February 2013

Trustworthy Computing Next

Key Points

- In 2002, Bill Gates outlined three key tenets that still define trustworthy computing today: security, privacy, and reliability. But the role of computers in everyday life is changing, and each of these aspects must be fundamentally redefined to meet new challenges.
- Security models need to take a more holistic approach that encompasses prevention, detection, containment, and recovery. Privacy governance needs to replace the current notice and consent model with a framework based on use. Reliability models need to supplement the traditional reliance on data replication and redundancy with a new engineering intelligence that focuses on software that detects, isolates, and repairs outages.
- Governments have a special role in advancing trustworthy computing because they have both the power to catalyze markets through incentives and the ability to dictate behavior through regulation. Governments should also work to establish rules for sharing public and private data and for international access of data by government.

BACKGROUND

On January 15, 2002, Bill Gates sent an email to all Microsoft employees announcing Trustworthy Computing, defining its key tenets as security, privacy, and availability (which is now referred to as reliability).

Since 2002, important changes have occurred in these three areas. New threats and cyber warfare have challenged computer security professionals. People are now connected through a host of Internet-enabled applications, creating massive new global data flows that strain the traditional notice and consent model that protects privacy. Reliability must be improved to accommodate the greater dependence on cloud computing, with large-scale systems promising anywhere, anytime access.

The core attributes of trustworthy computing are as important as ever, but this new set of challenges requires innovative solutions, which Microsoft refers to as Trustworthy Computing Next.

- To meet the security challenges of increasingly determined and persistent adversaries, organizations should adopt a holistic security strategy that encompasses prevention, detection, containment, and recovery.
- To adjust to the privacy implications of a data-rich world, organizations need to craft principles that protect privacy while reaping the benefits that only the massive aggregation of computer data (sometimes referred to as big data) can bring.
- Finally, to build the reliability that information and communications technology (ICT) depends on, organizations need to recognize the complexity of evolving ICT systems, and create products and services that can be flexible in times of failure.

MICROSOFT APPROACH

Trustworthy Computing Next addresses the changes to the online world in each of the three aspects of trustworthy computing: security, privacy, and reliability.

- **Security.** Threats can challenge almost any part of an ICT system, making absolute security impossible. This more dangerous threat environment requires a new model of computer security that consists of prevention, detection, containment, and recovery. While these elements are not new, many organizations have not dedicated their efforts to the strategies necessary to ensure that if part of the network is compromised, the adversary is well contained. Security strategies have also not focused on capturing, correlating, and analyzing audit events from across an enterprise to detect anomalies that reveal attacker movement.
- **Privacy.** It is clear that the privacy challenges in a cloud-enabled world cannot be addressed by traditional privacy principles that focus on the collection of data and the notices provided at the time it is collected—a notice and consent privacy model. The use of data serves as a better starting point for defining the obligations related to personal information. A model based on use is better suited for both the organizations that collect data from individuals and others who may use it. This model requires organizations to be transparent, offer and honor appropriate choices, and ensure that they assess and manage the risks to consumers related to the use of their data.
- **Reliability.** With technology embedded in so many aspects of everyday life, reliability must achieve a level not possible today. To bring this about, two fundamental changes must occur. First, companies must leverage the cloud and its big data to create engineering intelligence—the ability to understand both internal and cross-organizational dependencies. For example, simply watching data flows between networks may reveal significant dependencies that were previously not understood.

  Second, organizations need to stop thinking of reliability solely in terms of redundancy and data replication, which are insufficient to ensure high levels of reliability in the cloud. The traditional emphasis placed on preventing failures in software needs to be supplemented by an increased focus on software that detects, isolates, and repairs (or works around) failures associated with composite computing systems.

POLICY CONSIDERATIONS

- **Government's special role in protecting the Internet.** Governments have both the power to catalyze markets through incentives and the ability to dictate behavior through regulation. Governments also play a unique role in responding to online threats from enforcing criminal laws to protecting a nation from military attacks.
- **Establish rules for sharing public and private data.** Because many cyber attacks impact both public and private infrastructure, the need for a public-private partnership is clear even though the rules for sharing critical information are not. Government and industry must work to create effective mechanisms for sharing data that enhance security.
- **Establish rules for international data access by governments.** Governments need to agree upon a new framework for international assistance that goes beyond traditional mutual legal assistance treaties (which say that the country where data sits has jurisdiction over that data). Under a new framework, countries could agree that there should be a formal process for accessing data.

Helpful Resources

Microsoft Trustworthy Computing Next
www.microsoft.com/twcnext