ONE YEAR AFTER COLLATERAL MURDER RELEASE, DOD'S NETWORKS ARE STILL GLARING SECURITY PROBLEM

As I have posted several times, the response to WikiLeaks has ignored one entity that bears some responsibility for the leaks: DOD's IT.

Back in 2008, someone introduced malware to DOD's computer systems. In response, DOD announced it would no longer allow the use of removable media in DOD networks. Yet that is precisely how Bradley Manning is reported to have gotten the databases allegedly leaked. In other words, had DOD had very basic security measures in place they had already been warned they needed, it would have been a lot harder for anyone to access and leak these documents.

Often, when I have raised this issue, people are simply incredulous that DOD's classified network would be accessible to removable media (and would have remained so two years after malware was introduced via such means). But it's even worse than that.

A little-noticed Senate Homeland Security hearing last month (Steven Aftergood is one of the few people who noticed) provided more details about the status of DOD's networks when the leaks took place and what DOD and the rest of government have done since. The short version is this: for over two months after DOD arrested Bradley Manning for allegedly leaking a bunch of material by downloading information onto a Lady Gaga CD, DOD and the State Department **did nothing**. In August, only after WikiLeaks published the Afghan War Logs, they started to assess what had gone wrong. And their description of what went wrong reveals not only

how exposed DOD was, but how exposed it remains.

Two months to respond

Bradley Manning was arrested on or before May 29. Yet in spite of claims he is alleged to have made in chat logs about downloading three major databases, neither DOD or State started responding to the leak until after the Afghan War Logs were published on July 25, 2010.

The joint testimony of DOD's Chief Information Officer Teresa Takai and Principal Deputy Under Secretary for Intelligence Thomas Ferguson explains,

> On August 12, 2010, immediately following the first release of documents, the Secretary of Defense commissioned two internal DoD studies. The first study, led by the Under Secretary of Defense for Intelligence (USD(I)), directed a review of DoD information security policy. The second study, led by the Joint Staff, focused on procedures for handling classified information in forward deployed areas.

In other words, "immediately" (as in, more than two weeks) after the publication of material that chat logs (published two months earlier) had clearly explained that Manning had allegedly downloaded via Lady Gaga CD months earlier, DOD commissioned two studies.

As State Department Under Secretary of Management Patrick Kennedy explained, their response was no quicker.

> When DoD material was leaked in July 2010, we worked with DoD to identify any alleged State Department material that was in WikiLeaks' possession.

It wasn't until November—at around the time when NYT was telling State precisely what they were going to publish—that State started responding in earnest. At that time—over four months after

chat logs showed Manning claiming to have downloaded 250,000 State cables—State moved its Net Centric Diplomacy database from SIPRNet (that is, the classified network) to JWICS (the Top Secret network).

DOD's exposed IT networks

Now, frankly, State deserves almost none of the blame here. Kennedy's testimony made it clear that, while the WikiLeaks leak has led State to enhance their limits on the use of removable media access, they have systems in place to track precisely who is accessing data where.

DOD won't have that across their system for another year, at least.

There are three big problems with DOD's information security. First, as the Takai/Ferguson testimony summarized,

> Forward deployed units maintained an over-reliance on removable electronic storage media.

It explains further that to make sure people in the field can share information with coalition partners, they have to keep a certain number of computers accessible to removable media.

> The most expedient remedy for the vulnerability that led to the WikiLeaks disclosure was to prevent the ability to remove large amounts of data from the classified network. This recommendation, forwarded in both the USD(I) and Joint Staff assessments, considered the operational impact of severely limiting users' ability to move data from SIPRNet to other networks (such as coalition networks) or to weapons platforms. The impact was determined to be acceptable if a small number of computers retained the ability to write to removable media for operational reasons and under strict controls.

As they did in 2008 after malware was introduced via thumb drive, DOD has promised to shut off access to removable media (note, Ferguson testified thumb drives, but not CDs, have been shut down for "some time"). But 12% of the computers on SIPRNet will still be accessed by removable media, though they are in the process of implementing real-time Host Based Security System tracking of authorized and unauthorized attempts to save information on removable media for those computers.

In response to a very frustrated question from Senator Collins, Ferguson explained that DOD started implementing a Host Based Security System in 2008 (the year DOD got infected with malware). But at the time of the leak, just 40% of the systems **in the continental US** had that system in place; it was not implemented outside of the US, though. They weren't implemented overseas, he explained, because a lot of the systems in the field "are cobbled together."

In any case, HBSS software will be in place by June. (Tech folks: Does this means those computers are still vulnerable to malware introduced by removable media? What about unauthorized software uploads?)

Then there's data access control. DOD says it can't (won't) password protect access to information because managing passwords to control the access of 500,000 people is too onerous for an agency with a budget larger than Australia's gross national product. Frankly, that may well be a fair approach given the importance of sharing information.

But what is astounding is that DOD is only now implementing public key infrastructure that will, first of all, make it possible to track what people access and—some time after DOD collects that data—to start fine tuning what they can access.

> DoD has begun to issue a Public Key Infrastructure (PKI)-based identity credential on a hardened smart card.

> This is very similar to the Common Access Card (CAC) we use on our unclassified network. We will complete issuing 500,000 cards to our SIPRNet users, along with card readers and software, by the end of 2012. This will provide very strong identification of the person accessing the network and requesting data. It will both deter bad behavior and require absolute identification of who is accessing data and managing that access.
>
> In conjunction with this, all DoD organizations will configure their SIPRNet-based systems to use the PKI credentials to strongly authenticate end-users who are accessing information in the system. This provides the link between end users and the specific data they can access – not just network access. This should, based on our experience on the unclassified networks, be straightforward.
>
> DoD's goal is that by 2013, following completion of credential issuance, all SIPRNet users will log into their local computers with their SIPRNet PKI/smart card credential. This will mirror what we already do on the unclassified networks with CACs.

[Takai defines what they're doing somewhat just before 88:00]

Note what this says: DOD is only now beginning to issue the kind of user-based access keys to protect its classified network that medium-sized private companies use. And unless I'm misunderstanding this, it means DOD is only now upgrading the security on its **classified** system to match what already exists on its **unclassified** system.

Let's hope nothing happens between now and that day in 2013 when all this is done.

And this particular problem appears to exist beyond DOD. While the two DIA witnesses mostly blew smoke rather than provide a real sense of where security is at (both blamed WikiLeaks on a "bad apple" rather than shockingly bad information security), the testimony of DNI's Intelligence Community Intelligence Sharing Executive Corin Stone seems to suggest other parts of the IC area also still implementing the kind of authentication most medium sized corporations employ.

> To enable strong network authentication and ensure that networks and systems can authoritatively identify who is accessing classified information, the IC CIO is implementing user authentication technologies and is working with the IC elements to achieve certificate issuance to eligible IC personnel in the first quarter of fiscal year 2012.

So that's the issue of removable media and individualized access tracking.

Which leaves one more big security hole. According to Takai/Ferguson, DOD didn't—**still didn't**, as of mid-March—have the resources in place to detect anomalous behavior on its networks.

> Limited capability currently exists to detect and monitor anomalous behavior on classified computer networks.

This confirms something Manning said in chat logs: no one is following the activity occurring on our networks in Iraq (or anywhere else on SIPRNet, from the sounds of things), and flagging activities that might be an intrusion.

The part of the Takai/Ferguson testimony that details very hazy plans to think about maybe implementing such a system (pages 6-7) is worth a gander just for the number of acronyms of titles of people who are considering maybe what to implement some time in the future. It's all a

bunch of bureaucratic camouflage, IMO, to avoid saying clearly, “we haven’t got it and we haven’t yet figured out how we’re going to get it.” But here are the two most concrete descriptions of what the Department of **Defense** plans to do to make sure no one is fiddling in their classified networks. First, once they get HBSS completely installed, then they will install an NSA audit program on top of that.

> One very promising capability is the Audit Extraction Module (AEM) developed by the National Security Agency (NSA). This software leverages already existing audit capabilities and reports to the network operators on selected audit events that indicate questionable behavior. A great advantage is that it can be integrated into the HBSS we have already installed on the network, and so deployment should be relatively inexpensive and timely. AEM is being integrated into HBSS now and will be operationally piloted this summer.

But in the very next paragraph, Takai/Ferguson admit there are better solutions out there. But DOD (again, with its budget larger than the GNP of most medium sized countries) can’t implement those options.

> Commercial counterintelligence and law enforcement tools – mostly used by the intelligence community – are also being examined and will be a part of the overall DoD insider threat program. These tools provide much more capability than the AEM. However, while currently in use in some agencies, they are expensive to deploy and sustain even when used in small, homogeneous networks. Widespread deployment in DoD will be a challenge.

In other words, DOD wants to be the biggest part of the intelligence community. But it and its

budget bigger than Brazil's GNP won't implement the kind of solutions the rest of the intelligence community use.

Department. Of. Defense.

Now, let me be clear: DOD's embarrassingly bad information security does not, in any way, excuse Bradley Manning or the other "bad apples" we don't know about from their oath to protect this information. (Note, there was also testimony that showed DOD's policies on information sharing were not uniformly accessible, but that's minor compared to these big vulnerabilities.)

But in a world with even minimal accountability, we'd be talking about fixing this yesterday, not in 2013 (five years, after all, after the malware intrusion). We'd have fired the people who let this vulnerability remain after the malware intrusion. We'd aspire to the best kind of security, rather than declaring helplessness because our very expensive DOD systems were kluged together. And we'd be grateful, to a degree, that this was exposed with as little reported damage as it has caused.

If this information is really classified for good reason, as all the hand-wringers claim, then we ought to be using at least the kind of information security implemented by the private sector a decade ago. But we're not. And we don't plan on doing so anytime in the near future.