|  |
| --- |
| **The ability to link specific users to specific IP addresses is being lost!**  **Tracking and tracing attack packets to the machine from which they came from in a sophisticated attack is indeed a daunting task.**  **There are possible solutions to the extremely difficult technical and policy problems with this issue.**    **One primary purpose for tracking and tracing attacks is to deter future attacks by punishing or**  **sanctioning the individuals or entities that originated them.**   * **To accomplish this, a direct link must be drawn between the IP address of the machine that originated the attack and the individual or entity that set the attack in motion.**   **However, several Internet trends are making it increasingly difficult to link IP addresses of machines to the entities or individuals who use them**   * **In the early days of the Internet, every connected machine was assigned a *static* (or relatively permanent) IP address.** * **However, the 32-bit address field of the current IP protocol limits the number of possible addresses, and the tremendous growth of the Internet threatens to eventually make IP addresses a scarce resource.**   **Already, organizations consider IP addresses to be a limited resource and are using schemes, such as the *Dynamic Host Configuration Protocol (DHCP)*, to share a pool of IP addresses among their users’ machines.**   * **For example, an ISP will typically assign a *dynamic* IP address to a dial-in user, from a pool of IP addresses owned by the ISP.** * **The dynamic IP address will remain valid until the user’s modem connection to the ISP is terminated.** * **Upon initiating a new dial-in session, the user will most likely be assigned a different dynamic IP address.** * **An attack that is traced to one of an ISP’s dynamically assigned IP addresses can only be linked to an individual through the ISP’s logs and record keeping and is dependent on the ISP’s willingness to collect, preserve, and divulge that information.** * **Many ISPs inform their customers (via “terms of use” agreements) that information about a customer’s use of their service may be made available to law enforcement or other governmental authorities at the ISP’s sole discretion.**   **By and large, ISPs have a strong incentive to cooperate, at least domestically, with law enforcement and governmental authority!**   * **Far more serious erosions in the ability to link an IP address to a particular user or entity are the appearance of “pay as you go” ISPs and the growth of (and ability to anonymously purchase) mobile wireless computing devices.** * **“Pay as you go” ISPs, and in particular prepaid Internet access cards, allow one to purchase Internet access time without a monthly commitment or long-term contract and, unlike the traditional ISP arrangement, require little or nothing in terms of identification.** * **A potential attacker who pays cash (or uses a stolen credit card) can achieve nearly complete anonymity in accessing the Internet.**   **Consider a fast-growing mobile digital technology called Global System for Mobile Communications (GSM), which integrates voice, high-speed data, fax, paging, and messaging**   * **GSM mobile devices incorporate a Subscriber Information Module (SIM) “smart” card, which provides the authorization to use the network.** * **An individual can go into a store, put down cash, and anonymously buy a wireless phone/computing device with a prepaid subscriber agreement (Subscriber Information Module).** * **One of the services available under GSM is the General Packet Radio Service (GPRS). Here is a brief description from the GSM Association’s web site**   **For example, an anonymizer might embed a token in a packet in order to allow for the later identification of the IP address of the user, if the packet was found to be involved in an attack.**   * **The information necessary to link the token to the user’s IP address would retained at the anonymizer site for a limited amount of time.**   **For the first time, GPRS fully enables Mobile Internet functionality by allowing inter-networking between the existing Internet and the new GPRS network.**   * **Any service that is used over the fixed Internet today—File Transfer Protocol (FTP), web browsing, chat, email, telnet—will be as available over the mobile network because of GPRS.** * **In fact, many network operators are considering the opportunity to use GPRS to help become wireless Internet Service Providers in their own right…**   **Because it uses the same protocols, the GPRS network can be viewed as a sub-network of the Internet with GPRS capable mobile phones being viewed as mobile hosts.**   * **This means that each GPRS terminal can potentially have its own IP address and will be addressable as such.** * **The tenuous link between a particular IP address and an individual or organization can be almost entirely obscured by using mobile devices and services (such as a Java-enabled PC/phone) that can be purchased anonymously to access the Internet.**   **I use the term "realm switching" to refer to transferring information from one type of communications technology to another, such as moving packets from a mobile realm (e.g., GPRS) to the traditional Internet**   * **The ability to track, trace, and understand (e.g., correlate the different aspects of) an attack that crosses multiple realms is limited in the extreme.** * **However, the technical ability to track and trace attacks across the Internet to the IP address of origin is still so difficult a task at present that today’s attacker has little motivation to take additional steps, such as realm switching or using prepaid Internet access cards, to achieve further anonymity.**   **As the basic technology to trace an attack to its IP address of origin improves, we would expect attackers to take these additional steps to thwart attempts to discover their identity.** |

|  |
| --- |
|  |