Advantages And Disadvantages Involved In Honeytokens Information Technology Essay

Published: 23rd March, 2015 **Last Edited:** 23rd March, 2015

As Honeytokens is a part of Honeypot technology and is considered as its cousin, it gets all the positives and negatives from them. But that does not mean they do not have any attributes of its own. In this part we are going to see why is worth to give using Honeytokens and Honeypots a thumbs up Its mentioned before that Honeytokens are part of Honeypot technology such that it inherits all attributes of that technology.

First and foremost advantage of a Honeytoken is its concept, which is quite simple. Its like keeping a cheese to capture a mouse in mousetrap. The mouse here is none other than hacker/insider. In this context we are not using a mouse trap, instead we allow mouse to have a sumptuous meal and we take a good look of its activities. By allowing mouse to have its meal we can track down where does it have its burrow and when does it come and how does it go unnoticed each time. In the end it can be nabbed and leave it in some far place(if resident is so kind-hearted) or can just kill it. Same applies in professional environment, if an insider or an attacker, we can either block them from doing it or by giving dishonourable discharge, in case of insiders, and get him/her arrested and pursue legally by collecting evidence.

Next advantage of a Honeytoken is its simplicity. As defined by Lance Spitzner[1], a Honeytoken is not necessarily mean to be a computer. It is just a fake digital entity. That means a Honeytoken can be anything from a mere credit card number to a record in database, a small text file to multi page PDF file. This gives Honeytokens an edge over other measure which needs a lot of infrastructure in place to get implemented.

Another advantage of a Honeytoken is its cost efficiency. As it is mentioned before that a Honeytoken is just a fake digital entity this naturally means is low in cost as there is not much machines to deploy for this purpose. Even a computer with Celeron processor with 128-256 MB RAM is enough to deploy Honeytokens. And this also means there is no need to buy any security ware license like anti-virus key, no need of an external security personnel to check or monitor this and thus keep wallet a bit heavy.

Flexibility is another trait of Honeytokens that adds a feather in its cap. The usage and implementation of is all limited to our creativity as said by Lance Spitzner[1]. We can use Honeytokens to just detect breach in our system or to track down origin of attack or to find out the insiders in the organisation and can even be used to single out attackers in certain situations.

Next advantage of Honeytokens are it maintains only a small data set[1], in fact only a zero data set. It is because it does not keep log of each and every activity of system which naturally involves storing a lot of data that may even lead to thousands of Tera Bytes(TB), Honeytokens would just trip an alarm that too only if an attacker interacts with that. This also means there would not also be any kind of data overload because of Honeytokens.

It should also be kept in mind that Honeytokens are quite difficult to be evaded by an attacker because of its perfect cover, as it is present among millions of legitimate data and its ability to lure attackers by posing like real data, which it is not.

Another advantage of Honeytokens is risk of loss is minimal. Suppose if we are using an e-mail id to detect whether our mailing list is compromised there are chances that the e-mail id being used as a Honeytoken may get hacked and hijacked, but the loss of that e-mail id does not really going to pinch, in fact it may lead us to ponder about yet another security loop hole within our system.

Honeytokens are also very adaptable as it can used flexibly. It can be used alongside other intrusion detection system to monitor any abnormal and unusual activity happening. Thus makes it easily adapted to work cohesively with other security technologies. Apart from this it is also capable of answering some of flaws of intrusion detection systems[1] by pointing out all kind of breach whenever it gets accessed.

Some of other advantages of Honeytokens are, it can even detect a breach if an attack is encrypted

because it does not analyse what kind of attack being performed on them, all it does is just check has it been accessed and used or not. And it also not limited by difference in protocol, it can detect an attack from any version of Internet Protocol(IP), it does not matter if the attack is carried out through IPv4 or Ipv6 or one tunnelled within another to conceal traffic. Honeytokens does not mind about any of these hindrance.

Honeytokens also has solid record in avoiding false positive and false negative rates. False positive occurs when a security system raises an alarm tha there has been a breach in system but turns out to be a normal interaction. False negative is vice versa of false positive, it occurs when a security system allows an unauthorized access or an action in its perimeter and consider it to be a normal action such that fails to raise an alarm. Honeytokens deals with this pretty easily. Any kind of interaction with a Honeytoken is of course a breach, and it does not matter even if it is done by head of the organisation, which makes it easy to find the attack such that the organisation can act accordingly, this addresses false positive problem. Honeytokens does not keep quiet and fail raise an alarm because it does not have any productive value and it would be only kept isolated so that no one gets access to it. Therefore if a Honeytoken is accessed, it just can not sit silent and consider it as a normal action instead gives an alert to administrator that security has been compromised, this addresses false negative problem effectively.

Most of the advantages mentioned above for Honeytokens are also advantage of Honeypots[2]. It can also be verified with source mentioned. Another thing to notice in these advantages mentioned sums up to one attribute of Honeytokens, like rivers ending up in ocean. That attribute is none other than simplicity. All the advantages of Honeytokens are present just because it is simple and got no complexity involved in it. Thus these are the reason why we can give Honeytokens a thumbs up to use in our security system.

5.2 What are the drawbacks?

This section discuss about why should we give Honeytokens and Honeypots a thumbs down. It is mentioned is previous section that all the advantages sums up to one attribute. Unfortunately that attribute is also one and main disadvantage of Honeytokens. But the case of Honeypots is entirely which would come to light later in this section. We would have detailed analysis in each and every disadvantage of Honeytokens and Honeypots.

The first disadvantage is its biggest advantage, its simplicity. As it is simple by it form it means that it cannot be deployed. Honeytokens can be considered as David and attackers and insiders like Goliath(in this context Goliath is so powerful than past one). Its obvious that David cannot slay Goliath with bare hands, so he used sling to kill him. Here Honeytokens need much more fire power than just a sling. It needs to have its arsenal equipped with some powerful tools. Those powerful tools are none other than Intrusion Detection Systems(IDS), which can either be network based or host or both of them altogether. In fact Honeytokens here is a small tool when compared to other systems. So it is not advisable to forsake other existing technology for sake of Honeytokens.

Another disadvantage is it cannot identify an unauthorized activity[1] according to Lance Spitzner. He asserts that Honeytoken can only detect an unusual behaviour which means it cannot pin point source of attack and identity of an attacker. Thus it is evident from this point that Honeytokens cannot be used on its own.

Next drawback is Honeytokens can only identify breach when it happens to it but cannot detect when some other part of system is being compromised. It means Honeytokens set off an alarm only when an attacker access that particular Honeytoken, only then attack can be sensed. But attacker does not access this Honeytoken but gets hold and access other legitimate files around it, it cannot detect attack carried out on those legitimate files. This is considered as a serious drawback of Honeytokens.

Another drawback is pointed out by a report written by Nicholas Thompson in The New York Times, which says at times Honeytokens can also be bypassed when attackers change the property of Honeytoken they steal by compressing or by assigning a password[3] which may conceal key data's like fake credit card number or fake account number, that intrusion detection systems like sniffers are looking for.

There are couple of flimsy disadvantages of Honeytokens as well. First among them is its relatively a new method in practice, although it is used widely there has not been a giant breakthrough regarding Honeytokens. Another disadvantage is perception of section people on Honeytokens. Certain section of people, people with either no-knowledge or minimal knowledge about security, consider Honeytokens to prevent an attack from happening and also expect Honeytokens to yield results, which is contrary to its characteristic.

Another reason that Honeytokens may lose ground in a legal battle is since it is a fake record and data it collects is so minimal it cannot be submitted as an evidence to charge the attacker. So Honeytokens alone cannot possibly be submitted as an evidence. It would only be fruitful if Honeytoken evidence is submitted along with data's collected from other Intrusion Detection Systems(IDS).

Apart from these Honeytokens also has some legal issues, it is not actually restricted to Honeytokens alone but Honeypots is general, in fact onus of every issue lies on Honeypots[4]. The reason for this legal confusion is because this is a fledgling technology which only technically enlightened can understand such that laws are really difficult to create, and there is also no past reference if a case involves Honeypots or Honeytokens.

Now coming to point, first legal issue to be considered is entrapment. This is a problem because if plaintiff brings this issue as a case it means that the attacker did not come and performed unauthorized actions voluntarily instead plaintiff itself forced him/her to carry out that action. This is commonly misunderstood issue. According to Lance Spitzner Honeypots/Honeytokens has and can never be considered as a tool to trap an attacker One thing we got to understand here is we are just going to keep the Honeytokens into our database and do not give an open invitation and set a booby trap for outsiders to come and gain an unauthorized access. If entrapment is placed forward to prosecute an attacker then he/she can use thi same issue as a defence to escape conviction.

One common misunderstanding regarding Honeytokens in this issue must be made clear to everyone. Neither Honeytokens nor Honeypots does carry a tag around saying â€œHack me if you canâ€. It is just another data or network owned by an organisation that does not have any value. So if attackers intrude into this Honeypot or access the Honeytoken it is all done by their conscience but not by forcing them. In fact purpose c Honeypots or Honeytokens is to induce an attacker and inducement can never ever be a trap, because either with Honeypot/Honeytoken in network or not attacker would carried out an attack anyway. That Honeypot/Honeytoken just act as an illusion, but entrapping means string events that leads an attacker to carry out an attack, which he/she would not have, if trap has not been set. According to Anne Flanagan[5] it is important to set the purpose of Honeypots and Honeytokens be only to detect anomalies and protect the organisation from attacks and not to force intruder to attack th network and also said a Honeypot in purposeful operation cannot be considered as an entrapment as cited in laws of countries like United States of America, Canada, United Kingdom and Australia.

Second issue to address is liability. There are chances when Honeytokens we deployed may turn against us. At times attackers may use Honeytokens we created for an illegal purpose in their daily life. For example if an attacker gets hold of a fake credit card number and if security administrators fai to recognise that, attacker may use it buy products using that Honeytoken. Situation may get much worse if organisations own Honeypots/Honeytokens used for Denial of Service(DoS) attacks. This holds organisation liable for being negligent on their part. Although the problem is not really with Honeytoken still can be held as potential factor for liability.

According to both Lance Spitzner and Ralph Poore This problem can be overcome by condensing outbound traffic from Honeypot network or not allowing Honeytoken to leave the network[6][7]. They also say that it can be attractive enough to lure an attacker, because attracting an attacker doe not count for trapping. But if an attacker start misusing it by storing illegal informations and use system in Honeypot network to intrude break into other networks then network administrator must take necessary steps to stop that attack being carried out. The network administrators must also make sure from their legal team whether using Honeytokens are allowed as some countries does not allow illegal information to be stored in database, otherwise non-compliance may lead to liability.

Another valuable solution for this problem was mentioned by ISG alumni Carla. D. Holder in her dissertation stating that Honeypots must be audited quite regularly[8] because it must be presented as an evidence if an attacker is to be prosecuted. Apart from auditing an organisation must also prov that Honeypots were immaculate before being attacked by an attacker(if the attack is not for first time then network administrator must clean up an patched the Honeypot after its first attack such that it cannot be compromised another time and can withstand next attack) such that when submitted as an evidence it could hold its integrity before court of law, along with log recorded before and after the attack on Honeypot.

Third issue is privacy. If an attacker accesses Honeytokens it may immediately set off an alarm such that security personnel may track down source c attack and with much more sophisticated approach even attackers login credential can be recovered. It is feared that collected login information can be disclosed by organisation that holds that data. But at times purpose of this Honeytoken may come into scene. If it is solely used for protection purpose it is given an exemption according to Service Provider Protection[4] in United States of America. But this exemption is not available if it is used for research purposes. Production Honeypots comes under exemption but not for Research Honeypots. For an organisation to avail this protection it must prove that it has deployed its Honeypots and Honeytokens within bounds of production server[9]. But there is a loophole in this exemption as well that it is not legal to intercept encrypted communication says Jerome Radcliffe[10]. Even if organisation place its Honeypots or Honeytokens in a Demilitarized Zone(DMZ), which is organisation's network for external services like internet, it can stressed that it is deployed in DMZ only to protect both production server and DMZ server by monitoring anomalies[9].

Sometimes its considered that just because an organisation owns a network, which is Honeypot in this context does not give them power to monitor each and every activity of an attacker. There are several yardsticks, especially in country like United States of America regarding this issue asserts Richard Salgado[9] that too if the deployed Honeypot belongs to government or an organisation run by government and there are also limitation for Honeypots owned by private organisations unless they prove intent of attacker is malicious. One way they can avoid this problem is by putting up a notice on their networks saying that it is a private network space and only authorized users are allowed and would be under surveillance constantly. This enables shield against offenders defence claim, but even this does not give full power to scrutinise personal informations but to defend from an future implications. Another way out to this problem is intercepting communication with consent[10] of communicating parties which would save lawsuit for the organisation if they put up notice in a visible manner and even if attackers bypass their way to network avoiding this notice they can b held against law for flouting organisation's policy.

It is also considered by certain parties that using Honeytokens or Honeypots are unethical just because it is posing as legitimate entity which it really is not. Michel Kabay says that[11] if someone enters his network in an unauthorized manner it does not matter whether network is legitimate or its contents they must be punished whatsoever provided the network clearly marked as private one and meant for authorized users. It is equivalent to trespassing which illegal regardless of worth of property. By this Michel Kabay tells the world that using Honeypots or Honeytokens are ethical.

Sometimes it is also difficult to charge an attacker especially if he/she is out of jurisdiction of the place where organisation is because it is difficult to resolve which states law to apply for the issue. So cross-border issue stands as another legal hurdle for Honeytokens. Thus these are the reasons wh we can give Honeytokens a thumbs down to use.

Although some of the above mentioned issues does not really involve Honeytokens or Honeypots directly still it is believed to play a potential and pivotal role in each issues. It is only in hands of legal experts from various countries around the world to resolve this conflict

And from these analysis it is quite evident that Honeytokens as a technology has a lot of advantages but only few drawbacks. Most of its drawbacks are related only to legal tangle it is caught in. Now it is up to organisations to use it wisely to go unscathed from these tangles.

[1] Honeytokens: The Other Honeypot- Lance Spitzner, http://www.symantec.com/connect/articles/honeytokens-other-honeypot

[2] Honeypots: Simple, Cost-Effective Detection- Lance Spitzner,

http://www.symantec.com/connect/articles/honeypots-simple-cost-effective-detection

[3] New Economy; The ''honeytoken,'' an innocuous tag in a file, can signal an intrusion in a company's database- Nicholas Thompson,

http://www.nytimes.com/2003/04/28/business/new-economy-honeytoken-innocuous-tag-file-can-signal-intrusion-company-s.html?pagewanted=2

[4] Honeypots: Are They Illegal?- Lance Spitzner, http://www.symantec.com/connect/articles/honeypots-are-they-illegal

[5] Honeypots: a sticky legal landscape?- Anne Flanagan,

http://www.allbusiness.com/legal/laws-government-regulations/618213-1.html

[6] Honeypots: Tracking Hackers- Lance Spitzner, Addison-Wesley Professional, September 2002

[7] Attractive Hazard: Entrapment or Forensic Tool?-Ralph Poore,

Information Security Journal: A Global Perspective, Volume 11 Issue 6, January 2003

[8] Honeypots: Legal and Technical Issues- Carla D. Holder, Dissertation: ISG-RHUL, 2006

[9] Know Your Enemy, 2nd Edition, Chapter 8:Legal Issues- Richard Salgado, Addison-Wesley

[10] CyberLaw 101: A primer on US laws related to honeypot deployments- Jerome Radcliffe,

SANS Institute InfoSec Reading Room, February 1, 2007

[11] Honeypots, Part 4: Liability and ethics of honeypots- Michel Kabay, http://www.networkworld.com/newsletters/sec/2003/0519sec2.html