HW CWE SIG Meeting

Friday, June 14, 2024

Members in Attendance

Gananand G Kini	Monroe, Bruce	Hallman, John (DI SW ICS DVT SM)
Bob Heinemann	Mell, Peter M. (Fed)	Charles Timko (Red Hat)
Alec J Summers	Constable, Scott D	Evan Bryers
Steven Christey Coley	Bojanova, Irena V. (Fed)	Jason Oberg (Cycuity)
Gage Hackford	Frost, Sandy	Mohan Lal
Nicole Fern	Ahmed, Faheem	Swami, Shivam
James Pangburn	Ford, Thomas	Das, Amitabh
Mike Borza	Rich Piazza	Iyer, Priya B
Forbes, Justin	Kepa, Krzysztof	Salehi, Soheil
Sathyamurthi Sadhasivan	Masike, Takunda	
Manna, Parbati K	Milind Kulkarni	

Agenda

- Co-chair announcement
- Usability Task Micro Updates
- Mapping Diagrams

Housekeeping

- Next meeting: July 12th, 12:30 – 1:30 PM EST (16:30 – 17:30 UTC), MS Teams.
- Contact: cwe@mitre.org
- Mailing list: hw-cwe-special-interest-group-sig-list@mitre.org
- Minutes from previous meetings: https://github.com/CWE-CAPEC/hw-cwe-sig

Announcements

- CWE 4.15 release will be July 16

Co-chair Announcement and Remarks

Manna Parbati has been selected for co-chair.

Manna Parbati: Thank you, everyone. I have been involved with this project for a long, long time and it started with a few of my friends and colleagues at Intel who are I believe they are here Harish, Arun,

Jason, Bruce; I do not know if Dinesh is here, but on the MITRE side like Alec, Ganu, we started in the Jones Farm. We were trying to figure out if there were going to be, should we need a separate category for figuring out which are the main weaknesses or not. It is so gratifying to see that right now it is. We have a special interest group. There are so many people from the industry who are contributing. I'm so thankful to be working with you guys. I have learned so much about it. I'm not telling you what my vision is because you know, I do not want to steal my thunder so. It has been a great privilege and pleasure to work with you till now, and I really hope that that is going to be the continual path forward. You can see my bio here. I do not want to talk more about my academic stuff, but I am a standup comedian on the amateur level. I'm a musician and those are the kind of things I like, I really like to make jokes, and if you do not dare to work with me, trust me, I'm going to punish you with dad jokes which are even worse than Bhagwan poetry. So, you have been warned.

Usability Task Micro Updates Initial Goals

Bob: There is a user experience working group. They are working through:

1. Make it easier to consume the content.
2. Looking at the descriptions themselves and make sure they are written in a more precise way. Attacker focused language will be taken out.
3. Extended description is looking to be removed.
4. Adding images to support the summary of the weakness itself.

Question: From laptop or mobile?

Bob: Focus is a laptop. Consumption on mobile device isn't part of this discussion.

Bob: Lots of talk around about how to make some changes to the way that elements and weaknesses themselves are presented to make it easier to consume the content. This is what's being referred to as usability work or the usability task.

Also discussed micro and macro changes:

1. Micro changes deal with just the entries themselves how the how the data is displayed in the entry - this is referring to the micro updates.
2. Macro changes deal with the broad changes in the website itself and the infrastructure potential infrastructure changes.

Within this first release 4.15, we're looking to make a few changes to some subset of the top 25 CWE entries, which are software focused. Things that are above the fold or translate to the website, the things that you can read before you start scrolling on the website. In practice we are looking to take a look at this weakness and the descriptions themselves and making sure that they're written in a more concise way. Any language dealing with consequences or attacker focused language or technical impacts would be taken out.

The initial effort is focused just on the top 25 entries. No current plans for hardware CWEs, but as this rolls out over time, there may be some interest in applying this to the hardware CWEs.

Google Drive link has a set of mock-ups that you can take a look at and make comments in line in the Google Doc, or you can send comments directly to Bob.

***CWE – 22 Mockup* – Graphic displayed**

- Left this is what the entry looks like today.
- Right is proposal of what a new entry would look like.

Community Feedback

Jason: I have a question about the scope? How do you define the scope about which ones will be prioritized and why is hardware CPE being called out to not be in scope right now? Is it coming from the most used entries or hard to understand from a criteria that you receive like feedback from the user that you prioritize first or what some other criteria are you thinking about currently?

Bob: As a team, we haven't really thought through criteria in that way. There has been, not within this user group, but within other user groups for CWE, mostly on the software side, there's been a lot of feedback about the difficulty of processing the amount of and density of the entries. There was a priority for this release to show that we're making some progress on that. Internally we made the decision just to focus on the top 25 because they're highly visible, but after that a sort of prioritization scheme is not something that we had decided on. If here's comments from that group of how to do that, we would we'd like to hear that as well because we're still figuring that out.

Jason: I can understand top 25 is having a lot of visibility for those entries and for anyone new it will help them to be on top of the most important ones and I think the flip side of it is that since it is already on top 25, it is well aware by the community and maybe even have more collaterals outside of CWE that helps to explain that entry. I'm thinking for the benefit for hardware CWE, right? If we want to get more people to understand this new domain, especially those coming from a domain like software that are not familiar with the usual practices or the concepts that we bring in, it seems to me that it may worth more to prioritize over highways to be, especially some of those block diagrams or flowcharts can help explain the system concept much clearer than a software concept that may not require such a block diagram to show the relationship. Just a suggestion for your consideration.

Bob: could you just summarize your suggestions? Let's consider that there should be, in our next round of prioritization for usability and for these micro changes, some subset of hardware CWEs.

Jason: Yeah, for the reason that hardware CVE is still new to the general community and hardware CVEs typically focus on system and components interaction for people who may not have the background, they would be able to appreciate through a diagram, a block diagram how those relationship works.

Bob: Yes, that is good feedback. I think the work that's involved now in the usability changes is there's a read the rewrites of the description themselves or the modifications and that's challenging from the standpoint of we want to make sure that we're not expanding the scope accidentally or unintentionally or narrowing the scope because that has mapping consequences. But if this group feels that there is a hardware set to be used that would just benefit just with the addition of an image in the description, we could do that separately than the usability updates that we're doing now in the top 25. Involves the descriptions themselves. That’s actually a lot lighter of a lift.

Shaqfat: When I look at the CWEs on the website, they are arranged in a hierarchical way, right? I could navigate down and then I can handle the related ones as well. But sometimes when I'm in my company, I

would like to have them in the form of Excel or something or the XML format, but all of them are in a flat hierarchy.

I was wondering if there is any like plan on improving those so we keep when we export it to other formats, we keep the hierarchy and relations between things. Like Nick said, so when it's exported to XML, it's like child nodes.

Bob: There's actually there's actually been a JSON API that we are working on, which may help in terms of accessing the corpus in a way that's conducive to what you're trying to do or your workflow.

Action: What I can do is I can follow up with Rich that's been leading that to see where we're at and may even be able to get you some early access to that if that's an interest to you.

Shaqfat: Yes, please. That would be really interesting.

Mapping Diagram/Decision Tree

Describes flow chart at the bottom here. Graphically provides an easy to follow way out of the four transient execution weaknesses and answers the questions of how do you know which one to map and what particular vulnerability to map to.

We wanted to highlight that this diagram exists and that we are able to add images to the vulnerability mapping notes. If there are other entries that you feel that would benefit from a similar diagram, please let us know and especially if you could provide said diagram.

Arun: Is it possible to add this kind of mapping at the class level for them? Could we add this for the related ones at least?

Bob: This example, it is at the class level, and I think these have the most value at the class level. **We can take this conversation offline, or Matt can link up with Arun.**

Jason Fung: Since its already top 25, if we want to get more people to understand this domain it seems that its worth more to prioritize block diagrams and flow charts

Summary

- Effort to make the CWE entries easier to use and consume
- Initial effort is focused on CWE Top 25 entries
- Currently there are no plans for HW CWEs
- Current set of mockups are available for public comment

Covert Channel Coverage in CWE

Quick recap. Jason mentioned covert channel should be visible in view. If covert channel should be there, here are a few aspects to consider:

1. Where should it be?
2. Is the covert channel focused on a hardware weakness?
3. Do we need to tweak it?
4. Should have a separate for hardware? There are enough of these that you'd have to have a separate class.

Jason: At a baseline, it should naturally just fit into the HW view. Covert there are 2 adversaries trying to collude. It seems like both should be added.

This is described as more of a side channel, but at the same time, CW208 does not exist in the hardware view.

Question: Are covert channels weaknesses?

Bob: This is a theoretical type discussion and it's not a quick solution but I just like to hear other people's views on just using the term covert channels is when we're referring to weaknesses.

Question: Do we really think that is weakness?

Hareesh: I think more than language semantic industry wise it has become. Something that is intuitively understood. I think if we drill down to language wise, then yeah, it's debatable.

Irena: I have a strong opinion on two points. The first one is it's better CWs not to overlap. The second one is the covert side, are practically the exploit vectors that the attacker uses to actually achieve a failure. What creates the channels would be the weakness, but some channels don't even require a weakness, they just are there by themselves. There's no accusation for them, like from hardware or software directly.

Industry view on Covert Channel (from Intel)

Manna: So, here is a quick recap of what we went through. We have had quite vigorous discussion regarding a number of aspects of Covert Channel. For example, Jason, the Oberg, the Oberg, Jason, it should, I mean, he mentioned the very salient point that the covert channels should be covered in our hardware view. If you look into the view today, it is not there. And then, well, if it is going to be there, where it should be. That is the point where Paul had chimed in and we found that actually it can find home in more than one category like the security flow issues, general circuitry and logic design concerns, or even just debug and test problems, all those kind of things. And finally Bruce had chimed in that if you look at the current CWE entry for the cover channel, the way theCWE- 514 is written, it's like very much tailored and it only exists in software and it needs to be tweaked. So here are the main questions. Do we really need to modify this entry because right now the covert channel that is if you look at it in the CWE it is pretty much a bare bone entry - like I mean it is just the timing and storage to children those kind of stuff. Do we need to modify it to ensure that there are more hardware centric concerns?

And there is the philosophical question that Covert channel - is it focused on a hardware weakness, or is it really a great attack kind of like it is more of a what the attacker did to achieve rather than just due to a weakness inherent in the hardware. Which way should we think about?

Right now, this is what we have in the CWE. This is a class level, not a pillar level. And it is a child of CWE-1229, which is creation of the emergent resources, which if I remember correctly, that itself also a class, not a pillar. And right now, we are allowing a vulnerability to be mapped to this one. And like after careful review and all, However, if you look at it, it is right now the parent of only the timing channel and the storage channel. There are many, many other covert channels that are possible, like I mean, I do not even want to go through all of it. The kind of electromagnetic radiation, even the acoustics. There are even, for example, like the temperature based, the sensor based. There are so many different ways you can have a covert channel depending on the hardware we are using. For example, if we are using a switch mode power supply, then just by looking at the power analysis we can have a covert channel. Should we be having even more children like that way rather than having just a storage and timing? So that's an open question.

So this is where Intel kind of stepped in. One reason Intel tried to kind of formalize all these side channel and covert channel these discussions was that after the Spectre and Meltdown there was a lot of other exploits and pretty liberal usage of the terms like this is a side channel, this is a Spectre-like side channel, hey this one is like Meltdown 2, those kind of all different kind of things. So Intel thought it will be a good idea to figure out and have a kind of formalized way of what is a channel, what are the different kind of channels. And that's where Intel basically told that like, if you are thinking about computer system then all the communication which is happening, you can call it a channel, like communication channel. There can be only two types. One is a legitimate communication channel, for example, if you are having a an Ethernet or maybe just a pipe IPC communication socket, those kind of things that is the legitimate way to entities are communicating. However. They are could also be Unintended communication channels and Those are the ones which we are calling the “incidental” channels. If you are thinking from a programmatic point of view, you can think of them as the side effect. So these incidental channels, why they happen? Well, the way we have created the microarchitecture, whenever we are architecting a CPU or any similar computing things, there are invariably resources which we create, which are shared by multiple things. For example, if we are trying to access the memory, there is going to be a memory bus. Now, if it is a multi-core system, there could be memory accesses coming from two different cores. So right now they are trying to vie for the same shared resources. So what are you going to do? Are you going to create a dedicated memory bus for every core? Sure, doing that would give you great isolation. But there are many, many bad effects of that, too. It will consume a lot of power and there are many, many such things. The point is that in order to create an optimum product, there are going to be sharing of resources. And the moment you involve some sharing of resources, then there are going to be contention and there are going to be ways in which an attacker might be able to use that, how that contention can be played to their benefit. So that's why all those incidental channels, they are happening. And the two channels which Intel has categorized under the incidental channels are the covert channel and the side channel. And the way we are differentiating between the two is that, In case of over channels. The adversary is not only going

to just listen, but they are also going to send something. So what are they going to send? Of course they are going to send something valuable, some secret. Therefore, in order for it to be qualifying as a covert channel, the adversary is also going to be having access to the secret first. And then they are going to control accessing the secret, transmitting the secret, and then receiving the secret. On the other hand, if we just want to contrast it with the side channel, there most of the time the adversary is just listening. So that is the main categorization which we are doing at Intel kind of formalizing so that people do not suddenly start talking about. Hey, this is a side channel, this is like Spectre.

And here is the question. Right now. The cover channel, which one we have defined, the CWE-514, that is a child of the CWE-1229 that the creation of emergent resources. I understand that the name is not very intuitive kind of thing, which does not tell like thinking, okay, what the heck is emergent resources? But like the incidental channels like the side channels is one thing, but of course there are different ways like you can use like for example with the advent of Crypto like there might be ways an adversary might just trick you into (mining the coins for you all those kind of things). So that way you are also providing your resources to an adversary. So. Right now this is our parent for CWE-514 but we are not fully sure like is it a proper parent-child relationship, like it should be a sibling kind of thing here with the CWE-1229.

So, Intel has once again tried to come up with a kind of comprehensive strategy and categorization of what are the different kind of incidental channels and how we can even think about mitigating them. So there are, when we are talking about incidental channels, like I mean, we are, I mean, of course, remember, it covers both covert and side channels, like those are both incidental channels. If it is legitimate channel, it is not like a covert or side, those kind of things. So the CPU physical incidental channels, it could be like due to the power. You know, there are a lot of power analysis tools and the acoustics, just the noise from there.

Even temperature, by how much heat it is generating even that could give away like what kind of computation are going on and the EM radiation. There is one thing common of all these things. You kind of need a physical proximity to measure all these things. These are kind of not available internally. You kind of need to be sitting next to the actual computing resource. And this was one of the things which CIA in the height of the Cold War. CIA and all the intelligence community was really anal about like well, if somebody is going to measure all the things they have to transmit, they would require a power source. So either it got to be making sure that nobody who does not have the clearance come near the computing, or make sure that there are no batteries because you require a battery if you have to transmit too far. However, there were even a lot of stories where no batteries were required, especially one specific the seal which was presented by the Russians to the American ambassador in Russia and The NSA took it apart and found that there are absolutely no batteries inside it. So therefore they let it be there, but they did not know that when they thought that no power was there, but the Russians from outside the embassy they would irradiate it with the microwave and it will actually emit back

and that was the time it was getting the power. So however, so the reason we differentiate between things that. All these entities which are supposed to be requiring a physical proximity, right now that is kind of changing. Why? Because we are kind of also sometimes making these things available by the software itself. One great example of that would be that RAPL, which is the Runtime Average Power Limit. And why Intel created this? I think it came in Sandy Bridge. Anyway, basically to let the drivers and other people who write on x86 like hey, there's a great interface. You can measure the power of the cores. You can measure the power consumption of all the memories, GPU, everything very, very fine tuned. How to optimize your program so that it is not power hungry? RAPL helped with those kind of things. Unfortunately, with great power comes greater responsibility. We made it easy for the good guys writing the device drivers, and the bad guys thought, oh, this is great. Now I do not need to be sitting next to the computer for measuring its power. I can just access the RAPL interface itself, and that's going to give me all the fine-tuned access of exactly how much power is being used wherever. And right now, when the Cryptographic operations is running or some other thing is running, There is DPA like I have the precise information. I mean this is what happens when you make it available via software. I'm pretty sure that you guys remember all the Volkswagen and those kind of where instead of measuring the emission from the tailpipe. All these car manufacturers they told will just tell the emission how much you are emitting just in the software itself. You just plug in your input to our ODB2 port, and the software itself will give you the thing. And we all know how it turned out.

To conclude, do we need to tweak the CWE-514 (Covert Channel) for the more hardware-centric concerns? And or there should be a completely new covert channel like weakness for hardware (like do we have for one for software one for hardware those kind of things)? And, do we accept that Covert Channel is due to a weakness in the hardware or like it is mostly for the like attacker focused those kind of differentiation. Do we put it in the hardware view coverage view (it is not there today).

Hareesh: I think for, I don't know, if we're trying to define for weakness, I would say for like in covert channel, I would like second, like it should have a separate sort of weakness category for like hardware. Because I don't know if you want to split in terms of the different ways the channels can be existing and if each new method is a weakness but there are enough of these that you would have to have separate class and there is enough sort of hardware specificity right because behavior of circuitry defines or creates these so things that are covert channel because of some hardware logic. Physical characteristic that would need to be in some separate hardware. Right, and I think you were presenting like the Relation with the other where it is currently. Yeah, that also probably has to be. Changed or more because that category seemed a bit weird just on the description.

Jason Oberg: So, yeah, I think personally, I think at a baseline there's, was it CW385 that's covert channel that I can see in the research topics view to me that should naturally just fit into the Hard review mean even as written. It's general enough. That's one thing and I think there's a whole notion obviously of covert and covert and side channel, right which have subtle differences, I think more about Covert there's two adversaries trying to collude and time era side channels. Typically, it's leaking something Unexpectedly in some respects but but in both cases, there's also CWE 208 which is more of a side channel and Neither of those, neither CW385 nor 208 in the hardware view, and it seems like both should be added. And actually, coincidentally, CW208 actually has a hardware example, but it doesn't exist in the hardware view. So that may, that's just an oversight or mistake or something. But that would be my suggestion, at least to start. This is described more of a side channel, but at the same time, 208 has, one of the demonstrative examples is in system Verilog, but actually CW208 does not exist in the hardware view. At least I could not find it.

And then I would, on the covert channel side, there's CW385, which seems like just as worded, it's general enough that I think could fit into the hardware view. And it's not currently today. Actually, even the parent of 385, which is, I think it's just more generally on covert channels. Yeah, it's just called covert channel 514, right? I think that's, yeah, that's what you're referencing here. Sorry. It seems like an easy, non-disruptive solution to CWE. So that's what I would propose.

Bob Heinemann: I found that the concept of incidental channels um is more of um talking about more of a uh behavior um that could lead to could lead to a vulnerability um but that's more of a I guess a fundamental I guess theoretical type discussion and it's not like a quick solution but I just like to hear other people's views on Just using the term covert channels is when we're referring to weaknesses. Do we really think that is weakness? That's out. That's that language is rooted in and weakness terminology.

Khattri, Hareesh: I think more than language semantic industry wise it has become. Something that is intuitively understood. That's a good point. And more treated as weakness. But yeah, I think if we drill down to language wise, then yeah, it's debatable.

Bob Heinemann: So we'll have to sort of cut this off here. We're at 1.31. I don't want to hold anyone any longer. So we do have this system Verilog topic. I'll send that out as a mailing list topic. And then I just want to thank everyone for the robust discussion and just let everyone know that the next meeting is July 12th. I hope everyone can make it and definitely we'll be following up on the comments we had here today on sort of the mapping diagrams. We'll sort of take the discussion on the covert channels and then hopefully maybe when we come back

next month we can we can present some proposals and see what people think. All right, with that, everyone have a good afternoon and take care. Thank you all.