COST-EFFECTIVE LONG TERM SOLUTION FOR THE TENSION OF DATA ENCRYPTION ON THE PRIVACY

Dr. Myung-Ho Yoon, Northeastern Illinois University, m-yoon@neiu.edu
Dr. Andy Chen, Northeastern Illinois University, h-chen@neiu.edu

ABSTRACT

The traditional providers-users' model may present a real tension between the need of national security and the citizen privacy. In this presentation, we will design the detailed protocol that can be coordinated among security enforcement, encryption providers, and users. It will protect the privacy of users and also provide the needed information for the security enforcement. With this new protocol, security enforcement will be updated without any need to catch the fast changing of the encryption technology, and the civil liberties' demand on strong personal privacy will also be satisfied.

Keywords: Data encryption, security, privacy, information accessibility

INTRODUCTION

The war on terrorism has presented a need for government to know the possibility of terrorists communicating through encrypted Internet messages. The perpetrators and security enforcement instantly became a visible confrontation. As a result, it is needed to check all network transmissions to uncover the perpetrators. On October 26, 2001, President Bush signed into law the USA Patriot Act - "The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act". On February 2003, a draft legislation prepared by the Department of Justice - "The Domestic Security Enhancement Act" gave government further power in surveillance, wiretapping, restrictions on encryption, detention, and prosecution (8). Australia's Cybercrime Bill 2001 was passed with no debate although some privacy advocates called it a "knee-jerk reaction" to security problems. In Germany, Interior Minister Otto Schily called for limited data protection laws (6).

These new security laws broaden government's power to monitor Internet communications, but those acts in no way reduce businesses' obligation to protect customer privacy (7). Critics worried that these bills will undermine the basic open government principle and raise the possibility of losing the system of checks and balances that any good system must maintain. Without a new perspective, the traditional providers-users' model may present a real tension between the need of national security and the citizen privacy.

In this paper, we will design a knowledge acquisition protocol that can data mine all intelligences perpetrations through network transmission with data warehousing and expert knowledge interface and intervention capabilities (4, 5). That is, we will provide a knowledge acquisition filter through an algorithm that can be computerized with pre-setup intelligences and a frame for situational and emerging intelligence to assess all contextual security perpetrations. This knowledge base, processed through computers rather than humans, and detached from storing the

real contents, will protect the privacy of users and also provide the needed information for the security enforcement.

This knowledge acquisition data warehousing protocol will add value for security enforcements, encryption providers, users, and the entire internet community. With this new protocol, security enforcement will be updated continuously without any need to deal with the fast changing of the encryption technologies. The worries of civil liberties on the privacy and the sound system of checks and balances are also satisfied because through computerized processing all the evidences on the network intelligence activities are dealt with in an "arm-length" manner and can be used to maintain the basic open governing principle.

A Long-Term System Perspective

There have been other times of national crisis, where emergency legislations and measures passed - the Alien and Sedition Acts of the 1790s, the suppression of free speech during World War I, etc. (8). From a long-term system perspective, these legislations and measures are actions in the spirit of the time. As usual, the system that does not provide added value to the long-term system will not be supported as the time changes. The critiques and proponents of the USA Patriot Act are a reflection of time and contribute to their intelligences on the maintenance of the checks and balanced system.

From a long-term system perspective, it seems to us that the network intelligence and security system is an ever renewal, boundary-expansion, knowledge-intensive, multiple value-seeking phenomenons. For the analysis and later on the strategic management purposes, we are going to, temporarily, view the entire network perpetrating activities as experimentations testing on the robustness of the entire global telecommunications and security networks. And thus perpetrators become quality engineers alerting network experts and security specialists on the potential problems looming ahead. With this new perspective, network experts and security experts have to have an engaging tool to collect the results of the experimentations and thus be able to extend their expert knowledge. Therefore the new configuration of these domain activities will be the intersection of three social worlds:

1. Knowledge world:
   Network and security experts ➔ Network and security knowledge system ➔ Perpetrators (hackers or enemy attackers)

2. Operating physical world:
   Encryption privacy providers ➔ Physical network system ➔ Users activities

3. Checks and balanced world:
   Civil liberties ➔ Sound system ➔ Security enforcements

Through this new perspective, it seems obvious that all three social worlds have a common purpose - the physical network system should be studied and protected to provide the best utilities and welfare and least interruptions for users and society as a whole. The enemies or rivals from a conventional perspective become a balance duel cooperating through the common

efforts and purposes and competing through different angles, activities and value orientations. It also seems easier to accept the traditional understanding and stance that there is a cooperating and competing checks and balanced between providers and users as well as between civil liberty and government administrations. However, it seems to remain much difficult to accept that hackers or foreign attackers are a part of the checks and balanced system symbiotically engaging each other to enhance the general welfare of the e-commerce. Fortunately, this new perspective is only used to help resolving a cost-effective long term solution for the tension of currently affecting data encryption on privacy.

Strategic Management Analysis

For analysis, we assume that a system has entropy, that is, without self-renewal and continuously expanding on its boundary, eventually the system can no longer provide services to the new demands. We also assume that each member in the system will act for seeking the highest value and least cost return from his/her own perspective. Moreover, we assume that if there is no checks and balanced system, through self-fulfilling of highest value and least cost return, a system will run to the extreme that it will destroy itself. Then all members in the system, for the purpose of survival, may not know what other members will do to them, but will work hard to learn the system and to anticipate what all creative ways his/her cooperating and competing duel can do to minimize their values and increase their costs (1, 2).

From this behavioral framework, a network expert or a government security enforcement people can not continuously prevent perpetrations unless they continuously bring add value to enhance the security and structure stability of their system. On the other hand, a perpetrator can not penetrate a system continuously without constantly digging out the hole of the system. Since both sides of the competing duels work hard to enhance their own values, the system extends its own life and thus benefiting the other two worlds: the operators-users and the checks and balanced social worlds.

Similarly, in the operators-users world, the operators will work continuously to increase their revenues and reduce their costs. Users will demand more services with less cost. Both of them will come to resist any additional burdens to the benefits of their living system, which include the burdens of any higher cost over benefit add-on measure. Without further explanation, this kind of self realization applies to the watch-dog and administration world.

Therefore, the name of the real game is to provide all three social worlds with a tool to enhance their intelligences and reduce their work. The tactics is to engage all members of this system to contribute their intelligence to expand the boundary of this system to generate for all members of all worlds, and that is the tool we are presenting - a knowledge acquisition data warehousing system that is coupled with real-time intelligence input.

Logical Design

Our purpose now is to design a computer system that will filter the hidden, surprised incidents on the real time telecommunication networks into a clear, manageable knowledge base with a

connection to the risk management team for real-time action. We classify the hidden, surprised incidents into three categories:

1. Routine perpetrations with pre-installed checking and prevention routines
2. Non-routine perpetrations but logically possible to check and prevent.
3. Non-routine perpetrations with no solution available in the near term.

We call the first two categories as familiar and the third category as strange. For the familiar cases, there is no need to be checked by human; moreover, computer software can be much efficient checking on its simple variations like re-labeling and simple combination of different familiar cases. One of the problems of the familiar cases is its cumulative effect and side-effects on the critical situations. For this, the data warehousing of this knowledge base can also provide a real-time check to uncover the hidden gradually cumulative perpetrations. To be cautious, non-routine familiar category should be transferred to the human experts for further investigation on its potential ramifications.

The third category is strange to our system even on its logical extension. This incident indicates a creative mutation of perpetration has been produced and thus alarms the need for the network and security expert to extend their knowledge boundary and to prepare a new semantic frame to assist the software system. If a strange case is situation oriented, the situation should be subject to strategic analysis to uncover its new tactics or scope for enhancing their added value. If a strange case is from a new player, the new player should be analyzed to see the overall game plan and thus its cumulative effect.

When the network and security experts have already detected a change in situation, and since the entire system is a dynamic life system, the experts should immediately upgrade the semantic frame that assist the capability of the filtering software. The filtering software should, in real-time, check the system structure vulnerability by itself. If it detects any weakening process, be it a thin safety buffer or a possible activation of trigger events on the existing safety buffer, the system should alarm the network and security experts for upgrading the semantics frame.

Semantics Frames and Man-Machine Interfaces

We assume that perpetrations are a chaos process (3). Before learning a new method through its practice, a perpetrator's actions are a fractal recursively re-applying its method and tactics on to the new vulnerable areas. The task of the network and security experts is to install a disarming mechanism on this known fractal so that its method and tactics have no vulnerable area to apply to. We call this disarming mechanism a semantic frame. Through the man-machine interfaces, the disarming mechanism will be installed into the filtering system to fend out the new routine perpetrations.

There is a possibility that even the network and security experts cannot create a new solution to disarm a new strange case. Or there is a possibility that the system cannot detect a strange case before it has done some destructions to the system. In this case, the system is also a tracking facility whose data can be used to create a double smoke to prevent the perpetrators to learn the effect of their new experimentations and to hide the new protect measures on the preventive structural re-strengthening for protecting the major interests of the three system social worlds.

Protocol

A. Start checking.
B. Case 1: Routine violations checks
    Process 1.1 Check perpetrators memberships.
        - If an old member, check its cumulative effect and its intention
        - If a new member, assess the new membership configuration.
C. Case 2: Non-routine logically reachable checks
    Process 2.1 Check perpetrators memberships.
        - If an old member, check its cumulative effect and its intention.
        - If a new member, assess the new membership configuration.
    Process 2.2 Kick out to be processed by human experts.
        - Document its newly added impact.
        - Documents its new scope, if it's modified.
        - Documents its new rules, if it's modified.
D. Case 3: Strange case
    Process 3.1 Handed to human expert team to do level of risk analysis.
        Level 1: Situation simple and risk low
            - Classify it as case 1 for keeping track.
        Level 2: Situation simple and risk high
            - Classify it as case 2 for continuously checking and prevention.
        Level 3: Situation complex and risk low
            - Decompose situation and check classify it as case 2 for further impact analysis.
        Level 4: Situation complex and risk high
            - Decompose situation and continuously checking.
            - Actively pursue strategic planning and prevention.
E. Continuously checking from Start.

CONCLUSION

The protocol sets up a new framework and mechanism to bring the innovation, changes, and relevancy decision needs into the well known traditional provider-violator dynamics. We hope that the new knowledge acquired through this protocol will help security and network experts produce timely prevention measures and therefore will be always better than the violators will do. That is, through this knowledge acquisition filter hidden surprised attacks from perpetrators will be transformed into clear and manageable situation. Moreover, through the balanced effort of expert and security teams, the acquired knowledge helps enhancing the robustness of the telecommunication and security networks.

Since the need of new knowledge for network and security enforcement is brought into the loop of this contended social world, there will be no need for security enforcement to continuously re-establish its requirement and thus will help them save unnecessary expenses.

REFERENCES

1. Brandenburger, A. M. and B. J. Nalebuff (1995). The Right Game: Use Game Theory to Shape Strategy, Harvard Business Review, (73), 57-71.
2. Courtney, H., J. Kirkland, and P. Viguerie (1997). Strategy under Uncertainty, Harvard Business Review, (75), 66-79.
3. Gleick, J. (1987). Chaos: Making a New Science. Penguin Books.
4. Hsieh, C. and B. Lin (2002). Web-Based Data Warehousing: Current Status and Perspective, Decision Sciences Institute 2002 Annual Meeting Proceedings, 1421-1426.
5. Hsu, J. (2002). Web Minding: A survey of World Wide Web Data Mining Research and Applications, Decision Sciences Institute 2002 Annual Meeting Proceedings, 753-758.
6. MacKenzie, K. (2001). Cybercrime Laws Passed, Australian IT, http://australianit.news.com.au/articles/0,7204,2944524%5E153006%Enbv%E,00.html.
7. McDougall, P. (2001). IBM: Privacy is Still Top of Mind, Informationweek, (34), 34.
8. McKenna, B. (2003). A Question of Balance: When National Security is on the Line, How Far Should We Go to Protect Civil Liberties? AFT On Campus (May/June).