Joseph Tsai
CSS 517 Autumn 2020 – Research Paper

Security, trust, and privacy collide: An analysis of how Zero Trust Networks address Privacy by Design concerns

Abstract

This paper analyzes the usage of Zero Trust Networks (ZTN's) through the Privacy by Design (PbD) framework presented by Ann Cavoukian (Cavoukian, 2009). Each Privacy by Design tenet is evaluated against practical implementations and core components of a Zero Trust Network, ultimately allowing for discussion of how well a Zero Trust Network could fulfill the given tenet. Results of the research performed show that Zero Trust Networks are not inherently privacy-centric systems. While there are key components of a Zero Trust Network that can be leveraged to better meet Privacy by Design needs, ultimately, the level of privacy for any Zero Trust Network is determined by the level of privacy-focused investment given to the network.

1 Introduction

The concept of castles is one that dates back to medieval times. The corresponding model for trust when thinking of castles is relatively straightforward: So long as someone is allowed past the moat and into the castle walls, they are most likely a trusted individual. While this approach may have worked well in medieval times, such an approach could be seen as ineffective in the modern times of securing computer networks.

With such a security model, it is typical to view any device, application, or system in the network as trustworthy. However, recent research has shown that this implicit trust can be considered a vulnerability (Campbell, 2020). That is, security professionals can no longer trust the very devices on their network. It is in this realization that we see the rise of a new network security model: Zero Trust Networks (ZTN's).

In what would seem to be a parallel timeframe, multiple privacy regulations have come to fruition. Such regulations include: the California Consumer Privacy Act (CCPA), the European General Data Protection Regulation (GDPR), and the upcoming New York Privacy Act. With the ramifications for non-compliance directly impacting company financials, there has been a shift in ideology that privacy can no longer be a secondary thought for systems (Langheinrich, 2001).

The GDPR even requires that privacy be considered as part of system designs in order for companies to be compliant (Goddard, 2017). It could be argued that in order to effectively meet the needs of an organization, that security professionals and privacy professionals must collaborate to meet both security, privacy, and compliance needs. Hence, usage of a Zero Trust Network model presents an opportunity to better secure computer networks, while also providing leverageable mechanisms that can address privacy concerns.

2 Methods

This research paper explores the potential bridge between security and privacy in the Zero Trust Network (ZTN) model through analyzing each Privacy by Design (PbD) tenet as stated by the International Association of Privacy Professionals (IAPP) and looking at practical implementations of a ZTN for each PbD tenet. The section headings of the paper indicate each tenet and within each section, provide additional details on the given tenet. Each tenet was obtained through Ann Cavoukian's publication regarding the seven foundational principles for privacy by design (Cavoukian, 2009).

There is no single way to create the ideal and standard ZTN (Kindervag, 2010). However, there are practices that security professionals can apply which assist in the fulfillment of a network that embodies a ZTN. For purposes of this discussion, any component of a network that provides methods of least privilege access, analysis of each access request, or enforcement of operational policies (Rose et al., 2020) will be considered as potential pieces of a ZTN.

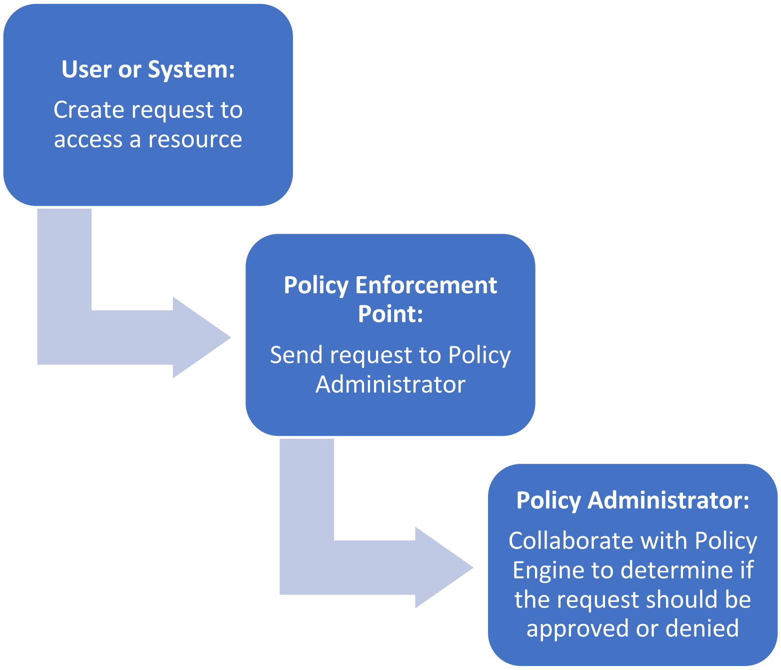
3 Discussion

3.1 PbD Tenet One: Proactive, Not Reactive; Preventative, Not Remedial

This first tenet states that privacy must be proactively considered and implemented throughout an organization rather than being an afterthought in order to be effective. With this shift to proactive measures, the first bridge into how a ZTN can address privacy concerns is established: A ZTN requires that the concept of a traditional network be fundamentally changed to a proactive security stance (Kindervag, 2010). Rather than construct a network where a perimeter is built and security is considered as a subsequent overlay, ZTN requires the engineers of the network to begin from secure principles and construct the network from this starting point.

One standard practice that displays how security is proactively built into a ZTN is through the usage of a Policy Enforcement Points, Policy Administrators, and Policy Engines (Rose et al., 2020). At a high level, all requests to systems within a ZTN must follow a process where each request is verified.

Figure 1: Potential process by which a request can be made and reviewed prior to being approved or denied in a ZTN.


User or System:
Create request to access a resource
Policy Enforcement Point:
Send request to Policy Administrator
Policy Administrator:
Collaborate with Policy Engine to determine if the request should be approved or denied

A ZTN proactively has security components as part of its design, as the structure for creating and establishing requests creates scenarios where access of least privilege is invoked. The question remains: How does this request structure address concerns for proactively considering privacy? It is here that another component of ZTN's gains relevance: Trust Engines.

A Trust Engine could be considered a component of ZTN that essentially calculates a trust factor for each request (Rose et al., 2020). Typically represented as a number, if a trust factor is within a given range of trust for a particular asset, then a request is approved. If not, then the request is denied. For purposes of discussion within this research, the Trust Engine was considered as part of the Policy Engine that assists with evaluating the approval of requests.

It is in the usage of a Trust Engine that proactive considerations of privacy can be analyzed. By having Trust Engines in place, there are components of privacy which can be considered within each request.

Consider the following scenario: A system which sends marketing emails to customers needs to obtain relevant email addresses. The request is made at the Policy Enforcement Point, and details such as the system's certificate, requested information, and operating system version are included. Taking these variables into account, one could view this request as having a rather high trust score. A ZTN could take this one step further with contextual analysis and verify this against the marketing system configuration to ensure that a reasonable number of records for customer emails are being requested, along with making sure that the email is being sent at the right time.

The hypothetical example provides two relevant insights: Least privileged access has been considered as a key component of the system through the usage of the Policy Engine, and privacy has been proactively considered through limitation of access to the system.

The topic of privacy itself has multiple facets, but one key component of privacy is the confidentiality of information which is being accessed (Rocha et al., 2011). As seen in the prior example, it is clear that with the usage of a limited access structure, that this component of privacy is inherently considered.

Altering the prior example, consider the case where a user makes the request instead of a system. Perhaps the Trust Engine could provide higher trust scores to those within the marketing department than those who were not, but would still mark user accounts as less trustworthy than systems for a given request. It could be that in such a Trust Engine, systems are typically expected to interact with the data directly through requests to the relevant systems. Such configuration of the Trust Engine allows for the proactive consideration of privacy through the limited access to data on systems within a ZTN.

Understandably, data access is not the only component of privacy that security and privacy teams must consider when constructing systems. These additional facets of privacy are considered and discussed within the subsequent tenets.

3.2 PbD Tenet Two: Privacy as Default

Privacy as default has a greater focus on understanding why information is being collected, how much information is being collected, as well as how long that information is retained for (Cavoukian, 2009). One relevant question that can be posed in relation to this tenet is: How does a ZTN analyze the information it is collecting for potential privacy concerns?

Frankly, the answer to this question is not straightforward due to this fact: The most effective ZTN's require usage of historical information for future contextual decision making (Lukaseder et al., 2020).

For example, consider the scenario where a user accesses a company's webpage. The user's browser sends a request to load the homepage for the company's website, which subsequently sends browser information to the Policy Administrator. This presents a decision point: the company can decide to store information about the request in such a way that the company would be able to create a linkage back to the specific user, or the company can choose to use the information to determine if the page should be loaded or not, and then subsequently delete the information originally sent in the request.

On one hand, there is most likely enough context in this case that the company can make a decision whether or not to trust the given connection. Perhaps approving the loading of the webpage is not harmful to the company in this given instance.

However, consider the case where a malicious actor has attempted to apply a Denial of Service (DoS) attack to the business. If no context for the requests to the company's webpage had been retained for the Trust Engine to leverage, then the DoS attack may ultimately be proven successful. It is the combination of real-time analysis of trust as well as comparisons to historical data that better informs the Policy Engine to ultimately decide to trust or deny a given connection.

However, the question still remains: Is a ZTN private by default? One facet of the answer seems to depend on how privacy is considered in the collection of information for a ZTN to leverage and is thus up to the given company. However, as explored in tenet one, there are components of a ZTN which can strengthen the confidentiality stance of a company to sensitive data.

3.3 PbD Tenet Three: Privacy Embedded into Design

This tenet has three main components: systematic approaches to privacy, detailed considerations of privacy risks, as well as minimization of privacy risks through proper technology architecture and usage (Cavoukian, 2009). There is a clear call to collaboration in this tenet between privacy professionals and technology professionals. That is not to say that there cannot be privacy professionals who are also technology professionals and vice versa, but this tenet focuses on the intersection of privacy risks with the design of the technical systems which need to handle identified privacy risks.

Again, this tenet reaches a similar conclusion to that of tenet two. A ZTN in itself does not immediately guarantee that privacy risks are considered, just as how a ZTN does not cover all security risks. The evaluation and degree to which privacy is included in the design of any given ZTN depends on the organization's investment and focus for how the network is designed. One company may put great emphasis on privacy and thus we may see that company have much more robust Policy and Trust Engines.

On the other hand, other businesses which may not retain sensitive information may choose to not consider privacy concerns to a high degree, yet they could be considered a safer company to work with due to their data retention practices. Hence, privacy embedded into design is comprised of the degree to which the given company requires of themselves, as well as what their risk appetite is. A ZTN alone does not provide a company with privacy considerations throughout its design just as much as security considerations are thought of throughout a network's design.

3.4 PbD Tenet Four: Full Functionality- Positive Sum and Not Zero Sum

Security and usability could be seen as residing within conflicting camps. That is, the more one gains, the more the other suffers (Kainda et al., 2010). The same situation arises when considering aspects of privacy. Some could believe that the less information a company can collect, the less functionality is available for a given user, and the more information a company collects, the better the experience is for the user. Is there a way that privacy concerns can be addressed in this situation?

Rather than dive into specific details regarding how ZTN's can accomplish this goal, the problem can be analyzed using a hypothetical approach. The question of exploration for this tenet is this: If a user has the exact same experience on a ZTN as well as a non-ZTN, then has this tenet been fulfilled?

For purposes of discussion, let it be established that the privacy of the data has already been considered. That is, all data required to run the full functionality of a given user experience is sanitized, collected, and obtained in a manner than users have actively agreed to.

On one hand, one could come to the realization that ZTN's are by definition not front-end tools (Kindervag, 2010). ZTN's are the networks that user experiences run on. So long as the customer is able to make the same requests and actions that they were able to perform on a non-ZTN network, the user experience can still be considered as having full functionality with a secure experience.

For example, consider the scenario where a user would like to load any resource that a company owns. These resources can be any webpage or service that the company offers. In a non-ZTN network, perhaps requests are made to a load balancer that acts as a request server, which forwards traffic to the corresponding resource. Such a scenario is a standard operation that many companies would expect to face. In a ZTN, the same steps occur, but with the consideration of a Policy Enforcement Point working with the Policy Administrator and Trust Engine to determine the approval of the request. To the user of the network, the experience is the exact same in that the webpage loads. This example shows a key feature of a ZTN: The backend approvals to relevant systems does not impact the overall front-end user experience.

When analyzing this tenet from a ZTN perspective, we find that a ZTN would not create a scenario where user experiences suffer. If anything, those experiences become more secure. The crux of the exploration for this tenet reveals that while ZTN's do not change how users may interact with a given system, it is a more privacy-centric problem outside the scope of ZTN's as to what information those users are granted access to. Essentially, ZTN's do not change the user experience from non-ZTN's, although ZTN's could be seen as not necessarily improving the privacy posture of a given user experience, either.

3.5 PbD Tenet Five: End-to-End Security – Lifecycle Protection

At first glance, it would seem that this tenet is certainly fulfilled within a ZTN. In other words, how could a network built for improvement in security posture not fulfil this privacy tenet? However, it should be noted that this tenet also expresses concerns for secure methods for deleting data (Cavoukian, 2009).

One can analyze the lifecycle of data into the following components: intake, maintenance, and deletion. As explored in the prior tenets, a ZTN can certainly assist an organization with how such information is accessed and by what systems, but it cannot in of itself determine for an organization how data will be handled at each step. Nevertheless, a ZTN does seem to offer the most help at the maintenance stage through its usage of the Policy Engine and Trust Engine.

Similar to what was discussed in tenet one, the leverage of the Policy and Trust Engine allows for access to the data to be restricted to a higher degree, thus improving the confidentiality stance of the network. Each request is analyzed and thus, allows for limited access to sensitive information. Simply put, higher trust scores could be required for what the organization deems as more sensitive pieces of information.

To address the concerns specific to retention of data, a company could take an approach where there is time to live for a given piece of information (Reardon et al., 2013). This column could reside in a database table and once the time to live has been reached, subsequent trust scores are greatly lowered because the data is to be purged. Essentially, only absolute critical requests would be handled, such as that of an automated job which is configured to delete the data. Hence, a ZTN can provide a mechanism for limiting access to data even after it is marked for deletion, depending on the chosen deletion mechanism.

As for data intake, this is primary covered in the discussion of tenet three. The security of such connections at the intake phase can follow best practices for data in transit, such as utilizing encryption means during the ingestion of data. However, these principles are agnostic of network type; both ZTN's and on-ZTN's can utilize such best practices.

3.6 PbD Tenet Six: Visibility and Transparency

The focus of this tenet is related to accountability of how personal information is handled, openness regarding information management practices, as well as compliance efforts (Cavoukian, 2009). Such tasks seem more appropriate for privacy engineering teams rather than the teams which would configure a ZTN, but usage of a ZTN could be included in communication with users. Perhaps descriptions of the Trust Engine could be given, but this must be balanced with maintaining company confidentiality as it pertains to the security configuration of sensitive systems.

It should also be noted that multiple privacy regulations describe limiting access to systems storing sensitive information, such as the Health Insurance Portability and Accountability Act (HIPAA) and Family Educational Rights and Privacy Act (FERPA) (Tessler, 2014). As stated in prior tenets, ZTN's are structured to implement such mechanisms through the usage of Policy Administrators, Policy Engines, and Trust Engines.

4 Conclusion and PbD Tenet Seven: Respect for User Privacy that is User-Centric

The final tenet of Ann Cavoukian's Privacy by Design principles seems to encompass the prior six tenets. This tenet calls for organizations to take a firm stance to respect user privacy, and keep user privacy concerns at the forefront of the organization's focus (Cavoukian, 2009). One may view this final tenet as the overall message that Ann Cavoukian was striving to communicate through the establishment of the seven Privacy by Design principles.

It is in this tenet that the relationship between Zero Trust Networks and the seven Privacy by Design tenets is made clear. Throughout this exploration of the overlap between Zero Trust Networks and Privacy by Design, this research paper found that Zero Trust Networks provide a framework and the tools for which Privacy by Design can be implemented. That is to say, Zero Trust Networks alone cannot fulfill the Privacy by Design principles and are not inherently considerate of consumer privacy. ZTN's require investment within the areas that best overlap with privacy, such as in the use of Policy and Trust Engines, in order to have privacy as a key component of its design.

Further research is needed to explore how well ZTN's can be used as a tool or framework for other consumer and business needs beyond privacy. Similarly, further research can be performed related to the Privacy by Design framework to evaluate what technologies can best support the implementation of the framework.

The implications of research regarding technologies via different frameworks could lead to greater collaboration within organizations to meet organizational needs. It could be that such collaboration will produce the innovation and ideas that will ultimately create new technologies and frameworks to come. As this paper has found within this intersection of security and privacy alone, it would seem that it is at these intersections of studies that there is great potential waiting to be explored.

References

Campbell, M. (2020). Beyond Zero Trust: Trust Is a Vulnerability. *Computer*, *53*(10), 110–113. https://doi.org/10.1109/MC.2020.3011081

Cavoukian, A. (2009). Privacy by design: The 7 foundational principles. *Information and Privacy Commissioner of Ontario, Canada*, *5*.

Goddard, M. (2017). The EU General Data Protection Regulation (GDPR): European regulation that has a global impact. *International Journal of Market Research*, *59*(6), 703–705.

Kainda, R., Flechais, I., & Roscoe, A. W. (2010). Security and usability: Analysis and evaluation. *2010 International Conference on Availability, Reliability and Security*, 275–282.

Kindervag, J. (2010). Build security into your network's dna: The zero trust network architecture. *Forrester Research Inc*, 1–26.

Langheinrich, M. (2001). Privacy by design—Principles of privacy-aware ubiquitous systems. *International Conference on Ubiquitous Computing*, 273–291.

Lukaseder, T., Halter, M., & Kargl, F. (2020). Context-based Access Control and Trust Scores in Zero Trust Campus Networks. *SICHERHEIT 2020*.

Reardon, J., Basin, D., & Capkun, S. (2013). Sok: Secure data deletion. *2013 IEEE Symposium on Security and Privacy*, 301–315.

Rocha, F., Abreu, S., & Correia, M. (2011). The final frontier: Confidentiality and privacy in the cloud. *Computer*, *44*(9), 44–50.

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero Trust Architecture*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207

Tessler, C. Z. (2014). Privacy, restriction, and access: Legal and ethical dilemmas. *School of Information Student Research Journal*, *4*(1), 5.