Securing Your System
Computer Security
Peter Reiher
June 2, 2016

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

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
- Rolling out to other government agencies
- But nothing in them is specific to US government
- Prioritized list

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

How The SANS List Is Organized

- For each control,
  - Why it's important
  - Quick win
  - Visibility/attribution
  - Configuration/Hygiene
  - Advanced
- With a little text on each
- Not all categories for all controls

1. Inventory of Devices on Your System

- Why is this important:
  - If you don't know what you have, how can you protect it?
  - Attackers look for everything in your environment
  - Any device you ignore can be a point of entry
  - New devices, experimental devices, "temporary" devices are often problems
  - Users often attach unauthorized devices

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

2. Inventory of Software on Your System

- Why it's important:
  - Most attacks come through software installed on your system
  - Understanding what's there is critical to protecting 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 machines, etc.

3. Secure Configurations for Hardware and Software

- 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
  - Also an issue with keeping configurations up to date

Quick Wins

- Create standard secure image/configuration for anything you use
- If possible, base it on configuration known to be good
  - E.g., those released by NIST, NSA, etc.
- Validate these images periodically
- Securely store the images
- Run up-to-date versions of SW

4. Continuous Vulnerability Assessment and Remediation

- Why it's important:
  - Modern attackers make use of newly discovered vulnerabilities quickly
  - So you need to scan for such vulnerabilities as soon as possible
  - And close them down when you find them

Quick Wins

- Run a vulnerability scanning tool against your systems
  - At least weekly, daily is better
- Fix all flaws found in 48 hours or less
- Examine event logs to find attacks based on new vulnerabilities
  - Also to verify you scanned for them

5. Controlled Use of Administrative Privileges

- Why it's important:
  - Administrative privilege gives attackers huge amounts of control
  - The more legitimate users who have it, the more targets
    - Phishing attacks, drive-by downloads, password guessing, etc.

Quick Wins

- Use automated tools to validate who has administrative privileges
- Ensure all admin password/phrases are long and complex
  - Force them to change often
- Change all default passwords on new devices
  - Firewalls, wireless access points, routers, operating systems, etc.

More Quick Wins

- Store passwords hashed or encrypted
  - With only privileged users allowed to access them, anyway
- Use access control to prevent administrative accounts from running user-like programs
  - E.g., web browsers, games, email
- Require different passwords for personal and admin accounts

Yet More Quick Wins

- Never share admin passwords
- Discourage use of Unix *root* or Windows *administrator* accounts
- Configure password control software to prevent re-use of recent passwords
  - E.g., not used within last six months

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 machines have reasonably synchronized clocks (e.g., use NTP)
- Include audit log settings as part of standard configuration
  - And check that
- Ensure you have enough disk space for your logs

More Quick Wins

- Use log retention policy to ensure you keep logs long enough
- Fully log all remote accesses to your machines
- Log all failed login attempts and failed attempts to access resources

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

- Make sure all users' browsers are up to date on patches
- Remove non-essential components from web servers and keep essential ones updated
- Turn on pop up blockers and don't accept third party cookies
- Use a spam filtering tool on email and use the Sender Policy Framework

8. Malware Defenses

- Why it's important:
  - Malware on your system can do arbitrary harm
  - Malware is becoming more sophisticated, widespread, and dangerous

Quick Wins

- Run malware detection tools on everything and report results to central location
- Ensure signature-based tools get updates at least daily
- Don’t allow autorun from flash drives, CD/DVD drives, etc.
- Automatically scan removable media on insertion
- Scan all email attachments before putting them in user mailboxes

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

- Why it's important:
  - Many systems install software automatically
  - Often in weak configurations
  - These offer attackers entry points
  - If you don't need and use them, why give attackers' that benefit?

Quick Wins

- Turn off unused services
  - If no complaints after 30 days, de-install them
- Use host-based firewalls with default deny rules on all systems
- Port scan all servers and compare against known intended configuration
- Remove unnecessary service components

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
  - You need to be able to get it back

Quick Wins

- Back up all machines at least weekly
  - More often for critical data
- Test restoration from backups often
- Train personnel to know how to recover destroyed information

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

- Create documented configurations for these devices
- Periodically check actual devices against your standard configurations
- Turn on ingress/egress filtering at Internet connection points

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

- Black list known bad sites or white list sites you need to work with
  - Test that periodically
- Use a network IDS to watch traffic crossing a DMZ
- Use the Sender Policy Framework (SPF) to limit email address spoofing

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

- Use full disk encryption
  - On all mobile devices
  - On all devices holding particularly critical data
- Other measures are more advanced

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

- Put all sensitive information on separate VLANs
- Encrypt all sensitive information crossing the network
  - Even your own internal 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 what wireless devices are in your environment
- Make sure they run your configuration
- Make sure you have administrative control of all of them
  - With your standard tools
- Use network access control to know which wireless devices connect to wired network

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
- Produce automatic daily report on all old/unused/expired accounts
- Create procedure to quickly delete accounts of departed employees

More Quick Wins

- Monitor account usage to find dormant accounts (disable them eventually)
- Encrypt and move off-line all files belonging to dormant accounts
- Lock out accounts after some modest number of consecutive failed login attempts

17. Security Skills Assessment and Training

- 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

- Assess what insecure practices your employees use and train those
- Include appropriate security awareness skills in job descriptions
- Ensure policies, user awareness, and training all match

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

- Install and use special web-knowledgeable firewalls
  - To look for XSS, SQL injection, etc.
- Install non-web application specific firewalls, where available
- Position these firewalls so they aren't blinded by cryptography

19. Incident Response Capability

- Why it's important:
  - Probably you'll be attacked, sooner or later
  - You'll be happier if you're prepared to respond to such incidents
  - Can save 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 problems should be reported
- Know which third parties can help you
- Make sure you employees know what to do when there's a problem

20. Penetration Testing 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
- Keep careful control of any user accounts and software used for penetration testing

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