Who is moving forward?

The forward coordination action receives funding from the European Community's Seventh Framework Programme (FP7/2007-2013) under grant agreement no 216331. The project is led by a consortium of universities and research centers, consisting of the following partners:

Vrije Universiteit Amsterdam. The Vrije Universiteit (established 1880) is a private University with over 15,000 students in 12 faculties. The Computer Science Department consists of about 50 faculty members, tens of postdocs and over 40 Ph.D. students.

FORTH-ICS. The Foundation for Research and Technology - Hellas (FORTH) is the largest Greek state R&D center. The Institute of Computer Science (ICS) is staffed by approximately: 25 Ph.D's, 70 engineers, and many research assistants and trainees.

Chalmers University of Technology. Chalmers was founded in 1829. More than 10,000 people work and study in the university. Expertise in the Department of Computer Science and Engineering (CSE) ranges from mathematical logic to applied industrial work.

IPP BAS. IPP-BAS has a leading position among the scientific institutions in Bulgaria in the field of Computer Science. The staff of IPP-BAS consists of 108 people and the research staff includes 62 people, working in 7 departments.

Institut Eurécom. Institut Eurécom (founded 1992) is a non-profit research and teaching institute. The Corporate Communications department is staffed by six professors and assistant professors, two research engineers, and a dozen junior researchers.

Technical University Vienna. TU Wien is the largest technical university in Austria and among the leading technical institutes in Europe. The Secure Systems Lab (project coordinator of forward) is composed of 2 faculty members, 5 PhD students, and nine Master's students.

forward

http://www.ict-forward.eu/

forward IS A COORDINATION ACTION THAT AIMS AT PROMOTING COLLABORATION AND PARTNERSHIP BETWEEN RESEARCHERS FROM ACADEMIA AND INDUSTRY INVOLVED IN THE PROTECTION OF ICT INFRASTRUCTURES AGAINST CYBER THREATS SUCH AS MALICIOUS CODE (VIRUSES, BOTNETS, SPYWARE), SPAM AND PHISHING.

Preparing for future threats

History has shown that the security research community is ill-prepared to deal with new types of threats and nuisances on the Internet. Regardless of the nature of the threat (spam, worms, phishing, denial of service), it takes time for experts in the field to come together, study the problem domain, form alliances, obtain funding, and finally pit their wits against those of the attackers. It takes even longer before practical solutions are developed.

While predicting the future is difficult, extrapolating current technological trends and reasoning about potential risks is hardly crystal ball research. A well-known example is RFID. An RFID tag is a small, extremely low-cost chip that can be used for purposes like identification and minimal processing. By adding RFID tags to everything, from pets to products, industry aims to use RFID technology to create the “Internet of Things”.

However, researchers have shown that tags can be used to propagate malware, which in turn has led to a concerned industry scrutinising security issues in RFID, forming alliances with universities, and each other. All this happened before hackers were able to

The forward way to go

Rather than “yet another project to deal with yet another threat,” forward will identify, network, and coordinate research efforts to deal with future threats in general. *Before* they occur.

At a glance

- Duration: Jan 2008-Dec 2009
- Total cost: 889,950€
- EC Contribution: 889,950€
- FP7 Info: ICT Work Programme 2007-08, Objective 1.4
- Coordinator: Vienna University of Technology
- Contact:

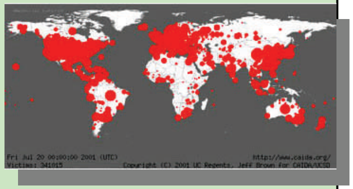
Prof. Christopher Kruegel
Treitlstrasse 183-1
1040 Vienna, Austria
email: chris@auto.tuwien.ac.at

How to move forward?

The need for a project like **forward** is not only clear from the research community's past track record in dealing with new threats (see also: ”where have the worms gone?”). It is also urgent, because security research in Europe is fragmented, consisting of modest-sized groups scattered around the continent. Moreover ICT is a complex field that involves and impacts many domains and pose direct threats to privacy of citizens, critical infrastructure (power, financial institutions, the transport system) and many other aspects. All of the above have already been targeted by internet attacks.

Where have the worms gone?

Code Red, NIMDA, Slammer, Blaster: the big worms of the first years of the millennium swept across an unsuspecting planet in hours - sometimes minutes - causing millions of Euros of damage. As a consequence, fast spreading flash worms were all the rage among security experts and millions of Euros were spent on projects to counter them. Unfortunately, by the time practical counter measures for flash worms were developed, they had all but disappeared. Instead, hackers forced security researchers to worry about stealth worms, botnets, phishing sites, attacks on mobile phones, and whatever new threats emerged in recent years.


Fri Jul 20 00:00:00 2001 (UTC)
Victims: 341015
http://www.caida.org/
Copyright (C) 2001 UC Regents. Jeff Brown for CAIDA/UCSD

Each time there is a new threat, industry and the research community alike scramble to deal with it. Alliances are formed, research grants applied for, projects started, prototype solutions developed, refined, discarded. And all too often, the response is too late.

What is needed is more **coordination**. What trends in technology are likely to lead to new types of attack? What is the nature of such attacks? What would be needed to address the problems? What groups are active in a particular field and how can we bring them together? This is why we need **forward**.

Objectives

Convinced of the need for the project, we now list the ways in which we want to achieve the project goals. Within **forward** we will:

- establish focused Working Groups to perform in-depth analysis of specific threats
- set up a community platform to enable continuous review of the threat landscape
- build a community by way of face-to-face workshops involving major players in the relevant fields
- compile threat scenarios to outline roadmaps of future research

Working Groups

The first major activity in the **forward** project was to organise a workshop with many experts in the field. The workshop took place in Göteborg in April 2008. The talks and discussions during the workshop have led to the establishment of the following three Working Groups.

WG1: Smart Environments

Mobile phones, RFID, and other systems with many mobile, networked devices present new threats with a huge potential impact. Because of their nature, the security measures must change. For instance, they are limited by power concerns, and physical presence in hostile environments. On the other hand, they may benefit from exchanging information with other devices. Similarly, smart environments in homes, trains and cars (car control and vehicular networks), etc. present new threats and new opportunities. WG1 will study security in such environments.

WG2: Malware and Fraud

Online fraud, phishing, scams, credit card abuse, and other fraudulent activities have been the scourge of the Internet for several years now. Malware can be loosely defined as all software that is installed on a machine without the user's consent. In this Working Group we will consider new developments in malware and the ways in which it evades detection and analysis, as well as the underground economy and the movement towards criminal profit.

WG3: Critical Systems

The final Working Group will look at threats that in the future could impact our critical infrastructure, such as power, transport, water, financial institutions, etc. Even today, these are occasionally targeted by attackers. However, as their ICT systems are increasingly interlinked, their vulnerability grows and so does the probability of so-called knock-on effects or chain reactions.