RETHINKING DE-PERIMETERISATION:
PROBLEM ANALYSIS AND SOLUTIONS

André van Cleeff, Roel Wieringa
University of Twente
Drienerlolaan 5 7522 NB Enschede The Netherlands

ABSTRACT
For businesses, the traditional security approach is the hard-shell model: an organisation secures all its assets using a fixed security border, trusting the inside, and distrusting the outside. However, as technologies and business processes change, this model loses its attractiveness. In a networked world, “inside” and “outside” can no longer be clearly distinguished. The Jericho Forum - an industry consortium part of the Open Group – coined this process de-perimeterisation and suggested an approach aimed at securing data rather than complete systems and infrastructures. We do not question the reality of de-perimeterisation; however, we believe that the existing analysis of the exact problem, as well as the usefulness of the proposed solutions have fallen short: first, there is no linear process of blurring boundaries, in which security mechanisms are placed at lower and lower levels, until they only surround data. To the contrary, we experience a cyclic process of connecting and disconnecting of systems. As conditions change, the basic trade-off between accountability and business opportunities is made (and should be made) every time again. Apart from that, data level security has several limitations to start with, and there is a big potential for solving security problems differently: by rearranging the responsibilities between businesses and individuals. The results of this analysis can be useful for security professionals who need to trade off different security mechanisms for their organisations and their information systems.

KEYWORDS
De-perimeterisation, security perimeters, Jericho Forum, data-centric security

1. INTRODUCTION

All need for security starts with the assumption that there is an asset that is potentially threatened by an “outside” influence. It needs to be protected. Because of this need, businesses define the policies that should be used to secure it and implement the necessary technical measures. However, such an approach is only possible if we can identify the asset, why we want to protect it and actually have the capabilities to do so. In a networked world, where systems are built on top of other systems, and interact with yet other ones, the precise asset can be hard to define, let alone secure through our own intervention. The Jericho Forum (2005) called the process of blurring boundaries de-perimeterisation and it poses significant security challenges to security professionals, whether they are designing or managing information systems. Solving the security problems caused by de-perimeterisation is hard, because new technologies are constantly being introduced that further blur the IT security landscape. Currently, mobile internet is becoming mainstream, and so is virtualisation - on the horizon cloud computing is already looming.

In order to effectively secure today’s information systems and build the next generation securely, we need to understand how de-perimeterisation occurs. To this end, we analyse the process. Our analysis shows that de-perimeterisation is not a cumulative process towards more connected systems. Instead, we observe a cyclic process in which the basic trade-off between accountability and business opportunities are balanced based on risk assessments. In this process, there is no end result, where security mechanisms are mostly oriented at the data level as suggested. Data level security can indeed be beneficial, but also has limitations, which we discuss, and needs to be complemented by other technical mechanisms. After this analysis, in the final section, we then discuss alternative organisational mechanisms for balancing security with business opportunities.


2. DE-PERIMETERISATION

According to the Jericho Forum, de-perimeterisation occurs when an organisation does not own or control its IT infrastructure or is not accountable for it, or when individuals are employed by more than one organisation. To this definition we want to add that de-perimeterisation also implies increased, flexible and often unknown connectivity between systems. This leads us to formulate three essential elements of de-perimeterisation:

- It involves different legal entities
- It involves the creation of new connections between systems
- These connections are undocumented or unknown

De-perimeterisation threatens organisations in several ways. First, dependencies are obscured: in a networked world, it is not hard to create very complex systems of systems, which work flawlessly for some time. However, these systems have structural dependencies that only become apparent when something goes wrong. For example, in 2007, the Internet phone service Skype went offline for some time after a massive reboot of Windows machines, following an update (Saran 2007). Obviously, Skype was dependent on the patching process of Windows, but this was unknown before the event. As de-perimeterisation continues, such events can become more likely.

Second, risk assessment becomes harder: existing methodologies, such as the Common Criteria (2006) use protection profiles for specifying security requirements, as well as the concept of target of evaluation, for the system for which the risk assessment is done. In many situations, networks of systems cannot be clearly defined - we might have some security requirements but we lack information about what kind of systems we are dependent upon. Thus, it is very difficult to do any kind of risk assessment when the boundaries between systems are blurred.

Figure 1: trends according to the Jericho Forum.

Figure 1 shows the Jericho Forum’s view of the historical development of de-perimeterisation (Jericho Forum 2007b, p.1). According to this model, the trend is toward more connectivity. However, we argue that the real trend is closer to an oscillation than to a straight line. If we examine the rise of the Internet, we can indeed find that once isolated systems of universities and businesses were connected. But this brought along security problems, and the networks were partly disconnected using firewalls. Over time, the internal organisational networks grew until they were too big to be secure: they had to be compartmentalised again. Finally, new technologies such as mobile devices and the service-oriented-architecture lead to new
connections, and we can expect new security perimeters to be established for these in the future. This version of events is depicted in figure 2.

Figure 2: alternative view.

The oscillation is due to the interplay of two sets of opposing forces, one in the direction of connectivity (de-perimeterisation), and one in the direction of (re)-perimeterisation. The forces in the direction of connectivity include the desire for cost reduction, flexibility and speed of business, facilitated by technological developments. Enterprises see the advantages of e-business and open up their networks. Universities want to develop and utilise the new infrastructures for their own research. For many new technologies, their impact on security is not clear. Parties that are not aware of this, or do not consider it a problem (such as consumers), will take the risk and adopt the technologies. Thus, there is no incentive to invest early on in security features.

Once technologies become mainstream, different forces come into play, leading to re-perimeterisation. Vulnerabilities will be found, and potential users will demand security features to be fitted to the new technology, before integrating it in their systems. Additional forces include the need for accountability, proper allocation of benefits in a business network, privacy, safety and reliability and company confidentiality. Our prediction is that this oscillatory trend, rather than the linear Jericho trend, will continue because none of these forces in play will go away.

3. DATA-CENTRIC DE-PERIMETERISATION

We will now discuss the applicability of data-centric security, and point out alternative approaches.

3.1 Review and critique

The Jericho forum has proposed to go with the flow of de-perimeterisation by placing a perimeter around the data, rather than around the entire infrastructure of the organisation (Palmer 2005, Jericho Forum 2007a). Several technical mechanisms are proposed in two key articles by Agrawal et al. (2002) and Grandison et al. (2007). There are several arguments for implementing security on the data itself. As stated by Grandison et al., security must be data-centric because only the data has real business value: the network of an organisation is of no serious concern if there is no sensitive data on it. A firewall is unnecessary if there is no risk of a security breach.
Secondly, it does not make sense to have a security perimeter include more than is strictly necessary. In general, perimeters do not scale: if a system grows, the difference in security levels between the inside and the outside diminishes: on a network of 10 servers all of them could possibly be trusted, but this is not the case if the network is expanded to include a thousand servers.

A third argument is about business opportunities. The Jericho Forum (2005) argued that organisation-level security perimeters actually hinder business rather than facilitate it. To enable cooperation with other organisations it makes sense to facilitate access to IT assets at the lowest possible level, and use these assets as building blocks for new business constellations. Whether this is a good strategy depends on the potential risk versus the reward and should be subjected to a risk assessment.

Fourthly, there are many situations in which organisations change shape, whereas the data will remain relatively stable. For example, a hospital might be reorganised and restructured many times, whereas the patients and their data will remain fixed. Putting security policies as the data level can be a form of future-proofing security. Wherever the data will be in the future - it will be known how it should be secured.

We identified several key forms of data-level security, which are listed below:

- **Data level security – database-centric**
  The illustrative example here is the Hippocratic database (Agrawal, Kiernan, Srikant & Xu 2002), which takes its name from the Hippocratic oath that doctors must take to protect their patients and keep their information confidential. Ideally a database should adhere to the same principles. On top of it, other applications can be built.

- **Data level security - sticky policies**
  In contrast to the Hippocratic databases, where the data is stored centrally, we can associated a data item with “sticky policies” (Bandhakavi, Zhang & Winslett 2006) that cannot be separated from the data, no matter where it goes. DRM technology can be considered an example of this scheme. Sticky policies usually require a trusted environment in which the data can flow; in the case of DRM this can be special hardware that prevents copying.

- **Data level security – encryption**
  Another approach is to encrypt data inside the database such that it cannot be read or modified by unauthorised parties. This is actually one of the requirements of the PCI standard (2006, p.5) for credit card numbers. Users that need access to the data need a key to decrypt it. Some systems also make it possible to search through the data but these functions are usually limited. Encryption can also be combined with sticky policies: data can only be decrypted by those parties for which the appropriate access rights have been set in a policy (Cf. Cheung and Newport, 2007).

Generally, there are three main issues with data-level security:

1. **Integrity and accountability checks at the organisational level remain necessary**
   Support for security attributes such as integrity often requires perimeters around larger structures then data, sometimes even at the organisational level. As a practical example, consider the security system for a banking application: first, observe that data integrity cannot be determined at the level of individual bank accounts: if a sum of money is transferred, integrity is at least determined at the level of those accounts involved: the total amount of money before and after the transactions should be the same. In fact the expected level will be higher because we also must consider the interest that is generated by the two accounts and the time it takes to transfer the money between the two accounts. Finally, it is the bank that is accredited for performing financial transactions and it will be tempted to prove its security at the organisation level. For legal reasons alone, we need to know what is inside and what is outside of the organisation. This is an “undocumented” but essential function of the security perimeter.

2. **The security of data itself cannot be assessed at face value**
   Data is always generated by applications and by users, whose interactions can be very complex. If we can only study the end result, we cannot assess how secure it is. We need to understand the computational and business processes that resulted in the data creation.

3. **Data needs to be exchanged with other systems**
   Even if we can store data securely in a Hippocratic database, we will still need to export it at some time: in a networked world, communication of data with other organisations and individuals is a necessity. However, assessing the security of the other parties is beyond the capabilities of any database. Thus the problem of maintaining a secure data exchange cannot be addressed at the data level.
3.2 Alternatives

To place the usefulness of data centric security in context, and point out other approaches, we will now discuss several alternatives for data centric security mechanisms.

Network perimeters

Network or firewall security allows us to limit data flow between different systems, by inspecting and filtering the traffic that goes between them. There are two typical scenarios: in the first, we need to protect an asset against outside influences, in the second case, we want to prevent information from leaking into the environment. The Jericho Forum (2005) has argued for their abolition, claiming that they hinder business rather than support it. A general requirement for such forms of security is that the network infrastructure must be under control of the organisation.

Endpoint perimeters

Endpoint security dictates that all communication between nodes (endpoints) must be secured and that each node must be responsible for maintaining its own security. Policies for endpoints can be centrally managed. Forms of endpoint security are server and client firewalls, anti-virus software on client PCs, VPN and SSL/TLS connections. In the case when the network infrastructure is fragmented and communications between nodes are ad-hoc, endpoint security limits the security implications: the network (apart from reliability) does not have to be secured anymore.

Ideally, each endpoint is a very simple system which is easy to secure. Unfortunately, for an end-user, an endpoint normally means a PC, which is so complicated that it is not reasonable to assume its security in many cases. It is also a single point of failure - once an endpoint is hacked, the security of the entire communication is breached.

Multi-layer perimeters

Some have argued that security can only be achieved by partitioning systems into different zones, each having different security levels, allowing for a defence-in-depth. Typically, the inner-most part is the best secured part. In situations where services are outsourced, this model can be extended (Walker 2005) to include an extended security perimeter. The reason for using multi-layer security is that there are distinct parts of a system or organisation that need to be better secured than others; while the parts that surround it are also under the control of the organisation. As such, it allows for defence-in-depth. The drawback of multi-layered solutions is that they can become very complicated, especially when a layer has to be partitioned itself, for example because each business partner requires its own environment.

Internet perimeter security

A more radical (and currently only hypothetical) approach is to put a perimeter around the entire Internet. Such an approach is foreseen by Lessig (2006). “Ideally”, Internet access is restricted to those systems and individuals that have identified themselves properly. There have been a number of initiatives that would support such an architecture but so far, attempts to create even limited forms of identity layers (for example Microsoft Passport (Microsoft 2008b)) have failed. With a functioning identity layer, trust becomes easier to organise, as organisations do not have to build the trust network themselves. The drawbacks are also clear: the entire infrastructure of the Internet would need to be changed, and privacy would be lost if everyone and every device is identified.

4. ORGANISATIONAL RE-PERIMETERISATION

In the previous section, we discussed technical solutions, their applications and limitations. These are not the only mechanisms for re-perimeterisation: because de-perimeterisation is a phenomenon that involves blurring the boundaries between organisations, the solutions can also involve the restructuring of the perimeters between organisations, and between organisations and individuals.
4.1 Organisational re-perimeterisation

With organisation re-perimeterisation, we try to partly undo some of the causes of de-perimeterisation. For example, when the management of applications was outsourced, it can be insourced again, and placed under control of the organisation.

The main advantage of this approach is that it reduces the amount of legal parties involved. This perimeter type is typically used in financial institutions and governments. An important motivation for this approach is that certain risks are simply unacceptable and must always be treated, and cost is less of an issue. Organisational perimiterisation can be done on the condition that the organisation has control over its network and has the available expertise to maintain it.

The biggest problems with this solution can be cost and lost business opportunities: it can be very difficult to manage applications properly; it required highly trained and expensive personnel.

4.2 Individual perimeters

An alternative to organisation level security is to make every individual responsible for keeping himself and his own devices secure (Cf. Hartel 2006). Generally, a system uses individual-centric security if the burden of maintaining security is put down on individual users. It can be argued that the only reason for centralised administrative control is when ownership does not coincide with individuals. If a person works on his own laptop on his own project, on his own document, in his own free time, there is a perfect match and no organisational security perimeter is needed: it would only complicate the situation.

An example of individual-centric security is the usage of individual laptops and mobile phones: rather than having a uniform set of desktops in place, where everyone can login at any PC, organisations are now shifting towards a concept where users all have their own laptop. Some systems that store medical information also use individual-centric solutions, for example Microsoft Healthvault (Microsoft 2008a) or Google Health (Google 2008). Here individuals can manage their own medical information and decide themselves who will get access to these records (for example which doctor or which family member).

The concept is not always applicable, for example when someone is assembling cars on a conveyor belt, or is doing a bank transaction for a company as an employee. Organisations are a natural way to structure economic activity (Cf. Coase 1937). It is impossible to think of building a passenger aeroplane alone. In such cases, individual centric security is at odds with organisational alignment.

A specific disadvantage is that individual centric security has a tendency to mutate into other forms of security: in the healthcare domain for example, a medical file could be controlled by one patient, but he still has to give some authorisations to a hospital, because he cannot authorise all nurses individually. On social network sites, “organisational accounts” appear. For example, Warner Bros, a multi-billion dollar company, has its own user account on YouTube called “warnerbrosrecords”. This leads to the conceptual problem of which employee (or employees) of Warner Bros has access to this accounts, and whether user rights are managed by either Warner Bros or by YouTube. Another issue is that users can be incapable of securing their systems. It is already hard for a healthy individual to maintain her own laptop, install patches and configure the firewall, but it is even harder for a sick person to manage the authorisations to his medical file.

4.3 Virtual organisation perimeters

Concerning organisational perimeters, we can also create new structures, or so called virtual organisations (Mowshowitz 1997) between organisations, effectively reducing the amount of connections between different legal entities. Virtual organisation are extensively used in grid computing, where separate institutions use resources from yet other organisations or even individuals. By combining the institutions into one virtual organisation, the resource owners only need to deal with one entity. Another typical case is in outsourcing relations, where a separate unit is created to monitor a service-level agreement. On the downside, virtual organisations require trust in the other parties and a virtual organisation is still yet another organisation, and can thus also introduce new complexity, because employees become a member of two organisations rather than just one.
4.4 Federated perimeters

Another solution direction is to use federated systems (Gebel 2005). If security cannot be addressed on the organisational level, it could be implemented at the inter-organisational level, by putting a security perimeter around multiple organisations. In a federated solution, several organisations agree to use a shared security solution, the features of which can be used by all participating organisations.

Federated systems can especially help with identification and authorisation. If someone is identified at one organisation, he can use his credentials at another organisation. Just as with virtual organisations, the advantage of federated security is that the amount of connections between organisations can be reduced drastically. An example of a solution that supports federation is Microsoft’s Active Directory where management domains can exchange identify information. For federations to work, multiple organisations must come to some form of agreement and sometimes legal problems prevent information sharing.

5. CONCLUSION

We have defined the concept of de-perimeterisation and argued that it is not a steady process, but a cyclic one. In one cycle, different forces accelerate de-perimeterisation, after which other forces slow it down, leading to re-perimeterisation. There are basically two methods for “re-perimeterisation”:

1. We can put technical security perimeters around different parts of IT: for example around data, around endpoints or try to use a multi-layered approach.
2. We can re-arrange legal constructions: organisations can grab control of their own infrastructure, shift the responsibilities towards individuals, create new organisations or cooperate with existing entities.

Each of these perimeters has its own advantages and disadvantages, which are outlined in figure 3. Together, the options provide a framework that IT and business architects can use for developing secure, re-perimeterised solutions, which can survive in today’s networked world.

<table>
<thead>
<tr>
<th>Approach</th>
<th>Re-perimeterisation mechanism</th>
<th>Pre-Conditions</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technical</td>
<td>Data - database-centric perimeter</td>
<td>Communication less important than storage</td>
<td>Mostly useful for confidentiality</td>
</tr>
<tr>
<td></td>
<td>Data - sticky policies perimeter</td>
<td>Environment is trusted</td>
<td>Mostly useful for confidentiality</td>
</tr>
<tr>
<td></td>
<td>Data - encryption perimeter</td>
<td>Processing is less important than storage</td>
<td>Mostly useful for confidentiality</td>
</tr>
<tr>
<td></td>
<td>Endpoint perimeter</td>
<td>Endpoints can be secured</td>
<td>Introduces single point of failure</td>
</tr>
<tr>
<td></td>
<td>Multi-layer perimeter</td>
<td>Ability to manage complexity</td>
<td>Increases complexity</td>
</tr>
<tr>
<td></td>
<td>Internet perimeter</td>
<td>Privacy and legal problems are solved</td>
<td>Privacy is reduced</td>
</tr>
<tr>
<td>Organisational</td>
<td>Organisation perimeter</td>
<td>Expertise, control must be available</td>
<td>Lost business opportunities</td>
</tr>
<tr>
<td></td>
<td>Individual perimeter</td>
<td>Control and ownership rest by the individual, expertise</td>
<td>Leads to complex workarounds</td>
</tr>
<tr>
<td></td>
<td>Virtual organisation perimeter</td>
<td>Cooperation and trust are possible</td>
<td>Introduces new complexity</td>
</tr>
<tr>
<td></td>
<td>Federation perimeter</td>
<td>Cooperation and trust are possible</td>
<td>Results in loss of control</td>
</tr>
<tr>
<td></td>
<td>Network perimeter</td>
<td>Network and protocols must be controllable</td>
<td>Increases cost</td>
</tr>
</tbody>
</table>

In the future, we would like to develop a more formal model of de-perimeterisation, which combines the technical and organizational perspectives. We also intend to link it to identity: one of the recurring problems
in de-perimeterisation is identification. When organisations are cooperating, they lack context information and need to know with whom and with which IT systems they are dealing. This problem is also related to the emerging discipline of context-aware security (Cf. Neisse, Wegdam, and Van Sinderen, 2006).

ACKNOWLEDGEMENT

We thank Pieter Hartel, Pascal van Eck, Wolter Pieters and Trajce Dimkov for their help with the paper. This research is/was supported by the research program Sentinels (www.sentinels.nl). Sentinels is being financed by Technology Foundation STW, the Netherlands Organization for Scientific Research (NWO), and the Dutch Ministry of Economic Affairs under project number TIT.7628.

REFERENCES