

Jericho Architecture

Architectures for a Jericho Environment

Paul Simmonds

Global Information Security Director, ICI



Jericho Vision

Vision

- To enable business confidence beyond the constraint of the corporate perimeter, through
 - Cross-organizational security processes
 - Shared security services
 - Products that conform to Open security standards
 - Assurance processes that when used in one organization can be trusted by others

Jericho Mission

Mission

- Act as a catalyst to accelerate the achievement of the vision, by
 - Defining the problem space
 - Communicating the collective vision
 - Challenging constraints and creating an environment for innovation
 - Demonstrating the market
 - Influencing future products and standards

Timetable

- A period of 3-5 years for the achievement of its Vision, whilst accepting that, in fact, its Mission would be ongoing beyond that.

Jericho Participants

Abbot Laboratories

ABN AMRO Bank

Airbus

BAPLA

Barclays Bank

BAE SYSTEMS

Boeing

BBC

BP

Cabinet Office (UK)

Cable & Wireless

Clearstream

Credit Agricole

Credit Suisse First Boston

Deloitte

Deutsche Bank

DKW

Eli Lilly

Ernst & Young LLP

Geisinger Health System

GlaxoSmithKline

HBOS

HSBC

ICI

ING

Iron Mountain

JPMorgan Chase

KPMG LLP (UK)

Lloyds TSB

Lockheed Martin

MBNA Europe Bank

National Australia Bank Group

Northern Rock

Olswang Solicitors

PA Consulting

Pfizer

Procter & Gamble

Qantas

Reuters

Rolls-Royce

Romeike

RBS

Royal Dutch/Shell

Royal Mail

Standard Chartered Bank

The Open Group

UBS Investment Bank

UKCeB (Council for e-Business)

Unilever

Uni. of Kent Comp. Labs

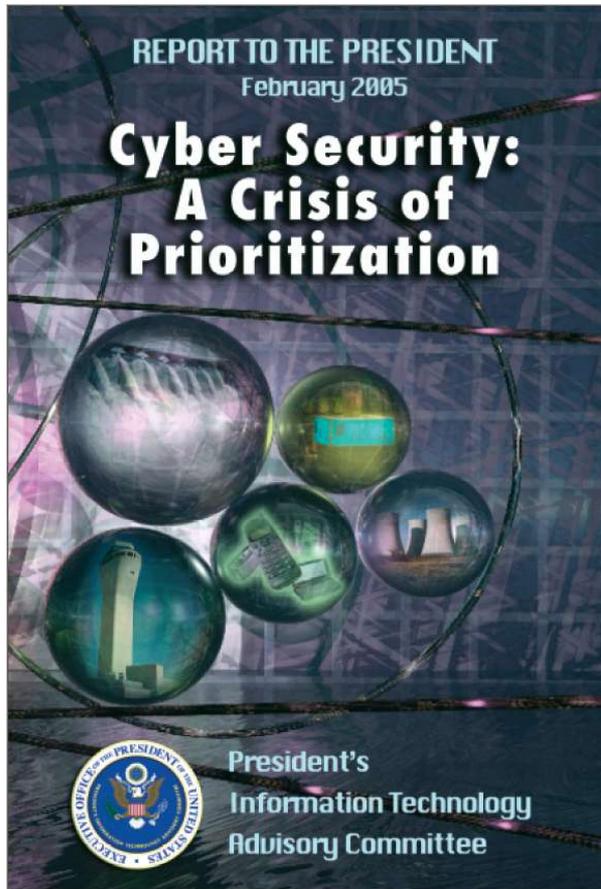
YELL

WIIFM** Drivers

1. Supports outsourced / utility security model
2. Jericho supported standards – not products
3. Jericho to highlight issues with standards-based implementations
4. Jericho principles should flow down into consumer grade products / services where applicable
5. Jericho implementation will reduce cost and increase security and ability to do business (ROSI).

** *What's in it for me*

Cyber Security: A Crisis of Prioritization



- **Cyber Security: A Crisis of Prioritization** (February 2005) http://www.itrd.gov/pitac/reports/20050301_cybersecurity/cybersecurity.pdf
- A broad consensus among computer scientists is emerging that the approach of patching and retrofitting networks, computing systems, and software to “add” security and reliability may be necessary in the short run but is inadequate for addressing the Nation’s cyber security needs.

Cyber Security: A Crisis of Prioritization

- **Fundamentally New Security Models, Methods Needed**
 - Addressing cyber security for the longer term requires a vigorous ongoing program of fundamental research to explore the science and develop the technologies necessary to design security into computing and networking systems and software from the ground up.
 - The vast majority of cyber security research conducted to date has been based on the concept of perimeter defence.
 - In this model, what is “inside” an information system or network is protected from an “outside” attacker who tries to penetrate it to gain access to or control its data and system resources. However, once the perimeter is breached (whether by virtue of a technical weakness such as a software vulnerability or an operational weakness such as an employee being bribed or tricked to reveal a password), the attacker has entirely free rein and can compromise every system connected in a network with not much more effort than is required to compromise only one.

Cyber Security: A Crisis of Prioritization

- Fundamentally New Security Models, Methods Needed (cont.)
 - This weakness of the perimeter defence strategy has become painfully clear. But it is not the only problem with the model. The distinction between “outside” and “inside” breaks down amid the proliferation of wireless and embedded technologies connected to networks and the increasing complexity of networked “systems of systems.”
 - One element of a more realistic model for cyber security may be a principle of mutual suspicion: Every component of a system or network is always suspicious of every other component, and access to data and other resources must be constantly reauthorized. More generally, cyber security would be an integral part of the design process for any large, complex system or network.
 - Security add-ons will always be necessary to fix some security problems, but ultimately there is no substitute for system-wide end-to-end security that is minimally intrusive.

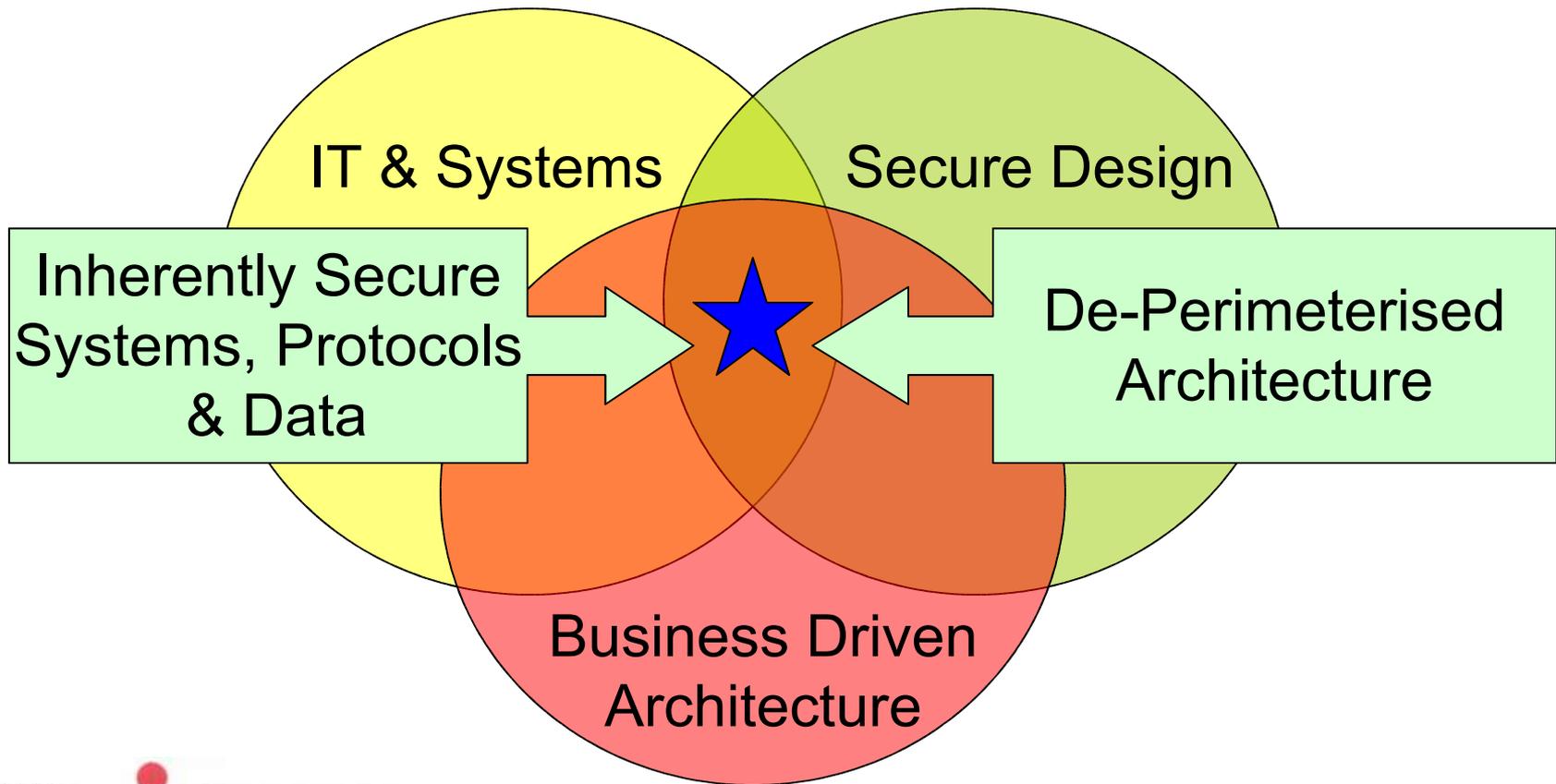
Jericho Architecture

Background

- Jericho Forum does not have a monopoly on good security!
- To refine what are Jericho Architectural principals vs. Good Secure Design
- Build on the work in the visioning document
- To define key items aligned with the message that make this specifically Jericho.
- To clarify that there is not just one “Jericho solution”

Jericho Architecture

Jericho principals vs. Good Secure Design



Jericho Architecture

1. General Principles
2. Network
3. System
4. Protocols
5. Authentication
6. Data

General Principles

1. Can operate in an insecure / hostile environment
2. Is inherently secure*
3. Can communicate with all it's resources securely using just the Internet
4. Interoperability – assurance (trust) level can be ascertained by another
5. Simple, scalable – not too complex and thus n! problem
6. Protection as close as possible to the item being protected

* *"Inherent Security" - That everything is;*

- *Authenticated*
- *Protected against unauthorised reading (probably Encrypted)*
- *Repudiatable*

Network

Jericho supports the "Martini" concept

– any IP address, any time, anywhere

- Do we (Jericho) care?
- Is QoS (especially inside businesses) a business or security question?
- Is Internet QoS essential to the Jericho principle of being to operate your business on the Internet?

Options in a corporate environment

8. The network should only allow authenticated protocols to flow
 9. The network should be capable of allowing only permitted traffic
- * *Implication of architecture and especially encrypted protocols potentially limit some network capabilities*

Systems

***The “Trick or Treat” principle, the doors are locked
– no one is answering***

3. Systems* are capable / responsible of defending themselves
4. Any use of open protocol has protocol based IDS
 - **pids** – protocol intrusion detection
 - **aapids** – application aware protocol IDS
5. Application needs to be self defending
6. Connection to other systems authenticate at;
 - Group level (part of ICI and thus requires an ICI certificate)
 - Machine/System/function level (this is an AD domain controller)
 - Thus; I’m an ICI AD Domain controller and will only replicate / securely communicate with other ICI AD Domain Controllers

* System: an entity, could be PC, motherboard component, or ERP system, multi-server web application

Protocols

FTP & Telnet – “Just say NO!”

Secure Protocols

- Only inherently secure protocols should be used
- The protocol should not encapsulate another insecure protocol (IPSec / VPN etc.)
- The protocol should be capable of authenticating itself

Insecure Protocols (http for example)

- Only used where interaction with non-trusted environment essential
- Protocol must be validated against application.

Authentication

"If you are not on the list you are not coming in"

3. All communications are authenticated
4. Strong, federated, authentication required
5. Strong / Appropriate levels of trust
6. Mutual Authentication – need to trust both source and destination
7. Open, pervasive, works globally
8. All items should be authenticated
 - Users
 - Computers
 - Protocols

Data

"I've always marvelled at these companies' ability to say they care about consumer privacy with a straight face."*

- All data is inherently secure
- Data should only be readable by the person(s) intended.
- The data itself should be protected (encrypted)

* Ray Everett-Church, PrivacyClue on ChoicePoint data theft

http://news.com.com/ChoicePoint+data+theft+widens+to+145,000+people/2100-1029_3-5582144.html

Issues

Good Security, Standards and Perception

Technology that is not specifically Jericho related

- “Trumpet Technology” support technology that supports the Jericho Vision but is good security rather than Jericho vision specific

Standards

- The Jericho Forum are the arbiters of standards that work in the corporate environment
 - Balance between innovation, royalties, patents, fair use and open standards

Perception

- Fully open == unobtainable
 - Solutions should be fit for (corporate) purpose (pragmatic solution aka 80/20 rule).

Jericho Challenge

Why the Jericho Challenge?

- Jericho Forum does not have a monopoly on good security
- Jericho Forum does not have a monopoly on visionary thinking
- Many organisations will choose not to formally join Jericho
- Jericho may not appeal to the academic world, small specialist start-ups and individuals

However the Jericho Forum wants to be as inclusive as possible.

Jericho Challenge

Going forward the Jericho Forum needs to. . .

- Change the mindset of security and IT professionals
- Facilitate the discussion on new secure de-perimeterised architectures
- Enable everyone to start developing Jericho-type architectures and solutions
- To re-enforce that there is not just one “Jericho solution”

Jericho Challenge

The Jericho Challenge – 2005 . . .

- In collaboration with Black Hat, this global competition challenges any team of technology experts to design a secure architectural solution that is open, interoperable, viable, and operates in a de-perimeterised environment
- Initially papers to be presented (if successful) at Blackhat Las Vegas
- Papers will be independently judged against Jericho principles
- Prizes will be awarded!

Jericho Challenge

The details

- Deadline for entries is May 30th, with selected papers presented in July 2005.
- Papers should be submitted in the normal manner for Blackhat submissions and will be subject to the normal scrutiny
- Papers should be clearly marked as wanting to be considered for the Jericho Challenge.