MyNet: a Platform for Secure P2P Personal and Social Networking Services

D. N. Kalofonos, Z. Antoniou, F. D. Reynolds, M. Van-Kleek,
J. Strauss, and P. Wisner
Nokia and Massachusetts Institute of Technology

PerCom 2008

Presented by: Matthew Tan Creti

PURDUE UNIVERSITY

MyNet

- MyNet - a platform for secure P2P personal and social networking services
- Built on top of UIA that provides
  - Ubiquitous connectivity with network overlays
  - Device group management enables non-expert users to easily organize and share their resources within their social neighborhood
- Problem: Today managing pervasive access to personal devices, content, and services is too complex for non-expert users

Built on Top of UIA

- UIA communication platform
  - Permanent location independent device identifiers bound to personal names
  - Ubiquitous connectivity
  - Distributed device group management
- Devices and users
  - A device can be uniquely identified by its EID
  - Devices with multiple-user accounts have a unique EID to identify each device/user pair
  - Users (and groups) are identified as a set of EIDs

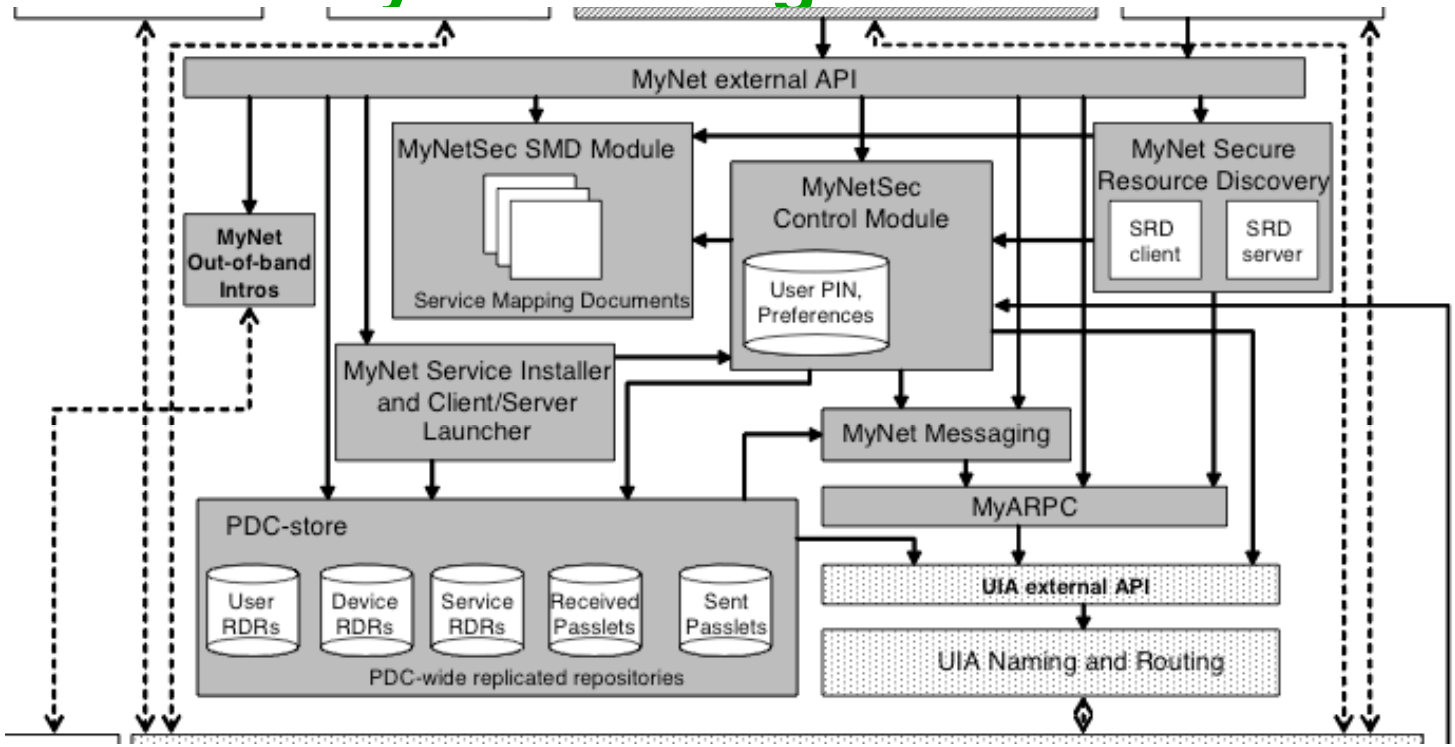
Built on Top of UIA (cont.)

- Imprinting
  - A new device becomes a MyNet device though the process of *Imprinting* the owner's identity, profile, and secret (e.g. PIN)
  - The owner secret protects against misuse of critical tasks
- Personal Device Clusters (PDC)
  - An imprinted device can be merged with other devices to create a Personal Device Cluster
  - For two devices to merge, owner authentication is required on both devices
- Social Contacts
  - A social contact is established between two users though the *Introduction* process
  - Through UIA routing information, SIDs, and EIDs are exchanged

Basic Design Concepts

- Services and Content
  - Each device can run one or more user-services (a user perceived service)
  - Each user-service may be one or more distributed elementary services
- Groups
  - A user can create groups of users or devices
  - A user based group can define the recipient of access control privileges
  - A device based group can define the target of access privileges
  - There are built in groups such as “world”, “my direct contacts”, and “my extended contacts”

System Design: Middleware



- Adding devices and contacts is done by an *out-of-band introductions* module (e.g. Near Field Communication (NFC) or Bonjour)
- During introduction discovery records including overlay routing information are exchanged, bootstrapping the MyNet resource discovery
- MyNet-"aware" applications can use a remote procedure call layer (RPC) called MyARPC to exchange messages
- A persistent messaging service guarantees a one-way message will be delivered to a destination EID whenever a device comes online

System Design: PDC-Wide State Replication

- MyNet applications and services can share state across instances running on various devices in a user's PDC using the PDC-store
- Currently PDC-store is used for Resource Discovery Records (RDR) and Passlets
- Optimistic replication provides eventual delivery
- Conflicts in state are reconciled using timestamps for now

Secure P2P Resource Discovery

- Resource Discovery Records (RDR) correspond to devices, services, content, and contacts (users)
- The *Secure Resource Discovery* (SRD) module creates an RDR for a device, each new user a device is introduced to, and each MyNet-"aware" and MyNet-"enabled" service
- Discovery process
  1. Resource registration: New RDRs are created when a device is imprinted, a device or contact is introduced, or a service or content is installed using the *Service Installer and Launcher*
  2. User sets discovery permissions: MyNetBook is used to crate a Resource Discovery Passlet that specifies which of the user's RDR may be revealed to a specific user
  3. Resource discovery/browsing: The Secure Resource Discovery client (SRD-client) sends a MyARPC request, and the SRD-server of a device in the target PDC returns the authorized RDR
  4. Service launching: When a user selects a service RDR, the corresponding client-side application is launched

Security: Passlets

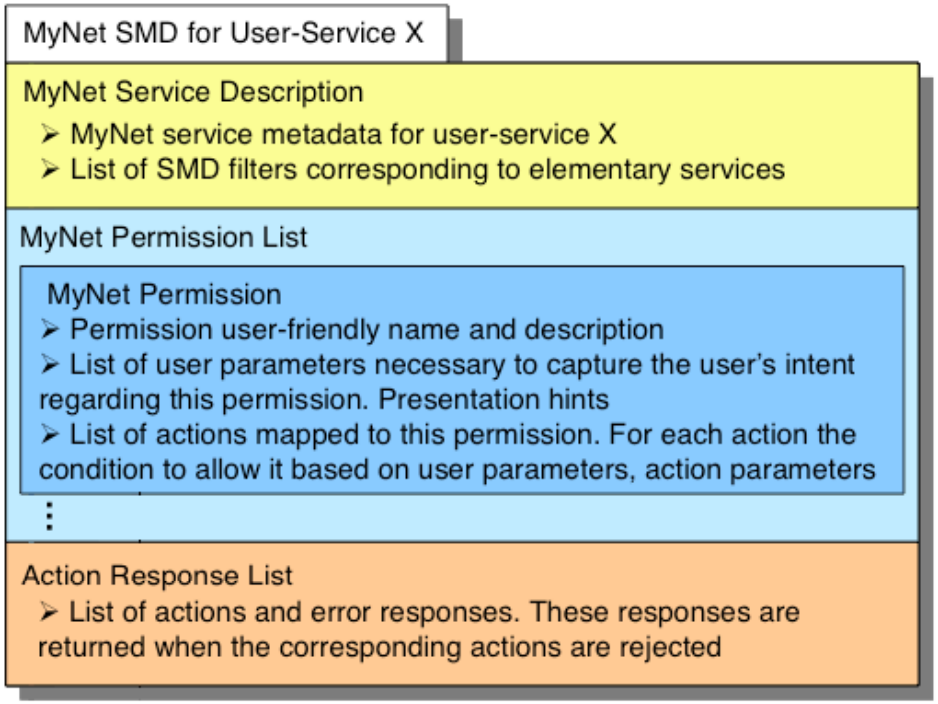
- Each device has a Dynamic Firewall, which intercepts all overlay traffic before it reaches hosted servers
- The firewall makes decisions based on security policies expressed by Passlets
- Passlets define user-level permissions (permissions meaningful to a user) by exposing a user-friendly part and connecting that to a system representation
- All passlets have information about *who* is giving permission, *to whom*, *for* what, and *for how long*
- A PDC-wide Boolean flag is set to true if permission is for all PDC instances of a service
- The PassletID is a unique 128-bit number
- Passlets are stored in sent and received passlet repositories (in the PDC-store) and are replicated across the PDC

Security: Passlets and the Firewall

- Cumulative Passlets (cPasslets)
  - Internal structures created and maintained by MyNetSec
  - Provide a snapshot of the cumulative effect of permissions granted to a user or by a user through a series of Passlets
  - cPasslets are continuously updated based on Passlets being sent, received, revoked, and expired
- Dynamic Firewall
  - Assembles traffic into units directed to exactly one elementary service as defined by the Service Mapping Documents (SMD) module
  - SMD filters sort the traffic into units that unambiguously specify the destination service, filters are defined in the order of the stack of protocol layers
    1. IP layer (UIA-IPv6)
    2. Transport layer (TCP,UDP)
    3. Service transport layer (HTTP, RTP)
    4. Service invocation layer (SOAP)
    5. Service ID layer

Service Mapping Documents (SMD) Module

- The SMD Module parses SMD documents from installed services to provide information to MyNet discovery and security modules
- SMDs are XML documents containing
  - The user-service description used to create Resource Discovery Records (RDRs)
  - Description of one or more elementary distributed services
  - A list of user-level permissions mapped to RPC actions
  - A list of error codes



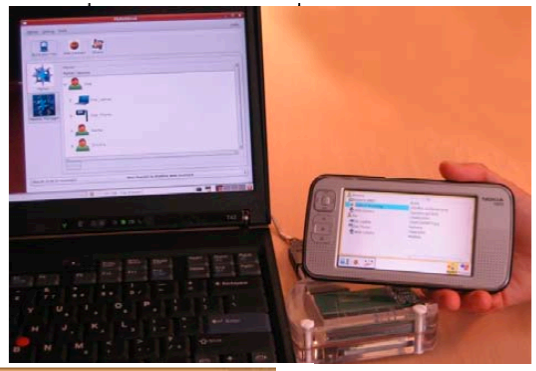
MyNetBook

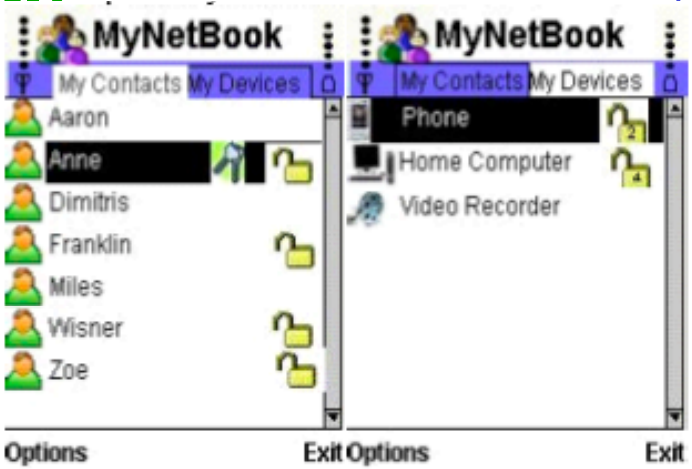
- A set of UI tools that use the MyNet API to provide user-friendly interaction with the PDC
  - MyNet Imprinting - passes user data into the PDC-store and MyNetSec modules during imprinting
  - MyNet Manager - retrieves discovery records
  - MyNetService Manager - allows the user to install and launch services
  - MyNet Viewer - the front-end GUI application
  - MyNetSec - create, edit browse, and revoke Passlets
  - Introduction manager - uses API calls from the Out-of-Band Introductions module to introduce new devices and social contacts

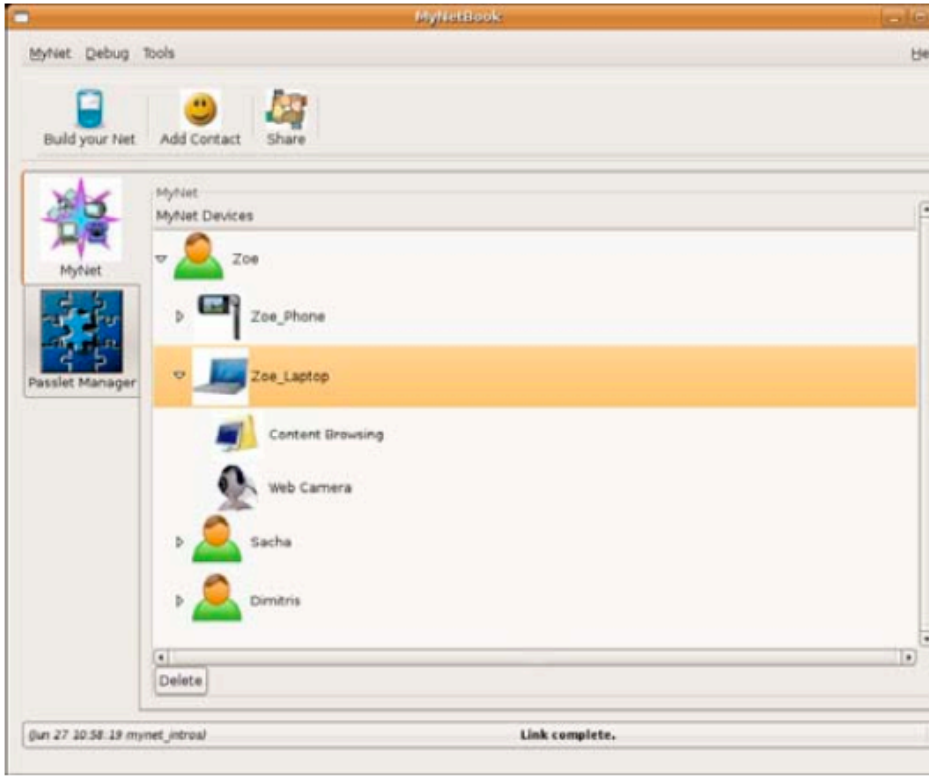
MyNetBook (cont.)

- Personal Network Navigation
  - Devices are shown as the children of the user and services are the children of devices
  - Social contacts appear as children of the PDC owner
- Introductions
  - Simple point and click gestures
  - Gestures can be interpreted differently based on context (e.g. add personal device, add social contact, bootstrap network connectivity, invoke service discovery, give access rights, share, launch an application…)

MyNetBook (cont.)







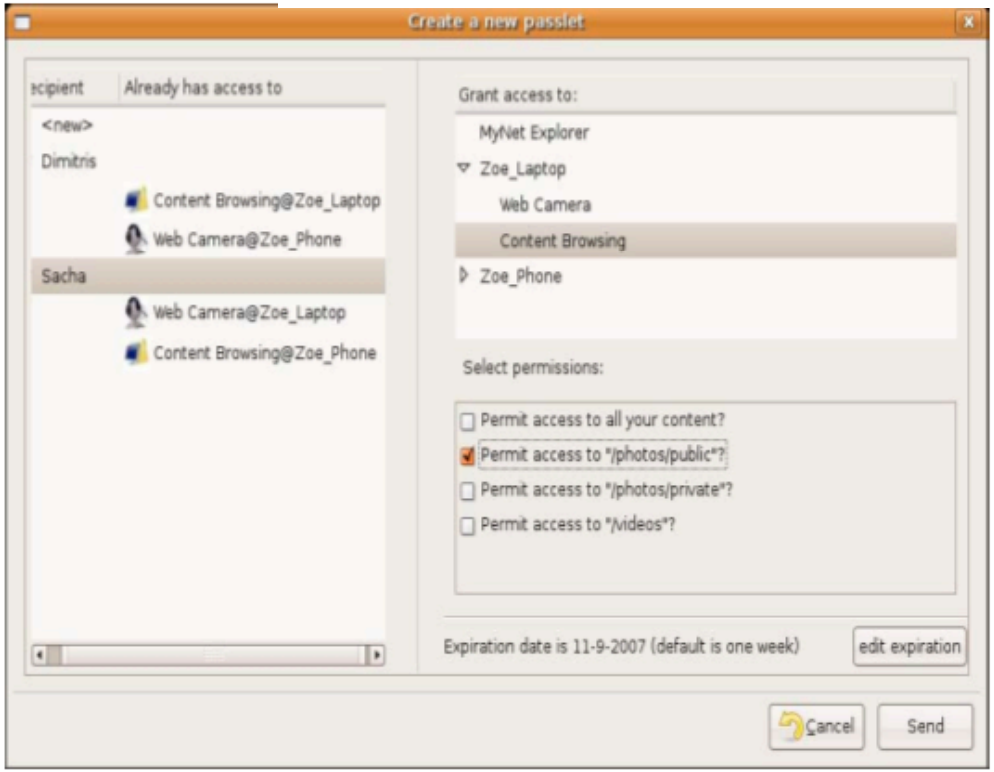


Figure 4: The MyNet Viewer

Figure 5: The MyNet Passlet Manager tool.

Evaluation

Table 1: Key usability test results.

ISSUE	YES	IN PART	NO
Users understand the end result of imprinting	77%	15%	8%
Users can create, navigate and access a PDC	100%	-	-
Users associate sharing with new contacts	54%	39%	7%
From the GUI, users deduce the Passlet metaphor	64%	-	36%
Users can issue and revoke Passlets	100%	-	-
Adding contacts and sharing raises privacy issues	75%	25%	-
Users prefer TAPing over other wireless proximity modalities for portable devices	78%	7%	15%

Table 2: Feature availability.

Properties: / Services:	Service Sharing	Access Control	Remote Access	F2F	Scalability	Identity Management	Content Limitations
Email	no	yes	yes	no	limited	service[5]	limited[4]
VPN	difficult	no[2]	yes	no	yes	enterprise[6]	no
USB	no	yes	no	yes	limited	user	limited[4]
BTH	no	yes	no	yes	limited	user	limited[4]
UPNP	yes	no	no	yes	limited	no	no
DFS	no	difficult	difficult	yes	yes	enterprise[6]	limited[4]
Httpd	difficult[3]	difficult[1]	difficult	yes	yes	no[7]	no
Twango	no	yes	yes	no	limited	service[5]	limited[4]
Flickr	no	no	yes	no	yes	service[5]	limited[4]
FaceBook	no	limited	yes	no	yes	service[5]	limited[4]
MyNet	yes	yes	yes	yes	yes	user	no