Securing Home Networks protocols

*A*SWN'04

K. MASMOUDI,
H. AFIFI

Boston, 08/2004

MAGNET

My Personal Adaptive Global NET

- 6th PCRD Integrated Project
- Goal : provide secure communication infrastructures for personal networks (PANs)
- Considerations :

1. Adaptive security mechanisms supporting the user's security needs in **various usage scenarios**
2. Provide a secure communication in a distributed and ad-hoc manner
3. Cross-layer optimization of security protocols supporting capabilities of a wide range of devices

Problem statement

- Security as a coherent service is not yet available
- Current security mechanisms (IPSec, SSL, …) are not enough adaptive and customizable
- Security often doesn't match the user's needs and expectations

Outline

- Introduction to home networks
- Home networks security
- Remote access scenario
- Protocol specification and validation

Introduction

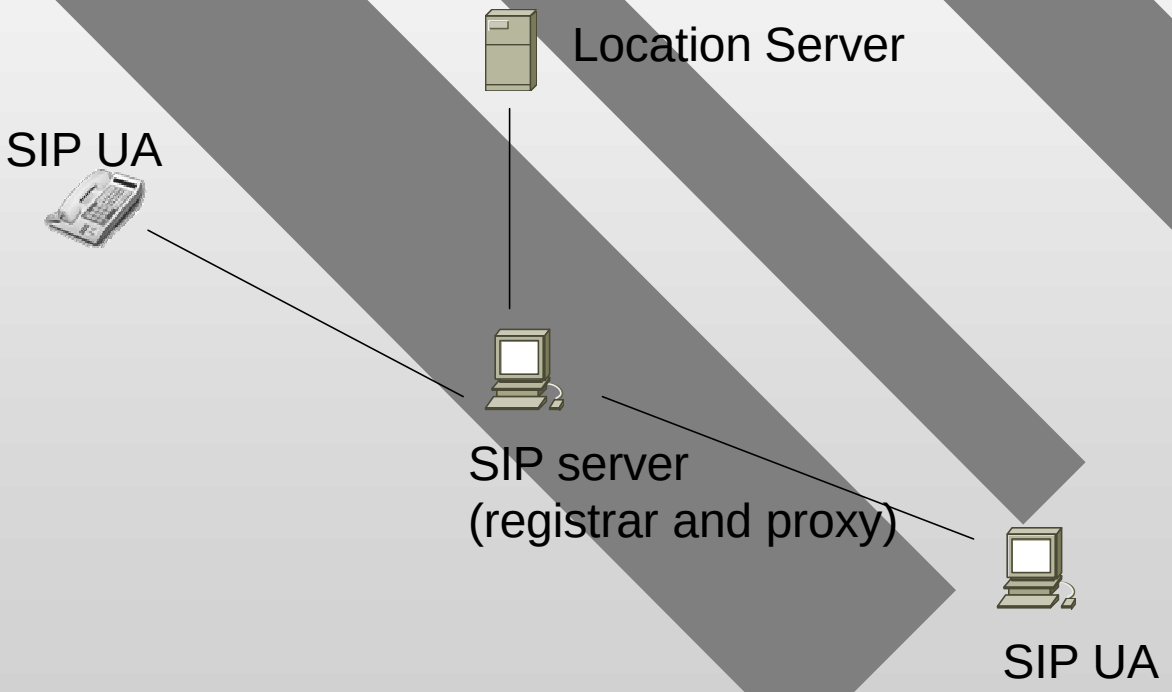
- Home computing environment evolving to home networking with mobile and wireless devices
- Multiple applications : multimedia, monitoring, communication…
- Heterogeneous technologies, resources and computational capacities

Home networks middlewares and protocols - UPnP

- Peer-to-peer network connectivity of intelligent appliances, wireless devices and PCs of all forms
- Standard-based connectivity to ad hoc or unmanaged networks
- UPnP is a set of client/server protocols implying many coexisting devices (clients or servers)
- The device (usually a physical entity) may host several home networking services, one or more device types…

Home networks middlewares and protocols - SIP

- SIP : signaling protocol for real-time sessions



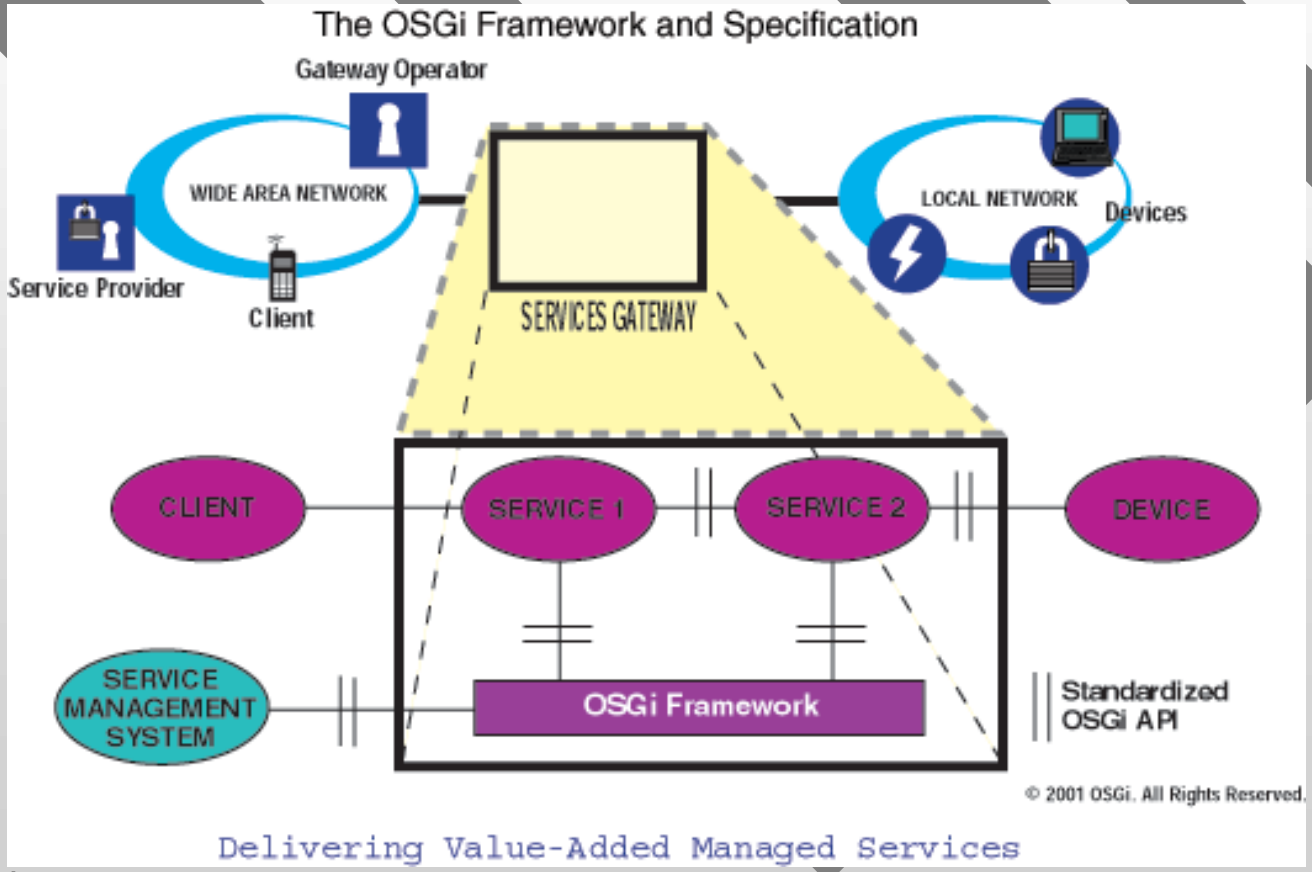
Home networks middlewares and protocols - OSGi

- OSGi : A Java-based environment (J2RE+OSGi framework) in which downloadable bundles of services managed by a registry can be run
- OSGi leverages numerous intra-home protocols and architectures by providing to the services provider an abstraction level of the underlying network
- Security may be deployed as a super-bundle

Home networks middlewares and protocols - WS

- Web service : a software system identified by a URI, whose public interfaces and bindings are defined and described using XML.
- Interpret XML-based SOAP messages
- Not limited to HTTP (e.g. HTTP not suitable for long-running tasks)
- Web services are self-describing (via metadata)

Home networks middlewares and protocols - OSGi



Securing HN (security components)

- Application level: UPnP, OSGi, SIP
- Transport Level: SSL/TLS
- Network Level: IPSec
- Link Level: BT, 802.11i,etc

State of the art of SIP security

- end-to-end mechanisms :

1. basic SIP authentication,
2. digest authentication and
3. S/MIME application layer encryption.

- hop-by-hop mechanisms are implemented on lower protocol layers, and is not a feature of SIP itself. They include

1. IPSec (IP security),
2. TLS (Transport Layer Security), with SIPS URI scheme when TLS is used.

What if you start from the beginning?

- We start from user requirements
- We start from a scenario
- We want to protect the whole communication scenario
- The previous solutions secure specific layers and should be used as a toolkit for complex scenarios.
- Security level should be set on the basis of the profile or the user's decisions.

A Simple Scenario example

- a distant terminal (belonging to the provider) communicates with a wireless home network component
- Devices may have low computational capacities or be battery-supplied

? a security-dedicated entity is needed (the Residential Gateway). It performs heavy cryptographic operations.

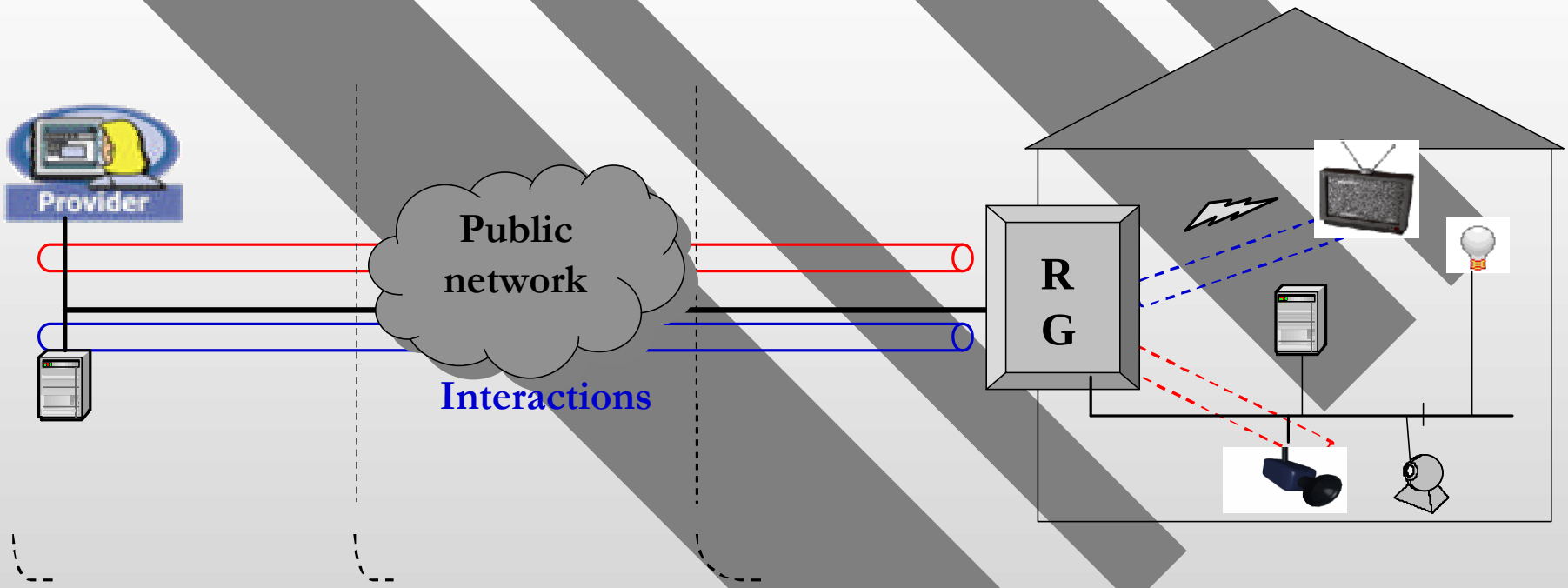
? two cases:

1. The device belongs to the HN owner
2. The device belongs to the provider but is located into the HN

Security policy : case 1

- RG and each component share a secret used to cipher session-keys while distributed. This secret may be exchanged when a component joins the network for the first time or during the device discovery phase.
- The RG negotiates authentication and session keys for the Home Network components. Keys are periodically refreshed, and act as logical access tokens.
- Anti-replay achieved by means of sequence numbers or counters.
- Confidentiality is achieved by symmetric stream (layer2) encryption. Message authentication with HMAC guarantees also integrity.
- In order to prevent a rogue CN from controlling a component, incoming messages are systematically checked.

Security policy : case 1

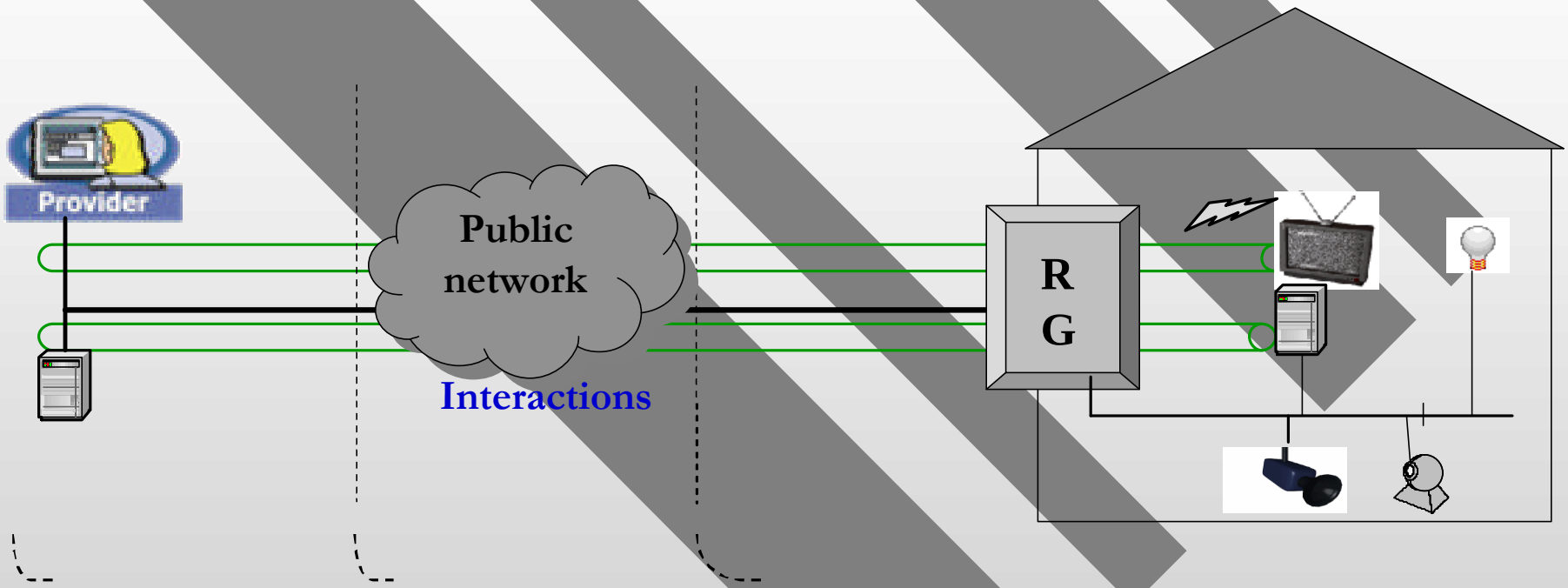


Provider domain Carrier domain Home network domain

Security policy : case 2

- Same security needs: integrity coupled with message authenticity, correspondents' authenticity, confidentiality, anti-replay and availability.
- the owner has limited control on the device. The secure tunnel is directly established end to end between the provider and the devices. The session keys are derived and distributed by the provider controller.
- The only control of the residential controller (gateway) is a negotiation of the controlled communication ports but no message scanning is possible, this is useful for NAT and firewall traversal.
- The provider's authentication is controlled by the RG.

Security policy : case 2



Provider domain Carrier domain Home network domain

Security protocol : case 1

Residential gateway

Device

Request access

Device located

Exchange nonces and authentication through signature

Pre-master secret enc. With RG public key

Session keys generation and distibution

Session encrypted key 1

Session encrypted key 2

Security protocol : case 2

Residential gateway

Device

Request access

Device located

Exchange nonces and authentication through signature

Session keys generation and distibution

Session encrypted

Control for DOS

Validation

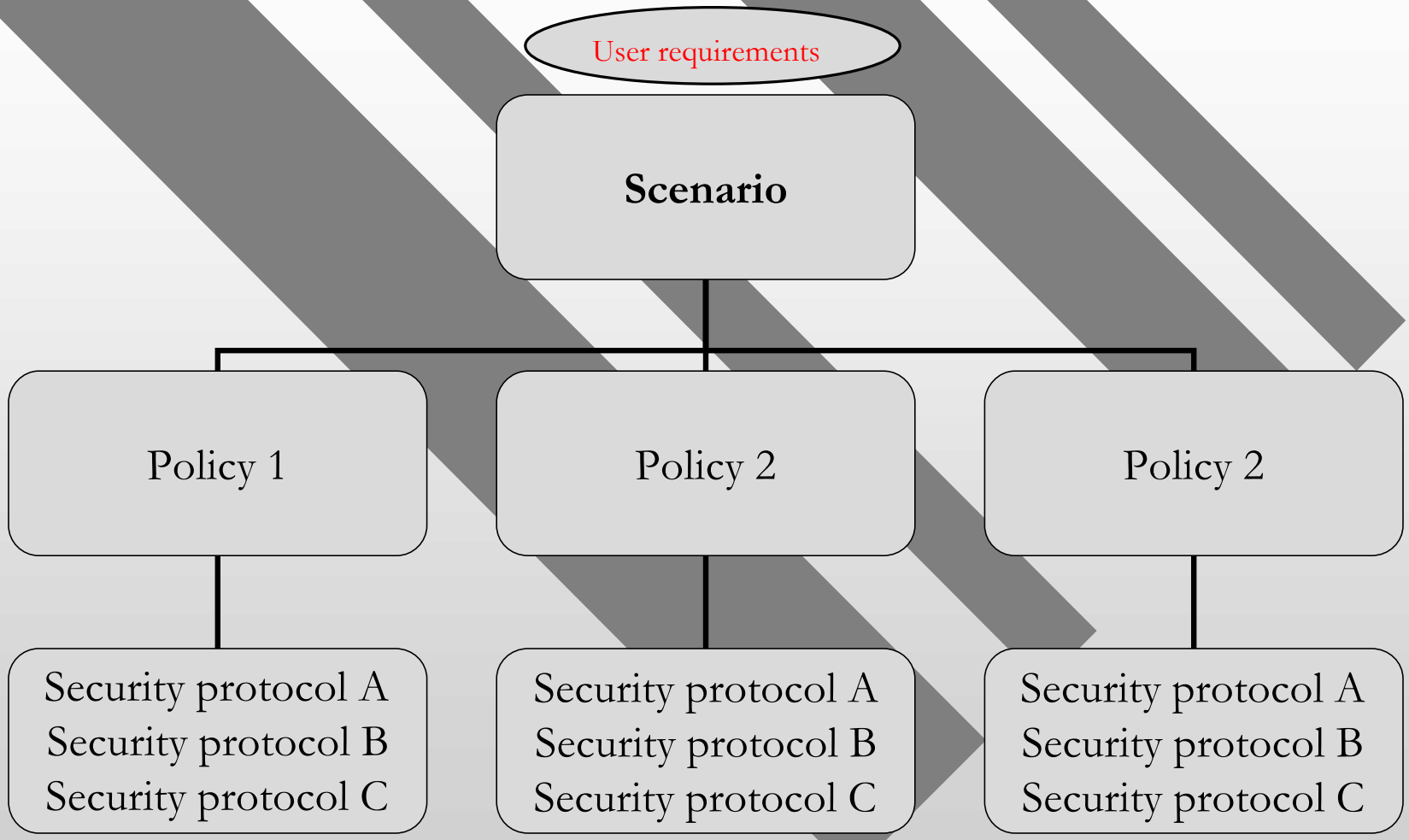
- We used an online model checking tool, called *Hermes*

www-verimag.imag.fr/~Liana.Bozga/eva/hermes.php

- verifying cryptographic protocols using a protocol specification language called LEAVA

Secrets: SK(h); Ka; shr(h,h); (h represent a *Principal*)	
GoodPatterns: {xs}_PK(h); {xs}_Ka; {xs}_shr(h,h)	BadPatterns: Vide

Conclusion


User requirements
Scenario
Policy 1
Policy 2
Policy 2
Security protocol A
Security protocol B
Security protocol C
Security protocol A
Security protocol B
Security protocol C
Security protocol A
Security protocol B
Security protocol C