Using Deception to Shield Cyberspace Sensors

Mason Rice, Daniel Guernsey, Sujeet Shenoi

Chapter 1

USING DECEPTION TO SHIELD CYBERSPACE SENSORS

Mason Rice, Daniel Guernsey and Sujeet Shenoi

Abstract The U.S. President's Comprehensive National Cybersecurity Initiative calls for the deployment of sensors to help protect federal enterprise networks. Because of the reported cyber intrusions into America's electric power grid and other utilities, there is the possibility that sensors could also be positioned in key privately-owned infrastructure assets and the associated cyberspace. Sensors provide situational awareness of adversary operations, but acting directly on the collected information can reveal key sensor attributes such as modality, location, range, sensitivity and credibility. The challenge is to preserve the secrecy of sensors and their attributes while providing defenders with the freedom to respond to the adversary's operations.

This paper presents a framework for using deception to shield cyberspace sensors. The purpose of deception is to degrade the accuracy of the adversary's beliefs regarding the sensors, give the adversary a false sense of completeness, and/or cause the adversary to question the available information. The paper describes several sensor shielding tactics, plays and enabling methods, along with the potential pitfalls. Well-executed and nuanced deception with regard to the deployment and use of sensors can help a defender gain tactical and strategic superiority in cyberspace.

Keywords: Cyberspace sensors, deception, sensor shielding

1. Introduction

At 6:00 a.m., just before power consumption reaches its peak, a computer security expert at an electric power utility receives the text message, "Fireball Express," indicating that a cyber operation is being executed on the utility's assets. The expert is a covert government agent, who is embedded in the power utility to monitor cybersecurity breaches. Only the CEO of the company is aware of her status as a government agent.

Months earlier, the embedded agent created a honeynet at the utility to draw cyber operations conducted by adversaries. The honeynet presents an intruder with a carbon copy of the utility's SCADA systems. Meanwhile, to enhance situational awareness, U.S. intelligence has secretly implanted sensors in core Internet routers across America. The "Fireball Express" alert was triggered by correlating information gathered from the honeynet and the Internet sensors. The analysis indicates that the operations are being conducted by a nation state adversary.

U.S. officials must act quickly. Directly confronting the nation state adversary about the intrusion at the utility could reveal the existence of the honeynet and, possibly, the presence of the embedded agent. How can the U.S. maintain the secrecy of its sensors while responding strongly to the intrusion?

This paper presents a framework for using deception to shield cyberspace sensors from an adversary. In particular, it categorizes cyberspace sensors and their attributes, outlines sensor shielding tactics, plays and enabling methods, and discusses the potential pitfalls. Well-executed deception can shape the beliefs of the adversary to the advantage of the defender, enabling some or all of the sensor attributes to be shielded while providing an opportunity for the defender to confront the adversary about its cyber operations. The paper discusses several examples of deception and presents options for shielding sensors, including the sensors in the fictional Fireball Express scenario at the electric power utility.

2. Sensors and Deception

Sensors provide information about the state of an environment of interest and the activities of entities in the environment. Sensors are characterized by their modality, location, range, sensitivity and credibility. The modality of a sensor refers to its detection mechanism (e.g., electronic, thermal, magnetic, radiant and chemical) [9]. The location and range of a sensor specify the location and space in which the sensor can operate effectively. Sensitivity refers to the ability of a sensor to detect stimuli and signals; cyberspace sensors may be tuned to detect specific viruses and worms, rootkits and network probes. The credibility of a sensor is a function of its reliability and durability. Reliability refers to the ability of a sensor to correctly measure the parameter of interest while durability refers to the ruggedness of the sensor and its tamper resistance.

The attributes of a sensor determine its secrecy. In general, if one attribute of a sensor is classified, the existence and/or use of the sensor may be classified [4]. However, the existence of a sensor may be public knowledge, but its attributes could be classified. For example, the location, basic sensitivity, credibility and one of the modalities (magnetic) of the U.S. underwater sound surveillance system (SOSUS) may be known, but its true sensitivity and other modalities are closely guarded secrets [11].

The importance of maintaining the secrecy of sensors cannot be overstated. Scholars believe that the shroud of secrecy surrounding U.S. and Soviet satellite reconnaissance capabilities may have led to the Strategic Arms Limitation Talks

(SALT) I and II in the 1960s and 1970s. Shortly after one of the talks, the U.S. publicly acknowledged its use of satellite reconnaissance without providing details about the specific modalities (e.g., optical and electrical) and sensitivity. Although the Soviets released little information about their capabilities, it was widely believed that they had the ability to monitor U.S. compliance of the arms limitation agreements. As a result, the SALT documents used the ambiguous phrase "national technical means of verification" [8]. Sensor secrecy and the resulting uncertainty in the monitoring capabilities of the two countries likely facilitated the SALT agreements during the height of the Cold War.

When using any instrument of national power – diplomacy, information, military and economics – it is often necessary to manipulate the response to sensor signals in order to mask one or more sensor attributes. Reacting in an obvious, unnuanced manner to sensor data about an adversary can compromise the sensor. For example, Al Qaeda was quick to recognize after attacks by U.S. forces in Afghanistan that the U.S. could track targets based on cell phone signals and other electronic transmissions. As a result, Osama bin Laden and other terrorists resorted to sending messages via courier [12].

Historically, deception has been used very effectively when exerting instruments of national power [5, 13]. Deception increases the freedom of action to carry out tasks by diverting the adversary's attention. Deception can persuade an adversary to adopt a course of action that potentially undermines its position. Also, deception can help gain surprise and conserve resources. This paper discusses how deception can be used to obscure one or more attributes of cyberspace sensors.

3. Deception Framework

A deception strategy should deliberately present misleading information that degrades the accuracy of the adversary's beliefs, give the adversary a false sense of completeness, and/or cause the adversary to misjudge the available information and misallocate operational or intelligence resources. With regard to preserving sensor secrecy, the goal of deception is, very simply, to cause the adversary to have incorrect or inaccurate impressions about the modality, location, range, sensitivity and/or credibility of the sensor.

Figure 1 illustrates the goal of a deception strategy that seeks to preserve sensor secrecy. The white squares at the bottom of the figure represent the true sensor attributes that are known to the defender. The black squares at the top of the figure denote a combination of true, assumed or false sensor attributes that the defender wants the adversary to believe. To accomplish this goal, the defender creates a "deception play," represented by the black circles in the middle of the figure. The deception play provides false information about the modality and location of the sensor, no information about the sensor range, and true information about the sensitivity and credibility of the sensor. Note that the adversary may already hold certain beliefs about the sensor attributes prior to the execution of the deception play by the defender.

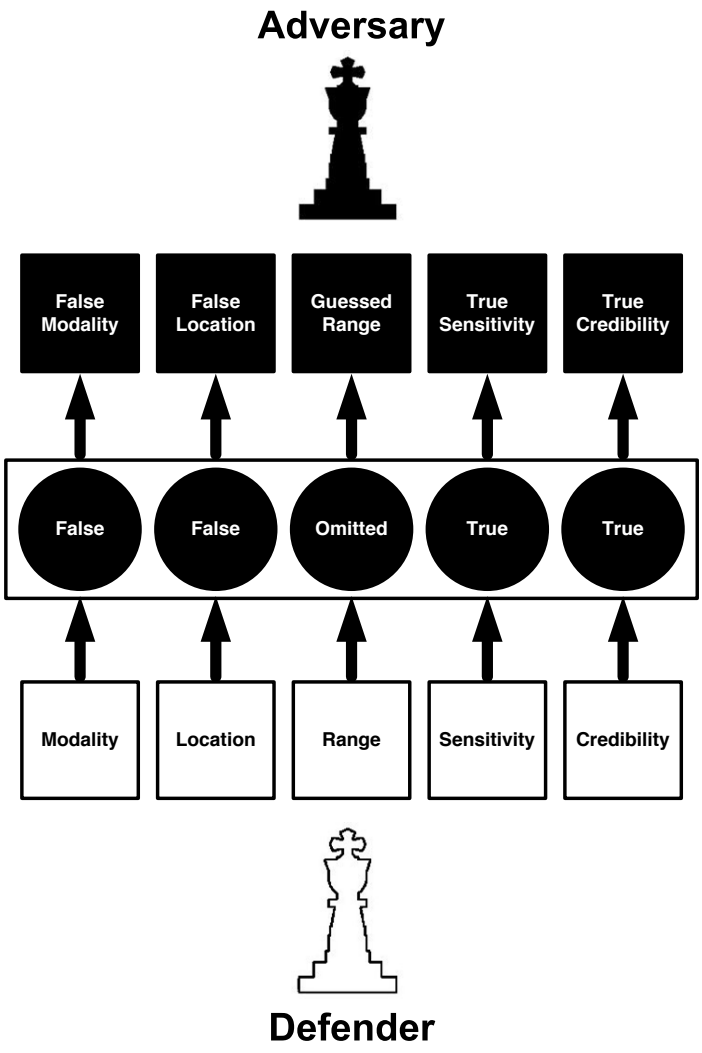


Figure 1. Deceiving the adversary.

A deception play typically targets the adversary's intelligence, surveillance and reconnaissance capabilities to shape the adversary's beliefs [15]. The U.S. Department of Defense has adopted the "See-Think-Do" deception methodology [15]. The methodology focuses on the adversary's cognitive processes: (i) See – what portions of the defender's environment or activities does the adversary observe? (ii) Think – what conclusions does the adversary draw from the observations? and (iii) Do – what actions may the adversary take upon analyzing the observations?

Table 1. Passive deception techniques.

Concealment	Concealment uses natural cover, obstacles or distance to hide something from the adversary. Concealment is the earliest form of military deception. An example in the cyberspace domain is the embedding of sensors in networking gear.
Camouflage	Camouflage uses artificial means to hide something from the adversary. Note that covering military equipment with vegetation is an example of camouflage rather than concealment. An example in the cyberspace domain is the generation of artificial network traffic by a honeynet to camouflage cyber operations such as intelligence gathering.

An example of the See-Think-Do methodology is Operation Bodyguard, the deception plan instituted in advance of the D-Day invasion [15]. The Allies conducted air raids, sent fake messages and even created a phantom army to convince the German High Command that the landing point would be Pas de Calais. The German High Command saw the deceptive operations (see), believed that Calais would be the target of the assault (think), and redirected forces that could have been placed in Normandy to defend Calais instead (do).

The scope of a deception play is limited by the time and resources available for its planning and execution, the adversary's susceptibility to the deception, and the defender's ability to measure the effectiveness of the deception. Additionally, the lack of accurate intelligence and cultural awareness can hinder a deception play. The best outcome for a deception play is for the adversary to fall for the deception. Note, however, that the defender may have a satisfactory outcome even if the play drives the adversary to believe something other than the truth.

4. Deception Constructs

This section discusses the principal deception constructs. These include the classes of deception, deception plays, deception principles and the types of information collected by the adversary.

4.1 Classes of Deception

Deception involves two basic premises, hiding something real and showing something false [5]. This gives rise to two classes of deception: passive and active.

- **Passive Deception:** Passive deception focuses on hiding. It tends to be "safer" than active deception because it does not seek to instigate action on the part of the adversary [5]. Techniques for hiding include concealment and camouflage (Table 1).

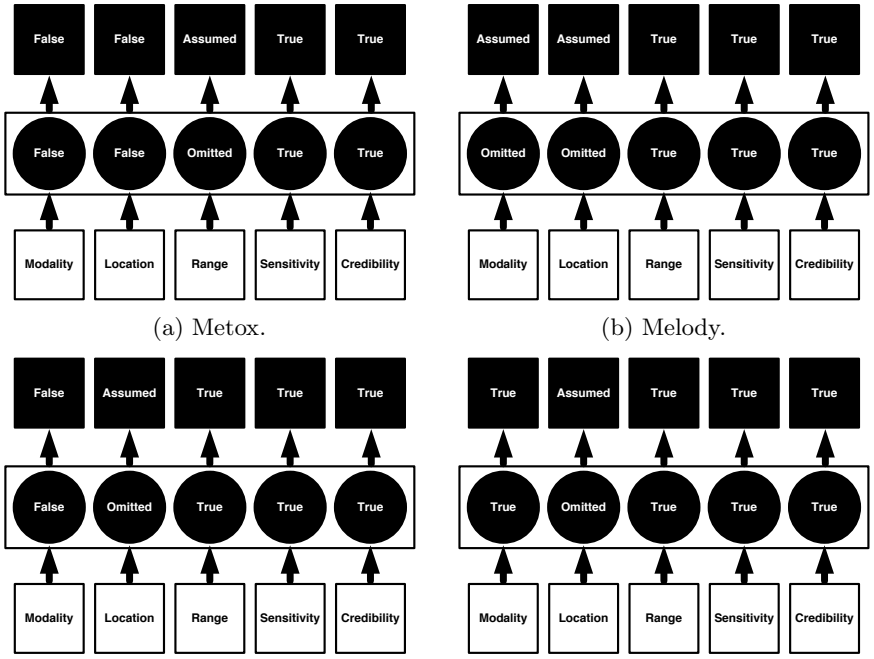
Table 2. Active deception techniques.

Planting False Information	The adversary obtains information that results in an incorrect or inaccurate belief. An adversary can be fed false information, for example, via a newspaper article or an Internet posting.
Ruse	The defender impersonates the actions or capabilities of another entity to cause the adversary to have an incorrect or inaccurate belief. An example is the delivery of fake orders and status reports in the enemy's language. A cyberspace example involves spoofing the return IP addresses of packets.
Display	The defender makes the adversary see or believe something that is not there. An example is the positioning of fake artillery pieces and dummy aircraft. A cyberspace example is the generation of fake Internet traffic to create the illusion that a system has more or less capabilities than it actually has.
Demonstration	The defender conducts an operation that conveys an incorrect or inaccurate belief to the adversary. A cleverly orchestrated demonstration can lead the adversary to make a tactical or strategic error. During the year prior to the 1973 Arab-Israeli war, Egypt repeatedly moved its troops to the Israeli border, only to recall them. The Israelis were conditioned by the demonstrations, and were thoroughly surprised when the Egyptians invaded. A cyberspace example involves the defender performing repeated probes of the adversary's network before escalating its activities and corrupting a key asset.
Lying	The defender tells a lie, which causes the adversary to have an incorrect or inaccurate belief.

- **Active Deception:** Active deception focuses on showing something (e.g., knowledge and capabilities) that is not real [5]. It tends to be more "risky" than passive deception because it seeks to instigate action on the part of the adversary. Active deception techniques include planting information, ruses, displays, demonstrations and lying (Table 2).

4.2 Deception Plays

Insight into the thought process of the adversary enables the defender to outthink the adversary [5, 6]. An example of engaging insight is the use of absolute truth in a deception play. Absolute truth involves telling the truth in a situation where the adversary is unlikely to believe the truth – perhaps because of a strong prior belief. Another example is omission, which involves the exclusion of some information. Omission is common in politics, especially during an election campaign when a partial revelation of an opponent's voting record can gain votes. Omission also can be used to hide contrary evidence



(a) Metox. (b) Melody.

(c) Weapons seizure. (d) Osama bin Laden.

Figure 2. Example deception plays.

and create ambiguity, especially when the adversary is predisposed to certain beliefs.

Active and passive techniques can be used individually or in combination to create plays that are intended to deceive an adversary. Masking, misleading, mimicking and confusing are four of many possible plays that can hide the real and show the false [2, 7]. Masking may involve camouflage and concealment, while misleading may involve planting information, ruses, displays, demonstrations and lying. Misleading could be as simple as transmitting a clear, unambiguous false signal or as complex as planting information for an adversary to find, lying to a third party who will pass the information on to the adversary and conducting ruses under the guise of the adversary. Mimicking involves copying some object or behavior (i.e., ruse). Techniques for confusing an adversary include raising the noise level associated with a specific act or acts to create uncertainly and/or paralyze decision making, or to purposely depart from an established pattern of activity by inserting random actions in a well-known activity.

Figure 2 presents four historical deception plays. Each deception play is expressed – as in Figure 1 – in terms of the actual sensor attributes, the deception play and the desired adversary beliefs.

Metox During World War II, the British could approximate the location of German U-boats using highly sensitive communications intelligence (COMINT) and then pinpoint their exact locations using radar [6]. The Germans installed Metox radar detectors on their U-boats to enable them to evade British attack vessels. In response, the British changed the frequency of their tracking radar, and used deception to protect their COMINT sources. The British also arranged for German agents to acquire two pieces of spurious intelligence. One was that the Royal Navy had abandoned radar in favor of infrared detectors; the other was that Metox produced a signal that RAF planes could target.

The Germans acted on the spurious intelligence. They developed a paint that reduced the infrared signatures of U-boats, and worked to suppress the Metox emissions. Eventually, the Germans realized that the British had merely changed their radar frequency, and they attributed the U-boat sinkings exclusively to the British radar systems. The deception play enabled the British to preserve the secrecy of their COMINT sources.

Figure 2 shows that the deception story provided inaccurate information about the modality and location of the sensor, omitted range information, and revealed information about sensor sensitivity and credibility.

Melody The 1972 Anti-Ballistic Missile (ABM) treaty between the United States and the Soviet Union prohibited the development and testing of ABM systems. Soon after the treaty was ratified, the U.S. detected Soviet cheating via a highly classified feature of Project Melody that intercepted Soviet missile tracking radar signals [10]. During subsequent negotiations in Geneva, then Secretary of State Henry Kissinger confronted his Soviet counterpart with the dates and times that the Soviets had cheated on the treaty. The cheating stopped and the Soviets began a "mole hunt" for the spy who gave the information to the United States. America got its way without compromising its Melody sensors.

Figure 2 shows the components of Kissinger's deception play. Note that the play omitted the modality and location of the sensors, but it was effective because the Soviets were paranoid about spies in their midst.

Weapons Seizure Deception was likely used in 2005 when the Bush administration disclosed that it worked with other nations to intercept weapons systems bound for Iran, North Korea and Syria [14]. In particular, senior Bush administration officials stated that Pakistan had "helped" track parts of the global nuclear network. By naming Pakistan as the source of the information, the U.S. hid the true modality of its sensor, omitted the sensor location and revealed its range, sensitivity and credibility (Figure 2).

Osama bin Laden The final example, involving the decision of Osama bin Laden and other terrorists to send messages by courier instead of via electronic means, cannot be characterized as deception because the U.S. had no intention of hiding its COMINT capabilities [1]. However, the example shows

how a defender can use a deception play (Figure 2) that exaggerates its sensor capabilities, bluffing an adversary into using another mode of communications that it may have already compromised.

4.3 Deception Principles

Fowler and Nesbitt [6] identify six general principles for effective tactical deception in warfare: (i) deception should reinforce the adversary's expectations; (ii) deception should have realistic timing and duration; (iii) deception should be integrated with operations; (iv) deception should be coordinated with the concealment of true intentions; (v) deception realism should be tailored to the setting; and (vi) deception should be imaginative and creative. These principles were developed for tactical deception in warfare [13], but they are clearly applicable to shielding cyberspace sensors.

Several other deception principles have been developed over time. Three of the more pertinent principles that are part of the U.S. military doctrine are:

- **Magruder's Principle:** It is generally easier to reinforce an adversary's pre-existing belief than to deceive the adversary into changing a belief. The German Army applied this principle in the Wacht am Rhein (Watch on the Rhine) Operation during the winter of 1944. The code name led U.S. forces to believe it was a defensive operation, when in fact it was offensive in nature.

- **Exploiting Human Information Processing:** Two limitations of human information processing can be exploited in deception plays. The first is that humans tend to draw conclusions based on small data sets, although there is no statistical justification for doing so. The second is that humans are often unable to detect small changes in a measured parameter (e.g., size of opposing forces), even though the cumulative change over time can be large.

- **Jones' Dilemma:** Deception generally becomes more difficult as the number of sources that an adversary can use to confirm the real situation increases. However, the greater the number of sources that are manipulated, the greater the chance that the adversary will fall for the deception.

Interested readers are referred to [15] for additional details about these and other deception principles.

4.4 Adversary Information Gathering

A clever adversary is always collecting information about the defender. The information collected by the adversary can be categorized as: (i) known facts, (ii) secrets, (iii) disinformation, and (iv) mysteries [3].

- **Known Facts:** A known fact is information that is publicly available or easily confirmed. In the past, the U.S. intelligence community would

rarely release known facts. Typically, the State Department would serve as a conduit for the release of intelligence, such as Khrushchev's "secret speech" of 1956 that denounced Stalin. In contrast, the intelligence community now routinely releases information for public consumption, such as the World Factbook on the CIA's website. The defender could use known facts to bolster its deception play with elements of truth.

- **Secrets:** A secret is information that is not intended to be known to the adversary. Examples include economic data and sensor attributes. Secret information collected by the adversary invariably contains gaps and ambiguities. It may be beneficial for the defender to design a deception play that leads the adversary to believe that a secret collected by the adversary is disinformation.

- **Disinformation:** Disinformation can be expected to be discarded by the adversary once it is identified as disinformation. Therefore, it is imperative that the deception play be as consistent as possible to convince the adversary of the authenticity of the information.

  Disinformation can distort the adversary's confidence in its intelligence channels [3]. This, in turn, may affect the credibility of other adversary assessments. Paradoxically, the damage usually occurs when disinformation is successfully exposed. For example, in the late 1950s, the Soviets deliberately exaggerated their ballistic missile numbers. The deception was revealed when the first U.S. reconnaissance satellites showed that the Soviets had only deployed a few SS-6 missiles. The discovery of the deception caused U.S. analysts to doubt the credibility of other (most likely true) information they had gathered about Soviet military strength.

- **Mysteries:** A mystery cannot be resolved by any amount of secret information collection or analysis [3]. This can occur, for example, when multiple outcomes are probable, and the number of outcomes cannot be reduced by any means available to the adversary.

5. Cyberspace Sensors

Cyberspace sensors may be used for a variety of purposes, including system monitoring, fault detection and data collection. Our focus is on sensors that detect cyber operations – the attack, defense and exploitation of electronic data, knowledge and communications.

In the context of cyber operations, sensors may be placed in assets belonging to the defender, adversary and/or third parties. The sensors may be located in communications channels and networking devices such as routers, switches and access points. Sensors may also be placed in computing platforms: servers (platforms that provide services); hosts and edge devices (clients and mobile devices); and SCADA devices (e.g., programmable logic controllers and remote terminal units).

It is important to recognize that sensors may be positioned external to computing and communications assets. Examples include human beings located at control centers, and mechanical devices and physical systems that are connected to computing and communications assets. Sensors may also integrate and correlate data received from other embedded sensors.

Several types of sensors can be defined based on the adversary's knowledge and beliefs about the values of the sensor attributes:

- **Open Sensor:** All the attributes of an open sensor are known to the adversary.
- **Covert Sensor:** All the attributes of a covert sensor are not known to the adversary. The very existence of the sensor is hidden from the adversary.
- **Phantom Sensor:** A phantom sensor does not exist. However, the adversary believes that the sensor exists and knows some or all of its attributes. In other words, the adversary believes it to be a non-covert sensor.
- **Obfuscated Sensor:** An obfuscated sensor is a non-covert sensor for which the adversary has incorrect or incomplete information about at least one attribute.

6. Shielding Cyberspace Sensors

This section discusses several tactics, plays and enabling methods for shielding cyberspace sensors.

6.1 Shielding Tactics

A shielding tactic involves a single action on the part of the defender. The tactics are categorized according to the actions and their relation to reality. Active and passive deception techniques are employed to hide and/or reveal certain sensor attributes.

- **Revealing Tactic:** A revealing tactic exposes one or more sensor attributes to the adversary.
- **Masking Tactic:** A masking tactic uses a passive deception technique (e.g., camouflage or concealment) to hide one or more sensor attributes.
- **Misleading Tactic:** A misleading tactic uses an active deception technique (e.g., planting false information, implementing a ruse, display or demonstration, or lying) to falsify one or more sensor attributes.
- **Distraction Tactic:** A distraction tactic distracts or redirects the adversary's activities. This play should not reveal any of the sensor attributes.

6.2 Shielding Plays

Shielding plays implement one or more shielding tactics. A shielding play is categorized according to the sensor attribute values that are believed by the adversary to be true after the play is executed by the defender.

The four plays described below are in conformance with the See-Think-Do methodology.

- **Open Sensor Play:** An open sensor play reveals the correct values of all the sensor attributes to the adversary. Complete knowledge about a sensor serves as a deterrent because the adversary knows that the defender can detect an unfriendly act and may retaliate. Of course, complete knowledge about a sensor enables the adversary to take countermeasures.

- **Covert Sensor Play:** A covert sensor play hides the existence of a sensor, including all its attribute values. Such a sensor is similar to the "gatekeeper" submarine that was secretly positioned near a Soviet port to collect data about Soviet nuclear submarines. A covert sensor has limited use (on its own) because it is often the case that the adversary needs to know that some type of sensor exists to detect an unfriendly act on the part of the adversary.

- **Phantom Sensor Play:** A phantom sensor play is designed to convince the adversary that the defender has a sensor that, in reality, does not exist. A phantom sensor play could implement a misleading tactic that involves the defender being told about the adversary's activities by a third party, but revealing to the adversary that the activities were detected by a sophisticated sensor.

- **Sensor Obfuscation Play:** A sensor obfuscation play releases some (correct or incorrect) information about the sensor to the adversary but hides enough information so that the adversary cannot subvert detection by the sensor. An example involves the defender's sensors detecting Trojans placed by the adversary on several computing assets, some owned by the defender and some owned by third parties. However, the defender confronts the adversary with the Trojans discovered on its assets, but does not mention the Trojans placed on the third party assets. This play shields the sensors on the third party assets by not revealing information about their location and range.

6.3 Enabling Methods

Sensors are shielded by executing plays based on the deception framework and constructs described above. Numerous variations of the plays exist, giving the defender considerable leeway to demonstrate to the adversary that the defender knows about some asset or activity by revealing incorrect or no information about one or more of the sensor attributes.

Two enabling methods, shepherding and distraction, are especially useful in situations involving multiple sensors.

- **Shepherding:** Shepherding involves convincing the adversary and/or other parties to adjust their activities to the advantage of the defender. Shepherding has at least three variants. One is to convince the adversary to shift its activities so that they can be detected by an open sensor. Another is to move a non-covert sensor to where the adversary is conducting activities. A third is to shepherd a third party sensor to where the adversary is conducting activities. A honeynet can be used as a shepherding tool. Note that the defender can use the honeynet to implement an open sensor play on one sensor and other plays on the other sensors.

- **Distraction:** Distraction is designed to progressively divert the adversary's attention from secret sensor attributes. This method can be used to create confusion (possibly panic) inside the adversary's network. Consider a situation where the adversary releases a worm that tunnels into the defender's network. In response, the defender conducts a display (or ruse) that releases the same worm in the adversary's network – intending for the adversary to believe that the worm was erroneously released in its own network. To reinforce this belief, the defender plants information in the media that the adversary's experiments with cyber capabilities infected its own network with a worm.

7. Shielding Play Pitfalls

The efficacy of a shielding play is limited by the amount of time and resources available for its planning and execution, and the adversary's susceptibility to deception [15]. Despite the best efforts of the defender, a shielding play can fail for many reasons. The adversary may not see all the components of the play, may not believe one or more components, be unable to act, or may decide not to act or act in an unforeseen way even if all of the components of the play are believed; also, the adversary may simply discover the deception [15].

The failure or exposure of a shielding play can significantly affect the adversary's operations. For this reason, the defender should understand the risk associated with an action that is based on the assumed success of a shielding play. In general, there are two broad categories of deception failures: the defender does not design or implement the shielding play correctly or the adversary detects the deception.

Even if a shielding play is successful, it is possible for the adversary to compromise the defender's feedback channels [15]. Another problem is that unintended third parties may receive and act on the deceptive information intended for the adversary. The risks associated with these eventualities must be weighed carefully against the perceived benefits of the shielding play.

A shielding play can be discovered by the adversary via direct observation, investigation or indirect observation [16, 17].

- **Direct Observation:** Direct observation involves sensing and recognition. The adversary relies on one or more sensors (e.g., a network port scanner or packet sniffer) to discover the shielding play.

  Any attempt to defeat the adversary's discovery process must consider how, when and where the adversary receives information. The defender must then target the adversary's detection capabilities and/or information gathering processes. For example, the installation of a firewall can prevent the adversary from conducting a port scan. Alternatively, the deployment of a honeypot can compromise the port scanning process by providing incorrect information.

- **Investigation:** Investigation involves the application of analytic processes to the collected evidence rather than direct observation. An investigation helps discover something that existed in the past, or something that exists but cannot be observed directly. Note that an investigation relies on the analysis of evidence; it cannot be used for predictive purposes because evidence of future events does not exist.

  An investigation can be thwarted by compromising the adversary's evidence collection and/or analysis processes. Actions can be taken to alter the available evidence, or to diminish or misdirect the adversary's analytic capabilities. These actions are simplified if the adversary has a bias or predisposition that aligns with the shielding play.

- **Indirect Observation:** Indirect observation involves a third party (human or machine) that has discovered the deception either by direct observation or by investigation. Indirect observation is defeated by compromising the third party's ability to make a direct observation and to conduct an investigation. Alternatively, the defender could target the communication channel between the third party and the adversary.

8. Fireball Express Reprise

The Fireball Express dilemma involves three (initially) covert sensors: the embedded agent, honeynet and Internet sensors. If the U.S. decides that it must respond to the adversary's cyber operation, it must acknowledge that something was detected by one or more of its sensors. Three possibilities (of many) are: (i) open the honeynet sensor; (ii) obscure the honeynet and embedded agent sensors; and (iii) obscure the embedded agent and honeynet sensors, and create a phantom sensor.

The first option involves conducting an open sensor play on the honeynet sensor. The play could involve one or more revealing tactics. One revealing tactic could be the public announcement by the U.S. that it caught the adversary "red-handed" accessing the honeynet, which was installed as a defensive measure to secure the critical infrastructure. This play would reveal the existence of the honeynet and its corresponding sensor attributes to the adversary.

The second option, obscuring the honeynet and embedded agent sensors, involves using a sensor obfuscation play coupled with shepherding. The sensor obfuscation play may be accomplished by employing a revealing tactic and a misleading tactic. The revealing tactic discloses the sensitivity, range and location of the honeynet and the embedded employee. One approach is for U.S. authorities to publicly announce that "anomalous activity" was discovered at the utility and request blue team assistance. The blue team is a shepherded open sensor that assumes the credit for detecting the adversary's activities via the misleading tactic.

The third option, obscuring the embedded agent and honeynet, and creating a phantom sensor, involves an obfuscation play, a phantom sensor play and a distraction method. The obfuscation play uses a revealing tactic that blocks the adversary's entry into the honeynet by implementing strong access controls. The play reveals the sensitivity, location, range and credibility of the embedded agent and honeynet sensors, but it does not reveal their modalities. The adversary is deceived via a distraction tactic and a misleading tactic. The distraction tactic is a brief denial-of-service (DoS) implemented by ARP poisoning the adversary's network. The misleading tactic plants information that indicates the U.S. has placed sensors in the adversary's network. The planted information is designed to make the adversary believe that the DoS attack was a side-effect of the sensor placement. The distraction and misleading tactics are designed to make the adversary believe that a phantom sensor exists in its core network. This phantom sensor could have the effect of deterring the adversary from conducting cyber operations until the sensor is detected.

The Internet sensors are intended to remain covert in the three U.S. response options. Thus, each option corresponds to a covert play conducted on behalf of the Internet sensors. Note that many other combinations of tactics, plays and enabling methods can be used to achieve the same outcome.

9. Conclusions

The global reach of the Internet and the difficulty of detecting and attributing attacks make sensors invaluable in defensive operations. Maintaining the secrecy of key sensors and their attributes is vital for several reasons. Adversaries can bypass or develop countermeasures for known sensors. Secret sensors with exaggerated capabilities can create confusion, even fear, on the part of the adversary.

Deception can be used very effectively to shield cyberspace sensors. The deception-based shielding tactics and plays presented in this paper provide the defender with broad situational awareness and the flexibility to respond to adversary operations. Moreover, the tactics and plays enable the defender to shape the adversary's beliefs about the sensors, helping the defender gain tactical and strategic superiority in cyberspace.

Note that the views expressed in this paper are those of the authors and do not reflect the official policy or position of the U.S. Department of Defense or the U.S. Government.

References

[1] J. Bamford, *The Shadow Factory*, Doubleday, New York, 2008.

[2] J. Bell and B. Whaley, *Cheating and Deception*, Transaction Publishers, New Brunswick, New Jersey, 1991.

[3] B. Berkowitz and A. Goodman, *Strategic Intelligence for American National Security*, Princeton University Press, Princeton, New Jersey, 1989.

[4] G. Bush, Executive Order 13292 – Further Amendment to Executive Order 12958, as Amended, Classified National Security Information, The White House, Washington, DC (www.archives.gov/isoo/policy-documents/eo-12958-amendment.pdf), 2003.

[5] J. Dunnigan and A. Nofi, *Victory and Deceit*, Writers Club Press, San Jose, California, 2001.

[6] C. Fowler and R. Nesbit, Tactical deception in air-land warfare, *Journal of Electronic Defense*, vol. 18(6), pp. 37–79, 1995.

[7] S. Gerwehr and R. Glenn, *Unweaving the Web – Deception and Adaptation in Future Urban Operations*, RAND, Santa Monica, California, 2002.

[8] W. Laqueur, *The Uses and Limits of Intelligence*, Transaction Publishers, New Brunswick, New Jersey, 1993.

[9] D. Patranabis, *Sensors and Transducers*, Prentice-Hall of India, New Delhi, India, 2004.

[10] E. Poteat, The use and abuse of intelligence: An intelligence provider's perspective, *Diplomacy and Statecraft*, vol. 11(2), pp. 1–16, 2000.

[11] J. Richelson, *The US Intelligence Community*, Westview Press, Boulder, Colorado, 1999.

[12] J. Risen and D. Rohde, A hostile land foils the quest for bin Laden, *New York Times*, December 13, 2004.

[13] N. Rowe and H. Rothstein, Two taxonomies of deception for attacks on information systems, *Journal of Information Warfare*, vol. 3(2), pp.27–39, 2004.

[14] D. Sanger, Rice to discuss antiproliferation program, *New York Times*, May 31, 2005.

[15] United States Department of Defense, Military Deception, Joint Publication 3-13.4, Washington, DC, 2006.

[16] J. Yuill, D. Denning and F. Feer, Using deception to hide things from hackers: Processes, principles, and techniques, *Journal of Information Warfare*, vol. 5(3), pp. 26–40, 2006.

[17] J. Yuill, F. Feer and D. Denning, Designing deception operations for computer network defense, *Proceedings of the DoD Cyber Crime Conference* (www.jimyuill.com/research-papers/DoD-Cyber-Crime-deception-process.pdf), 2005.