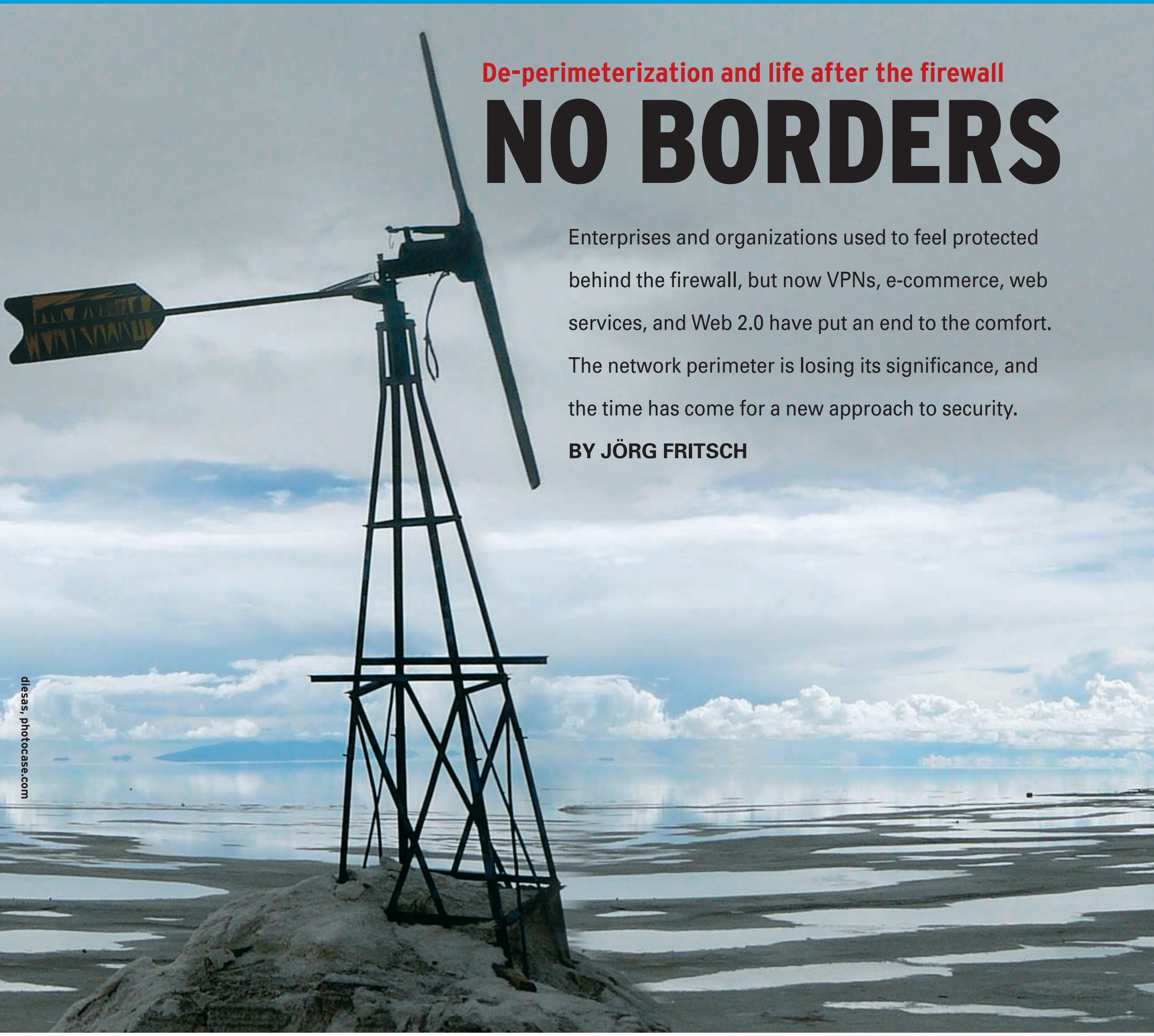

diesas, photocase.com

De-perimeterization and life after the firewall

NO BORDERS

Enterprises and organizations used to feel protected behind the firewall, but now VPNs, e-commerce, web services, and Web 2.0 have put an end to the comfort. The network perimeter is losing its significance, and the time has come for a new approach to security.

BY JÖRG FRITSCH

Firewalls used to be the pride of any security department. A well-designed firewall protected the internal network, and a lot of ports needed to be open on the firewall. Servers advertised their services to anyone on the LAN.

This black and white view of the secure internal network and the evil external network was never really as simple as it looked – identity thieves and disgruntled colleagues have always been a part of the corporate scene – still, the system seemed to work somehow. Without firewalls, the current conception of the Internet – with online shopping, home banking, and VPNs – would be totally unthinkable.

On today's networks, security specialists have a difficult time enforcing the traditional segregation of "inside" and "outside." New borders are opening up all over the place. Remote access via VPN, cellphones, PDAs, roaming notebooks, web services, and Web 2.0 technologies are slowly rendering the firewall obsolete. In the past, each server application had a clearly defined port and was easily controlled at the firewall, but almost all services in today's web service model use http/https and port 80 or 443. This emphasis on http makes it difficult to disambiguate services at the network perimeter.

Although this problem sounds like a serious threat, some experts believe this paradigm shift is an opportunity. Instead of repeating past errors by refining and extending the outdated firewall concept, why not devise a whole new approach to security that is tailored to the more complex reality of today's networks?

The Jericho Forum [1] is an international security organization dedicated to advancing a new vision for network security. At the center of that vision is a concept they call *de-perimeterization*, which overturns the traditional view of the network as a finite space with an inside, an outside, and a perimeter. According to the Jericho Forum, the threats faced by today's networks are so vast and varied that "…The only reliable security strategy is to protect the informa-

tion itself, rather than the network and the rest of the IT infrastructure."

The Jericho Forum is a loose grouping of ISM (Information Security Management) experts affiliated with the Open Group [2], an umbrella organization comprising the joint forces of the Open Software Foundation [3] and X/Open Limited. Open Group is well known for its Single Unix Specification and other initiatives.

The Open Group trademarked the term "Boundaryless Information Flow" to echo this theme that modern networks should not depend on perimeter boundaries for protection. (According to unofficial sources, the trademark was necessary to avoid vendors misusing the term for advertising purposes without actually adhering to the principles.)

This vision of a secure network without borders is embodied in the Jericho Forum's "Commandments," which are available in PDF form from the Jericho Forum web page (see the box titled "Commandments").

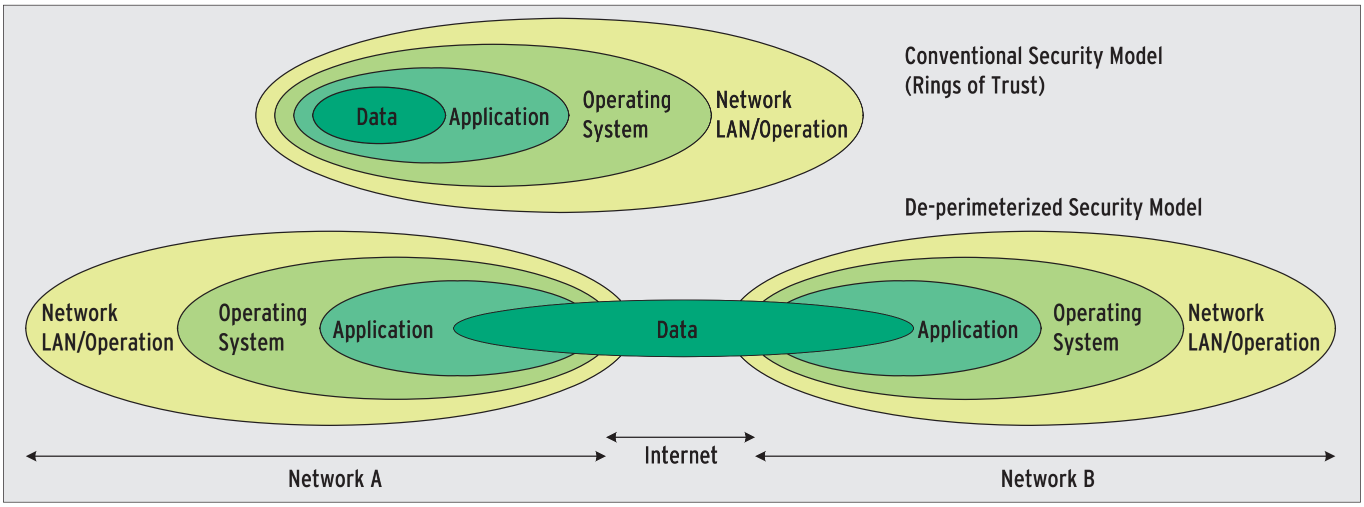

Figure 1: Conventional security models attempt to safeguard components from each other. The traditional "Rings of Trust" model (above) hardens each ring against the surrounding ring. The de-perimeterization model, below, assumes data is independent of context and must not depend on an application, operating system, or network for protection.

The commandments are a collection of security principles – some equivalent to contemporary "best practices" advice and others quite radical and new. The work of the Forum boils down to an emphasis on four areas: encryption; secure protocols – above all, SSL/TLS; secure systems; and authentication and authorization at the data level

The concept of protecting the data itself, rather than simply restricting access to the machine that holds the data, is a fundamental feature of this new approach. Another tenet of this de-perimeterized reality is that *all* networks are untrusted. Each device must be capable of defending itself – even when placed on the open Internet.

Figure 1 sketches this new vision of the data-independent network. At the top, you can see legacy data and information with clearly defined perimeters. The Rings of Trust model is designed to support communication from the secure side (i.e., the side closer to the core) to the insecure side. At the bottom of the image is the new model. Data exists independently of network boundaries and must not rely on any application, computer, or network for security.

In a perfect world, information would possess attributes to make sure that viewing or modifying data was restricted to authorized persons only. Data would be useless in the wrong hands. This approach, often referred to as Information Rights Management, IRM [4], entails more than just encrypting the data.

At present, many manufacturers are working on frameworks that support authentication and authorization directly at the data level – Oracle, EMC/RSA, and Microsoft DRM to name just a few. Some solutions are already available in part, although they are frequently tied in too closely to the DRM model. Thus far, it is hard to say which technology will assert itself. Standalone solutions are pointless; after all, de-perimeterization aims to facilitate the flow of information.

Some critical elements required to implement the vision of the perimeterless network are still missing – first and foremost, secure terminal devices. Although Linux has an excellent reputation in this respect, it is still too vulnerable.

The inherently secure systems that de-perimeterization relies on should not

The Jericho Forum is an international IT security thought-leadership group dedicated to defining ways to deliver effective IT security solutions that will match the increasing business demands for secure IT operations in our open, Internet-driven, globally networked world. Our members include multi-national corporate user organizations, major security vendors, solutions providers, and academics, working together to:

- drive and influence development of new architectures, inter-workable technology solutions, and implementation approaches, for securing our de-perimeterizing world
- support development of open standards that will underpin these technology solutions.

Click on a link in the left column to go directly to a topic you're specifically interest in.

Jericho Forum 2008 Spring Conference

Olympia, London, Tuesday April 22nd

Register here

Next Members Meeting

Friday, February 29, 2008

See details

De-perimeterization explained

The huge explosion in business use of the Web protocols means that:

- today the traditional "firewalled" approach to securing a network boundary is at best flawed, and at worst ineffective. Examples include:
  - business demands that tunnel through perimeters or bypass them altogether
  - IT products that cross the boundary, encapsulating

Scripts Currently Forbidden | <SCRIPT>: 6 | <OBJECT>: 0

Figure 2: The Jericho Forum advocates policies, practices, services, and standards for a de-perimeterized Internet.

INFO

[1] Jericho Forum: *http://www.jerichoforum.org*

[2] Open Group: *http://www.opengroup.org*

[3] Open Software Foundation: *http://en.wikipedia.org/wiki/Open_Software_Foundation*

[4] Oracle Information Rights Management: *http://www.oracle.com/technology/products/content-management/irm/*

be vulnerable to hijacking attacks on account of a minor programming error. And there is much to do on the application front. Web browsers in particular are continually in the news with critical security holes.

If you are a road warrior who works with a portable computer in hotel rooms, on customer premises, or at conferences, you know that today's Internet is not far removed from the ideal of de-perimeterization. But danger lurks around every corner, whether from laptop theft or a carefully crafted attack on a protocol, application, or system. Let's hope that de-perimeterization will give us better protection than today's assortment of firewalls, virus scanners, and VPNs. ■

Commandments

The Jericho Forum's vision for de-perimeterization is embodied in a document known as the Jericho Forum Commandments, which is available through the Jericho Forum page (Figure 2) of the Open Group website [1]. The 11 commandments of the Jericho Forum are:

Fundamentals

1. The scope and level of protection should 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.

Surviving in a Hostile World

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.

The Need to Trust

6. All people, processes, and technology must have declared and transparent levels of trust for any transaction to take place.

- Trust in this context is establishing an understanding between contracting parties to conduct a transaction and defining the obligations of each party.
- Trust models must encompass people/organizations and devices/infrastructure.
- Trust level may vary by location, transaction type, user role, and transaction risk.

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 authorization frameworks must support the trust model.

Identity, Management, and Federation

8. Authentication, authorization, and accountability must interoperate/exchange outside of your locus/area of control.

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

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.

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.

11. By default, data must be appropriately secured when stored, in transit, and in use.

- 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.