International Telecommunication Union

European IPv6 Task Force

IPv6 FORUM

Enabling end-2-end security

Wolfgang Fritsche

IABG

Workshop on IPv6
Geneva, 22-23 June 2005

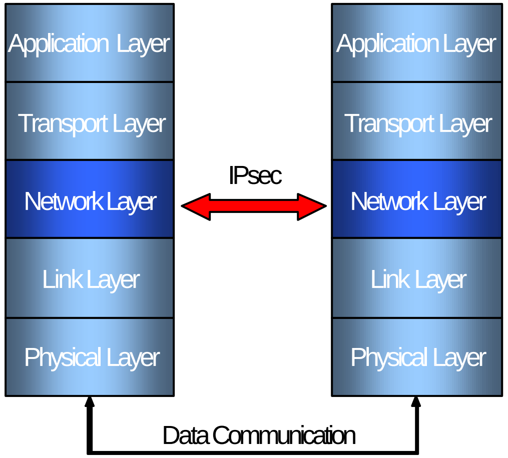
Agenda

- IPv6 security - facts & fiction
- IPv6 privacy - facts & fiction
- SEINIT- Deploying IPv6 security
- Summary

IPv6 security-
facts & fiction

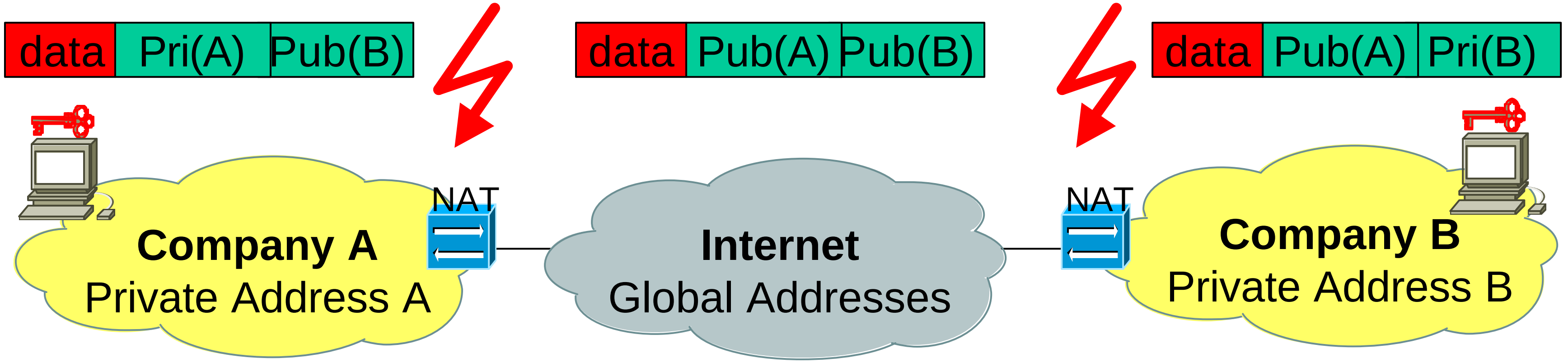
IPsec

- Is IPsec for IPv6 more secure than IPsec for IPv4?
  - *Clear answer: NO!*
- There cannot be a major difference, as
  - The IPsec functionality is on the same protocol layer
  - The IPsec protocol specification is the same
  - The algorithms / cryptography to be used are the same



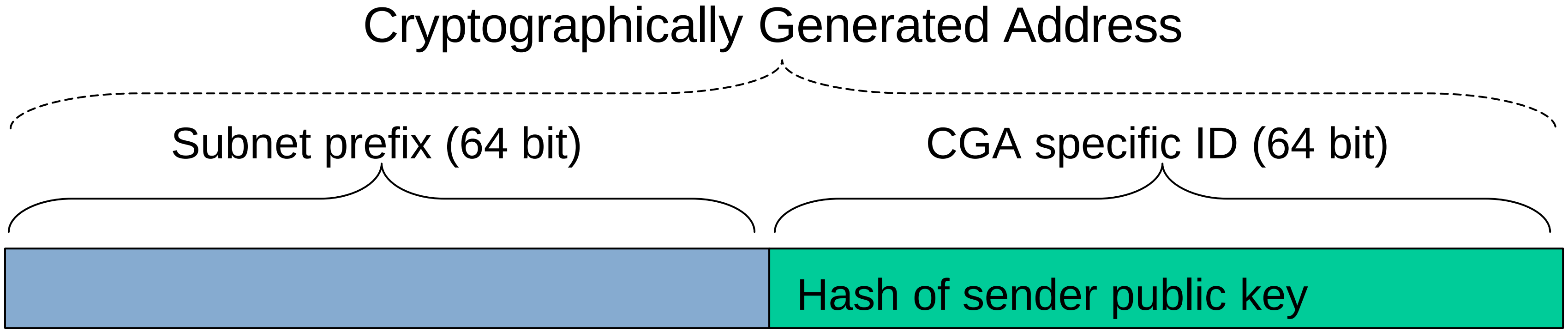
IPsec ctnd.

- However, IPsec deployment will be easier in IPv6 due to the disappearance of NAT boxes
  - NAT boxes modify IP packets and break therefore the end-to-end transparency
  - This modification also breaks end-to-end IPsec
  - Workarounds are complex and costly and often not possible at all
-



Cryptographically Generated Addresses

- **IPv6 addresses, which carry hashed information about public key in the identifier part**
- **Benefits**
  - **Certificate functionality without requiring a key management infrastructure**
  - **Solution for securing IPv6 Neighbor Discovery (resolve chicken-egg problem of IPsec)**


Cryptographically Generated Address
Subnet prefix (64 bit)
CGA specific ID (64 bit)
Hash of sender public key

The side benefit of large address space

- IPv6 uses 2^{64} addresses on a link instead of usually less than 2^{8} for IPv4
- Attacks based on simply scanning a whole network
  - would need years for performing it
  - would thereby consume a massive bandwidth on the scanned link
  - are therefore no longer appropriate
- However
  - one needs to take care about the addressing of server (use of arbitrary identifiers)
  - one needs to secure neighbor discovery messages

Viruses, worms and spam

- **Viruses, worms and spam are today some of the most annoying penetrations**
  - They infect user equipment
  - Consume significant network / computation resources
  - Have a large scale distribution
- **Can IPv6 prevent me from that?**
  - NO, as viruses, worms and spam are an application level problem, and have to be defended there
  - In the same way IPv4 cannot help here
  - However, IPv6 could make their fast distribution more complex (network scanning for vulnerable systems is more complex in IPv6)

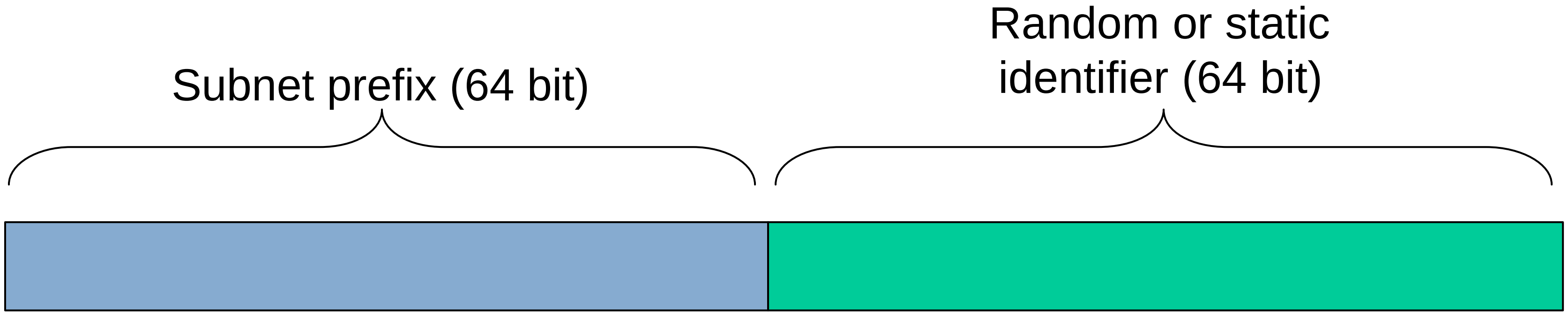
IPv6 security products

- The main security product manufacturer support meanwhile IPv6 for IPsec, firewalling, IDS, ...
- However, some of these products are just copies from IPv4 and don't reflect IPv6 specifica, e.g.
  - Extended use of ICMPv6 requires different firewalling policies
  - Reflect the increased use of IP Multicast instead of Broadcast on local links
  - Make use of IPv6 address aggregation for more effective ingress filtering
  - Discard fragmented packets sourced from / destined to intermediate systems
  - Efficient support of tunneling, which will be intensively used during IPv6 transition
- Further work is required here

IPv6 privacy - facts & fiction

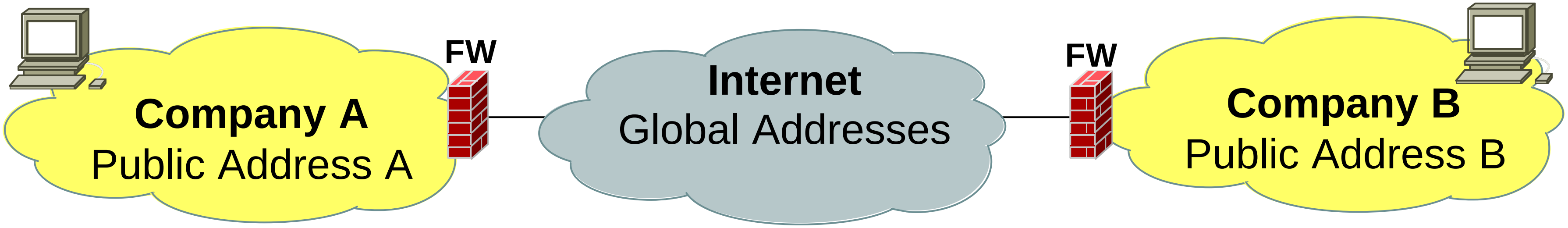
Tracability of (mobile) users

- In stateless IPv6 address autoconfiguration identifiers can be derived from HW (static part in address)
- Does this mean that I‘m trackable (location, sites visited, ...)?
  - IPv6 supports also random identifiers for privacy reasons
  - These random identifiers are default setting in some operating systems



Disappearance of NATs

- Without NAT boxes my home / company devices will have public addresses
- Does this mean that I‘m easily reachable from outside and therefore also more affected by attacks?
  - NO, as NAT boxes do not give any security or privacy.
  - A (host) firewall can effectively shield parts which should not be reachable from outside.
  - Even more, a firewall can provide application layer security, a NAT box can not



Workshop on IPv6
Geneva, 22-23 June 2005

SEINIT

Deploying IPv6 security

SEINIT overview

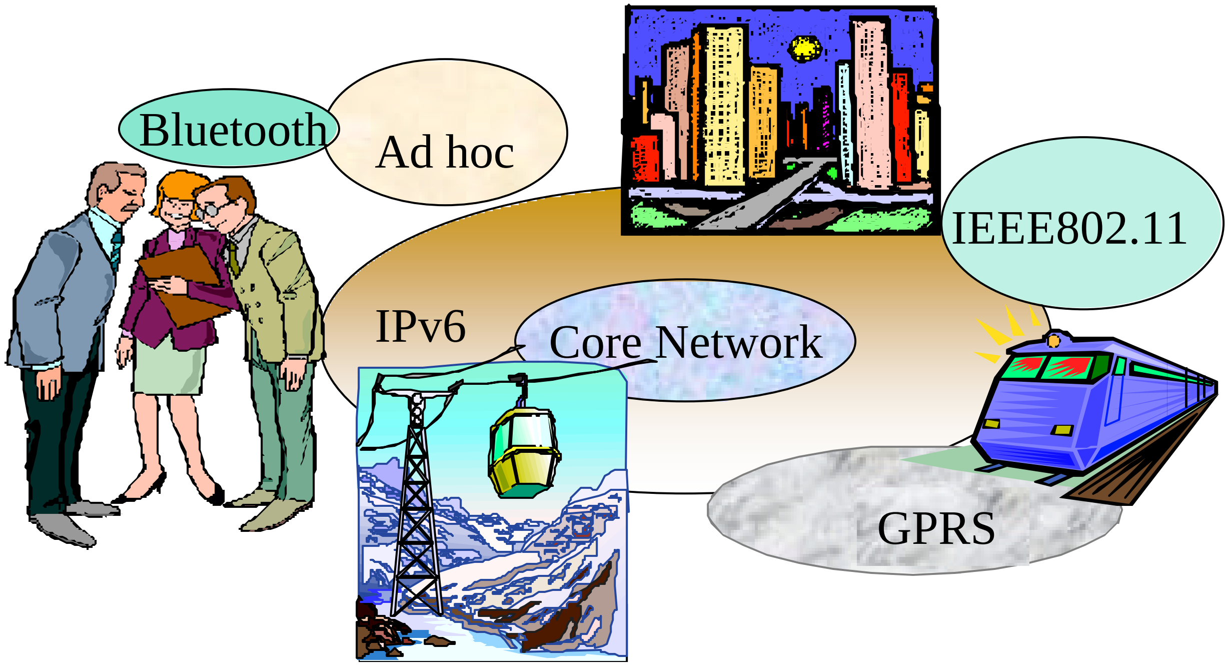
- FP6 call-1 project: Security Expert Initiative
- 2 years project: Dec. 2003 – Nov. 2005
- Budget: 8 M€ (3.9 M€ EU contribution)
- 12 Partners
  - Thales Communications, Alcatel, BT, T-Systems NOVA, IABG, ENST, KYOS, THALES (UK), UCL, UMU, WIT, ISOC
- Public deliverables will be made available at:
  - www.seinit.org

SEINIT goals

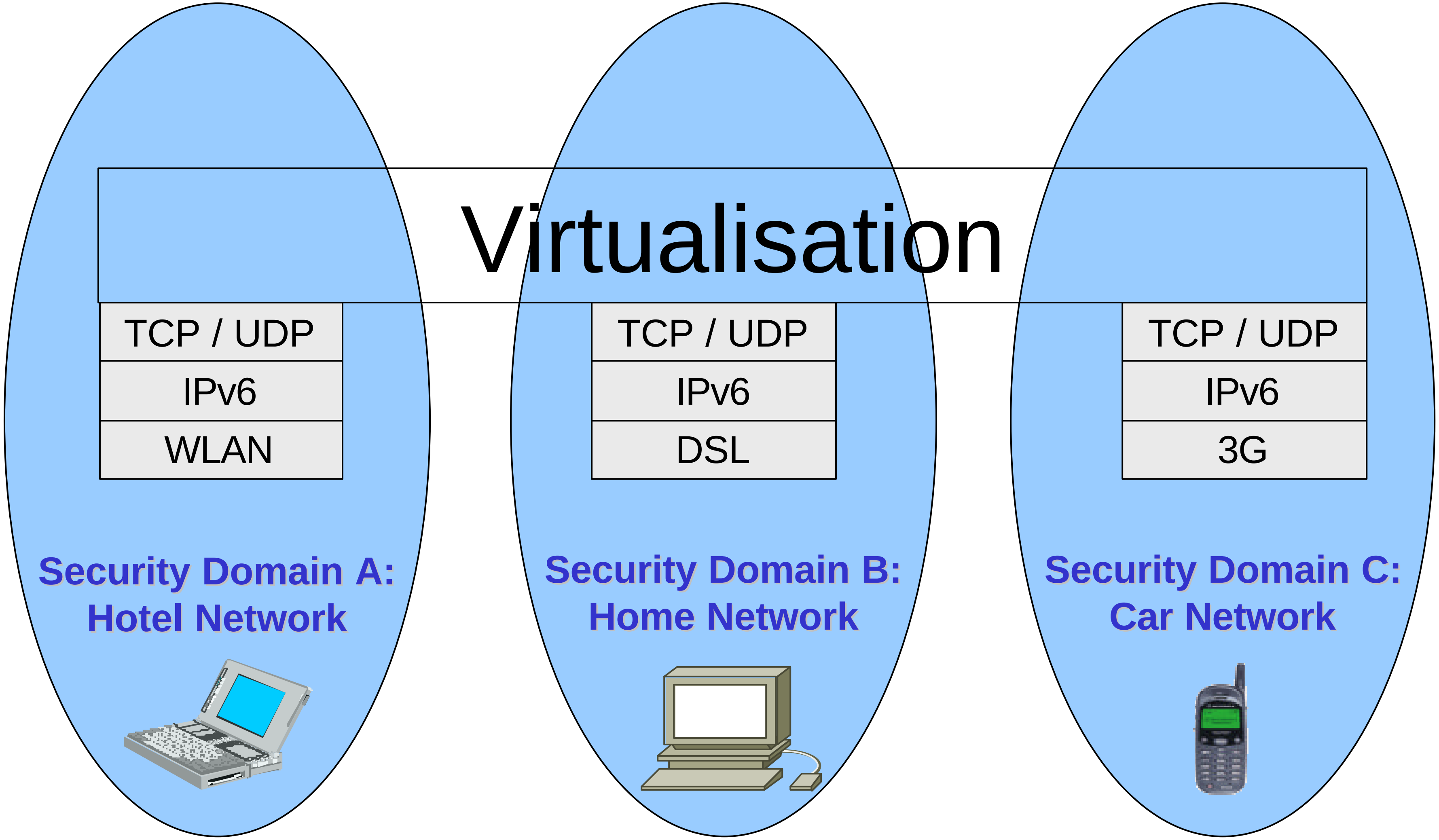
- Key project goals
  - Investigate emerging security technologies
  - Research on new security models and policies
  - Specify security architectures involving heterogeneous underlying networks
  - Develop prototypes of new security components
  - Provide training to users, manufacturer, ISPs, …

SEINIT – Heterogenity of …

- Access networks
- Protocols
- Applications
- User devices
- Security policies
- ambience



SEINIT – principle of virtualization



Virtualisation

TCP / UDP
IPv6
WLAN

TCP / UDP
IPv6
DSL

TCP / UDP
IPv6
3G

Security Domain A:
Hotel Network

Security Domain B:
Home Network

Security Domain C:
Car Network

SEINIT - Status

- Research
  - **Many emerging security technologies initially investigated, such as CGA, PANA, honeypots, ...**
  - **Investigations done on security policy handling**
  - **Initial architecture for heterogeneous ambience defined**
  - **IPv6 prototypes for CGA, PANA, honeypot, policy management, ... developed**
  - **Virtualisation approach implemented in middleware**
- Demonstration
  - **First demonstration of middleware done during annual EC conference November 2004**
  - **Next demonstration scheduled for 28 June 2005 within EC review**
- Contact to DHS
  - **Contacts established via ISOC to US Department for Homeland Security**

Summary

Summary

- IPv6 security
  - IPsec for IPv6 and IPv4 are equal in security strength, however, disappearance of NAT will ease deployment
  - CGAs are an efficient mean to secure ND on local links
  - Network scanning is more difficult with large IPv6 address space
  - IPv6 could make the fast distribution of viruses, worms and spam more difficult
  - Available security products need to consider more detailed IPv6 characteristics
- IPv6 privacy
  - IPv6 has an efficient mechanism for preventing the tracing of IP addresses
  - Disappearance of NAT won‘t harm privacy and security

Contact

Wolfgang Fritsche

Manager Advanced IP Services

Phone: +49 89 6088-2897
Email: fritsche@iabg.de