Welcome

2nd Jericho Forum Annual Conference
25th April 2005
Grosvenor Hotel,
Park Lane, London
Hosted by SC Magazine
Welcome & Housekeeping

- Richard Watts
  Publisher,
  SC Magazine
Agenda

- 11.05 Opening Keynote – “Setting the scene” - Paul Fisher, Editor SC Magazine
- 11.15 The Jericho Forum “Commandments” - Nick Bleech, Rolls Royce
- 11.30 Case Study: What Hath Vint Wrought - Steve Whitlock, Boeing
- 12.00 Real world application: Protocols - Paul Simmonds, ICI
- 12.15 Real world application: Corporate Wireless Networking - Andrew Yeomans, DrKW
- 12.30 Real world application: VoIP - John Meakin, Standard Chartered Bank
- 12.45 Case Study: Migration to de-perimeterised environment - Paul Dorey, BP
- 13.15 Lunch
- 14.30 Prepare for the future: The de-perimeterised “road warrior” - Paul Simmonds
- 14.50 Prepare for the future: Roadmapping & next steps - Nick Bleech
- 15.15 Break (Coffee & Tea)
- 15.45 Face the audience: (Q&A) - Moderated by: Paul Fisher, Editor, SC Magazine
- 16.45 Summing up the day - Paul Fisher, Editor, SC Magazine
- 17.00 Close
Some of our members

ICI
Belarc
Foreign & Commonwealth Office

Royal Mail
Cabinet Office

Dresdner Kleinwort Wasserstein

C&C Technology Consulting

We never forget who we’re working for™

LOCKHEED MARTIN

QANTAS
P&G

Standard Chartered

ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

EPFL

GSK

NEXUS

cybertrust

Qualys

Lilly

Capgemini

Consulting, Technology, Outsourcing

THE UNIVERSITY OF AUCKLAND
NEW ZEALAND

THE UNIVERSITY OF KENT
10 YEARS 1985-2005

IBM

ING

PHILIPS

CSIRO

Symantec

OBVIOUS A Telephone Company

BOEING

Novartis

NEC

Deloitte

Motorola

JERICHO FORUM
Opening Keynote

- “Setting the scene”

- **Paul Fisher,**
  *Editor SC Magazine*

[Image of SC Magazine Awards 2006]
Setting the Foundations

- The Jericho Forum “Commandments”

- Nick Bleech
  *Rolls Royce & Jericho Forum Board*
I have ten commandments. The first nine are, thou shalt not bore.

The tenth is, thou shalt have right of final cut.
Rationale

- Jericho Forum in a nutshell: “Your security perimeters are disappearing: what are you going to do about it?”
- Need to express what / why / how to do it in high level terms (but allowing for detail)
- Need to be able to draw distinctions between ‘good’ security (e.g. ‘principle of least privilege’) and ‘de-perimeterisation security’ (e.g. ‘end-to-end principle’)
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, not a ‘bible’
  - “A benchmark by which concepts, solutions, standards and systems can be assessed and measured.”
Structure of the Commandments

- Fundamentals (3)
- Surviving in a hostile world (2)
- The need for trust (2)
- Identity, management and federation (1)
- Access to data (3)
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.
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.
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.
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.
6. All people, processes, technology must have declared and transparent levels of trust for any transaction to take place.

- There must be clarity of expectation with all parties understanding the levels of trust.
- Trust models must encompass people/organisations and devices/infrastructure.
- Trust level may vary by location, transaction type, user role and transactional risk.
The need for trust

7. Mutual trust assurance levels must be determinable.

- Devices and users must be capable of appropriate levels of (mutual) authentication for accessing systems and data.
- Authentication and authorisation frameworks must support the trust model.
8. Authentication, authorisation and accountability must interoperate/exchange outside of your locus/area of control.

- People/systems must be able to manage permissions of resources they don't control.
- There must be capability of trusting an organisation, which can authenticate individuals or groups, thus eliminating the need to create separate identities.
- In principle, only one instance of person/system/identity may exist, but privacy necessitates the support for multiple instances, or once instance with multiple facets.
- Systems must be able to pass on security credentials/assertions.
- Multiple loci (areas) of control must be supported.
Finally, access to data

9. Access to data should be controlled by security attributes of the data itself.

- Attributes can be held within the data (DRM/Metadata) or could be a separate system.
- Access / security could be implemented by encryption.
- Some data may have “public, non-confidential” attributes.
- Access and access rights have a temporal component.
Finally, access to data

10. Data privacy (and security of any asset of sufficiently high value) requires a segregation of duties/privileges

- Permissions, keys, privileges etc. must ultimately fall under independent control
  - or there will always be a weakest link at the top of the chain of trust.
- Administrator access must also be subject to these controls.
Finally, access to data

11. By default, data must be appropriately secured both in storage and in transit.

- Removing the default must be a conscious act.
- High security should not be enforced for everything:
  - “appropriate” implies varying levels with potentially some data not secured at all.
Consequences ... is that it?

Desired Future State

Customers

Vendors

Work Types

Needs
Principles
Strategy

White Papers
Patterns
Use Cases

Guidelines
Standards
Solutions

Continuum

Standards and Solutions

Jericho Forum

Standards Groups
Consequences...is that it?

- We may formulate (a few) further Commandments ... and refine what we have ... based on
  - Your feedback (greatly encouraged)
  - Position papers (next level of detail)
  - Taxonomy work
  - Experience

- Today’s roadmap session will discuss where we go from here

What I have crossed out I didn't like. What I haven't crossed out I'm dissatisfied with.
The Jericho Forum “Commandments” are freely available from the Jericho Forum Website

http://www.jerichoforum.org
Case Study

- What Hath Vint Wrought

- Steve Whitlock
  Boeing
  Chief Security Architect
  Information Protection & Assurance
Prehistoric E-Business
Employees moved out...
Associates moved in...
The Globalization Effect

- is physically located inside 's perimeter and needs access to and

- is located physically outside 's perimeter and need access to

- 's application needs access to 's application which needs access to 's application

- is located physically inside 's perimeter and need access to
De-perimeterisation

- **De-perimeterisation**...
  - ... is not a security strategy
  - ... is a consequence of globalisation by cooperating enterprises

- **Specifically**
  - Inter-enterprise access to complex applications
  - Virtualisation of employee location
  - On site access for non employees
  - Direct access from external applications to internal application and data resources
    - Enterprise to enterprise web services

- **The current security approach will change:**
  - Reinforce the Defence-In-Depth and Least Privilege security principles
  - Perimeter security emphasis will shift towards supporting resource availability
  - Access controls will move towards resources
  - Data will be protected independent of location
Restoring Layered Services

Infrastructure Services

- **Network Services**
  - DNS
  - DHCP
  - Routing
  - Directory

- **Security Services**
  - Identity / Authentication
  - Authorisation / Audit

- **Other Services**
  - Systems Management
  - Print
  - Voice

Virtual Data Center

PEP
Defense Layer 1: Network Boundary

An externally facing policy enforcement point demarks a thin perimeter between outside and inside and provides these services:

Legal and Regulatory
- Provide a legal entrance for enterprise
- Provide notice to users that they are entering a private network domain
- Provide brand protection
- Enterprise dictates the terms of use
- Enterprise has legal recourse for trespassers

Availability
- Filter unwanted network noise
- Block spam, viruses, and probes
- Preserve bandwidth, for corporate business
- Preserve access to unauthenticated but authorised information (e.g. public web site)

Substantial access, including employees and associates will be from external devices.
Defense Layer 2: Network Access Control

Policy Enforcement Points may divide the internal network into multiple controlled segments.

Segments contain malware and limit the scope of unmanaged machines.

No peer intra-zone connectivity, all interaction via PEPs.

Rich set of centralized, enterprise services

Enterprise users will also go through the protected interfaces

All Policy Enforcement Points controlled by centralized services

Enterprise users will all go through the protected interfaces

Rich set of centralized, enterprise services

Policy Enforcement Points may divide the internal network into multiple controlled segments.

Segments contain malware and limit the scope of unmanaged machines.

No peer intra-zone connectivity, all interaction via PEPs.

Defense Layer 2: Network Access Control

Infrastructure Services

Network Services
- DNS
- DHCP
- Routing
- Directory

Security Services
- Identity / Authentication
- Authorisation / Audit

Other Services
- Systems Management
- Print
- Voice

All Policy Enforcement Points controlled by centralized services

Enterprise users will all go through the protected interfaces

Rich set of centralized, enterprise services

Policy Enforcement Points may divide the internal network into multiple controlled segments.

Segments contain malware and limit the scope of unmanaged machines.

No peer intra-zone connectivity, all interaction via PEPs.
Defense Layer 3: Resource Access Control

All access requests, including those from clients, servers, PEPs, etc. are routed through the identity management system, and the authentication and authorization infrastructures.

Controlled access to resources via Policy Enforcement Point based on authorization decisions.

Qualified servers located in a protected environment or virtual data center.

Additional VDCs as required, no clients or end users inside VDC.
Defense Layer 4: Resource Availability

Enterprise managed machines will have full suite of self protection tools, regardless of location.

Critical infrastructure services highly secured and tamperproof.

Administration done from secure environment within Virtual Data Center.

Resource servers isolated in Virtual Cages and protected from direct access to each other.
Identity Management Infrastructure

- Migration to federated identities
- Support for more principal types – applications, machines and resources in addition to people.
- Working with DMTF, NAC, Open Group, TSCP, etc. to adopt a standard
  - Leaning towards the OASIS XRI v2 format
Authentication Infrastructure

- Offer a suite of certificate based authentication services
- Cross certification efforts:
  - Cross-certify with the CertiPath Bridge CA
  - Cross-certify with the US Federal Bridge CA
  - Operate a DoD approved External Certificate Authority

Associates: authenticate locally and send credentials
External credentials: First choice – SAML assertions
Alternative – X.509 certificates

Boeing employees use X.509 enabled SecureBadge and PIN
Authorization Infrastructure

- Common enterprise authorization services
  - Standard data label template
  - Loosely coupled policy decision and enforcement structure
  - Audit service

Policies: legal, regulatory, IP, contract, etc.
Attributes: principal, data, environmental, etc.

Data

Applications

PDPs and PEPs use standard protocols to communicate authorization information (LDAP, SAML, XACML, etc.)
Resource Availability: Desktop

- Anti Virus
- Anti Spam Anti Spyware
- Host Based
  - IDS / IPS
- Active Protection Technology
- Trusted Computing, Virtualization
- Physical Controls
- Port and Device Control
- Software Firewall
- Encryption, Signature

Layered defenses controlled by policies, Users responsible and empowered, Automatic real time security updates

Health checked at network connection

Policy Decision Point
Resource Availability: Server / Application

Application Blades

Application Blade Detail

Server 1 Hardware

Server 1 Host OS

Server 1 Virtual Machine

Server 1 Virtual Network

Separate admin access

Policy Decision Point

No internal visibility between applications

In line network encryption (IPSec)

Virtual Network

Guest OS

Guest OS

Server N

Application A

Application B

Application C

Application A

Application in line network encryption (IPSec)

Application A

in line network packet filter

Virtual Network

Separate admin access

No internal visibility between applications
Resource Availability: Network

Multiple networks share logically partitioned but common physical infrastructure with different service levels and security properties.

Security Service Levels for:
- Network Control
- Voice over IP
- High Priority
- Special Projects
- General Purpose
Task patterns may be managed holistically.

All resources logically isolated by PEPs.

PEPs breached only for duration of task.
Supporting Services: Cryptographic Services

Centralized smartcard support

Encryption applications use a set of common encryption services

Key and Certificate Services

Policy driven encryption engine

Policy Decision Point

Policies determine encryption services

All keys and certificates managed by corporate PKI

PKI Services

Encryption and Signature Services

Code

Applications

Whole Disk

File

Data Objects

Tunnels

E-Mail

IM

Other Communications
Supporting Services: Assessment and Audit Services

- Log Analyzer
  - Logs collected from desktops, servers, network and security infrastructure devices
  - Policies determine assessment and audit, level and frequency

- Vulnerability Scanner
  - Automated scans of critical infrastructure components driven by policies and audit log analysis

- Log Analyzer
- Policy Decision Point
- IDS/IPS Sensors
- PEPs and PDPs
- Servers, network devices, etc.
Protection Layer Summary

Access and Defense Layers

Services by Layer

Access Flow

Layer Access Requirements

Internet
- External Services (public web, etc.)

Defense Layer 1: Network Boundary

Intranet
- DNS, DHCP, Directory Services

Defense Layer 2: Network Access Control

Enclave
- Basic Network Enclave Services

Defense Layer 3: Resource Access Control

Resource
- Application and Data Access

Defense Layer 4: Resource Availability

Service
- Only Administrative Access

Identification
- Authentication
- Authorization

Authentication
- Authorization
- Audit

Authorization
- Audit
- Secure Location
Real world application

- Protocols

- Paul Simmonds
  ICI Plc.
  & Jericho Forum Board
Problem

- Image an enterprise where;
  - You have full control over its network
  - No external connections or communication
    - No Internet
    - No e-mail
    - No connections to third-parties
  - Any visitors to the enterprise have no ability to access the network
  - All users are properly managed and they abide by enterprise rules with regard to information management and security
Problem

- In the real world nearly every enterprise;
  - Uses computers regularly connected to the Internet; Web connections, E-mail, IM etc.
  - Employing wireless communications internally
  - The majority of their users connecting to services outside the enterprise perimeter
- In this de-perimeterised world the use of inherently secure protocols is essential to provide protection from the insecure data transport environment.
Why should I care?

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

- New protocols are enabling secure application to application communication over the Internet
- 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, trust level and risk.
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.
Protocol Security & Attributes

- Protocols 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.
The need for open standards

- The Internet uses insecure protocols
  - They are de-facto lowest common denominator standards
  - But 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”

- An inherently secure protocol is;
  - Authenticated
  - Protected against unauthorised reading/writing
  - Has guaranteed integrity

- 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
Proprietary Solutions

- Vendors are starting to offer hybrid protocol solutions that support
  - multiple security policies
  - system/application integration
  - degrees of trust between organisations and communicating parties (their own personnel, customers, suppliers etc.)

- Resulting in proprietary solutions that are unlikely to interoperate, and whose security may be difficult to verify

- Important to classify the various solutions an organisation uses or is contemplating.
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
# Good & Bad Protocols

<table>
<thead>
<tr>
<th>Secure</th>
<th>Insecure</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Point Solution</strong> (use with care)</td>
<td><strong>Never Use</strong> (Retire)</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>AD Authentication</td>
<td>NTLM Authentication</td>
</tr>
<tr>
<td>COM</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Use &amp; Recommend</th>
<th>Use only with additional security</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMTP/TLS</td>
<td>SMTP</td>
</tr>
<tr>
<td>AS2</td>
<td>IMAP</td>
</tr>
<tr>
<td>HTTPS</td>
<td>POP</td>
</tr>
<tr>
<td>SSH</td>
<td>FTP</td>
</tr>
<tr>
<td>Kerberos</td>
<td>TFTP</td>
</tr>
<tr>
<td>AD Authentication</td>
<td>Telnet</td>
</tr>
<tr>
<td>COM</td>
<td>VoIP</td>
</tr>
<tr>
<td>NTLM Authentication</td>
<td>VoIP</td>
</tr>
<tr>
<td>SM</td>
<td>SNMP</td>
</tr>
<tr>
<td>SMB</td>
<td>NFS</td>
</tr>
</tbody>
</table>
Implementing new systems

- 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.
Paper available from the Jericho Forum

Real world application

- Corporate Wireless Networking
- Andrew Yeomans
  *DrK*W &
  *J*ericho Forum Board
Secure wireless connection to LAN

- Corporate laptops
- Use 802.11i (WPA2)
- Secure authenticated connection to LAN
- Device + user credentials
- Simple?
Not just laptops

- But also...
- Audio-visual controllers
- Wi-Fi phones
Blinkenlights?

- Play <Pong> with mobile phone!

Photo: Dorit Günter, Nadja Hannaske
Guest internet access too

- Mixed traffic
- Trusted or untrusted?
- How segregated?
Laptops also used at home or in café

[Diagram showing network connections and security measures]
Security complexity

- Need location awareness
- 802.11i if corporate wireless link
- VPN if not corporate
- Still not perfect security, insecure connections needed to set up café/home connections
- Security on direct connections too
Jericho visions

- Secure application protocols
- Common authentication
- Inter-network roaming

Costbucks coffee

Internet

QoS gate

LAN

Servers

AD

Guest

Corporate

AV

USB

USB

USB
Today’s complexity
Challenges to the industry

1. Companies should regard wireless security on the air-interface as a stop-gap measure until inherently secure protocols are widely available.
2. The use of 802.1x integration to corporate authentication mechanisms should be the out-of-the-box default for all Wi-Fi infrastructure.
3. Companies should adopt an “any-IP address, anytime, anywhere” (what Europeans refer to as a “Martini-model”) approach to remote and wireless connectivity.
4. Provision of full roaming mobility solutions that allow seamless transition between connection providers.
The Jericho Forum Position Paper
“Wireless in a de-perimeterised world”
is freely available from the Jericho Forum website
http://www.jerichoforum.org
Real world application

- Voice over IP

- John Meakin
  Standard Chartered Bank
  & Jericho Forum Board
The Business View of VoIP

- **It’s cheap?**
  - Cost of phones
  - Cost of “support”
  - Impact on internal network bandwidth

- **It’s easy?**
  - Can you rely on it?
  - Can you guarantee toll-bypass?

- **It’s sexy?**
  - Desktop video
The IT View of VoIP

- How do I manage bandwidth?
  - QoS, CoS

- How can I support it?
  - More stretch on a shrinking resource

- What happens if I lose the network?
  - I used to be able to trade on the phone

- How can I manage expectations?
  - Lots of hype; lots of “sexy”, unused/unusable tricks

- Can I make it secure??
The Reality of VoIP

- Not all VoIPs are equal!
  - Internal VoIP
    - Restricted to your private address space
    - Equivalent to bandwidth diversion
  - External VoIP
    - Expensive, integrated into PBX systems
  - “Free” (external) VoIP (eg Skype)
    - Spreads (voice) data anywhere
    - Ignores network boundary
    - Uses proprietary protocols – at least for security
The Security Problem

- Flawed assumption that voice & data sharing same infrastructure is acceptable
  - because internal network is secure (isn’t it?)
- Therefore little or no security built-in
- Internal VoIP
  - Security entirely dependent on internal network
  - Very poor authentication
- External VoIP
  - Some proprietary security, even Skype
  - Still poor authentication
  - BUT, new insecurities
VoIP Insecurity: An Example

Internet

1BPN PSAC
Infrastructure SCB GWAN

iPlanet Proxy

skype authentication service
skype supernode
skype node
neighbour relationships in skype network
node to skype supernode network relationship
survivability in skype network
To Make Matters Worse.....

- Why would you just want internal VoIP?
- Think of flexibility?
  - Remote working; mobile working; customer calls
- Think of where the bulk of voice costs are?
  - Think de-perimeterised
  - Think Jericho!
Recommended Solution/Response

- **STANDARDISATION!**
  - Allow diversity of phones (software, hardware), infrastructure components, infrastructure management, etc

- **MATURITY of security!**
  - All necessary functionality
  - Open secure protocol
    - Eg crypto
    - Eg IP stack protection
Secure “Out of the Box”

- Challenge is secure VoIP without boundaries
- Therefore...
  - All components must be secure out of box
  - Must be capable of withstanding attack
  - “Phones” must be remotely & securely maintained
  - Must have strong (flexible) mutual authentication
  - “Phones” must filter/ignore extraneous protocols
  - Protocol must allow for “phone” security mgt
  - Must allow for (flexible) data encryption
  - Must allow for IP stack identification & protection
Challenges to the industry

1. If inherently secure VoIP protocols are to become adopted as standards then they must be open and interoperable.
2. The Jericho Forum believes that companies should pledge support for moving from proprietary VoIP protocols to fully open, royalty free, and documented standards.
3. The secure VoIP protocol should be released 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 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 Jericho Forum Position Paper

“VoIP in a de-perimeterised world” is freely available from the Jericho Forum website

http://www.jerichoforum.org
Case Study

- Migration to a de-perimeterised environment

- Paul Dorey
  *BP & Jericho Forum Board*
Desktop Migration Strategy

- Previous Environment
- Drivers for Change
  - Business
  - Technology
  - Security
- Migration strategy
Current Architecture

- Flat Architecture
- Heterogeneous
- Barriers & Chokepoints
- “Us” and “Them” Solutions?
  - Wireless
  - VPNs
  - IDS/IPS
  - Discovery
  - Push Patch/Cfg.
  - NAC/NAP
Business Drivers (BP)

- Significant operations in 135+ countries
- Many users ‘on the road’, globally
- Large and increasing home-working
- Much use of outsourcers & contractors
- Many JVs, often with competitors
- Opening up to customers

The architypical ‘virtual enterprise’

- Wasting money on private networks
- Create barriers to legitimate 3rd parties
- Hard to define what is inside vs. outside?
Technology Drivers …

- Exploding connectivity and complexity (embedded Internet, IP convergence)
- Peer to peer, sensory networks, mesh, grid, mass digitisation
- Machine-understandable information (Semantic Web)
- De-fragmentation of computers into networks of smaller devices
- Wireless, wearable computing
Security Drivers

- Insiders
- Outsiders inside
- Port 80 and Mail traffic get in anyway
- Hibernating or ‘rogue’ devices
- Firewall rule chaos
- VOIP & P2P
- Stealth attackers
- Black list vs. white list
- False sense of security
Migration to the new model

1. Internal Managed.  
2. Managed VPN  
3. Self Managed & Gateway  
4. Commodity/Allowance
“In the Cloud” Security Services

- Automated Patching
- Anti-malware - heuristic
- Trusted Device Certification
- “Clean” mail, IM, Web
- Federated Identity/Access
- Provisioning
- Alert (“Shields Up”)
- Protection of ‘atomic’ data
- Trusted agent introduction  
  - (White Listing)

Can be ‘in the cloud’ or provided internally to ‘cloud resident’ devices
Desktop Strategy – Vision

**Beyond PassPort**
- seamless, secure access
- expose app not network

**PassPort**
- good apps access
- full network access
- wired & wireless access

**Explorer**
- internet based
- simplify client
- wireless access

**Applications & Access Strategy**
- Simplify client, apps and access

- choice of Device Connectivity Support

Auto-maintaining
User provided
Support choice

User maintained
BP provided
Self supported

BP maintained
BP provided
BP supported

Internet accessible
Bus Apps

Virtual Bus Apps

MDC

2006 Delivery
Maximise value during transition to vision

Net

BP

Apps

Internet hosted services

Consolidated Data Centres

<< $< $ = $
Desktop Strategy – Delivery of Vision

**Beyond PassPort**
- seamless, secure access
- expose app not network
- choice of Device Connectivity Support

**Delivery of Vision**
- Single, consumer-style client environment
- Seamless, secure connectivity
- Enhanced functionality, freedom and choice

**Auto-maintaining**
- User provided Support choice

\[ \Leftrightarrow \] \$  

**BP maintained**
- BP provided
- BP supported

**MDC**
- Access Security

**Net**
- Internet accessible Bus Apps
- Virtual Bus Apps

**BP**
- Auto-maintaining User provided Support choice

\[ = \] \$
Access Strategy - Scenarios

Access to applications from the Internet

**Strategic**
- **SSL**
  - No client software
  - Device and location agnostic
  - Firewall friendly
  - Connects at the application layer
  - Only requires access security
  - No direct contribution to single sign-on
  - Requires generic Infrastructure Access Service (ie. SSL gateway)

**Tactical**
- **IPSec VPN**
  - Installed client software
  - Device and location specific
  - Non-firewall friendly
  - Connects at the network layer
  - Requires additional device and access security
  - No direct contribution to single sign-on
  - Requires proprietary Infrastructure Access Services (ie. VPN gateway)

**Current**
- **BP Services**
  - File
  - ~2008
  - (SRA)

- **BP Services**
  - Intranet
  - ~Q2007
  - (RDP/HTTP)

- **SharePoint**
  - ~2008 (SRA)

- **Outlook 2003**
  - (RPC/HTTP)

- **New business application**
  - Requires generic Infrastructure Access Service
  - (ie. SSL gateway or per app ISA)

- **Legacy business application**
  - Requires proprietary Infrastructure Access Services
  - (ie. VPN gateway)

- **Shrink-wrap application**
  - Offline use
  - ~Local Virtual App

- **Remote Virtual App**

**Timeframe is now unless otherwise stated**

Microsoft native feature
Application Strategy - Scenarios

Exposure of applications to clients
(independent of underlying access mechanism)

Strategic
- Smart Client
  - smart client, self-updating client
  - direct SSL access to Smart application
  - eliminate compatibility issues
  - provide software update capability
- Remote Client
  - remote client, self-updating client, no offline capability
  - access via Infrastructure Access Services
  - eliminate compatibility issues
  - provide software update capability
- Thick Client
  - on-demand client, non-self-updating
  - access via Infrastructure Access Services
  - eliminate compatibility issues
  - provide software update capability

Tactical
- Current
- Thick Client
  - full thick client, non-self-updating, compatibility testing required = $ access via Infrastructure Access Services (ie. VPN gateway)

Browser
- SharePoint
- New business application
- Legacy business application
- Remote Virtual App
- Local Virtual App
- Shrink-wrap application (offline use)
- Outlook 2003 (RPC/HTTP)
BP PassPort

Backup and restore as a service
Internet connectivity
Vendor updates

In the Cloud Security Services
Internet Hosted Services
Expose BP Services to the Internet
Virtualise Business Applications
Software Self Provisioning
Expose BP Applications to the Internet
Remove Machine Domain Membership

Beyond PassPort

Backup to file server or no backup solution
BP network & Internet connectivity
Controlled updates and policies
Business Apps Local (scripted/tested)
Shrink-wrapped Apps Local (scripted/tested)
BP provided device
BP provided support
Perimeter / Device Security

BP PassPort Explorer

Backup to local device
Internet connectivity
Vendor updates
Business Apps Remote (scripted/tested)
Shrink-wrapped Apps Local (not scripted/tested)
BP provided device
BP provided support

Activity set prioritised in terms of
- ITStrategy
- Business Strategy
- Lunch
- Resume at 2.30pm
Fri, May 12, 2006
Motorola Center, Schaumberg, Chicago, IL, USA

- 09.00 Arrival
- 09.30 Welcome & Housekeeping
- 09.35 Opening Keynote: Setting the scene
- 09.50 The Jericho Forum Commandments
- 10.45 Break
- 11.00 Real world application: Protocols
- 11.20 Real world application: VoIP
- 11.40 Real world application: Corp. Wireless Networking
- 12.00 Case Study: Boeing: What Hath Vint Wrought?

- 12.30 Case Study: BP: Migration to a de-perimeterised environment
- 13.00 Lunch
- 14.00 The future: The de-perimeterised road warrior
- 14.45 The future: Roadmap & next steps
- 15.30 Break (Coffee & Tea)
- 15.45 Face the audience: Q&A
- 16.45 Summing up the day
  Bill Boni, Motorola
- 17.00 Close
Prepare for the future

- The de-perimeterised “road-warrior”
- Paul Simmonds
  *ICI Plc.*
  & Jericho Forum Board
Requirements

Voice over IP
Mobile e-Mail
Location & Presence
Web Access
E-mail / Calendar
Voice over IP
Corporate Apps

Wi-Fi, Ethernet
3G/GSM/GPRS
Wi-Fi / 3G
GSM/GPRS
Wi-Fi / 3G
GSM/GPRS
E-mail / Calendar
Corporate Apps
Requirements – Hand-held Device

- **VoIP over Wireless**
  - Integrated into Corporate phone box / exchange with calls routed to wherever in the world

- **Mobile e-Mail & Calendar**
  - Reduced functionality synchronised with laptop, phone and corporate server

- **Presence & Location**
  - Defines whether on-line and available, and the global location

- **Usability**
  - Functions & security corporately set based on risk and policy.
Requirements – Laptop Device

- **Web Access**
  - Secure, “clean”, filtered and logged web access irrespective of location

- **e-Mail and Calendar**
  - Full function device

- **Voice over IP**
  - Full feature set with “desk” type phone emulation

- **Access to Corporate applications**
  - Either via Web, or Clients on PC

- **Usability**
  - Functions & security corporately set based on risk and policy
  - Self defending and/or immune
  - Capable of security / trust level being interrogated
Corporate Access – The Issues

- Corporate users accessing corporate resources typically need;
  - Access to corporate e-mail (pre-cleaned)
  - Access to calendaring
  - Access to corporate applications (client / server)
  - Access to corporate applications (web based)
Putting it all together – Corporate Access

E-mail / Calendar secure protocol

Secure App Protocol

https Access to Corporate Apps

Corporate Perimeter / QoS Boundary

Internet
Web Access – The Issues*

- Single Corporate Access Policy
  - Regardless of location
  - Regardless of connectivity method
  - With multiple egress methods

- Need to protect all web access from malicious content
  - Mobile users especially at risk

* This will be the subject of a future Jericho Position Paper
Putting it all together – Web Access

Corporate Perimeter / QoS Boundary

Proxy Server

Proxy Chain

Safe

Internet Filtering & Reporting Service

Safe

Unsafe

Internet

Web Server
Voice /Mobile Access - The Issues

- Mobile / Voice devices require;
  - Connection of any VoIP device to the corporate exchange
  - Single phone number finds you on whichever device you have logged in on (potentially multiple devices)
  - No extra devices or appliances to manage
  - Device / supplier agnostic secure connectivity
Putting it all together – VoIP Access

Corporate Perimeter / QoS Boundary

Authentication System

VoIP Server

sVoIP

sVoIP

Internet

sVoIP

sVoIP

Imbedded Soft-phone

Home Office
Issues - Trust

- NAC generally relies on a connection
  - Protocols do not make a connection in the same way as a device

- Trust is variable
  - Trust has a temporal component
  - Trust has a user integrity (integrity strength)
  - Trust has a system integrity

- Two approaches;
  - Truly secure sandbox (system mistrust)
  - System integrity checking
Putting it all together – System Trust

- AppServer
- Secure App Protocol
- Query
- Integrity Query
- Integritiy Module
- Corporate Perimeter / QoS Boundary
- Internet
- Sandbox
- System Trust Broker Service
An inherently secure system

- When the only protocols that the system can communicate with are inherently secure;
  - The system can “black-hole” all other protocols
  - The system does not need a personal firewall
  - The system is less prone to malicious code
  - Operating system patches become less urgent
An inherently secure corporation

- When a corporate retains a WAN for QoS purposes;
  - WAN routers only accept inherently secure protocols
  - The WAN automatically “black-holes” all other protocols
  - Every site can have an Internet connection as well as a WAN connection for backup
  - Non-WAN traffic automatically routes to the Internet
  - The corporate “touchpoints” now extend to every site thus reducing the possibility for DOS or DDOS attack.
Paper available soon from the Jericho Forum

- The Jericho Forum Position Paper “Internet Filtering and reporting” is currently being completed by Jericho Forum members.

http://www.jerichoforum.org
Prepare for the future

- Road-mapping & next steps

- Nick Bleech
  Rolls Royce & Jericho Forum Board
We want a story that starts out with an earthquake and works its way up to a climax.
Two Ways to Look Ahead

- Solution/System Roadmaps (both vendor and customer)
- Security Themes from the Commandments
  - Hostile World
  - Trust and Identity
  - Architecture
  - Data protection
Solution/System Roadmaps

- Work Types
  - Needs
  - Principles
  - Strategy
  - White Papers
  - Patterns
  - Use Cases
  - Guidelines
  - Standards
  - Solutions

- Desired Future State
- Customers
- Vendors

- Continuum

- Standards and Solutions

- Jericho Forum
- Standards groups
## Potential Roadmap

### Key Components

<table>
<thead>
<tr>
<th>New &amp; evolving technologies (partial)</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Firewalls (Filter/DPI/Proxy)</td>
</tr>
<tr>
<td>• Anti-Virus Anti-Spam</td>
</tr>
<tr>
<td>• Cl/Svr Patch Mgmt</td>
</tr>
<tr>
<td>• IPSec VPN</td>
</tr>
<tr>
<td>• SSL/Web SSO</td>
</tr>
<tr>
<td>• Proxies/IFR for Trading Apps</td>
</tr>
<tr>
<td>• - Web/Messaging</td>
</tr>
<tr>
<td>• DS point solutions</td>
</tr>
<tr>
<td>• IPS point solutions</td>
</tr>
<tr>
<td>• Dev config</td>
</tr>
<tr>
<td>• Firewalls (Fltr/DPI)</td>
</tr>
<tr>
<td>• Anti-Virus/Spam</td>
</tr>
<tr>
<td>• Svr Patch Mgmt</td>
</tr>
<tr>
<td>• Proxies/IFR for Trading Apps</td>
</tr>
<tr>
<td>• - Web/Messaging</td>
</tr>
<tr>
<td>• DS point solutions</td>
</tr>
<tr>
<td>• TL/NL gateways</td>
</tr>
<tr>
<td>• XML point solutions</td>
</tr>
<tr>
<td>• Fed. Identity</td>
</tr>
<tr>
<td>• Intrusion correlation &amp; response</td>
</tr>
<tr>
<td>• Micro-perim mgmt &amp; device firewall/config</td>
</tr>
</tbody>
</table>

### 60% Adoption Pre 2006

- Firewalls (Fltr/DPI)
- Anti-Virus/Spam
- Svr Patch Mgmt
- Proxies/IFR for Trading Apps
- DS point solutions
- TL/NL gateways
- Fed. Identity
- Intrusion correlation & response
- Micro-perim mgmt & device firewalls/config
- Fed’d surface OS & client/svr patching
- Virtual Proxies/IFR
- XML subsetting
- P2P trust models
- Interoperable DS

### Key Obsoleted Technology

- Dial-up security
- Simple IDS
- IPsec VPN
- Firewall-based proxies
- Proxies/IFR for - Web/Messaging
- XML point solutions
- Clnt ’service releases’
- Hybrid IPsec/TLS gateways
- Proxies/IFR
- Standalone AV
- Fltr Firewalls
- Svr ’service releases’
- Fed. Identity

<table>
<thead>
<tr>
<th>60% Adoption Pre 2006</th>
<th>2006</th>
<th>2007</th>
<th>2008</th>
<th>2009</th>
</tr>
</thead>
<tbody>
<tr>
<td>60% Adoption Pre 2006</td>
<td>2006</td>
<td>2007</td>
<td>2008</td>
<td>2009</td>
</tr>
<tr>
<td>Dial-up security</td>
<td>2006</td>
<td>2007</td>
<td>2008</td>
<td>2009</td>
</tr>
<tr>
<td>Simple IDS</td>
<td>2006</td>
<td>2007</td>
<td>2008</td>
<td>2009</td>
</tr>
<tr>
<td>IPsec VPN</td>
<td>2006</td>
<td>2007</td>
<td>2008</td>
<td>2009</td>
</tr>
<tr>
<td>Firewall-based proxies</td>
<td>2006</td>
<td>2007</td>
<td>2008</td>
<td>2009</td>
</tr>
<tr>
<td>Proxies/IFR for - Web/Messaging</td>
<td>2006</td>
<td>2007</td>
<td>2008</td>
<td>2009</td>
</tr>
<tr>
<td>XML point solutions</td>
<td>2006</td>
<td>2007</td>
<td>2008</td>
<td>2009</td>
</tr>
<tr>
<td>Clnt ’service releases’</td>
<td>2006</td>
<td>2007</td>
<td>2008</td>
<td>2009</td>
</tr>
<tr>
<td>Hybrid IPsec/TLS gateways</td>
<td>2006</td>
<td>2007</td>
<td>2008</td>
<td>2009</td>
</tr>
<tr>
<td>Proxies/IFR</td>
<td>2006</td>
<td>2007</td>
<td>2008</td>
<td>2009</td>
</tr>
<tr>
<td>Standalone AV</td>
<td>2006</td>
<td>2007</td>
<td>2008</td>
<td>2009</td>
</tr>
<tr>
<td>Fltr Firewalls</td>
<td>2006</td>
<td>2007</td>
<td>2008</td>
<td>2009</td>
</tr>
<tr>
<td>Svr ’service releases’</td>
<td>2006</td>
<td>2007</td>
<td>2008</td>
<td>2009</td>
</tr>
<tr>
<td>Fed. Identity</td>
<td>2006</td>
<td>2007</td>
<td>2008</td>
<td>2009</td>
</tr>
</tbody>
</table>
Hostile World Extrapolations

- Convergence of SSL/TLS and IPsec:
  - Need to balance client footprint, key management, interoperability and performance.
  - Server SSL = expensive way to do authenticated DNS.
  - Need a modular family of inherently secure protocols.
  - See Secure Protocols and Encryption & Encapsulation papers.

- Broad mass of XML security protocols condemned to be low assurance.
  - XML Dsig falls short w.r.t. several Commandments

- Platforms are getting more robust, but:
  - Least privilege, execute-protection, least footprint kernel, etc. ... WIP
  - Need better hardware enforcement for protected execution domains.
  - Papers in preparation.

- Inbound and outbound proxies, appliances and filters litter the data centre - time to move them ‘into the cloud’.
  - See Internet Filtering paper.
Trust and Identity Extrapolations

- ‘Trust management’ first identified in 1997; forgotten until PKI boom went to bust.
  - Last three years research explosion
- Decentralised, peer to peer (P2P) models are efficient
  - Many models: rich picture of human/machine and machine/machine trust is emerging.
  - Leverage PKC (not PKI) core concepts; mind the patents!
- ‘Strong identity’ and ‘strong credentials’ are business requirements.
- ‘Identity management’ is a set of technical requirements.
  - How we do this cross-domain in a scalable manner is WIP.
- At a technical level, need to clear a lot of wreckage.
  - ASN.1, X.509 = ‘passport’, LDAP = ‘yellow pages’ ... etc.
- Papers in preparation.
Architecture Extrapolations

- Enterprise-scale systems architecture is inherently domain-oriented and perimeterised (despite web and extranet).
  - Client-server and multi-tier.
  - Service-oriented architecture -> web services.
  - Layer structure optimises for traditional applications
  - Portals are an attempt to hide legacy dependencies.

- Collaboration and trading increasingly peer-to-peer.

- Even fundamental applications no longer tied to the bounded ‘enterprise’:
  - Ubiquitous computing, agent-based algorithms, RFID and smart molecules point to a mobile, cross-domain future.
  - Grid computing exemplifies an unfulfilled P2P vision, encumbered by the perimeter.
  - See Architecture paper.
Data Protection Extrapolations

- Digital Rights Management has historically focused exclusively on copy protection of entertainment content.
- ‘Corporate’ DRM as an extension of PKI technology now generally available as point solutions.
  - Microsoft, Adobe etc.
  - Copy ‘protection’, non-repudiation, strong authentication & authorisation.
  - ‘Labelling’ is a traditional computer security preoccupation.
- Business problems to solve need articulating.
  - The wider problem is enforcement of agreements, undertakings and contracts; implies data plus associated ‘intelligence’ should be bound together.
- Almost complete absence of standards.
- Paper in preparation.
What about ‘People and Process’?

Jericho Forum assumes a number of constants:

- Jurisdictional and geopolitical barriers will continue, and constrain (even reverse) progress.
- Primary drivers for innovation and technology evolution are:
  - Perceived competitive advantage / absence of disadvantage.
  - Self-interest of governments and their agents as key arbiters of demand (a/k/a/ the Cobol syndrome).
- IT industry will continue to use standards and patents as proxies for proprietary enforcement.
- Closed source vs. open source is a zero sum.
How are we engaging?

- **Stakeholders WG: chair - David Lacey**
  - Corporate and government agendas
  - Our position in the Information Society

- **Requirements WG: chair - Nick Bleech**
  - Business Scenarios, planning and roadmapping
  - Assurance implications

- **Solutions WG: chair - Andrew Yeomans**
  - Patterns, solutions and standards
  - Jericho Forum Challenge
Conclusions

- A year ago we set ourselves a vision to be realised in 3-5 years
- Today’s roadmap shows plenty of WIP still going on in 2009!
- Want this stuff quicker? Join us!

I never put on a pair of shoes until I've worn them at least five years.
The Jericho Forum Position Paper “Architecture for de-perimeterisation” is freely available from the Jericho Forum website

http://www.jerichoforum.org
Break

Tea & Coffee served

Resume at 3.45pm
- Face the audience

- Moderated by;
  Paul Fisher,
  *Editor SC Magazine*
Summing up the day

Paul Fisher,  
*Editor SC Magazine*
The Jericho Forum – 2nd US Conference

Fri, May 12, 2006
Motorola Center, Schaumberg, Chicago, IL, USA

- 09:00 Arrival
- 09.30 Welcome & Housekeeping
- 09.35 Opening Keynote: Setting the scene
- 09.50 The Jericho Forum Commandments
- 10:45 Break
- 11.00 Real world application: Protocols
- 11.20 Real world application: VoIP
- 11.40 Real world application: Corp. Wireless Networking
- 12.00 Case Study: Boeing: What Hath Vint Wrought?
- 12.30 Case Study: BP: Migration to a de-perimeterised environment
- 13.00 Lunch
- 14.00 The future: The de-perimeterised road warrior
- 14.45 The future: Roadmap & next steps
- 15.30 Break (Coffee & Tea)
- 15.45 Face the audience: Q&A
- 16:45 Summing up the day Bill Boni, Motorola
- 17:00 Close
JERICHO FORUM
Shaping security for tomorrow’s world

www.jerichoforum.org