SystemEXPERTS

Wireless VPN's: Enablers and Inhibitors

Philip Cox

Consultant

Thursday September 13, 2001

Focus of this Session

- The overall focus of this session is to identify the issues that affect our ability to cost effectively deploy a secure, manageable, and robust mobile VPN (mVPN) infrastructure

What are the Inhibitors?

- Limited resources
- “Lossy” networks
- Low bandwidth
- IP mobility issues as the user moves from base to base
- Authentication questions

Inhibitors, cont.

- Billing and service model
- Security of Elliptic Curve Cryptosystem (ECC)
- Incompatibility between wireless NIC drivers and VPN client software
- Little to no commercial development
- Let’s look a bit deeper …

Limited Resources

- CPU
  - Wireless devices have historically not had the memory and CPU speed to support the necessary encryption processing
- Memory
  - RAM & non-volatile
- Power
- I/O
  - Keypad
  - Screen
  - Color

Low Handheld Bandwidth

- Cellular is where the problem lies
  - 9.6-19.2k is the best at this time
  - 3G technology will make this better, but we are a long way off
- WLANs are pretty quick, giving better than T1 speed in most cases
  - 802.11b up to 11Mbs
  - 802.11e +20Mbs
  - 802.11a & Hyperlan are even faster (54Gbs)

“Lossy” Networks

- Wireless networks are more “lossy” than their wired cousins
- Makes it hard on connectionless protocols
- if the VPN is using a UDP-based key exchange protocol, like IKE, it will be dog slow
  - If it completes at all
  - TCP-based systems will have more success
    - But the VPNs are usually proprietary
    - SSH is not

Network Latency

- Many Wireless networks introduce latency beyond what certain protocols can handle
- Example:
  - Default PPTP cannot handle the latency of satellite networks
    - Typically more than a second, instead of a tenth of a second or less
- You will need to change parameters to try and tweak the implementation to behave over satellite
- A specialized gateway to "proxy" your requests

IP mobility

- issues as the user moves from base to base
- Mobile IP
  - RFC 2002: IP Mobility Support
    - transparent routing of IP datagrams to mobile nodes in the Internet
  - RFC 2003: IP Encapsulation within IP
    - specifies a method by which an IP datagram may be encapsulated (carried as payload) within an IP datagram, as a means to alter the normal IP routing for datagrams
  - RFC 2004: Minimal Encapsulation within IP
    - This document specifies a method by which an IP datagram may be encapsulated (carried as payload) within an IP datagram, with less overhead than "conventional" IP encapsulation that adds a second IP header to each encapsulated datagram
  - RFC 2006: Management Information Base (MIB) for Mobile IP
    - Based in SMIv2

Authentication questions

- How do you do it?
  - Use standard authentication mechanisms?
    - They interoperate, but are probably too inefficient for the devices and networks
  - Use SIM-card-based authentication
    - If using the SIM card, are all your eggs in one basket?
    - How many SIMs do you want to carry ☺
- Is there a single source?

Billing and service model

- All this needs to be paid for
- Billing models will have to accommodate the fact that you can’t see the traffic
  - Will be per packet/per minute versus "stateful"-ness of the VPN connection
- This is *arguably* the most important factor in widespread deployment

Security of Elliptic Curve Cryptosystem

- It is a relatively new technology
  - Because it's new, it will take time to be reviewed
  - Much already done, but time will tell
- Offers significant efficiency savings due to its added strength-per-bit
  - This is advantageous in many applications, particularly when computational power, bandwidth, or storage space are limited

Wireless Card Incompatibility

- Firmware support and driver support are different for different chips
- Developers develop to a platform, thus leaving others out …
- An WLAN example:
  - Orinoco cards work with Ashley Laurent VPN client
  - Orinoco cards don’t appear to work with IRE/SafeNet client
    - This scenario actually involved extra Orinoco drivers for RAS-style authentication with a wireless access server and the problem may be these RAS drivers (not the radio card drivers)
  - VPN clients insert themselves into the stack in different ways, and manufacturers haven't yet rigorously tested compatibility of wireless NIC/VPN client combos.
  - computationally challenged PDAs and handsets can't grind out 3DES

Little to no commercial development

- At this point in time, there is not significant development into this arena
- It is new technology, so this should change drastically in the next year or so

So What's the answer?

- Laptops
  - Many solutions, as numerous as the wired VPN clients you can buy
  - Basically IPSec, PPTP, L2TP, and Proprietary
    - Lots of tunnel types: SSH & SSL/TLS
  - Could consider them interoperable (maybe ☺)
- Handhelds
  - Almost all are proprietary
  - IPSec is on the rise though
  - Certicom "movianVPN" seems to have the most "brand" recognition

A closer look at movianVPN

- Supports Popular Handheld Devices
  - IPSec client for Palm and WindowsCE
- Supports two-factor authentication such as SecureID (for Alcatel, Cisco, and Nortel gateways)
- Uses Certicom's Elliptic Curve Cryptography (ECC) for Internet Key Exchange (IKE)
- Broad Number of Wireless Connectivity Options
  - CDPD, CDMA, GSM, iDEN, Wireline

movianVPN, cont.

- Basis for iPassConnect PDA service
  - Requires a modem and two pieces of software on the PDA
  - Lightweight version of iPass' dialer, called iPass Synch and movianVPN
    - Users dial up an iPass-affiliated ISP, then establish a VPN
- Interoperable with Leading VPN Gateways
  - Alcatel 7130 Secure VPN, Check PointTM VPN-1, Cisco VPN Concentrator 3000, Intel® NetStructureTM 3100 Series (For Palm: Handspring Prism only), Nortel Contivity Extranet Switch, Radguard clPro, Symantec PowerVPN Series

Viatores 3.0 Mobile VPN (mVPN)

- Ecutel Inc. (www.ecutel.com)
- Seamless roaming
- Basic client server technology
- Based on
  - Mobile IP
  - IPSec

Other Commercial VPNs

- Texas Instruments/SafeNet VPN
- Columbitech's Wireless VPN
- Bell Mobility’s Wireless VPN
- Ericsson Wireless Office VPN
- MobileLogic Wireless VPN
- V-One SmartGate/SmartPass
  - Palm III/V, Windows CE/ PocketPC
- GoAmerica
  - Just VPN from their server to your site

Conclusions

- Some of the inhibitors have to do with wireless devices more so than laptops
- Things will be getting better over time
- Within the next 3 years solutions will be in wide spread use

References

- VPN Mail List @ Security Focus
  - vpn@securityfocus.com
- Web Sites
  - http://kubarb.phsx.ukans.edu/~tbird/vpn.html

SystemEXPERTS

LEADERSHIP IN SECURITY

Philip Cox
Consultant

Phil.Cox@SystemExperts.com
530-887-9251 direct
530-887-9253 fax
978-440-9388 main
http://www.SystemExperts.com/

NETWORLD +INTEROP