New York Conference 2007
at Infosecurity NY 2007
Jacob Javits Center, New York, NY

September **11th, 2007**

The program handed out to attendees to this conference, including the agenda and speaker information, and all the speaker presentations are available at http://www.opengroup.org/jericho/presentations.htm .

The conference attracted much interest and coverage in the US press, including in Network World: http://www.networkworld.com/news/2007/091207-jericho.html?page=1
and many mentions by US-based bloggers, including the following 2 insightful reactions:
http://securityincite.com/blog/mike-rothman/the-daily-incite-september-17-2007
Rational Security - http://rationalsecurity.typepad.com/blog/

After the **Welcome and Introduction,** Bill Cheswick (Lead Member of Technical Staff, AT&T Research) gave the opening Keynote presentation - **40 Years of Internet Security and the Future for Firewalls**. This was particularly apt coming from Ches, who has been widely recognized as the "father of the firewall". Ches acknowledged it is possible at times to go "Internet skinny-dipping"—using the Internet securely without a firewall and even antivirus defense; the dangers of intrusion are going to be there, and you're giving up a layer of security, but it is possible to plunge into the Internet without perimeter defense. Skinny-dipping has worked for him. However placing sandbox defenses around services is key here. For businesses today, the limitation in foregoing perimeter defense is that you will not stop a DDoS attack, so you still need a walled garden. Ches considered one of the best approaches for the future of security is in the realm of virtualization software - virtualization allows building of a machine with a very robust sandbox.

Paul Simmonds (Global Information Security Director, ICI, and Jericho Forum Board Member) followed with reminders on what the Jericho Forum truly represents. In his **Myths and Realities about De-Perimeterization** presentation, he corrected false representations that many have tried to sensationalize – in particular, the Jericho Forum does not recommend tearing down firewalls; it's message has always been to raise awareness that perimeter firewalls are no-where near as effective as they used to be, so we need to deploy additional network security measures which secure your network operations. Paul showed how business demands have driven IT connectivity requirements consistently, and predicted where it is taking us – to full de-perimeterized working … driven by business demands to lower costs, increase flexibility/agility, and deliver faster working. The Jericho Forum is showing how to approach these challenges

- by defining the principles (commandments) that secure solutions must satisfy,
- by describing a "Jericho Forum blueprint" in which de-perimeterization is the concept of architecting security for the extended business boundary,

©The Open Group, 2007

- by developing an architecture for a computer system that is designed to collaborate, or use services, from systems that are outside of your locus of control
- by publishing Position Papers which highlight key issues arising from the effects of de-perimeterization.

Steve Roop (VP Products & Marketing, Vontu - replacing Joseph Ansanelli, CEO of Vontu who was indisposed) discussed **Security for a Wide Open World**, emphasized that the value is your "data", so you need to take effective measures to prevent data loss. This must involve deploying a data-centric policy that is content-aware, so that increasing security attaches to increasingly confidential business data, both in detecting it and in protecting it from loss/leakage – at rest, in motion, and at the endpoint. Steve presented his data-centric security "commandments", and noted the question we should keep asking ourselves in the context of data loss prevention is "Do you know where your data is?"

Dan Blum (Senior VP & Principal Analyst, Burton Group) shared his thoughts on **Rethinking Security Architecture in Light of De-perimeterization.** Dan recognized that enterprise security architecture must change to shift many controls from the network to the endpoints, data centers, information repositories and applications, and that clear issues, architecture targets, and challenges, are coming up over the next 2-3 years – a major one being "What's the future for the Network's role in delivering security?" He characterized the choices as between an Overlay Model and a Network perimeter Model, and discussed the architecture vision and challenges in each model. Looking to the future he sees:

- Application front end networks
- Endpoint security in silicon
- Network access or admission control (NAC)
- Virtual desktops and sandboxes
- Improved identity assurance
- Federation
- Web services / SOA security

and he recommended we

- Assume that both perimeter and overlay models will be needed in many cases and must co-exist
- Work towards securing endpoints
- Set up new boundaries and control points at the data center edge
- Segregate critical systems into secure subzones within larger data centers
- Focus on policy, accountability and awareness – it's not just a technology problem!

Carl Ellison, Architect, Microsoft) considered the **Security Architecture Implications of De-Perimeterization** – what are our target infrastructure designs and what are the steps we can take today to get there. Carl acknowledged the problems of what he termed "isolation boundaries" that no longer offer adequate security since many companies today have to open up network holes in them in order to conduct business. We've been tunnelling everything over Port 80 because that one is open in the firewall. The network perimeter is gone, despite the dream that some people want to hang on to that it's not gone, though Carl refers the term "re-perimeterization". He shared Ches's enjoyment in "skinny-dipping" in the Internet since Windows SP2 was installed, and now with Vista. He explained that he's confident because of the host firewall. But we still have to open it up

©The Open Group, 2007

for e-mail, the Web and file-sharing. Microsoft servers today can raw an isolation boundary around the activity, by using Microsoft's "Server and Domain Isolation" technology. Based on IPSec authentication, this technology allows network managers to issue a certificate permitting them to join domains based on security policies and Active Directory groups. Carl explained that what's admitted into the isolation boundary doesn't have to be a machine belonging only to his company; we can divide machines into multiple addressable things that can join different domains, with firewall policies for these domains, though managing all of the IPSec connections in this envisioned environment is a challenge which needs further development work. Carl also shared Ches's view that one of the best approached to deliver the kind of de-perimeterized security the Jericho Forum advocates may lie with virtualization. Microsoft intends to have a virtual-server product out by mid-2008.

David Ting (Founder & CTO, Imprivata) gave a presentation on **Security Convergence – Myth to Reality**. He surveyed the many data protection regulations and mandates applicable in several countries and regions of the world, and noted that despite these we still suffer severe security breaches, incurring substantial costs – to reputation as well as financial. He referred to Carnegie Mellon University's Computer Emergency Response Team (CERT) on their findings and advice. His "security convergence" approach is perceived as having many definitions – including for identities, workflows, credentials, devices – and of course we are familiar with identity being linked with the role or context in which the identity (person or machine) is acting. Determining identity involves validating the identity's identifiers, confirming the location of the identity, and enforcing access policy, then auditing (track, trace, report). He then built up in successive slides his concept of identity convergence, summarized the security requirements involved, and demonstrated their validity by mapping them onto the CERT Common Sense guidelines.

Nishant Kaushik (Principal Architect, Identity Management, Oracle) explained their approach to **Understanding Identity as a Service** (IDaaS). The concept is that by externalizing identity as a standards-based service for business applications, we can devolve all application identity requirements into a common enterprise layer, so that as organizations move towards Service Oriented Architectures (SOA), identity components and management capabilities are made available as a service in that architecture. In this way, IDaaS will provide identity in a consistent, reusable way to all applications/services. Nishant demonstrated the validity of this approach by examining how each layer in his IDaaS structure – comprising identity provider, authentication, role provider, authorization, provisioning, audit – successfully handles the requirements. He then checked how IDaaS meets the requirements as presented in the Jericho Forum's Spring 2007 Conference. While there is much still to do to bring IDaaS to market, the concept is proven, and it supports a de-perimeterized environment. Nishant invited follow-up through his Oracle blog at http://www.talkingidentity.com. He closed with an interesting slide proposing steps towards measuring your Identity Management maturity, in 3 levels: tactical (low); process-centric (medium); aligned (high).

Jeffrey Wheatman (Research Director, Security & Privacy, Gartner Group) gave his view on **Best Practices in Security Architecture**. He acknowledged we must keep up with changing business environments requiring new thinking on how best to secure them – de-militarized zone (DMZ) boundaries are embattled by today's environment involving complex applications, increasing regulations, increased connection methods, the need to protect assets (including from the internal network), mobility of endpoints, data center protection, virtualization, and more. He asserted there will always be a perimeter - it's a matter of moving it to the right place for each component in the

©The Open Group, 2007

system, and adopting a coordinated safeguard approach rather than a single safeguard. In a world where systems have 2,000 rules in their firewalls, adding more rules in response to respond to new business problems becomes unmanageable. The Jericho Forum doesn't say the perimeter is going away; the edge will change, but it won't go away. While the road ahead isn't necessarily clear, technologies such as virtualization may end up making a difference for security. Jeffrey considered embedding network security in endpoints, IPS (primarily at the edge and in blocking mode), having a separate security control plane from the system infrastructure, Web application firewalls, and content monitoring and filtering for data loss prevention (mirroring Vontu's earlier consideration of data at rest, in motion, and at the endpoint. New threats and technology will continue to emerge, and there is still much room for innovation. Network and host security will have to communicate but they are unlikely to become one and the same. He viewed encryption of MPLS and internal links as likely to remain niche, with Quantum cryptography remaining niche until at least 2011. His conclusions looking ahead were:

- Maintain your separate network security control plane — but take advantage of embedded network security capabilities where possible
- Move beyond just default IPS blocking - integrate endpoint intelligence and network behavior analysis (NBA), try out innovative new solutions, including content-aware security (CMF/DLP)
- Maintain awareness of where and how emerging point products are converging

In the closing **Panel Q&A Session**, Paul Simmonds repeated that the Jericho Forum has never said we didn't want any firewalls; we're simply saying, understand why you're using a firewall and its limitations. In fact, you might end up using more firewalls if it reduces your attack surface. However, in a large corporate network, the network firewall today works more as a quality-of-service boundary than as a security service. He added that de-perimeterization for most corporations is a fact of life. It's happening whether you realize it or not. There is today a mismatch of the legal business border, the physical border and the network perimeter. As an example, he noted that for his company to do business with Wal-Mart, Wal-Mart insist that ICI establishes a direct connection between the ICI and Wal-Mart enterprise-resource planning (ERP) systems, so they can place orders and ICI can sell paint. This business partnering situation is increasingly the norm, leaving the firewall as a perimeter full of holes. John Meakin (Group Head of Information Security at Standard Chartered Bank, and a Jericho Forum Board member), added that the goal is to find a security model that best fits your business, and the Jericho Forum is trying to find a more balanced mix of security solutions that thinks beyond viewing the network firewall as sufficient.

Published by The Open Group, Thames Tower, Station Road, Reading, RG1 1LX, UK
©The Open Group, 2007