BITS Pilani
Pilani | Dubai | Goa | Hyderabad

Cyber Security

Essential Cyber Security Controls

Dr. Ramakrishna Dantu

Associate Professor, BITS Pilani

Disclaimer and Acknowledgement

- The content for these slides has been obtained from books and various other source on the Internet
- I here by acknowledge all the contributors for their material and inputs.
- I have provided source information wherever necessary
- I have added and modified the content to suit the requirements of the course

Agenda

- The Threat Landscape
- Understanding Vulnerabilities
- Common Cyber Attacks
  - Stages and Patterns
  - Targeted and Non-targeted Attacks
  - Reducing exposure to Cyber Attacks
- Essential Cyber Security Controls
  - Boundary firewalls and Internet gateways
  - Secure configuration
  - Whitelisting and execution control
  - User access control
  - Password policy
  - Content checking

Essential Cyber Security Controls

Overview

- The Essential Cyber Security controls involve a set of controls which, when properly implemented, will provide organizations with basic protection from the most prevalent forms of threats coming from the Internet
- In particular, it focuses on threats which require low levels of attacker skill, and which are widely available online
  - Boundary firewalls and Internet gateways
  - Secure configuration
  - Whitelisting and execution control
  - User access control
  - Password policy
  - Content checking

Source: Information Risk Management: A practitioner's guide by David; Sutton

Boundary Firewalls and Internet Gateways

Boundary Firewalls and Internet Gateways

Overview

- A firewall or Internet gateway protects internal networks and systems against unauthorized access from the Internet
- A firewall monitors all inbound and outbound traffic and restricts it to only authorized connections
  - Such restrictions are achieved by applying configuration settings known as firewall rules
- A Firewall is a barrier that sits on the edge of your network (the trusted network) separating it from the rest of the internet (the untrusted network)
- The role of a Firewall is:
  - to prevent those that are not permitted access to your network
  - to stop them from being able to gain control or visibility of your data or systems
  - to provide secure access for those external to your network that you wish to permit access
- This could include the provision of a VPN or certain network ports being open to third-party services, such as a VoIP phone system, for example.

Source: https://www.itgovernance.co.uk/boundary-firewalls-and-internet-gateways

Boundary Firewalls and Internet Gateways

Securing Firewalls

- For all firewalls (or equivalent network devices), an organization should routinely follow these:
  - Change any default administrative password to an alternative strong password – using best practices – or disable remote administrative access entirely
  - The admin interface used to manage boundary firewall configuration should not be accessible from the Internet
    - Unless there is a clear and documented business need
  - This admin interface must be protected by one of the following controls:
    - A second authentication factor, such as a one-time token; or
    - An IP whitelist that limits access to a small range of trusted addresses
  - Block unauthenticated inbound connections by default
  - Firewall rules that are no longer required should be removed or disabled in a timely manner
    - E.g. because a service is no longer required

Source: https://www.itgovernance.co.uk/boundary-firewalls-and-internet-gateways

Securing Firewalls Contd…

- For all firewalls (or equivalent network devices), an organization should routinely follow these:
  - Each rule that allows network traffic to pass through the firewall (e.g. each service on a computer that is accessible through the boundary firewall)
    - should be subject to approval by an authorized individual and documented
    - the documentation should include the organization's need (business case)
  - Unapproved services, or services that are typically vulnerable to attack should be disabled (blocked) at the boundary firewall by default
    - E.g., server message block (SMB), NetBIOS, tftp, RPC, rlogin, rsh or rexec
  - Use a host-based firewall on devices that are used on untrusted networks such as public Wi-Fi hotspots
    - A host-based firewall is a firewall software that runs on an individual computer or device connected to a network
    - These types of firewalls are a granular way to protect the individual hosts from viruses and malware, and to control the spread of these harmful infections throughout the network.

Source: Information Risk Management: A practitioner's guide by David; Sutton

Secure Configuration

Secure Configuration

Overview

- Secure configuration refers to security measures that are implemented when building and installing computers and network devices in order to reduce cyber vulnerabilities
- Security misconfigurations are one of the most common gaps that hackers look to exploit
- According to a report by Rapid7, internal penetration tests encounter a network or service misconfiguration more than 96% of the time
  - Rapid7 is a provider of security data and analytics solutions enabling organizations to implement an active approach to cybersecurity
- According to SANS Institute and the Council on CyberSecurity,
  - Following an inventory of your hardware and software, the most important security control is to implement secure configuration
  - The SANS Institute (www.sans.org), founded in 1989 specializes in information security, cybersecurity training, and selling certificates

Source: https://www.itgovernance.co.uk/secure-configuration

Secure Configuration

Why is Secure Configuration Important?

- Manufacturers often set the default configurations of new software and devices to be as open and multi-functional as possible
  - E.g., in the case of a router this could be a predefined password
  - E.g., in the case of an operating system, it could be the applications that come preinstalled.
- It’s easier and more convenient to start using new devices or software with their default settings, but it’s not the most secure
- Accepting the default settings without reviewing them can create serious security issues, and can allow cyber attackers to gain easy, unauthorized access to your data
- Web server and application server configurations play a crucial role in cyber security
- Failure to properly configure the servers can lead to a wide variety of security problems
- Computers and network devices should also be configured to minimize the vulnerabilities and provide only the services required to fulfil their intended function

Source: https://www.itgovernance.co.uk/secure-configuration

Secure Configuration

Hardening Guides for Securing Technologies

- Initial installation of technology (E.g., an OS, a Web Server, a Database Sever) with its default configuration usually works fine
  - Assuming proper installation
- Most important step, is to harden the system and make sure it as secure as possible
- Hardening guides are specific to the technology and can be obtained from the manufacturer or developer of the software
- Internet Interest Groups for more popular OS and Applications also provide their hardening guides based on their experience or best practices
- Sometimes a technologist who has gone through this process might document and share their hardening guides and process with others

Source: YouTube - Secure Configuration Guides - CompTIA Security+ SY0-501 - 3.1

Secure Configuration

Key Technologies that Require Secure Configuration

- Web Server
  - MS Internet Information Server, Apache HTTP Server, etc.,
- Operating System
  - Windows, Linux, iOS, Android, etc.,
- Application Server
  - Programming Languages, Runtime Libraries, etc.,
- Network Infrastructure Devices
  - Switches, Routers, Firewalls, IPS, etc.,.

Source: YouTube - Secure Configuration Guides - CompTIA Security+ SY0-501 - 3.1

Secure Configuration

General Rules and Guidelines

- For computers and network devices, your organization should routinely:
  - Remove and disable unnecessary user accounts
  - Change default or guessable account passwords to something non-obvious
  - Remove or disable unnecessary software
  - Disable any auto-run feature that allows file execution without user authorization
  - Authenticate users before enabling Internet-based access to commercially or personally sensitive data, or data critical to the running of the organization

Source: https://www.itgovernance.co.uk/secure-configuration

Secure Configuration

General Rules and Guidelines

- For password-based authentication, the organization should:
  - Protect against brute-force password guessing by limiting attempts and/or the number of guesses allowed in a certain period
  - Set a minimum password length of at least eight characters
  - Change passwords promptly when the user knows or suspects they have been compromised; and
  - Have a password policy that informs users of best practices.

Source: https://www.itgovernance.co.uk/secure-configuration

Secure Configuration

General Rules and Guidelines

- As a minimum:
  - Unnecessary user accounts (e.g. Guest accounts and unnecessary administrative accounts) should be removed or disabled immediately
  - Any default password for a user account should be changed to an alternative, strong password
  - Unnecessary software (including application, system utilities and network services) should be removed or disabled
  - The auto-run feature should be disabled (to prevent software programs running automatically when removable storage media is connected to a computer or when network folders are accessed)
  - A personal firewall (or equivalent) should be enabled on desktop PCs and laptops, and configured to disable (block) unapproved connections by default.

Source: Information Risk Management: A practitioner's guide by David; Sutton

User Access Control

User Access Control

Overview

- Access control involves selective restriction of access to data
  - Meaning, they provide access to users based on what they are permitted to see and use
- It consists of two elements:
  - Authentication – a technique used to verify the identity of a user
  - Authorization – determines whether a user should be given access to data
- Under module 2, we already discussed
  - Discretionary Access Control (DAC)
  - Nondiscretionary Access Controls
    - Mandatory Access Control (MAC)
    - Role-based access control (RBAC)
    - Attribute-based access control (ABAC)
  - Originator-controlled Access Control (ORCON or ORGCON)
    - Originator (creator) of information controls who can access information
- Here, we focus more on the general rules and guidelines

Source: https://www.itgovernance.co.uk/access-control-and-administrative-privilege

User Access Control

General Rules and Guidelines

- To be effective, access control requires the enforcement of robust policies
- Organizations must determine the most appropriate access control model based on the type and sensitivity of the data they are processing
- Privilege accounts (e.g. administrative accounts), should be assigned only to authorized individuals, managed effectively, and provide the minimum level of access to applications, computers and networks
- Authenticate users before granting access to applications or devices, using unique credentials
- Remove or disable user accounts when no longer required
- Implement two-factor authentication, where available
- Use administrative accounts to perform administrative activities only
- Remove or disable special access privileges when no longer required

Source: https://www.itgovernance.co.uk/access-control-and-administrative-privilege

User Access Control

General Rules and Guidelines

- As a minimum:
  - All user account creation should be subject to a provisioning and approval process
  - Special access privileges should be restricted to a limited number of authorized individuals
  - Details about special access privileges (e.g. the individual and purpose) should be documented, kept in a secure location and reviewed on a regular basis (e.g. quarterly)
  - Administrative accounts should only be used to perform legitimate administrative activities, and should not be granted access to email or the Internet
  - Administrative accounts should be configured to require a password change on a regular basis (e.g. at least every 60 days)
  - Each user should authenticate using a unique username and strong password before being granted access to applications, computers and network devices
  - User accounts and special access privileges should be removed or disabled when no longer required (e.g. when an individual changes role or leaves the organization) or after a pre-defined period of inactivity (e.g. 3 months)

Source: Information Risk Management: A practitioner's guide by David; Sutton

Whitelisting and Execution Control

Whitelisting and Execution Control

Overview

- Whitelisting is a cybersecurity strategy under which a user can run only those applications that are approved by the administrator
- Instead of keeping track of malicious code that should be blocked, security administrator compiles a list of approved applications that a computer or mobile device can access
- It requires explicit approval to run the applications
- In essence, the user has access to only a limited set of functionality, and what they can access has been deemed safe by the administrator
- This is very restrictive. it is an extreme lockdown measure that, if implemented properly, can keep many cybersecurity problems at bay
- Disadvantages:
  - It can be quite inconvenient and frustrating for end-users, requires careful implementation and proper ongoing administration, and isn't a foolproof barrier to attacks.
- Advantages:
  - We know exactly what kinds of applications are or can be run on our systems
- Bottom line: nothing runs unless approved

Source: https://www.csoonline.com/article/3562429/whitelisting-explained-how-it-works-and-where-it-fits-in-a-security-program.html

Whitelisting and Execution Control

Blacklisting & Graylisting

- Blacklist
  - It is the exact opposite of whitelisting
  - Nothing on the "blacklist" can be executed
  - Blacklist is a list of different entities that have been deemed to be malicious so those are the ones that you actually want to block from the get go
  - There is a lot less administrative overhead, but this allows any application that is not blacklisted
- Graylist
  - Graylist is a list of different objects that haven't been established as harmful or malicious or non-harmful or non-malicious
  - Once additional information is actually obtained, the graylist items can be either moved to a whitelist or to a blacklist
- National Institute of Standards and Technology (NIST) defines the concept of whitelisting and blacklisting in their special publication NIST SP800-167
  - https://csrc.nist.gov/publications/detail/sp/800-167/final

Source: Cyber Security - Exploring Application-level Whitelisting/Blacklisting by Omar Santos

Whitelisting and Execution Control

What threats does whitelisting fight?

- Application whitelisting is a great defender against two different kinds of security threats
  - Malware:
    - Malicious software payloads like keyloggers or ransomware won't be able to execute if they're not on the whitelist
  - "Shadow IT"
    - Shadow IT is the use of information technology systems, devices, software, applications, and services without explicit IT department approval
    - End users or individual departments may try to install programs on their computers that are insecure or aren't properly licensed
    - If those apps aren't whitelisted, the rogue departments are stopped in their tracks, and IT will be informed about the attempt

Source: https://www.csoonline.com/article/3562429/whitelisting-explained-how-it-works-and-where-it-fits-in-a-security-program.html

Whitelisting and Execution Control

How do you create an application whitelist?

- Two different approaches
  - One:
    - using a standard list (supplied by the whitelist software vendor) of applications typical for our type of environment, which can then be customized to fit
  - Two:
    - is to have a system that you know is clear of malware and other unwanted software, and scan it to use as a model for a number of other machines
      - The second method is a good fit for kiosks or other public-facing devices, which run a limited set of applications and don't require much by way of customization

Source: https://www.csoonline.com/article/3562429/whitelisting-explained-how-it-works-and-where-it-fits-in-a-security-program.html

Whitelisting and Execution Control

Challenges in Application Whitelisting

- There are practically hundreds or thousands of files and applications in the system with the legitimate need to be actually present and running on that system
- So, the challenge is in
  - Continuous management of what is and what is not in the whitelist
  - Keeping track of what is and what is not allowed in a system

Source: Cyber Security - Exploring Application-level Whitelisting/Blacklisting by Omar Santos

Tools for Managing Whitelists

- Modern application whitelisting solutions can keep track of the changes happening on a system when approved changes are made to the whitelists
- Most commercial operating systems have some whitelisting functionality built in, including Windows 10 and macOS
- App stores (used to install applications on iOS and Android devices), can be seen as a form of application whitelisting
  - they ostensibly only allow applications that are certified to be safe
- There are third-party vendors who offer more powerful or more granular application whitelisting software
  - These are often rolled into larger offerings or security suites
- Popular examples include:
  - AppLocker, a Microsoft offering for its enterprise OS editions
  - BeyondTrust, which has offerings for Mac and Windows as well as Unix-like OSes
  - PolicyPak, which works on on-prem and remote computers
  - Centrify, which emphasizes zero-trust principles across its product suite
  - Kasperksy Whitelist, a collaborative hosted service

Source: https://www.csoonline.com/article/3562429/whitelisting-explained-how-it-works-and-where-it-fits-in-a-security-program.html

Whitelisting and Execution Control

How is application whitelisting accomplished?

- The NIST guide breaks down the various attributes that can be used for this purpose:
  - The file name
  - The file path
  - The file size
  - A digital signature by the software's publisher
  - A cryptographic hash
- Which attributes should be used and how much weight should be given to each is key to the art of whitelisting

Source: https://www.csoonline.com/article/3562429/whitelisting-explained-how-it-works-and-where-it-fits-in-a-security-program.html

Requirements for Whitelisting Software

- NIST points out that full-on applications aren't the only potential threat to a computer
- Whitelisting software needs to keep on top of various libraries, scripts, macros, browser plug-ins, configuration files, and, on Windows machines, application-related registry entries
- Different vendors can deal with these with varying levels of granularity
- Some whitelisting software can also whitelist specific behavior from even approved applications, which can come in handy if hackers manage to hijack them
- And whitelisting software should also integrate with the permissions structure of your operating system, whitelisting applications for some users (like administrators) but not others.

Source: https://www.csoonline.com/article/3562429/whitelisting-explained-how-it-works-and-where-it-fits-in-a-security-program.html

Whitelisting and Execution Control

Whitelisting Best Practices

- A whitelisting program is only as good as the list itself
- IT isn't static; some of your software will fall out of use, some will need to be updated in ways that could cause the whitelist to fail to recognize it, and new software will become necessary for your organization to fulfill its mission
- Roll out whitelisting in phases to make sure we don't disrupt enterprise-wise operations if something goes wrong
- Spend time to make sure we get a correct whitelist
- Think of it as an opportunity to audit what applications your organization has installed across your IT infrastructure — and which ones it really needs
- Develop a whitelisting policy to ensure what goes into the list
- Don't neglect the maintenance of your whitelist
- This maintenance requires resources; you'll either need to have staff for whom this is part of their duties, or you'll need to pay your vendor for this service, or some combination of the two.

Source: https://www.csoonline.com/article/3562429/whitelisting-explained-how-it-works-and-where-it-fits-in-a-security-program.html

Whitelisting and Execution Control

Where whitelisting fits into a security program

- Whitelisting isn't a one-size-fits-all tool, and it may not be an ideal endpoint solution for every computer under your purview
- Three scenarios where application whitelisting makes sense:
  - On centrally managed hosts connected to other computers
  - On computers in a high-risk environment
  - On laptops or kiosks where users do not have administrative privileges
- Whitelisting isn't a security panacea, and has to fit into a larger security landscape within your organization
- You'll still need anti-malware, endpoint protection, and perimeter defense systems to protect computers for which whitelisting isn't appropriate, or to catch what whitelisting misses

Source: https://www.csoonline.com/article/3562429/whitelisting-explained-how-it-works-and-where-it-fits-in-a-security-program.html

Password Policy

Password Policy

Overview

- Most system compromises are the result of weak passwords
- A few reasons
  - Users create easy-to-guess passwords
  - Administrators often forget to remove default accounts and passwords on devices
  - Unused accounts contain passwords that don't change
- Users should select good passwords and periodically change them
- Password guessing and cracking attacks are common ways of gaining unauthorized entry to networks
- If given enough time, even the best passwords can eventually be broken
- Strong passwords act as deterrent against password guessing attacks and buys additional time against cracking attacks

Source: Network Security Bible, 2nd Edition by Eric Cole

Password Policy

Guidelines to Enforce Strong Password

- The following guidelines enforce a strong password policy:
  - The password must be at least eight characters
  - It should contain both alphanumeric and special characters
  - A user can't reuse his/her last five passwords
  - Passwords must change every 60 days
  - Accounts are locked out after three failed login attempts

Source: Network Security Bible, 2nd Edition by Eric Cole

Guidelines to Enforce Strong Password

- The following examples allow the enforcement of the password policy at the operating system level:
- Password aging
  - Allows forcing the user to change his password periodically
- Minimum length
  - Allows the enforcement of a minimum password length
- Non-dictionary words
  - Allows stopping the user from selecting a password that is in a standard dictionary
- Password uniqueness
  - Allows specifying the number of new passwords that users must select before they can reuse a previous one
- New password
  - Allows setting a minimum number of characters required for the new password that is different from the previous password

Source: Network Security Bible, 2nd Edition by Eric Cole

Password Policy

Create Good Passwords

- The following best practices provide additional guidelines for creating strong passwords:
  - Use passwords with upper and lower case letters
  - Don't just capitalize the first letter, but add other uppercase letters as well
  - Use a combination of uppercase, lowercase, numbers, and special characters
  - Create a password that can be typed quickly without having to look at the keyboard
  - This deters "shoulder surfers" from attempting to steal passwords
  - The more critical an account, the more frequently it should change

Source: Network Security Bible, 2nd Edition by Eric Cole

Password Policy

Create Good Passwords

- The following best practices provide additional guidelines for creating strong passwords:
  - Root and Administrator passwords should be changed more frequently than users' passwords
  - Never use the username in any form as a password
  - Never use first names, middle names, last names, initials, or nicknames as a password
  - Don't use words contained in dictionaries
  - Don't use personal information that is easily identified, such as pet names, children's names, car make or model, address, and so on
  - Don't use a password containing just numbers or characters
  - Don't write down passwords
  - Don't tell anyone a password
  - Don't use shared accounts
  - Don't use a password that is overly long
    - Long passwords are difficult to remember and it is more likely that it will have to be written down
  - Make a password easy to remember but hard for others to guess
  - Use passphrases instead of passwords
    - A passphrase is a sentence that you type in as a password
  - While it does take longer to type it, it is easier for the user to remember and harder for an attacker to guess

Source: Network Security Bible, 2nd Edition by Eric Cole

Password Policy

Audit Passwords

- Regular password auditing should be performed to check the strength of passwords and to enforce the password policy
- Make sure before performing any password auditing that approval is received from the legal department
- Once this is done, create a process for regular password auditing
- Password cracking tools such as Cain or John the Ripper can also be used
- When the password cracking is complete, note the passwords that do not follow the proper policy and lock out the accounts of those in violation
- Next, send an e-mail to the users of these accounts with a copy of the password policy
- Require them to sign a copy of the policy before unlocking the account
- Multiple violations may result in disciplinary action
- Be sure when performing password cracking to perform the cracking on an offline system and do not store the cracked passwords on a computer
- If these are forgotten and left on the system an attacker or malicious user may stumble across them and use them to the attacker's advantage

Source: Network Security Bible, 2nd Edition by Eric Cole

Content Checking

Content Checking

Overview

- Content inspection is a technique frequently employed by network-based data loss prevention solutions
- Content inspection involves examining data in order to identify:
  - regular expressions or patterns that are indicative of sensitive data
    - E.g., patterns used in social security and credit card numbers
  - keywords that indicate sensitivity
    - E.g., "confidential"
- Content inspection works by capturing data packets in transit on a network and analyzing their content for sensitivity
- Content inspection is useful when categorizing or classifying data
- Content inspection often includes pre-configured rules for payment card industry data (PCI), personally identifiable information (PII), protected health information (PHI), and other standards

Source: https://digitalguardian.com/blog/what-content-inspection

Content Checking

Overview

- In addition to the content-level inspection performed by the IDS, specific content inspection should also be performed on Web server traffic and other application traffic
- Some attacks evade detection by containing themselves in the payload of packets, or by altering the packet in some way, such as fragmentation
- Content-level inspection at the Web server or application server will protect against
  - attacks such as those that are tunneled within legitimate communications
  - attacks with malicious data
  - unauthorized application usage

Source: Network Security Bible, 2nd Edition by Eric Cole

Content Checking

Types of content checking

- Binary code in HTTP headers
- HTTP or HTTPS tunneling
- URL directory traversal
- Excessive URL header length
- Cross-site scripting
- Malicious URLs
- Inspect file transfers
- Inspect mail attachments

Source: Network Security Bible, 2nd Edition by Eric Cole

Content Checking

Benefits of Content Inspection

- Content inspection provides data visibility to help organizations see exactly where their PCI, PII, PHI, and other sensitive data resides and control how it is used
- Automatic identification and classification of sensitive data such as social security numbers, credit card information, and personal health data in files and emails – without human intervention
- Providing visibility into file and device activity on networks
- Restricting use to authorized users and devices
- Once data is classified and tagged through the content inspection process, data loss prevention solutions can monitor its use to enforce corporate policies and protect against intentional or accidental exfiltration of sensitive data from the corporate network

Source: https://digitalguardian.com/blog/what-content-inspection

Content Checking

Content Inspection Helps with Regulatory Compliance

- It has never been more critical to protect sensitive data than it is today
- Gaining full visibility into your data and knowing that it is correctly being classified is the first step toward protecting your data
- Content Inspection helps organizations meet regulatory compliance for data protection
- The content inspection process enables companies to comply with data protection regulations – such as PCI-DSS, HIPAA, FISMA, and others – by automatically encrypting or applying other protections to their regulated data
- Content inspection technologies provide visibility into where regulated and other sensitive data resides on the network, what users are accessing it, and how it's being used
- This visibility is critical for demonstrating compliance and is also helpful in passing security audits.

Source: https://digitalguardian.com/blog/what-content-inspection

Thank You!