Electronic Dead Drops

-FirmWarez

Revision 0.2
17 Aug 2014

The rule is there are always exceptions to the rule. In security, it is often claimed that "security through obscurity is not true security". For many applications this proves true, but there are exception to this rule, including one that is still a fundamental component of spy tradecraft, one that is used by many who work in the shadows.

There are numerous examples of obscurity triumphing in security. Numbers stations are classic: in the clear spy transmissions from identifiable locations but because they use a one time pad, they are secure. Or at least secure enough for the intended message. Someone planning a major action involving well-trained armed gentlemen requires truly secure plans and communications. However at the moment of initiation of said activity, the "go" message can be transmitted in the clear, publicly, without any encryption or obscurity. The required attention to security of a message therefore seems to be related inversely to the expected lifetime of the message and the amount of information communicated in the message. Yelling "go" to start a terrorist attack is both of short expected lifetime – now is all that matters – and very short on information. The critical component of that message is the protected by all of the security that went in to planning the action.

Espionage is often viewed as the surreptitious gathering of information. This is only half the story; intelligence involves both the gathering and conveyance of information. It tends to be intrinsically understood that the gathering of intelligence is clandestine; however often times the transmission of information must occur in completely hidden channels.

Another real world application of the exception to the "security through obscurity" mantra is the classic spy tradecraft technique of a dead drop. Basically a dead drop is a secret place used to convey information or materials. A dead drop can be in plain sight, such as a chalk mark on a building or other public item; this was actually used by the Soviet spy Aldrich Ames, and was also shown in the movie "Enemy of the State". They can also be highly obfuscated, such as hollow spikes hammered into the ground, which allow two-way transfer of information and items.

The dead drop is a purely obfuscated method of potentially anonymously transferring information, initiating events, and sharing material. It relies entirely on obfuscation; either by hiding the drop, or by "one time pad" like encoding such as the chalk marks. Dead drops allow for potentially anonymous transfer, in that the parties utilizing the drop need not know anything about one another, however they must take care in accessing the drop to protect anonymity as well as the drop itself.

Dead drops are utilized by many outside of the espionage world. The "hide a key in a fake rock" ploy is a dead drop for the consumer masses; those who trade in black market goods also use the techniques. (http://www.gulf-daily-news.com/NewsDetails.aspx?storyid=368894) Secret hiding places and marks are ancient and can serve operators if approached with care.

The concept has evolved with technology. In 2006 the Russian federal security service accused the British of using wireless gizmos in hollowed rocks as dead drops. See http://news.bbc.co.uk/2/hi/europe/4639758.stm. The concept is very simple, those who know can drop off or leave information via wireless. Using short range transceivers, all this method requires is the knowledge of the drop, and walking close to the fake rock. No direct interaction is involved with the drop, other than proximity; a nice plus in protecting anonymity. Of course the downside to any radio frequency based device is that it produces a signature that can be detected.

Electronic dead drops can be implemented with numerous technologies, from very simply to the extremely complex and layered. This paper is intended to explore some of these options and to spark public discussion among technologists on how to either implement or discover these techniques. Some simple techniques have been deployed by technology enthusiasts in the wild, such as gluing a USB drive to a building or other fixed site; however this paper intends to address more sophisticated possibilities; those that could be utilized by persons needing to exchange electronic messages in a very hidden manner.

Technologies that have been identified as viable dead drops include wireless networking, traditional radios, infrared, power line communications, steganographed images, and RFID. With all of these physical layer technologies, there are possible numerous implementations of communications protocols. Some of these will mimic the "spike in the ground" function of two-way communications, others will function more like the chalk on the mailbox indication. These techniques, like traditional dead drops, typically require access to the intended location and since they rely on obfuscation, are vulnerable to discovery.

In the case of electronic dead drops, "access" can mean physical access to the site, as in the traditional methods, or purely electronic access. If one chose to use steganography as a dead drop communication method, gaining electronic access to a networked kiosk in a mall would be an ideal situation for a one-way dead drop. Being in a very public place allows for an operator to approach the drop without generating suspicion. For lengthy messages, the operator in the know uses a cell phone or other camera equipped device to snap images and apply the appropriate software filter them. Simply instructions can be conveyed in numerous ways – inclusion or exclusion of images in an advertising kiosk; visible but slight changes to a splash screen.

Another method that could require potentially require only electronic access – but could of course be completed with direction physical access to a location, would be to modify the firmware in a wireless access point. By modifying the code the access point could

trigger messages based on certain MAC address or malformed packets. The approaching operator has a WiFi-enabled device with similar functionality modifications. Messages from the access point could be deleted after successful transmission. Triggering on a certain MAC address or malformed packet would minimize the chance of accidental discovery. The MAC address could be entirely arbitrary, the operator's device spoofing the required address for the transaction. As stated this technique could potentially be implemented on a remotely compromised access point, or by planting a specific one. There are numerous methods available for trigger message communication with such a scheme, from low level artifacts like MAC addresses to filtering http get requests. The complexity of a TCP/IP enabled device and it's firmware allow for tremendous options when developing a restricted communications protocol.

The electronic dead drop need not use something as complicated as an access point with an embedded OS running high level protocols. There are much simpler, but equally ubiquitous technological opportunities for sending information to the right person. One of them is nearly everywhere, but doesn't draw attention the same way a networked access point might: infrared. In practically every television remote control, we are surrounded by infrared communications. Typically this is in the form of modulated IR in the tens of KhZ range. Transmission techniques are simple even on the smallest of microcontrollers; reception equally simple due to low cost detectors with built in demodulators.

Like other dead drop methods infrared based systems can be uni- or bi-directional. Very small transceivers could be fabricated, allowing operatives to walk past and send and receive messages. The complexity of such a system would be limited only by the processing capability designed in. Uni-directional dead drops could be incorporated in to television remotes. One can imagine the very Hollywood spy scene of one operative paying a bartender to "press this button on this remote" if someone orders a certain drink. Infrared components are inexpensive and easy to design in. If it comes on an electronic conference badge, odds are it's cheap and easy.

Another method that leans towards the "simpler than an OS in an access point" side is utilizing basic RF systems, such as transceiver modules in the ISM (industrial, scientific, medical) bands. These frequencies are common enough so that traffic may not attract too much undue attention. For lowest probability of intercept such systems would utilize a CDMA type spread spectrum radio.

These techniques could be applied to any wireless communication system, limited primarily by the operator's level of technical skill. 802.15.4, Bluetooth, RFID are all candidates for simple and sophisticated electronic dead drop schemes.

While wireless systems have tremendous advantages, including the fact that operators need not physically interact with the drop, they do suffer from the electronic signature of being intentional radiators of either RF or infrared. Infrared can be detected easily with both military grade night vision and low cost cameras (see http://www.firmwarez.com/?p=1766). Detecting radio frequency signals is a standard part of electronic warfare. A person with average technical skills can scan for most RF transmissions with standard lab

gear such as spectrum analyzers; the author has been told that military grade monitors can detect even the spurious nature of spread spectrum signals.

Hard-wired dead drops further hide the nature of being intentional radiators by limiting the amount of detectable radio frequency produced. While such a system would require direct physical contact of operators, they could be deployed in a manner that such contact would not arouse suspicion.

Texas Instruments, Echelon, and other firms have developed chipsets for communications over standard residential and commercial AC power lines. These can be designed to fit within a standard outlet box, and both obtain power and communicate over the AC power line. The Echelon power line based smart transceivers are utilized in numerous commercial space control systems and can be firmware upgraded over the AC. A sophisticated operator could potentially deploy modified firmware to one of these devices that included dead drop functionality. A promising concept here would be to develop a common AC powered item such as a phone charger, possibly even communicating directly with the phone. When the operator plugs in the charger, the charger and the power line base can exchange messages.

Typically these power line can communicate quite effectively across a single phase within a structure, but their signals are usually greatly attenuated by transformers, typically keeping them captive with a single residential structure or single section of commercial spaces. This provides operators with the opportunity to using a large space with a building as a dead drop, while the critical fixed base unit can be placed in the most secure location, behind heavy appliances or access panels. Additionally the fact that these communications schemes are attenuated by transformers helps in obscuring the transmissions and decreasing the probability of intercept. Power line communications can be very simple messaging type protocols, or more sophisticated like LonWorks. Either is an opportunity for a hidden in plain sight method of transmitting secret information.

The types of electronic dead drops is limited only by the creative and technical skills of the developers. Any electronic method capable of sending a message could be utilized as a dead drop. New technologies, such as no-touch charging systems, will offer new opportunities for surreptitious communications. While this paper focuses on hardware specific solutions, software only dead drops utilizing internet communications could be deployed in similar ways.

While some proponents will faithfully stand by the “security through obscurity is not security” mantra, there are times when obscurity is the protection for transactions. Dead drops have tremendous history in spy tradecraft as well as other activities. Applying various electronic technologies to the concept can allow for further obfuscated message exchange.