Fixed-Mobile Convergence: Critical Issues for Wireline and Wireless Carriers

For traditional wireline carriers, Fixed-Mobile Convergence (FMC) represents an opportunity to reclaim market share and revenue lost to mobile telephony. At the same time, wireless carriers are looking to reduce connectivity costs. According to ABI Research, operators will invest $450 million in capital infrastructure over the next five years and generate $97 billion in service revenue from FMC applications by 2011. To achieve this remarkable return on investment, carriers must resolve critical usability issues, install accounting systems that enables network usage billing for all consumers, and employ security measures that meet consumer privacy demands.

To enable consumers to move across different networks without disrupting voice or data, carriers will need proven solutions that support Internet Engineering Task Force (IETF) protocols like MOBIKE and Mobile IP, enable the widest possible deployment by supporting the largest range of gateway vendors, and deliver world-class security that meets the most stringent government criteria.

INTRODUCTION

For traditional wireline carriers, Fixed-Mobile Convergence (FMC) represents an opportunity to reclaim market share and revenue lost to mobile telephony by embracing new technologies like DSL, VoIP, and WiFi networks backed by broadband. Meanwhile, wireless carriers look to take advantage of the less expensive connectivity options that make them more competitive.

From a user's perspective, it is inconvenient to carry and monitor multiple physical devices. Also, needing different devices and having separate billing for each creates administrative and operational inefficiencies that can impact an organizations bottom line.

> ***"Operators are seeing their core voice revenues come under pressure from VoIP, and they need to minimize call substitution. One way is to provide services over the broadband fixed network using a mobile device. Both dual use and single use devices will be able to do that over Wi-Fi and micro cellular access points in the home and office."***
>
> Ian Cox,
> ABI Research analyst

With a guiding vision of enabling people to move seamlessly between WLANs in corporate offices, public hot spots, and homes using the same mobile device, it is unsurprising to find that carriers, handset manufacturers, hardware vendors, and networking solution providers are laying the groundwork for the convergence of Wi-Fi and cellular technologies.

Already, leading handset manufacturers like Motorola and Nokia are marketing dual-mode handsets that have both Wi-Fi and cellular capabilities. According to Infonetics Research, the Wi-Fi phone market is expected to reach $3.7 billion by 2009. This is up from $125 million in 2005 .

And given the strong growth in the market, ABI Research found that wireline and wireless network operators will invest over $450 million in capital infrastructure over the next 5 years for fixed-mobile convergence. Further,

ABI Research predicts that operators will generate $97 billion in service revenue from FMC applications in 2011 – mainly from offering lower fixed-line call charges to mobile users.

Experts agree that consumers and businesses will benefit from this revolution in telecommunications, but for the FMC model to be fully embraced by network operators, industry must resolve challenges relating to the creation of secure, billable, and user-friendly services.

FIXED-MOBILE CONVERGENCE GAINING MOMENTUM

The adoption of Bluetooth technology is a good case study for FMC. Specifications that ensured interoperability and security were finalized in 1998. Today, Bluetooth technology is used in over 1 billion devices. Given the fact that the benefits of FMC extend to a larger base of consumers and the positive impact FMC will have on wireline and wireless carriers, strong global adoption of FMC technology is expected.

Already, T-Mobile USA has rolled out a dual-mode Wi-Fi-Cellular service to its customers in Seattle. Customers using the service are able to make unlimited calls on their cellular phones when they are on a Wi-Fi network.

And given the results of a recent Sage Research survey, other carriers are expected to follow suit. Conducting a survey of IT decision-makers in companies with over 1,000 employees relating to Fixed-Mobile Convergence, Sage Research was able to rank the key perceived benefits of FMC. According to the research, the highest ranked benefits were having a single number and bill for mobile employee communications, increasing employee accessibility, and boosting employee productivity. Participants also ranked the availability of integrated PBX features and reducing corporate cellular expenses as high secondary benefits. [1]

Although wireline and wireless carriers will drive many critical decisions, the burden of developing new specifications will fall to handset vendors. In fact handset vendors like Motorola and Nokia are already tackling the problem by building dual-mode devices that can use both traditional wireless networks as well as unlicensed mobile access (UMA) networks that offer cheaper connectivity for voice and data.

IPSEC: A CRITICAL PART OF FMC ADOPTION

The key to widespread adoption is the seamless hand-off and roaming between cellular and fixed IP-based wireless networks, such as Wi-Fi and Bluetooth. Regardless of the application (data, VoIP, etc.), the IP address assigned to the user is based on the point of network attachment. If the user moves from a cellular network to a WiFi network, the IP address assigned to the device changes. IPSec based VPNs utilize the IP address of the device. If the IP address changes, the session for the old IP address needs to be terminated and a new session established utilizing the new IP address. For the user, this means logging in again, which might entail entering a password, security token ID number, etc. This is bothersome and undermines the value of converged fixed and mobile networks for end-users.

[1] http://www.crn.com/showArticle.jhtml?articleID=193501713

Beyond the issue relating to ease-of-use, the FMC model needs to demonstrate that networks are secure and capable of protecting customer privacy. For example, in a FMC scenario where wireline carriers enable customers to use a single handset at home, in the office, or while on the road, a carrier will transport calls using VoIP rather than cellular networks. But VoIP lacks full-featured security support.

Signaling can be secured by running SIP protocols over an SSL connection, but SSL can't encrypt the channel that contains the actual voice or data transmission. And since the FMC model necessitates calls traversing over untrusted networks, standards bodies like UMA (www.umatechnology.org) and 3GPP (www.3gppp.org) have chosen IPSec – one of the oldest and most proven IETF security protocols – as the best way to protect customer privacy.

Using IPSec, carriers can create an encrypted tunnel that authenticates a user by way of a VPN gateway and a password, SecureID token, or digital signature. Internet Key Exchange (IKE), which provides the initial negotiation of IPSec, sets all the required parameters for the tunnel (i.e. encryption type, authentication type, etc.). UMA and 3GPP have both proposed extensions to IKEv2 that provide companies with a common standard to ensure interoperability. Two standards IKEv2 standards that are critical to FMC adoption by users and industry are MOBIKE and Mobile IP.

ENABLING SEAMLESS ROAMING WITH MOBIKE AND MOBILE IP

MOBIKE

The Mobility and Multihoming (MOBIKE) protocol was developed by the Internet Engineering Task Force (IETF) as a mechanism to maintain IPSec Tunnels when a user moves his point of network attachment, and the IP Address changes, as defined in RFC 4555. MOBIKE is based on Internet Key Exchange Version 2 (IKEv2 – RFC 4306) protocol. During the IKE Initialization exchange (IKE_INIT) between the client and the gateway, the peers inform each other that they support MOBIKE.

Later, after VPN tunnel establishment, the client may detect that it has moved to a new point of network attachment, resulting in a change to its IP address. The client then sends an INFORMATIONAL message to the gateway, using the new IP Address, and containing a request to update the security association addresses (UPDATE_SA_ADDRESSES). All further traffic sent by the client uses this new address. The gateway, upon receipt of the UPDATE_SA_ADDRESSES will start using this new address as the destination in its outgoing traffic.

In addition, MOBIKE provides a mechanism called "return routability check," which can optionally be used to determine if the peer is reachable using the new address. MOBIKE also provides a mechanism for handling clients that are located behind Network Address Translators (NAT). Further details on these capabilities can be found in RFC 4555.

The primary mobility feature of MOBIKE enables everything inside the IPSec tunnel to be remain unaffected by the changes to the tunnel header IP address. As a result, applications running inside a MOBIKE-controlled IPSec tunnel might not detect the movement since their IP addresses remain constant. The MOBIKE protocol should be able to perform the following operations:

INNOVATIVE PRIVACY PROTECTION

- Inform the other peer about the peer address set
- Inform the other peer about the preferred address
- Test connectivity along a path and thereby detect an outage situation
- Change the preferred address
- Change the peer address set
- Ability to deal with Network Address Translation devices

Mobile IP

Mobile IP is an IETF standard communications protocol that is designed to allow mobile device users to move from one network to another while maintaining a permanent IP address. Mobile IP is fully described in IETF RFC 3344.

Mobile IP provides an efficient, scalable mechanism for roaming within the Internet. Using Mobile IP, nodes may change their point-of-attachment to the Internet without changing their IP address. This allows them to maintain transport and higher-layer connections while moving. Node mobility is realized without the need to propagate host-specific routes throughout the Internet routing fabric.

Mobile IP enables a mobile node to have two addresses - a permanent home address and a care-of address, which is associated with the network the mobile node is visiting. There are two kinds of entities in Mobile IP:

- A home agent stores information about mobile nodes whose permanent address is in the home agent's network.
- A foreign agent stores information about mobile nodes visiting its network. Foreign agents also advertise care-of addresses, which are used by Mobile IP.

When a node wants to communicate with the mobile node, it uses the home address of the mobile node to send packets. These packets are intercepted by the home agent, which uses a table and tunnels the packets to the mobile node's care-of address with a new IP header, preserving the original IP header. The packets are decapsulated at the end of the tunnel to remove the added IP header and delivered to the mobile node.

When acting as sender, a mobile node simply sends packets directly to the other communicating node through the foreign agent. If needed, the foreign agent could employ reverse tunneling by tunneling mobile node's packets to the home agent, which in turn forwards them to the communicating node.

The Mobile IP protocol provides:

- An authenticated registration procedure by which a mobile node informs its home agents of its care-of addresses
- An extension to ICMP Router Discovery, which allows mobile nodes to discover prospective home agents and foreign agents; and
- The rules for routing packets to and from mobile nodes, including the specification of one mandatory tunneling mechanism and several optional tunneling mechanisms.

MOBIKE AND MOBILE IP IN THE REAL WORLD

To support a VPN connection to the home network, several processes are possible. One common example – which is specified by 3GPP2 in X.S0028-200 v0.3 – IKEv2 is used to establish the VPN tunnel to the security gateway. The initial IPSec tunnel is created using the temporary Mobile IP address (received from the gateway) as the Tunnel Inner Address (TIA). The Home agent address is retrieved from the gateway during this IKEv2 exchange. The Mobile IP client uses the Home Agent to complete the Mobile IP Registration, and obtains the Home Address (HoA) or the real IP address that it is assigned.

If the HoA is the same as the TIA, then the original IPSec tunnel can be used to protect traffic between the home agent and the mobile node. If the HoA is different than the TIA, then a new IPSec tunnel will be created using the HoA. This process requires that the IPSec/IKEv2 protocol stack be "Mobile IP Aware." The mobile IP stack and the IPSec stack need to exchange TIA, HoA and HA information.

If the user moves to a new IP network, MOBIKE can be used to update the IPSec tunnel endpoints without the need to re-negotiate Mobile IP and IKEv2. Without the inclusion of MOBIKE, the client would need to re-negotiate both Mobile IP and IKEv2. This would force the user to log back into the VPN.

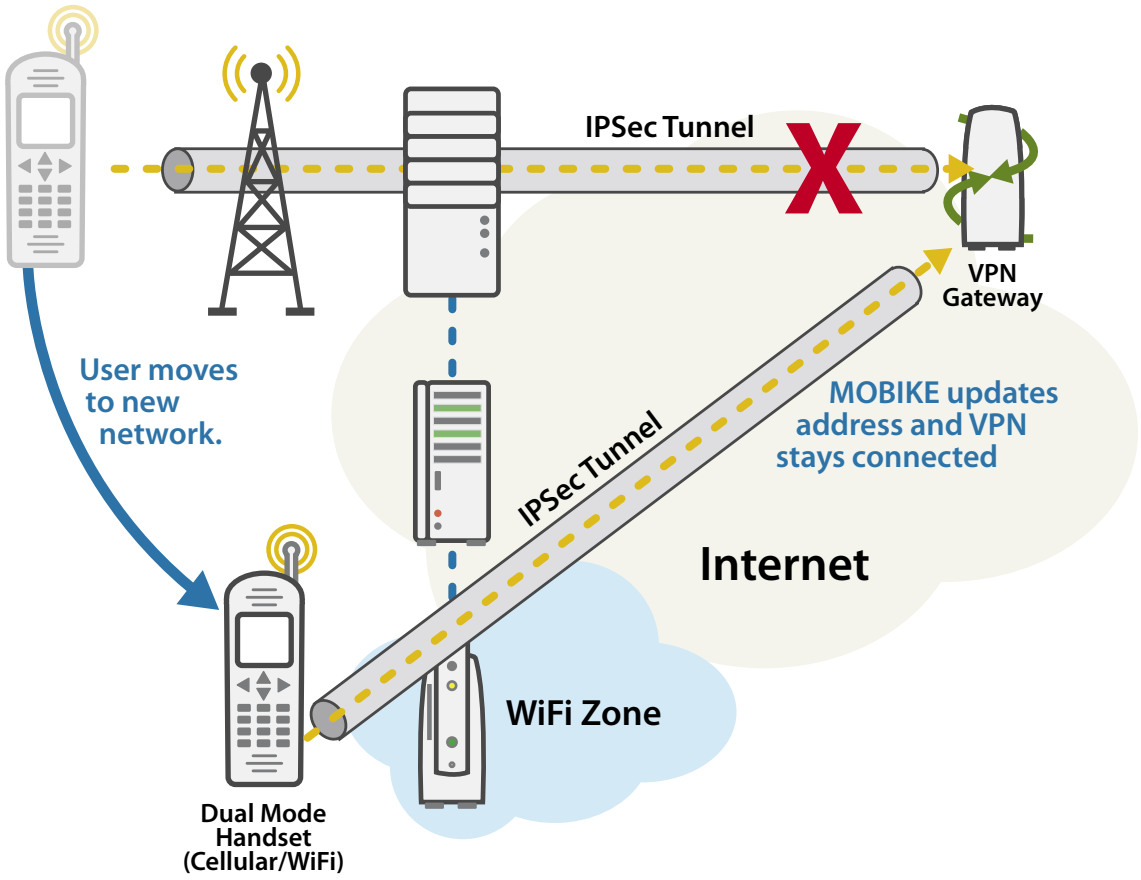

Figure 1: Demonstrates how MOBIKE helps keep users connected to their VPN.

Without MOBIKE, moving between a cellular and Wi-Fi networks becomes problematic because the IKE protocol will need to re-negotiate and establish a new Security Association every time a user moves between networks. As a result, an individual will lose his connection to a corporate VPN every time he migrates from one network to another. Since IKE will terminate the initial VPN connection, users will have to initiate a new VPN connection and re-enter passwords. With MOBIKE, the IP address associated with the IKE_SA is updated. The outer tunnel address is changed, but this is transparent to applications. VPN usage isn't disrupted and users don't need to go through the login procedure again.

The Mobile IP stack enables users to move between networks without interruption by ensuring that IPSec is notified of any new IP addresses generated. Certicom Security Builder IPSec 2.10 provides API that enables Mobile IP to inform IPSec of these address changes.

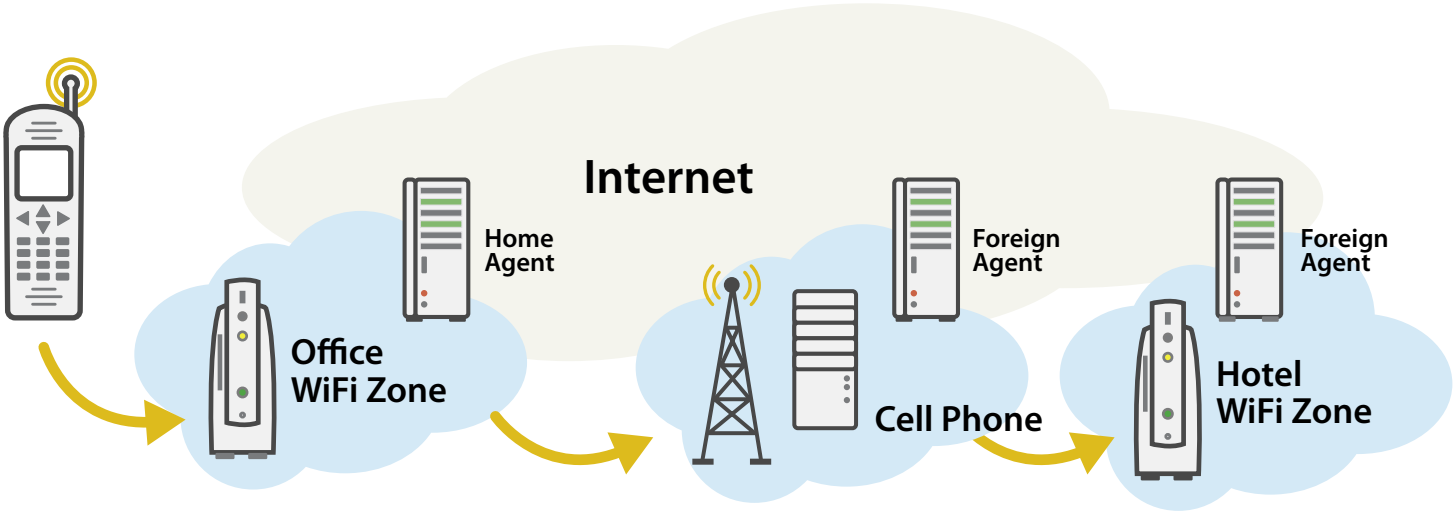

Figure 2: Demonstrates how Mobile IP (RFC-3344) allows for total user mobility across different networks. Shows how Home Agent Tunnels all traffic to the user, regardless of point of network attachment

CERTICOM IPSEC 3.0: ENABLING SECURE VPN ACCESS ACROSS CELLULAR AND WI-FI NETWORKS

Based on award-winning technology, Security Builder IPSec 3.0 is a cross-platform IPSec module that enables developers to easily embed standards-based VPN access into resource-constrained devices.

With the smallest code size and the industry's widest gateway support, Security Builder IPSec 3.0 provides efficient security and enables better performance than is normally achievable with traditional IPSec implementations.

This proven solution, which is used by the world's leading handset manufacturers like Sony Ericsson, Nokia, and Motorola, now supports the latest industry standards – including IP Key Exchange version 2 (IKEv2), MOBIKE, and Mobile IP. As a result, developers can use Security Builder IPSec 3.0 to build advanced applications for Unlicensed Mobile Access (UMA), Internet Multimedia Subsystems (IMS), Fixed Mobile Convergence (FMC) and other emerging third generation partner project (3GPP) services.

And when configured with Security Builder GSE, a FIPS 140-2 Validated cryptographic module, devices and applications quickly gain government-approved security.

Security Builder IPSec 3.0 is a mature product and as such it supports a variety of cryptographic algorithms including 3DES, AES, ECDH, RSA, Diffie-Hellman, SHA-1, SHA-2, MD5 and EAP. Security Builder IPSec also provides authentication support for one-time-password tokens (i.e. SecurID or Safeword). This can be further extended to provide support for smartcards and cryptographic hardware acceleration.

Unlike most other IPSec toolkits, where developers must test and create a compatible implementation with each individual VPN gateway vendor, Security Builder IPSec 3.0 includes pre-defined profiles that allow immediate compatibility with most leading VPN gateway vendors. Certicom continually monitors VPN compatibility and adds new features regularly so that developers can focus on their primary development goals, not VPN updates.

In addition, Security Builder IPSec builds on Certicom's expertise with constrained platforms and can be used to secure communication on a variety of devices. Compile the code to provide only those features you need for compact implementations and gain better performance than is normally achievable with traditional IPSec. Elliptic Curve Cryptography (ECC)-based algorithms—supported by industry leading VPN Gateways—enable faster key exchanges, while IKEv2 provides for greater standardization and faster IPSec tunnel negotiations.

To learn more about IPSec 3.0, visit: www.certicom.com/ipsec

about certicom

Certicom protects the value of your content, applications and devices with security offerings based on Elliptic Curve Cryptography (ECC). Adopted by the National Security Agency (NSA) for classified and sensitive but unclassified government communications, ECC provides the most security per bit of any known public-key scheme.

Visit www.certicom.com.

North America 1.800.561.6100
EMEA +44.20.7484.5025
International +1.905.507.4220
E-mail info@certicom.com
www.certicom.com