Practical Cyber Security for Cyber Security Practitioners

Prof. Sandeep Kumar Shukla

Department of Computer Science and Engineering

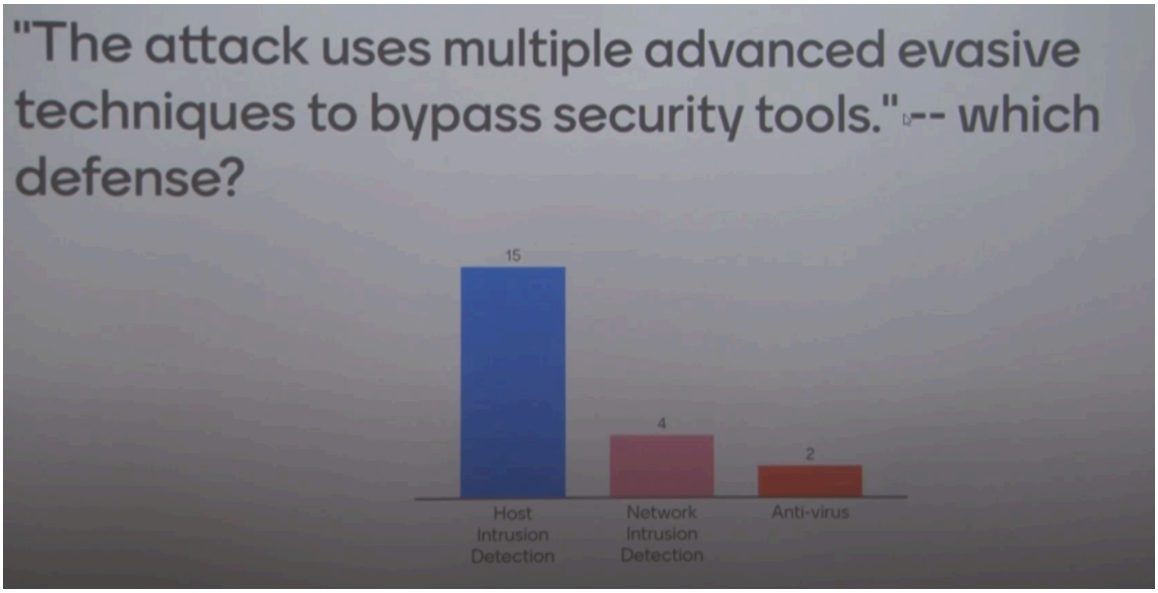
Indian Institute of Technology, Kanpur

Lecture 15

Introduction to MITRE DEF3ND Framework

So we are going to look at the MITRE defend framework. MITRE Defend framework basically connects digital artifacts or the entities, digital objects like an URL, like a binary file, like an IP address, various types of digital objects or artifacts that are found when an attack happens or when the attack is ongoing. And based on those digital artifacts, you do detection, you do forensics afterwards. So, DEFEND is another knowledge base from MITRE.

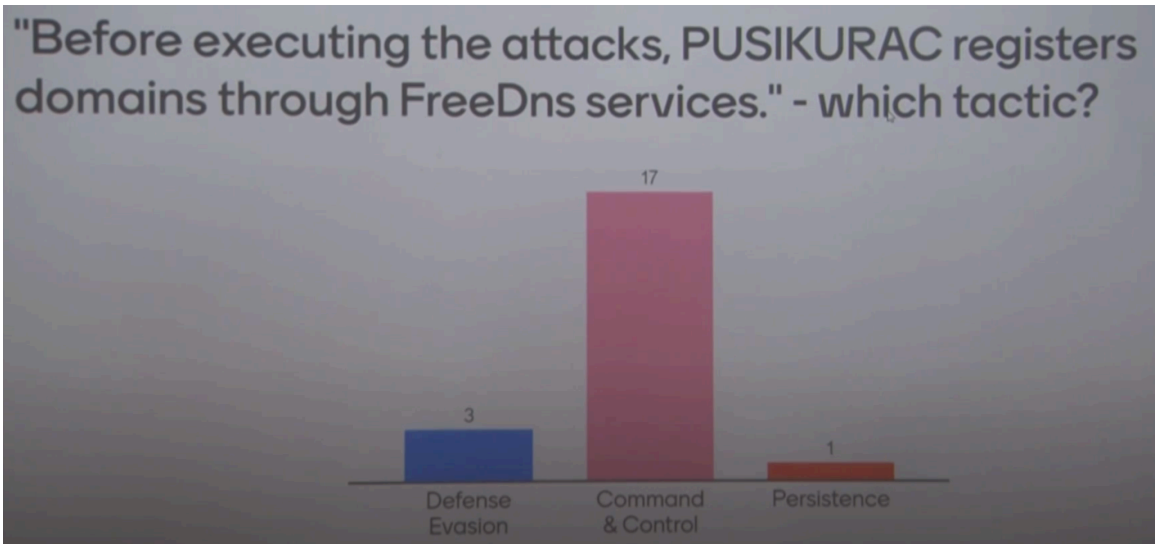
that catalogs the various tactics the defenders can use to defend the infrastructure that they are supposed to defend against the attacks. So once we have understood the attacker's side, we are actually going to the defender's side. So those are the two things that you have to think about. Now before we go into MITRE's DEFEND framework, let me as usual go into finding out where you are. By the way, you can use menti.com and use that code. So, I want to see where we are. So, here I have a sentence from a threat report.



and I am asking which tactic is best. So everybody thinks this is defense evasion. That is

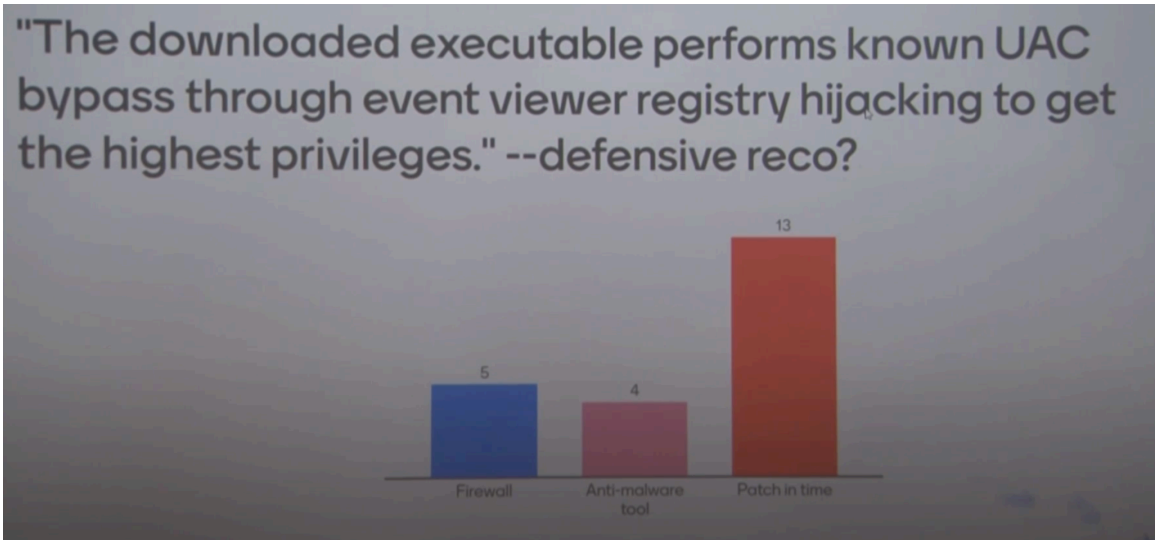
right. It's very clear from this sentence that this is about defense evasion. And certainly this is not reconnaissance or impact.

It's simple. So what defense would you use? What would be your defense recommendation for this? That the attacker is bypassing security tools. So, antivirus is what the attacker first switches off, right? So, this antivirus usually runs and you can actually configure it to be switched off. So, antivirus is probably not the right solution. network intrusion detection will not tell you what is happening inside the devices right so the defense tactics are being evaded at the endpoints right so endpoint detection is probably what you need.



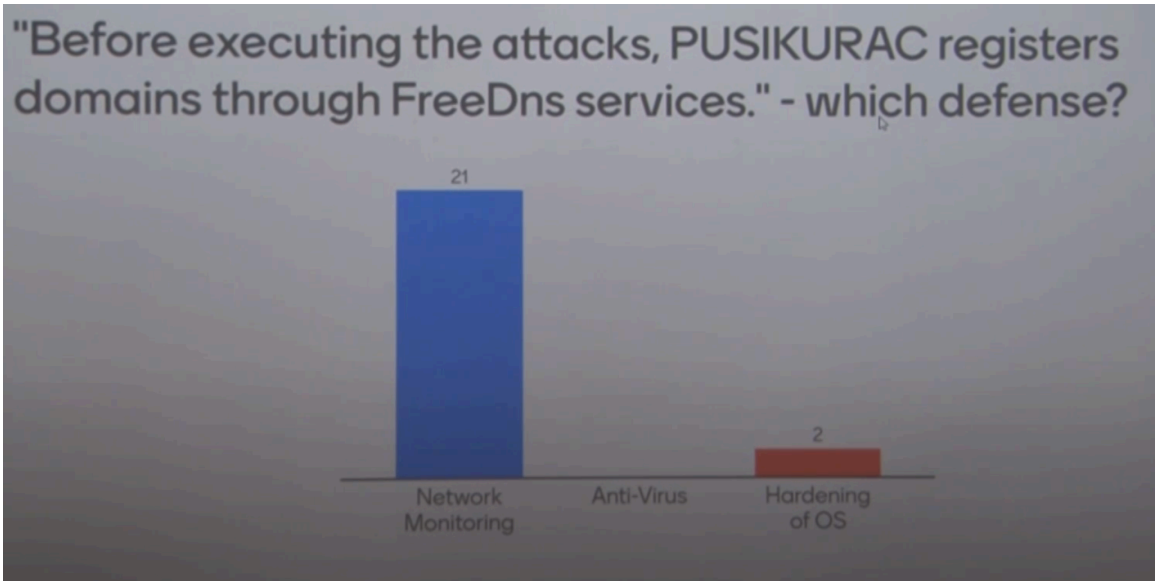
right, okay so let's see, another tactic question, before executing this attacks, it registers domains to free DNS services. Okay, so this is certainly not persistence or defense evasion, right, you are basically trying to create this command and control. If resource development was given as one of your choices, then it would have been resource development, right? But I intentionally did not give that choice so that you can say command and control. So now another one, the downloaded executable performs known UAC. What is UAC? User Access Control.

So, UAC bypass through event viewer registry hijacking to get the highest privilege. So, now you are getting the highest privilege. So, there is no question that this is about privilege escalation. But after having seen the results of the midterm first question, I wasn't sure that even this will be 100% here, but I am pleasantly surprised. So here is the downloaded executable that performs UAC.

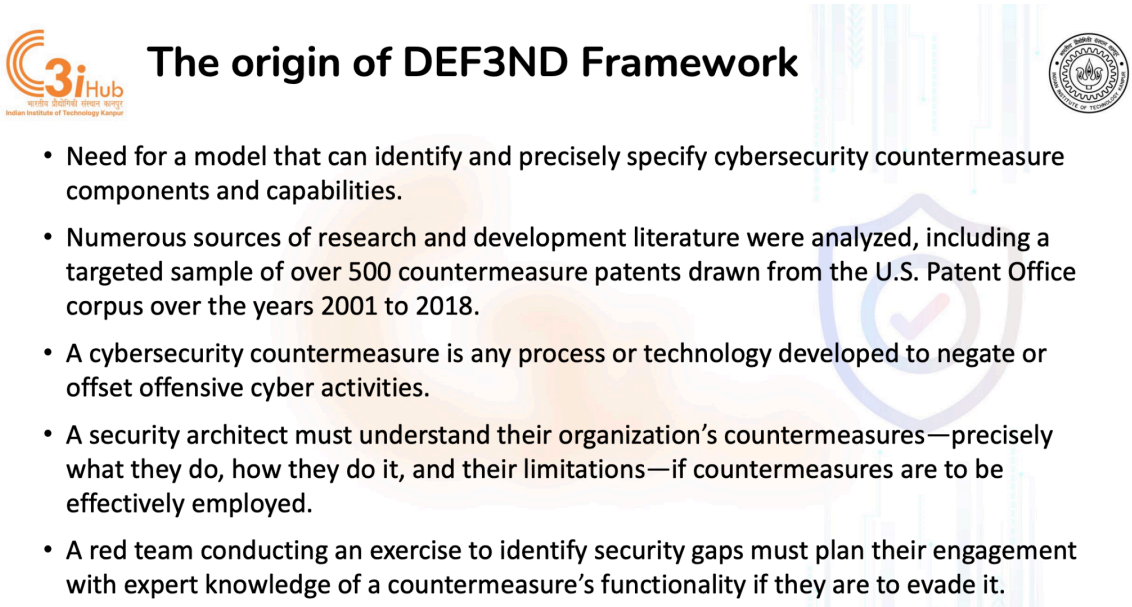


What will be your defensive recommendation? See, the sentence is saying that there was an UAC bypass which is already a known UAC bypass. What does that mean? That means there is a known vulnerability in this event viewer registry, whatever the component is. So the reason why it happened, the threat actor could exploit it, is because you did not patch it in time. So, patching is the solution, defense recommendation. Firewall and anti-malware will not help you here because you have left unpatched components.

And then about this domain thing, what would be your defense recommendation? So how will the hardening of the OS help here? It won't help, right? You have to check whether some unknown domains are being contacted by your machines so that you know that there is a command and control activity going on. So the situation is pretty scary. Now what can we do? So we cannot really.



So MITRE felt that their ATT&CK framework was very successful. Everybody was referring to it for describing how the threat actors behave in their system. They were being used to describe the modeling the behavior of the malware.



They were being used to exchange threat information between various organizations and CISOs. So they felt that they have done quite well with respect to cataloging the various tactics and techniques. And they treat this as more like a knowledge base. But then they also have other resources that they developed over time that they could relate to the MITRE ATT&CK framework. So one of the good resources that you might have not seen is MITRE Cyber Analytics Repository or CAR.

CAR Link:https://car.mitre.org/analytics/

So this is a very useful site for a knowledge base for those who are working on cyber security, especially those who are working for operational cyber security. So if you go and look at their full analytic list, So now what is analytics? This analytics is basically for detection. So you actually want to detect certain things. For example, here is, and they named these analytics methods, and this is a leaving document, which means that you can add more analytics here in the future. So here, for example, I'll show you one of them.

This is what they call autorun, right? So autorun basically detects whether somebody has created or modified a system process or scheduled a task or a job, or logged in, auto start execution, execution flow, hijacking, and all that stuff. So Autorun is actually a software that you can get from, so you can download Autorun from Sysinternals. So Microsoft Sysinternals gives you a lot of tools. So Autorun is one of those tools. So, if you actually look at autoruns, for example, it will tell you what are the different tasks and processes

that are running.

And from that, you can check whether their signature has been the binary from which this process has been created, whether their signature is matching with their original creator's signature and so on. then you can actually check whether your system has something suspicious. That doesn't mean that you will always be able to detect it because many times signatures are digital signatures. It has been the case that in many attacks, the digital signature of legitimate actors have been stolen and used like in the case of Stuxnet, but at least it gives you visibility, right? So for example, I have one process running here whose signature is not verified, right? So I should be suspicious, although I know what it is.

This is for... Similarly, here I have a service for which the file is not found. The agent file has not been found, so there is some problem here. This has been part of my startup folder or Autorun, but it is not there. Here is a Microsoft driver which seems to be not verified.

That is highly suspicious. Here is another one for which the file has not been found. So Autorun basically is a tool that gives you some idea about what tasks are running automatically in your system and what binaries they are running from and whether the binary has been digitally signed and whether the signature has matched. And then from that you can make certain inferences. It doesn't mean that you will stop all possible persistence types of tactics, but it gives you some ideas. So but the point here is that for example if you want to know there is if you want to know whether there are SMB events SMB is the SMB protocol that is for communication so I want to know whether there are some SMB events so here.

So what they are giving here is a Zeek script for detecting whether at port 445 where SMB protocol runs, something is happening, right? So this tells you, so you can use it in your system, so in your detection system, so in your network intrusion detection system. So, what I'm trying to show you is that this is an excellent resource already for getting various scripts and tools that exist right now for detection of various things, various tactics that MITRE ATT&CK framework already given. There is also another resource called CAPEC. Sorry. So this is the common attack pattern enumeration and classification.

CAPEC Link:https://capec.mitre.org

So this is also dependent on CAPEC, this thing, dependent on the MITRE framework

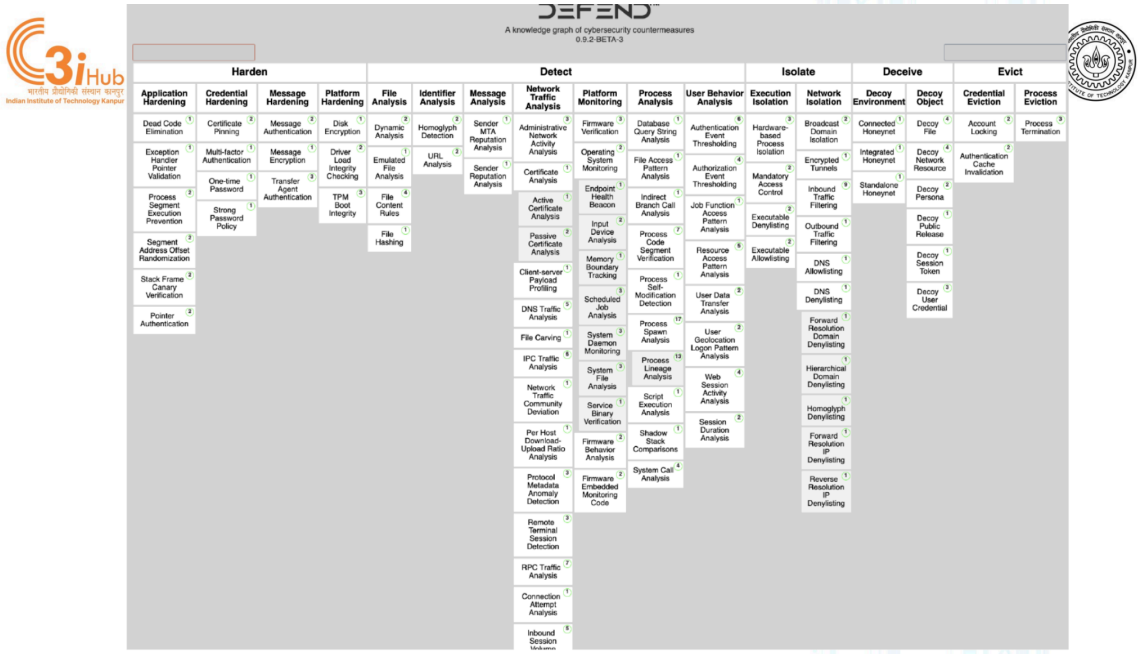
and the common weakness enumeration. So common weakness enumeration is the common weaknesses in softwares and systems and hardware also. So, what MITRE felt is that since 2008-09 when they came up with the ATT&CK framework till 2018 when they came up with the framework of DEFEND, between that time they realized that their frameworks and the resources that they're creating associated with the framework together is creating a lot of impact and they realize that we could actually do more impact if we actually catalog the various defense tactics and then connect these defense tactics with what we call digital objects or digital artifacts. which we actually capture to detect or do post-mortem, like do the forensic analysis, right? Because attacks usually leave behind certain footprints or certain signatures or certain digital objects like a malware or an URL that has been accessed or an IP address that has been accessed, or some messages that came for phishing. These are all digital, what we call digital artifacts.

These digital artifacts are used, very useful for forensic analysis. And therefore, they are really connected to the, they connect the ATT&CK and DEFEND framework, right? Because attack is basically various tactics and techniques that generates those artifacts and DEFEND often uses these artifacts to create the defense mechanism such as detection, right. So that's what the history of the DEFEND framework is. So that was the need for a model that can identify and precisely specify the countermeasures that you have to take against the various attack techniques and tactics. So they actually went through various patents, research papers, websites and so on to figure out what are the different countermeasures that people are using, what tools they are using for countermeasures and so on between 2001 and 18.

And then they decided that, okay, so any kind of technology or process that somebody uses, I should catalog them. And the reason why this is important is because like we understand now the threat actors activities in terms of 14 tactics. It is important as a CISO or as a cybersecurity architect of my organization to understand what are the different countermeasures and how to classify them as something is for system hardening, something is for detection, something is for eviction, something is for deception. So all these different tactics. And also a red team that is conducting a red team exercise should also understand the countermeasures so that they can try to evade them.

So that's the test of the security or that is what the blue team, blue team is supposed to do the security. and red team is supposed to break the security so the red team has to understand what the blue team has done with a standardized vocabulary right so so that there is no misunderstanding of what they are doing so this is what the DEFEND matrix looks like so we have all seen ATT&CK matrix so this is the DEFEND matrix so in defend matrix we see on the top there are 5 tactics, so this is much more manageable because there are only 5 instead of 14. So first is harden, second is detect, isolate, deceive

and evict. So these are 5 different tactics. And there is a, even though this is supposed to be like ATT&CK, this is a knowledge base.



Like in ATT&CK, we don't say that these are sequential, right? So we say that, okay, one can actually do reconnaissance once it is inside your system. It has done execution, persistence, maybe privilege escalation at that point it can again do reconnaissance and that was the basic idea of unified kill chain right that you can have this thing round and round again and again right so so there is no really implied sequence in the attack framework But implicitly, there is a temporal relation, right? So without an execution, you cannot think about persistence. Without persistence, you can do a lot of things, but lateral movement requires execution first, right? And things like that. So here also, like unless you detect, you cannot isolate, right? So you have to isolate a system only after you detect that there has been an attack. Similarly, if you cannot evict unless you detect, right? So there is some temporal relation between these tactics, but normally we treat this as a knowledge base.

And from a knowledge-based point of view, we say that, okay, so these are five tactics and then there are sub-tactics, right? So sub-tactics in the sense of hardening. Hardening is the process of creating better configuration. better you know ability to you know tune the system so that or tune the protective measures or tune your software so that it does not fall victim to an exploitation. So that is a hardening process right.

So here you see that there is application hardening. Credential hardening, message

hardening, platform hardening, right? So we'll go through this in detail later, but just to give you an example, application hardening, right? So what is an application hardening? So you write an application, you compile it, you run it, and then there is a buffer overflow vulnerability in it, right? Or it has a privilege escalation vulnerability. or it has a null pointer access vulnerability, right? So you have to actually test for those or you have to run what we call SAST tools or static analysis tools or dynamic analysis tools or DAST tools to find out those problems, right? And then we have to fix them, right? So fixing them will harden the program, right? but you can also harden it by doing other things so those of you who have taken a class on application security you have done you have seen that we do various things to stop the application from falling victim to buffer overflow vulnerability exploitation. Like we do, for example, address space layout randomization, right? We actually do use canaries, right? We actually do what is called DEP or the data segment execution prevention, data execution prevention, right? So there are various techniques we use to stop a program from executing a buffer overflow, right? Similarly, you can do various things to ensure that your code does not have exploitable segments. There is something called return-oriented programming that is used to avoid these protections against buffer overflow. So we actually do date code elimination to actually make sure that there is no part of the code that is not used by the program but it is unnecessarily there because somebody can then use it for return-oriented programming type of attacks.

So, application hardening has many different techniques. Now, this is not an exhaustive list of techniques. It can increase to more, like if you go to a different website, like six months later, you might find a few more in the application hardening, right? So, document. Similarly, credential hardening, right? So, multifactor authentication is a credential hardening, like hardening technique, right? So message hardening, message authentication, message encryption, and the API security would fall under message hardening here. Platform hardening, you do disk encryption, you do integrity checking, like we were seeing that verification of the binaries and their signatures and so on. So similarly, Detect has multiple different Sub tactics like file analysis, which basically is malware analysis and other types of binary analysis, identifier analysis, message analysis and so on.

So then you have network monitoring, platform monitoring. So these are intrusion detection, network intrusion detection, platform endpoint intrusion detection and so on. Then there are isolation techniques. So network isolation like network segmentations and then you have this execution isolation like putting things in separate virtual machines or putting them in the different containers or putting executions inside enclaves. So these are techniques that are related to isolation. Deceive is when you decoy, create decoys like honeypots, right? So honey credentials and so on.

And evict is once you have detected that somebody is inside your system, some malware is running in your system or somebody has access to your system through a compromised login or through user authentication bypass, you have to evict them. So you have to stop them from being able to execute inside your system. So this is the overall first look at the DEFEND metrics. So you can recognize all of these if you have done anything related to cyber protection of your own system or on somebody else's, you know, in some organizational system, you recognize all of these, you try to do many of these things, but this is a way to give them some kind of a framework in which they all are positioned. So now,

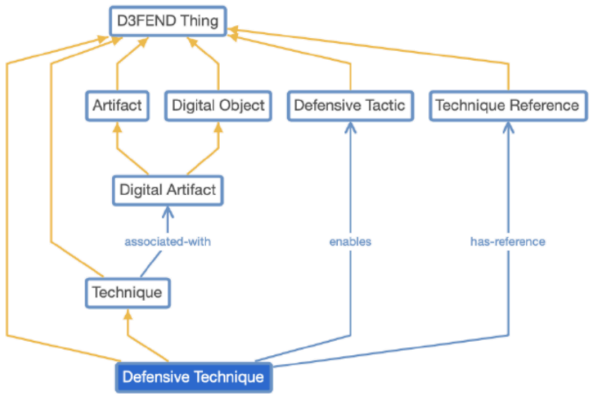


Fig. 4. D3FEND Core Knowledge Model

So now you have this diagram. Now this is something that is little problematic for you because you are not really familiar with semantic web and this entire knowledge graph. It's a whole community that is a knowledge graph community and in this community everything is, every kind of concept is put in an ontological context and there is a connection established between different concepts and there is a knowledge graph created and there is there are knowledge graphs in various domains right so there is a there is a entire open communities who are involved in creating knowledge graph and if you look at the DEFEND documentation you will see that they see this in a much grander vision, right? That entire DEFEND and ATTaCK and artifact this knowledge graph will eventually be part of a much larger knowledge graph, which eventually will be used by AI, generative AI agents and so on to actually answer questions and so on and so forth. But just to give you an idea about what they're saying, is see this yellow arrows are basically kind of like class derivation or hierarchy, class hierarchy and the blue arrows are basically the what we call attribute relations, right. So defensive techniques, right. So if you think about defensive technique obviously, a more generalized concept is technique.

Defensive technique is a special case of technique. Now technique is a special case of DEFEND thing. Now what is a DEFEND thing is a concept related to the DEFEND knowledge base or DEFEND framework. Anything in the DEFEND knowledge base or DEFEND framework is a DEFEND thing. Now if you see the technique. is associated with a digital artifact, right? Because any technique will either create a digital artifact or consume a digital artifact.

For example, if I want to detect whether there is a command and control activity, I will look for URLs and IP addresses, right? So URLs and IP addresses are digital artifacts. If I want to know if there is a phishing, then I would look for some kind of a phishing message or email and things like that, right? If I look for malware, if there has been an attack on malware, then I'll look for a malware artifact, right? So every technique is associated with a digital artifact. Artifact is a special case, is a generalization of digital artifacts.

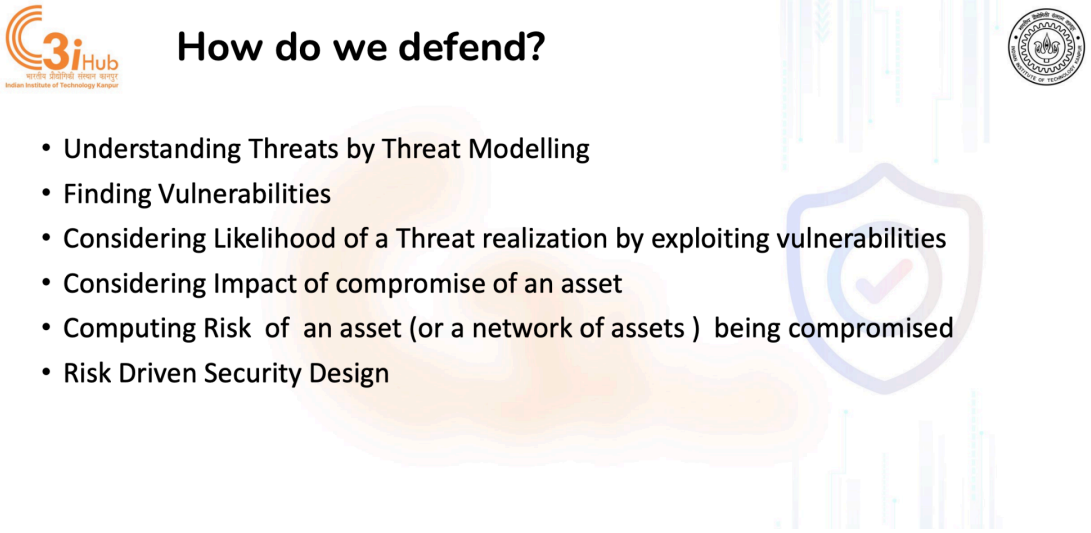
Artifacts don't have to be digital. It can be a physical artifact as well. An artifact is also a digital object, right? And a digital object or artifact, both are concepts within the DEFEND frameworks, so they are also DEFEND things, right? Now you see that digital artifact Okay, so a digital object is any object. Any file is a digital object. Any URL is a digital object. Any email address is a digital object.

Any kind of binary is a digital object. So you can think of any kind of digital object, any kind of memory segment is a digital object. So you can have various kinds of digital objects. Digital object becomes a digital artifact when either an attacker creates the digital object or touches that digital object or a defender uses, consumes the digital object or touches the digital object or reads that digital object. So this is what the defend framework is saying that any digital object may not be of interest. Only those digital objects are of interest to me if they are being created or touched by an attacker or if they are being used or read by a defender.

So that becomes a digital object, a digital artifact. Now you see that defensive technique has enabled, like we know that techniques enable tactics, right? So that's why you have techniques under tactics. So defensive technique will enable a defensive tactic and defensive technique usually has a reference. This is the documentation of the defensive technique that is the technique reference, right? So, they are also DEFEND things. They're part of the DEFEND knowledge base.

So this is what they call the core knowledge model. So the concepts here are very simple as far as you are concerned. You are not going to create knowledge base or knowledge

graphs and put that inside a semantic web database and all that stuff but for you important thing is to know what is digital artifact is and what are the defensive techniques are and what are the defensive tactics and the fact that all these things are part of the defend knowledge base idea. Now how do we defend normally right? So we understand the threats by threat model right and then we find vulnerabilities then we consider the likelihood of a particular threat by exploiting vulnerability. So if you do not have vulnerabilities, then even if you say, so what is a threat, right? So you can think, oh, somebody will steal my data, right? That's a threat that you're thinking of.

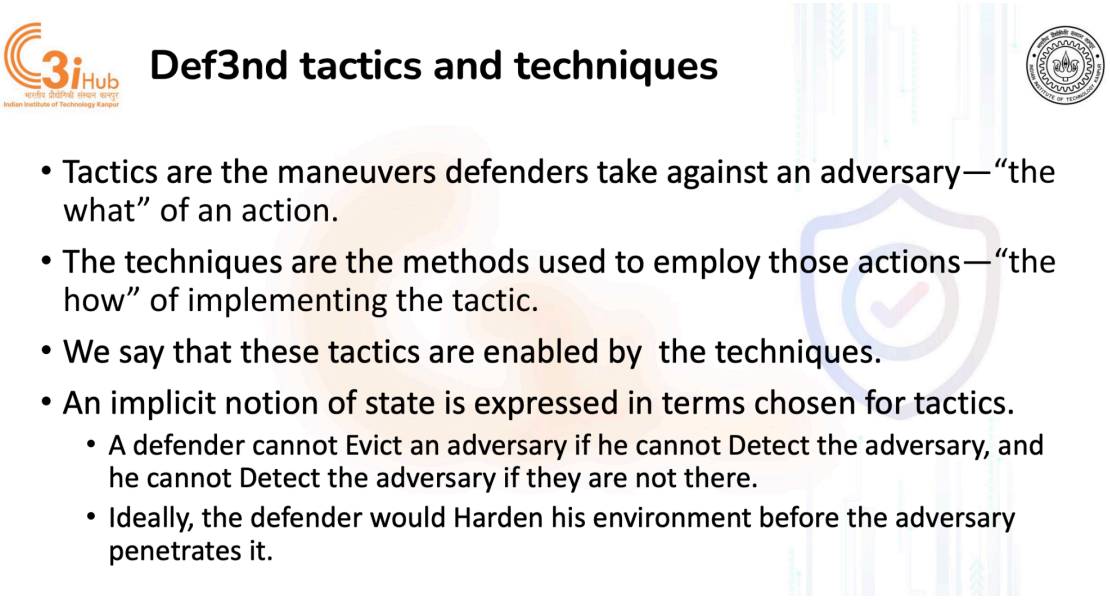


But if you do not have any vulnerability, which usually is not the case. You usually have some vulnerability somewhere, but if you do not have vulnerability, then your probability of that threat being realized is zero, right? But usually we would have some vulnerability, and if you have multiple vulnerabilities, that threat can be realized through any of these vulnerabilities. So the probabilities will add up, right? So the probability of exploiting that threat through this vulnerability versus that vulnerability, all that stuff will add up, right? So you consider the probability or likelihood of a threat being realized and then you also consider the impact of that threat on the asset, right? On a particular asset, right? So in this case, let's say your data, your research data, you're worried, you're doing PhD or master's and you are writing your thesis and somebody steals your data, yes? Yeah, so threat modeling is the process of imagining what can happen. For example, Let's say I have video cameras around the campus. Now, I will not look for whether my cameras are accessible by outsiders unless I have a threat in mind. So I will model the threat that some external person may want to track a particular student right, for stalking purposes.

So that's a threat model, right? Now, or you may want to say that some threat actor will turn off the video at a busy intersection on campus to create some physical attack, right? So that is a threat model. Once I have the threat model, then I will start thinking, is this

threat model actionable? Can somebody actually do it? Then I have to look for vulnerabilities, right? So then I will have to figure out whether the cameras or the network has vulnerability which can be exploited from outside and if it can be then what is the likelihood that is what is the likelihood that somebody will be able to vpn into the network our network and do this so all these calculations will tell me the likelihood of that having happening then i would have to consider what is the risk associated with that happening Now the risk associated with that happening could be considered high or low or medium depending on the other external exogenous information. For example, suppose there is a terrorist attack going on around the country. At that time the impact will be much higher than the impact assessment will be much higher.

Or it is on a particularly busy day like during Techkriti. Then we'll say the impact will be much higher. So in that way, I will consider the risk. So risk is basically threat times vulnerability times likelihood. So based on the risk, I will say, okay, these high risk things have to be defended first. If I have a budget for cybersecurity, then I will have to first do a risk assessment and then find out what is the highest risk asset.



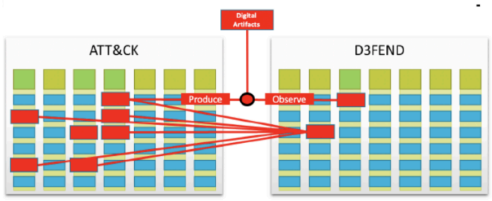
And then I have to put my resources first there. So that's the idea. So tactics are basically maneuvers defenders take against the adversary, the what of the action. What are they supposed to do? Are they going to be detected? Are they going to be evicted? Are they going to deceive? These are the what's. And the techniques are the methods employed to achieve that, right? So that techniques are basically what makes tactics actually work. So tactics are enabled by techniques. So this is a standard idea and as I said that there is an implicit notion of temporal state that for example you cannot evict unless you detect, right.

So even though we say that these are independent tactics but usually some tactics cannot

be done without a previous tactic being applied, right. So you cannot evict without detecting for example. or defender has to harden first before the adversary penetrates it, right? So hardening is done as a part of the design of the system, right? So there is a implicit temporal relationship. Okay, so now as I said that the ATT&CK and DEFEND are connected through the digital artifacts. So, digital artifacts are important and digital artifact ontology is a knowledge base that was created by MITRE and it is still being developed.

Digital Objects and Artifacts

- A key construct in D3FEND is the Digital Artifact Ontology (DAO).
- This ontology specifies the concepts necessary to classify and represent the digital objects of interest for cybersecurity analysis.
- In the D3FEND knowledge model, a digital object becomes a digital artifact when a cyber actor, either defensive or offensive, interacts with the object in any way.
- The Def3nd knowledge model is only concerned with capturing knowledge about digital artifacts relevant to known cyber actors and known technologies—not all possible digital objects or their representations.



7. Offensive and Defensive Techniques Mapping Via Digital Artifacts

So, it is again another living knowledge base. So as I look at the third one that I said that a digital object becomes a digital artifact when a cyber actor, either defensive or offensive, interacts with the object in any way. So a digital object becomes a digital artifact when it is being attached or used or created by an actor, either a threat actor or the defensive actor. So the knowledge model here is concerned with capturing knowledge about digital artifacts relevant to known cyber actors and known technologies, not all possible digital actors. So you have to catalog all the possible digital artifacts and then you have to consider them. For example, If you think about process injection, right? So you inject code inside a running process, right? So what would be the digital artifact? The digital artifact would be the content of the memory allocated to that process, right? So unless you actually have this concept that such a thing can happen, you will not think of that digital artifact at all.

So that's the reason why this cataloging and knowledge base creation is that things that I cannot imagine, somebody else has imagined, may be actually relevant to my organization. And then I have to refer back to this knowledge base.