MAJOR INITIATIVES IN CYBERSECURITY:

Public & Private Contributions Towards Increasing Internet Security

Internet security is the part of cybersecurity that, broadly speaking, relates to the security of Internet infrastructure, the devices connected to it, and the technical building blocks from which applications and platforms are built.

By design, the Internet is a distributed system with no central core or point of control. Instead, Internet security is achieved by collaboration where multiple companies, organizations, governments and individuals take action to improve the security and trustworthiness of the Internet, so that it is open, secure and available to all.

This paper intends to illustrate, by means of a handful of examples regarding Internet Infrastructure, that there are great number initiatives that are working, sometimes together and sometimes independently in improving the Internet's security. An approach we call collaborative security.

Internet Society

The Internet Society is a non-profit organization founded in 1992 to provide leadership in Internet related standards, education, and policy. With offices in Washington, D.C., and Geneva, Switzerland, it is dedicated to ensuring the open development, evolution, and use of the Internet for the benefit of people throughout the world. More information is available at: https://www.internetsociety.org.

11710 Plaza America Drive, Suite 400, Reston, VA 20190-5108, USA Rue Vallin 2, CH-1201 Genèva, Switzerland

INTERNET CORE SERVICES

Routing Infrastructure

The routing system that interconnects the Internet's tens of thousands of networks needs a secure foundation in order to improve its reliability. Example projects: working groups at the Internet Engineering Task Force (IETF) that work on BGP and RPKI, US National Institute of Science and Technology (NIST), and international Internet Routing Registries (IRR) are working to add security to existing protocols, define industry and government best practices, and create distributed databases that can be used to verify routing information for the entire Internet.

DNS Infrastructure

DNS translates human-friendly names into Internet addresses. A scalable and trustworthy DNS are required by every Internet user. Example actors: DNS Root Server Operators (root-servers.org), Internet Assigned Numbers Authority (IANA), and software developers like Internet Systems Corporation (ISC) and NLnet Labs are all involved in deploying a more secure DNS (DNSSEC), coordinating operation of all DNS root servers, and ensuring secure management of the DNS hierarchy.

Time Infrastructure

Accurate and synchronized time information is needed both within the Internet's cryptographic foundation and in many business applications, such as equities trading. Example projects: International Association of Electrical and Electronics Engineers (IEEE) 1588 and IETF Network Time Protocol working groups are defining new standardized security mechanisms for time synchronization as well as operational best practices for everyone.

Data Communications Security

Encryption of Internet Communications is a basic building block, ensuring privacy of personal and business data. Maintaining the protocols and selecting appropriate encryption algorithms is mainly handled by the IETF and US NIST, in cooperation with international government agencies and a community of hundreds of experts from academia, the public, and the private sector.

ENTERPRISES, PUBLIC AND PRIVATE ORGANIZATIONS

Corporate and Enterprise Security

Common frameworks for information security management systems and best practices help organizations worldwide to meet agreed-upon standards, analogous to common accounting standards such as GAAP and IFRS. Standards such as International Organization for Standardization (ISO) 27000-series and US NIST's SP800-53 series give organizations of all sizes a head-start in improving business information security.

END USERS AT HOME AND WORK

End User Device Hardware

Malicious software such as viruses and Trojan horses has caused billions of dollars of losses. The Trusted Computing Group (TCG) and Unified Extensible Firmware Interface (UEFI) Forum have developed hardware-based security such as a Trusted Platform Module and Secure Boot Environments to help combat specific types of malware.

Wireless LAN Security

The wide use of wireless LANs worldwide calls for strong security against eavesdropping and intrusions. The IEEE 802 Committee and industry groups such as the Wi-Fi Alliance are continuing to advance the state-of-the-art in protecting wireless LAN communications.

IoT

Internet of Things (IoT) connects a whole world of new devices to the Internet, many out of the reach of normal enterprise security management, creating severe security vulnerabilities in both home and business networks. Example groups working on improving IoT security include Alliance of Internet of Things Innovation (AIOTI), IoT Security Foundation, European Union Agency for Network and Information Security (ENISA), and the GSM Manufacturers Association (GSMA).

WEB SERVICES, INFORMATION, AND ECOMMERCE

Web Services Security and PKI

Most people interact over the Internet via the web, and HTTP is the most commonly used protocol to deliver web services. Adding security to HTTP is a focus of the World-Wide Web Consortium (W3C), and making encrypted and private HTTP easily accessible and trusted are part of the work of the CA/Browser Forum (CAB Forum), IETF's TLS, and HTTP/2 working groups, and the Let's Encrypt service of the Internet Security Research Group.

EMAIL AND MESSAGING

Email (Spam/Viruses/Phishing)

Email is a major vector for cyber-criminals to endanger individuals and organizations with ransomware, stolen credentials, and lost data. Example projects: Messaging, Malware, and Mobile Anti-Abuse Working Group (M3AAWG) and IETF email working groups are refining security standards for email, such as Domain-Keys Identified Mail (DKIM), along with best practices such as Domain-based Message Authentication, Reporting and Conformance (DMARC) to counter threats such as phishing.

IDENTITY

The proliferation of different accounts and passwords creates security and trust problems across the Internet. Identity services help users to carry a single identity with them. Groups such as the Fast Identity Online (FIDO) Alliance and the Open ID Foundation are working to improve security and privacy both for end users and web site operators.

TRACKING OF THREATS

Immediate operational security threats create chaos when InfoSec professionals are working without good information. A consortium of more than 90 organizations and software publishers, coordinated by MERIT in the US, publishes the Common Vulnerabilities and Exploits database that is used across the cybersecurity community as a basis for defining and fighting current threats. Groups such as the Forum of Incident Response and Security Teams (FIRST), US Infraguard, and private companies such as Verizon, Symantec, and Microsoft regularly collect and freely disseminate security information