



Position Paper

VoIP in a de-perimeterised world

Problem

With many large organisations seeking the cheapest options for internal long distance telephone calls, using the internet as a bearer is a very attractive option. Voice over IP (VoIP) is being increasingly deployed in the corporate environment to take advantage of company's existing Internet connections. It is estimated that in 2005, IP Telephony accounted for over 47% of all US long distance and international telephone calls. However, the problems inherent with normal phone conversations still exist, with additional problems added. Conversations can be monitored, hijacked, overheard and so on. With wire-connected telephone conversations, interceptions are more difficult unless undertaken by lawful interception, but with Internet connections being used, interception, recording/replay etc can happen anywhere on the network. VoIP has been sold using the flawed assumption that sharing the data infrastructure is acceptable because the internal network is secure. The lack of security built-in to VoIP products and protocols means that companies are unable to deploy VoIP securely in a de-perimeterised environment where the ROI is significantly more complex than just the replacement of an existing internal telephone exchange.

Why Should I Care

Potential cost saving on long-distance telephone/conference calls is a strong corporate driver, and VoIP may be (incorrectly) considered no less secure than standard phone calls. Verbal communications are as important to manage corporately as written communications are, as in many jurisdictions legally binding commitments may be made or breaches of ethics/law may be committed. Within a closed corporate environment, anyone with access to the network would be able to tap into conversations, record them for later analysis etc. With the dissolution and eventual removal of perimeters, this gets worse. Disclosure of important information through the use of VoIP may constitute an offence, because organisations should rightfully know that it is inherently insecure.

Vendors are attempting to overcome these issues by developing proprietary protocols to secure inter-organisational communication; generally by tailoring the main communications protocol used in VoIP (Session Initiation Protocol or SIP). These vendors, in order to protect their investment in firewall products, often wish to perpetuate the perimeter mindset – but even within the corporate perimeter, if maintained, VoIP is not secure. Other vendors have closed and proprietary products that enable VoIP between individual users, but these are not suitable for corporate use as one would have to know all likely recipient phone numbers or be able to find them on the vendor's Internet-based directory and this is not acceptable for most enterprises.

Jericho Forum Response

The protocols used to enable VoIP do not meet the requirement to utilise inherently secure protocols¹ (JFC#4²) and neither are the system and end-devices (phones) capable of being deployed on the raw Internet (JFC#5).

Currently corporate VoIP deployments generally make the flawed assumption that the Corporate Intranet is secure (JFC#11) and thus placing corporate voice traffic over a single shared network is an acceptable risk.

In a corporate environment, there is a need for a single VoIP system and associated enterprise directory to support a wide variety of end-devices - from hardware (dedicated) phones, to soft-phones and VoIP phones embedded into mobile/cell devices.

Clearly this mix of VoIP devices dictates the need for interoperability and an open, inherently secure, protocol that will enable an enterprise to deploy a device agnostic VoIP infrastructure giving a feature-rich, yet flexible environment that extends beyond the enterprise's perimeters. Such a system should work securely across both the enterprise and consumer/SME environments (JFC#3). This ability has been demonstrated with the GSM/GPRS/3G mobile standards which is based on an open, non-proprietary system.

Background & Rationale

The current industry position

VoIP uses a mix of proprietary protocols (tailored SIP and others) and generally defaults at the basic level (reduced operational capability) to the SIP protocol to which manufacturers pay lip-service. With each vendor tailoring their product's use of SIP differently, there is the potential for vendor lock-in across an organisation, and for interoperability problems in establishing calls where different, incompatible products and services are in use at each end.

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 (JFC#4).

Secure “out of the box”

All components in a VoIP implementation must be secure “out of the box” according to an industry agreed profile, must maximise interoperability and must be capable of withstanding attack (JFC#5).

If a VoIP environment is to be successful, then the end devices must be capable of being securely maintained and updated “down the wire” – an update methodology should be built into devices and be part of any secure VoIP standard (JFC#8).

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

End user / mutual authentication

Potentially a VoIP deployment inside the corporate environment can in some case mirror a plain old telephone service (POTS) deployment and use no authentication based on the compensation of a physical (building) security boundary.

However in a true de-perimeterised environment VoIP phones can be deployed in workers homes, hotels, temporary location, mobile cellular devices and other insecure environments, thus the device and protocol must support a standard and strong method of strong mutual authentication (JFC#7 & 8).

The self defending phone

Because VoIP is reliant on processor/software within a proprietary phone or provided as a soft client, it cannot be assumed that the device is fully protected against malicious software, or is fully patched. Also, a VoIP phone must be capable of surviving directly connected to the raw Internet (JFC#5). Thus a VoIP phone should only use an Inherently Secure Protocol (JFC#4). The device should ignore (black-hole) all other protocols.

VoIP Protocols

Any secure VoIP protocol must be open and interoperable. The protocol must be capable of ensuring:

- secure communications - specifically multi-hop (end-to-end encryption)
- organisational/business functional requirements such as forwarding, conferencing, etc.
- control and configuration of the end device
- end device update / maintenance / remediation
- end device and controller authentication
- strong and mutual user authentication (user-device, user-user, where required)

Working towards the future

When a VoIP device is capable of working using only inherently secure VoIP 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. This will allow VoIP to be deployed in a single phone system independent of the network.

Challenges to the industry

The numbering here provides for ease of reference and does not imply any priority.

1. If inherently secure VoIP protocols are to become adopted as standards then they must be open and interoperable (JFC#4)
2. The Jericho Forum believes that companies should pledge support for moving from proprietary VoIP protocols to a fully open, royalty free, and documented standards
3. A secure VoIP protocol reference implementation should be released under a suitable open source or GPL arrangement.
4. The Jericho Forum hopes that all companies will review their products and associated protocols and move swiftly to replacing current insecure/proprietary usage by inherently secure VoIP protocols.
5. End users should demand that VoIP protocols should be inherently secure
6. End users should demand that VoIP protocols used should be fully open

The way forward

The Jericho Forum believes that with the correct executive sponsorship, the major VoIP vendors could together easily enable their collective technical and security experts to design and define the necessary enhancements to the existing VoIP protocols.

The Jericho Forum would be willing to facilitate an environment where a specification could be developed within The Open Group.
