6. 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

7. Wireless Device 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

8. 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

9. 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

10. 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

11. 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

12. 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

13. 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

14. 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

15. 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