Fred Cohen & Associates - Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

Security Decisions: When to use deception

Deceptions increase the cost and complexity of attack for attackers while decreasing the effort required to detect, delay, and counter attacks. But deceptions also have some costs associated with their operation. So there is a tradeoff between the costs and benefits of deception, which makes it a risk management decision. But additional guidance may help to better understand this issue, and divide and conquer the solution to when and where to use deceptions, and when and where to avoid them.

The underlying key to understanding deception

The key differentiating issue in the use of deceptions that are not built into systems and operational by default is their use in mitigating against event sequences with potentially serious negative consequences.

> In order to be effective, such defenses must conceal event sequences that attackers are likely to attempt to exploit and that have serious negative consequences.
>
> They can do this preventively by adding more event sequences that are likely to be tried by the attacker and that do not have serious negative consequences, thus increasing the search space for the attacker.
>
> Alternatively, they can be used responsively once an attack attempt has been detected to cover event sequences with potentially serious negative consequences from the attacker while permitting normal users and uses to continue uninterrupted.

Options and decisions:

There are 5 basic alternative approaches to the use of deceptions:

1. **Never use deceptions:** It is infeasible to never use deceptions for defense.

   For example, almost all modern systems ask for user identification (UID) and password before revealing that login was denied, even though the use of an invalid UID could have triggered an immediate refusal and the indication that the UID is invalid can save time and effort in many circumstances. This provisioning of false or misleading information benefits security at a small cost to normal users. Similarly, when looking for files in a system, protected directories and files appear not to exist rather than having their name, size, and other characteristics revealed. This concealment is widely considered a necessary deception for effective protection. There are many other built-in deceptions in modern systems that either cannot be disabled or are difficult to work without.

2. **Use deceptions when they are built into existing systems:** The use of deceptions

that are built into existing systems is the default and it is widely used.

While this is an acceptable approach, it is far less effective than adding other deceptions at only a slightly higher cost. This option alone is reasonable for companies with less than $10,000 of annual information technology budget because it bears no added costs and has some amount of protective effect.

3. **Use deceptions at firewalls:** The use of deceptions at firewalls is strongly advised for any company with information technology in excess of $10,000 per year.

   While the utility of firewalls is substantial in terms of limiting attacks, the utility is greatly enhanced when the firewalls do not reveal available attack paths to attackers. When a firewall does not use deceptions, most attacks rapidly focus on the legitimate paths through the firewall and seek out any weaknesses that may remain. For less than $10,000 an effective deception system can be placed at most interfaces to a firewall, configured for standard deceptions that do not interfere with the firewall, and allowed to operate effectively without harm to the network. This also provides rapid notification of many classes of attacks and in many ways is more effective at detection of attacks than standard intrusion detection systems.

4. **Use deceptions within internal networks:** The same principles that apply to external attacks apply to the deception of attackers who have broken into the company network and insiders who wish to do unauthorized exploration of internal networks.

   By placing deceptions at internal firewalls and routers, internal scans and attacks are greatly disrupted while intrusion attempts are rapidly identified. Again, the cost is on the order of less than $10,000 per firewall or router, and in volume the costs get considerably lower. This approach is strongly advised for any company with an information technology budget in excess of $100,000.

5. **Use deceptions within systems:** We advise against the use of deceptions within computers or the use of pure honey pot systems for small to medium sized businesses unless they are in the computer security business.

   This technology is not yet mature and it is expensive and complex to operate. Its primary use today is for research and not protection.

Summary:

Always use built-in deceptions. Augment deceptions with network-based deceptions if your total IT budget is in excess of $10,000 per year. If your total IT budget exceeds $100K per year, deceptions should also be used at internal firewalls and gateways.

> "Oh what a tangled web we weave, when first we practice to deceive" - Sir Walter Scott MARMION - (1808)

But as we practice deception more and more, we gain an appreciation for when and where it works, and when and where we need to avoid it.