

Security Decision Making and Risk Management

Jeff King

May 22, 2007

What is Security?

- Classic definition:

A state of well-being of information and infrastructures in which the possibility of successful yet undetected theft, tampering, and disruption of information and services is kept low or tolerable.

- Not a binary state (secure / insecure)
- How low is *low*? How tolerable is *tolerable*?

What is Security?

- Security is a cyclical *process*.
 1. Inspection – evaluate the current status and appropriate levels of security (i.e., risk analysis)¹
 2. Protection – proactive process of creating an environment that is as secure as possible
 3. Detection – reactive process of determining inappropriate activities and alerting responsible individuals.
 4. Reaction – responding to a security incident, minimizing the impact.
 5. Reflection – follow-up processes necessary to evaluate the quality of the security implementation, and improve for the next iteration.
- How frequently should the cycle repeat?

¹Definitions from Pipkin, “Information Security”

A Security Example

You're a Tech student, living in an off-campus apartment with a roommate. To make some extra money, you set up a website where other students can meet and discuss class assignments. You make money from ads displayed on the site. The site runs on a server in your bedroom, connected through your DSL line.

Inspection

- Identify *threats, vulnerabilities, assets*.
- Assign *probabilities, consequences and values*.
- Consider *countermeasures or controls*, and their *costs*.
- Calculate *expectation* of different actions.

- Example:

Your site brings in \$300/month. One threat is an attacker breaking in to the webserver. If this happens, you expect the downtime to be a few days. You estimate the probability at 1% per month. You can get up to date security patches for your server software for \$1/month.

- Is subscription worth it? What other factors are there? How do we include those factors in our analysis?
- Analysis goes beyond what we normally consider security issues.

Protection

- Implementation of controls and countermeasures.
- May be technological, physical, policy, and/or human-oriented.
- Some controls are specific to one threat (e.g., encryption of logins prevents snooping on network)
- Some controls cover many threats (e.g., keeping backups of important data)
- Example: Realizing the value of the website's data, you perform daily backups to DVD.
 - Technological – DVD writer, backup software
 - Policy – backups are scheduled daily; human must insert new DVD

Detection

- Waiting for something bad to happen, and then (hopefully) detecting when it does.
- Helped by systems implemented in the “protection” phase.
- Systems can have technological components
 - Network intrusion detection systems
 - Anti-virus
 - Firewall logs
 - Heartbeat monitoring
- Human / Process components
 - People monitoring intrusion systems / firewall logs
 - Gathering external information (e.g., customer complaints)
- What controls should be used for our website example?

Reaction

- When bad things are detected, what do you do?
- Develop a plan (during inspection/protection phases) for dealing with some attacks.
- Technological components
 - Adding firewall rules based on detected misuse
 - Automatic failover of one site to another
- Human / Process components
 - Manual shutdown of some affected systems
 - Sysadmin restores from backup
- Example:

After learning that you went on a date with his ex-girlfriend, your roommate pours a bottle of Jolt Cola into your server. How do you react?

Reflection

- Examination of what went wrong (and right) with a security incident
- Blends naturally into next iterative phase of inspection
- What are our reflections on the Jolt incident?

Things to Remember

- Security is *never* done; it is a constant process.
- Attacks have cost. So do controls. There needs to be an analysis of which actions are “worth it.” (Principle of Adequate Protection)
- You must consider all attacks; protection must be balanced across threats, because attackers will always use the easiest route. (Principle of Easiest Penetration / Principle of Weakest Link)

Risk Analysis

- Absurdly idealized:
value of control = cost of control - (probability that control works * probability of incident * cost of incident)
- How do we come up with those numbers?
 - Research / analysis (ideally)
 - Heuristics (practically)
 - Intuition (yikes!)

Risk Analysis

- Costs come from many sources:
 - Initial investment in technology
 - Maintenance costs of systems
 - Use costs during security incidents
 - Use costs during *non-security* incidents (e.g., false alarms)
 - Direct impact on business
 - Impact on public perception of business
- Risks / threats come from many sources:
 - Casual attackers / collateral damage (worms, viruses)
 - Targeted, malicious attackers (financial gain)
 - Regulatory issues (violating laws gets you sued)
 - Accidents / Natural disaster (earthquake in data center)

Incentive Issues

- *externality* – cost or benefit from an economic transaction that parties “external” to the transaction receive
- Many decisions have impact on the security of others
- Often those bearing the cost of an attack are not those who have the power to implement a control
- Likewise, those who would have to bear the cost of a control may not receive security benefit
 - Example: why should a business spend money to keep your personal information private?
- Laws and regulations often exist to “internalize” externalities
 - Example: laws about disclosure of personal information
- Should we have software liability laws?