available at www.sciencedirect.com

www.compseconline.com/publications/prodinf.htm

Information Security Technical Report

Secure Mobile Architecture (SMA) – A way to fix the broken Internet

*Richard H. Paine**

6115 72nd Dr NE, Marysville, WA 98270, USA

Keywords:
Internet Protocol (IP)
Secure Mobile Architecture (SMA)
End-to-end
Public Key Infrastructure (PKI)
TempCert

ABSTRACT

The Internet is broken. There have been many attempts to fix it, but they are all complex and very difficult to implement and none of them answer the fundamental questions of what is wrong with it. The first basic flaw is the very nature of the Internet Protocol address. It is treated as both a name and an address to deliver the information to its end-to-end destination. In addition, the security of the protocol is dependent on that address. The second major flaw is the inability of the Internet protocols to address mobility with fast and secure handoff. The Secure Mobile Architecture (SMA) fundamentally addresses these flaws in the very nature of the Internet Protocols. It does this by treating the IP layer as an insecure transport layer. It requires four elements to effect this transformation of the Internet. It can be integrated into existing Intranets. It can function easily in the namespace of an Internet service provider (ISP), an enterprise, or governments. The rest of this chapter will take you through the architecture and its elements.

1. Introduction

The SMA architecture was published in February 2004. The group that developed it included representatives from Boeing, Lockheed, IBM, HP, Motorola, Netmotion Wireless, and a number of universities. In late 2003, Richard Paine started to lay the groundwork for a project to implement an SMA pilot through a Boeing Network Centric Operations (NCO) 2004 project. This funded project enabled the SMA project to develop an SMA Boeing Intranet infrastructure that is an integral part of the Boeing Intranet as a pilot. The features of the SMA pilot demonstrations in December 2004 are illustrated in Fig. 1.

The implementation was designed by Steven C. Venema of the Phantom Works (PW) M&CT Manufacturing Technology group. His experience was that many of the manufacturing problems he has run into are those associated with the network. There are four primary elements that are the major components of the SMA. Together, the four components make up the Secure Mobile Architecture (Fig. 2).

He took the major components from the architecture and implemented them in the following ways.

In order for SMA to be secure, there must be a secure means of authenticating the users. This secure means was being worked by the Manufacturing Technology group before SMA started and is known as Temporary Certificates, or ''TempCerts''. The TempCerts are being issued based on the Boeing secure badge and the ability of an authenticated user to obtain a certificate from the Boeing PKI for a limited amount of time. The focus of this limited amount of time is a shift in the factory that is generally 8–12 h long. This process time-limits the risk of storing a certificate on an end user device. The process is noted in Fig. 3.

The Host Identity Protocol (HIP) element of the SMA architecture enables secure communications by putting a cryptographic identity on every packet. One of the most persistent

* Tel.: +1 206 854 8199; fax: +1 425 865 2965.
E-mail address: richard.h.paine@boeing.com

1363-4127/$ – see front matter © 2007 Elsevier Ltd. All rights reserved.
doi:10.1016/j.istr.2007.04.003

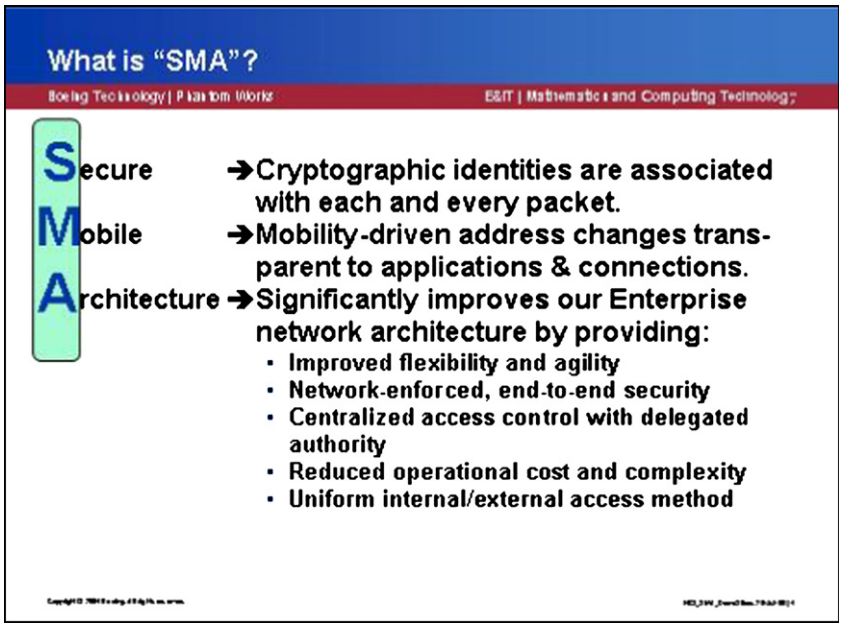

Fig. 1 – Definition of SMA.

problems on the Internet is the fact that security for the TCP/IP communications has previously always been based on an IP or an MAC address. This is a weakness that permeates and complicates all present and future work across the Internet. This weakness leads to spoofing and potential intercept of packets and applications on the network. This has led SMA to specifying the Internet Engineering Task Force's (IETF) HIP which provides a secure pair-wise end-to-end security association (SA) identified by a cryptographic identity. The cryptographic identity is included in every packet and sent across the network in this pair-wise SA. Fig. 4 shows the mechanism required and the packet orientation.

The implementation uses a virtual directory to retain information about the communications that enable SMA to be an effective namespace and still be a functional member of the Internet. There is a DNS proxy for the Internet namespace that intercepts any DNS requests in the namespace and checks against the directory for the current address, even for its own address. This address can be either an IPv4 or an IPv6 address. This allows the address to change without affecting the roaming mobile device. The mobile device can move throughout the namespace and retain the ability to transparently transition across network subnets and retaining their security association. In addition, all the packets exchanged in this namespace are identified by their cryptographic identity that is issued by the entity's PKI (Fig. 5).

By retaining the information in a directory or a database instead of in registers in the Operating System, the SMA network can be secure and mobile. In addition to the address being in a data store, part of the SMA is enabled by being location-enabled. The SMA secure network uses location to enable security zones and policy enforcement based on its knowledge

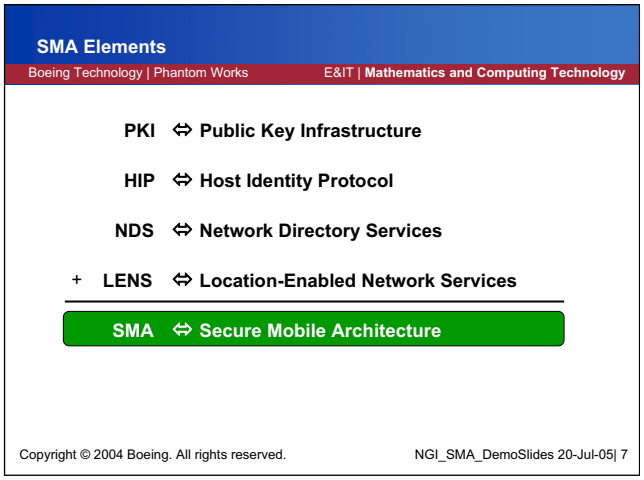

Fig. 2 – SMA elements.

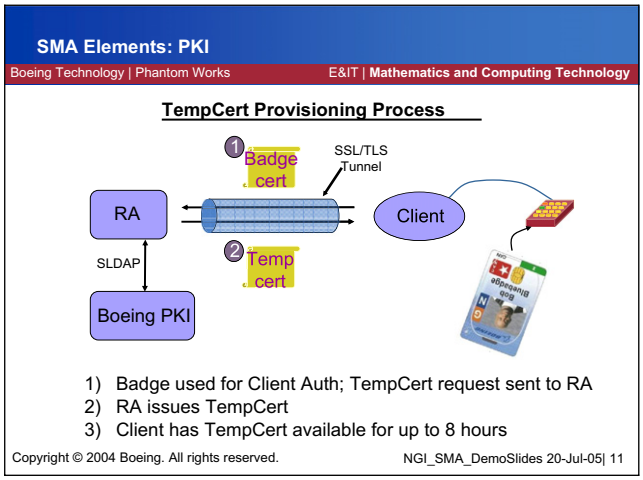

Fig. 3 – TempCert provisioning process.