- Ease of software development because of high re-usability and modularity
- Ease of update for detection and response against new cyberspace exploits

4. Some Technical Aspects of AMIDAR

The system architecture of AMIDAR prototype [2] is depicted in Figure 1. From the user's point of view, it is very important to see to it that the IT security product does not introduce noticeable performance hit on the computer systems and networks that it is protecting. Therefore, when designing AMIDAR, we have adopted the strategy:

- passive sniffing to monitor the networks and systems.
- distributed computing to arrive at the decisions of having detected intrusion attempts.

In other words, the ideas are to "image" or "mirror" IP data from the networks and systems, as well as to process IP data *on different machines*.

Now, given the same price, the performance of PC is doubled every year; it is cost-effective to run monitoring program (cyberspace sensor or imager) on the PC. What about the "brain" of AMIDAR, which is to process the IP and arrive at some conclusions? It too, is being run in the same PC that runs the monitoring program. The "brain" is distributed because for every monitor (sensor), there is a class of agents associated to it to detect cyberspace intrusion attempts. Essentially, AMIDAR has the following modules:

- *Network-based Intrusion Detection Module*
  - Network Monitor. Building upon *tcpdump*, this is an in-house developed network sniffer. It runs on a PC. It is high-performance in the sense that it can sniff packets from the network without missing any (on a 10 Mbit/sec traffic flow). Being a passive listener of the network traffic, the network monitor does not affect the network performance. They are most effective when deployed at strategic locations.
  - Network Intrusion Detection Agents. By processing the IP packets provided by the network monitor, this class of agents scans and monitors the network to check for abnormal and malicious network packets. It also has the functionality to record important network sessions. The agents run in the same PC that hosts the network monitor.
- *Firewall-based Intrusion Detection Module*
  - Firewall Monitor. Analogous to the network monitor, this is an in-house developed program that "sniffs" the log generated by the firewall software. It also runs on a PC, which is connected directly to the computer that runs the firewall.

- ♦ Firewall Intrusion Detection Agents. This class of agents parses the log data and look for events that are indicative of network-based attacks. Dropped packets, unusual network access traces are the things the agents look for. The agents run in the same PC that runs the firewall monitor.

- ❑ *Host-based Intrusion Detection Module*

  - ♦ Host Monitor. Host refers to information system servers such as email server, web server, database server, application server and so on. Analogous to the network monitor, this is an in-house developed program that "sniffs" the log generated by the server to be monitored. Host monitor runs on a PC, which is directly connected to the host.

  - ♦ Host Intrusion Detection Agents.This class of agents parse the log data and look for events that are indicative of attempted break-in via for example buffer overflow. It also keeps track of failed login events. The agents run in the same PC that runs the host monitor.

- ❑ *Intrusion Detection Module for Router*

  - ♦ Router Monitor. Connected directly to the router, router monitor is a PC-class machine that pulls event data from the router.

  - ♦ Router Intrusion Detection Agents. This class of agents parses the event data and looks for tell-tale signs of attacks targeted at the router itself. The agents run on the router monitor machine.

- ❑ *Central Controller*

  The central controller is the nerve centre of the intrusion detection agents. It controls, distributes and administers all the four classes of agents. It runs two background processes: the heartbeat listener and the alert listener. These two processes form the core to maintain authenticated communications with the agents distributed to the network monitors, firewall monitors, host monitors and router monitors. Whenever the detection agents have detected intrusions, they will report to the central controller for it to respond by, for example, paging the system administrators•.

5. Re-engineering AMIDAR for Internet Law Enforcement

In earlier sections, we have seen that AMIDAR is a network of distributed cyberspace sensors and detectors. The deployment of AMIDAR is about superimposing it on existing networks and computer systems to be protected.

In the context of Internet business, the law enforcement agency has a definitive role to play – to police the cyberspace. The objective is to provide a sense of security for Internet users to set up virtual shops and counters, and for consumers to purchase goods and services.

For law enforcement agency to police the cyberspace effectively, tools are needed. Quite analogous to the concept of neighbourhood police post, the various detection modules

• Other types of responses are conceivable and implemented, but they will not be discussed here to keep the paper concise.

can be deployed at virtual shops on the Internet. The central controllers, or a hierarchy of them can be deployed at the headquarters.

Unlike physical space, cyberspace respects no national boundaries. It is hopeless to stop and prosecute overseas hackers to come in and create sensational story lines on local mass media. Given this reality, which is not likely to improve for the next 5 years, the Internet business we have in mind is restricted to the local scene. In any case, multi-national and big companies have already started using the Internet to do their business, and they can afford to engage consultants, buy security products to protect themselves, and manage the risk. But what about local small- and medium-sized companies? What about local consumers who want to shop and buy goods and services available on the local market?

We know that every country is assigned a range of well-defined IP addresses. Technically, a router can be configured to filter IP packets based on IP addresses. Therefore, it is possible to restrict Internet business to the local market until an international framework for law enforcement is put in place♣.

We believe that a true indicator of success of Internet business in Singapore is the emergence of local companies to provide a wide range of goods and services to the local consumers via Internet. To create a local *virtual market place*, vibrant with billions of buy-and-sell transactions everyday, a framework and tool such as AMIDAR are indispensable to provide confidence and sense of security to the local population.

With AMIDAR deployed, the intrusion detection modules will establish an authenticated channel to communicate with the central controllers. Whenever intrusion attempts are detected, the central controllers will be alerted. Depending on the types of intrusions, central controllers at the physical neighbourhood police posts and HQ's of the law enforcement agency can respond accordingly.

6. Framework of I3

The underlying principle behind I3 is risk reduction, risk elimination, risk sharing and online fraud prevention, detection and response.

As in any trade, there will be a government registrar to grant license for setting up a virtual shop on the local Internet. Under the license, the virtual shop owner has to set up the following basic packages:

- Web server♥ that provides merchandised information to the requests originated from the local IP addresses
- Security services to provide end-to-end secure session to transmit credit card and other personal information#

♣ Of course, a local supplier can still establish its own *logically different* connectivity to the overseas business partners, distributors, resellers and customers.

♥ Only port 80 is open.

Many web servers and browsers have this security feature. To make it more secure, we will discuss a simple mechanism (Internet Shopping Protocol) in Section 8.

- Router that filters IP packets to allow only local IP addresses

- Intrusion monitor and detection agents that make "police report" at regular interval to the central controllers (housed in the physical confines of the law enforcement agency) in real-time.

We have discussed the link between intrusion detection and Internet law enforcement. What about the role of insurance coverage in this framework?

As credit card information, personal and financial information of the consumers will reside in the computers of the Internet merchants, the risk of losing the information to hackers has to be addressed. If a cyberspace incident has happened, the Internet merchant may be sued and liable to pay for the damages claimed by the customers. Therefore, it is wise and in fact advantageous from the business viewpoint to take up a suitable insurance policy. The objective is to share and manage the risk with the insurance companies.

In this proposed framework, our opinion is that insurance coverage should be instituted, just like every airliner must insure itself against air crashes. Although it increases the business cost somewhat, there are clear advantages to adopt this approach. In Singapore, consumers will feel more confident to shop on the Internet when they know that the virtual shops are

- officially registered

- monitored by the authorities in real time

- responsible to pay them for their losses (via the insurance mechanisms) should cyberspace incidents occurred.

In essence, all these measure are aimed at creating confidence in the consumers, and thereby increasing the consumer base.

From the viewpoint of insurance company, it is foolhardy to underwrite an insurance policy without a basis to estimate the risk involved. It is also possible that the virtual shop is deliberately "set on fire" by the owner itself, so as to claim the insurance money fraudulently.

To address the first problem, the insurance company can buy consulting services from competent security firms to conduct computer and network risk assessment if the insurance sum is large. If the amount is small, a software tool to check for systems' configurations may be sufficient to do the job. Whatever the case, both risk assessment and automated systems configuration checking are mature technologies in the computer security arena. In the I3 framework, the risk assessment can take into consideration the types of intrusions that AMIDAR can detect and handle. So it is possible to estimate the risk involved. The insurance premium, terms and conditions can then be determined accordingly.

For the second problem where an unscrupulous virtual shop owner is exploiting the insurance policy, computer forensics is indispensable here. Again, the Internet law enforcement agency has a role to play in this respect. In the proposed I3 framework, it is possible to base the "evidence" on the regular "police reports" sent by the Intrusion monitor and detection agents. In addition, the legal framework can be set up such that the insured sum is paid and distributed to the customers rather than to the virtual shop owners. This is because the consumers have lost their card numbers and personal

information, and therefore they are the ones that ought to be compensated. With this proviso, it becomes much harder for the unscrupulous virtual shop owners to succeed in the fraud without collaborating with the customers.

7. Fairness in Addressing the Concerns

In any business ventures, the return of investment should be proportional to the business risk. Since the consumers are paying money, the Internet business model should make it risk-free for them. On the other hand, since the suppliers are making money by getting their return from investing in the virtual shops, they have to be prepared to take the risk. Among other things, the suppliers are exposed to the risk of hackers attacking their virtual shops, and liable to pay the consumers for losing their credit card and personal information when a break-in occurs.

In the previous sections, we have addressed these concerns with the localized I3 model. To make it attractive for the small- and medium-sized companies to set up virtual shops, insurance policies and law enforcement with AMIDAR as described before are necessary. With these three components, the risk is shared and distributed to the insurance companies. Not only that, they can provide added assurance and confidence to the consumers who are buying from them. Therefore, suppliers' concerns (S1 to S3) have been addressed.

8. Shopping Protocol in I3

To address the concern C1 and concern C2 of the consumers further, we proposed a shopping protocol under the I3 framework. In this protocol, credit card service providers have a role to play as well.

- The credit card service provider generates tokens randomly and parcel out the tokens to their clients randomly.
- The credit card service provider sets up a number of secure servers on the Internet to provide the checking and verification services.
- Through the monthly statement of account received by hardcopy mail, the shopper obtains the tokens (say one hundred tokens per month).
- Each time when a consumer pays an item with his credit card, he sends one half of the token to the virtual shop (with his credit card number) and the other half to the credit card service provider.
- The virtual shop sends that half of the token he has received from the consumer to the credit card service provider.
- The credit card service provider checks if the combined tokens it has received is among one in the parcel of the consumer.
- The credit card service provider notifies both the supplier and the consumer of the verification results.
- Each token is valid for one purchase only. To do another purchase, the consumer has to use a different token in his parcel.

This is a preliminary and simplest version of the shopping protocol and there are many ways to improve it. The idea is to render it impossible for hackers who have managed to obtain the credit card information to derive any benefits. With this shopping protocol, on top of the credit card information, the hackers have to steal the tokens from the consumer as well[*].

Even if the consumer is tricked into transacting with a spoofed virtual shop, the hacker has to somehow intercept the other half of the token that is sent to the credit card service provider. This is by no means easy over the Internet.

In the case of purchase that involves delivery of goods, it is even impossible for the hacker to gain anything out of it, because by default, the goods will be delivered to the residential or office address of the consumer. If the consumer wishes to make a purchase and have the goods delivered not to him but to his loved ones as gifts, he can register their addresses with the credit card service provider. So in addition to checking the tokens, the credit card service provider can also check the delivery address. If the address for the goods to be delivered to is not one of the registered, the credit card service provider can quickly deduce that there is a fraud or anomaly and should contact the consumer immediately for clarification.

9. Remarks

The upshot of I3 framework is that it generates two supporting industries: insurance underwriting for Internet business, risk assessment and systems security evaluation and certification.

For the I3 framework to work, the relevant government bodies, the law enforcement agency, the IT security professionals and vendors, the insurance companies as well as the credit card service providers have to take part and play their respective roles. We emphasize that IT security technologies are available today and they can only do that much; the business, legal and social aspects are more important and complex.

10. Summary

E-commerce and more generally Internet business have yet to permeate into the society. Consumers stay at the sideline, feeling insecure to send credit card and other personal information across the Internet. Small- and medium-sized companies also find it not easy and risky to open virtual shops and counters.

Given this state of the affairs, we propose a I3 framework and its associated shopping protocol in the local context of Singapore. The I3 refers to Intrusion Detection, Internet Law Enforcement and Insurance Coverage. It encompasses technical, legal and financial dimensions. We have discussed Agent-based Monitoring, Intrusion Detection And Response (AMIDAR), which is useful for Internet law enforcement and insurance underwriting. To provide consumers with an even higher level of assurance, the shopping protocol within the I3 framework was also proposed.

[*] Of course, there is a remote chance that the hacker is so lucky to guess the token right for the first time. But the odds can be made as small as possible in designing the tokens. Failed attempts to guess the token will be detected easily.

11. Acknowledgement

We wish to acknowledge the support of the Directorate of Research and Development, as well as the useful discussions with the colleagues of Computer Systems Lab.

12. Bibliography

[1] Bill Hancock, *Security Views*, Computers & Security Vol. 17 (1998) 654-666

[2] *Next-generation Intrusion Detection and Response*, DSO Technical Report