Cracking time for different protocols

Technology, Information Technology

Running Head: CRACKING TIME FOR DIFFERENT PROTOCOLS CRACKING TIME FOR DIFFERENT PROTOCOLS By University name

City, State

Date

Cracking Time for Different Protocols

Different protocols affect the hacking time required to break. Different security protocols have different types and numbers of weak points that hackers need for infiltration or intrusion. Difference in protocols is evident in their design (Miltchev et al., n. d., p. 2). For example, TCP/IP has weak points that hackers can use to spoof IP addresses and attack TCP link requests within minutes. Another example is widely used security protocols that do not normally entail the provisions for dependable authentication as part of the central protocol. SMTP, POP3, and IMAP4 are mail transfer protocols that enable hackers to forge emails effortlessly (Miltchev et al., n. d., p. 2). This is because these protocols do not need the usage of encoded that could make sure the privacy or discretion of email messages.

Another example of how different protocol designs affect the time needed to hack is intrusion hacking. Intruders use a range of attacking mechanisms to acquire access to networks. These mechanisms consists of password-cracking mechanisms, protocol cracking, and manipulation instruments (Miltchev et al., n. d., p. 7). Detection mechanisms used by intruders help identify alterations and alternatives that occur inside networks faster in TCP/IP than POP3 or SMTP protocols. An IT team called Nohl attempted to crack the OTA protocol in 2011 and realized its design is far more secure

than any products by Microsoft or Linux. Hacking the OTA protocol took the team longer to get through by sending commands to a number of SIM cards than cards with other types of security protocols such as Java (Olson, 2013). Protocol performance affects cracking time by decreasing the number of surged weak points in the respective network. Protocols with significantly better performances have environments with few weak points. In such settings, a well performing protocol dos not timeout frequently (Miltchev et al., n. d., p. 7). For example, a study conducted on protocol HACK found out that it was better than SACK because of SACK's continuous timeouts. On the other hand, HACK was able to maintain data stream to some degree. This performance was in fact six times better in terms of output than SACK in the existence of surge errors (Balan et al., 2002, p. 359). Another case of the cracking time of protocols depending on the frequency of weak points is 2013's powerful supercomputer NUDT Tianhe-2 ability to crack a 128-bit AES code. Researchers estimated that the supercomputer would take over 333 million years to crack this key, which is significantly longer for breaking any code (Crawford, 2014).

High security protocols have an effect on performance, time, and mostly costs. This effect occurs because high security protocols identify packet loss because of hacking and recover the required data. The ability to detect these losses is an indication of the protocols' dominion over performance (Olson, 2013). The flexibility of distinct cryptographic elements enables the usage of different protocols by numerous applications such as file-system encoding and user-level procedures. For instance, high security protocol IPsec takes far less time to achieve secure network communications than other popular

security schemes. However, this level of security comes at a cost that produces adequate performance for practicality. For instance, WEP policies cost the least and IPsec policies cause substantial costs but offer stronger performance within a short period (Miltchev et al., n. d., p. 1).

References

Balan, RK, Lee BP, Kumar, KRR, Jacob, L, Seah, WKG, and Ananda, AL 2002, ‘ TCP HACK: a mechanism to improve performance over lossy links,’ Computer Networks, vol. 39, pp. 347–361.

Crawford D 2014, PPTP vs L2TP vs OpenVPN vs SSTP vs IKEv2, Best VPN, viewed 21 January 2015, https://www. bestvpn. com/blog/4147/pptp-vs-l2tp-vs-openvpn-vs-sstp-vs-ikev2/

Miltchev, S, Keromytis, AD, and Ioannidis, S n. d., A Study of the Relative Costs of Network Security Protocols, DARPA, pp. 1-8.

Olson P 2013, SIM Cards Have Finally Been Hacked, And The Flaw Could Affect Millions Of Phone, Forbes, viewed 21 January 2015, http://www. forbes. com/sites/parmyolson/2013/07/21/sim-cards-have-finally-been-hacked-and-the-flaw-could-affect-millions-of-phones/