Digital Agenda: European Commission supports research on Cyber security

Cybercrime is a growing global problem that no company or country can tackle alone. At any given time, an estimated 150 000 viruses and other types of malicious code are circulating across the internet, infecting more than a million people every day. Anti-virus software developer McAfee counts 75 million unique pieces of malicious malware code on its databases, with botnets spewing out spam that account for a third of all the emails sent every day. Bots are one of the most sophisticated and popular types of cybercrime today. They allow hackers to take control of many computers at a time, and turn them into "zombie" computers, which operate as part of a powerful "botnet" to spread viruses, generate spam, and commit other types of online crime and fraud. The worldwide cost of cybercrime is estimated at over €750 billion annually in wasted time, lost business opportunities and the expense of fixing problems.

In addition to developing wider cybersecurity strategies for Europe, the European Commission takes concrete actions to tackle cyber security risks (see
MEMO/11/842
and
MEMO/10/597
), and pools resources with national governments, industry, universities and NGOs, to develop innovative technologies to improve cybersecurity.

For the period 2007-2013, the European Commission has spent about €350 million in cyber security research; from 2013 to 2020, €400 million is earmarked to support key enabling & industrial technologies such as cyber security, privacy and trust technologies, and an additional €450 million is earmarked for 'Secure Societies' research which includes aspects of cybersecurity.

The following EU-funded projects address the big issues facing cybersecurity: cost, speed and long-term security; helping to keep computer users one step ahead of the hackers, Trojans (ty pe of
malware
that masquerade as a legitimate file or helpful program but whose real purpose is, for example, to grant a
hacker
unauthorised access to a computer)
and viruses plaguing the online world today.

Preventing cyber incidents

European experts are working to establish Syssec , a European 'Network of Excellence' (NoE) built on the age-old concept that prevention is better than cure. The NoE is focused on developing solutions for predicting threats and vulnerabilities before they occur, enabling potential victims of cyber-attacks to build defences before threats materialise. The network also identifies roadmaps on research that need to be implemented to reduce threats. The project has set up a 'Virtual centre of excellence' empowering collaborative research within the systems-security research community in Europe and is working on cyber-security education initiatives.

Security by design

Nessos (Network of Excellence on Engineering Secure Future Internet Software Services and Systems) focuses on fostering the design and development of secure software and systems for the 'Future Internet'. The aim is to ensure engineers and developers address security concerns at the very beginning of system analysis and design. The Nessos team creates secure service architectures and secure service design, enabling security assurance, establishing a risk-aware and cost-aware software development cycle, and delivering case studies for future internet application scenarios.

The need for quick software updates to counter emerging risks means there is less time to do testing and verification. The SecureChange project makes it possible to test only the new parts and maintain the security and integrity of the entire system. For example, an analysis conducted by the SecureChange team, spanning five years and six major version updates of a major open source browser, found that only around one third of the software code changed from one version to the next. In addition, a significant number of vulnerabilities were inherited by each new version from its predecessor, a phenomenon also common to other browsers.

In the 'Future Internet', users will move away from today's static services toward mixing and matching components and services depending on availability, quality, and price. The Aniketos project focuses on bringing security and trust to this heterogeneous environment. In such a world, applications are likely to be composed of multiple services from many different providers. Without a specific effort by policymakers and researchers, the end-user could end up having

few ways to guarantee that a particular service or service supplier offers the security they claim. The Aniketos team, which includes major industrial players and research institutes, develops new technology, tools and security services to counter this possibility.

Towards a secure internet of things

The TECOM project has helped make embedded computing systems more secure, by adapting technology originally developed for PCs to run on everything from smart phones to smart electricity meters. This is achieved through 'Trusted Computing' (TC), a well-established technology that uses both software and hardware for verification and implementation of integrity and security in personal computers and is now making the leap into embedded systems. This is considered very important as more embedded systems are used in devices always turned on and always connected to the internet, which thus become increasingly vulnerable to being hacked or infected with viruses and other malware.

Security in Cloud environments

With cloud computing, data is distributed and instantly accessible from anywhere at any time. Cloud infrastructure therefore also needs to be secure and trustworthy just as much as the applications and services that run on it. With the goal of building trustworthy clouds, the Tclouds project is focused on achieving a combination of security, privacy and resilience that can be widely applied across cloud services. It thus helps ensure the continued expansion of cloud infrastructure, resources and services for many years to come.

Cryptic solution

When it comes to securing data, be it in the cloud or on your network server, cryptography plays a major role. Every time you use a credit card, access your bank account online or send a secure e-mail, cryptographic algorithms are running behind the scenes. But as computers become more powerful, network speeds increase and data storage grows, the current methods of protecting information are being challenged. The Ecrypt project and its successor Ecrypt-II address these challenges. A Network of Excellence is bringing together 32 leading research

institutes, universities and companies, to develop improved tools, and to create more robust algorithms for digital signatures. Among the team's main achievements were eight new algorithms with the capacity to outperform AES, the Advanced Encryption Standard developed by Belgian researchers in the 1990s and subsequently adopted by the US government to protect classified information.

Useful links

EU-funded projects on trust and security

Cybersecurity on the Digital Agenda