File 20110128.0655: Weekly activity report 0173:

weekly activity report 173 (loughry)
Joe Loughry
Sent: 28 January 2011 06:55
To: Niki Trigoni; Andrew Martin; Joanna Ashbourn
Cc: otaschner@aol.com; anniecruz13@gmail.com; andrea@hpwtdogmom.org;
chip.w.auten@lmco.com; edloughry@aol.com; diane@dldrncs.com;
Joe Loughry; mmcauliffesl@comcast.net; tom.a.marso@lmco.com

Weekly activity report no. 20110127.1401 (GMT-7) sequence no. 0173, week 2 HT

The R'' developer met with the TMAN developer during an upgrade trip this week to compare the respective CDS software development organisations and CDS technical capabilities of the software. One of the findings is that the ST&E, CT&E and IV&V processes of TMAN are all different from RM to a surprising degree. DCGS, the primary customer of TMAN, has a single accreditor based in the same city as the TMAN developer; the relationship between developer and accreditor is reported to be close and cordial. The difference in ST&E practices appears to derive from:

1. The almost exclusively single-accreditor installation environment of TMAN (coming from the captive arrangement with DCGS);

2. A complete absence of IV&V in their ST&E accreditations (apparently not required by the DCGS DAA and out of scope certification-wise because TMAN is not approved for SABI) although something like IV&V is performed by contractor personnel;

3. Installers play a much smaller role in TMAN because the system is not field-configurable; installers need configure the network only; all parsing rules are implemented in compiled C++ provided at the factory.

4. TMAN digital signatures employ cryptography that uses PKE but not X.509 standard PKI.

The R'' developer reports that the new programme manager (over TMAN and RM) has almost completely been convinced by the software engineers that attempting to merge the two different CDS products would be a bad idea. While the CDS application domains overlap to some extent and the systems share a subset of capabilities and customers, their implementation details, reconfigurability and mechanism of configuration (the latter arising directly from the design via the software engineering process, and thereby ultimately from requirements) all differ sufficiently to make combining them an expensive proposition. (Difficulty of merging the SEE organisations was not investigated.) Indications at the present time are that parallel development will continue, with cost savings taken where they become apparent, such as the planned replacement of duplicate IAVA tracking responsibilities with single responsibility and dual reporting.

Related to the difference between installer skill sets, the R'' developer also reports encountering DoD 8570.01-M requirements in the field for the first time. Air Force sites in particular have begun to demand infosec certification of all contractor personnel entering the site. The developer currently has six qualified installers possessing IAT Level III and one with IAT Level II certification; the R'' developer is now pressing for all installers to pass the IAT Level II examination as soon as possible. Support from above the department level in the corporation has not become apparent yet, though it is known that several other programmes in the same facility are subject to 8570.

Data gathering continues on the R'' case study; the CT&E cycle of 5.0/5.01/5.02 has not completed yet. I am moving forward on coding and categorising earlier-collected data, currently up to September--November 2009. The R'' developer received a 5.0 (highest possible) rating on the Contractor Performance Assessment Report this week. I am still reading Glaser and Strauss (1967) on grounded theory, which cross-referenced me to a chapter by Coleman (1961) in another book by Hammond (1964a). I am using the coding methodology propounded by Glaser over the Straussian methodology, at least so far; that might change after I have read the later books in my to-read stack.

The 'Best Practices Guide for Operating a Cross Domain Solution on a Virtualized Platform' (NSA-IAD, 2011a) guidance was updated to version 10; I compared the new version to the old one, and some of the changes, reflecting current risk analyses of both homogeneity and heterogeneity in and on VMs with respect to CDS, were illuminating. In other work, the second emergency report asked for by the Air Force Research Lab sponsor was completed, this one heavy on the metrics. I needed to invent a framework for metrics that fit with the sponsor's Technical Council's call for data, but after a few go-rounds the sponsor was VERY pleased with the result and commented that his other projects were not as responsive. Always good to keep your funding sponsor happy, I suppose.

I am finalising travel arrangements to meet with several people in Oxford during a UK trip planned for 14th March. I received the GSS report comments of Prof. Kwiatkowska (DGS) for Michaelmas term. She checked the 'concerns' box on the report but said only that I need to work hard on the next confirmation report. I am doing that.

Colin Williams, Director of SBL, gave this week's Information Security and Privacy Programme seminar on 'Information Assurance in the Information Age; Towards an Historical and Social Context'. I participated via Skype on a borrowed laptop. For the next seminar, if I can pre-arrange access to a laptop in the seminar room with Skype, it would be of great benefit, as network connectivity was interrupted briefly with the hand-off to the 802.11 access point in the room Monday. Sound quality was excellent.

The presenter was illustrating growth of internet nodes in 1998--2008 when I came in, as a platform on which to build his argument for disruptive and destructive changes to societies and cultures. In 2001, something unique happened; developed countries took it up faster. What we have learnt from the event: (1) the world is more interconnected than we thought; (2) many of our assumptions were false; (3) the bad guys are doing a better job than security experts.

'When we look at the current world through the filters of our previous experience, we think it makes sense.' Wikileaks demonstrated a new kind of entity: its distributed existence was highly resistant to DDoS attack. The greatest centralised defences, the most impregnable shields, are worthless if a DDoS can prevent you communicating. Risk, threat and vulnerability have Cold-War definitions. We are telling ourselves a story about the things we think we understand [the preceding was paraphrased].

'We can't manage the properties of disruptive technologies. We might be able to manage the emergent properties.' The transformation imposed by the internet has already occurred. The fundamental economics of information distribution have been disrupted. This distribution has begun to be applied to the material world. [Description of affordable 3-D printers.] We are looking at these technologies from an outdated perspective. We can see aspects of the Frankenstein complex all over our culture’s literature. When speedy travel (i.e., railways, motor cars and aeroplanes) appeared, physicists and physicians were certain that death from asphyxiation would surely result. Today, we see the same alarmist extrapolation of sentient computers and genetic engineering.

Computer scientists see users as the insider threat. Users are perceived as passive, subordinate to the operation of the system. ‘This is the image of computer system security that we as computer scientists ‘sell’ to the users: padlocks and chains and firewalls. Rules and restrictions.’ ‘We [computer scientists] have inherited from the 1960s the notion of a priesthood and an esoteric language.’

Disruptive and destructive epochs in human history have repeatedly and continually resulted in the rise of new nations, new concepts, new allegiances forming. For example, the printing press disrupted the existing power of the Catholic Church, ‘changing the relationship of people with their divine’. Thinking about today, we have not cracked the problem of security and privacy on the internet. For example, what makes it acceptable for people to be anonymous on the internet? Consider the observed behaviour of teenagers and their apparently organic use of pseudonymity on social networks. Their elders at the same time exhibit a backlash against shopping on-line. ‘What are going to be the markers of privacy on the internet?’ A new social contract is needed. We have accepted protocols for cryptography and digital signing...

[At this point, I wanted to argue with the presenter regarding his assertion of ‘accepted protocols’. I would counter-assert that we barely have an accepted legal framework for photography---a 100 year old technology. Consider the patchwork of laws regulating photography of people in public places. In an era of ubiquitous mobile phone cameras, pervasive CCTV, automatic face recognition and terrorism, I claim the law is aeons behind where people are. What about the laws applying to photojournalists and libel? Those laws have barely kept up with news organisations’ acquisition of betacams. Nearly every person on the street has audiovisual recording capability, and soon many of those will be lifecams (viz. Gordon Bell). I think the difference between the uptake of cars (successful) and photography (problematic) is that photography is an information technology and cars are not.]

‘Wikileaks instantiated an entirely new framework of authorship and responsibility and ownership and control of information.’ [Discussion of the defence of Wikileaks by ‘Anonymous’. It has no locus of control, yet it coalesces on certain actions from time to time. How does it do that?]

The presenter’s final slide dealt with cyber warfare. Since 1995, we have had the ability to prosecute cyber warfare. What we do not have is a legal framework for it. There is a serious problem with attribution. There is a problem with control. For example, consider the principle of proportionality in the international rules of war. If someone shoots at you with small arms, it is not considered proportional to retaliate with a nuclear explosion. We have enormous capability but no legal or ethical framework in which to do so. Example: the attack on Estonia. It was arguably a violation of Article V, but how can you respond without a legal and ethical framework?

This was followed by a discussion of certification and accreditation in the civil arena. The schemes that exist are very close to those C&A schemes that existed for years in the military world. [Skype lost its connection to the supernode at this point and I could not get back in. Call ended approximately 1800 GMT.]

The Oxford Security Reading Group met Wednesday to discuss the new paper ‘Paranoid Android: Versatile Protection for Smartphones’ by Portokalidis, et al. (Austin, Texas: 26th ACSAC, 6--10 December 2010, pp. 347--356). Cornelius introduced the paper. Briefly, the authors propose to detect malware and certain kinds of dynamic attacks on smartphones by continuously running a synchronised emulation of each phone’s software environment on a centralised server in a VM, where greatly expanded hardware resources make it practicable to run much more extensive and resource-intensive security and integrity scanning processes than could practicably be run on a phone. This avoids having to run them locally---a drain on battery, CPU and memory. To maintain synchronisation of state between the mobile device and the security server, the authors developed ‘traces’ that encode changes of state on the phone in a relatively compact form and transmit them to the emulation server without significantly impacting either bandwidth or battery life of the mobile phone. They found that traces could be supported in no more than 2 kilobyte/sec of bandwidth even under heavy usage, and with a negative impact on battery life of about 30 percent. This, they argue, compares favourably with the cost---especially in battery life---of running anti-virus scanners directly on the phone. The authors present extensive data collected on the actual traffic levels of real devices with Paranoid Android (PA) running under realistic conditions of use.

In section 1, the authors consider characteristic differences between the security posture (and to a somewhat lesser extent, usage patterns) of mobile phones used by corporation officers and government employees vs non-official users. I mentioned that the U.S. Department of Defence spends $65 million a month on Blackberries alone. This prompted discussion about the number of devices in use in DoD, number of different platforms supported for official users, and the differences between the firmware load of a Blackberry approved for classified information vs unmodified COTS devices. Blackberry has implemented robust policy and procedures for remote wipe and kill which makes that vendor attractive to corporations that are security aware, but the company’s willingness to open its security protocols to various governments (quietly) is what has really led to Blackberry’s widespread adoption in the government sector of several countries.

John suggested that the method described in this paper might be more limited in general applicability than it first appears because of the different behaviour of different types of users with respect to downloading apps. The trace method implemented by the authors is oriented towards voice and messaging traffic. The intent here is protecting privacy. Dr Martin noted that attackers do not attack privacy for the sake of privacy; they are generally trying to steal something of value. John agreed that privacy does not have a clear canonical attacker. (I would remind everyone of the focus on corporate officers and official government users of smartphones in this paper; the value of the information protected by privacy in the present case is not personal information or individual bank accounts; it is classified government data and competition-sensitive corporate information, highly useful for insider trading and potentially as significant as large-scale market manipulation or international relations.)

Cornelius raised the technical issue of how to know how much information to record in the traces. The authors are trying to say two things in their presentation: that they have implemented recording of enough information to maintain a sufficient degree of state synchronisation between mobile and fixed emulations, and that the overhead (both in terms of battery charge consumption and bandwidth usage penalty) is acceptable or undetectable to mobile users. Dr Martin pointed to the large number of comms channels in a typical smartphone, all of which continually affect the state and virtually any of which could be a vector for malware injection. I wondered about the distinction between explicit malware injection and the more insidious implication of subtly corrupting the state of the mobile device through deliberate manipulation or simply degradation of environmental signals, such as GPS---I can think of attacks based on ‘moving’ the apparent location of a mobile device through spoofed locator signals, thereby interfering with distance bounding protocols or location-aware security of bank account transactions. This led to a discussion amongst several participants about data sizes: voice, photos, YouTube. The authors of the paper specifically did discuss the trace volume of voice calls and dismissed digital photographs as being an uncommon use case in high-security environments (a constraint I am not sure that I agree with). John commented on the secure storage protocol in section 2.2.2; there is concern that the cryptographic protocol does not have protection against replay. Related to that, something I read in a recent draft document of recommended practices for running Cross Domain Systems in a virtualised environment comes to mind: the suggested practice of VM rotation, that is, periodically resetting the VM of a virtualised CDS to interrupt the progress of an undetected attack. Dr Martin observed that in the case of the secure storage protocol, having an entirely predictable sequence of keys seems unfortunate. There is a possible DoS vulnerability here.

John said that the contribution of the paper is the replay scheme, not the conceptual attack detection, which the authors really don’t go into. This is related to IDSes that attempt to emulate the system they are trying to protect. I suggested that the scheme may be applicable to safety-critical or reliability-critical systems such as space probes, where the impossibility of sending a repair person makes it imperative to get software updates right. This sort of emulation, especially if combined with something John mentioned about ‘speeding up time’ would be an extremely valuable contribution to the reliability engineering of remote systems including interplanetary probes, airliners in flight, and communication satellites. Dr Martin noted the difference between software engineering update practices on these systems and mobile phones, and that is true but I claim that communication satellites at least are not dissimilar to mobile phones in that comsats host a multiplicity of communication channels that are critical to the success of the endeavour (because they carry paying traffic) without being part of the telemetry or control of the device.

The conclusion of Reading Group was that this paper is a nice idea but no one is quite sure it holds water; it is a good contribution (especially the measurements and the mechanism, just not so much the application of the technique yet) that will inspire more work in the area.

My current tasks, in priority order, are:

0. Need a supervisor meeting with Dr Martin.

1. Continue reading Glaser and Strauss (1967) and references derived from it.

2. List of codes and categories for September--December 2009 data on R’’. Pull together all the R’’ data into a single hermeneutic unit on ATLAS.ti.

3. Keep the list codes and categories general enough that it also works for R’ and R-zero. Keep adding hooks for event traces.

4. Figure out if I can use the chronological record in my lab notebook as a source for the ‘memo writing’ activity that occurs later [not done yet]

5. Plot tasks on a new Google Calendar as blocks in a 168-hour week. Establish limits on non-thesis work times [task left over from last week due to unplanned Air Force work]

6. Outline the survey journal article that the assessors asked for. I still need to find some good examples of how to write a survey article [waiting].

7. Outline new Chapter 1, revised Chapter 3, and completely new Chapter 4 [I want to have these in hand for Oxford in March.]

Joe Loughry
Doctoral student in the Computing Laboratory,
St Cross College, Oxford

End of WAR 0173.

References