37. Abusing Intrusion Detection

37. Abusing Intrusion Detection

On a high level, network intrusion detection can be thought of as wiretapping on a bulk scale. The NSA utilizes various "off-the-shelf" concepts including using various Network Intrusion Detection Systems and Databases, malicious code, and hadoop.

The NSA language is slightly different from the security language present in this class.

- A *selector* in NSA parlance is a piece of information that identifies what you are looking for, like an email address, a phone number, etc.
- A *fingerprint* in NSA parlance is an intrusion detection match
- An *implant* is a malcode or another piece of sabotage

The FISA (Foreign Intelligence Surveillance Act) Amendments Act section 702 states that if you are not a "US person", meaning you are not a US citizen or permanent resident, and you are located outside of the United States, then the NSA can obtain all your information through a US provider. If you are either a US person or are located within the United States, however, you are afforded a lot of protection due to the United States Constitution

The NSA is part of Five Eyes (FVEY), an intelligence alliance comprising of Australia, Canada, New Zealand, the United Kingdom, and the United States. These countries are parties to the multilateral UKUSA agreement, a treaty for joint cooperation in signals intelligence. The primary rule within FVEY is "when in country X, behave according to country X's laws".

The NSA's objective is, for a valid target (that is a non-US person outside of the US), to be able to collect all relevant communications. This, however, requires the capability to collect information on everyone since a valid target could be anyone, meaning that the NSA requires global capabilities. As such, the solution that the NSA employs is to collect all intelligence that they feasibly can on everybody and store it for as long as possible, assuming that at some point in the future they might need to search that information and hopefully find something useful. One issue of utilizing the aforementioned method, however, is that there is now too much information, and sifting through that information to find the relevant details is much more difficult.

Say, for example, that you are an analyst and you are watching an IRC chat between two "anonymous" people, and your task is to identify the two people involved in the conversation; the only information that you do have is that they both visited some article at some specified time. The first thing you might do is to use Signal Intelligence Flow (also known as the Digital Network Intelligence Flow) to develop an online pattern of life for these anonymous users, before using a computer network exploitation to invoke an "exploit by name" attack to take over their computers.

A majority of signals intelligence starts off with wiretaps, and the NSA's preferred system of doing so is called Xkeyscore Deepdive (a large majority, if not all, of which are overseas). These wiretaps are nothing more than scalable network intrusion detection systems (NIDS)! After the NIDS extracts the network information and parses the data packet to extract the metadata, it stores it within a dataframe. However, unlike conventional NIDS, if you want to evade the NSA monitoring, all you have to do is encrypt the data using some form of cryptography. In practice, Xkeyscore is primarily centered around an easy-to-use web interface with a lot of pre-canned search scripts for low-sophistication users along with a large number of pre-made "fingerprints" to identify applications, usages, etc.

Good transport cryptography causes significant problems when the NSA attempts to collect data; however, they are able to utilize some tricks to get around this (though a large majority of these don't work anymore). The wiretaps collect encrypted traffic and pass it off to a black-box elsewhere, usually at some datacenter. The NSA might come back at some point in the future having obtained the cryptographic key and might be able to then convert the ciphertext back into plaintext.