# Securing the Internet: threats, trends and tussles

Roger P. Karrer

Deutsche Telekom Laboratories, TU Berlin
Ernst-Reuter-Platz 7, D-10587 Berlin, Germany
roger.karrer@telekom.de
Phone: +49 (0)30 8353 58459, Fax: +49 (0)30 8353 58409

The Internet has been designed with the assumption that end systems can be trusted and are willing to cooperate in the Internet. As a result, the end-to-end argument has shaped the Internet architecture for several decades. However, the open paradigm where everybody can send anything to anybody at any time has led to incessant Denial of Service attacks, virus and worm spreads. Estimates of malware damage in 2004 run between 169 and 204 billion dollars, or roughly 281 to 340 dollars per Windows computer worldwide, a sharp rise by 100% compared to 2003. Recently, a study by ETH Zurich estimated that a massive Distributed Denial of Service (DDoS) attack on critical Internet elements for one week could produce an economic damage on an entire national economy of CHF 5.83 billion, or 1.2% of the GDP (from: `www.mi2g.com`).

We start this task with a simple question: is there such a thing as a perfect DDoS attack? Looking at recent trends in DDoS attacks, we notice that DDoS attacks are moving away from brute force attacks towards stealthy attacks. Brute force attacks may be able to deny the service of a target, but they are easy to detect and often counter-measures can be taken to identify and isolate the attacking traffic and thus to mitigate the effects of the attack. Therefore, attacks increasingly use sophistication, such as distributing the attack over an entire botnet [3], create attack traffic that are either low rate, such as Shrew or RoQ attacks [5], or use attack pattern that resemble legitimate traffic [2]. These attacks are hard to identify and thus hard to defend against - yet not impossible. Moreover, RoQ attacks trade off detectability for efficiency, i.e. they are hard to detect but their objective is "'only"' to reduce the service quality, not to entirely deny the service. Therefore, the obvious question is where we are able to come up with an attack scheme that entirely denies a service but has zero detection probability. In this talk, we will lay out the concept of such a new attack and show initial results on the efficiency.

Given this threat potential, the logical next question is how we can defend ourselves against such attacks. Towards this goal, we first take a step back and try to identify the reasons why such deadly attacks can be mounted. We argue that the culprit is a combination of the end-to-end principle and recent advances in network research. The end-to-end principle emphasizes the separation of "'intelligent"' end systems and the "'dumb"' network. As a result, any end system can send traffic from anywhere at any time to any destination at any speed. The advances in network research provide tools to gather information about the network status, including topology, link capacity and available bandwidth, and even provide enhanced feedback about the congestion status (e.g. ECN). These tools allow end systems to debug the network status, but at the same time allow attackers to optimize their stealthiness and their impact.

We derive two implications from the above analysis. First, the current Internet is increasingly hard to defend. In particular, flow-based schemes that try to identify malicious traffic inside the network are becoming inefficient because the difference between attack and legitimate traffic is fading. At the current stage, defenses based on Capabilities [1] seem the most promising solution, because they limit the ability to send data at any time to any destination. Capabilities have been proposed for end systems [3] as well as inside the network [4], and they are promising because they provide incentives for all participants (ISPs, server providers and users). Second, researchers are currently working on a clean Internet design, where a novel control plane is a vital part. Based on the above experiences, the protection of the control plane information is vital for the security of a future Internet. We argue that the tussle between security and end-to-end knowledge must be resolved by giving emphasis on security. However, at the same time, legal bodies are challenged to define the responsibilities of information providing and the value of information. If, unlike in the current Internet, network information is not longer accessible or can no longer be derived from public tools, ISPs could restrain the network information propagation and even sell information. We all are challenged to find the right balance between information privacy, business aspects and security.

## REFERENCES

[1] T. Anderson, T. Roscoe, and D. Wetherall. Preventing internet denial-of-service with capabilities. In *Proceedings of HotNets II*, Boston, Oct. 2003.

[2] M. Guirguis, A. Bestavros, and I. Matta. Exploiting the transients of adaptation for roq attacks on internet resources. In *Proceedings of IEEE ICNP'04*, Berlin, Germany, Oct. 2004.

[3] S. Kandula, D. Katabi, M. Jacob, and A. Berger. Botz-4-sale: surviving organized DDoS attacks that mimic flash crowds. In *Proceedings on NSDI'05*, Boston, MA, May 2005.

[4] R. Karrer and U. Kuehn. Edge-based capabilities: Joint end system and network protection against ddos attacks, 2006. 3rd place German IT Security Award.

[5] A. Kuzmanovic and E. Knightly. TCP-LP: a distributed algorithm for low priority data transfer. In *Proceedings of IEEE INFOCOM'03*, San Francisco, CA, Apr. 2003.