File 20110804.1135: Notes from UCDMO conference, day 4:

I talked with Bryan Fetter of Northrop Grumman about the Sentinel-XD manpack CDS. It contains a Xilinx FPGA running a PowerPC core and and a full version of Linux. It has two network interfaces and a battery pack in a box the size of a water bottle. From examining the hardware, I think it could run Radiant Mercury instead of the simple packet filter running inside it now. I suggested he talk to LM about providing an example of the box to test with.

0800 Frank Sinkular opened the general session. Please fill out the UCDMO conference survey. Next UCDMO conference will be in Orlando, 23–26 July 2012.

The next speaker was Major General Michael T. Flynn, on '21st Century Warfare'.

Thirty years experience in the IC. The current CJCS, Admiral Mullen, said that shifting coalitions in a multi-nodal world is the new reality, instead of security competition between opposing blocs. Arab uprisings this Spring were not predicted, and will probably go on for years.

'Those in power care about their boundaries; those not in power do not care about boundaries.'

'Decentralise until you're uncomfortable; then you have it about right.'

'Deliver complete solutions in 6 months or less, or be irrelevant.'

1. Theme: information sharing.

2. Provide senior leaders in designated combat zones with more authority to make information sharing decisions. The situation has been going on for ten years in this war. The authority already exists, but still we have people in the field having to ask permission for something that theortically they already have authority to do.

3. What would success look like from an information sharing perspective? When we're able to send data on the AMN from US SECRET to NIPRNET. In 2009, the US was way behind NATO in effective use of networks. There are 49 nations in the coalition in Afghanistan.

4. Technology should not drive requirements. Requirements should drive technology.

5. At the brigade and company level, the network has been found to be the main force multiplier.

6. The enemy operates cross-boundaries. The enemy does not care about boundaries. In the coalition environment in Afghanistan, field commanders in different regions cannot share information across internal boundaries, at present, as well as the enemy does.

'Only design tools that are multi-agency, multi-coalition.'

'USAFRICOM is learning the same lesson over again in Libya.'

AMN: Afghanistan Mission Network has been a success. What is needed is a ready-to-go coalition mission network for the next time. The U.S. may have to buy this, if NATO doesn't. Have it for the next time. Don't build the next one under fire. Build a deployable mission network, coalition-ready, in a box that can be dropped anywhere it's needed. Buy it now, because experience teaches it is going to be needed later and there won't be time to assemble it then.

One squad is responsible for 30–40 square miles in Afghanistan. Bandwidth is key.

Question from the audience: we have heard you have to be 55 years old to be in a leadership role; by the time we put something through out requirements and design reviews, it is stale. I see the press embedded in combat; suggest embedding acquisition people in the field to get them experience.

Answer: in the nineteen-seventies, Japanese automobile manufacturers involved the workers on the assembly line with the design engineers. Today we have acquisition people building networks that are technically excellent, but not useful. 'Your suggestion is an excellent one. If it can't be developed in six months or less, forget about it. What I hope is that ten years from now, all the young people we hired after 9/11, who have seen it, or maybe another ten years after that, will get into leadership positions.'

Comment from the audience: with the acquisition life cycle, with approvals to operate and approvals to connect, we can't see any way to speed it up. Keep pushing your message, General Flynn, about 'six months or less'.

Answer: 'flattening' scares a lot of people in the Pentagon. They want to keep their control. 'If you're in a leadership role in a contractor, you have to drive it.'

Question from the audience: what tools would you wish for, like in your article, 'Fixing Intel'?

Answer: 'some sort of beer dispenser'. A mission network that can communicate across all coalition partners. Bandwidth. Bandwidth is a combat multipler. Now, commanders plan how much bandwidth they need just as they plan how many bullets, how much water.

Question from the audience: tradeoff between risk to global C&C infrastructure and the free flow of information. Previously, there was not a weapon that could have knocked out our entire global C&C infrastructure, but now there is, and it's digital.

Answer: 'with all due respect to your experience, you're overstating it. Like when we thought the Russians were "ten feet tall". I am a security person. I have to provide access. We don't do risk analysis very well. We don't do risk management. People in the security community say 'no' by default. It's the traditional response. They always say no. If they say yes, they've just pulled something out of their inbox and they have to work on it. Humans are poor at judging risk. It is not in our DNA. But there is something above 'high risk'. It is failure. You have to be aware of when your caution is in danger of causing mission failure.'

Next speaker: Terence J. Meyer, CIO, CENTCOM on 'Flexible Cross Domain Solutions in Support of the Warfighter'.

To follow on the thread the General started on operational support for the warfighter, the Bottom Line Up Front (BLUF) is:

- get the right information
- to the right warfighter
- at the right time
- in a format he or she can use
- persistent and discoverable.

Coalition operations are not 'the new norm'; the've been around since Churchill.

Networks: four eyes, five eyes, NATO, ISAF (49 countries), CCTF (86 countries), JWICS, Stone Ghost, SIPRNET, SIPR REL, AMN, Centrix-GCTF (CX-G), Centrix-ISAF (CX-I), CX-CENTRAL, NIPRNET, NATO U, UGON, LEX, PIX (protected internet exchange [FOUO]), internet, NATO-S, BICES.

The Cross Domain Life Cycle: from requirements to capability.

- policy (national information disclosure policies)
- FDO (foreign disclosure officers—there are fifty or so of them, from CENTCOM down to SOFs)
- process
- training

There is no standard policy common to all levels from CENTCOM all the way to RC-South in Afghanistan, for dealing with data spills.

Enterprise Solutions:

- waiting for the enterprise solution doesn't always give the warfighter what they need.
- bandwidth is always a problem. Plenty of bandwidth at home. Solve the bandwidth problem in the field and you could extend the existing enterprise all the way out there—done.

Cross Domain User Guides: CENTCOM developing a matrix showing all networks to all networks and what are the guards in the way. What will they allow and what will they block from which networks to where?

Consolidated Dissemination Nodes: the first CDN was set up at Ft Belvoir, taking data off BICES and AMN, pulling it up to SIPRNET and storing it there in a dedicated NATO space. It is air gapped; implemented entirely on sneakernet.

Question from the audience: DoD is getting a lot of training pushed at us, but not getting training on the CDSes we need. Getting training on DADT instead of on information sharing.

Answer: services are responsible for Title 10 training, but there is no central policy for training on certain core capabilities: DCO, DCS.

Major General Flynn: we have a bunch of old people in leadership positions who are still fighting against their email. The younger people in the inventory will move up and flush them out eventually because the young people are collaborative by nature and much more effective operationally.

Conference presentations will be posted by mid-August at the following UCDMO web sites:

`http://www.intelink.gov/sites/ucdmo` (NIPR)

`http://www.intelink.sgov.gov/sites/ucdmo` (SIPR)

`http://www.intelink.ic.gov/sites/ucdmo` (JWICS)

1005 Calleen Torch, IC CIO/ICIA/RMIS/CAT, UCDMO, on 'Operational Penetration Testing'.

Calleen heads C&A test team for ODNI.

What is the IC CAT? CAT serves as the technical arm of the IC CIO.

Why perform operational pen testing?

- performance *at site*, on an *operationally configured system and its periphery*;
- allows testing of entire system without laboratory artifacts;
- testing in a more chaotic environment.

CAT follows a 'Blue Team' test approach:

- negotiate Rules of Engagement (ROE) beforehand;
- test boundaries;
- testing approved by system and network owner;

The model is best characterised as 'grey box' testing.

- share all processes and results—testing is completely transparent to site and programme;
- they come in at end of ST&E or Beta 2;
- they test as a malicious user;
- CAT openly solicits information from the system owner. They will use anything and everything they can get.

Testing usually runs 2 days to 2 weeks, depending on complexity of the system under test. They have done joint testing with JCDS and the UK.

They look first at the system documentation to develop the ROE, but they will explore undocumented rabbit holes they happen to find, such as undocumented servers they discover, for example.

Test Strategy:

- act as a simulated threat;
- malicious and technically competent insider;
- they will also access the system from internal and external networks;
- they do not usually review code except for scripts;
- they use all available commercial and open source attack tools with the latest attacks downloaded.

They never perform test actions that would be disruptive of the operational environment; they will back off before doing a DoS. They will stop testing and delay progress and report a problem instead of impacting the operational system.

Question from the audience: 'my concern is that as an adversary, the first thing I will try is to go straight through the flow process.'

Answer: IC CAT does look first at filter formats and will try testing the main flow first, because sometimes that is a vulnerability.

Question from the audience: do you do any assessment against the developer's toolset used to build the application? E.g., Java.

Answer: in general, we do not look at code, but we do look at things like the account creation process, etc.

Question: how does your pen testing play into reciprocity?

Answer: we look at reciprocity of accreditation packages, not reciprocity of ATO. We typically go in at the end of ST&E or Beta 2. We document every finding we make and write a mitigation for it. This is a good portion of your reciprocity. What is different is the environment of the next ST&E; only those differences, the local infrastructure, need to be retested for reciprocity to work.

Question: in terms of security validation and test coverage, how often do you see test plans that do not cover enough?

Answer: all the time. We look at that documentation and take it further. We don't usually work certification test plans—that's for the certification test team to do before we get there. We test as malicious users, the insider threat.

Question: what guiding documents in the IC define what are the pen testing requirements?

Answer: In DCID 6/3, there was a pen test requirement, but in SP 800-53, it's vague. There is a movement afoot to require pen testing.

Question from SAIC: what is your methodology for testing rule sets? Do you do beyond the developer's test procedures?

Answer: we go beyond.

Question: can you talk about the methodology?

Answer: we test edge cases, we feed the CDS Unicode to see what happens, we try things, we explore rabbit holes. Our team is knowledgeable on all the trusted OS's, but we go by instinct sometimes.

The team consists of Corrine Castanza, Dave Moran, Jerry (?) T(?), maybe one more.

Question: how are you called in? Who calls for pen test?

Answer: first, we are responsible for DNI systems. If three or more community systems are involved, that triggers a pen test. We look at community systems where DNI has funded part of it. We have done joint tests events with 4Eyes and 5Eyes community as well.

Question on pen testing in general. What are your thoughts on standardisation of pen testing methodology? To try to bring ip everyone's pen testing skills to a high water mark?

Answer: we are backed up 4–5 months. Not enough time for us to train others. We would like to bring other pen testers up to our level, but we don't have enough time or funding.

1037 Scott Lake, NSA IAS pen test team, on NSA laboratory-based penetration testing.

NSA have been reorganisation as you all are aware, but functionality will be unaffected. ADF and Mitigations are the two new organisations, made up of the previous SNAC.

Question from the audience: how and when are the NSA pen test team assigned?

Answer: we get called in on every CT&E and delta CT&E; in our ideal world, we do laboratory pen testing and pass our results to the DNI CAT to do operational pen testing. In a perfect world, UCDMO would like to see both teams assigned to all systems.

Question: 'from a DoD perspective, as a C&A practitioner and validator, our acquisition requirements say we must embed pen testing in acquisitions. So my question is, what is pen testing?'

Answer: 'you are going to hate my answer, but penetration testing is largely intuition; as soon as you document that methodology, you close doors. Pen testing is an investigation of failure modes. That looks like black magic to a lot of people. Checklists are only good for low-hanging fruit; what you really need is an inquisitive person who can look at something and think, "that looks funny" '.

From the new lead of NSA pen testing, who replaced Scott Lake, who is going down the hall to Mitigation: 'you will never do something that proves a system is completely secure, but you can document what you have done and build on that later'.

Question about what happens after CT&E or pen test. Will the mitigation team help fix problems found?

Answer: a lot of the time when we find flaws, we find a mitigation at the same time, and sometimes it comes back to us for regression testing. In future, all findings will be fed back to Mitigations to inform an improved architecture or guidance.

Question: 'this question is directed as NSA because they do more laboratory-based testing: is there a way to speed things up to meet MG Flynn's six-months-or-you're-irrelevant deadline?'

Answer: three months is our traditional penetration testing time frame. Even that is too long. See the next talk, on entry requirements for penetration testing.

Phyllis Lee: in reality, everything comes in at once. The schedule slides to the right, and the very last step before we can turn it on is ST&E.

Comment from the audience: there are too few penetration testers in the world—we need to move this capability out into the community.

Question from the audience: can you go into more detail about the tools you mentioned?

Answer: 'layer 2 and layer 3 tools speed up our work. Lately we have had trouble getting new tools. The waiver process and acquisition process to get these tools is an impediment. Sometimes the acquisition people try to download the tools and their anti-virus scanner goes off—well [rude remark] to that.'

Question: 'do we not want the user to learn the C&A process? If I have some minor configuration changes, how do I establish this communication channel?'

Answer: we understand that COTS software needs patches for newly discovered vulnerabilities, but it is still being worked through the policy how to handle that.

1100 Scott Lake on 'Penetration Testing Entry Requirements'.

NSA laboratory penetration testing: pen test is always required for a full CT&E; the decision is made on a case-by-case basis for delta testing.

The decision is not made on a specific standard—it was decided in the past by Scott Lake.

New method for deciding:

- Step 1: improve pen testing process and speed it up.
- Step 2: improve quality of pen testing.

New technologies will trigger a penetration test: use of multi-level databases, video transfer, a new OS not previously tested.

Major changes will trigger a penetration test: OS upgrade, e.g., TSOL to Solaris 10TX, REL4 SELinux to REL5 SELinux, architectural modification such as new transfer pipelines, new protocols; things that are security-relevant; the developer or vendor provides enough information to the pen testers organisation for it to decided whether the change is security relevant.

Minor changes will not trigger a pen test. Adding new software that has been previously thoroughly tested, for example OpenSSH, will not trigger a pen test. New filters added to a well-tested engine will not trigger a pen test.

Second step: background

1. NSA see many systems coming into the lab that are not ready; they are in the pen test lab only because some arbitrary schedule says it must be done now.

2. Insufficient documentation is common.

3. Insufficient installation process and procedures are also extremely common.

4. Lack of test interfaces—NSA loses time developing test interfaces.

5. Insufficient testing by the vendor beforehand. This leaves too much low hanging fruit that wastes the NSA pen testers' time.

Goals for the second step:

1. Standardise product readiness prior to pen testing.

2. Reduce the time to pen test.

3. Dig deeper during the pen test—find problems fundamental to the architecture. This is the kind of error they are most happy to discover, because it has the highest impact on future quality improvements to the CDS ecosystem.

4. Introduce measurable test cases for vendors to perform ahead of time.

These will be achieved through five categories:

1. Documentation from vendors: the LLD is often not provided or doesn't exist; NSA pen testers require access also to the engineers who wrote the LLD.

2. Separation strategy: vendor must share details of how their CDS separates domains. It is part of the LLD. Identify exactly how processes are restricted to accessing only authorised resources.

3. Required documentation for Separation Strategy: for example, if you are using Zones, what is the zone layout, show us the actual configuration files, and a list of notable processes running in each zone.

4. Hardening: describe all the hardening steps you took to bring a COTS OS up to code to be a CDS OS.

5. Third-party applications: provide a list of *every one* of these and how you configured them for security.

6. Data filtering and sanitisation strategy: list all potentially harmful user-generated or user-influenced guard-generated data.

7. Source code: including build scripts. This does not imply a full source review, but the penetration testers can save lots of time if they can immediately refer to the source code and quickly find the exact section involved in a potential problem. The source code should be well indexed so they can find the relevant section easily.

LAB SETUP:

1. Installation should be straightforward and simple. It should not take more than half a day. Fully automated installations are best. If your installers have to come to our lab and spend a week setting up, configuring, and tweaking poorly documented settings, that is not a good sign.

2. Support devices: the vendor must provide a list of all environment components needed, e.g., mail, LDAP, web servers, etc. The vendor may have to provide specialised equipment, but we have common items like web servers, mail servers, routers, and so on.

LOADED CONFIGURATION:

1. The configuration loaded on the device under test for NSA laboratory pen testing must be the *riskiest* configuration possible. All deployed filters must be included.

2. Passwords: please don't set all your passwords to the most complex possible. We have to type in those passwords. We promise we won't condemn you for setting easy-to-type passwords on your BIOS, operating system, and other places for the convenience of the pen testers. Don't use classified operational passwords, obviously. But as long as we can see you that support adequate password complexity for security in the field, we won't be displeased if you supply us with reasonable and easy to type passwords for the purpose of laboratory pen testing. Hint hint.

TOOLS:

1. Test data for the transfer CDS must be provided, an adequate suite of test data and full descriptions of the format of the test data.

2. Data delivery: vendors that use closed protocols must provide a complete description and a good test harness. It must allow us to susbtitute our own data in every field, to batch hundreds of messages

together, and to dig into the lowest level bit level representation of every data field. *The assumption must be that the protocol and processes can and will be compromised.* We use data fuzzing extensively in our testing, so make it easy to accommodate that.

WHITE BOXES:

1. You must provide a completely unlocked CDS for laboratory pen testing. The pen testers will immediately want to drop to single user mode and take a look around. So yes, you have to give us the root password.

2. Ideally, provide the CDS on virtual machines. Even better, give us one physical CDS and one virtual, clonable as many times as we need it. By providing a clonable virtual version, the testers can save time by not having to be afraid of breaking something.

Elizabeth Kralik, Code 5.8.3.10 `elizabeth.kralik@navy.mil` on 'Cross Domain Solutions Certification, Testing and Evaluations' in SPAWAR.

Agenda:

- CT&E labs
- SABI vs TABI vs TSABI
- The Navy CT&E process
- CT&E process
- Recently tested Navy CDS systems
- Reciprocity

We are located in Charleston at SPAWARSYSCEN Atlantic. The Army has a lab at Ft Huachuca, and the Air Force has a lab in Rome, New York.

SABI is mostly what we deal with. They have the CDTAB and DSAWG. SABI's focus is more on CT&E (certification) than on ST&E (accreditation).

TABI has no formal process.

TSABI means JWICS, basically. TSABI's focus is more on ST&E (accreditation) than on CT&E (certification), in which they have less interest.

THE NAVY C&A PROCESS:

Phase 0: (preliminary staging) takes 30 days.

Phase 1: (requirements, validation, and prioritisation) takes 45 days.

Phase 2: (solution development and evaluation) takes 60 to 240 days.

Phase 3: (validation) takes 60 to 120 days.

Phase 4: (operation and management) is an annual process.

THE CT&E PROCESS:

Pre-testing: CDS PMO works with NSA to enter their solution into Prism, an NSA system.

Testing: the Navy lab in Charleston receives a system from the vendor; the lab writes and executes tests, which are documented in CASTER (an NSA system).

Post-testing: The lab sends its CT&E report to NSA, who write a Technical Risk Rating (TRR).

Drew York on 'Reciprocity Testing of Radiant Mercury 5'

Agencies involved: DIA, NSA, UCDMO, DNI.

Testing approach:

- reviewed SRTM and vendor input to meet 800-53.
- evaluated vendor's FAT, which DIA witnessed.
- lab wrote 355 tests.
- NSA executed the tests and mapped them to RDAC.

Testing took place in Mar–Apr and June–July of 2010.

Technical Risk Ratings (TRRs) conducted by NSA in October and September 2010. Different TORAs were used, each with its own technical risk rating.

RECIPROCITY TESTING LESSONS LEARNT:

- test steps were shorter because a high level description of tests was used instead of detailed test procedures.
- Repeatability is Difficult. It was difficult to repeat tests precisely based on the high level descriptions.
- Vendor test results were accepted this time; traditionally, all tests are executed by the lab.
- shorter duration: less than two months vs the 4–6 months it usually takes us to do this.

RECENTLY TESTED SOLUTIONS:

DSG v3.1 (220 tests developed and executed) Aug–Oct 2010; TRR in November 2010.

MLTC v4.1 (119 tests) Jul–Sep 2010; TRR in October 2010.

NEST v1.1.1 (282 tests) Oct 2009–April 2010; TRR in May 2010.

NEXT v2.5 (105 tests) May–June 2011.

Question from the audience: was Radiant Mercury 5 tested at above SABI?

Answer: all our testing was done at a single level in a lab environment. Results were shared with the community.

Question: the level above SABI is trying to move to NIST. They have their security controls, we have our security controls, how do we know when to stop?

Answer: Dan Nichols has led the CSTG. The next thing is a standardised test report. We're not there yet, but we're working on it.

Question: of the 355 test cases on Radiant Mercury, how many were specific to one TORA?

Answer: testing was done irrespective of TORA. Did they repeat all 355 tests for every risk level? No.

Be sure not to confuse the terminology: TORA = Target of Risk Analysis (not to be confused with TOE), and TRR is Technical Risk Rating, not Test Readiness Review, in this context.

Question from the audience: do different labs test differently?

Answer: all labs are overseen by NSA and NSA provides our standardised testing policies and procedures.

1400 Track 3: Mike Mayhew of AFRL on 'Cross Domain Innovation and Science Group (CDIS) Overview'

This briefing is releasable to Five Eyes only.

Mr Mayhew is the CDIS Group Manager, AFRL/REIB, Information Handling Branch, Information Directorate, Air Force Research Laboratory in Rome, NY.

They have thirteen engineers looking for future CDS: 'we'll find it, help develop it, or invent it ourselves.'

Key partnerships:

- UCDMO: they recently had a programme review of 35 efforts in AFRL
- IC and DoD
- Air Force collaboration with the cryptologic group, space command, and cyber command.
- Industry; seven universities; 3 CRADAs with 2 more coming up; 20 companies working on cross domain; and 9 CDSes.

Cross Domain Community Outreach:

- CDTF
- IA Metadata Working Group
- National and International cross domain conference participation: AFRL goes to many conferences each year.
- act as SMEs for cross domain reviews

Transition Successes: AFRL helped develop the following familiar products:

- CD Web Services (ICASE)
- Purifile (hidden data identification tool)
- Collaboration Gateway (Cross Domain 1:1 and Group Text Chat)
- Assured RHR Workflow Enforcement Tools and Services (SAWES)

FUNDING:

CDIS Percentage of Efforts in FY11:

1 percent to early research (6.1)

19 percent to basic research (6.2)

23 percent to advanced research (6.3a)

29 percent customer funding

4 percent SBIR Phase I

24 percent SBIR Phase II

AFRL currently engaged in over 25 research efforts.

Cross Domain Innovative Technologies BAA created in FY11.

FY11–FY13 CDIS RDT&E $24 million funding vehicle. They request white papers, review them, request proposals from the best, review those, and then prepare a package.

Other vehicles: SBIR, STTR, CRADA.

CDIS lab: 40 hardware systems, 8 different active CDSes, 4-domain simulation capacity, full presentation capability, VMware server.

CDIS WAY AHEAD: they see four pillars holding up the GIG:

1. Secure data labelling
2. Data loss protection
3. Secure operating environment
4. Common enterprise.

The following 17 efforts will be divided into two groups: Collaboration, and Trust. Of the 35 efforts AFRL have going, here are around half of them:

TRL is Technology Readiness Level. TRL1 and 2 are at the level of basic technology research; TRL3 is getting into research to prove feasibility; TRL4 is technology development; TRL5 and 6 are technology demonstration.

First, the Collaboration efforts, actively sharing information with allies and partners:

1. Cross Domain Web Services Based Publish/Subscribe File Sharing. TRL5, Customer funding (6.3).
2. Cross Domain Voice over IP (CD VoIP). TRL4, AFRL (6.3).
3. CDS Dashboard. TRL3, Customer (6.3).
4. Probabilistic Redaction. TRL3, AFRL (6.2). AFRL just finished the 6.2 and is hoping to get some more funds to make a full prototype next.
5. Alert-to-Share. TRL4, SBIR II.
6. Web Data Aggregation. TRL4, SBIR II.
7. Service Discovery. TRL3–4, AFRL (6.2).
8. Next Generation High Assurance Tactical CDS Research. TRL1–2, CRADA (6.1/6.2).

Now, the Trust efforts: providing information confidentiality, integrity, and availability assurance:

9. Trusted Information Sharing. TRL4, AFRL (6.3).
10. Automated, Assurred Metadata. TRL3–4, ARFL (6.3).
11. Cross Domain Data Way Station. TRL4, AFRL (6.3).
12. Dynamic, Adaptive Security Policy Expression. TRL4, AFRL (6.3). Uses DFCF to pre-configure security policies and pre-accredit them, digitally signed, so the CDS operator can rapidly switch security polices and remain accredited.
13. Steganographic Detection and Extraction. TRL4, AFRL (6.2). It can detect signatures of known steganographic methods with 100 percent certainty, but cannot tell you there is no steganography in the data. They have recently moved to a classified development environment where they are working on high value information types, and are adding a new detector.
14. Cross Domain Identity Management. TRL3–4, Customer (6.2).
15. Advanced Trusted Computing (TC) Research. TRL3, Customer (6.2). They are developing TC Reference Implementations (TCRI).

FY12 CDIS R&D INITIATIVES:

16. Audit-based Sensing and Protection (ASP). TRL2–3, AFRL (6.2). This is a two year effort.
17. Behaviour Based Access Control (BBAC). TRL2–3, AFRL (6.2). This is a three year effort.
18. KLV Enrichment for Video Live-streaming And Retrieval (KEVLAR). TRL2–3, AFRL (6.2). This is a one-year effort with potential follow-on.

SUMMARY:

The CDIS group finds, matures, and builds new and innovative CDS technologies.

Question from the audience: you talked earlier about tactical CDS; can you talk more about it?

Answer: these are CRADA funded; we are looking for a tactical next generation device that can deal with limited connectivity and perhaps tie to a tactical guard in the field. Lighter on the troops than existing tablet or handhelds, with twice the capability.

Question: what specific scenario are you trying to meet?

Answer: What does a soldier need in a cross domain environment? Predator video sent to troops on the ground, for example. Situational awareness from Blue Force Tracking getting up to higher echelons.

Comment from the audience: 'I'm the security architect for Blue Force Tracking. That information is already getting sent to higher echelons.'

Question from the audience: about KEVLAR: do you cryptographically bind attributes to images?

Answer: How to we assure the metadata on video? Yes, using video watermarking, two ways: either we can first take a hash of just the KLV metadata, then cryptographically binding that to the video.

Question: do you know of any other cross domain initiatives for High to Low cross domain VoIP?

Answer: Yes. We invested money in Trident, but wanted to make sure there wasn't a covert channel where an adversary could corrupt the call or steal information. They added noise and beeps to the audio to warn all users that it is a cross domain call, so users will know to speak only at the lower level. Similar to the way it's done in cross domain chat, but for voice.

It also stores and logs all of these calls in a CloudShield box so you can go back later forensically and look for spills.

In future, we are looking to do it with VTC, so if you know how, check out the RIKA BAA and send us white papers.

References