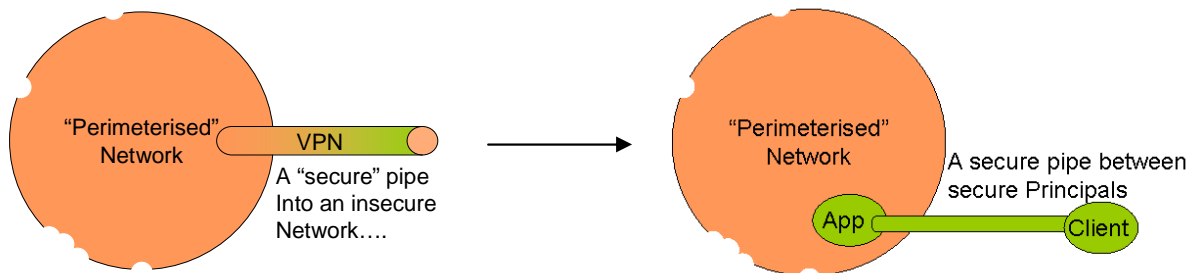




The Need for Inherently Secure Communications



Problem

Previously, 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 weren't 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 with most enterprises using computers that 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 are relying on our use of this old "Internal Trust" architecture to propagate. In the de-perimeterised world the use of inherently secure communications¹ is essential (JFC#4²) 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.

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

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. 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 everything on the inside!". This was even then a false statement. Luckily few individuals at that

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 Commandment number. See www.jerichoforum.org

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 architecture. 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 “untrust-worthy” network by the mis-use of IPSec, and building V“P”N tunnels. The key is in the “P”, for if the central network is not private the virtual network cannot be private either; to assume that they are, is to put information at risk. Simply put, the brand/image of companies are reliant on secure reliable information flows.

Recommendation/Solution

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 that will be 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!” would be similar to “Do you remember that people used to have outside lavatories!”

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 context (JFC#3), trust level (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: 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 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.

Jericho Forum 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 GPL arrangement.
4. Companies will review its products, protocols and services and consider replacing in-appropriate products, protocols and services, ie those that are not inherently secure.
5. Organisations should disclose to the public, the secure communications capability³ of transaction processes dealing with sensitive information assets.
(ie A user will be able to identify that Inherently Secure Communications are in use)
(A ISC 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.

Jericho Forum 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

³ An ISC certification scheme might be valuable here

Architecture Forum

- 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.)

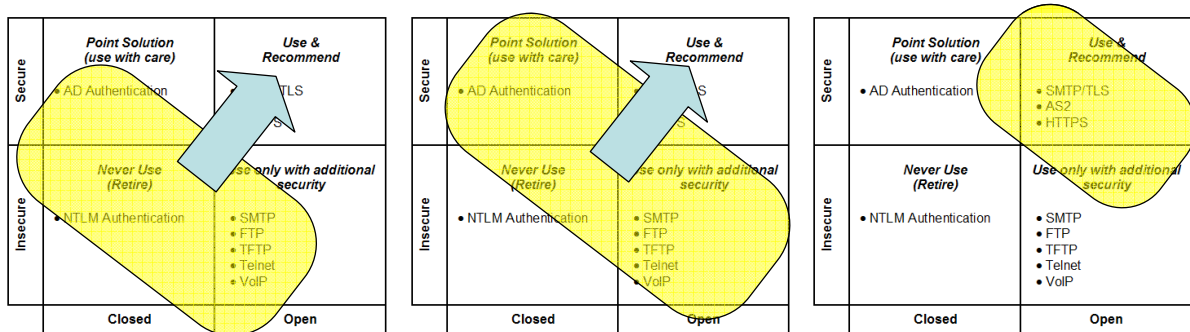
Protocol Usage Matrix

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

Secure	Point Solution (use with care)	Use & Recommend	
	<ul style="list-style-type: none"> • AD Authentication • COM 	<ul style="list-style-type: none"> • SMTP/TLS • AS2 • HTTPS • SSH • Kerberos 	
Insecure	Never Use (Retire)	Use only with additional security	
	<ul style="list-style-type: none"> • NTLM Authentication 	<ul style="list-style-type: none"> • SMTP • FTP • TFTP • Telnet • VoIP 	<ul style="list-style-type: none"> • IMAP • POP • SMB • SNMP • NFS
	Closed	Open	

Evolution not revolution

Today we predominantly operate in the lower left quadrant, there is a immediate win that can be gained by analysing existing protocols in use and moving to secure versions. Most modern system should easily be able to eliminate the reliance on closed & 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.