Research Lab Security Strategy and Design

Daniel Cordeiro Marques

University of San Diego

CSOL-500-01-FA20 - Foundations of Cyber Security

Professor Ash Mozano

October 24, 2020

Research Lab Security Strategy and Design

The final project scenario presents a large Information Technology company wishing to deploy a new research innovation lab. The facility will be onsite, and the lab will be available to employees and people outside of the company's personnel. The lab must support collaboration through flexibility and scalability while securing the corporate environment from external threats. This work proposes a security framework based on NIST (2018) and the "zero trust" model to support the development and deployment of the lab by outlining cybersecurity risks to the project and providing strategy and architecture to mitigate threats to the preservation of availability, utility, integrity, authenticity, confidentiality, and possession (Parker, 2014) of the company's information while addressing business requirements. The paper assumes that the lab will be located in a multi-floor building and share its physical and environmental controls (fire suppressants, heat and cooling systems, and access control mechanisms). It also considers a "bring your own device" (BYOD) model for the research lab and that researchers may not be in the same location. Finally, the paper does not make any financial considerations and focuses on high-level controls to separate the lab environment from the corporate environment.

Scope and Assumptions

Lab Facilities

The company will build the lab in its corporate office, a multi-floor facility that provides physical controls to address environmental threats such as floods and fire (fire suppressants, elevated floors, and emergency power). This paper also assumes that the building provides other essential security controls typically found on commercial facilities, including a badge scanning system with log collection capabilities, front desk check-ins and turnstiles in the lobby, video surveillance, and 24x7 guards.

Lab Environment and Services

To allow for a scalable and flexible solution, the company will deploy the lab environment in a private cloud. The lab's on-site Information Technology (IT) infrastructure provides Internet services so researchers can access the lab cloud. All resources will be available remotely, and an assigned lab administrator will be responsible for access control. Finally, the company will deploy the laboratory on a floor by itself.

Research Lab Security Strategy

Threats

The new lab exposes the company primarily to new external entities. In essence, it inserts into the company environment people and assets that are not managed by, or subject to, the company's security policies. Additionally, corporate users might abuse the lab environment to bypass security controls already in place and leak sensitive information. Shostack (2014, p. 32) proposes a scenario-based approach to threat modeling. The approach suggests asking "what can go wrong?" in the face of a business requirement, used in this paper to identify potential threats and vulnerabilities.

External research lab personnel can impersonate employees. External lab users may impersonate corporate personnel to bypass physical access controls in place and gain access to the corporate environment in an attempt to compromise the network, gain access to sensitive handled by corporate IT assets, or in physical documents. The security framework should consider the access control between the lab and the corporate facilities, clear identification of lab users and corporate personnel, security awareness, and company employees' training.

External users may use the lab network to launch attacks against the corporate network. Users in the lab environment may abuse the network and attempt to compromise the corporate network or launch denial of service attacks that affect business operations. The framework should employ network segmentation between the lab and the corporate network, continuous network monitoring, and access control to the lab network to address this scenario.

External users may connect unmanaged devices to the lab network. Users in the lab environment may bring their own devices and connect to the lab network. These devices might not be compliant with corporate security policies and expose sensitive assets to unknown threats. The strategy must consider a balance between usability, network segmentation, and access control to the lab environment.

External research lab personnel and internal users can launch attacks from the lab network against third parties. Users may abuse the lab network to launch attacks against other entities, exposing the company's IP address space. The strategy must address this by employing network segmentation between the lab and the corporate network and continuous network monitoring.

Corporate users may abuse the lab environment to leak sensitive information. Corporate users with access to the lab environment might abuse the lab's network infrastructure to bypass security controls in the corporate network that prevent information leakage. The plan should consider the isolation of the environment and restricting information flow between corporate and lab assets.

Security Framework

The framework follows the principle of “zero trust” (Microsoft, n.d.) to design security controls that address previously identified threats. The strategy follows an “assumed breach” approach; therefore, it considers the lab an untrusted and potentially hostile environment. Access to and from the lab should be explicitly verified and allowed or denied, considering the least privilege principle.

Management must update policies, controls, and procedures to align with this model, including:

- Physical security policies and procedures should address corporate buildings and lab facilities (NIST, 2020). Additionally, security awareness training should cover social engineering risks, implicit trust, and validating one’s identity before allowing corporate facilities access.
- Network security policies and procedures should consider the impact of unmanaged devices and an acceptable use policy covering the lab environment by external and corporate users.
- Data classification policies must cover sensitive information handled by company assets. Management should consider evolving the IT team to develop a solution to automate tagging and data classification (Forcepoint, 2019).
- The audit policy must also consider the constant evaluation of the newly implemented controls to ensure their efficacy and identify improvement opportunities.

Physical Security

The company should build the lab on an isolated floor. The lab should apply and follow the company's physical policies, procedures, and controls already in place.

Only personnel identified by electronic badges should have access to the lab environment. External personnel is not allowed on the corporate floors. Badges must be visible at all times. A centralized server will store the badge readers' logs, that will alert on the following:

- Attempts to access corporate facility by researchers
- Dual-entry attempts on corporate floors ("badging in" without "badging out," access to corporate floors after swiping the badge on turnstiles)

Third parties researchers must check in before receiving a badge to access the building. Security will re-evaluate the researcher's access every three months and cancel immediately if no longer required. If the researcher does not visit the facility for 30 consecutive days, security should revoke their access.

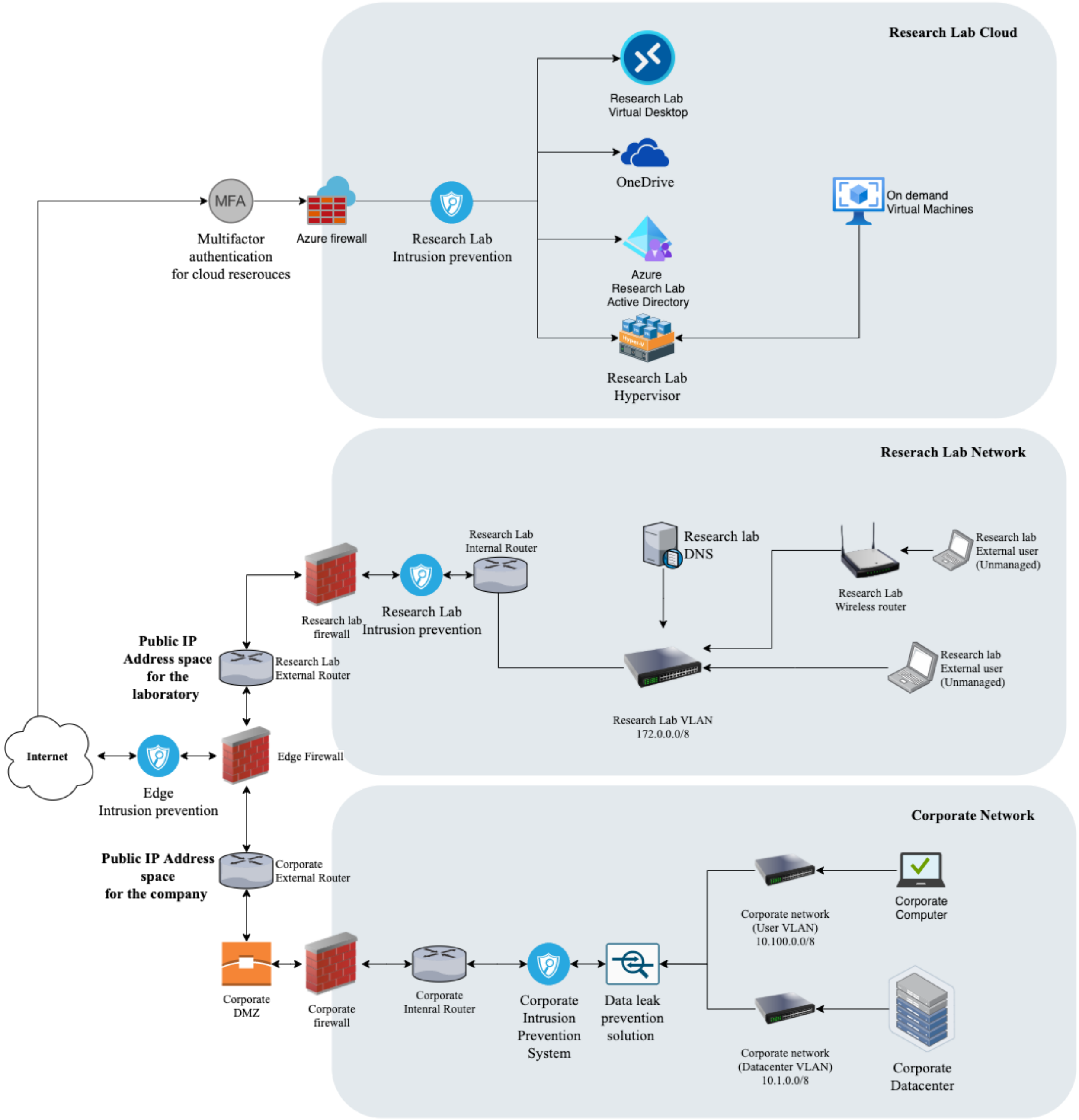
Finally, the company must educate employees to consider lab users as visitors without access to corporate facilities and report any attempts to violate security controls.

Network Security

The lab environment has two components: the physical lab network and the private cloud. Both domains are isolated from the corporate network; no connectivity is allowed between the lab and corporate networks. Before accessing the lab environment, users must read, accept, and follow the Acceptable Use Policy. The policy must provide mechanisms to hold the users accountable for keeping their systems updated and protected from the latest threats. Figure 1 provides a high-level network diagram of the architecture.

Figure 1

High-level network diagram including the corporate network, lab network, and private cloud.


Research Lab Cloud
Research Lab Virtual Desktop
OneDrive
On demand Virtual Machines
MFA
Multifactor authentication for cloud reserouces
Azure firewall
Research Lab Intrusion prevention
Azure Research Lab Active Directory
Research Lab Hypervisor
Reserach Lab Network
Research Lab Internal Router
Research lab DNS
Research lab External user (Unmanaged)
Research Lab Wireless router
Research lab firewall
Research Lab Intrusion prevention
Public IP Address space for the laboratory
Research Lab External Router
Research lab External user (Unmanaged)
Research Lab VLAN 172.0.0.0/8
Internet
Edge Intrusion prevention
Edge Firewall
Corporate Network
Public IP Address space for the company
Corporate External Router
Corporate Computer
Corporate network (User VLAN) 10.100.0.0/8
Corporate DMZ
Corporate firewall
Corporate Intenral Router
Corporate Intrusion Prevention System
Data leak prevention solution
Corporate network (Datacenter VLAN) 10.1.0.0/8
Corporate Datacenter

The lab environment has a dedicated IP address space. The company provides the lab with Internet connectivity and its own external IP address space. The designated IP addresses can help identify network traffic coming from the lab and support attributing attacks to the physical lab network.

Network segmentation. The corporate and research lab firewalls and routers segment both networks from each other, blocking packages between the two environments. The lab environment should have a separate Windows domain, provided by the private cloud's Active Directory (AD). Users who need to access the research lab wireless network must authenticate to the research lab domain. Corporate assets cannot access the lab wireless network. The research lab router should explicitly block corporate assets from accessing the network, and the lab administrator must add users to the appropriate group to allow wireless network access.

Corporate users collaborating with the research lab must use a designated cloud-based non-persistent virtual desktop, which follows a security baseline covering secure configuration and patch management. Users cannot copy data from and to the virtual desktop but can access private cloud resources according to their assigned privileges. Corporate users cannot authenticate to the cloud systems using corporate assets except for the virtual desktop.

Continuous security monitoring. The research lab firewall and intrusion prevention system (IPS) monitor the network for potential attacks originating from the research lab network. The cloud IPS monitors malicious activities within the private cloud. A server in the private cloud collects and cross-reference logs from all solutions (including corporate users attempting to access the lab network) and alerts security administrators when observing malicious activities. The security team must routinely verify the tool for activities not aligned with the lab's purpose and acceptable use policy.

A data leak prevention (DLP) solution on the corporate network monitors users attempting to transfer sensitive information outside of the corporate network. The solution leverages the data classification policy to determine when to alert the security team.

In the occurrence of a potential incident, the security team must take immediate action. Security must investigate the cause of the incident and evaluate the impact and violation of the acceptable use policy. The company must apply sanctions according to the event's impact, including the termination of user access.

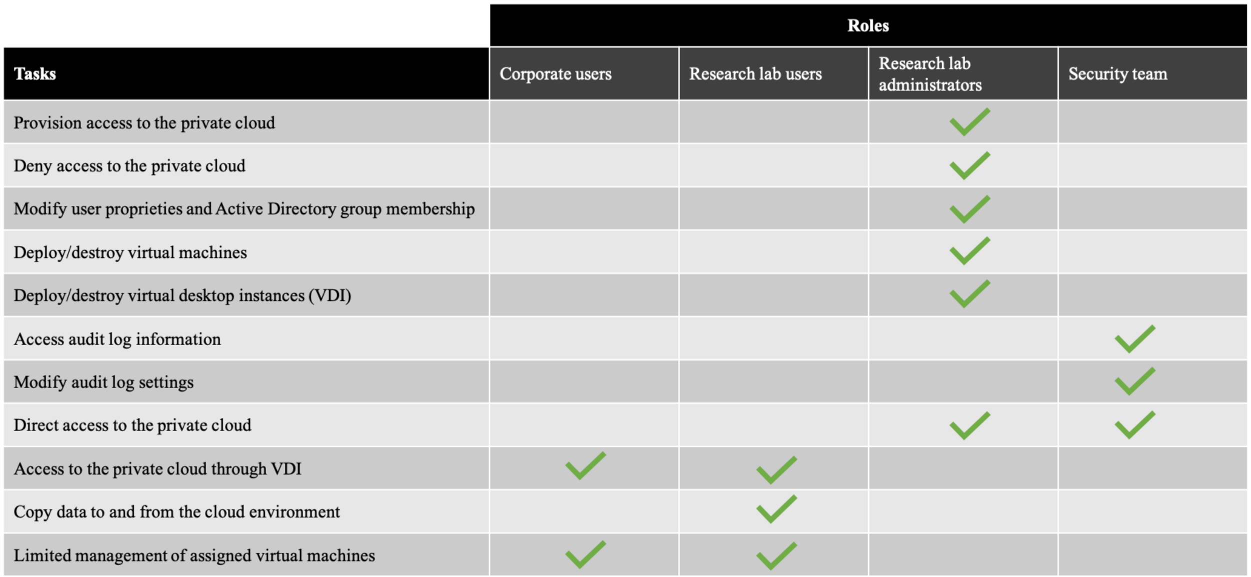
The central log server only allows information systems and users to add information. Data modification is not allowed; the server performs integrity checks during each operation.

Access Control In The Private Cloud

There are four roles in the private cloud: corporate users, research lab users, research lab administrators, and the security team. Corporate users are part of the company staff, using a managed device to access cloud services. Research lab users are third-party personnel associated with the lab, using an unmanaged device to perform their tasks. The research administrators are responsible for maintaining the lab functional and managing the resources and services deployed in the private cloud. Finally, the security team monitors the lab environment and responds to the research lab security incidents. Figure 2 illustrates a role-based access control (RBAC) model for the private cloud.

Figure 2

Role-based access control (RBAC) model for the private cloud.



	Roles			
Tasks	Corporate users	Research lab users	Research lab administrators	Security team
Provision access to the private cloud			✓	
Deny access to the private cloud			✓	
Modify user proprieties and Active Directory group membership			✓	
Deploy/destroy virtual machines			✓	
Deploy/destroy virtual desktop instances (VDI)			✓	
Access audit log information				✓
Modify audit log settings				✓
Direct access to the private cloud			✓	✓
Access to the private cloud through VDI	✓	✓		
Copy data to and from the cloud environment		✓		
Limited management of assigned virtual machines	✓	✓		

Before accessing the research lab private cloud, users must authenticate to the cloud's active directory (AD) using a combination of valid username and password along with a multifactor authentication (MFA) token; users cannot access the private cloud resources without authenticating. Only users registered by the third-parties collaborating in the research can have their access provisioned by the lab administrator. The same rules from the physical access apply to the private lab cloud, and an automated routine reconciles physical access to the building and remote access to the cloud. The cloud AD generates logs for failed and successful login attempts.

Virtual machine (VM) users can manage their resources in the private cloud. They can, for instance, install and remove software and choose to allow other users to access their VMs. However, they cannot change the baseline image settings (such as modify audit log capabilities, uninstall endpoint security software, and remove security patches). The VM operating system checks the user privileges before every action and generates audit logs for success and failures.

The central log server collects all authentication and authorization logs, and users are not authorized to access them.

Audit Capabilities

The logs stored in the centralized server must provide enough information to support troubleshooting and incident response capabilities, including after-the-fact investigations. Logs must identify the research lab environment users, the action performed, assets involved in the event, and a timestamp of the event. Administrators must perform integrity checks. The security team and the research lab administrators must create mechanisms to check the logs' integrity, such as append-only permissions and hashes. At a minimum, the centralized server should have the following logs:

- Successful and failed login attempts to the research lab wireless network.
- Research lab's network IPS events.
- Successful and failed login attempts to the private cloud Active Directory.
- Successful and failed login attempts to resources in the private cloud.
- Suspected traffic in the private cloud.
- Suspected activities in the cloud VMs.
- Suspected activities in the cloud Virtual desktops.

Finally, the security team should periodically review the logs for suspicious activities and verify its integrity. The research lab administrators and the security team must ensure the log server collects the required information from all systems in scope.

Incident Response

Leveraging the audit logs and the continuous monitoring tools, the security team should work with the research lab administrators to address security incidents. The security team must develop an incident response plan to track down the incident's source, identify the impact, and establish containment measures. If an incident is detected, the research lab administrator should consider revoking the offender's access to the lab environment and isolate the affected systems for further investigation. Finally, the security team should immediately notify the third-party associated with the user for additional measures.

Conclusion

Deploying a research lab infrastructure through new and unmanaged devices and personnel exposes the company to risks that the existing security policies and procedures may not address. Assuming a "zero trust model" by following the strategy to isolate the network and provide a private cloud environment allows scalability and flexibility while segmenting corporate assets from potentially compromised assets. Continuous monitoring of network traffic and endpoint systems helps address potential attacks against its IT infrastructure and information leakage. Finally, frequent auditing of logs allows the security team to quickly take measures against threats and evaluate controls' efficacy and efficiency.

References

Forcepoint. (2019). *The practical executive's guide to data loss prevention*. Whitepaper. https://www.mcafee.com/enterprise/en-us/security-awareness/data-protection/dlp-best-practices.html

Microsoft. (n.d.). *Zero trust maturity model*. Microsoft Security. Retrieved October 25, 2020, from https://www.microsoft.com/en-us/security/business/zero-trust

National Institute of Standards and Technology. (2018). *Framework for improving critical infrastructure cybersecurity* (version 1.1). U. S. Department of Commerce. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

National Institute of Standards and Technology. (2020). *Security and privacy controls for information systems and organizations* (Special Publication 800-53). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-53r5

Parker, D. (2014). Toward a new framework for information security. In S. Bosworth, M. E. Kabay, & E. Whyne (Eds.), *Computer Security Handbook* (6th ed., 3.1-3.23). John Wiley & Sons, Inc.

Shostack, A. (2014). *Threat modeling: Designing for security*. John Wiley & Sons, Inc.