2005

Honeypot Technologies and Their Applicability as an Internal Countermeasure

Craig Valli
Edith Cowan University

Honeypot technologies and their applicability as an internal countermeasure

Craig Valli
School of Computer and Information Science, Edith Cowan University
c.valli@ecu.edu.au

Abstract
Honeypots or honeynets are a technology that is rapidly maturing and establishing this archetype of countermeasure as viable and useful in modern network defence. Honeypot technology is now at a point of development where near real-time monitoring and forensic analysis of security events can occur. This paper explores the hurdles to be overcome for the internal deployment of honeypot technologies.

Keywords honeypot, internal, misuse, IDS, firewall

INTRODUCTION
Honeypots or honeynets are a technology that is rapidly maturing and establishing this countermeasure as viable and useful in modern network defence. However, most honeypot technology is designed to be outwards facing and consequently, it is not useful in reducing
the impact of internal cyber attacks in organisations.

Various recent security surveys (AusCERT, Australian High Tech Crime Centre et al., 2005; AusCERT, Australian High Tech Crime Centre et al., 2004; CSO Magazine et al., 2004; L. A. Gordon et al., 2004; L. A. Gordon et al., 2005; Richardson, 2003; Schneier, 2005) cite the most expensive and frequent forms of successful attack originating from within an organisation. These surveys quote that 60-90% of attacks are internally oriented. It seems incongruous that honeypot technology is not being deployed as an internal countermeasure to combat insider misuse of information systems.

It is now well established in the literature that honeypot class systems are effective in trapping and monitoring malicious activity (Honeynet Project, 2004; Spencer, 2004; Spitzner, 2002, 2003). Honeypot technology is now at a point of development where near real-time monitoring and forensic analysis of security events can occur. Typically, these systems are nearly all externally focused.

Honeypot systems tend to use deception as a key weapon. The deception is based largely on a premise of masking the real that is, an attacker is intentionally misled about a networks structure or weak points. An external entity wishing to gain access to a networked system has to perform certain perceptible and tangible probes on a network to gather intelligence on the network composition and structure. This probing may employ brute force or stealth either way much of this probing should be detected by even the most basic of intrusion detection systems.

Further to this initial probing the attacker must then craft attacks to penetrate the network which is already based *a posteriori* on the attack intelligence gathered. Hence, with some initial changes in perception by displaying the false advantage can be gained over the attacker. A simple example is the manipulation of the TCP/IP stack Operating System (OS) fingerprint of the probed host to indicate a different OS than is operating on the system. This is a deception with relative low complexity and low deployment cost and can be readily perpetrated against the external attacker. This deception can have a magnifying effect due to the *a posteriori* state that the prober believes to be true.

By comparison, the users within the organisation are almost gifted with omnipotence when compared to an external entity for gaining knowledge of network construction. Much of the knowledge that an internal user can gather through social interaction and engineering will be *a priori* giving them significant advantage when attacking systems. As an example, they would know that the main routers and switches of a network are a particular model and type because they will have sighted this in their physical locale (typically most devices display their brand and model visibly on the front panel). This type of internal intelligence gathering presents significant challenges for the composition of internally focussed honeypot systems to effectively deceive and ensnare internal miscreants.

HONEYPOTS, HONEYNETS, HONEYFILES...

Evidence presented in various publications and conferences would support the proposition that honeypots and derivative technologies are becoming a viable digital countermeasure(Gupta, 2002; Valli, 2003; Yek & Valli, 2003) . Honeypots have been found to be effective in retarding or negating the spread of malicious code such as network borne worms and spam (Oudot, 2003; Spencer, 2004).

For the purposes of this paper the semantics behind terms such as honeypots, honeynets and honeyfiles will be largely ignored. The paper is concerned more with operational and strategic issues of deployment and will refer to the term honeypot technologies (HPT) to encompass all of these technologies.

The principle underlying tenet of each honeypot deployment is the gaining of advantage by techniques of deception that allows for the successful misleading or decoying of the attacking entity be it a human or digital instance. This deception is achieved by the HPT being compromised or being seen as vulnerable so that valuable forensic information can be collected as a result of attempted exploit or penetration of that system by attackers. The information gathered from HPT can have a variety of uses and purposes with the paramount being that of providing advantage. The advantage can be either short term through mitigation of attacks or long term solving or overcoming an exploit as a result of analysing data collected.

Most current HPT have been constructed with the premise that attack will occur from outside a network from entities attempting to compromise or penetrate a system. Furthermore, most literature that is in existence about honeypots their morphology and *modus operandi* is likewise focussed at repelling the digital outsider. It would appear that internal honeypot construction, deployment and development is largely ignored, why?

This phenomena of external fixation is in direct contradiction to the evidence that is published from numerous computer and network security reports touted by industry and academics alike to advance security as an issue (AusCERT, Centre et al., 2004, 2005; Gordon et al., 2004; Gordon et al., 2005). These reports attempt to give vignettes of the status quo of the computer security threat landscape, and they consistently find or conclude that internal threats realise the most damage by monetary impact and number of incidents. Firewalls and Intrusion Detection Systems (IDS) are deployed to control and monitor internal assets in organisations yet HPT does not yet appear to be on the inside even though there is sufficient evidence to indicate their utility in detecting malicious behaviour.

Barriers to deployment?

HPT is rapidly maturing and is starting to see deployment in major organisations that are required to protect highly confidential or readily fungible commodities such as money. Businesses and governments are increasing surveillance of the workplace both physically and digitally.

It is interesting to posit if the barriers to the deployment technological or organisational? From a technology perspective it could be said it is true that most honeypot deployments are still highly experimental even the commercially supported solutions. HPT in some respects are probably more stable than the Intrusion Prevention System (IPS) suites offered by commercial vendors that some sites are using. The acceptance of IPS could be as a result of being sold as the replacement silver-bullet for IDS inability to detect newer forms of attack (Conry-Murray, 2005). IPS, IDS and firewall technology all have the comfortable and safe *modus operandi* of repelling the external hackers at the perimeter network interface.

By contrast, honeypots are almost the anti-thesis of IDS, IPS and firewall technologies taking the approach by using the principle extolled by Sun Tzu of keeping ones foes under closer observation than ones friends by bringing them inside the defensive perimeter and monitoring their every machination. This mode of operation is a significant change in mindset from the perimeter mentality on which most current network security is predicated. In the same way, that modern warfare has developed into network effects and operations likewise network security needs a similar paradigm shift from regimented compartments to network centric tactics.

One of the most often touted responses to the deployment of honeypots is the legal concept of ‘entrapment’ (Schultz, 2002). This area is highly contentious and, of course, varies greatly depending upon which

jurisdiction the concept of entrapment is viewed. It is not the purpose of the paper to debate these issues other than to highlight they exist for conventional externally faced honeypot deployments. Internally faced honeypot systems do present various ethical and moral problems to an organisation but no more than possible existing schemes of network based monitoring. For example, most organisations now record a users e-mail and World Wide Web usage often without the knowledge of the user. The entrapment argument could be applied to these existing scenarios of workplace surveillance. However, it is fair to say that properly constructed honeypot systems placed into an enterprise network that is controlled tightly by appropriate policy and procedure should not present problems in this regard. A honeypot in this situation should only encounter users who are in direct breach of company policy and whose actions are deliberate, malicious and intentional. This would include policy that restricts users to accessing services for which they are allocated and have legitimate use of. Furthermore, the honeypot system itself would contain warnings via banners or pop-up messages that accesses of these systems are for authorised personnel only and that action beyond this point is in breach of company policy. If the user then chooses to probe or attempts to compromise a system, they have made a conscious decision to do so and this could not be called entrapment.

Unlike external honeypots internally deployed honeypots would trap existing behaviours and threat patterns within the confines of the organisational network. Internal honeypots are possibly not having to respond to the new malicious code types or new exploits that an externally faced honeypot would due to their network depth in the organisation. Hence, the level of staff expertise needed to effectively manage one of those could be lower as they can utilise existing defaults within the systems that mitigate against known threats. Honeyfiles are a method that are not related to any particular exploit and are focussed squarely at determining if a file has been accessed.

Where IDSs fail internally is that they are looking for a particular binary sequence or compromise of a rule set for a single instance of behaviour, which they then respond to typically with a single action such as dropping the connection, which either succeeds or fails. IDS typically have poor mechanisms for allowing the forensic reconstruction of an incident beyond action taken by the IDS as their primary function is one of system protection and not that of data collection. HPT however, are designed to track and monitor all behaviours without prejudice even if there is interaction for example with an IDS in a honeypot system. HPT should be designed in such a way as to record an attackers actions and effects on a system at the not only the network layer but also the systems and applications layers. This approach enables security specialists to recreate the sequence of events or actions that resulted in an incident as all data should be present sufficient to all forensic reconstruction of an incident. This should then enable internal security personnel to adopt a learning paradigm in remediation of security incidents through the analysis of this data.

Internal users could also compromise valuable internal systems not seen or accessible by the Internet with conventional countermeasures in place, unable to detect this misuse as they are typically externally focused at the Internet egress point. Many organisations utilise firewall and Virtual LAN (VLAN) systems to control traffic flow to these high value networks and some even deploy IDS (Wilson, 2005) . IDS and Firewalls technologies can suffer from a lack of forensic completeness due to their *modus operandi*. At an organisational level, there are often trust elements at play that may make the deployment and even management of these contemporary countermeasures vexatious (Anonymous, 2003; Camardella, 2003; Fidler, 2004). This problem is possibly exacerbated by the perception of attacks being external (Briere, 2005; Robb, 2005).

The deployment of an internal honeypot to these high-value network segments could significantly reduce risk profiles within an organisation. This is because HPT could detect behaviours before they become issues and work as an early warning system to security administrators. For example, HPT could also effectively record unknown or unspecified errors in the security of existing systems for example, incorrect rights management settings for a particular server or service that allows an internal user probative abilities.

INTERNAL HONEYPOT DESIGN CONSIDERATIONS

The design philosophy for internal honeypots as compared to conventionally deployed external honeypots is affected on several levels. Firstly, external honeypots use the concept of exhausting an attacker's resources which given the finite constraints of a broadband Internet connection is an achievable maxim, although getting more remote as bandwidth increases. Honeypots that are deployed internally do not have this same ability as an internal abuser will typically be using a high-speed Ethernet connection with high levels of access to the honeypot. Network latency is normally measured in fractions of a microsecond and often on

the same network segment or in close proximity. Therefore, issues of network latency, system availability and reachability for the gathering of attack intelligence, or perpetration of attack, do not present a significant resource barrier for an internal abuser.

As mentioned earlier, an internal user will have a higher level of initial attack intelligence from which to attempt system surveillance or even penetration and compromise. For example, they can use legitimate network browsing tools such as Microsoft Network Neighbourhood to examine server naming conventions to significantly reduce the amount of guesswork or probing that an external attacker would have to undertake to garner the same results. This also allows an internal attacker to significantly narrow the detection window for existing countermeasures such as IDS, Firewalls and IPS as a result of this reduced activity. The reduced activity from an insider would possibly not trigger response from any countermeasure. In some cases the countermeasures will be configured to trust these internal entities allowing for a more extensive and secretive probing of the network. This is reduced further because of the lessened need for actual probing of the network to discover things such as operating system, patch levels, server application and other information that an external attacker would gather before attempting system compromise.

One of the other issues with deployment of internal honeypots is that of organisational leakage of the honeypot 'secret'. Most honeypot systems rely upon deception via masking that is the hacker is unaware that they are in a honeypot. If a malicious insider now knows a honeypot exists within the network then they may cease activity or adjust behaviour to suit, and be ultimately untrusting of any new additions to the network.

Topology will be an issue dependent upon the topology of the internal network. An external facing honeypot can add layers of network such as De-Militarized Zone (DMZ) and VLANs into the design. These are designed typically to delay and distract an external hacker; the internal design does not have this luxury. The internal user will have an understanding of the existing network topology and if the honeypot network topology likewise does not effectively and reliably mimic the existing real network topology then once again exposure of the internal honeypot is a high-risk proposition.

CONCLUSION

The use of honeypots as an effective countermeasure to external attack is a well proven concept. Much of the literature in this area of investigation focuses on the use of honeypots as external facing countermeasures to external attacks. There is very little, if any, literature available or experimentation being conducted on internally focused honeypots. This indicates the need for some exploratory and ongoing research in this area.

The *modus operandi* of internal honeypot deployment presents significant changes in focus and design from externally faced honeypots. Malicious insiders will have a significant tactical advantage over their external counterparts when probing, penetrating or compromising a network this is borne out by many of the security surveys are conducted around the world. This significantly changes some of the basic premises upon which existing honeypot technologies are deployed and has major impacts on design and deployment.

Internal honeypots offer a potentially viable method for tracking malicious insiders compared to other contemporary network countermeasures and this warrants further investigation. The high level of interaction and logging that is possible in a single instance is potentially superior to Firewalls, IDS and IPS. Where attacks may simply be denied by firewalls or IDS, a honeypot system will allow for greater surveillance and monitoring of the malicious insiders activities.

Future research in this area needs to be conducted into the practical implementation and deployment of internal honeypots within contemporary organisational settings. Deployment of internal honeypots is not a simple technical issue but also has potentially many organisational factors such as trust and insider malfeasance to contend with as disenfranchisers of this particular technology.

REFERENCES

Anonymous. (2003). Watching the watchers. *Country Monitor, 11*(37), 6.

AusCERT, et al. (2004). *The 2004 Australian Computer Crime and Security Survey* (report No. 4).

Queensland: University of Queensland.

AusCERT, et al. (2005). *The 2005 Australian Computer Crime and Security Survey* (report No. 5). Queensland: University of Queensland.

Briere, D. (2005). Defending the castle. *Network World, 22*(22), 37.

Camardella, M. J. (2003). Electronic monitoring in the workplace. *Employment Relations Today, 30*(3), 91.

Conry-Murray, A. (2005). Keep Attackers At Bay. *InformationWeek*(1046), 45.

CSO Magazine, et al. (2004). *The 2004 E-crime watch survey* (report). Pennsylvania: Pittsburgh: Carnegie Mellon University.

Fidler, S. I. R. (2004). Workplace Privacy Issues: Potential Pitfalls For Unwary Employers (with Forms). *Practical Lawyer, 50*(5), 43.

Gordon, L. A., et al. (2004). *2004 CSI/FBI Computer Crime and Security Survey* (No. 9). San Francisco: Computer Security Institute, Federal Bureau of Investigation's Computer Intrusion Squad.

Gordon, L. A., et al. (2005). *2005 CSI/FBI Computer Crime and Security Survey*: Computer Security Institute.

Gupta, N. (2002). *Improving the Effectiveness of Deceptive Honeynets through an Empirical Learning Approach.* Paper presented at the 2002 Australian Information Warfare and Security Conference, Perth, Western Australia.

Honeynet Project. (2004). *Know your enemy: Learning about security threats* (2nd ed.). Boston: Addison-Wesley.

Oudot, L. (2003). *Fighting Internet Worms With Honeypots*. Retrieved 5th August, 2005, from http://www.securityfocus.com/infocus/1740

Richardson, R. (2003). *2003 CSI/FBI computer crime and security survey* (report No. 8). San Francisco: Computer Security Institute, Federal Bureau of Investigation's Computer Intrusion Squad.

Robb, D. (2005). Erecting Barriers. *Computerworld, 39*(12), 42.

Schneier, B. (2005). *2005 Internet attack trends*. Retrieved 15 June, 2005, from http://www.schneier.com/essay-085.pdf

Schultz, E. (2002). Honeypots make headlines. *Computers & Security, 21*(6), 489.

Spencer, B. (2004). *Honeypots: A couple of production honeypots used to fight spam*. Retrieved 13 February, 2004, from http://seclists.org/lists/honeypots/2004/Jan-Mar/0025.html

Spitzner, L. (2002). *Know your enemy*. Indianapolis: Addison-Wesley.

Spitzner, L. (2003). *Honeypots - tracking hackers*. Boston: Pearson Education Inc.

Valli, C. (2003). *Honeyd - A fingerprinting Artifice.* Paper presented at the 1st Australian Computer, Information and Network Forensics Conference, Scarborough, Western Australia.

Wilson, J. (2005, June 25). The Two Sides Of Network-Security Devices -- Infonetics study shows secure routers and appliances are most popular. *VARbusiness,* 65.

Yek, S. & Valli, C. (2003). If you go down to the Internet today - Deceptive Honeypots. *Journal of Information Warfare, 2*(3), 101-108.

COPYRIGHT