

A Bunch of Security Stuff

Compelling Title, eh?

Jack Daniel

Community Development Manager, Astaro Corporation

Let's talk about stuff.

1. I'll throw out some ideas and maybe a rant.
 2. You think about it for a bit.
 3. You add comments or questions.
 4. Repeat.
- No skipping step 2.

PDFs are not nice

- Adobe is not nice, they have insecure code and patch slowly and poorly.
 - Flash, Shockwave, Reader, Acrobat- continuous string of vulnerabilities and exploits.
 - Foxit is only a little better
- PDFs can do things like launch executables, and can imbed executables.
- Disabling Javascript does not save you.
- Foxit is better, but not much.

PDFs are not nice

We used to think PDFs were safe and Word docs weren't. Now with XML-based formats, it is much harder to hide malware in Office, and PDFs are proving to be a huge problem.

- <http://www.f-secure.com/weblog/archives/00001903.html>
<http://www.f-secure.com/weblog/archives/00001923.html>
- <http://blog.didierstevens.com/2010/03/31/escape-from-foxit-reader/>

What to do about PDFs

- Use Firefox or Chrome with these tools:
- <http://blog.arpitnext.com/gpdf>
- Opens PDFs in browser, but in Google Docs instead of a PDF reader.

Jericho Forum Stuff

- Opengroup.org
- De-perimeterization is here.
 - No, they aren't trying to steal your firewalls.
- Who has a portable device of any kind?
 - Laptop, mobile phones, USB drives, webmail account...
- So where's this perimeter thing?
 - That's right, everywhere.

Jericho Forum Commandments

The Jericho Forum commandments define both the areas and the principles that must be observed when planning for a de-perimeterized future.

Whilst building on “good security”, the commandments specifically address those areas of security that are necessary to deliver a de-perimeterized vision.

The commandments serve as a benchmark by which concepts, solutions, standards, and systems can be assessed and measured.

Jericho Forum Commandments

Fundamentals

Jericho Forum Commandments

- 1) The scope and level of protection should be specific and appropriate to the asset at risk.
 - Business demands that security enables business agility and is cost effective.
 - Whereas boundary firewalls may continue to provide basic network protection, individual systems and data will need to be capable of protecting themselves.
 - In general, it's easier to protect an asset the closer protection is provided.

Jericho Forum Commandments

2. Security mechanisms must be pervasive, simple, scalable and easy to manage.
 - Unnecessary complexity is a threat to good security.
 - Coherent security principles are required which span all tiers of the architecture.
 - Security mechanisms must scale; from small objects to large objects.
 - To be both simple and scalable, interoperable security “building blocks” need to be capable of being combined to provide the required security mechanisms.

Jericho Forum Commandments

3. Assume context at your peril

- • Security solutions designed for one environment may not be transferable to work in another. Thus it is important to understand the limitations of any security solution
- • Problems, limitations and issues can come from a variety of sources, including geographic, legal, technical, acceptability of risk, etc.

Jericho Forum Commandments

Surviving in a
Hostile World

Jericho Forum Commandments

4. Devices and applications must communicate using open, secure protocols.
 - Security through obscurity is a flawed assumption – secure protocols demand open peer review to provide robust assessment and thus wide acceptance and use.
 - The security requirements of confidentiality, integrity, and availability (reliability) should be assessed and built in to protocols as appropriate; not added on.
 - Encrypted encapsulation should only be used when appropriate and does not solve everything.

Jericho Forum Commandments

5. All devices must be capable of maintaining their security policy on an un-trusted network.
 - A “security policy” defines the rules with regard to the protection of the asset.
 - Rules must be complete with respect to an arbitrary context.
 - Any implementation must be capable of surviving on the raw Internet; e.g., will not break on any input.

Jericho Forum Commandments

The Need for Trust

Jericho Forum Commandments

6. All people, processes, and technology must have declared and transparent levels of trust for any transaction to take place.
 - Trust in this context is establishing understanding between contracting parties to conduct a transaction, and the obligations this assigns on each party involved.
 - Trust models must encompass people/organizations and devices/infrastructure.
 - Trust level may vary by location, transaction type, user role, and transactional risk.

Jericho Forum Commandments

7. Mutual trust assurance levels must be determinable.
 - Devices and users must be capable of appropriate levels of (mutual) authentication for accessing systems and data.
 - Authentication and authorization frameworks must support the trust model.

Jericho Forum Commandments

Identity,
Management,
and Federation

Jericho Forum Commandments

8. Authentication, authorization, and accountability must interoperate/exchange outside of your locus/area of control.

- People/systems must be able to manage permissions of resources and rights of users they don't control.
- There must be capability of trusting an organization, which can authenticate individuals or groups, thus eliminating the need to create separate identities.
- In principle, only one instance of person/system/identity may exist, but privacy necessitates the support for multiple instances, or one instance with multiple facets.
- Systems must be able to pass on security credentials/assertions.
- Multiple loci (areas) of control must be supported

Jericho Forum Commandments

Access to Data

Jericho Forum Commandments

9. Access to data should be controlled by security attributes of the data itself.
 - Attributes can be held within the data (DRM/metadata) or could be a separate system.
 - Access/security could be implemented by encryption.
 - Some data may have “public, non-confidential” attributes.
 - Access and access rights have a temporal component.

Jericho Forum Commandments

10. Data privacy (and security of any asset of sufficiently high value) requires a segregation of duties/privileges.
 - Permissions, keys, privileges, etc. must ultimately fall under independent control, or there will always be a weakest link at the top of the chain of trust.
 - Administrator access must also be subject to these controls.

Jericho Forum Commandments

11. By default, data must be appropriately secured when stored, in transit, and in use.
 - Removing the default must be a conscious act.
 - High security should not be enforced for everything; “appropriate” implies varying levels with potentially some data not secured at all.

Jericho Forum Commandments

De-perimeterization has happened, is happening, and is inevitable; central protection is decreasing in effectiveness:

- It will happen in your corporate lifetime.
- Therefore, you need to plan for it and should have a roadmap of how to get there.
- The Jericho Forum has a generic roadmap to assist in the planning.

False Positives are good

- False Positive, when something is detected as something it isn't.
 - Valid email caught as SPAM.
 - Valid or allowed network traffic blocked by Intrusion Prevention Systems (IPS).
 - Files mistakenly detected as containing malware.
 - Many other examples, in many fields.

False Positives are good

- When did you see your last FP?
- If it wasn't recent, are you sure you aren't missing anything?
 - Really?
- It is a trade off.
 - Which side do you want to be on?

IDS vs. IPS

- IDS: Intrusion Detection System
- IPS: Intrusion Prevention System
- Many people don't see the fundamental difference between the two types of systems.

IDS vs. IPS

- IDS: Intrusion **Detection** System
- IPS: Intrusion **P**revention System
- Many people don't see the fundamental difference between the two types of systems.

IDS vs. IPS

- IDS is a detection system, monitoring the network for potential malicious traffic.
- Missing *anything* is bad.

IDS vs. IPS

- IPS is a blocking technology, inline and designed to protect your network.
- This means an FP will block legitimate network traffic.
 - That is bad.
 - Which is why IPS is generally tuned cautiously.

IDS and IPS Tuning

- Both need to be tuned.
 - Report after report proves this.
 - Most recently an NSS Labs report.
- IPS really needs to be tuned for your environment.
 - Only rules which apply to traffic on your network should be active.

Security Appliance Tuning

- Firewalls, IPS systems, Web and Mail filters, much more- all require tuning.
- After much work in the area, I am proud to present:

Jack's Grand Unified Theory of
Security Appliance Tuning

NO

Security Appliance Tuning

Jack's Grand Unified Theory of Security Appliance Tuning

- Does not mean always say NO, but it means the default position should deny access.

FUD Watch: APT

- APT: Advanced Persistent Threat
 - Or Adaptive Persistent Threat
 - Or Adaptive Persistent Adversary
- The Hype Machines have grabbed this since the Google “Aurora” attack.
 - Which becomes less clear with each passing day.

FUD Watch: APT

- The term may have been abused, but the underlying problem is very real.
- A determined attacker can beat you.
 - Patience is more important than skill. But true APT comes from skilled attackers.
 - You only have to make one mistake to fail.
 - They can make thousands and still succeed.
- Persistence is the key.
 - Once in your systems, advanced attackers STAY, and leverage your systems against you.

Rugged Software Manifesto

- But Jack, we aren't coders.
- It is OK, this is a good idea, and understandable whether you write code or not.

Rugged Software Manifesto

- Joshua Corman, David Rice, and Jeff Williams put this together to give general guidance to developers, and see where it goes.
- Insecure software is one of the fundamental weaknesses we battle in securing our systems and our information.
- Agile, waterfall, other things I haven't thought about since taking the CISSP exam don't address security.

Rugged Software Manifesto

- I am rugged - and more importantly, my code is rugged.
- I recognize that software has become a foundation of our modern world.
- I recognize the awesome responsibility that comes with this foundational role.
- I recognize that my code will be used in ways I cannot anticipate, in ways it was not designed, and for longer than it was ever intended.
- I recognize that my code will be attacked by talented and persistent adversaries who threaten our physical, economic, and national security.
- I recognize these things - and I choose to be rugged.
- I am rugged because I refuse to be a source of vulnerability or weakness.
- I am rugged because I assure my code will support its mission.
- I am rugged because my code can face these challenges and persist in spite of them.
- I am rugged, not because it is easy, but because it is necessary and I am up for the challenge.

Security BSides

BSides is a community driven conference, built by and for the information security community. BSides events create opportunities for attendees to both present and participate in an intimate atmosphere that encourages collaboration and honest discussions.

Security BSides

- BSides events are free to attend.
 - There may be a “tip jar” out at some events.
 - Some optional events (such as after parties) may have a fee.
- All are welcome to attend, engage, and submit talks.
 - We do ask that you RSVP, see the event page for details.
 - This helps with event planning, refreshment ordering, venue layout, etc.

Security BSides

- The first event was at a house in the desert in Las Vegas during BlackHat US last year.
- Next was a smaller event in Mountain View, CA in December.
- Then another big one, in San Francisco, during RSA.
- Most recent was in Austin, during SXSWi.
 - The after party is now (in)famous:
 - Hackers on a Duck

Security BSides

- Next up: Boston. At Microsoft NERD in Cambridge.
 - Saturday and Sunday, April 24-25
 - The weekend after SOURCE Boston.
 - Plenty of space for more attendees.
 - A few speaking slots open.
 - There will also be unconference-style sessions in alternate rooms.

Security BSides

- Late July: Las Vegas.
 - Goal is to top everything done so far.
 - Without burning down any houses. Or anything.
 - Wednesday and Thursday July 28-29.
 - Coinciding with BlackHat USA, before DefCon.
 - We may have upset a big conference last year.
 - If they were upset last year, just wait...

Security BSides

- <http://www.securitybsides.com> is the starting point for all things BSides.
- Past event info.
 - Including audio, video, photos, media.
- Current events.
 - Schedules and Streaming video.
- Upcoming events.
 - Registration and talk submission.
 - Lodging and other information.

Thank You

- jdaniel@astaro.com
- [Blog.uncommonsensesecurity.com](http://blog.uncommonsensesecurity.com)
- [Twitter: @jack_daniel](https://twitter.com/jack_daniel)
- Are you LinkedIn to Astaro?
<http://www.linkedin.com/e/gis/139679/189D6C6oEC64>
- Astaro on Facebook:
<http://www.facebook.com/pages/Astaro/107041096353>