

---

# Segurança de Comunicações em Redes Locais

---

André Zúquete  
IEETA/UA



# Motivação

- As LANs sempre foram consideradas ambientes computacionais seguros
  - Não existem arquitecturas de segurança para lidar com problemas de segurança em LANs
  - Os protocolos de gestão e configuração de LANs não são protegidos
- Mas uma LAN já não pode ser considerada um ambiente computacional seguro
  - A sua gestão é sensível a inúmeros ataques locais
    - Recorrendo a escuta e personificação (*spoofing*)
  - As máquinas podem ser comprometidas por ciberpragas
  - Pode não existir confiança mútua entre todos os utentes de uma LAN
    - Os utentes podem mesmo não se conhecer ...

# Problemas de segurança em LANs:

## Alguns exemplos

- Controlo de acesso de nível 1 (físico)
  - A solução actual baseia-se no 802.1X
  - Mas um utente autorizado pode não ser um utente confiável!
- Endereçamento e comutação de nível 2 (lógico)
  - Roubo de endereços L2 (*MAC addresses*)
  - Envenenamento de *caches* ARP (*ARP cache poisoning*)
  - Envenenamento de *caches* de endereços L2 nos *switches*
  - "Conversão" de *switches* em *hubs*
- Configuração, encaminhamento e interacção de nível 3 (rede)
  - Servidores DHCP falsos
  - ICMP *Redirects* falsos
  - Personificação / escuta de comunicações locais
    - Exemplo: envenenamento de *caches* DNS dos clientes

# Protecção da LAN:

## Mecanismos de segurança necessários (1/2)

### ■ Autenticação

#### □ De utentes

- No acesso à LAN
- No acesso a serviços da LAN
  - DHCP, DNS, *gateway*, etc.
- Na interacção com outros utentes da LAN

#### □ De serviços da LAN

- Serviço de autenticação de utentes
- Serviço de DHCP, de DNS, de *gateway*, etc.

# Protecção da LAN:

## Mecanismos de segurança necessários (2/2)

- Autorização de utentes
  - No acesso à LAN
  - Na reserva de recursos da LAN
    - Exemplo: endereços IP
- Confidencialidade e integridade das comunicações locais
  - Cifra do tráfego local
  - Controlo de integridade de tráfego local

# Proposta:

## SLAN (*Secure LAM*)

- SLAN é uma arquitectura de segurança para uma LAN
  - Possui um serviço base de distribuição de chaves de sessão
  - As chaves de sessão servem para proteger interacções locais
    - Autenticação e controlo de integridade de transacções de configuração
      - DHCP e ARP
    - Confidencialidade e integridade de comunicações IP locais
  - É uma solução baseada fundamentalmente em software
    - Na sua quase totalidade independente dos dispositivos de *hardware* da rede
  - É transparente para os utentes
- As máquinas de uma SLAN podem:
  - Decidir sobre a sua política de protecção
  - Negociar acordos específicos de segurança com outras máquinas da SLAN

# SLAN:

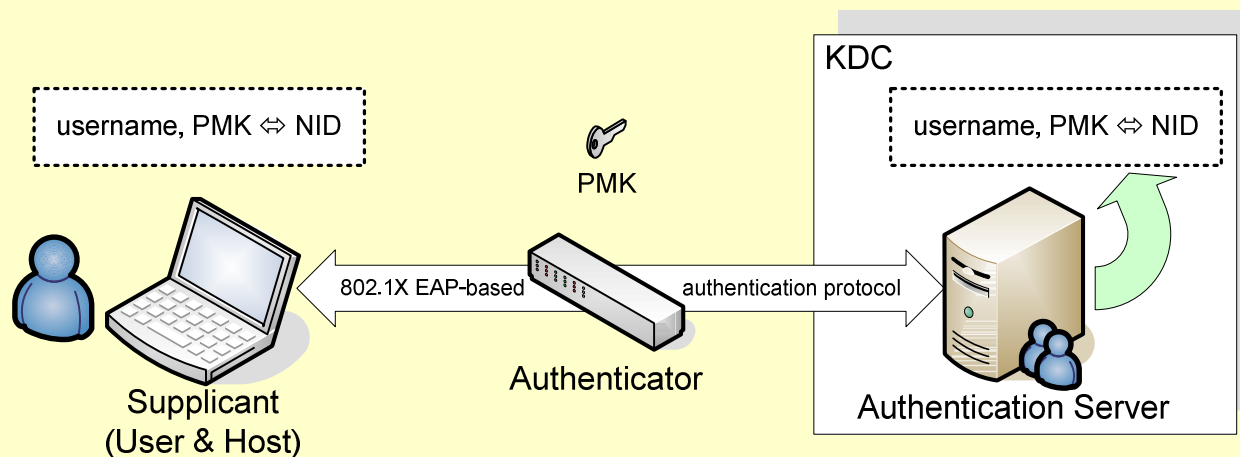
## Aproximação seguida

- Tem um serviço de distribuição de chaves (KDC)
  - Estende o serviço base de autenticação e autorização 802.1X
  - Fornece chaves de sessão para pares de máquinas SLAN autenticadas
- Um novo identificador de máquinas autenticadas SLAN
  - NID (*Network ID*)
- Adaptação das mensagens dos protocolos DHCP e ARP
  - Distribuição de chaves de sessão
    - **Key Propagator** ≈ Kerberos Ticket
  - Protecção de contra tentativas de personificação (*spoofing*)
    - Inclusão de MACs calculados com chaves de sessão
    - Distribuição de mapeamentos autenticados entre endereços IP e L2
      - **IP-L2 Propagator**
- Novas políticas de reserva de recursos da rede
  - Reserva de recursos via DHCP segundo a identidade do utente

# Arquitectura SLAN (1/7):

## Serviço de distribuição de chaves (KDC)

- O KDC estende um Servidor de Autenticação 802.1X
  - A **Pairwise Master Key (PMK)** calculada no âmbito do 802.1X é guardada e usada pelo KDC para autenticar uma máquina e o seu utente
  - A PMKs são usadas para autenticar mensagens trocadas entre máquinas SLAN autenticadas e o KDC



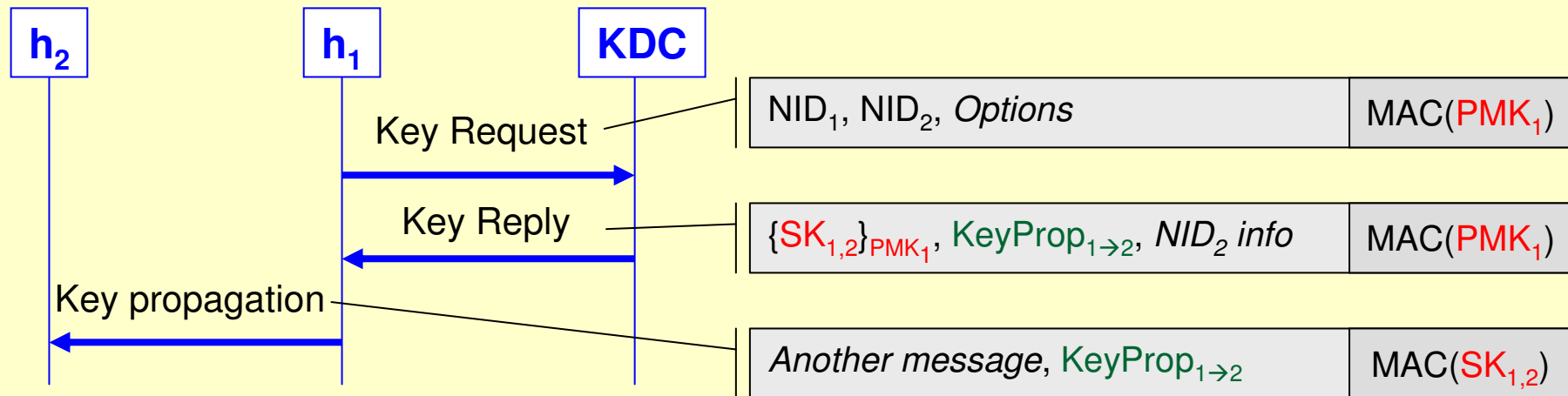
# Arquitectura SLAN (2/7):

## Identificação de máquinas com o NID (Network ID)

- Os endereços L2 and IP são facilmente falsificáveis
  - Logo não podem ser usados para reservar recursos sem uma prova de pertença
- Numa SLAN usa-se NIDs para identificar máquinas
  - $NID_{host} = \text{digest}(\text{username}, PMK_{\text{username}, \text{host}})$
  - Uma NID é um identificador temporário sem colisões
    - É válido enquanto a respectiva PMK for válida
  - Não é um identificador secreto
    - Mas a sua apropriação deverá ser infrutífera
- A reserva de recursos na SLAN deverá ser baseada na identidade do utente
  - Exemplo: reserva de endereço IP através de DHCP
  - A identidade do utente deverá ser fornecida pelo KDC dado o NID da sua máquina

# Arquitetura SLAN (3/7):

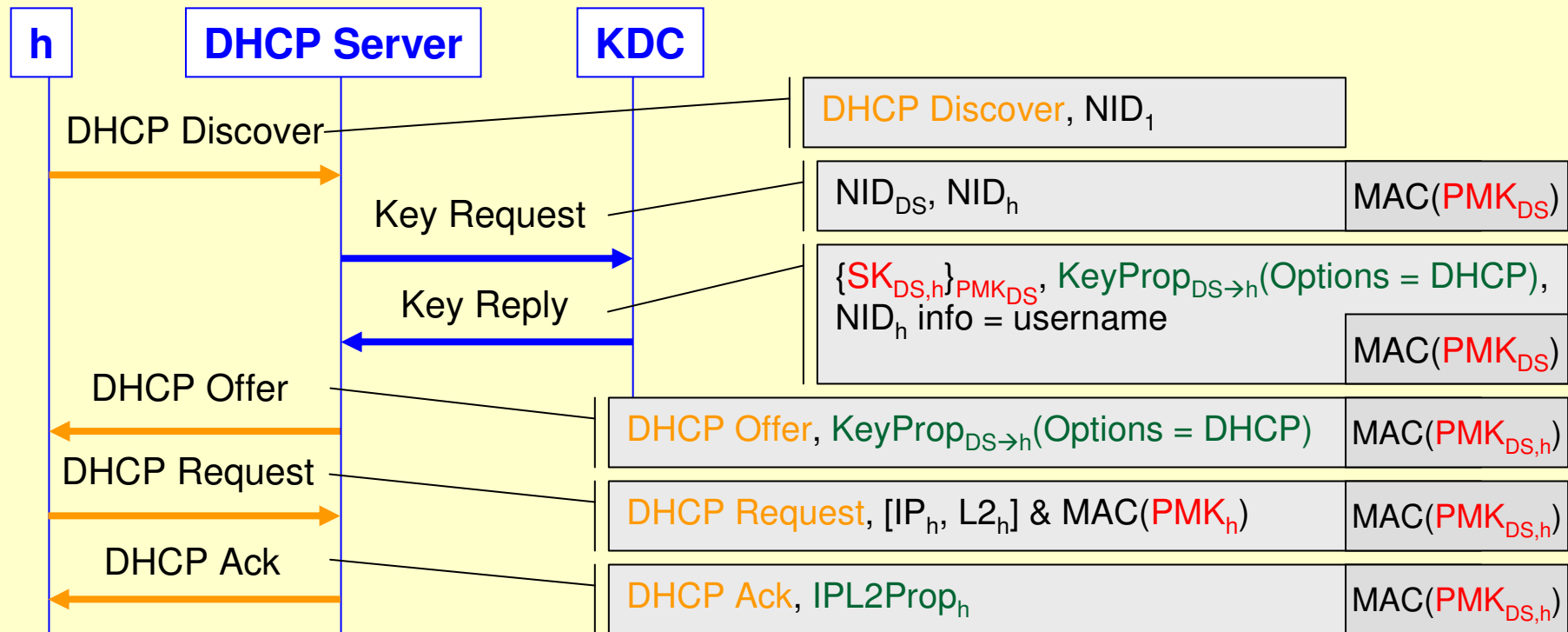
## Protocolo base de distribuição de chaves de sessão



$KeyProp_{1 \rightarrow 2} \equiv \{NID_1, NID_2, SK_{1,2}, Options\}_{PMK_2}$

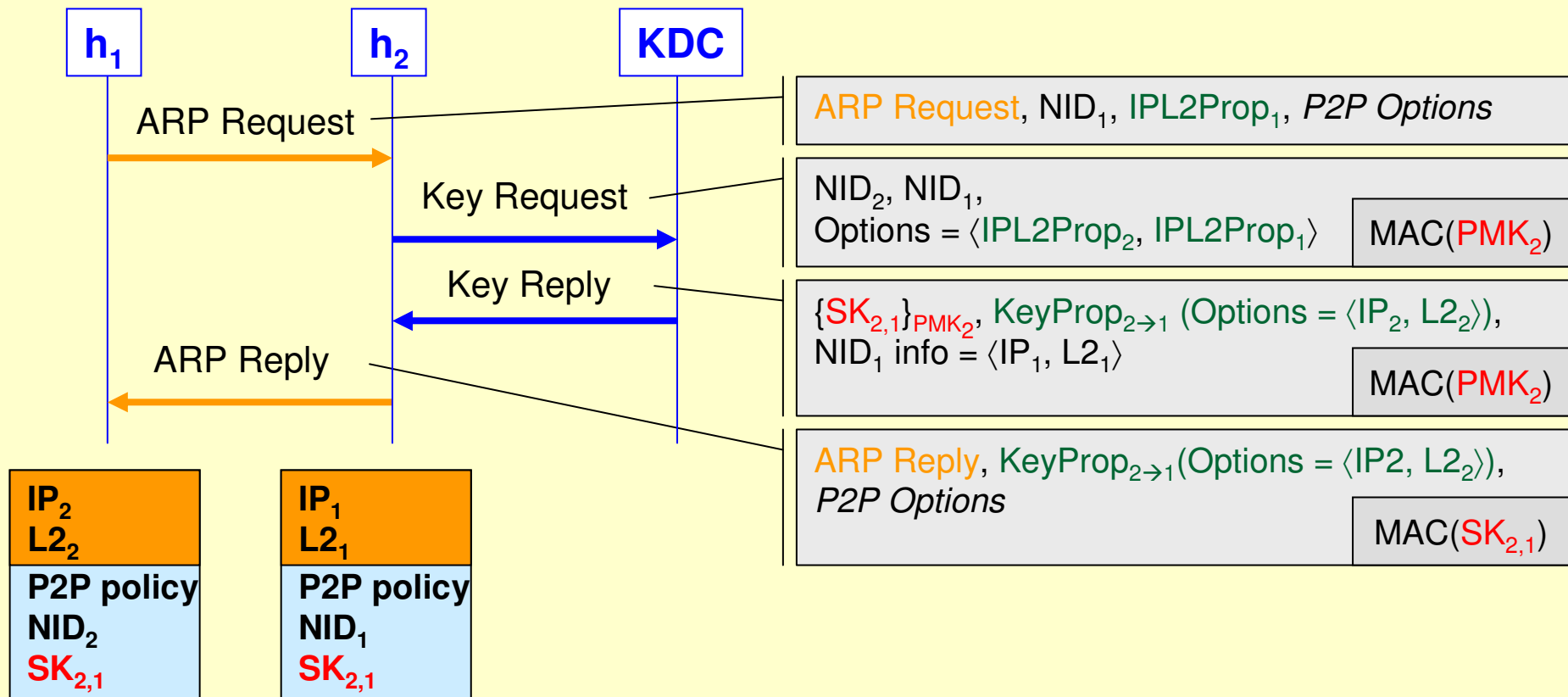
**h1 attributes:** IP-L2 addr mappings, network services (DHCP, gateway), etc.

# Arquitetura SLAN (4/7): DHCP seguro



$$\text{IPL2Prop}_h \equiv \left[ [\text{IP}_h, \text{L2}_h] \& \text{MAC}(\text{PMK}_h) \right] \& \text{MAC}(\text{PMK}_{\text{DS}})$$

# Arquitetura SLAN (5/7): ARP seguro



**Final ARP cache entries**

# Arquitectura SLAN (6/7):

## Interacção local segura entre máquinas

- Cada par de máquinas pode escolher como usa a chave de sessão distribuída no âmbito do último ARP seguro
  - Para instalar e configurar SAs IKE
  - Para instalar e configurar SAs IPSec
  - Etc.
- A escolha é definida pelas *P2P Options* usadas no protocolo ARP seguro

# Arquitectura SLAN (7/7):

## Novas políticas de segurança

- As máquinas não são livres de escolher o seu endereço IP
  - Precisam de obter o endereço IP e um *IP-L2 Propagator* de um servidor DHCP reconhecido pelo KDC
- A reserva de recursos via DHCP muda
  - Devem ser usados nomes de utentes em vez de endereços L2
- Tempo de vida das credenciais usadas na SLAN
  - O tempo de vida das PMKs define o tempo de vida das credenciais usadas numa SLAN
    - *Key Propagators* e *IP-L2 Propagators*
  - O tempo de vida *leases* DHCP deverá estar relacionado

# Avaliação da segurança

- Apropriação abusiva de endereços L2
  - Deixa de ser útil para reservar recursos via DHCP
  - Pode mesmo assim ser usada para baralhar as *caches* dos *switches* (DoS)
- Servidores DHCP falsos
  - Os clientes DHCP podem validar as respostas dos servidores DHCP através de chave de sessão partilhadas com um servidores DHCP autorizados
- Envenenamento de *caches* ARP
  - As *caches* ARP são construídas a partir de informação distribuída através dos *IP-L2 Propagators*
  - Esta informação é autenticada pelo KDC
- Personificação / escuta de comunicações locais IP
  - Pode ser evitada usando IPSec e as chaves de sessão SLAN

# Trabalhos relacionados:

## Cobrem apenas parte dos problemas

- Fundamentalmente protecção do protocolo ARP
  - S-ARP
  - TARP
    - IP-L2 tickets
  - Crypto-Ethernet NIC / SLL
    - Distribuição de chaves P2P usando chaves assimétricas
  - S-ARP
    - Chaves assimétricas, certificados dos endereços IP, assinaturas digitais
  - Secure ARP
    - KDC com chaves de longa duração por máquina
    - Não distribuí chaves para outros fins, implica sincronização de relógios
- Aspectos negativos comuns
  - Nenhuma integração com mecanismos de controlo de acesso à LAN
  - Nenhuma solução para a apropriação indevida de endereços L2
  - Servidores DHCP não autenticados
  - Não há inter-operação com outros protocolos
    - Por exemplo: IPSec
  - Fase inicial de distribuição de chaves de autenticação

# Realização:

## Prototipo concretizado em Linux

- Desenvolvido para testar o ARP seguro
  - Protocolo com o KDC realizado sobre tramas Ethernet
  - Pré-distribuição de PMKs e de *IP-L2 Propagators*
  - Uso de chaves de sessão para criar SAs IPsec AH

N.	Length (bytes)	Source address (L2 or IP)	Dest. address (L2 or IP)	Description
1	94	00:0c:29:8c:1c:e4	ff:ff:ff:ff:ff:ff	ARP: who has 192.168.202.133
2	143	00:0c:29:bb:87:3f	00:0c:29:76:6f:f8	ethertype 0x0801
3	143	00:0c:29:76:6f:f8	00:0c:29:bb:87:3f	ethertype 0x0801
4	126	00:0c:29:bb:87:3f	00:0c:29:8c:1c:e4	ARP: 192.168.202.133 is at 00:0c:29:bb:87:3f
5	122	192.168.202.131	192.168.202.133	AH(spi=0x82fa0685,seq=0x1) ICMP echo request, id 12095, seq 1
6	122	192.168.202.133	192.168.202.131	AH(spi=0xe4d0b21d,seq=0x1) ICMP echo reply, id 12095, seq 1

# Conclusões e trabalho futuro

- Uma nova arquitectura de segurança para LANs
  - Estendendo a arquitectura 802.1X
  - Um novo paradigma de identificação de máquinas/utentes
    - NID, baseado num nome e numa chave
  - Distribuição autenticada de chaves de sessão
  - Transacções DHCP e ARP seguras
  - Novas políticas de reserva de recursos
    - Endereços IP, *leases* DHCP.
- Protótipo concretizado em Linux
- Trabalho futuro
  - Procura de alternativas para a protecção de interacções IP locais
  - Uso de outros KDCs (Kerberos, etc.)
  - Adaptação a outros tipos de redes locais
    - Ad-hoc, IPv6, etc.