Anti-Jamming Technology Evaluation Criteria

Global Internet Freedom Consortium
http://internetfreedom.org
March 2007

Developing an effective Internet anti-jamming technology is a real challenge. Our field experience in the past 8 years indicates that, to successfully defeat Internet blocking, filtering, and monitoring by oppressive regimes, technology innovation, systematic deployment, and dynamic infrastructures are critical. Many of the achievements in this field are ground-breaking, and there are no counterparts in other Internet applications. Therefore, to evaluate an Internet anti-jamming technology, it is essential to use the leading players in this field as references.

Currently there are five (5) leading players in this arena, at least for serving the Internet users in China. Dynaweb by Dynamic Internet Techonology, Ultrasurf by Ultrareach, and Garden by Garden Networks, have been the "three swordsmen" as affectively known by the Chinese Internet users and around for many years. Two newer systems, Gpass and Firephoenix by the Worlds' Gate, Inc., debuted in the summer of 2006, and have gained popularity quickly. Since all these 5 systems have been targeting Chinese users, they have not received much well-deserved media exposure in the English world, but their user base and success have not been surpassed by any other commercial or free software.

Each of these 5 systems has its unique technological innovations and features, and is well tuned towards real-world applications. Together, they form a multi-dimensional space for Internet information flow, and make Internet information jamming extremely difficult, if not impossible. Using each system's unique strength as a benchmark, it serves well to gauge any other anti-jamming technologies.

1. Overview of Internet jamming technologies

The most advanced Internet censorship technologies are implemented in China, under the auspices of its multi-billion dollar "Golden Shield" project. There are three major jamming technologies deployed there:

- IP blocking. Powerful firewalls are deployed on the edges of the Chinese Internet, each with a regularly updated black-list of IP addresses, most of which are websites or other services they do not want users to access. The black-list is manually updated occasionally.
- DNS hijacking. This malicious mechanism can redirect a clueless user to a totally different website from what he intends to, by sniffing the user's domain name

resolution (DNS) request and supplying the user with a false reply. Currently many of the blocked websites (e.g., www.voa.gov) are done this way.

- Content filtering. Their firewalls constantly capture and analyze the content of every user's Internet traffic, and will cut off their two-way Internet communication once the firewalls matches any pre-defined signatures, such as sensitive keywords, especially in Chinese (e.g., "Falun Gong"). Sometimes the signature database is updated to include traffic patterns they gleaned from binary traffic data.

These three jamming mechanisms work independently but simultaneously. Each mechanism serves as a censoring layer of the firewall's functionality, thus forming a three-layered firewall with varying strength and features in each layer. Any successful anti-jamming technology needs to penetrate all the 3 layers to make it work.

2. Overview of operation environment for anti-jamming technologies

The operation environments in censorship nations are complex, hostile and unpredictable. Factors such as government control, economic development, and social and cultural influences, together with Internet technology development, all play a role in making the operation environment for anti-jamming technologies extremely heterogeneous, and in making an anti-jamming system difficult to survive and thrive. For example, in China, a significant portion of Internet users surf the web on computers at "net bars", which normally host tens or hundreds of PCs with shared Internet connectivity. These computers are centrally managed by the net bar owners, and central and local governments have various mandates to the administration of the machines. Often these computers are required to install monitoring software developed by the government, to monitor and report users' activities to local police. In addition, these computers usually have anti-virus software installed developed by local computer companies, and often intentionally misidentify anti-jamming programs as viruses. Moreover, these PCs are under such tightly control that sometimes it is impossible to install programs on the hard disk.

Outside net bars, users in China employ diverse means to get online, as shown in Table. 1. Each connection category is shared by numerous local and national ISPs, all of which follow government's instructions to implement various censorship rules and varying degrees of enforcement.

Table 1. Internet connectivity categories by Chinese users, as of January 2007. (Source: Chinese Internet Network Information Center, http://www.cnnic.cn/)

SUBSCRIBER LINES	DIAL-UP	BROADBAND	CELLPHONE DIAL-UP
27.10 Million	39.00 Million	90.70 Million	17.00 Million

3. Technology evaluation criteria

3.1 Technology superiority

* Innovation. An anti-jamming system needs to have unique technology strength to defeat the sophisticated filtering technologies. Most conventional approaches, such as open http proxies, do not go very far. Nowadays an anti-jamming system has to do much better than that to be useful (sentence not clear). For example, Garden pushed the envelope of http proxies to an unprecedented extreme, and successfully penetrated the Chinese 3-layered firewall with ease and reliability. Other four players also have their own innovations with field-proven achievements.

* Scalability. It is easy to develop a tool to support a few users, who only want to access a few websites. However, it is very challenging to build a system which can potentially support millions of users simultaneously, who want to visit any website they like. Such a scale would need advanced technological design, especially when such a scale would become a huge target on the radar screen of the jamming side. Dynaweb and Ultrasurf have demonstrated such scalability. For example, Dynaweb supports more than 20 million web hits per day in average from Chinese users.

* Resilience. To survive the complex Internet environment described above, an anti-jamming system needs to be extremely resilient and robust. For example, Ultrasurf has successfully defeated the mis-identification by various anti-virus software programs on Chinese users' computers. More importantly, an anti-jamming tool has to respond quickly to the changing configuration of the jamming firewalls. For example, back in May 2006, the Chinese firewall system implemented a new signature in their firewall to target Dynaweb and Ultrasurf, and rendered both tools ineffective. But in less than 48 hours, Dynaweb team reverse-engineered the new filtering signature, and developed a counter-measure. The counter-measure was promptly communicated to Ultrasurf and other anti-jamming tools and all services were quickly restored.

* Universality. Earlier anti-jamming tools only supported users to visit web pages. Nowadays users desire protected access to emails, instant messaging, video streaming, etc.. Therefore it is critical for an anti-jamming system to support multi-protocol communications. For example, both Gpass and Firephoenix support streaming media and communication applications. Firephoenix also protects *all* Internet protocols out of box, without user configuration. Dynaweb has also implemented multi-media streaming support. These capabilities distinguish the five systems from other players, which are still only support http/https protocol for websites.

3.2 Usability

* User interface. It is critical for an anti-jamming software to have a clear and intuitive user interface, as the users range from all age groups and technical levels. More importantly, the user interface has to be in the users' native language, because most users in the oppressive regimes are not proficient in English. Gpass, for example, can automatically detect a user's language setting on their computers and display the native language automatically. Other 4 systems have similarly capability for native language support.

* User support. Timely technical support for users in their native language is also a must for a successful anti-jamming system. After many trial-and-errors, the five systems are now share a unified technical support platform, www.qxbbs.org, which each system has its own user forum, where users can share their experiences and developers can provide technical support. For example, there are more than 20,000 posts on Dynaweb's support forum, with information ranging from technical tips, user complements, and reports from China of new jamming test results, etc.

3.3. Infrastructure support

* IP pool management. The Chinese firewall keeps a black-list of IP addresses, and once a service's IP is in it, a user can no longer connect to the service. The Chinese net police actively monitor the IP addresses of the anti-jamming services, and constantly put these IPs in their black-list. This is a practical challenge other tools have not been designed to face. However, the five anti-jamming tools have developed a unique and powerful infrastructure to automatically detect the blocking of individual IPs, and change a service's IP immediately once it is detected blocked.

* Promotion and delivery of anti-jamming software. Due to the very nature of the Internet censorship, users cannot get the information when a new anti-jamming software is released, or an exiting one is updated, and even if they are aware, they can not download the software as most likely the websites hosting the software are blocked. Therefore, there need to be channels to market the new software to users, and deliver the product to them before they acquire any anti-jamming software in the first place. For example, Dynaweb can inform users of new releases via email and instant messaging, and most of the software packages from the five players have a small enough size to be emailed to users.

* Integration for a one-step full solution: To the end user, anti-jamming technology alone is often not enough. For example, users who first come to use our anti-jamming system may not know where to find online contents and communication tools to use, especially in their native languages. Some users wish to host their websites, blogs, forums, and emails etc outside the control of the repressive regimes, and want to be assured that the hosting parties do not cooperate with the repressive regimes to compromise their safety and privacy. As an essential component of Internet application, some users would like to

search online information truly free of political and commercial bias, especially in their native languages. (Background: even big companies like Yahoo and Google cooperate with CCP, censor the search results, and gave user information to CCP.) With the above observation, we believe that an integrated, one-step, full-service solution is important to achieve the ultimate end result.

For example, the Worlds' Gate, Inc, developed a web portal, named the Freedom Portal (edoors.com), which is composed of several platforms designed for ease of use by Internet users in repressive regimes to achieve maximum social impact. The *content platform* enables users to browse, create, organize and subscribe to content. The *communications platform* enables users to connect, interact, organize, and mobilize themselves. The *search platform* indexes, ranks, and classifies web pages of a targeted language (e.g., Chinese), and enables users to search the whole (e.g., Chinese) web as well as materials in the content platform, free of censorship. The *advanced web applications platform* enables users to increase productivity and perform advanced tasks on the web. Finally, the high-capacity *anti-jamming delivery platform* makes the services in all other platforms available to users in the targeted repressive country (e.g. China). These platforms are highly integrated in the portal.

4. Special consierations

4.1. Test environment

From our experience, we stress here the importance of evaluating an anti-jamming technology in realistic operation environments. Test results in ideal lab settings can only reveal the basic functionality of the tested system, but more important features unique to anti-jamming technologies can not be easily or realistically verified in such tests, such as the survivability in a hostile environment, scalability with large number of users, and resilience to unpredictable changes in the jamming technologies or in other factors. For example, the earthquake in Taiwan in late December 2006 damaged major undersea fiber cables, and caused a months-long Internet traffic jam between China and North America. Most users even had a hard time to connect to un-jammed websites in North America. However, Dynaweb users can successfully access most websites over the world despite the cable cut during this period, thanks to Dynaweb's global deployment of its network and users' traffic took a detour to Australia, and avoided the jammed link.

4.2. Abuse prevention

Internet anonymity is usually accompanied by abuse and illicit activities, exemplified by illegal sharing of copyrighted materials over some peer-to-peer (P2P) networks. Though all the five anti-jamming systems have strong security and anonymity support that rivals P2P networks, the outstanding feature of these five systems is their controllability. Each of the five systems has unique mechanisms to monitor and analyze user behavior and content, and can control users access to our anti-jamming channels in near real-time if needed. For example, all five systems have been actively filtering out pornography content, mainly in the interest of conserving system resources at present. Some systems, such as FirePhoenix, analyzes users access patterns to identify anomalous activities, with graphs such as Fig. 1 shown below. All these measures can also be used effectively to prevent Internet-based terrorist activities. This has great advantage over the P2P-based networks, such as Tor (http://tor.eff.org/), which, once deployed, one has no control of what users can do with such an anonymity infrastructure.

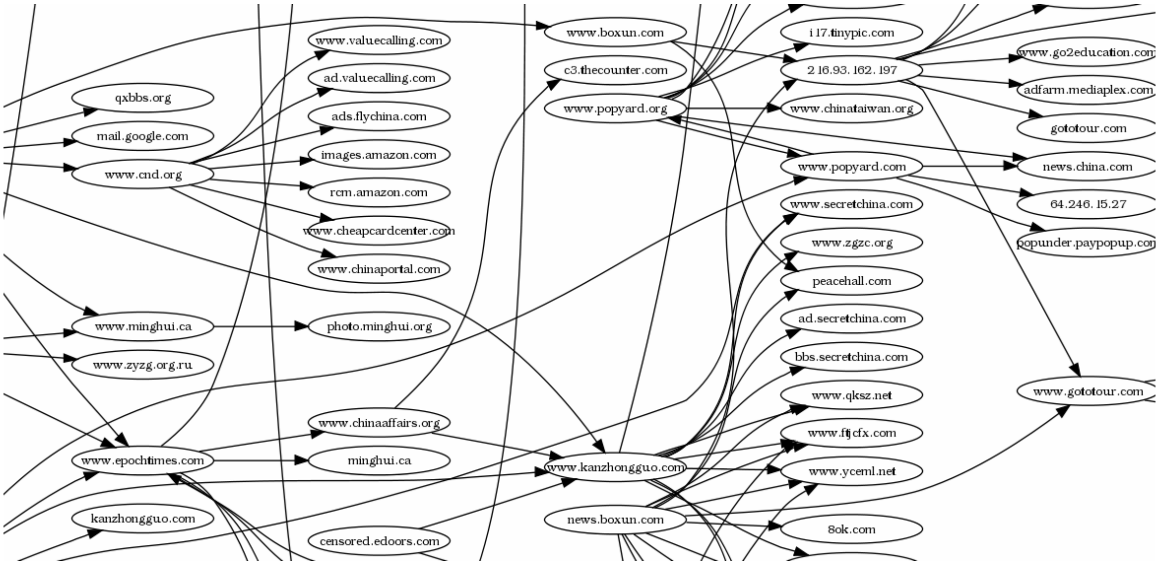

Figure 1. Part of the link-graph derived from FirePhoenix users' web-surfing activities. FirePhoenix uses such graph to monitor users access patterns and to discover anomalous activities when needed.

Summary

In summary, for an anti-jamming system to be successful, it has to demonstrate strong technology innovation, good usability, and has a mature support infrastructure for its daily operation. More importantly, it has to be tested in realistic, hostile, complex and unpredictable environments, such as those in China. The five leading players, Dynaweb, Ultrasurf, Garden, Gpass and Firephoenix, have all been time- and field-tested, and have set the industry standard in this challenging and unique field. They can serve as the benchmarks for evaluation of new or existing anti-jamming systems.