Provided by:
ICT Results
http://cordis.europa.eu/ictresults

ICT Research

The policy perspective

© NJ – Fotolia

Freedom in Europe:

Securing our technological future

European Commission
Information Society and Media

This brochure has been produced for the Information Society Policy Link (ISPL) by the *ICT Results* editorial service. ISPL is an important part of the Information Society and Media Directorate-General's goal to draw clear lines between policy, policy-making and European research in the field of information and communications technology (ICT).

ISPL publications and other news are available via the website:
http://ec.europa.eu/information_society/activities/policy_link/

ICT Results is an online editorial service established on behalf of the Information Society and Media Directorate-General.

The service's main aim is to:
- raise the visibility of ICT-funded research results
- support projects' access to markets and encourage uptake of innovations
- raise awareness of European ICT programmes and activities

ICT Results website: http://cordis.europa.eu/ictresults
More reports in this series on *ICT Results*:
http://cordis.europa.eu/ictresults/index.cfm?section=news&tpl=publication

© david hughes – Fotolia.com

Justice, freedom and security... the European way

In this report produced for the publication series ICT Research: The Policy Perspective, we look at how information and communication technology (ICT) is vital for our security. It can protect us from threats, deliver fair and consistent justice and underpins our free and progressing society. European ICT research must never cease to find innovative ways to guarantee Europe's mission for stability, freedom, trust and economic development.

Despite the concerns and issues making today's news or last year's reports, Europe has arguably never been a safer and more comfortable place to live.

Governments have set their sights on some of the major concerns of our times, from pollution and climate change to international people smuggling. Even the impact of events that seem impossible to control, such as natural disasters, can be monitored and mitigated thanks to advanced forecasting and emergency planning.

And with technological advances, security services are getting more sophisticated in tackling new forms of crime on and off-line. Criminals are caught and brought to justice and terrorist plots are thwarted across borders.

Yet recent surveys show that EU citizens want the issues of security, justice and freedom to be among the top priorities for robust action by governments and public authorities. We cherish being able to live in comfort and, when all the defences are up and running and we feel safe, perhaps we can afford to worry more about what might happen if the security measures failed.

Water everywhere

Flood, storms and industrial accidents are the most feared disasters in Europe.

92% of Europeans think that centralised EU involvement in crisis management is a good idea.

[Eurobarometer 2009]

Freedom and democracy for the future

It took generations to build our democratic values. Europe must now foster them and carry them into the digital age.

Our freedom and security – and a fair judiciary system – is enshrined in Europe at the very highest level within the **Charter of Fundamental Rights** and subsequently incorporated into law through the **Treaty of Lisbon**. These key documents affirm the rights of every European citizen in the areas of human dignity, freedom, equality, solidarity, citizenship and justice.

Europe works hard to guard the 'four freedoms' – the free movement of people, goods, services and money – which form the basis of the Single Market and provide the bedrock for most EU law. The efforts to improve our security, uphold democracy and freedom and deliver fair justice take place at all levels of the EU and in all spheres of its government and administration – from open collaboration, EU legislation and regulation, awareness-raising activities and numerous cooperative actions including R&D.

In November 2004, the European Council adopted the **Hague Programme** which set objectives to be achieved in the areas of freedom, security and justice to 2010. "The citizens of Europe rightly expect the European Union, while guaranteeing respect for fundamental freedoms and rights, to take a more effective, joint approach to cross-border problems such as illegal migration, trafficking in and smuggling of human beings, terrorism and organised crime, as well as the prevention thereof," the Council stated. The Commission's subsequent **Action Plan** set 10 priority areas accompanied by a range of concrete actions.

It is clear from the Action Plan that in many areas, from tackling terrorism to managing migration, ICT will play an increasingly important role, especially for securely exchanging and protecting information between different agencies across Europe, analysing data and enabling action to be risk-based and intelligence-led.

Powerful technology, dire consequences

ICT is at the heart of almost everything we do – and this pervasiveness could bring about its own downfall if the technology fails in any way. We are now so reliant on ICT that when something goes wrong, everyday activity virtually comes to a standstill. The EU **Directive on the identification and designation of European Critical Infrastructures** specifically mentions the ICT sector as one of Europe's critical infrastructures.

So we have to be sure that systems will not crash or fail. It is crucial that we can trust hardware and software to be robust, resilient and reliable, especially in extreme circumstances such as natural disasters, terrorist attack or hacking. ICT must be trustworthy.

Trustworthiness is just one aspect of the much broader issue of trust. The information society can only succeed and flourish if there is trust – trust in the technology and trust between users. Trust is a concept that lies at the heart of society; it forms communities and enables interactions. Trust effectively facilitates human transactions and economic activities by reducing risks. There is even factual evidence of a significant positive correlation between the level of trust in a society and its level of prosperity and economic competitiveness.

In the past we have relied on physical recognition and face-to-face communication to establish identity and trust. Today, it is vital to understand how the mechanisms of trust and identification can be translated into the digital age.

Certainly citizens must feel safe from the possible risks of electronic commerce and interactivity. Users must be educated on the risks and how to avoid trouble. Meanwhile, the way ICT systems are built, deployed and linked must help to harden systems to the potentially damaging effects of crises or criminals who try to exploit technology for illegal activity.

The central supporting role of ICT in society is the tenet of the **i2010** framework strategy. The i2010 – and its likely follow-up strategy– promotes the contribution of ICT for the economy, society and

"Trustworthy systems and practices have always been part of the essence of European societies. Whether written as legal code, simply practiced as a code of honour, by habit induced through education or based on secure and reliable technology and management, trustworthy systems provide the glue that holds together elements across the entire societal spectrum – needless to say that with the Web coming of age, our systems and practices should keep pace."

Trust in the Information Society: A Report of the Advisory Board RISEPTIS

© Tyler Olson – Fotolia.com

personal quality of life. The initiative seeks to drive forward the transformation of Europe into an information society where its competitive strengths and social leadership are based on ICT and knowledge.

The Commission's **Communication on a Secure Information Society** of May 2006 outlined the principles that have guided the Commission over the past four years in its work to ensure that the ICT systems we so heavily rely on can be fully trusted.

The Commission's strategy is based on dialogue, partnership and empowerment involving all stakeholders – including public administrations, the IT industry, individual users and the **European Network and Information Security Agency** (ENISA) which was set up under the EU's **eEurope** policy to boost internet security. The aim is to develop a coherent approach to network and information security (NIS) issues whilst striking the balance between security (and a need to access information) and privacy – a fundamental right that pervades policy at all levels.

The role of ICT in security, freedom and justice is therefore double-pronged. Firstly, as a tool, it can enhance our security measures – with techniques ranging from image analysis to ensuring the interoperability of police databanks across Europe. But secondly, ICT is in itself a target of attack; it must be heavily protected from malicious intrusions.

The EU has established policies and funds research and other projects that address both of these aspects.

Protecting infrastructure

The **European Programme for Critical Infrastructure Protection** outlined a series of actions that would help Europe identify its vital services and networks and develop ways to protect them from all types of threat. A **Specific Programme for Prevention, Preparedness and Consequence Management of Terrorism and other Security-related risks** (CIPS) forms part of this activity and makes available €140 million between 2007 and 2013 and is part of the wider €745 **Framework Programme for Security and Safeguarding Liberties** (SSL).

Reflecting the importance of the telecommunications and networks infrastructures, the Commission launched in 2009 an ICT-specific policy initiative on **Critical Information Infrastructure Protection** (CIIP), which focuses on prevention, preparedness and awareness and defines a plan for immediate actions to strengthen the security and resilience of CIIs. The actions proposed by the communication are conducted under and in parallel with the **European Programme for Critical Infrastructure Protection** (EPCIP). It also follows recent recommendations from specialist ICT security interest groups of the G8, the UN and the OECD.

Protecting citizens

The **Specific Programme for Prevention of and Fight against Crime**, also part of SSL, seeks to protect citizens and businesses against illegal activity. Here, there is more focus on using ICT as a tool to enhance detection and prevention along with legislation to define legitimate uses of ICT.

The Commission also recognises the absolute requirement for enhanced data protection coupled with stronger privacy protection, especially online. Here legislation goes back to the 1995 **Directive on Data Protection** and the so-called **e-Privacy Directive** in 2002. In 2007, the Commission outlined its support for **privacy-enhancing technologies** to supplement the role of legislation.

Network and information security, a definition

"The ability of a network or an information system to resist […] accidental events or malicious actions that compromise its availability, authenticity, integrity and confidentiality […]".

Legislation and regulation is important, but it must be coupled with technology. Legislation and regulation must go hand in hand with technological solutions. You cannot enforce legislation or expect compliance if there are not technological aids at the disposal of citizens, businesses and security agencies. This is why most infrastructure and information security policies explicitly stress the importance of strategic research.

Research

Security is a priority theme of the **Seventh Framework Programme** (FP7). The objective of the **Security Theme** is to develop the technologies and knowledge for building capabilities needed to ensure the security of citizens from threats such as terrorism, natural disasters and crime, while respecting fundamental human rights including privacy.

Aspects of the Security Theme are complemented in the **ICT Theme**, specifically under the banner of 'Trust and security' in Challenge 1 – Pervasive networks and service infrastructures. Reflecting the complementarity between several strands of European policy, a joint security/ICT call was launched in 2007 for research proposals on the topic, including contingency planning for energy and transport networks, modelling and simulation, intelligent surveillance and ICT support for first responders in crises occurring in critical infrastructures.

The 2009-2010 ICT Work Programme focuses on measures to make future networks more 'trustworthy'. Trust, the work plan states, is earned when ICT systems are "secure, reliable and resilient to attacks and operational failures; guaranteeing quality of service; protecting user data; ensuring privacy and providing usable and trusted tools to support the user in his security management."

But there is also a clear shift to larger-scale demonstrations and the application of security systems in real-world contexts. The **ICT Policy Support Programme** of the **Competitiveness and Innovation Programme** funds pre-competitive research of large demonstrations and implementations of solutions with the aim to prove the commercial viability of products and services. Building on the focus of its related predecessor programme **eTEN**, annual work programmes have highlighted the need for thematic networks to bolster cooperation and collaboration on several issues including privacy protection, radio frequency identification (RFID), biometrics and trusted information infrastructures.

Long-term, visionary research and pilot studies to promote technology uptake are fundamental in Europe's fight to realise the full benefits of the future internet whilst upholding – even enhancing – every citizen's fundamental rights.

© Verisakeet – Fotolia.com

Meeting the challenges

When it comes to Europe's digital agenda there are many factors creating uncertainty, says Viviane Reding, Commissioner for Information Society and Media: "intrusive business practices that use personal data without respecting the users' will or even without informing them; losses of personal data due to inappropriate security measures; malicious activities such as phishing and spyware, to name just a few.

"If this process continues, we may face a crisis of consumers' trust in online services. If citizens have no confidence in the digital economy and refuse to participate, this could undermine all our efforts to make the societal and economic benefits of the information society become a reality.

Trust is a pre-requisite to freedom, to justice, to the success of the information society. But it has to be earned...

Protection from threats

First, citizens and critical European infrastructures – including ICT networks and their telecoms backbone – must be protected. Natural, man-made and malicious incidents threaten us all the time. Research is imperative to ensure that our defences are based on the most innovative and secure technologies possible. Citizens won't trust ICT until they feel safe.

Trustworthy ICT

Technology is pervasive in society, but just how reliable is it? What happens when systems fail or criminals get control? Europe is driving forward research into cutting-edge hardware and software security technologies for networks and services. It is also developing technologies that give users more control of their precious personal data.

Safety online

In many ways surfing has never been so dangerous – it is easy to quickly be out of your depth. Illegal content, identity theft and invasion of privacy are rife on the internet, but Europe affirms that citizens have a right to be secure from harm. More research is needed to find better ways to stay safe whilst giving users more control of their personal information.

More information:

**Charter of Fundamental Rights:
www.europarl.europa.eu/charter/**

**Treaty of Lisbon:
http://www.europarl.europa.eu/charter/default_en.htm**

**Action Plan on Hague Programme:
http://ec.europa.eu/justice_home/news/information_dossiers/the_hague_priorities/**

EPCIP: http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/l33260_en.htm

i2010: http://ec.europa.eu/information_society/eeurope/i2010/index_en.htm

**Strategy for Secure Information Society:
http://ec.europa.eu/information_society/newsroom/cf/itemlongdetail.cfm?item_id=2766**

The European Commission's First Report on the implementation of the Data Protection Directive: http://eur-lex.europa.eu/LexUriServ/site/en/com/2003/com2003_0265en01.pdf

CIPS: http://ec.europa.eu/justice_home/funding/cips/funding_cips_en.htm

Security and Safeguarding Liberties: http://ec.europa.eu/justice_home/funding/intro/funding_security_en.htm

CIIP: http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/index_en.htm

Prevention of and Fight Against Crime: http://ec.europa.eu/justice_home/funding/isec/funding_isec_en.htm

**Data Protection Directive:
http://ec.europa.eu/justice_home/fsj/privacy/**

e-Privacy Directive: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:HTML

FP7: http://cordis.europa.eu/fp7/

ICT PSP: http://ec.europa.eu/information_society/activities/ict_psp/index_en.htm

eTEN: http://ec.europa.eu/information_society/activities/eten/index_en.htm

© PaulPaladin – Fotolia.com

Fighting on multiple fronts

You are under attack! Every day you confront certain risks, maybe from a terrorist plot, more likely from a computer virus. But you rarely experience serious disaster thanks in part to advanced technology. However, threats constantly change, so research must stay ahead of the game – not least because the very ICT we rely on is also on the hit list.

The EU is built on the premise of 'four freedoms' – the free movement of people, goods, services and money – and fundamental human rights.

But freedom is not a given. It can only be truly enjoyed when we are protected from the forces that threaten to take it away. And when disaster strikes, we need to be able to quickly return back to normality, for example by mitigating the impact of natural disasters and delivering fair justice to criminals.

The EU is working at all levels to ensure that security, freedom and justice is in place for all citizens wherever they are.

The Hague Programme sets out the work of the Commission to establish Europe-wide protection of freedom. The programme's objectives are implemented in part through several funding programme that support innovative projects to complement this work. In particular, the current General Programme for Securing and Safeguarding Liberties is driving political, collaborative and operational solutions and improvements to our security, especially in the area of terrorism and cybercrime.

Safety from threats

Europe feels like a safe place to live – but that is only because our defences are working! At a personal level and as an entire community, the threats, from flooding to terrorism, can be quite real. European research is looking at how ICT can help protect us from disaster.

ICT gets special attention from policy-makers. We rely on it, and because it is a critical infrastructure, it needs careful protection.

The i2010 initiative recognises that ICT security is an essential aspect of the information society as poor security will limit the uptake of ICT or even put people and infrastructures at risk. Advanced ICT can both prevent disasters and help rebuild – the role of ICT in safety is therefore one of the three action lines of the ICT and Sustainable Development i2010 flagship, currently under preparation.

Europe is investing significantly in research to find new ways to exploit the power of ICT to protect citizens and business – and the ICT infrastructure itself – from all manner of threats. It is funding research that exploits ICT for fighting crime, including cybercrime, terrorism and improving the collaboration of law enforcement agencies across the EU. At the same time, the future internet must be built on an infrastructure that is robust and reliable and able to withstand malicious attack or software/hardware failure.

Global Monitoring for Environment and Security

Another joint ICT-focused initiative is GMES. It is a joint effort of the European Commission and the European Space Agency to assure the long-term interoperability, availability and reliability of earth observation data which is increasingly used by security operators, particularly for crisis management and planning.

The ICT Work Programme of the Sixth Framework Programme dedicated significant sums to research into the use of ICT in disaster management and mitigation. Projects funded explored ICT applications and developments in scenarios ranging from forest fires to large-scale environmental pollution incidents.

Some of this work continues under the Security theme in FP7. Research in this theme focuses on four security missions: the security of citizens, the security of infrastructures and utilities, intelligent surveillance and border security, and restoring security and safety in case of crisis. FP7 research focuses on new methodologies and technologies to complement the policy and operations projects supported by the Securing and Safeguarding Liberties Programme.

In 2007, the Commission launched a joint call from the Security and ICT themes of FP7. Its objective was to increase the security and dependability of key infrastructures of modern life, such as energy production sites and transmission systems, storage and distribution, information and communication networks, sensitive manufacturing plants, banking and finance, healthcare, and transportation systems.

Thanks to the development of new powerful ICT-based defences, the aim is that we will continue to live in relative comfort and calm.

Eurojust

Set up in 2002, Eurojust helps in the fight against serious crime across the EU. It is made up of senior and experienced judges, prosecutors, or high-ranking police officers – one from each Member State. Eurojust has the power to ask national authorities to undertake an investigation or prosecution. It also helps to coordinate activities between authorities across Europe, sometimes setting up joint investigation teams.

© µDrones

Projects in focus

µDrones
AWARE
MICIE
VIKING
eJustice
CASELEX

European researchers have developed a small robotic drone capable of helping save lives in emergency situations or preventing terrorist attacks in urban areas. Drones, known as unmanned aerial vehicles (UAVs), have proven to be of great value in military operations, but so far, their advantages have not been fully exploited for civilian uses.

The EU-funded **µDrones** project has developed a 50cm helicopter-like drone that is capable of sensing and avoiding objects in its flight path. The new drone can carry out missions autonomously in places with obstacles, such as in an urban area or inside a building. It could be used to patrol sensitive areas to detect intruders, find the survivors of a disaster or detect chemical spills.

"Mobile multi-sensor surveillance systems, able to be deployed quickly to analyse a situation, will boost the efficiency of the security teams," says Christophe Leroux, the project's coordinator. "By combining sensors and robots, we can develop applications to search and warn, and to detect hazardous materials."

The team also developed the software and hardware so the drone can locate its position in the air, navigate autonomously, and respond to unexpected events, such as an obstacle. Mission planning, collision avoidance and trajectory determination have been built into the drone's software and hardware. The software's visual memory map allows it to return home along its previous flight path.

The drone could be used by the emergency services, security patrols and during natural disasters to help rapid response crews.

Natural disasters can also wreak havoc with the communications and transportation infrastructures, making relief work all but impossible. But the work of the **AWARE** project has come up with a solution: a self-deploying sensor network.

Autonomous, unmanned helicopters similar to the µDrone device, form part of the network and act as communications relays. They can drop sensors to the ground to fill in gaps and transmit live aerial footage which, combined with the data from ground sensors and cameras, and be used by rescue or recovery teams.

The AWARE researchers developed the software, middleware and control system for the helicopter, coupled with a ground wireless sensor network with both fixed nodes and nodes carried by vehicles and people. Helicopters can even work in a coordinated fashion to carry heavy loads together as a team. The system could also be used for surveillance and counter- terrorism applications.

Meanwhile initiatives like the **MICIE** project are eager to establish a Critical Infrastructure Warning Information Network (CIWIN). MICIE is to design and implement what it calls its "MICIE alerting system" that identifies, in real time, the level of possible threats induced on a given critical infrastructure (CI) by "undesired" internal or external events. Whenever such events occur, the MICIE alerting system will support the CI operators, providing them with a real-time risk level (for example, green, yellow, red).

Similarly, the **VIKING** project, approved in the FP7 Security/ICT joint call, looks at the security of the ICT control systems in the electric power infrastructure. Keeping these systems secure and resilient to external attacks, as well as to internal operational errors, is thus vital for uninterrupted service. However, this is challenging since the control systems are extremely complex and need to respond in real time. VIKING researchers are looking to develop more secure and robust industrial control systems for this power generation and the grids that carry the power.

Of course, there will always be people attempting to carry out malicious attack, whether in the physical world or through the internet. But Europe is making sure that those who are caught get fair justice. The highly successful **eJustice** project has developed several technologies to make legal procedures more efficient and effective across Europe. Among its many results is a biometric e-ID which is easier to use than the e-signatures currently in place in the electronic exchange of legal information. A software package makes it easier to put legal workflows onto the web and trace the progress of a case from the perspective of legal professionals or their clients. A French data security firm, Mobilegov, is one of the more high-profile outcomes of eJustice.

The **CASELEX** project, funded through the EU's eTEN programme, provides subscribers with up-to-date legal proceedings from across Europe and a wealth of European case law. The aim is to boost the exchange and supply of important cases that will prove decisive and help to make the judicial processes associated with EU law more efficient.

More information

µDrones www.ist-microdrones.org

AWARE http://grvc.us.es/aware

MICIE www.micie.eu

VIKING www.vikingproject.eu

eJustice and MobileGov www.mobilegov.com

CASELEX www.caselex.com

ICT and 'security, freedom, justice' stories on ICT Results: http://cordis.europa.eu/ictresults/ (enter search terms 'security', 'protection', 'critical infrastructure', 'freedom', 'justice')

http://cordis.europa.eu/fp7/ict/

http://cordis.europa.eu/fp7/security/home_en.html

© Yong Hian Lim - Fotolia.com

Trust me, I'm a computer

We tend to have a love-hate relationship with technology: great when it works, hell when it doesn't. So despite the penetration of ICT into almost every aspect of our lives, we still don't always trust it. But European researchers are finding new techniques to keep things running and make networks and services inaccessible to cybercriminals. As networks get more trustworthy, Europe should benefit from rapid expansion of the future internet.

Reliable and trustworthy ICT

ICT underpins Europe's Lisbon strategy for growth and jobs. Indeed, it accounts for 40% of the growth in productivity in the EU. But cybercrime is on the increase and chaos ensues when computers crash – can research find better ways to make ICT more reliable and build up trust?

We cannot afford to miss out on the opportunities offered by next-generation ICT. The 'internet of things', the semantic web and cloud computing are already appearing and evolving all the time. Will we be willing to accept and use these solutions? Only if we can be assured that the systems are dependable and secure, that they will not fail us and that they will keep our privacy intact.

We need to trust that our networks and back-bone infrastructure are secure, that the services we use are reliable. "Hackers, criminals, terrorists and other malevolent entities have shown how easily the Web's weaknesses can be exploited," notes a report by the high-level i2010 group RISEPTIS, that was set up to recommend research priorities in the area of trustworthy ICT.

"This exposure has been facilitated by a lack of user awareness and sensitivity, technologies and infrastructures that were not developed with such threats in mind, and the fact that governance and jurisprudence have not kept up with developments," the report continues.

Europe is uniquely placed, RISEPTIS argues, "to play a leading role in the development of trust and security in the future Information Society, as the latter evolves in terms of new technologies (products or services) and new policies (directives or regulations)."

The development of more reliable, resilient and – ultimately – trustworthy ICT systems is a key research activity of the ICT Work Programme of FP7. Research in this area is focusing on new technologies and methods to make ICT more dependable and trustworthy.

The FP7 ICT Work Programme identifies several key enabling technologies that can make networks and services more secure and therefore more trusted.

Biometric technologies: authenticate people according to one or more of their intrinsic

physiological or behavioural features (e.g. fingerprints, eye features, facial characteristics, voice or gestures). Current research is looking at how to make biometrics more secure (fingerprints can also be 'stolen') whilst the ICT PSP Work Programme envisages a thematic network to promote biometric technologies in a wide variety of commercial and public-sector contexts.

Cryptography: is at the heart of data security, yet is not used widely. The eSignatures Directive attempted to promote wider use of the technology and establish interoperability in eSignatures between EU countries. Whilst the Commission's Action Plan on e-signatures and e-identification seeks to facilitate cross-border public services in the EU, FP7 research is developing next-generation cryptosystems.

Trusted computing: an established technology combining hardware and software to verify the integrity and security of computers. The challenge is to extend the range of trusted computing to networks.

Secure software engineering: provides the methodologies and tools needed to design, implement and test complete and secure software systems and to adapt existing systems as their environment evolves.

Seven projects have so far (end 2009) been funded to further develop and refine these technologies and move them towards wider uptake and commercial application. BEST, a thematic network funded through the ICT PSP, is dedicated to building consensus and fostering collaboration among stakeholders in the biometrics sector.

© Ildogesto - Fotolia.com

Projects in focus

SWEB
SELFMAN
GEMOM
OpenTC

If public authorities can't set an example of trustworthy ICT then what hope is there for anyone else?

Secure services and infrastructure are absolutely essential for e-government services to be accepted and used throughout society. The **SWEB** project has created secure, interoperable and affordable software for supplying cross-border government services over a mobile device. The software is especially useful for countries without an extensive fixed-line infrastructure – such as those in the Western Balkans. "With this software, regional public administrations could skip the step of electronic government and enter directly into the provision of mobile government services," says project coordinator Petra Hoepner.

The prototype software created by SWEB essentially turns a smart phone or other mobile device with computing power into a means of securely transmitting official documents containing private information. The team used a pilot infrastructure made up of servers hosting the SWEB software and services in each municipality, one or more workstations hosting the client application used by the civil servants, and mobile devices or smart phones loaded with the mobile application for the test users.

Authentication was provided through a security token, a digital means of communicating a user's identity. Other security services time stamped the documents.

Trustworthiness is not all about security and privacy. Reliable and robust systems are also essential. One of the problems of high-powered internet applications is that they typically need teams of experts to maintain them, so it is hardly surprising that sometimes they fail. But the **SELFMAN** project has developed technology that lets certain applications and services fix themselves.

"We wanted to make big internet applications easy," says project coordinator Peter Van Roy, "so that all the management problems you normally have are handled by the system itself. It will take the internet to the next level."

Self management is based on four principles: self-configuring, -tuning, -healing and -protecting.

The SELFMAN architecture and components have been used to build some impressive applications. These include a prize-winning distributed Wikipedia that can handle far more queries than the current version, a commercially successful media streaming service, and a graphics program that lets multiple users collaborate on a design.

The FP7 **GEMOM** project is also looking at fault detection and repair in networks. The premise of its research is that the notion of a 'fault' includes the loss of a connection, low bandwidth or compromised security. The project team hopes to build and deploy a prototype of a messaging platform that demonstrates its evolutionary, self-organising and self-healing properties whilst remaining secure.

Herbert Petautschnig, a researcher at Austrian technology group Technikon, thinks trusted computing (TC) technology could dramatically reduce threats from hackers, viruses and spyware that today frequently cripple the online world. Trusted computing technology combines hardware and software security measures to ensure that only verified machines can interact and only legitimate software can run.

The **OpenTC** project developed several proof-of-concept applications for the technology. In one, called private electronic transaction (PET), the team showed how it can verify and secure online transactions, such as accessing a bank account. In another, they showed how the technology can provide secure remote access to corporate networks, both keeping company information safe on an employee's home PC and ensuring that the employee's personal information, photos and games are not visible to their employer.

The ability of TC technology to keep data and processes safely isolated from each other can be extended to enable virtual data centres. As demonstrated by IBM, TC software could be used by data centre operators to provide virtualised resources to different clients while sharing the underlying physical infrastructure, thereby ensuring different companies' data remain separate and secure. The project has also released openSUSE, a TC-ready version of the Linux operating system.

Output from OpenTC is being exploited and transferred in several related projects. TECOM, for example, aims to put TC solutions into smart phones and mobile computing applications. It is also being promoted within the PrivacyOS ICT PSP network.

More information

SWEB http://www.sweb-project.org/

SELFMAN http://www.ist-selfman.org/

GEMOM http://www.gemom.eu/

OpenTC http://www.opentc.net/

ICT and 'security, freedom, justice' stories on ICT Results: http://cordis.europa.eu/ictresults/ (enter search terms 'security', 'protection', 'critical infrastructure', 'freedom', 'justice')

http://cordis.europa.eu/fp7/ict/

http://cordis.europa.eu/fp7/ict/security/fp7_en.html

© Onidji – Fotolia.com

Combating crime in cyberspace

Legislation in the EU is tough on cybercrime, but people and businesses are not careful enough with their personal data, making it easy for criminals to steal their identity. Europe is combining legislation, cooperation and research to give us holistic protection online.

The web is fully integrated into our lives. We use it to get directions to an appointment, look up train times, send messages to family and friends and order the weekly shopping. But is it safe? How far are you from a criminal's clutches?

The EU is committed to fighting crime on the internet. Cybercrime includes attacks on ICT infrastructure and services, for example hacking, denial of service threats and identity theft. It also includes more traditional criminal activities that have merely 'moved' on to the web, such as child pornography.

Along with its efforts to protect critical infrastructures and promote new ICT that is reliable, secure and trusted, the EU is investing significant effort into fighting crime – both criminal acts against ICT services and infrastructure (see previous chapter) and criminals using ICT for their real-world operations.

The 2001 European Convention on Cybercrime entered into force in 2004. This document, also signed by non-EU states, contains common definitions of different types of cybercrime and lays the foundation for judicial cooperation between signatory states. The Commission also represents the interests of the EU on the G8 Lyon Group, an expert group that assesses existing international agreements and mechanisms and makes recommendations on how to fight organised crime, including high-tech crime.

Safe on the internet

The web is rapidly becoming our primary source of information, education and communication. But cyberspace can be a scary place; people may suddenly find themselves faced with illegal content or the victim of a virus or an online scam. It takes technology to help people navigate safely in the virtual world.

European anti-cybercrime policy is presented in the 2007 Commission Communication 'Towards a general strategy on the fight against cybercrime' which highlights the fight against child sexual abuse material on the internet, actions to counter massive attacks against information systems and combating identity fraud as three priority areas.

The Commission also actively develops new anti-cybercrime initiatives, especially by promoting cooperation between Member States to close legal loopholes. Specific projects to drive innovation and foster cooperation are funded though the Specific Programme for Prevention of and Fight against Crime which is part of the Securing and Safeguarding Liberties Programme.

The Safer Internet Programme and its predecessors focus specifically on the issue of illegal content and child pornography on the web. Past projects were fundamental in establishing hotlines and monitoring centres in each Member State. The programme has also funded projects to develop systems for labelling content and providing guidance on the risks of the internet and child protection. For example, the **SIP-BENCH** project has thoroughly evaluated the effectiveness of about 30 web-filtering applications.

Data protection – the business perspective

- 91% of organisations think that data protection is a "necessary requirement".
- 63% say that improvements are still needed.

[Eurobarometer 2008]

A private presence in public

The issues of data protection and privacy take high priority under the 'trusted networks and security' objective in the FP7 ICT Work Programme.

"Do you want the internet to turn into a jungle?" Commissioner Reding asked in April 2009. "This could happen, you know, if we can't control the use of our personal information online. Now, privacy is a particular value for us Europeans; a value reflected in European laws for many years. However, in spite of the many advantages of technological development, there is an undeniable risk that privacy is being lost to the brave new world of intrusive technologies. On the global information highways, personal information is increasingly becoming 'the new currency'".

The EU passed legislation as early as 1995 on how personal data could be processed and exchanged in Europe (Directive 95/46/EC). This legislation is reinforced for digital data through the so-called e-Privacy Directive (Directive 2002/58/EC). But legislation must be supported with technology, and more work is needed to enhance privacy protection and stimulate its uptake.

People often talk about the balance between security (which may require law enforcement and crime prevention teams having access to information) and privacy (which respects individuals and lets them control what they disclose to whom). But this is not a 'zero sum' relationship. More security does not imply less privacy, nor vice versa. Research into ICT trust and security addresses the two issues in parallel; the aim is to improve security and strengthen privacy in tandem.

The Commission stated its support for privacy enhancing technologies (PETs) in a communication in 2007. "The Commission expects that wider use of PETs would improve the protection of privacy as well as help fulfil the data protection rules... PETs should be developed as a tool to ensure that the law is respected and not breached."

Significant research in FP6 has led to major developments in data protection, online privacy and security of e-identities. This work is being built upon in FP7, focusing particularly on user-centric models of e-ID management and further developments in other privacy enhancing technologies.

The great success of FP6 research means that some technologies are ready for commercial development and widespread uptake. The European Privacy Open Space (PrivacyOS) network, funded through the ICT PSP, brings together a wide range of stakeholders to foster the development and deployment of privacy infrastructures and technologies for Europe, including e-ID cards, encryption and privacy seals. The **STORK** initiative, meanwhile marks a major step towards an interoperable and trustworthy ID management platform in Europe.

The STORK ICT PSP project expects to establish a European e-ID Interoperability Platform that will allow citizens to establish new 'e-relations' across borders, just by presenting their national e-ID. The platform is being piloted in five cross-border e-government services.

Are citizens worried about data protection on the web?

- 64% "concerned or very concerned"
- 48% "data adequately protected"
- 77% "only limited awareness"

[Eurobarometer 2008]

Projects in focus

I-Dash
FIVES
PRIME
PrimeLife
SWAMI
AWISSENET
TAS3

Police forces worldwide are struggling to crack down on the massive rise in illegal child abuse videos over the past five years. The **I-Dash** project, funded through the Sfaer Internet Programme, aims to develop new tools that will let enforcement officers process video material (potentially) containing child sexual abuse and coordinate investigations at a European level. The project involves some of the leading European centres in video processing technology, but is also working closely with end-user partners who will help to distribute the new tools to other agencies across Europe.

The **FIVES** project, meanwhile, is developing tools that can speed up the process of investigating the terabytes of data often stored on equipment seized in investigations. File and fragment matching technologies, and cutting-edge image comparison software, will help to sort items into known illegal content and highlight potentially new illegal content.

The **PRIME** project, meanwhile, has developed a comprehensive identity management toolkit that could stop people leaving a trail of personal information across the web that criminals could steal for illegal purposes. In 2008, the PRIME technology was given a prestigious 'Best Privacy Technology' award by the International Association for Privacy Professionals (IAPP).

Two basic rules govern how people can better protect themselves online, according to specialists. First, we need to "separate contexts" so that observers cannot accumulate sensitive data – basically, by making it much harder for cyber-spies to join the online dots of our lives. Second, and crucially, we have to really keep track of what we do disclose.

These rules form the basis of the concepts and prototypes developed within the PRIME project. "Our main aim is for people to gain autonomy over their personal data, so they can make informed decisions on what information they provide online," says project partner Marit Hansen of Germany's Independent Centre for Privacy Protection.

Like a good poker player who never fully reveals his hand, good identity management (IDM) means choosing and developing appropriate partial identities. For example, OnionCoffee is a PRIME software module written in Java to help end-users exchange information anonymously over the internet.

The EU-funded project has put together a toolbox, console (interface for managing identity online) and middleware (software to glue components together) to help individuals and organisations wrest control of their online identities. The tools PRIME developed marry the need for accountability (i.e. proving you are 18 to enter certain websites) with the need for anonymity.

A key component is the use of so-called "private credentials" derived from certificates issued by, say, professional ID providers, such as online payment operators, on different pseudonyms for the same person.

Our privacy would also be better protected if organisations were better at looking after and processing our data more responsible. "Sticky policies" can also be written into IDM applications so that the policy literally travels on the back of the data being transferred. This means, if data is passed on (legally) to third parties, the policy stays with the data, thus protecting the source's privacy (i.e. that means you and I).

Another web-based system developed by PRIME also helps us keep track of what we have already put out in cyberspace. The 'Data Track' tool in PRIME's console works like the web-history in your browser, monitoring the 'what', 'to whom' and 'when' of online transactions.

Output from the PRIME project forms one of two alternative systems for user-centric e-ID (the other is owned by Microsoft). The PRIME system is now being applied in several other projects including **PrimeLife** which is applying PRIME's technologies for web mail and social networking. It wants to show how people can avoid leaving a cyber-trail of personal data.

The **SWAMI** project has looked into the privacy issues related to ambient intelligence (AmI) where our surroundings detect our presence and exchange data. They have found that while most AmI scenarios paint the promise of the future in sunny colours, there is a dark side to AmI. The researchers came up with several dark scenarios. They show how malicious hacking could cause accidents, lead to intellectual property theft or the loss of personal information.

According to project information coordinator David Wright, the darkest scenario of all is the threat to our personal space. "The most disturbing aspects of this new technology are already around us today, in the steady erosion of personal privacy," he says. "Because of threats to our society, most people are willing to compromise on their personal privacy in order to gain greater security. Yet – and this must be a serious concern – is our security actually better than before we gave up this privacy?"

Privacy enhancing technology can be built into fourth-generation mobile devices, to alert the user to any data-privacy risks present within specific surroundings. The FP7 project **AWISSENET** is developing more resilient and secure AmI networks. Among its aims are the development of more secure routing protocols and intrusion detection and recovery systems.

Architectures are certainly crucial for trusted services. The large FP7 **TAS3** integrated project will develop and implement an architecture with trusted services to manage and process distributed personal information. This architecture will be dependable and robust but at the same time also cost-effective and reliable. The personal information that will be processed and managed can consist of any type of information that is owned by or refers to people.

The TAS3 architecture will be tested in an enterprise human resource management system and in the healthcare sector where it will form the backbone of a treatment planning system.

More information

I-Dash http://www.i-dash.eu/

FIVES http://fives.kau.se/

PRIME https://www.prime-project.eu/

PRIMELIFE http://www.primelife.eu/

AWISSENET http://www.awissenet.eu

TAS3 http://www.tas3.eu/

ICT and 'security, freedom, justice' stories on ICT Results: http://cordis.europa.eu/ictresults/ (enter search terms 'security', 'protection', 'critical infrastructure', 'freedom', 'justice')

http://cordis.europa.eu/fp7/ict/

http://cordis.europa.eu/fp7/ict/security/fp7_en.html

What's inside?

Content for this publication was provided by the *ICT Results* editorial service, working to showcase breakthrough ICT research in Europe. It is part of a series of domain surveys drawn together from articles featuring EU-funded ICT research.

ICT Results

http://cordis.europa.eu/ictresults

European Commission contact:

The ICT Information Desk Office
BU25 02/160
B-1049 Brussels, Belgium
Fax: +32 2 296 83 88

Information Society and Media: Linking European Policies

Further information:

FP7 ICT Work Programme
http://cordis.europa.eu/fp7/ict/

Information Society Policy Link initiative:
http://ec.europa.eu/information_society/activities/policy_link

European Commission
Information Society and Media