File 20110727.1958: A very interesting email exchange just went by involving the government programme office, developer, and certifier. I was asked to give an opinion; I wrote:

```
From: Loughry, Joe
Sent: Wednesday, July 27, 2011 7:48 PM
To: Miller, Kevin R
Cc: Christensen, Craig M
Subject: RE: CD foreign release

In the following discussion, I shall talk about guards in general, avoiding
specifics for the reasons we discussed.  More particularly, PL-4 guards with
more functionality than, for example, a CUBIC one-way device or a data diode.
Guards with at least the functionality of a packet inspection device.

The security policy requires that the device be used in a controlled
environment with cleared users.  I reference the superseded DCID 6/3 Appendix
E, which made it clear that foreign persons were not to be allowed privileged
accounts on the device.

The device is extremely resistant to attack from the network.  This has been
verified and endorsed by NSA under the auspices of the certification testing
of 5.0.1.  Their penetration testers were unable to defeat it, cause a denial
of service, or compromise the system when they controlled the network.  The
certification testing did not extend to source code analysis, beyond the
developer's own quality assurance measures which do extend to static source
code analysis for weaknesses.  Recall the report by [redacted] that prompted
the guard developer to acquire and begin using static source code analysis.
That was a moderately motivated attacker with high skill and moderate
resources; they did not spend a huge amount of time on it, nor did they use
exotic tools.

It was not designed for resistance to reverse engineering by an attacker with
unlimited access to the console and hardware.  A typically configured guard in
the field is stripped of unnecessary data formats not essential to the
mission, hence would not expose vulnerabilities in unavailable data formats.
But the core system would be fully exposed to reverse engineering, including
reverse engineering of the parser/formatter, input and output channel
executable code, remote monitoring and maintenance executable code, and
hardware (including a representative sample of NICs) and TEMPEST measurements.

There are no protections against reverse engineering.  The operation of the
integrity monitoring system is open to be observed.  The GUIs and the
parser/formatter can be put on a test bench and exercised with unlimited
amounts of test data.

Analogous situations have arisen in the past.  Prepaid electric meters (used
in parts of Scotland and Africa), PCI-compliant credit card point of sale
terminals used throughout Europe, and cable TV set-top boxes used in America
have all been successfully reverse engineered by highly motivated attackers
with medium to high resources (i.e., academic security researchers) and high
skill taking advantage of the unlimited access available to users.  To a
lesser extent, highly tamper-resistant FIPS 140-2 cryptographic modules have
been compromised with partial success by highly motivated attackers with high
skill and high resources (e-beam probing).  The best current example of a
highly motivated and high skill attacker with unlimited resources, against
admittedly an unprotected target, is Stuxnet.  If the guard is exported
outside Five-Eyes, you must assume as the worst case that a Stuxnet-level
attacker with high skill, high motivation and unlimited resources will
eventually obtain and examine it.  The value of the information handled by the
guard at certain locations makes the cost-benefit tradeoff attractive to
foreign intelligence agencies.
```

It would also be wise to assume that attackers have a complete collection of IAVM reports and read them with interest.

-Joe Loughry CISSP-ISSEP

-----Original Message-----
From: Miller, Kevin R
Sent: Wednesday, July 27, 2011 2:26 PM
To: Loughry, Joe
Subject: FW: CD foreign release

Joe,
Give me a call to discuss this. I would like to get some of your inputs.

Kevin R. Miller
303-932-4786

-----Original Message-----
From: Christensen, Craig M
Sent: Wednesday, July 27, 2011 12:36 PM
To: Miller, Kevin R
Subject: FW: CD foreign release

Coming down to talk to this.

-----Original Message-----
From: Griffin, Dan J CIV PEOC4I, 613A0 [mailto:daniel.griffin@navy.mil]
Sent: Wednesday, July 27, 2011 9:15 AM
To: Christensen, Craig M
Subject: EXTERNAL: RE: CD foreign release

Left a vm. Give me a call.

Dan Griffin
APM
Radiant Mercury, PMW 130
619-524-7344/DSN 524-7344
619-204-2716 (C)

-----Original Message-----
From: Griffin, Dan J CIV PEOC4I, 613A0
Sent: Wednesday, July 27, 2011 7:37
To: Sinkular, Francis James
Cc: Rubel, John P CTR OPNAV N2\N6F1136; john.p.rubel@accenture.com; Bowden, Dennis [USA]; Lazarski, Edward F Jr CDR PEOC4I, 613A0
Subject: RE: CD foreign release

Frank,

Thank you for the update. I will tell the P5CTS Program that we are on hold.

Dan Griffin
APM
Radiant Mercury, PMW 130
619-524-7344/DSN 524-7344
619-204-2716 (C)

-----Original Message-----
From: Sinkular, Francis James [mailto:fjsinku@nsa.gov]
Sent: Wednesday, July 27, 2011 5:35
To: Griffin, Dan J CIV PEOC4I, 613A0
Cc: Rubel, John P CTR OPNAV N2\N6F1136; john.p.rubel@accenture.com; Bowden, Dennis [USA]
Subject: RE: CD foreign release

Dan,

Spoke with them and Mark Morrison. Aris has been trying to contact you, he has spoken with his contacts in DTSA and right now the instructions are to put these sales on hold for the immediate future and they develop some interim guidance for handling these requests. On another note, I attended the Flag Panel yesterday and the question of what is the risk to the GIG if we these things beyond five eyes? The task has fallen to me (again) to pull together a team from NSA, AFRL, ODNI, SPAWAR Charleston, UCDMO to discuss the designs of CD's and what is if any the risk to the GIG. Basically the so what factor. I am toying with the idea of asking a couple of PMO's to participate also and you would be one of them.

Frank Sinkular
Acting Director
Unified Cross Domain Management Office
Army Research Lab
room 110, building 601
2800 Powder Mill Road
Adelphi, MD 20783
240-373-0796
fjsinku@nsa.gov

-----Original Message-----
From: Griffin, Dan J CIV PEOC4I, 613A0 [mailto:daniel.griffin@navy.mil]
Sent: Tuesday, July 26, 2011 3:52 PM
To: Griffin, Dan J CIV PEOC4I, 613A0; Sinkular, Francis James
Cc: Rubel, John P CTR OPNAV N2\N6F1136; john.p.rubel@accenture.com; Bowden, Dennis [USA]
Subject: RE: CD foreign release

Frank,

Did you get a chance to speak with Gus and Aris and what was the outcome of your discussion with them? I need to get back to P5CTS guys so they can move forward or not with their plan.

Thanks,

Dan Griffin
APM
Radiant Mercury, PMW 130
619-524-7344/DSN 524-7344
619-204-2716 (C)

-----Original Message-----
From: Griffin, Dan J CIV PEOC4I, 613A0
Sent: Tuesday, July 12, 2011 11:44
To: Sinkular, Francis James
Cc: Rubel, John P CTR OPNAV N2\N6F1136; john.p.rubel@accenture.com; Bowden,

Dennis [USA]; Lazarski, Edward F Jr CDR PEOC4I, 613A0
Subject: RE: CD foreign release

Frank,

Thanks for the call. My SIPR and JWICS below just in case you need it.

SIPRNET: daniel.griffin@navy.smil.mil
JWICS: dgriffin@spawar.navy.ic.gov

-----Original Message-----
From: Sinkular, Francis James [mailto:fjsinku@nsa.gov]
Sent: Tuesday, July 12, 2011 11:10
To: Griffin, Dan J CIV PEOC4I, 613A0
Cc: Rubel, John P CTR OPNAV N2\N6F1136; john.p.rubel@accenture.com; Bowden, Dennis [USA]; Lazarski, Edward F Jr CDR PEOC4I, 613A0
Subject: RE: CD foreign release

Dan,

Wow...talk about throwing a grenade into the room! This would rankle a few more people than just Gus and Aris. I am trying to pull this meeting together as soon as possible to insure we do the right thing. I also think we need to move this up to SIPR as things may get dicey my SIPR address is fjsinku@nsa.smil.mil. For now buy as much time as possible, probably a few weeks. When I met with Aris last week he thought one of the first steps was to have DTSA or some other entity put a cease and desist notice out until all of this gets figured out. See you on SIPR.

Frank Sinkular
Acting Director
Unified Cross Domain Management Office
Army Research Lab
room 110, building 601
2800 Powder Mill Road
Adelphi, MD 20783
240-373-0796
fjsinku@nsa.gov

-----Original Message-----
From: Griffin, Dan J CIV PEOC4I, 613A0 [mailto:daniel.griffin@navy.mil]
Sent: Tuesday, July 12, 2011 1:00 PM
To: Sinkular, Francis James
Cc: Rubel, John P CTR OPNAV N2\N6F1136; john.p.rubel@accenture.com; Bowden, Dennis [USA]; Lazarski, Edward F Jr CDR PEOC4I, 613A0
Subject: RE: CD foreign release

Frank,

Called several times but you were not in. I wanted to talk to you about another potential FMS case and to get your take on how we should proceed.

We participated in a telcon yesterday with a US Navy FMS Case Manager and the USAF P5 Combat Training Systems (P5CTS) FMS Program Manager. P5 CTS is the same program office that provided an RM to Poland. This FMS sale, as it was with Poland, their product is part of a bigger FMS case involving F-16's to Moroccan RAF. They are also looking at another FMS sale to Saudi Arabia.

They would like us to be part of their FMS sale on both. I explained to them about NII/DoD CIO's concerns and they understand but they would like our answer soon so they could develop a backup plan if we cannot support them.

Based our discussion on FMS sale to Poland back in April at the RMUG, I would gather that Aris Yortzidis and Gus Guissanie would have a serious concern with these FMS sales. If you were in my place how would you proceed? Who has the final word on exporting CDS technology? Is Aris the right person to start from? Does he already know about Poland?

Do you also know if there are other guards that being sold to a foreign country?

Dan Griffin
APM
Radiant Mercury, PMW 130
619-524-7344/DSN 524-7344
619-204-2716 (C)

-----Original Message-----
From: Sinkular, Francis James [mailto:fjsinku@nsa.gov]
Sent: Tuesday, July 12, 2011 7:41
To: Griffin, Dan J CIV PEOC4I, 613A0
Cc: Rubel, John P CTR OPNAV N2\N6F1136; john.p.rubel@accenture.com; Bowden, Dennis [USA]
Subject: RE: CD foreign release

Gus is the Deputy Assistant Secretary of Defense (DASD) for Identity and Information Assurance so he is policy and Aris works in his organization as a rep for the Defense Technology Security Administration (DTSA) read action officer. Gus was one of the seniors who voted that no release of CDS technology to NATO and Aris is going to help us see what needs to be done in the ITAR process to make sure due diligence is done. We are going to try and have a meeting next week to develop a way forward. Don't know how all this will play out, it may be that there will be a few more hoops to jump through if it is a NATO sale, nothing goes to NATO, too bad you can't stop it, or something else. Will keep you guys posted.

Frank Sinkular
Acting Director
Unified Cross Domain Management Office
Army Research Lab
room 110, building 601
2800 Powder Mill Road
Adelphi, MD 20783
240-373-0796
fjsinku@nsa.gov

-----Original Message-----
From: Griffin, Dan J CIV PEOC4I, 613A0 [mailto:daniel.griffin@navy.mil]
Sent: Monday, July 11, 2011 4:52 PM
To: Sinkular, Francis James
Cc: Rubel, John P CTR OPNAV N2\N6F1136; john.p.rubel@accenture.com; Bowden, Dennis [USA]
Subject: RE: CD foreign release

Frank,

What is Aris Yortzidis's and Gus Guissanie's position within their organization? Are they both at the policy or action officer level? Do you know what their concerns are with respect to CDS?

Dan Griffin
APM
Radiant Mercury, PMW 130
619-524-7344/DSN 524-7344
619-204-2716 (C)

-----Original Message-----
From: Sinkular, Francis James [mailto:fjsinku@nsa.gov]
Sent: Thursday, July 07, 2011 5:06
To: Yortzidis, Aris CIV NII/DoD-CIO; Griffin, Dan J CIV PEOC4I, 613A0
Subject: CD foreign release

Dan,

I would like to introduce you to Aris Yortzidis from Gus Guissanie's shop. He will be helping us resolve the foreign release issue and may need to ask you a few questions so he understands the history better. I know it has been a couple of months since we talked but getting to the right people has been a challenge. Hopefully, now that Aris is involved we can move this forward and come to an acceptable resolution for all involved.

Aris,

Dan is the PM for Radiant Mercury and a good guy , he will do all he can to help you out.

Regards,

Frank Sinkular

Acting Director

Unified Cross Domain Management Office

Army Research Lab

room 110, building 601

2800 Powder Mill Road

Adelphi, MD 20783

240-373-0796

fjsinku@nsa.gov <mailto:fjsinku@nsa.gov>

I think this is a highly significant email exchange, not only because of the range of people mentioned and involved in it. While approval for foreign military sales of RM was recently obtained, I have heard, it was not expected that any of those sales would be outside the Five Eyes countries, who could be expected not to transship the guard outside NATO. As I said on a phone call with Kevin Miller and Craig Christensen, who is to say the guard—or a bit copy of the disk—wouldn't be transshipped from Germany to Bosnia to Libya to North Korea to China, where the highly motivated and highly skilled attackers with unlimited resources are?

Not sure how much of this I can write about in an open source dissertation, but it is interesting and relevant.

References