Security Issues in IDN

Yashar Hajiyev[1], Ali Shahintash[2]

Computer Engineering Department, Qafqaz University
[1]yhajiyev@qu.edu.az, [2]asahintas@qu.edu.az

***Abstract*— The International Domain Names program for web domains, is biggest change to the internet since invention of the World Wide Web. It is way to building really multicultural Internet. However all good intentions needs to be protected from expected and unexpected treats. Subject paper gives some brief to security issues related with IDN**

***Keywords*— IDN; Internet security; Cyber Squatting; Spoofing**

I. INTRODUCTION

Until recently we perceived Internet as predominately English "speaking" medium and we have become accustomed that the URL (Uniform Resource Locator) is only way to designate a informational resources in virtual space. Because Internet was populated by English speaking users and resources, it was logical that rules for creating labels of URL required to use ASCII characters comprising 2÷63 characters consisting of only English alphabet (a-z) letters. The tremendous increasing of internet users over past 15 years took place foremost because of growing of non-native English speaking subscribers. For now, it suffice to say that the share of last ones is 64% in total 3 billion users all around globe. That has begotten boom in developing of content in native languages and strengthen users' demand on how to write URLs in their native languages. Apparently, the ASCII-code based denoting system wasn't able to meet those new demands.

Users of many European Latin alphabet used countries like Hungary, Germany and etc. got used to "flatten" their language by giving up all inherent diacritics or accents. Cyrillic alphabet used countries were made to "Romanize" – to transliterate Cyrillic letters to Latin. The situation with Arabic, China and others alphabet were even more confused.

In 2003 ICANN launched program – Internationalizing Domain Names in Applications (IDNA) with RFC 3492 standard that introduce Punycode for transliterating non-ASCII symbol to specific combination of several ASCII characters.

In 2014 ICANN in managing of domain name system has initiated of building globally-inclusive Internet and more international web. Program enables to use in endings of web address the suffixes that consist of non-Latin characters, like Arabic, Chinese, Cyrillic and etc..

The sequel was a massive increase in number of options of national scripts based web addresses affordable to subscribers or entities. For instance, a world brand company may registry domain with own name and do brand websites more memorable. The new native language based domains allows business structures to indicate their local identity to specific national customers, following the example.

II. ESCORT IDNA FROM CYBER-SQUATTING

From subscribers' perspectives, it is worth keeping an eye on IDNA domain names, and remaining wary of new ones as they emerge. Despite the names even in national scripts themselves do not offer any tangible benefits for users, they will drastically alter landscape of web, and without any doubt get us to rethink how we navigate web for information resources.

Nevertheless, launching of few thousands new domain names brings about heaps of subitaneous problems. Most foreseeable among them is the risks associated with cyber-squatting. Evidences say that malicious get registrations of domain name of active government bodies or famous brands, and either uses it to discredit those brand's business prestige or blackmail and force them to purchase that domain back at speculative prices.

The big companies in order to minimize the threats from cyber-squatters prefer registering cautiously the domains that reflects the names of company famous products, trademarks and etc.. brands. That way companies tries to except options for intruders to use them even in national script based domains.

In order to set down of illegal usage of brand names ICANN founded up Trademark Clearinghouse as centralized repository of validated trademarks, where real owners of trademark can register their brands, to set down others using them.

However, it is hardly doable to truck on illegal using of trademarks through numerous IDNA domains.

In fact the situation was worsened for companies because they have to own thousands of domain names in defensive portfolios following common practice in the .com era.

Thus, the expenses of companies related with protection of their business images in virtual space will increase because they have to apply all efforts to ensure their invulnerability.

From other point, the implementation of national scripts based new web address suffixes would potentially do it harder for internet subscribers to understand whether or not a site is legal – especially if national scripts come into the equation. In fact, the similarity between letters in many national scripts is "fertile ground" for cyber intruders trying to trick web users into visiting illegal wrong web recourses.

IDNA will noticeably increase risk of spam because during searching the different search engines would offer different illegal sites visiting of which might enroll you to list of unsolicited mailing list. As one of the possible approaches for search engines might be set down websites that use these new domain extensions in the short term, ensuring that they will appear at very end of search results.

The number of new IDNA gTLDs [4] grows permanently, and domain industry is reaping the benefits. Regardless of some new security problems, they are necessary; the new extensions will be broadly employed.

III. SPOOFING ATTACK THREATS IN IDNA

One of the remarkable interests of customer is to know if a IDNA based URL is part of a phishing attack is to compare the domain name with host to their expectations for the legitimate site. Particularly, if randomly received email asks subscribers to provide personal and bank information to a website with the doubtful domain name is not as likely to receive submissions as a website that was hosted under a more reasonable sounding name. To make links look more legitimate the different types of common techniques used currently and recently. First email would be to have link text telling about thing, at the same time is has to anchor actually point to other URL.

Other artifice is to confuse the subscribers by altering the URL to imitate a valid sounding name in credentials part of URL, however actual host name is hidden in trailing part.

Other direction of attack is to use symbol from national scripts that appears to be the same or very similar to another symbol. Consequently, it is easy to compose possible a word that looks the same as another word. From Unicode point of view that characters completely different, have different codes, but visual similarity spoofs us. In fact different letters makes the word not really be same spelling.

For instance it is well knows similarity between number 0 and letter O; the letters l (lower case L) and I (uppercase i) and etc..

In Unicode we have very similar characters exist from different national scripts. Some national symbols looks like exact duplicate of Latin letters. The Cyrillic characters a, c, e, o, p, x and y are identical to Latin.

CONCLUSION

The launching of International Domain Name program stimulates activity in many countries to launch web sites that has content and domain name in native languages. Internet is becoming to be multicultural.

Abovementioned is some analysis of some types of cyber attack that should be considered to undertake protective steps.

REFERENCES

[1] “Secure computing corporation. Digital certificates”. <http://www.securecomputing.com/gateway/digital_certificates.cfm>. 2008
[2] http://www.lookout.net/test-cases/idn-and-iri-spoofing-tests/
[3] http://nameprep.org/
[4] Conjecture corporation. “What are digital certificates”. <http://www.wisegeek.com/what-are-digital-certificates.htm. 2008>.