Drm and trusted computing

Technology, Information Technology

DRM AND TRUSTED COMPUTING The setup in which trusted computing when used to enforce DRM is vulnerable to man in the middle attacks (MitM) because of the ARP spoofing. This occurs when an authorized user causes network traffic between computers communication over the internet (Lockhart 2007, p. 84). As a result, the trick user is able to monitor the data shared between the communicating victims. This is dangerous since it exposes confidential information to the trick user, which might lead to access to personal and important information (Reid & Caelli 2005, p. 127). This is because the attacker has the freedom to interrupt data frames on a system, adjust the traffic or discontinue all traffic (Luettmann & Bender 2009, p. 131-138).

Similarly, According to Reid & Caelli (2005, p. 128), trusted computing is vulnerable to MitM attack when used to enforce DRM if the attacker acts as a proxy between two communicating users. This affects the flow of information because it is distorted or manipulated to suit the interests of the attacker. Computers that use unencrypted networks are vulnerable to attacks by the man in the middle because their network traffic is easily grabbed (Luotonen 1998, p. 120).

In order to avoid the vulnerability of trusted computing to MitM attacks when enforcing DRM, it is advisable for communicating computers to use encrypted network connections. This may be offered by the Https technology that makes it tricky for an attacker to interfere with the network traffic (Reid & Caelli 2005, p. 129). The Https is efficient because of the safe sockets layer (SSL) facility that shields the web-based network interchange from unauthorized users. The Https also uses certificates that can prove the

identity of the servers a computer is interacting with over the internet (Strebe 2006, p. 18-23).

List of References

Lockhart, A. (2007). Network security hacks. Beijing: OReilly.

Print.

Luettmann, B., & Bender, A. (2009). Man-in-the-middle attacks on auto-updating software. Bell

Labs Technical Journal, 3(2), 131-138.

Luotonen, A. (1998). Web proxy servers. Upper Saddle River, Nj: Prentice Hall.

Print.

Reid, J., & Caelli, W. (2005). “ DRM, Trusted Computing and Operating System Architecture.”

Australian Computer Society, Inc., 44, 127-135.

Strebe, M. (2006). Network Security Foundations Technology Fundamentals for IT Success.

Hoboken, John Wiley & Sons.