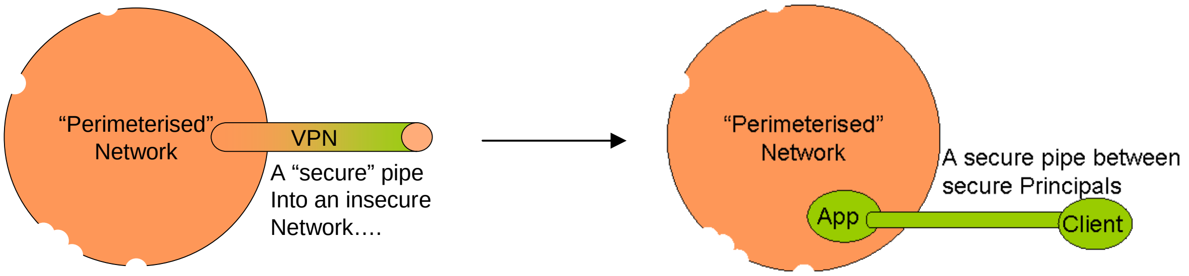
Jericho Forum™ – Technology Paper

(The need for) Inherently Secure Communications

(The Need for)
Inherently Secure Communications


"Perimeterised" Network
VPN
A "secure" pipe Into an insecure Network….
"Perimeterised" Network
App
Client
A secure pipe between secure Principals

Problem

In earlier times, if an enterprise presumed it had control over its network, and if it had few external connections or communication, it was feasible that the connections between operational computers probably were not an unacceptable risk. This required that any visitors to the enterprise with electronic devices had no ability to access the network, all users were properly managed, and that they abided by enterprise rules with regard to information management and security. This is now a rare situation. Most enterprises use computers that are connect to the Internet, employing wireless communications internally, with the majority of their users connecting to services outside the enterprise perimeter, and partners and collaborators regularly connecting to the enterprise's internal network with their own computing devices. Additionally there is the emergence of Targeting Trojans and Worms that rely on our use of this old "Internal Trust" architecture to propagate.

"Inherently secure communications, products, services and protocols, do not introduce unacceptable business

In the de-perimeterised world, the use of inherently secure communications[1] is essential (JFC#4[2]) to provide protection from the insecure data transport environment. Inherently secure communications products, services, and protocols should act as fundamental building blocks for secure distributed systems, adaptable to the needs of applications while adhering to requirements for security, compliance and performance.

Why Should I care

Most networks are fundamentally insecure. It won't matter what infrastructure you have; if the principals on the network are trusted without good cause, the network is inherently insecure.

Networks can be designed to be inherently secure. Traditionally they have not been so. Relying on the good behaviour of all principals on a network is a behaviour that characterised the "perimeterised" world - i.e. "We have big thick walls around us and we trust everyone and

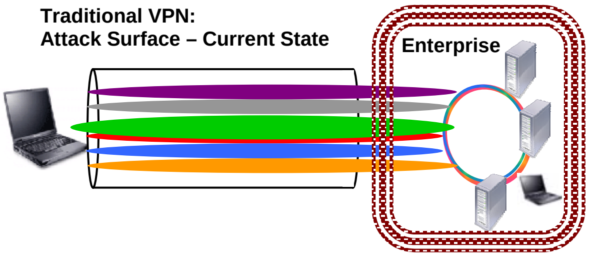
[1] An inherently secure communications protocol is authenticated, protected against unauthorised reading/writing (probably encrypted) and has guaranteed integrity (is non-repudiatable).

[2] The term JFC#n refers to the relevant Jericho Forum design principles - commandment number - see http://www.opengroup.org/jericho/commandments_v1.2.pdf

everything on the inside!”. This was even then a false statement. Luckily, few individuals at that time understood how to leverage this fundamental network architecture vulnerability; it was the realm of well-funded foreign state intelligence services, whose primary target was military secrets. Today, legitimate business demands for globalisation and collaboration and ‘Just-In-Time’ “everything” is accelerating the de-perimeterisation of our networks.

In addition, a growing number of economically-motivated organised criminals are now taking advantage of this growing vulnerability in our network architectures. Unfortunately, our network security architectures have not been adapting to this new environment; nor have protocols, products, or services been developed to resolve this growing threat. Many organisations continue to deal with the issue by simply extending their “untrustworthy” network by the mis-use of IPSec, and building V“P”N tunnels. The key here is in the “P”, for if the central network is not private the virtual network cannot be private either; to assume otherwise is to put information at risk. Simply put, the brand/image of all business organisations is reliant on secure reliable information flows.

The use of general purpose VPNs or tunnel technology carries with it additional risks. Typically VPNs carry all of the communications between a client and set of servers and are terminated at the enterprise perimeter. So, the security association is between a client computer and perimeter device, not a specific service. There are several points of vulnerability here. First, there is the potential for one protocol, once compromised, to target a different protocol or service. For example, a Trojan sent via E-Mail could actually be targeting a database server with a SQL Injection attack. A second issue is that since these VPNs usually terminate at the perimeter, the information they are carrying has the least protection at the enterprise’s weakest point. Thirdly, the security association is between the client and VPN service, not client and server. The following 3 diagrams illustrate these vulnerabilities and how they are successively minimised.

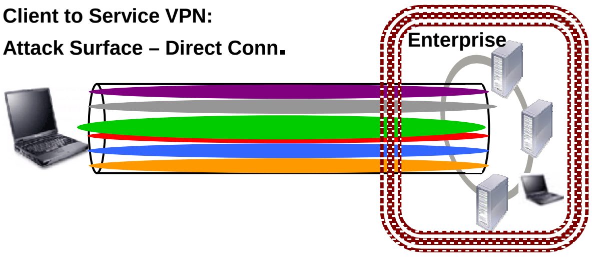


One general purpose tunnel for all traffic

- Weak protocols mixed with strong protocols allow malicious code to spread
- Single crypto codebase

Tunnel terminates at perimeter

- Information expose at weakest point
- No security assoc. between client & server
- Traffic mixed on intranet
- Easy to inspect traffic

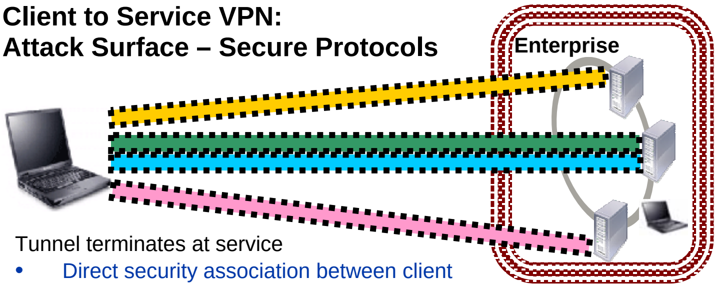


One general purpose tunnel for all traffic

- Weak protocols mixed with strong protocols allows malicious code to spread between protocols
- Single crypto codebase

Tunnel terminates at service

- Direct security assoc. between client and server
- Traffic not available to intranet
- Perimeter not needed
- Difficult to inspect traffic if still using perimeter controls



Client to Service VPN:
Attack Surface – Secure Protocols

Tunnel terminates at service

- Direct security association between client and server
- Traffic not available to intranet
- Perimeter not needed
- Difficult to inspect traffic if still using perimeter controls

Applications use built in tunnel capability

- Each protocol isolated
- Only services/ports in use exposed
- Greater risk of poor tunnel implementations

Recommendation/Solution

Rather than use a general purpose tunnel, Applications should incorporate their own secure tunnel technology. This technology, referred to here as inherently secure protocols/ communications, improves security in several ways:

- It supports the capability for the client to create a secure association directly with the server or service.
- The scope, or attack surface, is limited to the specific service or protocol involved in the communication. This limits the exposure both by reducing the number of protocols involved to just those associated with the requested service, and also by limiting the number of machines involved - from potentially the entire Intranet, to only the servers related to the invoked service. So, as in the example above, if a client is accessing E-Mail using a direct connection and sending a Trojan targeted at an SQL protocol, it will only reach the mail server, which will ignore it.

Some specific examples of applications that include inherently secure protocols as part of their communication capability are mentioned below.

As a minimum, all sensitive information should be communicated in an inherently secure manner which does not rely on the underlying security of the communications infrastructure of the collaborating organisations. Organisations should architect inherently secure methods of communications developed using Products, Services, and Protocols that are designed from the ground up always to meet the users’ expectations of Privacy, Safety, and Legitimacy, delivered through effectively managing the Identity, Confidentiality, Integrity and Availability of all the relevant principals. Imagine a world where all communications of sensitive information assets occur in a secure manner which cannot be cost-effectively compromised, and all non-public information is transmitted using appropriately secure communications products, services and protocols that integrate closely with each application and user.

The communications products, services and protocol(s) used should have the appropriate level of data security and authentication. The use of a protective security wrapper (or shell) around an application protocol may be applicable; however the use of an encrypted tunnel negates most inspection and protection and should be avoided in the long term.

It is essential that the properties of any protocol that underpin the trust relationships involved are transparent. Otherwise mismatches or implicit contextual assumptions will result in the associations between identities, keys, permissions and obligations between communicating parties. Basically, inherently secure communications, products, services and protocols, will not introduce unacceptable business risk. Inherent Security will become an "expectation" similar to "Dial Tone". "Do you remember when they used to transmit our information without securing it!" will be similar to "Do you remember when they used to deliver our mail by pony express!"

Background/rationale

Some organisations are utilising new protocols to enable secure application-to-application communication over the Internet. These are business-to-business protocols; more specifically ERP-system-to-ERP system protocols that include the required end-entity authentication and security to provide the desired trust level for the transactions. It takes into account the Jericho Forum design principles on Context (JFC#3), Trust Levels (JFC#7) and Risk (JFC#1).

There are a wide variety of application (system-level) protocols in use, but a much smaller number of secure protocols to choose from. In practice, integration may be poor or impossible, designers may make 'one size fits all' assumptions (JFC#3) about the security of a protocol for a particular purpose, or the requirements actually achieved may be short of the ideal when nominally secure protocols are built into actual implementations. The resultant protocol TCP/IP 'stack' will therefore be unfit for use in the de-perimeterised world.

The need for open standards – to provide Interoperability

The reason that the Internet still uses a set of insecure protocols is because these protocols are de-facto lowest common denominator standards, which are open and free for use. If all systems are to interoperate – regardless of operating system or manufacturer, and be adopted in a timely manner, then it is essential that protocols must be open and remain royalty free.

The need for default security: Secure "out of the box"

For inherently secure protocols to be adopted, it is essential that systems start being delivered with only inherently secure protocols, or with the inherently secure protocol as the default option.

Working towards the future

Currently, organisations have limited choices depending on their requirements and constraints for flexibility/manageability, trust, vendor interoperability, the need to deploy client software (agents, browser plug-ins etc.), and performance.

Vendors are starting to offer hybrid protocol solutions that support multiple security policies, system/application integration, and degrees of trust between organisations and communicating parties (their own personnel, customers, suppliers, etc.). Unfortunately the inevitable result is proprietary solutions that are unlikely to interoperate, and whose security may be difficult to verify. It is, therefore, important to start to classify the various solutions that an organisation uses or is contemplating using.

Ultimately, if a device is capable of working using only inherently secure protocols then it should be possible to utilise a TCP/IP stack that is immune from attack (other than a DoS attack) as any protocol that is not inherently secure would be simply ignored.

Additionally, if an organisation's border will only permit inherently secure protocols (potentially filtered at all routers) then the need for other traditional border protection may become irrelevant.

Challenges to the industry

1. Inherently secure protocols must be open, royalty free and interoperable (JFC#3)
2. Current proprietary inherently secure protocols should be made fully open, royalty free, and documented, or discontinued.

3. Inherently Secure Protocol reference implementations should be released under a suitable open source or General Public License (GPL) arrangement.

4. Companies should review their products, protocols and services and consider replacing inappropriate products, protocols and services, i.e. those that are not inherently secure.

5. Organisations should disclose to the public the secure communications capability of transaction processes dealing with sensitive information assets, i.e. a user will be able to identify if Inherently Secure Communications are in use. An ISC[3] certification scheme would be valuable here.

6. End users should be educated on the value of inherently secure protocols and how to recognise when they are in use.

The way forward

Requests to other Open Group Forums

Security Forum:

1. Develop “Inherently Secure Communications (ISC)”; Guidelines, Patterns, Use Cases, and Standards,
2. Develop examples of protocol mis-use
3. Refine the Protocol Usage Matrix below

Architecture Forum:

4. Refine the TOGAF to specifically incorporate Security Elements like ISC

(Probably needs a separate White Paper describing the implications of Jericho Forum commandments on the Architecture Forum’s TOGAF.)

(Continued – next page)

[3] ISC – Internet Systems Consortiun – www.ics.org

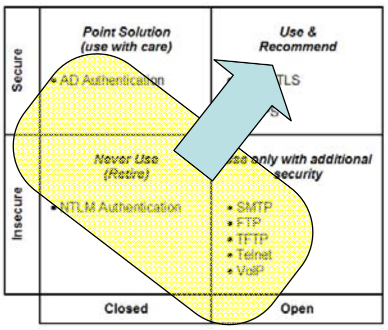
Protocol Usage Matrix

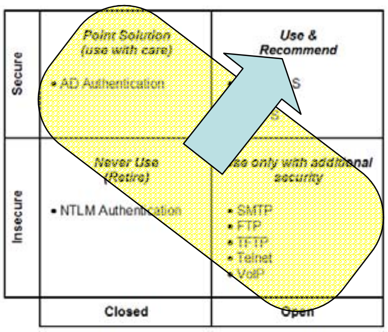
The matrix below is a simple method for organizations to assess the protocols in use within their systems.

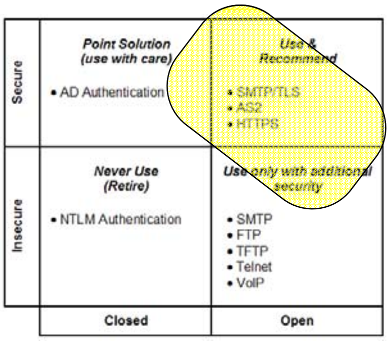
	Closed	Open
Secure	***Point Solution (use with care)*** • AD Authentication • COM	***Use & Recommend*** • SMTP/TLS • AS2 • HTTPS • SSH • Kerberos
Insecure	***Never Use (Retire)*** • NTLM Authentication	***Use only with additional security*** • SMTP • FTP • TFTP • Telnet • VoIP • IMAP • POP • SMB • SNMP • NFS

Evolution not revolution

Today we predominantly operate in the lower left quadrant of the protocol usage matrix, above. There is an immediate benefit that can be gained by analysing existing protocols in use and moving to secure versions. Most modern systems should easily be able to eliminate the reliance on closed and insecure protocols.







Today **Near Future** **Tomorrow**

As we progress, new systems should only be introduced that either have all protocols that operate in the Open/Secure quadrant, or operate in the Open/Insecure on the basis that anonymous unauthenticated access is the desired mode of operation.