2009

When You Can't See the Forest for the Domains: Why a Two Forest ModelShould be Used to Achieve Logical Segregation Between SCADA andCorporate Networks

Andrew Woodward
Edith Cowan University

Brett Turner
Edith Cowan University

Originally published in the Proceedings of the 10th Australian Information Warfare and Security Conference, Edith Cowan University, Perth Western Australia, 1st-3rd December, 2009

When You Can't See the Forest for the Domains: Why a Two Forest Model Should be Used to Achieve Logical Segregation Between SCADA and Corporate Networks

Andrew Woodward and Brett Turner
SECAU – Security Research Centre
School of Computer and Security Science
Edith Cowan University
Perth, Western Australia

Abstract

The increasing convergence of corporate and control systems networks creates new challenges for the security of critical infrastructure. There is no argument that whilst this connection of what was traditionally an isolated network, to a usually internet enabled corporate network, is unavoidable, segregation must be maintained. One such challenge presented is how to properly and appropriately configure an active directory environment to allow for exchange of required data, but still maintain the security goal of separation of the two networks. This paper argues that while separate domains may seem to achieve this goal, the reality is that a domain is not a security boundary, and in fact does not effectively segregate the networks. A more secure and robust barrier can be created through the creation of separate forests, which still allows for one-way trust relationships to be established between the two forests for authentication and data exchange. The paper concludes that there is no loss of functionality or communication through the use of two forests, but there is a loss of security if using one.

Keywords

SCADA security, critical infrastructure protection, active directory services.

INTRODUCTION

Process control systems (PCS) and supervisory control and data acquisition (SCADA) systems are responsible for controlling the majority of the industrial systems that modern society relies upon. These systems control everything from traffic lights through to large scale refineries. Additionally, all critical infrastructure providers also rely upon these systems for safety and reliability, through continuous monitoring and operation.

Traditionally SCADA systems were designed around reliability and safety, and if they were network connected they were connected on isolated internal networks for the purposes of control and management; essentially a closed system. Typically in these situations security was not a consideration due to the isolated nature of the systems and their closed nature. It should be remembered that these systems were implemented at a time when computing and information technology was also largely conducted in isolated installations or laboratories around the globe (Stouffer *et al*, 2007).

With advances in technology, we are becoming increasingly interconnected and interdependent on these connections for the full functioning of modern society. One of the main conduits and enablers for this has been the rapid expansion of the Internet. Correspondingly, as a result of the growth of the Internet there has been a convergence on the TCP/IP protocol suite as the dominant network protocol for business and industry. This has seen many hardware and software vendors, including SCADA vendors, align their products with this kind of reality (Igure *et al*, 2006).

This transition to a greater level of interconnectedness has impacted on the security posture of these systems. Threats and vectors that did not exist prior to this transition are now becoming realisable threats. There is also an increasing reliance on public telecommunications networks to link previously separate SCADA systems making them more accessible to attacks. The increasing use of published open standards and protocols, in particular Internet technologies, expose SCADA systems to Internet or network borne attacks, that were not practical on proprietary protocols that were used previously to control such systems. This increased interconnection of SCADA systems to corporate networks is a significant threat in itself, enabling and making them accessible to undesirable entities e.g. malfeasant insiders (Jackson-Higgins, 2007).

Much has been written about designing the physical network infrastructure in order to achieve segregation between the two networks (INL, 2006; Permann *et al*, 2006; Stouffer *et al*, 2007), but there is little to be found in terms of using logical barriers to achieve this goal. Common, obvious network security measures such as firewalls, demilitarised zones (DMZ), intrusion detection systems and virtual private networks (VPN) are all mentioned in these reports, but the access controls provided by using forests as security barriers are not discussed. This paper will examine the use of Active Directory in order to further achieve segregation through the use of logical separators. Further, it will compare and contrast the security issues involved in using a single forest with using multiple forests.

FORESTS, TREES, DOMAINS AND TRUSTS

In Active Directory terms, a forest is defined as two or more trees which do not share a contiguous namespace. A tree is a collection of domains which do share a contiguous namespace. A domain is a collection of computers, users, printers and other network resources which share a common directory database (Aubert 2004). In order to better understand the reason as to why domains within a tree do not achieve segregation, it is necessary to look at the history of the domain concept through the evolution of Microsoft's Server operating systems.

When Microsoft first introduced the concept of domains with its Windows NT server operating system, it was defined as being a security boundary. That is, members of one domain could not exchange information nor see network assets in another domain, unless trust relationships were explicitly defined (Figure 1).

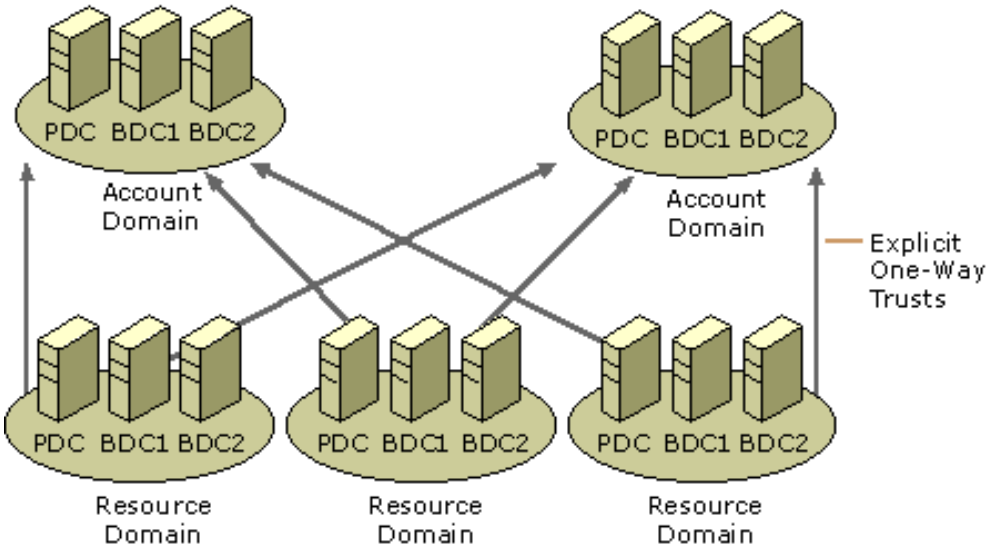

Figure 1: The Windows NT domain as security boundary model. There is no hierarchy and information is only exchanged where explicitly defined (Microsoft, 2009).

Such relationships could be established through the use of trust relationships, but these needed to be setup and configured by an administrator: they were not on by default. With the introduction of active directory with Windows 2000 Server, this was no longer the case, as this new logical hierarchy now included the forest, which was a superstructure over and above that of the domain (Figure 2). Additionally, domains within a forest would now trust each other by default. Of even greater import from a security perspective is that these trusts are transitive, with domains within a forest implicitly trusting one another, meaning that there is effectively no separation between two domains. That is, if domain A trusts domain B, and domain B trusts domain C, then domains A and C implicitly trust each other.

SECURITY RISKS OF THE SINGLE FOREST MODEL

Increasing the integration of the corporate and the SCADA networks offers a greater ease of availability of information from, and control access to, the SACDA network. That same access, while creating increased efficiency in business flows, also increases the attack face presented by the SCADA network. Corporate networks exist in an environment of distrust and operate on access only after authentication. SCADA devices exist in an environment of trust, void of authentication and trusting that whatever instructions sent to them are valid. Increasing the possibilities for breach from one network to the other is always going to be a matter of risk management. Given the trusting environment of a SCADA communications and the nature of a critical infrastructure network, the impact of a breach is going to be greater than in the untrusting environment of a corporate LAN.

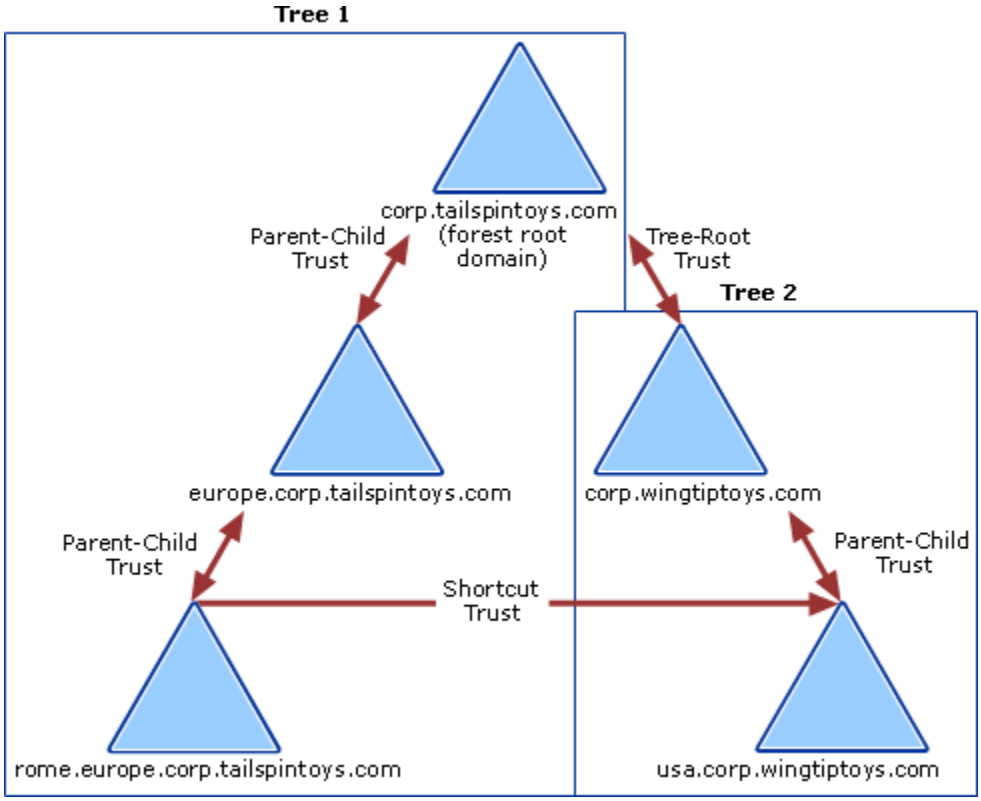

Figure 2: Domains within a single forest have two way transitive trusts by default, meaning that there is effectively no security barrier by default (Microsoft, 2006)

Any integration

The most significant security issue is that of firewall configuration. For a domain or even domains of a single forest to function they have certain communication and replication requirements. This means that the firewall(s) separating the two networks are vulnerable to misconfiguration. If the person configuring the firewall rules is not familiar with AD replication and communication requirements then those rules may be more permissive than needed. The securing of AD communication requires a combination of specific server and AD knowledge to reduce traffic to predictable ports and firewall operation and configuration techniques. If either of these is lacking then the other will suffer in either AD performance or overly permissive rules. Any of these oversights creates a possible breach in lower layered communications that could be exploited.

SSO also provides a single point of compromise. Any account that has legitimate cross-network authentication, whether this is intra-domain, inter-domain or inter-forest is a target for attack. The attack need not be overt either; a virus would be able to spread from the untrusting to the trusting environment through the means of automated authorization. The concept is an implementation of the principle of least privilege. Such authentication measures do not enable otherwise un-implementable access but rather is an ease of use feature.

As soon as an implementation shares a common AD schema it also shares common groups for authorization such as Domain Administrators, Backup operators, Server Operators, Enterprise Administrators and Schema Administrators. Some of these groups are only domain wide, some forest wide. The removal of these groups as avenues of attack improves only as segregation increases.

Single Domain

If Active Directory is configured as a single domain with multiple sites then SSO is not the only issue. Inappropriate group policies can be inadvertently applied to critical machines triggering unforeseen results. This model also allows the authentication and authorization of users through group membership. Security groups can be nested and the method is documented best practice. The obscurity such group membership creates can easily cause unintended access to sensitive resources.

A single domain also reduces the autonomy of the SCADA network. It adds additional groups that gain default authorization to resources such as the domain administrator and backup operators. Two domains in a single forest reduce the number of groups that are granted default authorization but groups that cross the domain boundaries, such as the Enterprise Administrators, do still exist. Such default authorizations provide avenues for elevation of privilege attacks.

A single forest implementation shares a common DNS structure, whether this is internal or external to AD itself it is required for the functioning of AD. The DNS is required to host the address of every AD object for AD to function and such can be queried for information such that normally unseen targets can be identified. Because AD requires DNS to run effectively, DNS itself becomes a target for attack. If DNS can be denied normal operations, AD in turn will cease to function effectively. Critical machines that are AD members may in turn have authentication or authorization issues and become victims of a denial of service attack. Such attacks, such as DNS cache poisoning, can in turn lead to the compromise of key machines such as domain controllers.

If Active Directory is configured as a single domain with multiple sites then replication is not the only issue. Inappropriate group policies can be inadvertently applied to critical machines triggering unforeseen results. This model also allows the authentication and authorization of users through group membership. Security groups can be nested and the method is documented best practice. The obscurity such group membership creates can cause unintended access to sensitive resources.

Privilege escalation is an attack that is used to gain additional authorization from a previously authenticated account.

SUGGESTED MODEL – A TWO FOREST APPROACH

In order to aid in achieving segregation between the corporate and process control networks, the suggested model for Active Directory is to use two forests with no established trusts. The absence of established trusts does not preclude the flow of information: rather, trusts are used primarily as a means of enabling background authentication in a single sign on environment. The absence of trusts between the two forests does place a certain amount of additional user overhead in the way of credentials but also functions as a safety mechanism to prevent unintentional or unwanted intrusions.

Microsoft's recommendations for when to use Multiple Forests

The Active Directory Service is a Microsoft product incorporated in their Windows Server product range. There is a large amount of information available from Microsoft in terms of planning, installing, deploying, configuring, maintaining and managing an active directory environment. Among these is a document detailing when it is appropriate to use a multiple forest environment or deployment. The first three of the seven reasons listed to justify the use of multiple forests apply to a SCADA environment, and are listed as follows:

- Service autonomy: The nature of the structure or operation requires full control of delivery of the directory service.

- Service isolation: The nature of the structure or operation requires full protection from interference with delivery of the directory service.
- Data isolation: Legal ramifications require full protection from interference with directory data.

  (Microsoft, 2003)

Whilst the reasons listed above are primarily business based, it can be seen that these criterion also apply to creating the segregation as required for a SCADA environment.

Why 2 Forests?

The primary reason for using two forests is the single sign on (SSO) mechanism used for authentication and authorization in the windows domain environment without a user having to provide authentication credentials once they have been validated. This mechanism is designed for streamlining authorization to resources in an untrusting environment for ease of access. Trusts are a means of extending this mechanism beyond the traditional domain model, enabling authorization to resources domains and even across forests.

The suggested model for any critical infrastructure integration would have to be a two forest approach. The reasons for this are that as integration increases additional vulnerabilities and avenues for misconfiguration are introduced. A two forest approach still allows for one way information flow into the business network while maintaining isolation. While single sign on is an ease of use feature it also reduces security by transferring authentication used in an untrusting network (corporate) for use in a trusting network (SCADA). Figure 3 illustrates a logical example where there are two forests, and a firewall separates the two networks. Obviously it would be necessary to open some ports in the firewall to allow for the two forests to exchange information.

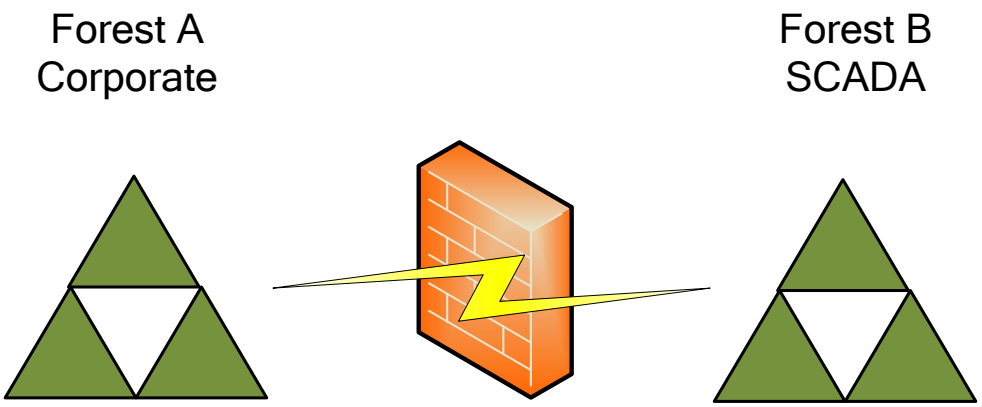

Figure 3: The recommended two forest model to create an Active Directory security boundary

A corporate network is based on the principle of an untrusting environment. That is access to resources is prevented until authorization is granted. Hosts do not automatically accept incoming requests until some form of trust (authentication/authorization) is established. By default, all entities are un-trusted until proven otherwise. This principle, the principle of least privilege, places security over performance.

A SCADA (critical infrastructure) network is a trusting environment. Any request is accepted as long as it is valid. This is done because it is accepted that all entities are trusted to “do the right thing”. This moves processing power that would otherwise been used establishing authorization into performance and response. In a real time network such as a SCADA network, this can be a vital factor when controlling devices requiring critical timing.

There are many risks in an untrusting network which are accepted by implication. When combining an untrusting (corporate) and trusting (SCADA) network the implicit acceptance of these risks that are built into every node of a

corporate environment are imposed upon the trusting environment which is likely to be ill prepared to deal with them.

CONCLUSION

This paper has not argued that segregation through use of the two forest model will protect a SCADDA or process control system network in of itself. As is best practice in securing any network, this segregation measure is best used as part of a defense in depth strategy. The usual security measures, polices and devices must still also be used. They are not mentioned specifically in this paper as that was not the focus, and has been covered in numerous reports by other agencies such as Sandia and Idaho National Laboratories.

The disadvantages, issues and security vulnerabilities that are inherent to the single forest model have been discussed in this paper, while the only advantages of using such a model relate to reduced overhead in installation and configuration. Specifically, the single forest model may be easier to implement, configure and administer than a two forest model, but it just is not as secure. While the two forest model will not necessarily defined against an external or malware based attack, it will certainly mitigate the insider threat, be it intentional or unintentional. It may also be that because Active directory configuration is not normally seen as a front line or obvious security measure, it is often overlooked.

At a fundamental, the choice between a single or two forest model comes to one simple factor: ease of administration. There is no task that cannot be achieved through the use of two forests, but it does mean that increased administration may be the cost. However, the cost of using administrative overhead as a reason not to use a two forest model means that logical separation is not achieved. If we are not able to continue the isolation of process control systems from corporate networks, it is only a matter of time until we see a targeted attack interrupt the supply of essential services, such as power and water. The consequences of this would be severe interruption to the business process for all concerned, and not just the control system operator. There may also be regulatory consequences, particularly if the result of a network and control system breach had environmental impact.

Finally, there is no process, function or communication in a single forest model that cannot be configured in a two forest model. The decision to use a single forest model over a two forest model must not be made on the basis that it may mean more work for IT administrators, as the cost of doing so is that segregation is not achieved, and the process control network is not as protected as it should be.

REFERENCES

Aubert, M. (2004). *MCSE Guide to Microsoft Windows Server 2003 Active Directory*. Thomson Course Technology, Boston: Massachusetts

Idaho National Laboratories (2006) Control Systems Cyber Security: Defense in Depth Strategies. Retrieved 10th October 2009 from http://csrp.inl.gov/Documents/Defense%20in%20Depth%20Strategies.pdf

Igure, V.M., Laughter, S.A. & Williams, R.D. (2006). Security issues in SCADA networks. *Computers and Security*. *25*(7), 498-506

Jackson-Higgins, K. (2007). SCADA state of denial. Retrieved 10th October 2009 from http://seclists.org/isn/2007/Apr/0068.html

Microsoft (2003). Multiple Forest Considerations. Retrieved October 12th 2009 from http://download.microsoft.com/download/0/2/6/026ee2e2-e06d-4660-b9db-6926fd200ed9/Multiforest_White_Paper.doc

Microsoft (2006). How domain and forest trusts work. Retrieved October 12th 2009 from http://technet.microsoft.com/en-us/library/cc773178(WS.10).aspx

Microsoft (2009). Examining the existing domain structure. Retrieved 12th October 2009 from http://technet.microsoft.com/en-us/library/cc960675.aspx

Permann, M., Lee, K., Hammer, J. & Rhode, K. (2006). Mitigations for security vulnerabilities found in control systems networks. In the *Proceedings of the 16th Annual Joint ISA POWID/EPRI Controls and Instrumentation Conference*, June 2006, San Jose California

Stouffer, K., Falco, J. & Scarfone, K. (2007). *Guide to industrial control systems (ICS) security*. USA: NIST