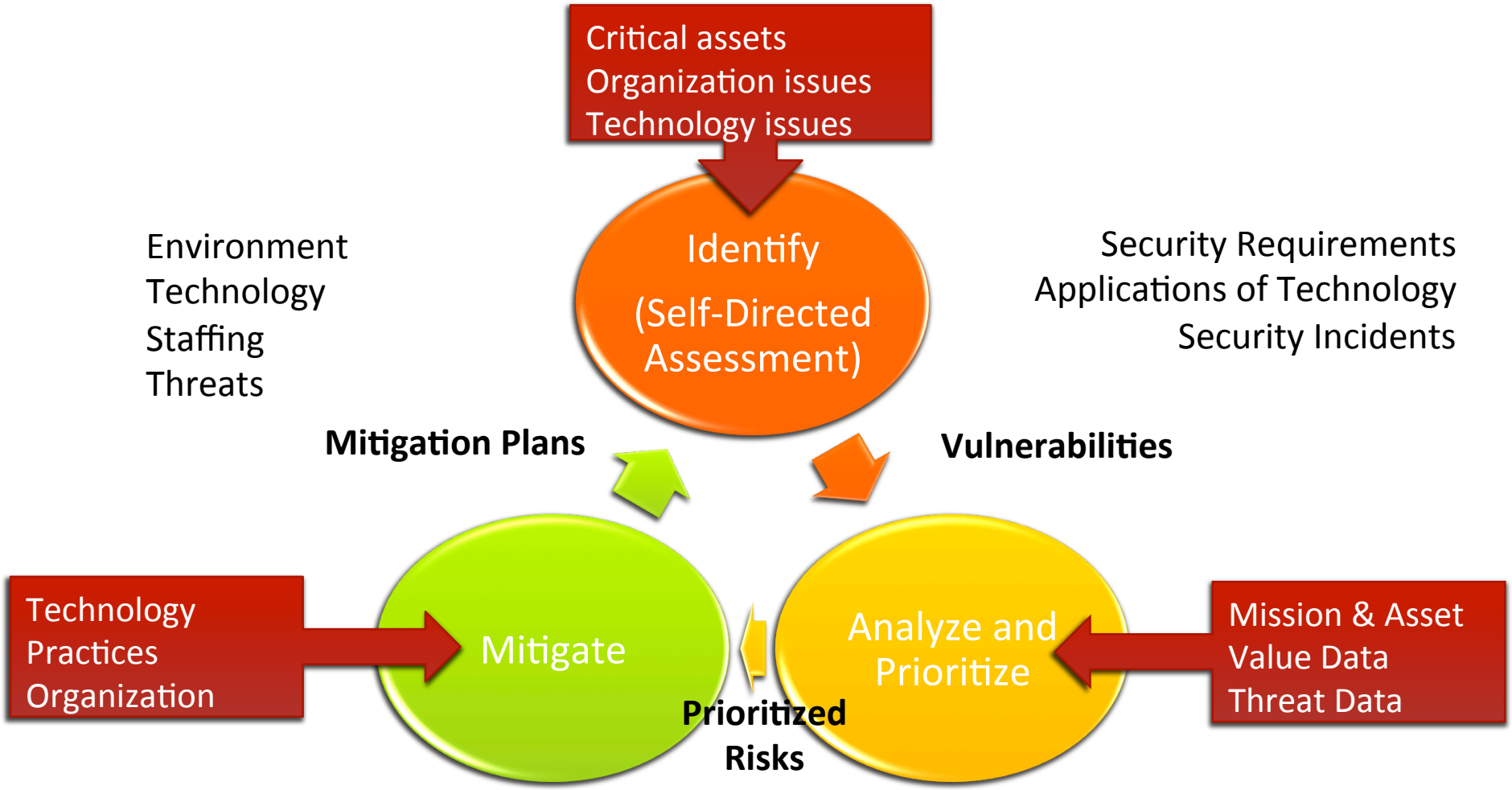
But there is Hope!

- Strong market for security professionals will eventually drive graduate and certificate programs.
- Increased understanding by technology users will build demand for quality security products; vendors will pay attention to the market.
- Insurance industry may provide incentives for improved business security practices.
- Technology will continue to improve and we will figure out (be educated on) how to use it: e.g., encryption, strong authentication, survivable systems
- Due diligence would go a Long-way: according to CERT/CC, 99% of Intrusions resulted from exploitation of known vulnerabilities or configuration errors where countermeasures were available (aka Religiously keep up with the Patches but …)
- Increased collaboration across government and industry.
  - Legislation on Software Liability Law ??
  - Government Procurement Standards ??

Introduction (Part 2)

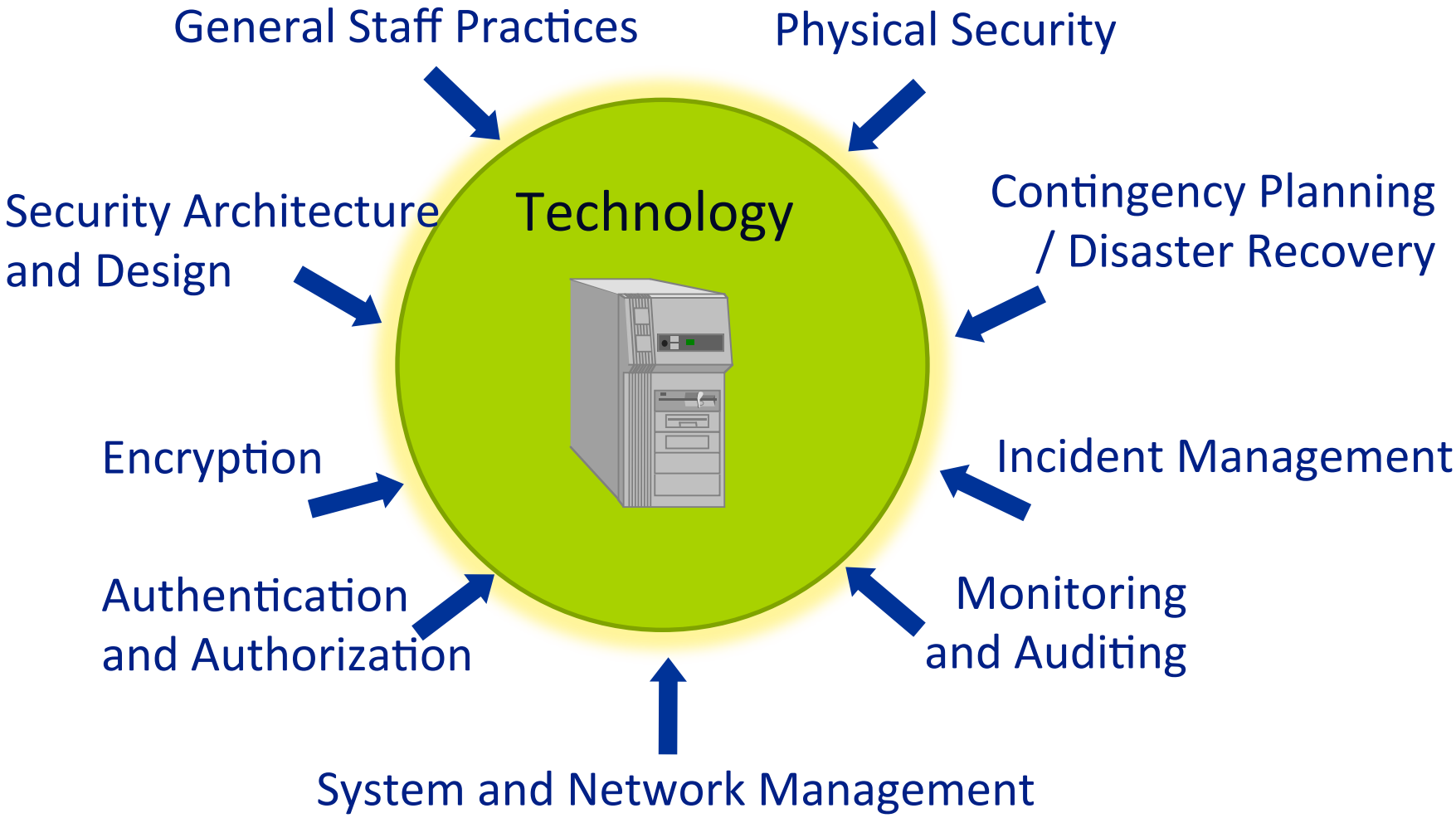
- Risk management
- Security engineering
  - Threat model / Security goals
  - Security policy
  - Security practice
- Security goals
- Many Facets of Cyber Security
  - Really, what can go wrong?
- Concluding Remarks

What can we do *now*?

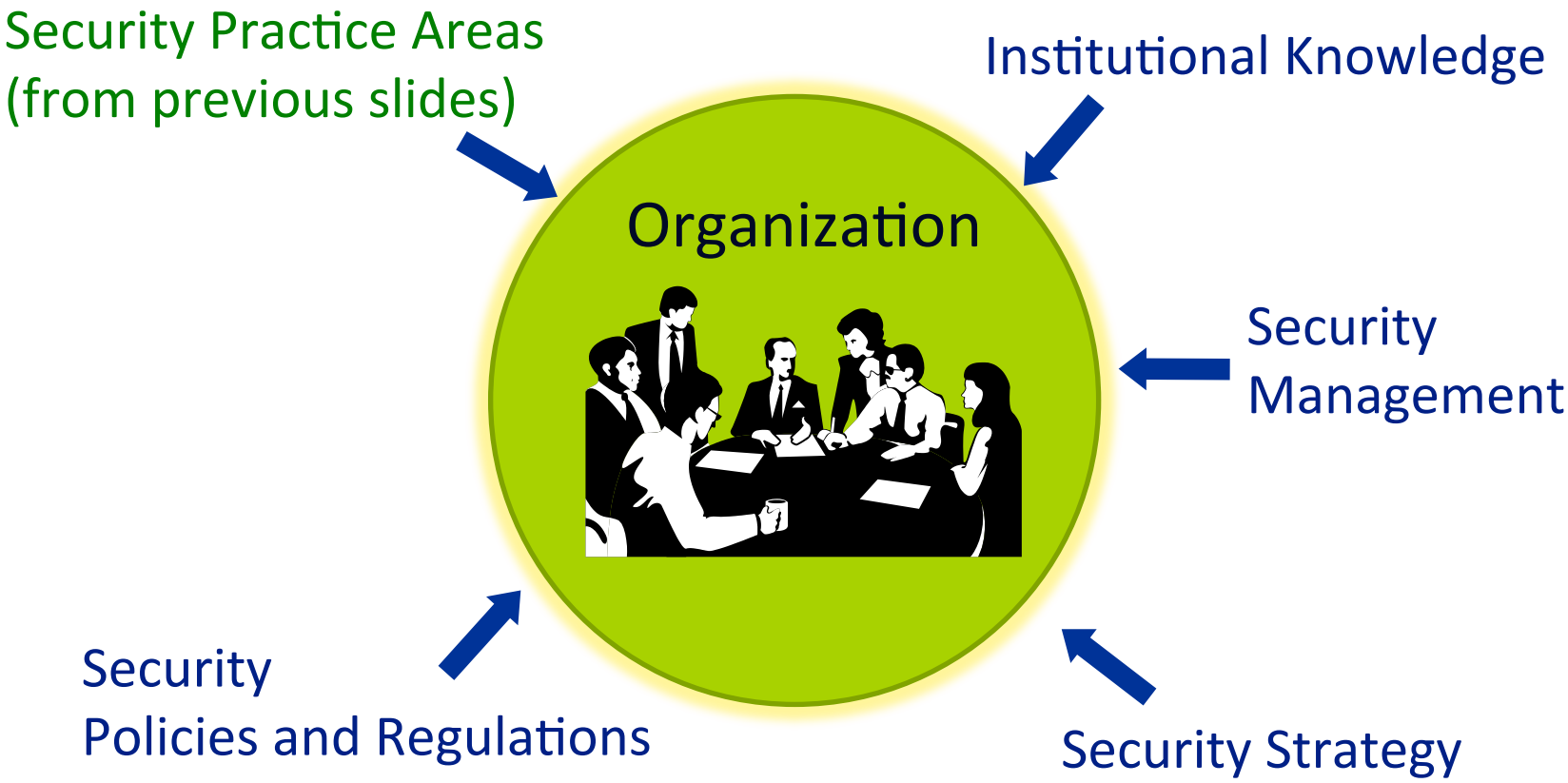


- Establish a Risk Management Process

Security Practice Areas



Go Beyond "Technology Only"



Intuitive Strategies ensuring Security

- Prevention: take measures that prevent your assets from being damaged
  - E-commerce as example: encrypt your orders, rely on the merchant to perform checks on the caller, don't use the Internet! :P
- Detection: take measures so that you can detect when, how, and by whom an asset has been damaged.
  - an unauthorized transaction appears on your credit card statement!
- Reaction: take measures so that you can recover your assets or to recover from a damage to your assets.
  - complain, ask for a new card (number), etc.

Security Engineering: Three Steps

- A methodology for tackling an information protection / assurance problem

1. Drawing up a threat model
2. Formulating a suitable security policy modelling what ought to be protected
3. Implementing specific protection mechanisms to enforce the policy

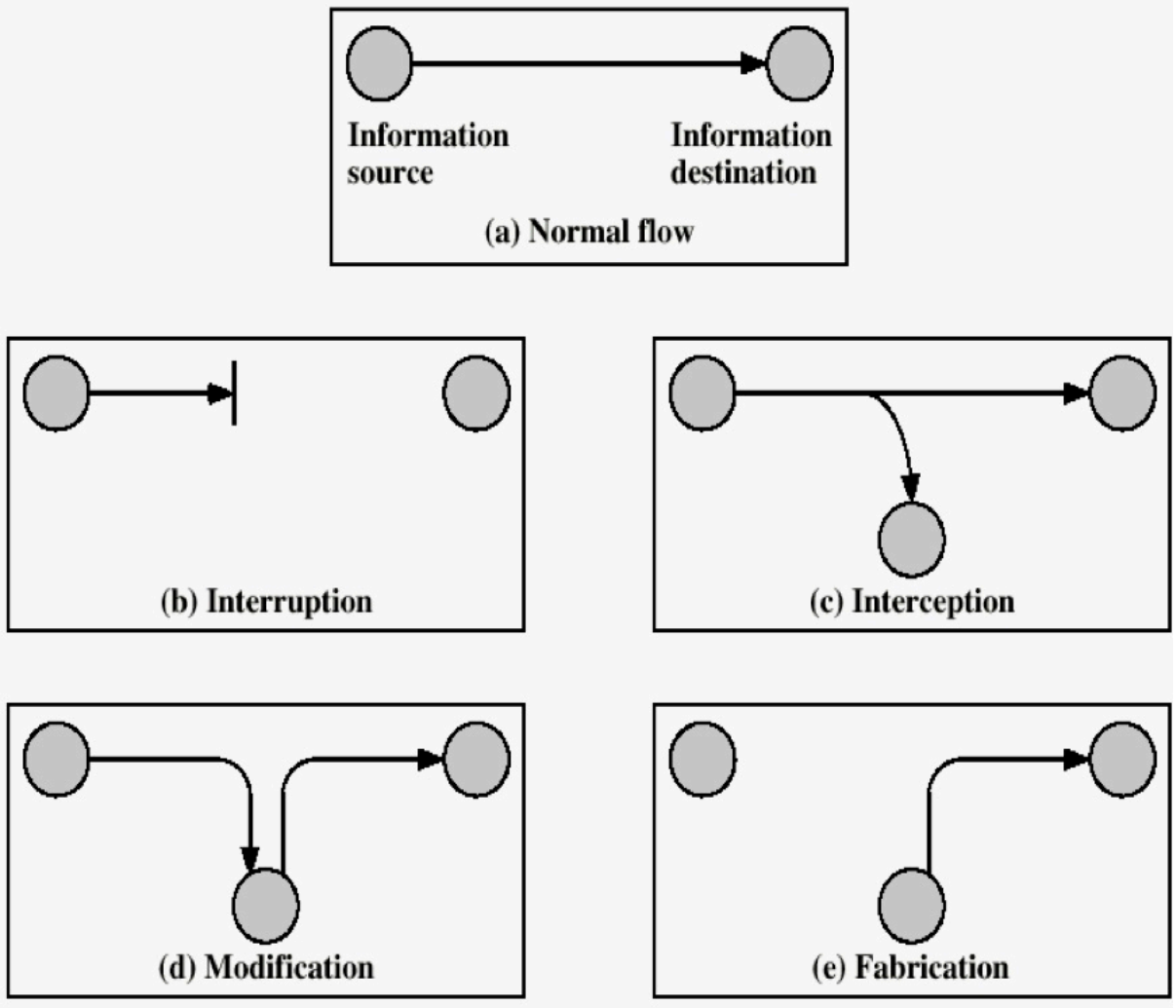
Drawing up a Threat Model

- Draw up via security requirement analysis

1. Identify assets to be protected and their value
2. Identify vulnerabilities, threats, and risk priorities
3. Identify legal and contractual requirements

Digression: Classification of Threats

- Leakage
- Tampering
- Vandalism

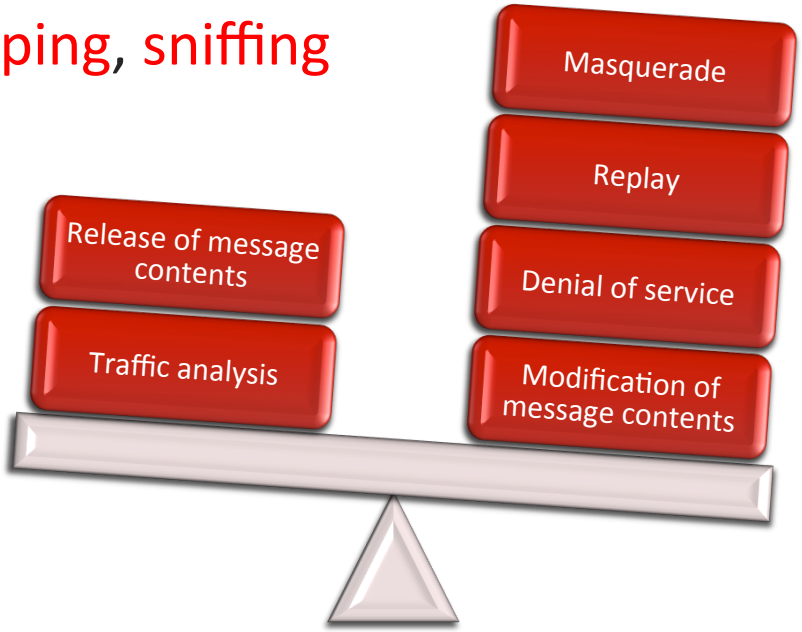


Further Classification

Passive Threats

Active Threats

- via eavesdropping, sniffing



Goals: CIA Triad

Goals / Services provided by Security

- Confidentiality (for your eyes only) vs. eavesdropping, sniffing, tracing
- Integrity (has not be altered) vs. tampering
- Authentication (you are who you say you are)
  vs. impersonation, masquerading, spoofing
- Access control (only the intended can "use" the resources)
  vs. unauthorized use / abuse of resources
- Non-repudiation (the order is final)
  vs. denying one's act, backing away from a deal
- Availability vs. (D)DoS attacks

Variants of Confidentiality

- Anonymity: ability to use a resource without disclosing identity/ location
- Copy protection: ability to control the use of information
- Information flow control: ability to control the flow of information
- Privacy: fair collection and use of personal data

More Variant of Confidentiality

- Unobservability: ability to use a resource without revealing this activity to third parties
- Information hiding, steganography (hidden writing, hiding message in other messages) e.g., digital watermarking
- *Cryptography* vs. *Steganography*
  - The former protects the content of messages
  - The latter conceals their very existence

Variants of Anonymity

- Pseudonymity: anonymity with accountability for actions
- Unlinkability: ability to use a resource multiple times without others being able to link these uses together
  - e.g., that girl in 4130 class is the same as that girl in 5310 class?
  - cf., HTTP “cookies” were introduced to provide linkability

Formulating a Suitable Security Policy

1. Which activities are or are not authorized
   Which states are or are not required, and
   Which information flows are or are not prohibited
2. Precise and even formal definition of such protection goals
   (E.g. procedural instructions for employees)
3. Should be well documented and followed

Digression: Security Policy

- "A security policy is a formal statement of the rules by which people who are given access to an organization's technology and information assets must abide"
- - From RFC 2196, Site Security Handbook

Why Create a Security Policy?

- To baseline your current security posture
- To set the framework for security implementation
- To define allowed and disallowed behaviors, practices
- To help determine necessary tools, and procedures
- To communicate consensus and define roles throughout the organization
- To define how to handle security incidents

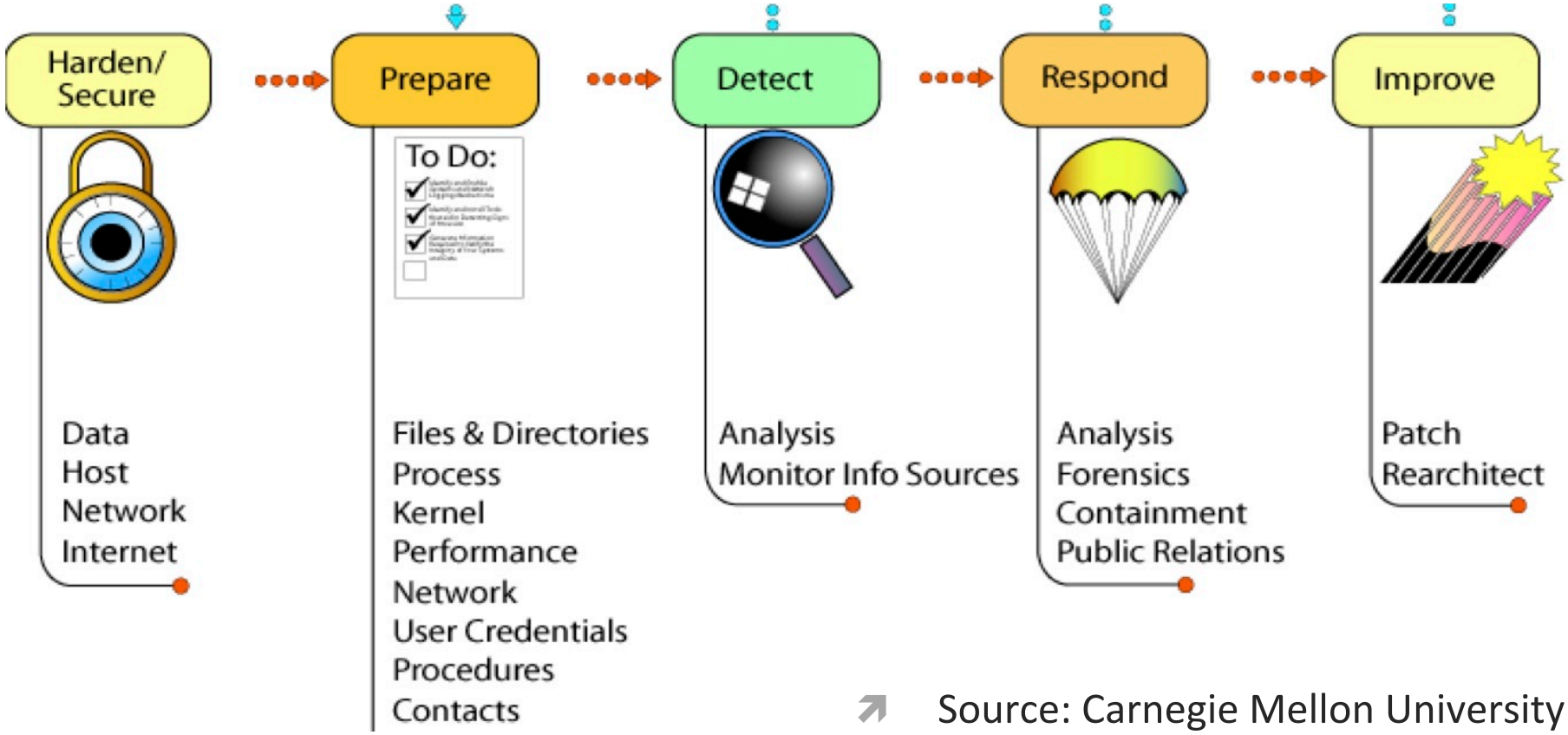
What should the Security Policy Contain?

- Statement of authority and scope
- Acceptable use policy
- Identification and authentication policy
- Internet use policy
- Campus access policy
- Remote access policy
- Incident handling procedure

Implementing Protection Mechanisms

- Is that all? Critical steps missing?
- Which step sounds the most difficult to you?

Security Practices Structure



Source: Carnegie Mellon University

Harden / Secure

- Install the minimum essential operating system and all applicable patches
- Remove all privilege/access and then add back in only as needed (“deny first, then allow”)
- Address user authentication mechanisms, backups, virus detection/eradication, remote administration, and physical access
- Record and securely store integrity checking (characterization) information

Prepare

- Identify and prioritize critical assets, level of asset protection, potential threats, detection and response actions, authority to act.
- Identify data to collect and collection mechanisms
- Characterize all assets, establishing a trusted baseline for later comparison
- Identify, install, and understand detection and response tools
- Determine how to best capture, manage, and protect all recorded information

Detect

- Ensure that the software used to examine systems has not been compromised
- Monitor and inspect network and system activities
- Inspect files and directories for unexpected changes
- Investigate unauthorized hardware
- Looks for signs of unauthorized physical access
- Initiate response procedures

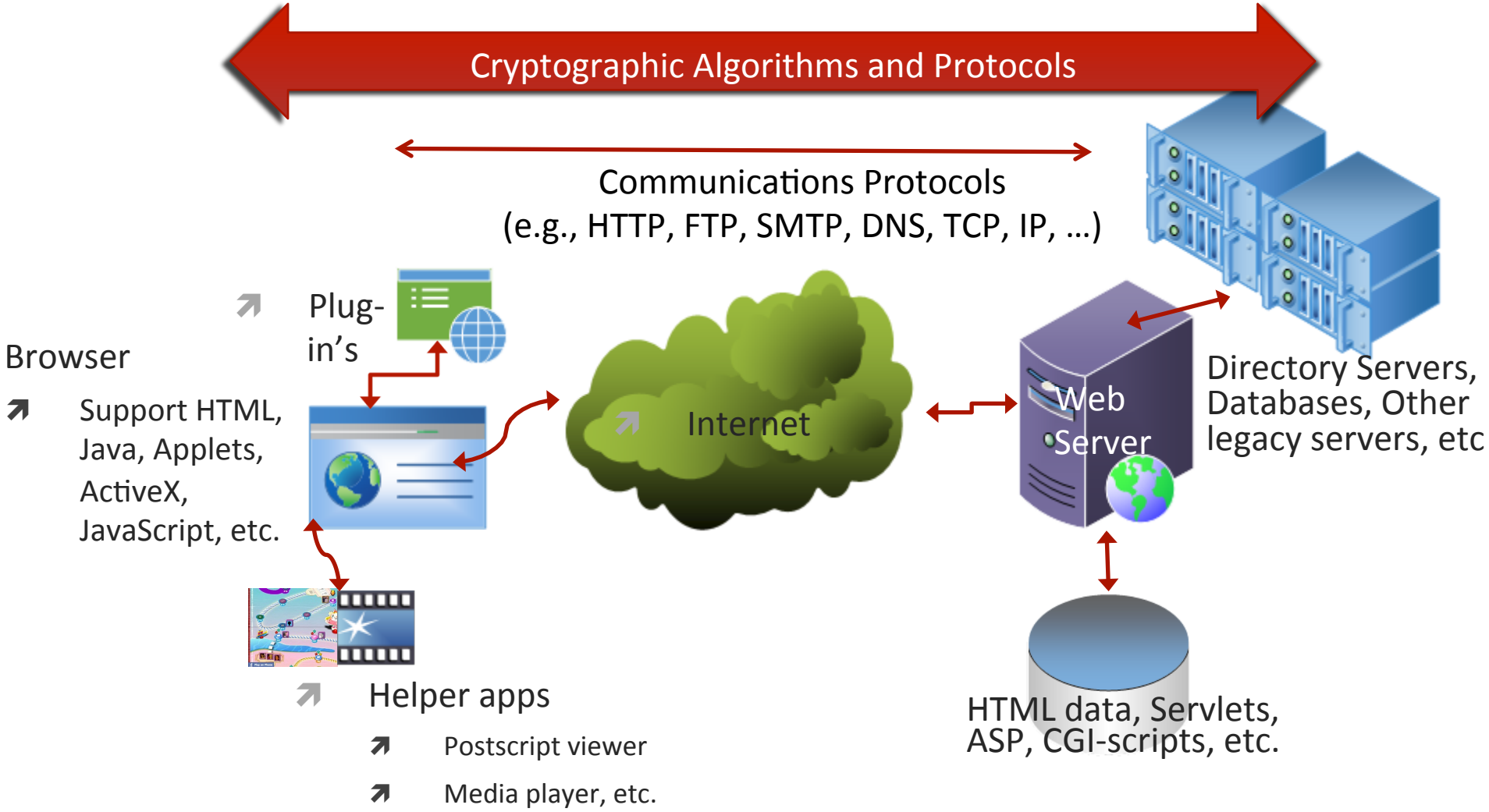
Respond

- Analyze all available information; determine what happened
- Disseminate information per policy, using secure channels
- Collect and preserve evidence, including chain of custody
- Contain damage
- Eliminate all means of intruder access
- Return systems to normal operation

Improve

- Identify lessons learned; collect security business case information
- Install a new patch (re-harden); uninstall a problematic patch
- Update the configuration of alert, logging, and data collection mechanisms
- Update asset characterization information
- Install a new tool; retire an old tool
- Update policies, procedures, and training

Many Facets of Cyber Security



What are the Problems?

- A Multitude of Insecure but widely-used protocol / services
  - IP, telnet, ftp, snmp, smtp
- Known and weak default settings
  - Passwords, SNMP community strings
- System / Protocol Design Errors
  - Setup and Access control errors
  - Improper application (combination) of Algorithms or Services
    - Misuse of RC4 in IEEE 802.11 Wireless LAN WEP; in MS Word, Excel
      - https://cs.uwaterloo.ca/~iang/pubs/wep-mob01.pdf
      - http://eprint.iacr.org/2005/007
    - Error-correcting encoding before encryption in GSM streaming cipher

More Problems

- Software Design / Implementation Flaws, e.g.,
  - Random seed derivation from process ID and real-time clock of early SSL in Netscape (unknown is the value of microseconds: 2^{20} possibilities)
  - Million-packet attack on SSL due to information-leaking in error message per PKCS ("oracle attack")
  - Lack Input validation and sanity checks
    - Buffer-overflow
    - CGI-script attacks
- Design Flaws in Cryptographic algorithms and Protocols, e.g.,
  - MD5, SHA1 both got "cracked" in summer '04 and Feb '05 resp.
  - MD5 (de facto industry standard, widely implemented/deployed) was totally broken by the end of '08 after published/used for > 15 years

(Probably) The Weakest Link

- End Users (esp. due to popular use of email and web browser)
  - under-educated
  - unaware of the profound security implications of what they do
  - also applies on software designers/developers!
- Ease-of-Use and Security are often at odds
  - Software/Hardware vendors often try to minimize the no. of phone calls to their help-line
  - by shipping products with “convenient” default settings
  - at the expense of exposing under-educated end-users of potential security threat

Countermeasures

- Cryptography Algorithms and Secure Procedures/Protocols
- Secure communications/networking protocols
- Practicing Secure Programming Techniques
- Building Secure Software
- Configuration Management and Monitoring Tools
  - Software Controls (access limitations in a data base, in operating system protect each user from other users)
- Authentication tools (smartcard)
- Security Perimeter Controls and Patrol (locks, firewall, Intrusion Detection, Virus Scanner)
- Policies (frequent changes of passwords)

Some Closing Thoughts

- Security is about Risk Management.
  - You cannot 100% eliminate all existing risks.
  - You can only better manage them with the given resources.
- Security is a Process.
  - It is not a piece of software or a box of hardware.
  - There is NO turn-key solution for providing Security for an Organization.
- Always Think Paranoid, *and*
- Practice Defense-in-depth (a.k.a. Belts and Suspenders)
- Education is Paramount !!
  - Not only for end-users
  - but also for programmers, engineers who are not security specialists !!