SSL VPNs: An IETF Perspective

IETF 72, Dublin

Paul Hoffman, VPNC

Overview

- Why this might be interesting
- Intro to SSL VPN technologies
- Where SSL VPNs use IETF technologies, and where they make up their own
- Some lessons learned

NIST SP 800-113, *Guide to SSL VPNs*

- Written by Paul Hoffman, Sheila Frankel, and others
- Published July, 2008
- Target audience: USgovt federal IT workers and managers, and other folks like them

Wide deployment of SSL VPNs

- SSL VPNs have completely swamped IPsec VPNs for remote access in recent years
- We’re still living with the perception that “setting up IPsec is hard”
- People have a perception that adding tunneling extensions to the OS is dangerous; somehow, having your browser do it for you silently feels better

SSL VPN technology taxonomy

- Two types of SSL VPNs: *portals* and *tunnels*
- Most SSL VPN gateways now offer both
- The difference is mostly invisible to users even though they are completely different technologies
- Some vendors have also rolled their own method, but they are often getting rid of those and standardizing on portals and/or tunnels

SSL portal VPNs

- “Allows a user to use a single standard SSL connection to a Web site to securely access multiple network services”
- The basic idea is that the SSL VPN gateway proxies web servers on the inside network and rewrites the URLs on the fly
- Example: “http://someinside.example.com/foo” might become “https://ourgateway.example.com/someinside/foo”

Problems with URL rewriting in portal VPNs

- URL rewriting is easy in theory, hard in practice, and certainly not an IETF standard
- Some web apps don’t do this right (mostly Exchange Outlook Web Access)
- Users expect file access, so portals need to make some file access page
- Javascript is difficult but tractable
- Flash, Flash competitors, and Java are really hard

Security issues with portal VPNs

- Most portal-based VPNs will proxy internal HTTPS hosts by terminating HTTPS on both sides
- This is a silent proxy-in-the-middle
- Some SSL VPNs will cache or hold authentication information for users to prevent them from having to log in to local web servers each time

SSL Tunnel VPNs

- “Allows a user to use a typical Web browser to securely access multiple network services through a tunnel that is running under SSL.”
- “Requires that the Web browser be able to handle specific types of active content (e.g., Java, JavaScript, Flash, or ActiveX) and that the user be able to run them.”

How SSL VPN tunnel applets work

- Lots (!) of different ways
- They even change between versions of the gateway firmware
- No standard port for tunneling
  - Some choose already-used ports “to get through firewalls”
- The tunnel method is often considered proprietary

Use of standardized technologies in SSL VPNs

- TLS
  - Most servers do TLS 1.0
  - Most use the MUST ciphersuites, some let you choose which ones need to be used
- HTTP
  - Almost all do HTTP 1.1
- Some standardized authentication mechanisms such as certs, EAP, and 802.1x

Non-IETF technologies

- Portal VPNs
  - URL re-writing by heuristics
  - Silent gateway-in-the-middle for HTTPS
- Tunnel VPNs
  - Pushing the tunnel applet to the browser
  - Type of tunneling (GRE, IPinIP, roll your own)
  - No interoperability is expected in the market

Lessons for the IETF (1)

- When we create hammers, others will invent new kinds of nails
- Remote access is often considered a different problem than gateway-to-gateway even if the solutions will end up providing similar security
- For many users, encryption that they understand is enough “security” to meet their needs

Lessons for the IETF (2)

- The IETF has signaled that lots of different tunneling mechanisms are good, so we should not be surprised when people make up their own or vary one of the standardized ones
- We have lots of standardized auth mechanisms, so vendors will often pick more than one of them