Defensible Digital Boundaries

Clark Thomborson  
Bojan Zdrnja  
Peter Gutmann  
Darren Bilby  
Andrew Lee  
Gordon Grant

University of Auckland  
University of Auckland  
Cryptoplumber  
Security-Assessment.com  
ESET LLC  
Resilience Corporation
What is a security perimeter?

- All actors inside the perimeter are either “authorised”, or else they are “intruders”.
- At the perimeter, we must
  - Identify
  - Authenticate, and then
  - either Authorise or exclude.
- Inside the perimeter, we should
  - Restrict (sandbox), Detect, Recover, Punish.
Defensible perimeters?

- **Platform**: boundaries are the I/O ports of a single computational device such as a laptop computer or cellphone.
- **Virtual**: boundaries are defined by the virtualising software and operating system on the host platform.
- **Service**: boundaries are platforms and connections to subsystems that provide specialised services, such as email, fileservice, Kerberos authentication, or identity management.
- **Facility**: boundaries are defined by “bricks and mortar”.
- **Corporate**: boundaries are defined by an ownership and management structure.
- **National**: boundaries are defined by a territorial (judicial) authority.
De-Perimeterisation!

- A corporate perimeter defines a QoS boundary (availability).
- Inner perimeter(s), e.g. individual platforms or virtual machines, defend integrity and confidentiality.
- The emphasis is on making connections between well-authenticated users on trustworthy (well-managed) platforms.
  - Identity management is a key requirement.
The Jericho Forum

- **What’s in it for us?** We need Security Solutions that support de-perimeterisation.
  - so we aim to stimulate a market for solutions to de-perimeterisation problems.
  - We want these solutions to use open standards, to improve interoperability and integration, both within our own IT systems and with our business partners.

- **Organisation?** User members own the Forum, vote on the deliverables, and run the Board of Managers (BoM).
  - Vendors have no voting rights on deliverables or on the BoM.
  - We now have 12 vendor members, and want more, because we need to work with vendors.
Some of our members

http://www.opengroup.org/jericho/