The Eight Rules of Security

The components of every security decision.

Understanding and applying these rules builds a foundation for **creating strong and formal practices** through which we can make *intelligent* and *consistent* decisions.

The Eight Rules

1. Rule of Least Privilege.
2. Rule of Change.
3. Rule of Trust.
4. Rule of the Weakest Link.
5. Rule of Separation.
6. Rule of the Three-Fold Process.
7. Rule of Preventative Action.
8. Rule of Immediate and Proper Response.

Some Definitions

Subject: the person, place or thing gaining access.

Object: the person, place or thing the subject is gaining access to.

Access: the level or degree of access given to the subject in relation to the object.

Context: the situation or circumstances surrounding the access (when and where).

1. Rule of Least Privilege

Allow only as much access as is required to do the job, and **nothing more**.

In addition, allow only as much access as an individual, group, or subject is capable of being *securely responsible for*.

Start from the point where nothing is allowed, then work from there ...

Practicing This Rule

1. Create all security policies from a stance of the *Rule of Least Privilege* – determine what is allowed, then disallow everything else.
2. Always begin by ***denying everything***.
3. Always include the *Rule of Least Privilege* in all of the following security practices:
   (a) Written policies.
   (b) Configurations for firewalls, proxies, routers, etc.
   (c) All administrative controls.
   (d) Workstation and end-user access privileges.
   (e) New apps, services and databases.
   (f) Physical access to sensitive areas and devices.

Applying This Rule

1. Start by writing, programming, placing or configuring controls to allow **no access**.
2. **Classify** the objects, the subjects and the contexts for access.
3. For each object, ask yourself: *Does the subject need it? Can the subject handle it? Is the context safe?*
4. Set the level of access to the object for each of the subjects (within their contexts)
5. **Document** all decisions made!

2. The Rule of Change

Every organization needs to be able to adapt and change if it is to survive. Change is unavoidable.

Every change to the business must be *managed*, *coordinated* and *considered* for possible security implications.

Changes should only occur after they have been proven to be safe.

Changes should be consistent, and should not introduce diversity.

Example: Handling Change

Assume a new patch is to be installed:

- Begin by backing-up your test server.
- Apply the patch to the test server.
- Test the patch on the test server.
- Sign-off on the validity of the patch on the test server.
- Back-up the production server.
- Apply the patch to the production server.
- Test the patch on the production server.
- Sign-off on the validity of the patch on the production server.

Practicing This Rule

Change Management is important!

There is no security measure that cannot be undone by someone making an unauthorized and unreported change to a server, network or workstation within an environment.

So ... control those changes!

Never change anything *on-the-fly!*

Managing Change Control

- Always implement Change Control.
- Work hard to ensure the Change Control process is efficient – that way, no one has an excuse not to follow it.
- Apply the Change Control process universally – there can be no exceptions!
- Scrutinize all security changes (obviously).
- Control desktop changes – have a ``desktop policy''.
- Do not be the ``guinea pig'' for any product or patch!
- As far as is possible, **standardize** on a handful of technologies.

3. The Rule of Trust

Be a friend to everyone, but trust few.

Because ... anything can, and will, happen!

Understand the full effect before extending trust to anyone or anything, and only trust that which is required (remember: Rule of Least Privilege).

Trust = Power (so, be careful).

A little paranoia is sometimes good, too.

Practicing This Rule

1. Trust nothing outside of your immediate control – this includes large vendors, partners, consultants and suppliers.
2. Look at all the angles before extending trust – if you trust A and they trust B, does this now mean that you trust B?
3. Make policies apply beyond all levels of trust – everyone has to abide by the policy, even you!
4. Maintain an accurate perception – a rule breaker can still be someone you trust.

Considering Extending Trust?

1. Is this object within your direct control?
2. Is this object required to conform to your security policies?
3. Is the security of this object properly maintained and monitored?
4. Is your organization allowed to monitor and review the object's logs?
5. Is your organization allowed to perform a vulnerability test on the object and its environment?
6. Does this object have a history of security issues or failures?
7. How many other entities have access to this object?

4. The Rule of the Weakest Link

A security set-up is only as strong as its weakest link.

Identify your environment's weakest link.

Protect your weakest link!

You can bet your job that attackers/crackers will be working hard to do identify your weakest link – don't help them!

Practicing This Rule

1. Continually search for the ``weakest link'', especially after every change to your environment.
2. Document **all** security weaknesses.
3. Do not attempt to ``hide'' any weak links: such a practice is a **VERY BAD IDEA**, as *There is No Security in Obscurity*.
4. Avoid introducing new weak links into your environment.

Common Weak Links

Check out the FBI list: http://www.sans.org/top20.htm

- Default installations.
- Bad passwords (end-users/administrators).
- Active modems (on desktops, routers, servers).
- Neglecting logging and monitoring.
- Unsecured backup/redundant connections.
- ``Temporary'' servers, workstations, devices.
- Neglected/un-tested backups.
- Unauthorized applications.
- Outdated anti-virus software.

5. The Rule of Separation

To secure something, separate it from other dangers and threats that exist around it.

Do not overload servers with multiple services, as the more services, the more potential exploits.

The *lowest common denominator* applies to shared services.

Practicing This Rule

1. Isolate important (or critical) services and data.
2. Isolate services that are more prone to attack (so that you can keep an eye on them).
3. Isolate all security services – don't overload your firewall with other services. Ensure you have *one security service to one device*.
4. Only group services based on common security factors.
5. Understand exactly what is being grouped together – don't randomly group services.

Isolating Services Scoring System

Consideration	0 Points	1 Point	2 Points	3 Points
The Cost if the Service Stopped Running?	None	Low	Medium	High
Cost of Data Compromised or Corrupted?	None	Low	Medium	High
Cost of Isolating Service?	High	Medium	Low	None
How Complicated is this Service?	Simple	Complex/ Unknown	Very Complex	-
Was this Service Developed to Work with the other Potentially Shared Service?	Yes	-	No	-
How Many Vulnerabilities have been Discovered and Patched in the Last Year?	0	>1	>3	>5

Score of 0-4: May indicate that the Service can be Shared with Services that have an EQUAL score.

Score of >5: May indicate that the Service should be Isolated from other Services.

6. Rule of The Three-Fold Process

Remember: Security does not stop with implementation!

Security is a *Three-Fold Process*, which must include:

- Implementation.
- Monitoring.
- Maintenance.

Practicing This Rule

1. Consider this rule from the beginning – be sure to budget for monitoring and maintenance. Always contract for the ``update service'' for firewalls, IDSs, virus scanners, etc., etc.
2. Be sure to understand all logging and maintenance controls – know what the logs tell you.
3. Keep up-to-date – check for updates often, review logs at least once a day, produce a status report of anything suspicious.

7. Rule of Preventative Action

Security can only be successful if it is accomplished through a proactive approach.

Typically, people and organizations tend to lean toward *reactive approaches*. This is not good.

Also, many resist proactive measures:

- Management want visible proof of the measures effectiveness in order to justify it.
- Users consider the measures over cautious and a burden: *it makes no difference, so why change?*

Why Proactive?

The main social dilemma here is that placing added security controls where there appears to be no security issues is scrutinized, while the reactive response is considered a glorious triumph.

To be a good security professional, and to overcome the many obstacles to security, we must always be proactive, despite our human programming.

Without taking proactive measures, an organization has little hope of remaining secure.

Practicing This Rule

1. Keep aware of current security issues – visits security web-sites, subscribe to e-mail alert services.
2. Perform regular tests on security devices – run vulnerability scanners.
3. Do not stop with just the common issues – try to find vulnerabilities before they happen.
4. Maintain a strong Three-Fold Process – always check for updates, always check the logs (at least every day, sometimes more often).

Keeping Up-to-date

Subscribe to e-mail alert services (free or paid).

Take 10 minutes a day to read about new security issues – do any apply to your organization?

Read security web-sites – study recent events: do any apply to your environment?

Check the incident reporting web-sites on a daily basis – you can be sure attackers/crackers are!

Security Update Resources

Free Services:

- http://www.securitytracker.com
- http://www.sans.org/sansnews

Paid Subscription Services:

- http://www.securityfocus.com
- http://www.vigilinx.com/security/vsis.html

Security Info, News, Updates, Tools

http://www.cert.org
http://www.incidents.org
http://www.dshield.org
http://www.infosecuritymag.com
http://icat.nist.gov
http://www.securitystats.com
http://www.mcafee.com/anti-virus
http://www.foundstone.com/knowledge/free_tools.html
http://www.insecure.org
http://www.antionline.com
http://www.wwisac.com

8. Rule of Immediate and Proper Response

The steps we take after an attack has occurred are just as important as the steps we took to prevent the attack.

There needs to be an organized response to an attack: investigate the details, analyze potential risks and plan future steps.

Many organizations react poorly to an attack, and can often cause more harm as a result.

Proper Response

- React Quickly – have the right tools, skills and processes in place to react without delay to an incident. A written policy should exist.
- React Properly:
  - Don't panic!
  - Don't get excited and don't overreact.
  - Be discrete.
  - Follow the previously-agree process.
- Document what happened.
- Learn from the incident – don't let it happen again.

Practicing This Rule

- Develop a good incident response plan and reporting mechanism.
- Have a very clear and widely known chain of command – be sure to follow it.
- React quickly – do not wait to see what will happen.
- Make sure everyone sticks to the plan – do not panic.
- Follow-up on the incident – incorporate discussions into staff briefing sessions.

Important Point

Unless it is written down, we have little power or authority to enforce the rules within any environment.

Using The Rules

By walking through the rules from start to finish, and asking if the matter at hand relates to any of them, the security process is *automatically* taking place.

By making sure each rule is included in the decision-making process, we can *avoid* most of the confusion and error commonly found in the security decision-making process.

Summary

1. Rule of Least Privilege.
2. Rule of Change.
3. Rule of Trust.
4. Rule of the Weakest Link.
5. Rule of Separation.
6. Rule of the Three-Fold Process.
7. Rule of Preventative Action.
8. Rule of Immediate and Proper Response.

Abide by the Virtues, but Live by the Rules!