File 20110723.0805: Notes from LM Cyber Security Un-conference: between continual interruptions from the fire alarm system, Padgett Peterson spoke on 'iAndroid'. Linux under the covers of most tablet operating systems. Two ways of malware protection: signature based and integrity managers—the second works better for tablets in today's environment.

Padgett will be teaching an ISSAP class soon.

Upgrading the OS on tablets is really hard. When buying a cheap one on sale, make sure it's not stuck with a totally obsolete OS and un-upgradable. I mentioned installing Bitcoin on my laptop and how long it reported it expected to take to generate a single bitcoin. Discussion of video cards.

Bharat Shah spoke on a new Security Controls Assessment Database application. It looks pretty useful. For example, during a NIST SP 800-53 Rev. 3 controls assessment,

- the application then also captures the associated requirement.
- then it facilitates doing the assessment.
- the assessor can type their findings directly into the database.
- 'Requirements Assessment Plan' screen puts all information in front of the government security evaluator.
- 'Requirements Assessment Status Report' screen tracks progress of each requirement.

Email `bharat.shah@lmco.com` for more information.

Next scheduled event in the un-conference: 'Security Throwdown': from the Verizon Data Breach Incident Report (DBIR), in 2009, only 6 of 90 break-ins involved vulnerabilities. In 2010, none did. So, does patching matter? One response from a participant: 'You can't patch stupid'.

Padgett: a vulnerability does not become a threat until you also have an exposure. E.g., if it's on an isolated network, it may be an unexposed vulnerability. Padgett is not a fan of signature scanners; he would prefer to know precisely what is on the system first, and then bring in a scanner.

Padgett: at one time, Lockheed was considered the leader in security. Now, is it getting too hard? Remote management of the cloud is the latest thing. The right way to do that is by having a separate management layer atop the cloud.

Request from Mike Greco: I should do an LM VTIS report on the UCDMO conference. I put it on my calendars.

Discussion of C&A. Mike Greco: the whole C&A process is crying for a database solution. (Mention of something called TurboIA, in the spirit of Turbotax.) Problem: existing COTS tools like 'Exacta' are incredibly expensive.

Next presentation: on Mac OS X Lion security:

- Mac OS X 10.3 'Panther' introduced secure deletion and FileVault.
- Mac OS X 10.5 'Leopard' introduced library randomisation, but it was considered ineffective by security researchers. An application layer firewall was poor, even though the OS had iptables functionality built-in, but Apple never turned it on by default. Sandboxes, application signing, secure guest account, and Time Machine were all introduced here.
- Mac OS X 10.6 'Snow Leopard' introduced anti-malware protection.
- And now, Mac OS X 10.7 'Lion' introduces:
  - an improved Address Space Layout Randomisation (ASLR) randomises stack and heap.
  - automatic security updates.
  - Sandboxing: Safari is split into separate parts; Javascript or plugins run in their own sandboxes. UPDATE: it's two sandboxed processes, according to another article I read.
  - Encrypted backups, finally.
    - Done at the block level, not at the file level.
    - Do not have to be logged out for home directory to get backed up.
  - 'Air Drop' allows setting up quick P2P networks to exchange files.

    - TLS encrypted
    - Apple ID used for authentication
    - Sets up appropriate firewall rules automatically
  - FileValult 2
    - Snow Leopard only encrypted the user's home directory, and interacted poorly with Time Machine.
    - Implements FDE and instant wipe of entire drive by deleting the key. You can choose to have Apple escrow the key for you.

The sequence of Mac OS X releases was:

1. Mac OS X 10.0 'Cheetah'
2. Mac OS X 10.1 'Puma'
3. Mac OS X 10.2 'Jaguar'
4. Mac OS X 10.3 'Panther'
5. Mac OS X 10.4 'Tiger'
6. Mac OS X 10.5 'Leopard'
7. Mac OS X 10.6 'Snow Leopard'
8. Mac OS X 10.7 'Lion'

References