IL-004 【既発表論文紹介】

Browser's "search form" issues and countermeasures

須賀祐治[†]
Yuji Suga

出典：The 19th Asia-Pacific Network Operations and Management Symposium (APNOMS2017), pp. 358-361

The surveys targeted are the SSL/TLS websites of regular members belonging to the association which is planning and managing related to bank systems. We investigated SSL/TLS sites of Top FQDN which are widely announced, so it was found that about half of them were in normal situation however half had problems such as FQDN mismatch. Moreover we also show the result of manually investigating the influence of the "search form" issues by carrying out some pattern classification on the path reached from the HTTP server of the Top FQDN to the user login page. Finally, the design guideline of HTTP/HTTPS sites is mentioned as one of countermeasures against this kind of problems.

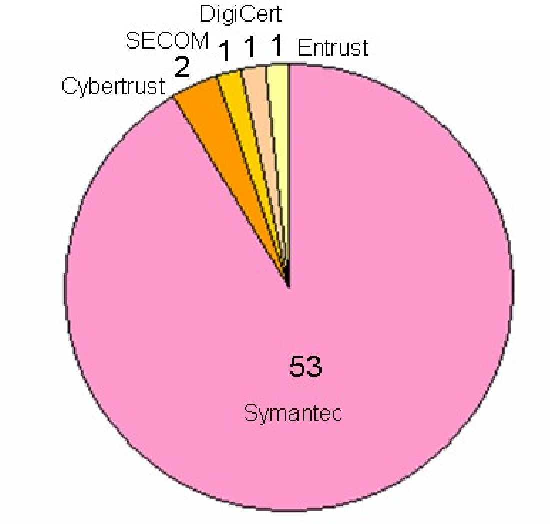
STATUS SURVEY AT APRIL 13TH, 2017

Protocol Version	Top FQDN banking sites (115 sites)	Banking login sites (58 sites)
SSL2.0	04.3%	00.0%
SSL3.0	34.8%	05.2%
TLS1.0	100.0%	100.0%
TLS1.1	67.0%	43.1%
TLS1.2	69.6%	62.1%

ACCEPTING VULNERABLE ALGORITHMS		
Using 40-bit algorithms for export controls	7.8%	00.0%
Using vulnerable algorithms	21.7%	00.0%

[†] Internet Initiative Japan Inc.

RATIO of EVSSL CERTIFICATE VENDORS on BANKING LOGIN SITES AT APRIL 13TH, 2017



Note that 25 certificates of 53 issued by Symantec were affected the invisible bug [1] on a certain browser.

[1] https://knowledge.digicert.com/ja/jp/generalinformation/INFO4287.html