ABSTRACT:

STATISTICAL ANALYSIS OF DHA PROTECTION SYSTEM'S RESULTS

Géza Szabó, szabog@crysys.hu
Boldizsár Bencsáth, boldi@crysys.hu
Budapest University of Technology and Economics Department of Telecommunications

Obtaining the e-mail addresses which are handled by the mail servers is the Directory Harvest Attack. The root of the problem in DHA is in the SMTP protocol itself: the e-mail servers, if they got the mail to a proper address, would not respond, simply accept it.

If the server got a mail to a non-existent address, then it would give a response either immediately or later whether the post office box exists or not. This process gives information about the e-mail addresses which are upkept by the server. The attackers use this information, sending huge amount of messages to the e-mail server. The addresses from which do not arrive response (so the server accepts the e-mail without negative signal) are gathered to a list. These addresses should belong to valid user accounts, so it is worthy to send uninvited mails to it.

In our presentation we would like to introduce our research, development, and show the results gained from the running of the implemented system. The implemented protection is component based developments, which are strongly coherent and use each other software elements to a high extent.

Last year we presented a possible implementation plan. We have continued this work, implemented the system and run it for a long period to collect data from attackers.

We would like to analyse the data collected by our system. We present which typical DHA attackers exist and whether it is possible to distinguish them unambiguously from each other based on just the attacker statistics. We compare the distribution of attackers by country in Europe. We review the Hungarian DHA situation based on internet access. With modern statistical methods we examine the question whether we can get answer for that why is DHA happening.