Chapter 7.5
XML Security with Binary XML for Mobile Web Services

Jaakko Kangasharju
Helsinki Institute for Information Technology, Finland

Tancred Lindholm
Helsinki Institute for Information Technology, Finland

Sasu Tarkoma
Helsinki Institute for Information Technology, Finland

ABSTRACT

In the wireless world, there has recently been much interest in alternate serialization formats for XML data, mostly driven by the weak capabilities of both devices and networks. However, it is difficult to make an alternate serialization format compatible with XML security features such as encryption and signing. We consider here ways to integrate an alternate format with security, and present a solution that we see as a viable alternative. In addition to this, we present extensive performance measurements, including ones on a mobile phone on the effect of an alternate format when using XML-based security. These measurements indicate that, in the wireless world, reducing message sizes is the most pressing concern, and that processing efficiency gains of an alternate format are a much smaller concern. We also make specific recommendations on security usage based on our measurements.

INTRODUCTION

In recent years, two developments in the computing landscape appear to be having a significant impact on the future. One of these is the rising popularity of XML (extensible markup language), which is now being used also for machine-to-machine messaging, most notably in the form of SOAP (World Wide Web Consortium [W3C], 2003a, 2003b). The other is the increasing number of available mobile devices with sophisticated networking capabilities, potentially heralding an age of truly pervasive, or ubiquitous, computing (Satyanarayanan, 2001; Weiser, 1993).

Copyright © 2009, IGI Global, distributing in print or electronic forms without written permission of IGI Global is prohibited.

In a pervasive computing situation, a person carries a small computing device, such as a smart phone or a PDA (personal digital assistant). These kinds of devices have much less processing power available than typical personal computers. They are normally battery powered, meaning that the available energy should not be squandered, especially as battery capabilities tend to increase very slowly over time. Finally, their connection to other computers, including to the Internet, will often be on a low-bandwidth, high-latency wireless link, though in some places more powerful devices can take advantage of wireless LAN (local area network) hotspots that provide much better network connectivity.

There has been concern that XML is not suitable for use on mobile devices due to its verbosity and processing requirements. Because of this, there have been proposals to replace XML with an alternate binary XML format, which would be compatible with XML on some level but is purported to be more compact and more efficient to process. When communicating with existing systems on a fixed network, gateways can convert between this binary format and XML to permit piecewise introduction of the new format. A well-known gateway-based solution is the wireless application protocol (WAP; WAP Forum, 2001a) that includes one of the earliest binary formats for XML (W3C, 1999).

However, compatibility achieved through gateways breaks down in the case of security features such as encryption and digital signatures. If serialized content is encrypted, a gateway cannot convert it, so the ultimate recipient needs to be able to understand the used format. In the case of signatures, the signature will be computed over the serialized form, so again the recipient will need to be able to regenerate that version.

In this article, we explore the effect of a binary format in the context of XML security, in particular to determine what benefits, if any, such a format could bring. We focus on communication between a mobile device using a wireless link and a server in a fixed network. While direct peer-to-peer communication between mobile devices is also an important topic, the issues of compatibility arise more strongly in the client-server case due to the number of existing deployed systems.

The main contributions of this article are a review of options for achieving compatibility between different formats and a comparison. We present extensive measurements, of both time and energy consumption, that were performed with real mobile devices over real networks. Finally, drawing on our measurements, we make recommendations for new features in XML security specifications that would support mobile devices better than is currently achievable.

We begin the article with usage scenarios supporting fine-grained XML security and an overview of the relevant specifications. We continue by presenting three different compatibility options to allow use of a binary format, and then show measurements using our proposed option. Next, we review related work, and finally conclude the article with specific recommendations and some view of the future.

XML SECURITY

There are several existing ways to secure network traffic, many of which can be deployed immediately without needing to worry about interoperability at the application layer. On the network layer, it is possible to use IP (Internet protocol) security (Kent & Atkinson, 1998) for authentication and encryption. Transport-layer connections can be secured with SSL (secure sockets layer; Freier, Karlton, & Kocher, 1996), which provides authentication and a secure communication channel. The problems with these are that they only secure network traffic, so stored data need to be reencrypted and re-signed, and they lack the granularity to support some use cases that require multiple transport-layer connections.

18 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:
www.igi-global.com/chapter/xml-security-binary-xml-mobile/26682

Related Content

The Benefits and Challenges of Mobile Technologies in Education: A Perspective for Sub-Saharan Africa
Julius Sonko (2015). *Promoting Active Learning through the Integration of Mobile and Ubiquitous Technologies (pp. 55-73).*
www.irma-international.org/chapter/the-benefits-and-challenges-of-mobile-technologies-in-education/115468

Resource Allocation for Multi Access MIMO Systems
Shailendra Mishraand D. S. Chauhan (2011). *International Journal of Mobile Computing and Multimedia Communications (pp. 36-50).*
www.irma-international.org/article/resource-allocation-multi-access-mimo/55866

Image-Based 3D Reconstruction on Distributed Hash Network
Jin Hua Zhongand Wan Fang (2018). *International Journal of Mobile Computing and Multimedia Communications (pp. 58-75).*
www.irma-international.org/article/image-based-3d-reconstruction-on-distributed-hash-network/214043

Taxonomies, Applications, and Trends of Mobile Games
E. Jeongand D. Kim (2007). *Encyclopedia of Mobile Computing and Commerce (pp. 928-932).*
www.irma-international.org/chapter/taxonomies-applications-trends-mobile-games/17197

Optimal Channel Assignment Algorithm for Least Interfered Wireless Mesh Networks
Tarik Mountassir, Bouchaib Nassereddine, Abdelkrim Haqiqand Samir Bennani (2014). *International Journal of Mobile Computing and Multimedia Communications (pp. 54-67).*
www.irma-international.org/article/optimal-channel-assignment-algorithm-for-least-interfered-wireless-mesh-networks/113772