Fred Cohen & Associates - Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

Moving target defenses with and without cover deception

Moving Target (MT) defenses have been identified as a key research area by the NITRD. This paper addresses some of the requirements for effective MT defenses based on experimental and theoretical notions associated with deception.

Background

According to http://cybersecurity.nitrd.gov/page/moving-target, [1] "Research into Moving Target (MT) technologies will enable us to create, analyze, evaluate, and deploy mechanisms and strategies that are diverse and that continually shift and change over time to increase complexity and cost for attackers, limit the exposure of vulnerabilities and opportunities for attack, and increase system resiliency. The characteristics of a MT system are dynamically altered in ways that are manageable by the defender yet make the attack space appear unpredictable to the attacker."

Some history of information-related MT defenses

The concept of MT defenses is not new, nor are the underlying concepts associated with driving up attacker complexity disproportionately to defender complexity. The concept ranges at least back to Shannon [2] who applied his information theory to break known ciphers, provided a proof that the only theoretically unbreakable cryptosystem was the so-called perfect cipher, introduced the concepts of diffusion and confusion, and introduced the concept of workload, which is the basis for using imperfect cryptosystems today. The concept of public key cryptography in general,[3] the RSA cryptosystem[4] in particular, and other public key cryptosystems depend on this concept of computational leverage.

Code obfuscation was widely examined in the mid-1980s and resulted in many examples associated with an obfuscated code contest [5] followed by the theoretical notion of using such techniques to protect operating systems [6] which included example transformation to obfuscate code so that attacker complexity would be driven up to predictable levels while defender complexity would remain relatively small. Subsequent work in this area has produced many papers and masters theses.

The various approaches to MT defense to date are oriented toward defense against computer network attack (CNA). A similar approach was taken with the approach of rapidly changing IP addresses and ports associated with systems under attack. [7][8] In experiment 4 of [7], attackers were forced to locate and relocate targets with and without additional deceptions present. The net effect was that the presence of additional deceptive defenses resulted in slower progress in the attack graph by attackers and fluctuation between deception and non-deception targets by attackers.

The generic attack graph relative to MT defenses

Attackers have been characterized by a generic attack graph used to discuss and analyze progress in attacks as well as to understand different situations. The generic attack graph, less deception, [8][11] is shown in Figure 1:

Further exploration of attack graphs for measuring the efficacy of defenses was also explored. [7] The net effect of MT technologies at the network level for can defense is to force the attacker to return to the "Find target" state even for identified targets, and to do so at a rate effective enough to prevent successful penetration and synchronization.

Terms

In this paper, we refer to attacker(s), defender(s), target(s) (the party or system being deceived), "Find target" (an activity of the attacker in the attack graph methodology), the protected unit (the system being protected by motion and\/or deception), computer network attack (CNA), and moving target (MT).

Challenges with CNA MT lacking deceptive cover

MT defenses such as those that alter Internet Protocol (IP) addresses and ports are problematic for several reasons, depending on the specifics of the situation. In particular, there are three situations to consider in this light; (1) distant, (2) proximate, and (3) enveloped:

1. Distant implies that the attacker is able to send signals to and receive returned signals from the protected unit. This limits the attacker to active probing of defender environments. This is the norm for remote Internet-based attack.

2. Proximate implies that the attacker is in the same position as the defender, so that each can observe and potentially interfere with signals from the other to third parties. This is the norm for attackers on the same network or attackers who have gained access to the same network as the protected unit through the attack process. Either an insider or an attacker who has achieved the "Expand Access" or "Exploit Access" state in the generic attack graph.

3. Enveloped implies that the attacker has gained so much control that all signals to and from the protected unit are under the complete control of the attacker. At this point, the protected unit observes only what the attacker permits it to observe and induces only the external effects attacker permits it to induce.

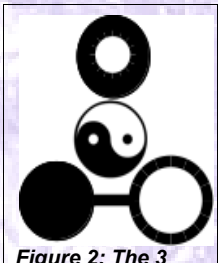


Figure 2: The 3 situations

The three situations may be graphically depicted as shown in Figure 2, where the top depiction is called the "enveloped" situation, the middle depiction is the "proximate" situation, and the bottom depiction is the "distant" situation. Envelopment can apply to either attackers enveloping the protected unit or defenders enveloping attackers, but only attackers enveloping the protected unit is relevant to the present discussion.

Without deceptive cover, specific methods may be applied to each situation to rapidly detect the movements of the protected units and, in effect, real time detection and response is feasible to different extents in different situations. For example, and without limit:

Distant attackers without deceptive cover

Distant attackers can use methods like broadcast pings to rapidly identify available IP addresses, and by doing so faster than the rate required to continue synchronization with the protected unit, can identify small subsets of the total address space to continue communications with. By near-simultaneous acts to continue communications with available protected unit addresses, movements can be bypassed. Of course there are many changes that could be made by defenders and compensating moves by attackers. Experimental results [7] showed that moderately skilled distant attackers with basic knowledge of the concept of operations could create semiautomated tools to allow rapid synchronization with such MT defenses in an hour or less when additional deception was not present.

Proximate attackers without deceptive cover

Proximate attackers can observe and send signals just as the protected unit can. In this situation, low-level protocols such as broadcast packets with MAC addresses sent to routers and switches may be observed, and local broadcasts may be used to rapidly identify local devices. In the proximate situation, attackers have far greater visibility which allows them to observe behaviors and rapidly track changes in addresses and similar behaviors. Identifying signals of all sorts become available, including potential attacks that allow the attacker to force connections to travel through the attacker. MT technologies at the network level are rapidly detected in this environment, and while a back and forth can still take place, it is far harder to prevent the attacker from almost instantly tracking movements and compensating for them in its attacks. Experimental results showed that moderately skilled attackers with proximate access could regularly defeat these defenses with existing tools in a matter of minutes when additional deceptive cover was not present.[7]

Enveloping attackers without deceptive cover

Envelopment takes the challenges of MT technology even further. Experimental attacks were essentially trivial to generate and uniformly successful in the enveloped situation.

Once in, game over

Perhaps the biggest challenge identified without deceptive cover is that once an attacker manages to gain entry into a protected unit, essentially all effects of MT defenses become extremely limited. To successfully defeat such defenses, the attacker need only formulate a way to create reliable communications over noisy channels where communications are started from the protected unit with responses from the attacker. Planted Trojan horses within the protected units permit, as an example, UDP traffic to and from the protected unit within well under a second, where the protected unit initiates a UDP packet (e.g., a DNS request) and the attacker responds to it. The protected unit Trojan horse receives the reply and treats it as desired to form a channel that adapts to movements in near real time without any explicit acts on the attacker's part. In practice, and as validated experimentally, once access is gained at the protected unit level of a normal user with the ability to run arbitrary commands, within less than a second, a Trojan horse can be automatically planted, and the effect of movement

of the protected unit from that point forward has almost no protective value.

The effect of adding deceptive cover

The challenges associated with MT as identified above relate to the fact that the deception afforded by movement can be readily and rapidly defeated by network topology mapping, behavioral detection, and other similar approaches that already exist and are already widely used by attackers as part of their efforts to "find target"s.

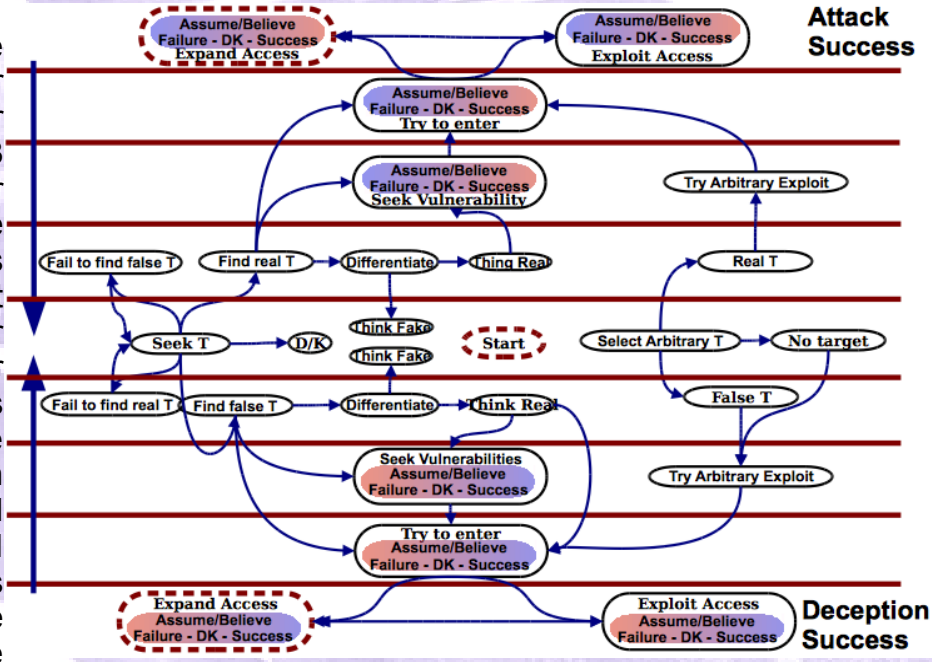
MT in this arena has two substantial effects; (1) making the "find target" operation slower and less certain, and (2) forcing attacks to return to the "find target" operation from other states in the attack graph at a rate associated with the movement rate. To the extent that the "find target" operation is the attack method being defeated by MT defenses, motion on its own has been experimentally shown to be of limited value.

The addition of deceptive cover, in the form of induced and suppressed signals, provides potential improvements to MT in the following ways.

Distant attackers with deceptive cover

Adding deceptive cover for distant deception targets provides involves inducing and suppressing return signals from the target's acts. While other protective measures may be used to suppress incoming signals, these are not deceptive methods with regard to the target, except to the extent that these methods are used to ultimately induce or suppress return signals.

For distant attackers, the attack graph under deception becomes far more complex. Figure 3 shows the attack graph for deceptive cover in the presence of deception, as identified in [8]. Starting at "Start", the distant attacker under deceptive cover encounters false positives and false negatives in the "find target" phase, and with deceptions at a non-trivial level of depth, the workload per false positive increases dramatically while the false negative tends to push the attacker into more fruitless "find target" activities.



Experimental results showed that the presence of false returns was effective in countering successful "find target" operations as reflected in the difference in progress in attack graphs over time between attackers under deception and not under deception in experiment 4 of [7]. Specific error induction was apparently achieved in these cases. [7][11]

Proximate attackers with deceptive cover

As and if the attacker progresses from “find target” to “identify vulnerability” or “exploit vulnerability”, the successful attacker gains proximate status with regard to other systems in the environment, including the protected unit. At this point, with deceptive cover in the local environment, the same problems with “find target” remain for the attacker, assuming the deception is adequate in each of two arenas; (1) the deception must induce and suppress return signals in the local area, and to the extent that it fails to do so effectively, the “find target” operation will be more successful, and (2) the deception must induce additional signals to cover the passive surveillance capabilities of the proximate attacker. In essence, this means that added cover in the form of false traffic is necessary in order to provide cover as the protected unit movements take place. Typically, this will be in the form of continuation of pre-movement sessions and session sequences after movement, induction of false sessions and session sequences prior to movement, and induction of false returns from false induced signals. These are more effective if placed in a larger deceptive context. [11]

Experiments involving proximate attackers showed that induced deceptive traffic was effective in defeating “find target” in proximate situations, [7] but the fidelity of these signals was inadequate to allow some of the more complex functions such as pre-movement sessions and session sequences coordinated to movement times.

Enveloping attackers with deceptive cover

With deceptive cover, such as automated responses on all unused ports, added protection against attacks may be afforded, but ultimately, in an enveloped environment, this will likely have limited effect. An example approach is to induce signals in response to all external signals and emit deceptive signals so that identifying applicable ports as they move requires differentiating between real and deceptive uses. This then implies that every protected unit as well as deception mechanisms must induce and respond to deceptive traffic, which drives up bandwidth utilization significantly and requires increased coordination and potential for fratricide.

The random strike attack strategy

The “random strike” attack strategy avoids many of the early elements of deception, in particular, the “find target”, “identify vulnerability”, and “exploit vulnerability” steps, by simply attacking at random. In this case, only false targets with a deceptive depth beyond simple network returns will continue to operate effectively. The attacker will have to spend time and effort after finding deceptive targets just as they would after finding non-deceptive targets. The advantage of MT in this case is that the attacker loses contact with the unit under attack, whether real of deceptive, at the movement rate. Planted Trojan horses in deceptive systems may further engage the attacker giving continuity of apparent service, thus consuming resources regardless of whether the unit is deceptive or protected.

Experiments undertaken to date only performed such activities for proximate situations, however indications are that similar deceptive effects could be attained, albeit at the cost of substantial overall network bandwidth reduction.

The need for content as well as MT

The limitations of deceptive cover come largely in the limits of the defender's ability to prevent the target from differentiating between legitimate and deceptive traffic and behaviors. At the level of network protocols and similar behaviors, deceptions have been implemented to the point where they have not been successfully differentiated and are not likely to be for the foreseeable future. This is due, in essence, to a design in which the systems used for deception are identical to the protected units.

However, even if protected units and protective deception systems are identical, in experiments performed to date in which deceptions were effective for indefinite periods, deceptions systems were successfully penetrated just as protected units were, without deception, and attackers gained access to and content from deceptive content from deception systems when under deception just as attackers not under deception gained access to and content from protected units when deceptions were not present.

The only remaining differentiator between deceptions and non-deceptions was the content that the attacker gained access to. For deceptions without the need for long-term efficacy, and for “capture the flag” exercises, it may be permissible to ignore issues of content, but for deceptions intended to last for a significant time period and have effects in the greater scheme of things, content must also be provided that survives scrutiny by attackers at issue for the duration of the period of deception. Failure to address the deception content issue ultimately leads to a failure of the overall deception, and as content deception detection becomes the issue, an arms race in this arena is likely to arise.

In addition, attackers who are not willing to stop at penetration of one system, can continue to attack system after system through the privilege expansion and exploitation processes, and in doing so, will eventually penetrate protected units, if allowed to continue without added controls put in place. Given enough time, such an attacker will persist at attacking system after system in the MT environment until they eventually succeed in penetrating protected units, with the time presumably proportional to the extent to which deception consumes the attack space relative to protected units.

In essence, response ultimately becomes necessary, and of course, to the extent that such response depicts the desired beliefs in the attacker, the attacker may be deceived over a long time period based on content retrieved. The net effect then is an increase in time to successfully attach, increased visibility of attacks to defenders, and long-term effectiveness of deceptive content.

In related work, responses involved removing access to protected units while deception was permitted to continue. This then makes time to penetrate protected units from a detected attack location infinite, once detected. Adaptation by attackers then allows them to consume increased resources to become moving attackers, which then produces a situation analogous to a force on force exercise in which attackers have more and more of their resources discovered and permanently deceived with time, while defenders continue to get attacked from more and more locations. [9][10]

Summary, conclusions, and further work

Without additional deceptive cover, MT CNA defenses have shown poor performance against moderately skilled distant attackers, worse performance against moderately skilled proximate attackers, and no effect against moderately skilled enveloping attackers. With deceptive cover, both moderately skilled and more highly skilled distant attackers have been successfully deceived. MT methods had mixed results on the “find target” step, but produced more effective overall results over longer time periods, apparently related to the synergistic effects of movement in the presence of deception.

For the proximate case, without additional cover, MT showed effects only over relatively short time frames of minutes to hours, and after that, were readily and repeatedly defeated. The effects of MT continued to create problems for attackers compared to non-MT situations, but even effort of less than an hour by moderately skilled attackers produced automation to largely overcome those difficulties. Once units were penetrated and Trojan horses put in place, a process that took seconds for highly skilled attackers and less than a minute for moderately skilled attackers, proximate attackers were effective at making steady progress.

For enveloped situations, MT without added deceptive cover was largely ineffective.

The addition of deceptive cover substantially altered the situation, resulting in long-term effectiveness of deceptions for the distant and proximate cases, with MT ultimately proving protective to the level of the mean time to penetrate the ratio of space taken by protected units to deceptive cover.

The use of content deceptions to enhance all of these methods was necessary in order to produce long-term success in the larger context.

References

[1] http://cybersecurity.nitrd.gov/page/moving-target

[2] C. Shannon, “Communications Theory of Secrecy Systems”, Bell Systems Technical Journal (1949):656--715.

[3] W. Diffie and M. Hellman, “New Direction in Cryptography”, IEEE, Transactions on Information Theory, 644-654, Nov, 1976, IT-22, #6,

[4] R. L. Rivest, A. Shamir, and L. Adleman, “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems”, Comm. of the ACM (February 1978) 21, no. 2:120--126.

[5] The International Obfuscated C Code Contest, http://www.ioccc.org/

[6] F. Cohen, "Operating Systems Protection Through Program Evolution", IFIP- TC11 `Computers and Security' (1993) V12#6 (Oct. 1993) pp.565 – 584

[7] F. Cohen, I. Marin, J. Sappington, C. Stewart, and E. Thomas, “Red Teaming Experiments with Deception Technologies”, 2001.

[8] F. Cohen and D. Kaoike, “Leading attackers through attack graphs with deceptions”, IFIP TC-11 Computers & Security, Volume 22, Issue 5, July 2003, Pages 402-411

[9] F. Cohen, et. al. “A Mathematical Structure of Simple Defensive Network Deceptions”, IFIP-TC11, Computers and Security, Volume 19, Number 6, 1 October 2000, pp. 520-528(9).

[10] F. Cohen, “A Note on the Role of Deception in Information Protection”, , IFIP-TC11, Computers and Security, 1998, vol. 17, no. 6, pp. 483-506(24).

[11] F. Cohen, “The Use of Deception Techniques: Honeypots and Decoys”, Handbook of Information Security, V3, p646. Wiley and Sons, 2006.

