Securing Your System
Computer Security

Peter Reiher

March 11, 2021

Putting It All Together

- We’ve talked a lot about security principles
- And about security problems
- And about security mechanisms
- And about bad things that have really happened
- How do you put it all together to secure your system?

Things That Don’t Work

- Just installing your machines and software and hoping for the best
- Simply buying a virus protection program and a firewall
- Patching something when you hear about a problem
- Running US government FISMA compliance procedures
  - Or any other paperwork-based method

Practicalities

- You don’t have the time or resources to do everything
- Your system isn’t the same as everyone else’s
- You should know by now that it isn’t a fix-once-and-forget problem
- In real systems, there are real constraints on what you can do

So What Will Work?

- One promising approach is outlined by SANS Institute
- Based on experiences of highly qualified security administrators
- The 20 Critical Security Controls
  - A checklist of things to watch for and actions to take
  - Technical, not policy or physical

The 20 Critical Security Controls

- Developed primarily by US government experts
- Put into use in a few government agencies
  - With 94% reduction in one measurement of security risk
- But nothing in them is specific to US government
- Prioritized list
- Based on 5 security tenets

Critical Tenets of Effective Cyber Security Defense

1. Offense informs defense
2. Prioritization
3. Metrics
4. Continuous diagnostics and mitigation
5. Automation

1. Offense Informs Defense

- Keep up to date on what attacks are really occurring
- Spend your efforts on defending against those attacks
  - Rather than against the "exciting" new attack nobody is really using

2. Prioritization

- Invest your efforts against attacks that pose the greatest risk to you
- Considering threat actors likely to attack you
- And the practicalities of taking the defensive measures

3. Metrics

- Establish security-meaningful metrics for your organization
- That make sense to all relevant parties
  - Executives as well as technical people
- Take actions based on what you measure

4. Continuous Diagnostics and Mitigation

- Continue measuring what’s happening at all times
- Expect to make changes in defensive mechanisms in response
- Validate that changes you make are effective in addressing what you measured

5. Automation

- Automate your defenses to the extent possible
- Also automate measurement of defenses
- And testing of defenses
- Vital for fast response and scalability

Nature of Controls

- General things to be careful about
  - Not specific bug fixes
- With more detailed advice on how to deal with each
  - Including easy things to do
  - And more advanced things if schedule/budget permits
- Mostly ongoing, not one-time

1. Inventory and Control of Hardware Assets

- Why is this important:
  - If you don’t know what you have, how can you protect it?
  - Even if you know, if you don’t control it, you can’t protect it
  - Attackers look for everything in your environment
  - New devices, experimental devices, “temporary” devices are often problems

Quick Win

- Install automated tools that look for devices on your network
- Active tools
  - Try to probe all your devices to see who’s there
- Passive tools
  - Analyze network traffic to find undiscovered devices
- Maintain an approved inventory of devices

2. Inventory and Control of Software Assets

- Why it's important:
  - Most attacks come through software installed on your system
  - Understanding what's there is critical to protecting it, as is being able to control it
  - Important for removing unnecessary programs, patching, etc.
- Looking for both authorized and unauthorized software

Quick Win

- Create a list of approved software for your systems
- Determine what you need/want to have running
- May be different for different classes of machines in your environment
  - Servers, clients, mobile devices, etc.
- Automatically check their integrity

3. Continuous Vulnerability Management

- Why it's important:
  - Most HW/SW default installations are highly insecure
  - So if you use that installation, you're in trouble the moment you add stuff
  - Previously secure installations become vulnerable if not updated

Quick Wins

- Create standard secure image/configuration for anything you use
- Based on configurations known to be good
  - E.g., those released by NIST, NSA, etc.
- Validate these images periodically
- Securely store the images
- Only allow updates to images over secure channels
- Use configuration management tools to enforce compliance

4. Controlled Use of Administrative Privilege

- Why it’s important:
  - Administrative privilege allows changes to system security
  - If you don’t control its use, unauthorized users can change things
  - Attackers commonly try to obtain admin privilege, once in your system

Quick Wins

- Change default passwords on all new installations, particularly those that run with high privilege
- Set up separate accounts for activities requiring admin privileges
  - Only to be used for administrative purposes
- Use multifactor authentication to obtain admin privileges (or at least strong passwords)
- Use automated tools to determine where admin privileges can be obtained

5. Secure Configurations for HW and SW Devices

- Why it’s important:
  - Default configs for many devices trade security for convenience
  - Individual users can’t develop or maintain secure configurations
  - So you need to provide them and enforce them

Quick Wins

- Maintain and document secure configurations for OS and other software
- Store secure configurations safely and monitor their status
- Develop management tools to periodically deploy secure configs to all devices

6. Maintenance, Monitoring and Analysis of Security Logs

- Why it's important:
  - Logs are often the best (sometimes only) source of info about attack
  - If properly analyzed, you can learn what's happening on your machines
  - If not, you're in the dark

Quick Wins

- Ensure all devices perform logging
- Ensure log entries contain all necessary information
- Ensure you have enough disk space for your logs
- Review logs regularly
- Use automated tools to correlate and analyze logs

7. Email and Web Browser Protection

- Why it's important:
  - Most successful attacks come through these vectors
  - Both social engineering and vulnerability exploitation
  - And most enterprises need to allow these activities

Quick Wins

- Only permit approved up-to-date versions of browsers, email clients, and extensions
- Use DNS filtering to prevent visiting known dangerous sites
- Limit use of scripting languages
- Log all outgoing URL requests
- Use a spam filtering tool on email and use the DMARC policy and verification
- Block unnecessary email attachments

8. Malware Defenses

- Why it's important:
  - Malware on your system can do arbitrary harm
  - Malware is becoming more sophisticated, widespread, and dangerous
  - Malware changes rapidly, so your defenses must, too

Quick Wins

- Run malware detection tools on everything and report results to central location
  - Update signature-based tools at least daily
- Limit use of external devices
  - Don't allow autorun from flash drives, etc.
  - Automatically scan removable media on insertion
- Use DEP, ASLR, virtualization, etc.
- Analyze malware detection events at a centralized site, not just locally

9. Limitation and Control of Ports, Protocols, and Services

- Why it's important:
  - Attackers look for entries to your systems
    - Especially obscure ones
  - Software is often installed automatically, in weak configurations
  - If you don't need and use them, why give attackers' that benefit?

Quick Wins

- Only run services that you actually need
  - Drop ports and protocols for any others
- Use host-based and app-specific firewalls with default deny rules on all systems
- Do automated port scan to compare against known intended server configuration
- Verify which services are visible from outside your organization

10. Data Recovery Capability

- Why it's important:
  - Successful attackers often alter important data on your machines
  - Sometimes that's the point of the attack (e.g., ransomware)
  - You need to be able to get it back

Quick Wins

- Back up all machines regularly
- Back up critical systems as system images, for fast restoration
- Ensure physical and cryptographic security of backups
- Make sure critical data has a backup not accessible from the machine’s OS
- Test restoration from backups often

11. Secure Configurations for Network Devices

- Why it's important:
  - Firewalls, routers, and switches provide a first line of defense
  - Even good configurations tend to go bad over time
    - Exceptions and changing conditions
  - Attackers constantly look for flaws in these devices

Quick Wins

- Make sure all such devices have the most recent security patches installed
- Create documented configurations and rules for these devices
  - Periodically check devices against them
  - Document changes to rules
  - Verify with automated tools
- Use two factor authentication and encryption to manage these devices
  - From a dedicated secure machine

12. Boundary Defense

- Why it's important:
  - A good boundary defense keeps many attackers entirely out
  - Even if they get in, proper use of things like a DMZ limits damage
  - Important to understand where your boundaries really are

Quick Wins

- Know where all your boundaries are
  - Periodically scan them from outside
- Allow only authorized protocols to transit your boundaries
- Black list known bad sites or white list sites you need to work with
- Use a network IDS/IPS to watch traffic crossing your boundaries
- Enable logging at boundary machines

13. Data Protection

- Why it’s important:
  - Many high impact attacks are based on your data being stolen
  - You need to encrypt such critical data so its loss is minimized
  - You need to know when critical data is leaving your custody
  - You need to understand how and why that happens

Quick Wins

- Know which data you have that is critical
  - Encrypt it over the network
  - Ensure its integrity
- Use full disk encryption
  - On all mobile devices, particularly those holding critical data
- Don't connect infrequently used data or systems to your network
  - Connect them only when needed

14. Controlled Access Based on Need to Know

- Why it's important:
  - If all your machines/users can access critical data,
  - Attacker can win by compromising anything
  - If data kept only on protected machines, attackers have harder time

Quick Wins

- Apply proper access control to all data
- Put all sensitive information on separate VLANs
  - Filter data moving between VLANs
  - Don’t allow workstation-to-workstation traffic
- Encrypt all sensitive information in transit
  - Even your own internal network
- Remove inactive data sets from production network

15. Wireless Access Control

- Why it’s important:
  - Wireless reaches outside physical security boundaries
  - Mobile devices “away from home” often use wireless
  - Unauthorized wireless access points tend to pop up
  - Historically, attackers use wireless to get in and stay in

Quick Wins

- Know and control what wireless devices are in your environment
- Separate VLAN for BYOD
- Use AES encryption on wireless LANs
- Use wireless IDS and scanning to detect unauthorized or badly configured devices
- Disable peer mode and unnecessary wireless peripheral device access

16. Account Monitoring and Control

- Why it's important:
  - Inactive accounts are often attacker's path into your system
  - Nobody's watching them
  - Sometimes even "left behind" by dishonest employees

Quick Wins

- Review your accounts and disable those with no current owner
  - Set expiration date on all accounts
  - Create procedure to quickly delete accounts of departed employees
- Monitor account use
- Use screen locks for unattended devices and log off inactive sessions

17. Implement a Security Awareness and Training Program

- Why it's important:
  - Attackers target untrained users
  - Defenders need to keep up on trends and new attack vectors
  - Programmers must know how to write secure code
  - Need both good base and constant improvement

Quick Wins

- Implement a security awareness program for employees
  - Update it regularly
- Train employees
  - To use strong authentication
  - To recognize and report common attacks
  - To properly handle important data
- Periodically test security awareness

18. Application Software Security

- Why it’s important:
  - Security flaws in applications are increasingly the attacker’s entry point
  - Both commodity applications and custom in-house applications
  - Applications offer large attack surfaces and many opportunities

Quick Wins

- Use only supported versions of software and keep them patched
- Install and use web-knowledgeable firewalls
- Install non-web application specific firewalls, where available
- Establish secure design and coding practices and train employees in them

More Quick Wins

- For in-house software, ensure it checks properly for errors
- Use automated testing methods and tools to check security of in-house software
- Maintain separate production and development systems
- Use only standard and accepted cryptographic algorithms and implementations
- Establish procedures for reporting vulnerabilities (including externally)

19. Incident Response Capability

- Why it’s important:
  - You’ll be attacked, sooner or later
  - You’ll be happier if you’re prepared to respond to such incidents
  - Saving you vast amounts of time, money, and other critical resources

Quick Wins

- Create written response procedures, identifying critical roles in response
- Ensure you have assigned important duties to particular employees
- Set policies on how quickly and thoroughly problems should be reported
  - Ensure employees know about them
- Know which third parties can help you
- Test procedures periodically

20. Penetration Tests and Red Team Exercises

- Why it's important:
  - You probably screwed up something
    - Everybody does
  - You'll be happier finding out what if you do it yourself
  - Or have someone you trust find it

Quick Wins

- Regularly perform penetration testing
  - From both outside and inside your system boundaries
  - With clear goals
- Carefully control user accounts and software used for penetration testing
- Look for unprotected information helpful to attackers

Applying the Controls

- Understand all 20 controls well
- Analyze how well your system already incorporates them
- Identify gaps and make a plan to take action to address them
  - Quick wins first
  - Those alone help a lot

Creating an Ongoing Plan

- Talk to sysadmins about how you can make further progress
- Create long term plans for implementing advanced controls
- Think for the long haul
  - How far along will you be in a year, for example?

20 Controls Is a Lot

- What if you can’t take the time for even the quick wins on these 20?
- You have just a little time, but you want to improve security
- What to do?

The Australian Signals Directorate Controls

- A body of Australia’s military
- They have a list of 35 useful cybersecurity controls
- Well, if 20 is too many, 35 certainly is
- But they also have prioritized just 4 of them

The ASD Top 4 Controls

1. Application whitelisting
2. Patch your applications
3. Patch your OS
4. Minimize administrator privileges

- In ASD’s experience, handling these four stops 85% of attacks

1. Application Whitelisting

- Only allow approved applications on your machines
- Use a technology to ensure others do not get installed and run
- Identify apps you actually need to run to do your business
- Outlaw all the others

Enforcing Whitelists

- If running Windows, you can use Microsoft AppLocker
  - Available with post-Windows 7 OSes
- Prevents apps not on the whitelist from running
- More challenging if you’re running Linux
  - MacAfee Application Control or configurations of SE Linux are possible
- Mac OS whitelisting also not perfect
  - Parental controls or whitelisting all apps signed by MacStore or identified developer

2. Patch Your Applications

- Apply patches to all applications you use
  - Especially those interacting with Internet
- Prefer up-to-date versions of software
  - Older versions may not have patches provided
- Ideally have a centralized method controlling patches for entire system
  - E.g., for Windows, Microsoft System Center Configuration Manager

3. Patch Your Operating System

- Go with most up-to-date releases of OS
  - E.g., desktop malware infections dropped 10x from XP to Windows 7
- Use system-wide tools that will apply patches to all machines you control
  - Microsoft System Center Configuration Manager, again
  - Similar tools available for Linux

4. Minimize Administrator Privilege

- Get rid of methods allowing users to alter their environments
  - Especially those allowing software installation
- Malicious intruders look for these capabilities
- Those allowing access to other machines especially dangerous

Further Controlling Administrator Privileges

- Use role based access control for admin privileges
  - If not available, separate accounts
  - Not normal administrator user accounts
- Avoid allowing admin accounts to have Internet access

Conclusion

- You can’t perfectly protect your system
- But you can do a lot better than most
  - And the cost need not be prohibitive
- At worst, you can make the attacker’s life hard and limit the damage
- These steps work in the real world