March 2024

De-perimeterising Zero Trust

Challenging metaphors in information security

Dr Matt Spencer and Dr Daniele Pizio
Centre for Interdisciplinary Methodologies, University of Warwick

About this briefing

The 'Scaling Trust' research project at the University of Warwick examines how is trust understood in the cyber security profession. This brief is an opinion piece drawing on our work studying the emergence of *de-perimeterisation* in 2000s information security discourse, including the Jericho Forum pressure group and Zero Trust. This work was based on interviews, archival research and narrative analysis, and looked at how conceptual shifts in security thinking take place. We report on some high level findings of potential interest to policymakers, and make some suggestions about the future of the field.

Context

One of the most consequential shifts in security communication in recent years has been the obsolescence of the perimeter-based approach to securing organisations. Organisations increasingly turn to 'Zero Trust' models of information security, in which security is not associated with a defended boundary, but with fine grained controls around all devices and assets, always monitoring, always verifying and always poised to deny access. This shift in thinking and in technology has been an enabler for the transition to cloud services and hybrid workplaces and a foundation for business today.

There is, however, a danger associated with the metaphor of 'Zero Trust' and its technologies of monitoring, access control, identity management and encryption. Where security is understood as suspicious and mistrustful, this can present a barrier to security teams adopting more collaborative and creative modes of engagement with the rest of the organisation. It also presents an obstacle to security teams identifying circumstances where trusting relationships are valuable to the organisation and need to be protected. Indeed, instead of protecting such relationships, Zero Trust may undermine them by creating the conditions for suspicion and blame, dampening collaboration and reducing resilience.

Policy recommendations

- Information security architects should focus on defining the value being protected within an organisation and recognise that where business value is generated by interpersonal trust, or by inclusive and collaborative work environments, the role of security may be to promote trust rather than to eliminate it.
- Product vendors should avoid presenting Zero Trust as a generic destination for best practice information security.
- Policymakers should draft a framework of principles for inclusive security, to support organisations in communicating the value of what is being secured.
- Cyber security educators should consider exposing students to interdisciplinary approaches to trust, communication, and metaphor as part of their training.

Key findings

Zero trust models are increasingly prevalent and work on the basis of heavy surveillance within a company or organisation's digital domain. Such approaches are often a replacement for older 'perimeter-based' models that focus security controls on the organisation's boundary. Zero Trust is often communicated with an narrative that represents employees as potential threats to security, whether this be through intent, coercion or mistake. Furthermore, the central metaphor that characterises the 'doer' of security as, ideally, having 'zero' trust in agents on the network reinforces an adversarial relationship between security and other employees, creating the expectation that users are untrusted and potentially at fault.

Conceptual change in information security often involves telling stories about the past, based on core metaphors, in which some things are remembered, and other things are forgotten. In our research we note that early advocates of de-perimeterisation saw the analysis of business value to be fundamental to 'de-perimeterising' the field. Members of the Jericho Forum were inspired by examples of asset destruction (such as ink-staining technologies used to protect cash in ATMs), measures that make sense only when you understand that what the bank wishes to protect may not coincide with what a thief wishes to obtain. This focus on explicating value, however, became far less visible once the Zero Trust model took over the de-perimeterisation agenda.

The neglect of value in Zero Trust can be attributed to its focus on technical solutions, on particular products and architectures that enable devices and applications to operate securely in untrusted environments. Our tongue-in-cheek title *De-perimeterising Zero Trust* refers to the need to return to this focus on value. This would enable organisations to identify key dependencies on trust, and to take steps to avoid its erosion due to Zero Trust technologies and ways of thinking. The avoidance of incidents can depend on people's ability to talk openly, without fear of blame, about instances in which they are not able to follow official procedure. Maintaining high trust within teams with critical responsibilities can thus be a vital source of learning and organisational resilience.

Conclusion

Zero Trust has a constitutive blindspot: the model is unable to account for forms of value that emerge from interpersonal trust. Where organisational resilience relies on people identifying and communicating problems with work processes, imposing security controls based on suspicion and surveillance may destroy value rather than preserve it. Characterising the security team as trusting and collaborative, emphasising the presence rather than absence of trust, may be a superior strategy in such contexts.

One area with potential to help us move beyond Zero Trust is the field of cyber deception. Technologies of deception, such as honeypots and decoys, can be implemented at many levels, from data and files, to network infrastructure, from applications and devices to user accounts. By tailoring security measures around attackers' interests, a deception-based strategy may help reclaim the trust of ordinary users.

One way in which government can help is by drafting guidance for inclusive security. This could provide a shared language for organisations to talk about what value is being secured, and who is being protected. Inclusive security could enable better traceability between values, security requirements, and the security measures that implement them, while also providing richer idioms for security professionals to understand themselves, for instance as enablers and collaborators, rather than as untrusting gatekeepers.

Further information

https://warwick.ac.uk/fac/cross_fac/cim/research/scaling-trust

Spencer, M., & Pizio, D. (2023). The de-perimeterisation of information security: The Jericho Forum, zero trust, and narrativity. *Social Studies of Science*

Pizio, D., & Spencer, M. (forthcoming). What is a Security Model? Models of trust and trust in models in cyber security.

The views contained in this briefing do not necessarily reflect the views of the University of Warwick.