The Dollar Cost of Cloud Security

Yao Chen, Radu Sion
Stony Brook Network Security and Applied Cryptography Lab
{yaochen,sion}@cs.stonybrook.edu

ABSTRACT

Cyber security is not merely about technology, it is also an economic issue. In this project, we explore the dollar cost environmental footprints of security in computing. To this end we derive the composite end-to-end costs for CPU cycles, networking (bit transfer) and storage in various environments. Computing environment types are differentiated according to scales and certain efficiency factors (such as Power Usage Efficiency or CPU utilization). For illustration purposes, we distinguish four different types: Home Users (H), Small Enterprises (S), Mid-size Enterprises (M), Large Enterprises/Clouds (L). We show its ballpark is between 0.58 and 26.02 US picocents (1 picocent $=\$1 \times 10^{-14}$). Then we evaluate per-bit costs for basic cryptographic primitives such as encryption, signatures, cryptographic digests, and cipher operating modes.

1. APPROACHES

We briefly describe the two steps in this project: analyzing the cost of computing, and evaluating the cost of cryptography.

1.1 Cost of Computing

Computing environment types are differentiated according to certain efficiency factors (such as Power Usage Efficiency or CPU utilization). Empirically, the larger a data center, the more efficient it can be run. For illustration purposes, we distinguish four different types:

- **Home Users (H)**. This setting constitutes a baseline for a simple home setup containing several computers. It features a set of peculiarities, including access to residential energy pricing, negligible cooling, rental and management costs.
- **Small Enterprises (S)**. We consider here any infrastructure of up to 1000 servers run in an enterprise. The cost structure features most of the usual suspects, including commercial energy and network pricing, cooling, space leases, staffing etc. Small enterprises however, do not afford custom hardware, efficient power-distribution, and cooling or dedicated buildings, among others. More importantly, small enterprises typically cannot be run at high utilization as they are under the incidence of business cycles and its associated peak loads.
- **Mid-size Enterprises (M)**. We consider here setups of up to 10,000 servers, often run in owned or leased dedicated data centers. Mid-size enterprises have access to better service deals for network service as well as more efficient cooling and power distribution. They are usually not fully global, yet could have several centers across one or two time zones, allowing increased independence from local load cycles as well as the ability to handle daily peaks better by load shifting.
- **Large Enterprises/Clouds (L)**. Clouds and large enterprises run over 10,000 servers, cross multiple time zones, with large data centers distributed across all continents and often in tens to hundreds of countries. Clouds have access to bulk-pricing for network service from large ISPs, often one order of magnitude cheaper than mid-size enterprises. These high speed networks allow global-wide distribution and integration of load from thousands of individual points of load. This flattens the daylight-driven load curve and allows for efficient peak handling and high utilization factors. Cloud providers often ask vendors for custom designed hardware and power supply components. Moreover, these providers run the most efficient infrastructures, and often are at the forefront of innovation.

The cost factors that come into play across all of the above levels can be divided into a set of inter-dependent vectors, including: hardware (servers, networking gear), building (floor space leasing), energy (running hardware and cooling), service (administration, staffing, software maintenance), and network service.

- **Server Hardware**. Hardware costs include servers, racks, power, and cooling equipment etc. We discuss network equipment later.
- **Energy**. Energy in data centers does not only include power, computing and networking hardware but the

entire support infrastructure, including cooling, physical security, and overall facilities.

- **Service**. Evaluating the staffing requirements for data centers is an extremely complex endeavor as it involves components such as software development and management, hardware repair, maintenance of cooling, building, network, and power services
- **Network Hardware**. To allow for analysis of network intensive protocols, we analyzed network transport service costs separately.
- **Green Means Savings** We will show that due to the cost/energy breakdown, designs for cost reduction or energy efficiency most often result in virtually interchangeable components. This is important, because it has the potential to entice profit-driven entities to behave environmentally friendly in the process of cutting costs, no small feat.

1.2 Cost of Cryptography

We will evaluate per-bit costs and energy footprints for basic cryptographic primitives such as encryption, signatures, cryptographic digests, and cipher operating modes. We suspect for example that, by construction, CBC mode is roughly 30-50efficient than CTR mode. This insight can save hundreds of millions, e.g., when deployed in ciphers for Google mail and other cloud computing infrastructures.