Security in Industry

Trade off between:

- Security

and

- Cost
- Convenience
- Usability

1 Security in Large Corporations

Locked down environments:

- Software has to be pre-vetted before being installed
- Often will have VMs/OS images with everything setup
- Network policies will be very strict

General security policies

- Need to have badge and swipe everywhere you go
- Very secure areas will be monitored/locked down
- Usually very locked down by default - need to escalate to managers to get approval
- Clean desk policy
- Heavy monitoring of production servers

Laptop security policies

- Screen locks
- Encrypted HDD
- Kensington locks
- Monitoring software

2 Attacks on Large Corporations

- Out of date software
- Exploit single server running software with security flaw
- Social engineering

3 Best practices

3.1 Login credentials

- Use strong hash function for passwords
- Salt passwords
- Secure your email and password database
  - No outside access
  - Limit who can access this server
  - Encrypt if possible

3.2 MFA

Pick at least 2 from:

- Something you know
- Something you have
- Something you are

3.3 Web Dev

- Add SRI checks on all 3rd party resources
- Keep software up to date
  - This is very important
  - Build in time to do this in estimates
  - OS deps, language, frameworks - all are important
- Use well maintained framework for web development
- Limit what users can upload
  - XSS attacks
  - SQL injections
  - CSRF attacks
- Never execute input from user directly
- Use a strongly typed language
- Keep it simple

4 AWS Security

- Port scanning is a good idea
- Security Groups allow for good security
  - Clump nodes together
  - Connection-oriented (only have to allow outbound for outbound TCP request)
- VPCs are complex but powerful
  - Network-level security
  - Now even work between AWS regions
- IAM profiles are very useful for security
  - Only give access to particular resources
- Use ELBs/ALBs with HTTPS enabled
  - Simple to setup and performant
  - Scales automatically
  - No need to deal with certs in application

5 Software Dependencies

Trust and package managers

- System packages vs programming language packages, which is safer?
  - GPG checks ensure that package you download was uploaded by maintainer
  - Usually system packages have to go through rigorous vetting process
  - Linux has been decades ahead of windows and mac os on this front

6 Anti-patterns

- Automatic minor version updates
- Depending on a lot of packages
  - Each dependent package is a liability
- Using packages which are no longer actively maintained
- Installing dependencies directly on servers:
  - This is bad for speed and security
  - Instead: bundle up dependencies with app using package/container/system image

7 Personal Security: Best practices

- Use 2FA
- Use secure apps
- Use a password manager
- Use TOR/SSH tunneling if you are on an unsafe connection
- Use an ad blocker
- Use Linux
- Go to conferences