**Week 4: Controlling Access**  
Nate Bachmeier  
September 8th, 2014  
CMGT 430: Enterprise Security  
University of Phoenix  
Facilitator: David Fedorchak

**Table of Contents**

[Controlling Access 3](#_Toc397966388)

[Access through Public Endpoints 3](#_Toc397966389)

[Common Attack Vectors 3](#_Toc397966390)

[Reducing Attack Surface 4](#_Toc397966391)

[Access from Untrusted Devices 5](#_Toc397966392)

[Secret Management 5](#_Toc397966393)

[Assume Hostile Networks 6](#_Toc397966394)

[Mobile Device Management 7](#_Toc397966395)

[Access through External Providers 7](#_Toc397966396)

[Identity Management 8](#_Toc397966397)

[Virtual LAN over WAN (Hybrid Clouds) 8](#_Toc397966398)

[Conclusions 9](#_Toc397966399)

[References 10](#_Toc397966400)

# Controlling Access

For every organization it is important to have control over their data, especially when it is to be exchanged between Internet facing actors. This occurs server side through web roles, client side through untrusted devices, or through external service providers.

Each of these communication profiles comes with various risks, which need to be called out. Once identified the threat landscapes can be understood; leading to proper reduction and mitigate of their associated attack vectors.

# Access through Public Endpoints

When a network application wants to accept input, it will bind to a connection to an endpoint that is accessible at an address (Silberschatz, Galvin, & Gagne, 2012). This address can then be made routable to different scopes; such private network (NAT), intranet, perimeter network (DMZ), or extranets (Goleniewski & Jarrett, 2007). The risk of attack increases as the number of machines capable of communicating with the endpoint increases.

Inside of an enterprise there are many devices (nodes) connected by many routes (edges). These form the network graph which an attacker will try to traverse in a breath first search pattern. As each additional node is compromised, the amount of evidence and credibility the attacker possesses grows exponentially allowing for viral growth (Grimaldi, 2004). Because of this potential threat it is critical to control access across each trust boundary.

## Common Attack Vectors

There are several different methods for an attacker to bypass the trust boundary and gain entry into unexpected parts of the system. The most direct method is by missing checks or validating on the client device. End users can reverse engineer and alter client binaries, removing the validation. Similar to this risk is security through obscurity, such as using non-standard ports. Obscurity mitigations are useful for a defense in depth strategy, but cannot be the only protection.

Another frequently method for losing control of a public endpoint is through mixing of encodings. For instance if user controlled argument is used to make a security decision and it is not properly escaped, then the decision could be made incorrectly. In web technologies cross site scripting (XSS) and SQL injection bugs are two of the most notorious (Conklin, White, Williams, Davis, & Cothren, 2012). These issues can be reduced through deploy of web application firewalls and other request filtration services.

Nontechnical attacks can also exist on public endpoints such as social engineering attacks, password brute forcing, dumpster diving for information, or even simply waiting for a person to login then leave the session unattended (Hernandez, 2012). These challenges can be addressed through proper user education.

## Reducing Attack Surface

Technical and procedural defenses can be used to keep unwanted visitors from using an organizations public endpoints. For instance the endpoint can be configured to respond only to clients with valid authentication certificates. This can make supportability more complex but is highly effective.

Another option is to scope the access, such as limiting the subnets that are allowed to communicate or the time of day that access is permitted (Morimoto, 2010). For example a temporary employee might work 9-5pm, so their account is scoped to allow logins between 6-9pm. Another might be an American based company that blocks access from Asian requests.

Deployment of smart filtering and monitoring can stop many script kiddy attackers (Microsoft, 2013) and notify the network security team of the attempt. Even if all attacks are being blocked it is still good to get notification of attempts. This may lead to reevaluation of the security strategy or prioritizing additional defenses.

# Access from Untrusted Devices

It used to be the case that all hardware connecting to an organization’s infrastructure was directly owned and controlled by that business. However over time the cost of hardware has decreased to the point a large number of professionals own their own smart phones, laptops, home PCs, etc. These devices are not trusted by the central authentication solution, nor do they provide assurances of state or compliance.

## Secret Management

An area of risk on these untrusted devices is credential management. There is nothing keeping the remote user from creating a file called “passwords.txt” then filling it corporate credentials. The file is unsecured and could be acquired by arbitrary malware or other users of the local device.

It is also common for remote employees to have shortcuts to initialize remote terminals and remote sessions into the corporate network. These present another series of risks as an attacker can break into a bank employee’s house instead of the bank itself. Ultimately this provides the same access and likely is significantly less fortified.

To reduce the exposure multifactor authentication (MFA) needs to be deployed for all remote employees. A common implementation might include smart cards or sending use of one time pins, through secondary channel. Another protection is to use certificates instead of passwords for remote employees, as the certificate can easily be revoked and reissued.

Another collection of mitigations might include the deployment of Network Access Protection (NAP). NAP performs various client side policy validations, such as antivirus is up to date or the local drive is encrypted (Morimoto, 2010). If these checks pass them the untrusted device is allowed to access the corporate network.

## Assume Hostile Networks

In the classic office scenario all computers on the network have IPsec deployed; which provides authentication, authorization, encryption, and verifiable watermarks that tampering has not occurred. In contrast the default scenario for a mobile device is to send all communication across untrusted and hostile networks.

To mitigate the hostile network dilemma, there are two common solutions. The first is to deploy private Wireless technologies across the impacted area. This can be costly or impractical as the radius of protection needs to increase. For instance protecting a single office is likely in the hundreds of dollars, while protecting a Metropolitan Area Network (MAN) could easily be in the 10s to 100s of thousands (Goleniewski & Jarrett, 2007).

Another solution is to leverage secure communication forwarding, such as Virtual Private Networks or SSL/TLS enabled proxies. Once deployed the end user will establish a trusted channel to an asset owned by the organization. Next they will send a subset of their traffic to that asset knowing that the medium is safe. When the traffic arrives at the upstream server it can then be forward to other parts of the intranet or extranet (Goleniewski & Jarrett, 2007). The forward traffic is then protected through the normal traffic protection schemes, making the mobile origin irrelevant.

## Mobile Device Management

From a business and risk management perspective it makes sense to have a device management story for all hardware owned by an enterprise. This encompasses numerous scenarios ranging from software deployment, patch management, to inventory of resources (Humble & Farley, 2010).

It also makes sense to expand that reach to hardware that is not owned by the enterprise, such as employee owned mobile devices. By managing both environments, a more consistent interface can be provided to the employees. There is also a more likely chance they will make the right choice if the right choice is the default (Ariely, 2008).

For example a user at home might frequently use VPN solutions to connect into the corporate environment. If they do not patch their system frequently this can lead to a threat and eventual attack surface increase of the network. However by enrolling that home machine in the MDM system, it is automatically receiving policy resulting in compliance remediation.

# Access through External Providers

Cloud offerings present an opportunity for savings along with an option to leverage domain expertise. This is largely due to economy of scale factors, which make it economically efficient to run workloads on outsourced resources. Since the cloud is not going anywhere it is important to understand concerns that are associated with its use (Russinovich & Minasi, 2014).

## Identity Management

All correctly implemented security decisions start with authentication, which can be complex as the environment spans multiple service providers. This is due to the multiple physical locations which all need to be kept in sync (Morimoto, 2010). Also each of these different locations might require different protocols or tools for replicating updates (Das, 2013).

If the environments drift out of sync, there can be periods where business policy is not being enforced. For instance a user account being deactivate might still be usable on cloud infrastructure for a couple more hours. To reduce this risk high bandwidth connections can be used to deploy updates.

Another mitigation could be the use of read-only domain controllers (RODC). RODC can be deployed inside of the service provider’s environment (Conklin, White, Williams, Davis, & Cothren, 2012). After being deployed the central authentication solution can prioritize the updates that are pushed downstream. This way security critical decisions happen more real time, and routine decisions can happen when convenient.

## Virtual LAN over WAN (Hybrid Clouds)

Many organizations can see the value in moving to the public cloud, but are unable to completely migrate. Perhaps due to political, regulatory, compliance, or other technical limitation (Marchewka, 2012). For these organizations the Hybrid cloud scenario has an appealing collection of benefits, and also associated risks.

A hybrid cloud is typically implemented as a private data center that leverages a secure network routing technology to use an isolated collection of cloud compute. For instance Contoso might have a data center in Austin, Texas that uses a VPN connection to access a Virtual LAN exposed from Azure, Amazon, or Google’s data center. Then large banks of processing power can be consumed on demand while retaining all confidential information on company owned hardware.

There are risks with this model such as one of those compute nodes becoming compromised. If this were to happen an attacker could follow the VPN channel back into corporate intranet. This threat can be reduced by limiting the endpoints into third party resources with privileged communications. Actors could still attack the parser code of the remote compute, though that can be mitigated through higher level languages or sandboxing technologies.

# Conclusions

Controlling access is an easy topic within a small circle of private machines. Though as the scope increases and begins to include extranet the risks grow significantly as does the complexity to administrate it.

However the benefits of publishing through the Internet can out weight the negatives. For instance untrusted devices can begin to communicate with corporate data, while doing so in a relatively safe and controllable manner. Another scenario is the use of external service providers such as cloud solutions. Outsourcing sections of the network can reduce costs and allow the business to focus more time and effort on their core business.

Though the threat landscape and challenges are manageable with proper planning and understanding. Once these issues are contained the value can be enjoyed safely, securely and with high availability.

# References

Ariely, D. (2008). *Predictably Irrational: The Hidden Forces That Shape Our Decisions.* Deckle Edge.

Conklin, A., White, G., Williams, D., Davis, R., & Cothren, C. (2012). *Principles of Computer Security: CompTIA Security+™ and Beyond (Exam SY0-301), Third Edition.* McGraw-Hill Company.

Cooper, D., & al., e. (2005). *Project Risk Management Guidelines: Managing Risk in Large Projects and Complex Procurements.* John Wiley & Sons, Ltd.

Das, S. (2013). *Your UNIX/Linux. The Ultimate Guide, Third Edition.* McGraw-Hill Company.

Goleniewski, L., & Jarrett, K. (2007). *Telecommunications Essentials. The Complete Global Source, Second Edition.* Pearson Education.

Grimaldi, R. (2004). *Discrete and Combinatorial Mathematics: An Applied Introduction, 5e.* Pearson Education.

Hernandez, S. (2012). *Official Guide to the CISSP CBK, Third Edition.*

Humble, J., & Farley, D. (2010). *Continuous Delivery: Reliable Software Releases through Build, Test, and Deployment Automation.* Addison-Wesley Signature Series.

Marchewka, J. (2012). *Information Technology Project Management. Providing Measurable Organizational Value, Fourth Edition.* John Wiley & Sons Inc.

Microsoft. (2013). *Best Practices for the Design of Large-Scale Services on Windows Azure Cloud Services*. Retrieved from Azure Documentation: http://msdn.microsoft.com/en-us/library/windowsazure/jj717232.aspx

Microsoft. (2013). *SIR Volume 16*. Retrieved from http://download.microsoft.com/download/7/2/B/72B5DE91-04F4-42F4-A587-9D08C55E0734/Microsoft\_Security\_Intelligence\_Report\_Volume\_16\_English.pdf

Morimoto, R. (2010). *Windows Server 2008 R2 Unleased, 1st Edition.* Pearson Education, Inc.

Russinovich, M., & Minasi, M. (2014, April). *Cloud Computing TechEd 2014*. Retrieved from Channel 9: http://channel9.msdn.com/Events/TechEd/NorthAmerica/2014/DCIM-B386

Silberschatz, A., Galvin, P., & Gagne, G. (2012). *Operating System Concepts, Eighth Edition.* John Wiley & Sons.