Measurement as a First Class Network Citizen

Paul Barford – University of Wisconsin – Madison

Measurement is essential to the daily operation and security of the Internet. The ability to measure was an explicit and intrinsic component of the original design of the ARPAnet as highlighted by establishment of the Network Measurement Center at UCLA, development of RFC 323 on the formation of the Network Measurement Group in 1972, and publication of the first empirical study, "On the Measured Behavior of the ARPA Network" by Kleinrock and Taylor in 1974. In hindsight, it is clear that the task of measurement in the early Internet was facilitated by the small size and limited capability of the infrastructure, and the fact that the entire infrastructure was controlled by a single group.

Obviously, over the past 30 plus years, things have changed from the perspective of Internet instrumentation and measurement. First, the explosion in size, diversity and complexity of the global network and its systems has made the technical and logistical tasks of instrumentation very difficult and very costly. Second, equipment vendors driven by market forces have developed measurement capability in a direction that enables but perhaps limits network operation. Third, the private and potentially conflicting interest of distributed administrative entities has, for the most part, precluded wide spread data sharing. While these difficulties have been the motivation for innovations in measurement methods by the research community, it can be argued that many of these techniques have been developed due to fundamental limitations in instrumentation capability and/or data availability.

This position paper argues that a next generation secure Internet must consider measurement as a first class network citizen. This means that measurement must be considered in all aspects of design, implementation/deployment and operation. In terms of implementation/deployment the state of the art network measurement includes (but is not limited to):

- Application and performance logging that takes place on end hosts such as web servers and network embedded systems such as web caches,
- SNMP and flow-based traffic logging that takes place on routers and switches for the purpose of network management, operations and accounting,
- Embedded packet capture and packet processing at line rate using systems such as Endace DAG cards and network processors,
- Embedded traffic monitoring and logging on systems that are part of network security infrastructures including firewalls and network intrusion detection/prevention systems (IDS/IPS),
- IGP and EGP routing configuration and update logging.

Standard best practices for network operations include the use of any or all of the aforementioned measurement systems. However, the level and specifics of use of any of these systems varies widely between administrative entities.

There are significant obstacles in designing the next generation secure Internet with comprehensive and effective measurement capability. These include developing methods for

overcoming barriers to data sharing. While research on data anonymization and data transformation have been underway for some time, even if these technological hurdles are overcome, there will remain significant cultural issues that are likely to be difficult to address. Next, comprehensive consideration must be given to the problems of determining the "what, where and how "of the technical aspects of taking measurements sufficient to support the management and security objectives of the next generation network. A good deal can be learned directly from measurement systems of today, however a clean slate design is likely to lead to greatly increased efficiency and effectiveness of measurement systems. Finally, as measurement architectures progress, liaison with equipment manufacturers will be essential to insure that these mechanisms are implemented in the systems that will be deployed in the new network.

Even if the obstacles listed above are overcome, there will still be several risks in developing the measurement component of the next generation secure Internet. It has been shown time and time again that the traffic behavior and use of the Internet (both legitimate and malicious) is extremely dynamic. Thus, the measurement architecture, to the extent possible, must be fluid enough to accommodate change. It is also clear that there will be a cost associated with enhanced measurement capability. While cost will always be a valid consideration, it must not preclude implementation of essential measurement components in the new architecture. Lastly, it is likely that enhanced measurement capabilities will result in new vulnerabilities in a next generation network. Therefore, the architecture in general and the measurement component in particular must be carefully assessed in order to limit the exposure to a wide range of malicious threats.