Secure Internet Solutions

Geoff Huston
Chief Scientist, Internet
Telstra

User Beware

- I am not a security expert
- I am a simple consumer of security solutions as a user of Internet-based secure services and applications

User Beware

- No security system is absolute
  - All security measures mitigate risk, not eliminate it
  - Security measures obey the law of diminishing return
  - Determine what level of risk is acceptable
  - Constantly review risk assumptions

The Issues

- Risks and vulnerabilities
  - DNS hijacking
  - Cache hijacking
  - Routing hijacking
  - Identity hijacking
  - Session hijacking
  - Session monitoring
- The Internet's base trust model is very basic
  - Security is an overlay, not an intrinsic property of the network itself

Secure Solutions

- What are the problems to be addressed?
  - Identity authentication
  - Application authentication
  - Third party intervention
    - monitoring
    - awareness
    - alteration
    - disruption or denial
    - hijacking

Security has many dimensions

- Secure end-to-end IP conversations
- Secure application-to-application conversations
- Authenticated communications
- Secure transport systems
- Secure VPNs

Security Building Blocks

- IPSEC + IKE
  - End-to-End transport
  - Gateway-to-Gateway transport
  - Includes header and payload checksum
  - Includes payload encryption

  - Compute load is high
  - IKE is not absolutely robust (evidently)
  - Cannot tolerate NATs in the transport path

  - Used in CPE devices for overlay VPNs

Security Building Blocks

- TLS (HTTPS)
  - Application-level payload encryption
  - Weak key exchange model
  - Prevents interception monitoring of the application traffic
  - No authentication

Security Building Blocks

- SSH
  - Secure telnet tunnels
  - Secure encrypted conversation between a roaming satellite and a SSH server
  - Supports tunnels for application access (using NAT at the server)
  - Used to support extensions of corporate access into public Internet environments
    - Road Warrior tools

Security Building Blocks

- Public Key Infrastructure (PKI)
  - Public / Private key infrastructure
  - Allows for third party validation of identity of the end systems
  - Allows for use of keys to perform encryption
  - Keys normally associated with the host system, not the user of the host

Security Building Blocks

- Secure Transport Systems
  - Data-link layer encryption
    - e.g. WEP for Wi-FI
  - Caveat regarding potential regulatory requirements for clear payload interception
  - Not end-to-end
    - No authentication

Secure VPNs

- Overlay VPNs with CPE-to-CPE IPSEC tunnels
  - Issues with TCP MTU negotiation
  - Issues with performance
  - Issues with key management

  - Vendor equipment available
  - Common VPN solution

Secure VPNs

- 2547bis MPLS VPNS
  - Use MPLS to switch from PE to PE across the provider core
  - Further encryption of payload not strictly necessary (VC-style functionality)
  - Requires explicit provider support
  - Inter-provider interoperability limited

Secure Roaming

- IPSEC tunnel as overlay on dial PPP access
- SSH tunnel as overlay on access

Secure Application Services

- Certificates are excellent
  - Requires initial overhead on certificate exchange
  - Good browser support
  - But not portable across hosts
- User/password + TLS is more flexible, but at a cost of higher vulnerability

Discussion

- Security is an overlay across the Internet, not an intrinsic part of the network itself
- Many security incidents are evidently the outcome of social rather than technical engineering