Internet connections for private users are becoming cheaper and faster. With such connections for the private home or apartment, the Internet has more to offer than web surfing, e-mailing, news groups or exchange of MP3 files.

E-services (electronic services) are the next frontier. An e-service can be any kind of software that offers a service to its end users by using the Internet. It relies on a permanent Internet connection and uses network-enabled smart devices in the home as its endpoints and points of user interaction. One e-service scenario allows e.g. home owners or tenants to remotely control their house or apartment by checking the alarm system or peeking into the refrigerator. More advanced services offer data communication between devices in the house and a service provider company. An e-service could e.g. be used by a health service company to remotely check on the network-enabled medical equipment of patients at home. An energy company could use an e-service for automated meter reading.

Our areas of interest are the security aspects of such an e-service enabled system in terms of confidentiality, integrity and availability. We deal with the following three projects:

1. Secure electronic software delivery. It ensures that e-service software is uploaded to the home in a controlled and authorised way.
2. Secure execution environment. It ensures that e-services do not eaves-drop on or starve each other, that they access only network nodes that they are allowed to access.
3. Authenticated user permissions. They ensure that users use the system according to pre-defined policies that are specific to each household.

The infrastructure we are exploring uses a residential gateway (c.f. figure) to connect IP-compatible home devices to the Internet. The gateway is basically a down-scaled firewall computer with two network cards and the only device within the home that is directly connected to the outside; i.e. all traffic to and from devices in the house has to go through the gateway.

The gateway is also used as a repository for all the e-service software in the house; all down- or uploads must be managed and controlled by the gateway. Whenever a connected device on the home network is turned on, it queries the residential gateway for new software destined for this device. Thus, for a successful update of home network nodes, only the residential gateway must be switched on at all times; update of other network nodes is done when the node asks for it.

The gateway ensures simple security policies by implementing a packet filter. But it is also used for more advanced security features that are controlled by a policy engine – our targeted area of research. The policy engine has the important task of a resource manager. It must ensure that no e-service starves another e-service by using too much RAM, disk space or bandwidth. In addition, it must enforce access control policies on the application level (access between different e-service applications) and user level (access to a service by a user). All these tasks must execute without impairing the platform they run on. In the case of the residential gateway, it must even be always turned on and always available, allowing only very little down time. Having a stable and reliable policy engine is a must for the gateway.

In our three research projects, we are specifically dealing with technologies for secure multicast, Java Virtual Machine with its sandbox, resource management and policy engines.