Securing Military Information Systems on Public Infrastructure

Pieter Botha, Shazia Vawda, Priaash Ramadeen, Alex Terlunen

Abstract: Military information systems require high levels of security to protect sensitive information within these systems. Encrypted private networks are a common method of securing such systems. However these networks are not always available or practical to set up in time for scenarios which require real time information. This may force communications to utilise public infrastructure. Securing communications for military mobile and Web based systems over public networks poses a greater challenge compared to private encrypted networks. Several security mechanisms from commercial enterprise and social networking systems were adopted and customised in order to secure Cmore, a Web based real time distributed command and control system developed by the Council for Scientific and Industrial Research (CSIR). This paper highlights the security architecture of Cmore and discusses some of the successes and challenges encountered during the design and development of the Cmore architecture. Cmore has been successfully utilised and tested in several field experiments and operations. The resulting security architecture can be applied to other Web and mobile systems.

Keywords: Internet, mobile, information security