
De-perimeterisation: fact or fiction?

Geraint Price

Information Security Group

Royal Holloway

Outline

- Introduction
- The Jericho Forum
- Where it works...
- ...and where it doesn't
- The future?
- Conclusions

Introduction

- There is no doubt that the majority of organisations' perimeters are becoming more porous.
- This has been driven by a number of factors, including:
 - Increased connectivity
 - Proliferation of mobile computing platforms
 - Increased reliance on electronic communication mechanisms (e.g. email, web)
 - An increased desire to share business information
 - Externalisation of computing resources (e.g. outsourcing)
- This has a clear impact on the security of information systems.

The Jericho Forum

- A group of individuals and organisations working collaboratively to highlight the issues surrounding *de-perimeterisation*.
- Published:
 - A Visioning Paper
 - A set of Commandments
 - A set of Position Papers
- Aim to influence technology vendors, standards organisations, business consumers.
- More information from:
 - www.jerichoforum.org

The Context for this Discussion

- What is this talk about?
 - We are not aiming to discredit the Jericho Forum
 - We agree with many – if not all – of their starting assumptions.
 - We agree with many – if not all – of their goals.
 - We agree that much still needs to be done to improve on the security of information in a truly open and distributed environment.
 - Our primary aim is to critically evaluate their concepts and proposals – and hopefully contribute to what is a very important discussion.

Some Laudable Goals & Statements

- “[...] *communication which does not rely on the underlying security of the communications infrastructure connecting the collaborating organisations.*”
- “[...] *reinforcing what has been known for years but rarely implemented, that unless security is built-in from the ground up it will rarely be effective.*”
- “*Many existing standards in this field are poorly specified, ambiguous, and difficult to understand and validate.*”

Some Unhelpful Goals & Statements

- *“We want to dispel the long-held belief that the firewall is the best place to implement security.”*
- *“Such a model would connect an organization and its business processes to all external stakeholders, seamlessly and securely, enabling employees, suppliers, and customers to collaborate, anytime, anywhere, and at the lowest cost to all.”*

The Jericho Forum Commandments

1. *The scope and level of protection should be specific & appropriate to the asset at risk.*
 - We couldn't agree more with this statement.
2. *Security mechanisms must be pervasive, simple, scalable & easy to manage.*
 - Again, a valid statement. However, in our opinion this puts a lot of onus on the security implemented to be "plug'n'play" – and this is hard.
3. *Assume context at your peril.*
 - Again, we couldn't agree more with this statement.

The Jericho Forum Commandments

4. *Devices and applications must communicate using open, secure protocols.*
 - Again, a solid goal, and known good practice (where possible).
5. *All devices must be capable of maintaining their security policy on an untrusted network.*
 - While this a laudable goal, the following sub-text is likely to cause friction with a combination of #2 and #3.
 - *“Rules must be complete with respect to an arbitrary context”.*
6. *All people, process, technology must have declared and transparent levels of trust for any transaction to take place.*
 - Again, a good goal. However, trust management is in its infancy.

The Jericho Forum Commandments

7. *Mutual trust assurance levels must be determinable.*
 - Requires advanced levels of trust management and mutual authentication – both are hard.
8. *Authentication, authorisation and accountability must interoperate/exchange outside of your locus/area of control.*
 - Implies a global (or semi-global) ID space, and interoperable permissions management – both are hard.
9. *Access to data should be controlled by security attributes of the data itself.*
 - Again, I agree in principle, but the technology to achieve this in an “arbitrary” context doesn’t (is unlikely?) to exist.

The Jericho Forum Commandments

10. *Data privacy (and security of any asset of sufficiently high value) requires segregation of duties/privileges.*
 - Again, I couldn't agree more, and will require a solid understanding of the context of the business process being secured.
11. *By default, data must be appropriately secured when stored, in transit and in use.*
 - Again, I couldn't agree more. However, I am unsure about how this will combine with #5 – the combination of *appropriately* and *arbitrary* is likely to be a difficult balancing act.

Where it Works...

- Protection of information at all stages of the information life-cycle – at rest and in transit.
- The ability to support remote workers (aka *road-warriors*) who need to access business process from home or some other premises.
 - These tend to be business process specific implementations which allow the client to connect securely back to the organisation's servers.
- Finally implementing known “good practice” and technology which has been missing previously.
 - So why now? Increased connectivity; business demand; lowering cost; an understanding of increased risk; ...

Where Are We Now?

- Mostly secure provisioning, and supporting, of internal services to work remotely.
- A few, specialised, cross-organisational processes and services.
 - e.g. ERP
- Implementations of known technologies.
- A reliance on *trusted third parties* (TTPs).
- A *digital umbilical cord* model.

...and Where it Doesn't

- Where the device is not owned by the organisation.
 - It could feasibly be extended to devices “owned” by a trusted partner organisation.
- In some of the more far-reaching goals of the Jericho Forum:
 - “anytime, anywhere” security...
- Extending the data security model to “arbitrary” platforms.
 - This is essentially DRM, which is fatally flawed.
- Contract and trust negotiation “on the fly”.
- Access Control at the content (paragraph/line) level.

Why Are These Scenarios More Difficult?

- Key Management is **HARD**.
 - This is particularly true if we have no *source of authority*.
- **Mutual authentication** is extremely difficult in an open system.
- Cross-organisational access control is difficult to implement and manage.
- Doing security well relies on context (JFC#3), which is generally an opposing force to flexibility (JFC#5).

The Future?

- Some questions which would be interesting to answer:
 - What % of business processes and transactions need this technology?
 - Do they differ in terms of the computational model from other services?
 - Can we leverage these differences?
 - Can we get away from TTP models?
 - Decentralised and P2P trust models are in their infancy.
 - Can we influence the next generation of architectures?
 - What do we need in terms of architectural support?

The Future?

- More work needs to be done on the following:
 - Context and business process specific flexibility.
 - Cross-domain Identity and Access Management is about much more than just the technology.
 - At least at the more far reaching goals that some of the Jericho Forum's Position Papers aim for.
 - A thorough analysis on where current technology falls short of the long-term goals, and how to close those gaps.
 - Scalable and cost-effective management of existing technologies.

The Hindrances

- The business driver.
- The underlying technology.
- Proofs of concept and pilot implementations don't always lead to workable, scalable and cost-effective solutions.
- The difficulty of managing these processes securely.
- Fighting commercial pressures.
 - Particularly in relation to: privacy; collaborative standards.
- Cost, cost, cost...
 - Not just financial, but also people, process and management.

Conclusions

- There is no doubt that the changing relationship between *inside* and *outside* the perimeter.
 - What I believe we are seeing is a *perimeter reformation*.
- Existing technology can be used to implement the changes to some degree.
- Further steps are likely to be hindered by technology that is immature, or very difficult to implement.
- Further work needs to be carried out on:
 - the security management;
 - the relationship between the business process and the security;
 - the relationship between the security and the business drivers.

Acknowledgements

- I would like to thank:
 - Terry Bebbington
 - Paul Simmonds

Q & A...

Thank you

Geraint Price

geraint.price@rhul.ac.uk