



Position Paper

The Need for Inherently Secure Protocols

Problem

In the situation where an enterprise has control over its network, and it has no external connections or communication, it is feasible that the connections between computers are not a problem provided that they work. This requires that any visitors to the enterprise have no ability to access the network and all users are properly managed and they abide by enterprise rules with regard to information management and security. This is now a rare situation with nearly every enterprise that uses computers regularly connected to the Internet, employing wireless communications internally and the majority of their users connecting to services outside the enterprise perimeter. In this de-perimeterised world the use of inherently secure protocols¹ is essential (JFC#4²) to provide protection from the insecure data transport environment. Ideally, secure protocols should act as fundamental building blocks for secure distributed systems, adaptable to the needs of applications while adhering to requirements for security, trust and performance.

Why Should I care

The Internet is insecure, and always will be. It doesn't matter what infrastructure you have, it is inherently insecure. Fact. However, enterprises now wish direct application to application integration to support just-in-time delivery and will continue to use the Internet as the basic transport medium.

Many companies 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. They take 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.

¹ An inherently secure protocol is authenticated, protected against unauthorised reading/writing (probably encrypted) and has guaranteed integrity.

² The term JFC#n refers to the relevant Jericho Forum Commandment number. See www.jerichoforum.org

Recommendation/Solution

While there may be some situations where open and insecure protocols are appropriate (public facing “information” web sites for example) all non-public information should be transmitted using appropriately secure protocols that integrate closely with each application.

The 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 properties of any protocol that underpin the trust relationships involved are transparent. Mismatches or implicit contextual assumptions in the associations between identities, keys, permissions and obligations between communicating parties will otherwise result.

Background/rationale

The need for open standards

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.

Secure “out of the box”

For inherently secure protocols to be adopted then it is essential that systems start being delivered preferably only supporting inherently secure protocols, or with the inherently secure protocols 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.

Challenges to the industry

1. If inherently secure protocols are to become adopted as standards then they must be open and interoperable (JFC#3)
2. The Jericho Forum believes that companies should pledge support for making their proprietary protocols fully open, royalty free, and documented
3. The Jericho Forum favours the release of protocol reference implementations under a suitable open source or GPL arrangement.
4. The Jericho Forum hopes that all companies will review its products and the protocols and move swiftly to replacing the use of appropriate protocols.
5. End users should demand full disclosure of protocols in use as part of any purchase.
6. End users should demand that all protocols should be inherently secure
7. End users should demand that all protocols used should be fully open

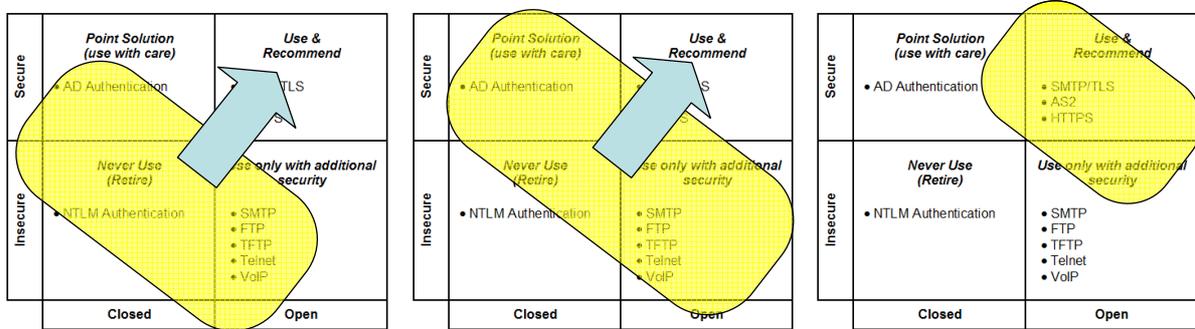
Protocol Usage Matrix

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

| | | | |
|-----------------|--|---|---|
| Secure | <i>Point Solution (use with care)</i> | <i>Use & Recommend</i> | |
| | <ul style="list-style-type: none"> • AD Authentication • COM | <ul style="list-style-type: none"> • SMTP/TLS • AS2 • HTTPS • SSH • Kerberos | |
| Insecure | <i>Never Use (Retire)</i> | <i>Use only with additional security</i> | |
| | <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 an immediate win 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 & 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.