

Real world application

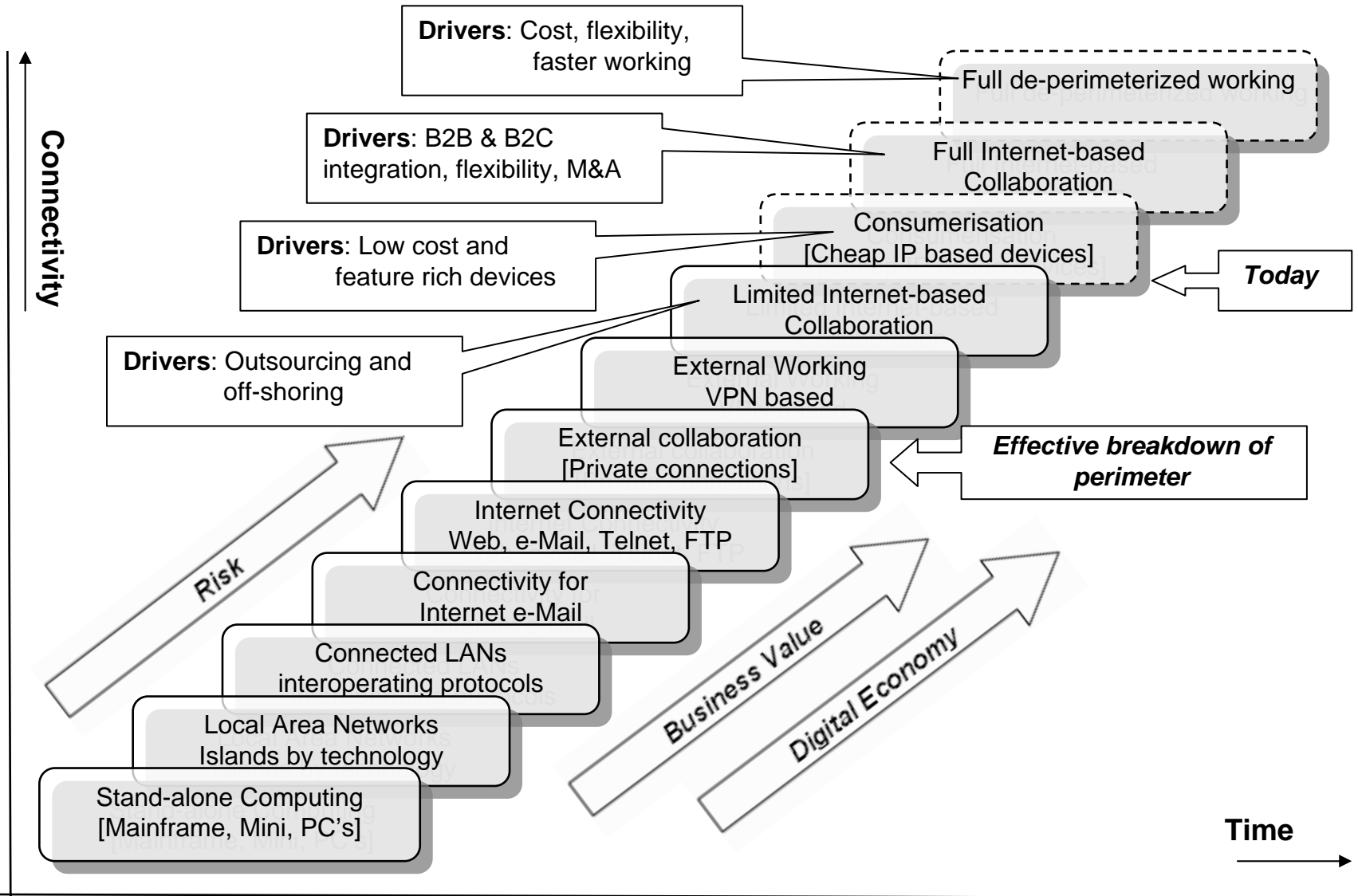
- **Evolving security architectures to deliver de-perimeterized solutions**
- Paul Simmonds
Jericho Forum Board

A brief introduction to the Jericho Forum

- The Jericho Forum aims to drive and influence development of security standards that will meet future business needs
- These standards will:
 - Facilitate the secure interoperation, collaboration and commerce over open networks
 - Be based on a security architecture and design approach entitled “de-perimeterisation”.
- Globally, more than fifty organisations, from all sectors, are working together to solve the problems posed by de-perimeterisation

History

- Computing history can be defined in terms in increasing connectivity over time;
 - starting from no connectivity,
 - to the restricted connectivity we currently have today;
 - islands of corporate connectivity behind their managed perimeter.



Trends and Signs

- Key indicators that indicate a de-perimeterized future:
 - Mismatch of the (legal) business border, the physical border and network perimeter
 - Business demanding that systems collaborate where B2B relationships exist
 - Good network connectivity and access for all business / operational relationships
 - Distributed / shared applications across business / operational relationships
 - Applications that bypasses perimeter security

Rationale

- Jericho Forum in a nutshell: “Your security perimeters are disappearing: what are you going to do about it?”
- Need to be able to draw distinctions between “good” security (e.g. “principle of least privilege”) and;
 - “de-perimeterized security” (e.g. “end-to-end principle”, “Secure collaboration”)

Why should I care?

- De-perimeterisation is a disruptive change
- There is a huge variety of:
 - Starting points / business imperatives
 - Technology dependencies / evolution
 - Appetite for change / ability to mobilise
 - Extent of de-perimeterisation that makes business sense / ability to influence
- So we need rules-of-thumb, or principles
 - “A benchmark by which concepts, solutions, standards and systems can be assessed and measured.”

Structure of the Commandments

The principles,

our benchmark by which concepts, solutions, standards and systems can be assessed and measured

- Fundamentals (3)
- Surviving in a hostile world (2)
- The need for trust (2)
- Identity, management and federation (1)
- Access to data (3)

Fundamentals

- 1. The scope and level of protection must be specific and appropriate to the asset at risk**
 - Business demands that security enables business agility and is cost effective.
 - Whereas boundary firewalls may continue to provide basic network protection, individual systems and data will need to be capable of protecting themselves.
 - In general, it's easier to protect an asset the closer protection is provided.

Fundamentals

2. Security mechanisms must be pervasive, simple, scalable and easy to manage

- Unnecessary complexity is a threat to good security.
- Coherent security principles are required which span all tiers of the architecture.
- Security mechanisms must scale:
 - from small objects to large objects.
- To be both simple and scalable, interoperable security “building blocks” need to be capable of being combined to provide the required security mechanisms.

Fundamentals

3. Assume context at your peril

- Security solutions designed for one environment may not be transferable to work in another:
 - thus it is important to understand the limitations of any security solution.
- Problems, limitations and issues can come from a variety of sources, including:
 - Geographic
 - Legal
 - Technical
 - Acceptability of risk, etc.

Surviving in a hostile world

4. Devices and applications must communicate using open, secure protocols.
5. All devices must be capable of maintaining their security policy on an untrusted network.

The need for trust

6. All people, processes, technology must have declared and transparent levels of trust for any transaction to take place.
7. Mutual trust assurance levels must be determinable.

Identity, Management and Federation

8. Authentication, authorisation and accountability must interoperate/ exchange outside of your locus/ area of control.

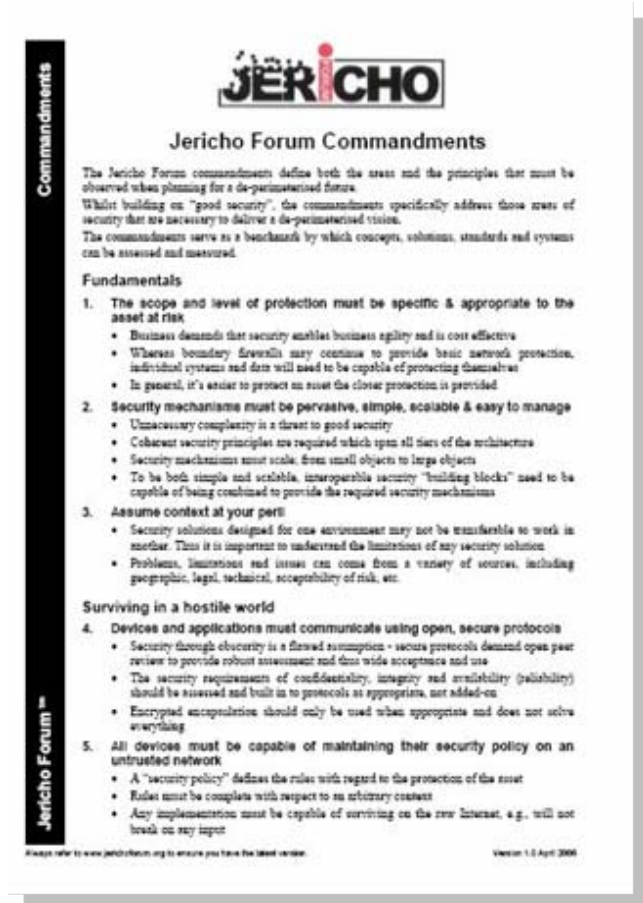
Access to data

9. Access to data should be controlled by security attributes of the data itself.
10. Data privacy (and security of any asset of sufficiently high value) requires a segregation of duties/privileges.
11. By default, data must be appropriately secured both in storage and in transit.

Paper available from the Jericho Forum

- The Jericho Forum “Commandments” are freely available from the Jericho Forum Website

<http://www.jerichoforum.org>



The image shows the cover of the Jericho Forum Commandments document. It features the Jericho Forum logo at the top, which consists of the word "JERICHO" in a stylized font with a red dot above the 'I'. Below the logo is the title "Jericho Forum Commandments". The document is framed by a vertical bar on the left side with the text "Jericho Forum" and "Commandments" written vertically. The main text of the document is visible, including an introduction and a list of commandments.

Jericho Forum

Commandments

Jericho Forum Commandments

The Jericho Forum commandments define both the areas and the principles that must be observed when planning for a de-perimeterised future.

Whilst building on "good security", the commandments specifically address those areas of security that are necessary to deliver a de-perimeterised vision.

The commandments serve as a benchmark by which concepts, solutions, standards and systems can be assessed and measured.

Fundamentals

- 1. The scope and level of protection must be specific & appropriate to the asset at risk**
 - Business demands that security enables business agility and is cost effective
 - Whereas boundary firewalls may continue to provide basic network protection, individual systems and data will need to be capable of protecting themselves
 - In general, it's easier to protect an asset the closer protection is provided
- 2. Security mechanisms must be pervasive, simple, scalable & easy to manage**
 - Unnecessary complexity is a threat to good security
 - Coherent security principles are required which span all tiers of the architecture
 - Security mechanisms must scale, from small objects to large objects
 - To be both simple and scalable, interoperable security "building blocks" need to be capable of being combined to provide the required security mechanisms
- 3. Assume context at your peril**
 - Security solutions designed for one environment may not be transferable to work in another. Thus it is important to understand the limitations of any security solution
 - Problems, limitations and issues can come from a variety of sources, including geographic, legal, technical, acceptability of risk, etc.

Surviving in a hostile world

- 4. Devices and applications must communicate using open, secure protocols**
 - Security through obscurity is a flawed assumption - secure protocols demand open peer review to provide robust assessment and thus wide acceptance and use
 - The security requirements of confidentiality, integrity and availability (CIA) should be assessed and built in to protocols as appropriate, not added-on
 - Encrypted encapsulation should only be used when appropriate and does not solve everything
- 5. All devices must be capable of maintaining their security policy on an untrusted network**
 - A "security policy" defines the rules with regard to the protection of the asset
 - Rules must be complete with respect to an arbitrary context
 - Any implementation must be capable of surviving on the raw Internet, e.g., will not break on any input

Always refer to www.jerichoforum.org to ensure you have the latest version. Version 1.0 April 2006

VoIP Insecurity

Wannabe VoIP Security Moron Cries VoIP Isn't Safe

Friday, August 31st, 2007 @ 8:38 am | News

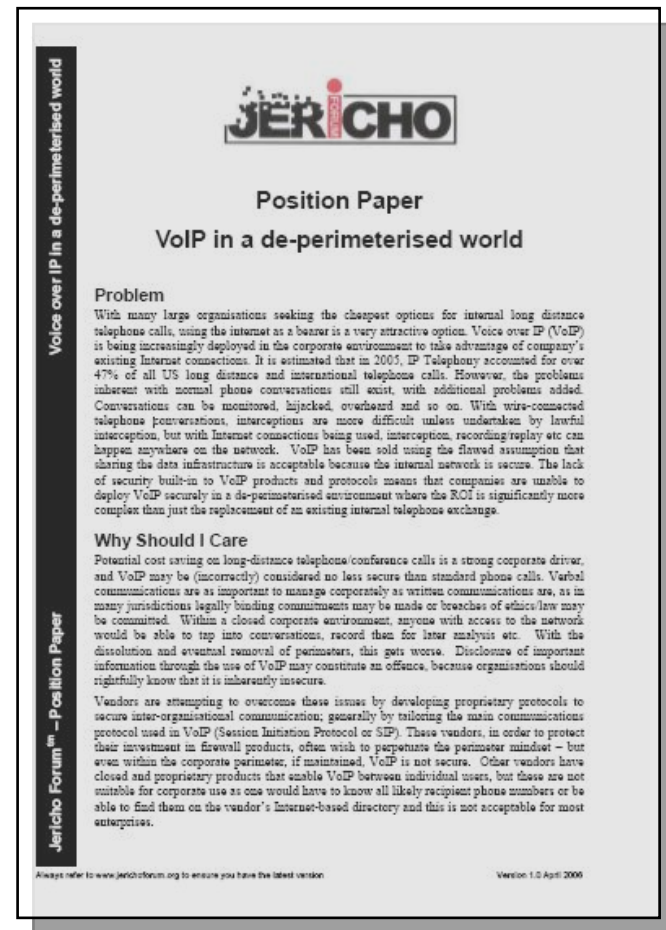
- An idiot named Paul Simmonds (a member of Jericho Forum's board of management) says: VoIP is not yet ready for use in businesses. "We don't consider VoIP to be enterprise-ready," Simmonds said.

Anon (<http://www.infiltrated.net/?p=10>)

Paper available from the Jericho Forum

- The Jericho Forum Position Paper “VoIP in a de-perimeterized world” is freely available from the Jericho Forum website

<http://www.jerichoforum.org>



JERICHO

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.

Always refer to www.jerichoforum.org to ensure you have the latest version

Version: 1.0 April 2006

Jericho Forum™ – Position Paper

Voice over IP in a de-perimeterised world



VoIP Business Requirements

- Return on Investment for;
 - Specific Computer to Telephony Integration
 - Greenfield site / refresh
 - Toll-bypass via the WAN / Internet
 - Distributed workforce
 - Integrated home/mobile workers
- Rarely a Return on Investment for;
 - Rip & replace existing office phone systems
 - More expensive (and complex) end devices
 - Patch process for all system components

VoIP vs. Jericho Forum Principles

1	Specific & appropriate to the asset at risk	If all low risk	☹
2	Security, simple, scalable & manageable	Not in Corp.	☹
3	Assume context at your peril	Pots vs VoIP	☹
4	Open & secure protocols.	No	☹
5	Maintain security policy on un-trusted net.	Web, TFTP etc.	☹
6	Transparent trust	None	☹
7	Mutual trust assurance levels	None	☹
8	Authentication outside of locus of control	None	☹
9	Access by security attributes of the data	None	☹
10	Data privacy requires segregation of duties	None	☹
11	Data appropriately secured	No	☹

The future

- Many - and in some cases most - network security perimeters will disappear
- Like it or not de-perimeterisation will happen
- The business and operational drivers will already exist within your organisation
- It's already started and it's only a matter of:
 - how fast,
 - how soon and
 - whether you decide to control it

Future challenges

- Data vs. Network
 - As networks open up and are shared the challenge is to protect the data
- Ad-hoc relationship
 - Shorter, more ad-hoc relationships are becoming the norm
- Collaborators, competitors and enemies
 - Our networks contain people we trust
 - Collaborators in one area competitors in others
 - Those we need to share with but do not trust

Architecting for a Jericho Forum Blueprint

- De-perimeterisation is the concept of architecting security for the extended business boundary
- It is not a solution in itself, but promises to:
 - Reduce complexity, unifying and simplifying solutions and generally reduce cost
 - Business flexibility, cost-effective bandwidth and infrastructure provision
 - Increased security thereby reduce business risk
 - Enable multi-vendor outsourcing
 - Simpler and thus more auditable environment
 - Provides true defence in depth

Collaboration Oriented Architecture

- A concept used to describe the design of a computer system that is designed to collaborate, or use services, from systems that are outside of your locus of control.

"... And so the first idea was to say, OK, let's have that boundary, that one perimeter, and use that, which has been a reasonable concept.

But, in fact, if we look what actually goes on in terms of consultants coming into your company, employees who are not on site that need full access capabilities, we can't think of that glass house, that kind of network topology as the way that we do this isolation, as the way we define what can connect to what.

So, we need a far more powerful paradigm in order to do this."

Bill Gates, RSA Security Conference keynote, February 2007.

Successful implementation of a Collaboration Oriented Architecture implies the ability to successfully inter-work securely over the Internet and will typically mean the adoption of the principles of de-perimeterisation.

http://en.wikipedia.org/wiki/Collaboration_Oriented_Architecture

Getting from where we are today . . .

- How to move from a secure network with poor process administration to insecure networks with secure protocols and processes
 1. Accept that you do not have a secure network
 2. Base all technology and design assumptions on this revised paradigm
 3. Start using de-perimeterized solutions today – they will work just as well inside a “secure” network
 4. Change mindsets within your organisation
 5. Join the Jericho Forum and collaborate in defining the direction for Information Security

Old Thinking vs. Jericho Forum Thinking

Old Mindset

- Connections to the secure network
- Connection-level authentication
- Authentication to access the secure network
- Secure tunnel from device to network connection point



New Mindset

- Connections to secure resources
- Protocol-level authentication
- Authentication to access individual secure resources
- Secure protocol from device directly to secure resources

Old Mindset vs. Jericho Forum Mindset

- **“CIA”:**
 - Confidentiality
 - Integrity
 - Availability
- Security
- Security
- Quality of Service

Risks and benefits

Risks

- Inflexible to respond to market demands
- Get it wrong and expose the business
- Keep adding more layers of security
- Cost and/or inability to manage
- Saddled with yesterday's technology

Benefits

- Flexible and adaptable solutions
- Increased levels of security
- Simpler, less complex security
- Cheaper to run, easier to manage
- Tomorrow's technology with ability to gain business advantage

Paper available from the Jericho Forum

- The Jericho Forum White Paper the “Business rationale for de-perimeterisation” is freely available from the Jericho Forum Website

<http://www.jerichoforum.org>



JERICHO

White Paper
Business rationale for de-perimeterisation

History
Computing history can be defined in terms of increasing connectivity over time, starting from no connectivity, to the restricted connectivity we currently have today with islands of corporate connectivity behind their managed perimeter.

Today
Today there are key indicators that every organisation will be seeing within their business that indicate a de-perimeterised future:

- The increasing mismatch of the (legal) business border and the network perimeter as business relationships becomes less distinct.
- Business demanding to directly interconnect systems where B2B relationships exist
- The need to have good network connectivity and access with all organisations with whom you have a business relationship.
- Distributed / shared applications across business relationships
- Increasing applications using technology that bypasses firewall security at the perimeter (typically using Web-based techniques that can legitimately traverse the perimeter)
- Increasing inability of traditional firewall and other network perimeter controls to combat malware that uses Web and e-Mail based techniques

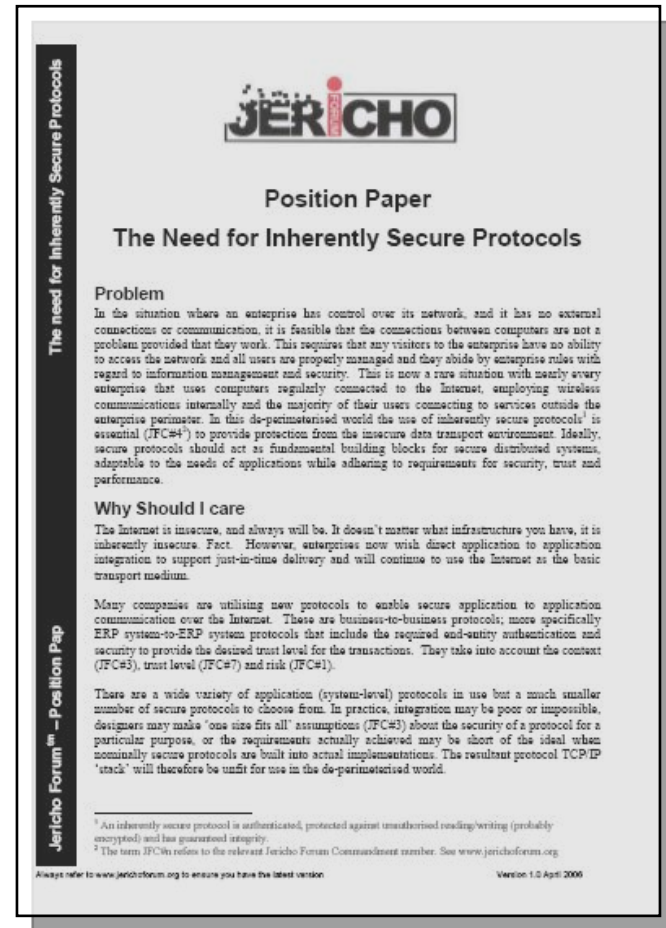
Always refer to www.jerichoforum.org to ensure you have the latest version

Version 1.0 January 2007

Paper available from the Jericho Forum

- The Jericho Forum Position Paper “The need for Inherently Secure Protocols” is freely available from the Jericho Forum website

<http://www.jerichoforum.org>



The cover of the Jericho Forum Position Paper "The Need for Inherently Secure Protocols" features the Jericho Forum logo at the top center. The logo consists of the word "JERICHO" in a bold, black, sans-serif font, with a red dot above the letter "I". Below the logo, the title "Position Paper" is centered, followed by the subtitle "The Need for Inherently Secure Protocols". The cover is framed by a vertical bar on the left side containing the text "The need for Inherently Secure Protocols" and "Jericho Forum™ - Position Paper". The main text on the cover is a preview of the paper's content, including sections on "Problem", "Why Should I care", and a note about the paper's availability.

JERICHO

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#4) 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#5), 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.

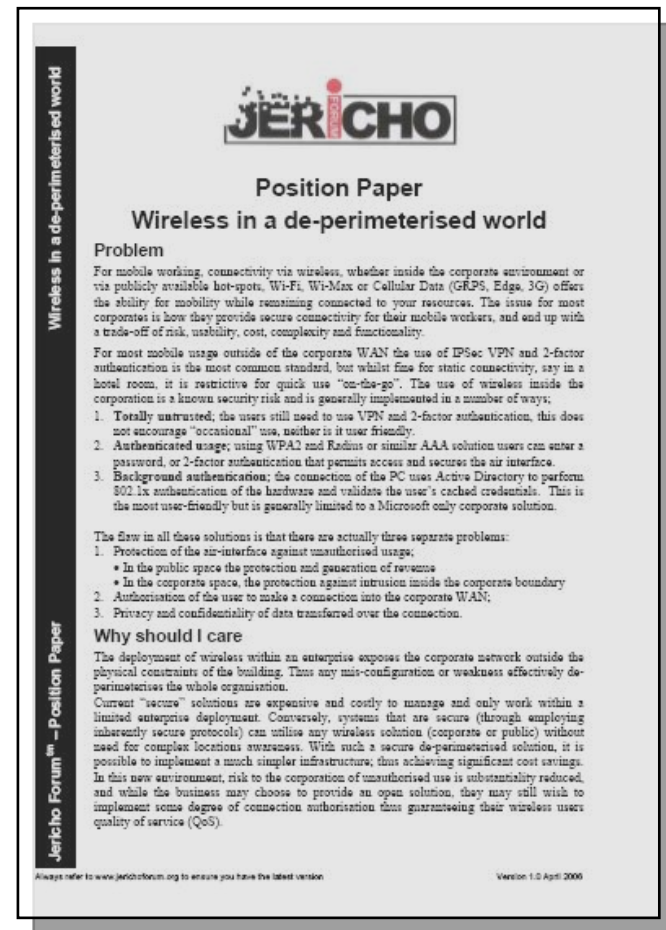
¹ An inherently secure protocol is authenticated, protected against unauthorised reading/writing (probably encrypted) and has guaranteed integrity.
² The term JFC#n refers to the relevant Jericho Forum Commitment number. See www.jerichoforum.org
Always refer to www.jerichoforum.org to ensure you have the latest version

Version: 1.0 April 2006

Paper available from the Jericho Forum

- The Jericho Forum Position Paper “Wireless in a de-perimeterized world” is freely available from the Jericho Forum website

<http://www.jerichoforum.org>



The image shows the cover of a position paper from the Jericho Forum. The title is 'Wireless in a de-perimeterised world'. The cover includes the Jericho Forum logo, a vertical title on the left, and a list of three numbered points under the heading 'Problem'. The text is in a clean, sans-serif font on a light background.

Jericho Forum™ - Position Paper

Wireless in a de-perimeterised world

JERICHO

Position Paper

Wireless in a de-perimeterised world

Problem

For mobile working, connectivity via wireless, whether inside the corporate environment or via publicly available hot-spots, Wi-Fi, Wi-Max or Cellular Data (GPRS, Edge, 3G) offers the ability for mobility while remaining connected to your resources. The issue for most corporates is how they provide secure connectivity for their mobile workers, and end up with a trade-off of risk, usability, cost, complexity and functionality.

For most mobile usage outside of the corporate WAN the use of IPSec VPN and 2-factor authentication is the most common standard, but whilst fine for static connectivity, say in a hotel room, it is restrictive for quick use "on-the-go". The use of wireless inside the corporation is a known security risk and is generally implemented in a number of ways:

1. **Totally untrusted;** the users still need to use VPN and 2-factor authentication, this does not encourage "occasional" use, neither is it user friendly.
2. **Authenticated usage;** using WPA2 and Radius or similar AAA solution users can enter a password, or 2-factor authentication that permits access and secures the air interface.
3. **Background authentication;** the connection of the PC uses Active Directory to perform 802.1x authentication of the hardware and validate the user's cached credentials. This is the most user-friendly but is generally limited to a Microsoft only corporate solution.

The flaw in all these solutions is that there are actually three separate problems:

1. Protection of the air-interface against unauthorised usage;
 - In the public space the protection and generation of revenues
 - In the corporate space, the protection against intrusion inside the corporate boundary
2. Authorisation of the user to make a connection into the corporate WAN;
3. Privacy and confidentiality of data transferred over the connection.

Why should I care

The deployment of wireless within an enterprise exposes the corporate network outside the physical constraints of the building. Thus any mis-configuration or weakness effectively de-perimeterises the whole organisation.

Current "secure" solutions are expensive and costly to manage and only work within a limited enterprise deployment. Conversely, systems that are secure (through employing inherently secure protocols) can utilise any wireless solution (corporate or public) without need for complex location awareness. With such a secure de-perimeterised solution, it is possible to implement a much simpler infrastructure, thus achieving significant cost savings.

In this new environment, risk to the corporation of unauthorised use is substantially reduced, and while the business may choose to provide an open solution, they may still wish to implement some degree of connection authorisation thus guaranteeing their wireless users quality of service (QoS).

Always refer to www.jerichoforum.org to ensure you have the latest version

Version: 1.0 April 2006

Paper available from the Jericho Forum

- The Jericho Forum Position Paper “Architecture for de-perimeterisation” is freely available from the Jericho Forum website

<http://www.jerichoforum.org>



Paper available from the Jericho Forum

- The Jericho Forum Eleven Principles or “commandments” are freely available from the Jericho Forum Website

<http://www.jerichoforum.org>



The image shows the cover of the "Jericho Forum Commandments" document. On the left side, there is a vertical black bar with the text "Jericho Forum" written vertically. At the top right, the "JERiCHO" logo is displayed. Below the logo, the title "Jericho Forum Commandments" is centered. The main body of the document contains an introduction paragraph, a section titled "Fundamentals" with three numbered points, and a section titled "Surviving in a hostile world" with two numbered points. At the bottom, there are two small lines of text: "Always refer to www.jerichoforum.org to ensure you have the latest version." and "Version 1.0 April 2000".

Jericho Forum

JERiCHO

Jericho Forum Commandments

The Jericho Forum commandments define both the areas and the principles that must be observed when planning for a de-perimeterised future. Whilst building on "good security", the commandments specifically address those areas of security that are necessary to deliver a de-perimeterised vision. The commandments serve as a benchmark by which concepts, solutions, standards and systems can be assessed and measured.

Fundamentals

- 1. The scope and level of protection must be specific & appropriate to the asset at risk**
 - Business demands that security enables business agility and is cost effective
 - Whereas boundary firewalls may continue to provide basic network protection, individual systems and data will need to be capable of protecting themselves
 - In general, it's easier to protect an asset the closer protection is provided
- 2. Security mechanisms must be pervasive, simple, scalable & easy to manage**
 - Unnecessary complexity is a threat to good security
 - Coherent security principles are required which span all tiers of the architecture
 - Security mechanisms must scale, from small objects to large objects
 - To be both simple and scalable, interoperable security "building blocks" need to be capable of being combined to provide the required security mechanisms
- 3. Assume context at your peril**
 - Security solutions designed for one environment may not be transferable to work in another. Thus it is important to understand the limitations of any security solution
 - Problems, limitations and issues can come from a variety of sources, including geographic, legal, technical, acceptability of risk, etc.

Surviving in a hostile world

- 4. Devices and applications must communicate using open, secure protocols**
 - Security through obscurity is a flawed assumption - secure protocols demand open peer review to provide robust assessment and thus wide acceptance and use
 - The security requirements of confidentiality, integrity and availability (reliability) should be assessed and built in to protocols as appropriate, not added-on
 - Encrypted encapsulation should only be used when appropriate and does not solve everything
- 5. All devices must be capable of maintaining their security policy on an untrusted network**
 - A "security policy" defines the rules with regard to the protection of the asset
 - Rules must be complete with respect to an arbitrary context
 - Any implementation must be capable of surviving on the raw Internet, e.g., will not break on any input

Always refer to www.jerichoforum.org to ensure you have the latest version.

Version 1.0 April 2000

Jericho Forum

Shaping security for tomorrow's world



www.jerichoforum.org