3GPP TSG SA WG3 (Security) meeting #46 S3-070xxx
Beijing, China , 13th – 16th Feb 2007

# 3GPP2 Network Firewall Configuration and Control

Michael Paddon
QUALCOMM
mwp@qualcomm.com

Adrian Escott
QUALCOMM
aescott@qualcomm.com

Anand Palanigounder
Nortel
anand@nortel.com

*Disclaimer:* This presentation reflects contributors view of the 3GPP2 NFCC and is neither reviewed nor endorsed by 3GPP2.

# Rationale

- Minimize ingress of unsolicited or unauthorized packets onto the air interface.
- Reduce exposure to:
  - unnecessary consumption of bandwidth
  - malicious traffic directed at handsets
  - unnecessary consumption of resources such as battery life and processing capacity
  - billing issues

# Status

- NFCC is a 3GPP2 project.
  - Requirements completed December 2004.
    - http://www.3gpp2.org/Public_html/specs/S.R0103-0_v1.0_041220.pdf
  - Architecture and detailed specification under development by TSG-X PDS working group.
  - Stage 2&3 work substantially complete.
  - This presentation is a snapshot of a work in progress.

3RD GENERATION PARTNERSHIP PROJECT 2 "3GPP2"

# Scope

- NFCC is a mechanism for authorized entities (typically handsets) to dynamically manage packet filter policy for **inbound** packets.
- NFCC is **not a firewalling technology.**
- **NFCC is not a replacement for a firewall on the handset.**
- **NFCC allows operators to define overriding policy on what is and is not allowed.**

# Operational Model

- NFCC defines a common operational model so that roaming handsets can inter-operate with visited networks.
  - Incoming packets are mediated by a packet filter, with policy defined by a pinhole set.
  - Initially, all inbound packets are denied.
  - All outgoing packets are unrestricted.
  - When an inbound or outbound packet initiates a session, that session is statefully filtered thereafter.
  - Authorized clients may create and destroy pinholes.

# Pinholes

- A pinhole is defined as a set of constraint vectors of the form:

  *<header-field, minimum, maximum>*

- *A packet that satisfies* ***all constraints matches the pinhole.***
- ***Pinholes come in two flavors:***
  - ***A whitehole specifies wanted traffic.***
  - ***A blackhole specifies unwanted traffic.***

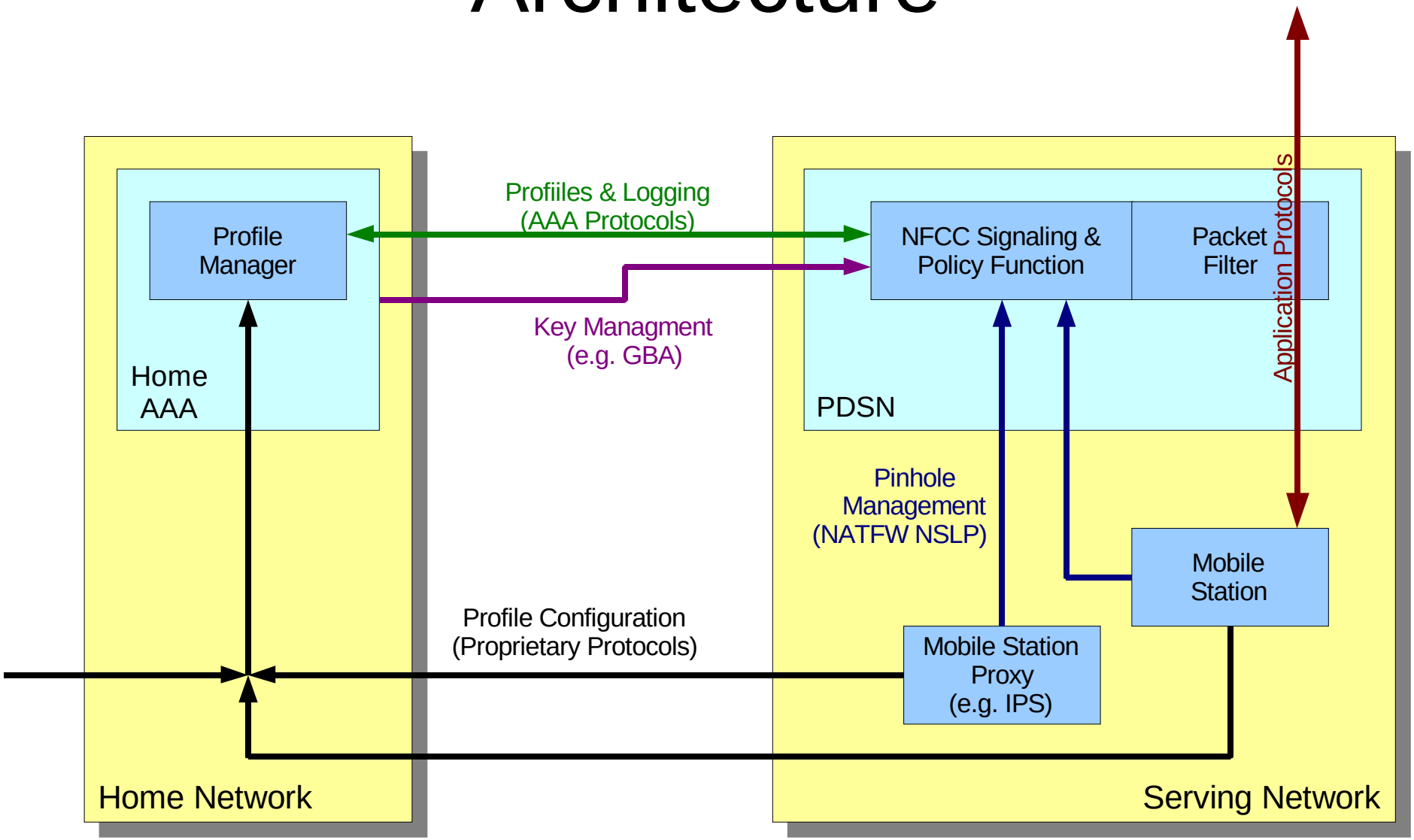
# Supported Header Fields

- IP version
- IP source and destination addresses
- IP payload protocol
- IPv4 DCSP (IPv6 class)
- IPv6 flow
- IPSec SPI
- ICMP type and code
- TCP source and destination ports
- UDP source and destination ports
- Others may be defined... (SIP fields?)

# Pinhole Sets

- Filtering policy is expressed as a pinhole set.
- A packet matches a pinhole set iff:
  - At least one whitehole is matched.
  - No blackholes are matched.
- Pinholes are independent of each other.
  - The order of definition doesn't matter.
  - Thus, implementations may build highly scalable classifiers that may be dynamically updated in an efficient fashion.

# Architecture



# Pinhole Management

- Pinhole signaling is performed using the IETF NSIS framework.
  - Signaling protocol is NATFW NSLP (with minor extensions).
  - Pinholes are soft state: they timeout if not explicitly removed.
  - Path-coupled signaling is used to automatically discover packet filters.
  - Path-decoupled signaling may be used by off path entities (i.e. proxies).

# Joining and Leaving

- When a mobile station joins a network:
  - The HAAA informs the Profile Manager.
  - The Profile Manager sends an initial pinhole configuration for the MS to the serving network's packet filter.
- When a mobile station leaves a network:
  - The PDSN informs the packet filter.
  - The packet filter revokes all associated pinholes.

# Incoming Flows

- When a mobile station (or a proxy) wants to permit or deny incoming flows:
  - The MS signals the packet filter with a request.
    - Each request is an atomic set of pinhole creation and destruction operations.
  - The packet filter may honor or reject the request.
    - The packet filter logs a reason to the Profile Manger whenever a request is rejected. This helps home operators diagnose subscriber problems.
    - The packet filter may also log other “interesting” information.

# Security Threats

- An attacker who succeeds in issuing illegitimate requests threatens the integrity of the network.
  - All NATFW signaling must be authenticated and integrity protected.
- An attacker who can observe pinhole signaling knows how to craft unsolicited packets.
  - All NATFW signaling must be confidentiality protected.
- An attacker who can replay signaling can open unwanted pinholes.
  - All NATFW signaling must be replay protected.

# Transport Security

- NATFW NSLP operates over GIST (General Internet Signaling Transport), and uses both datagram and connection based carriage.
  - Use DTLS to secure D-mode.
  - Use TLS to secure C-mode.
- Mobile stations use pre-shared symmetric key material.
  - GBA may be used to derive PSKs.
- Infrastructure elements may use symmetric or asymmetric key material.

# Mobile IP

- Mobile IP support is hard. But it can be made easier by restricting MIP scenarios.
  - MIPv4:
    - FAs are always outside the packet filter. Agent Advertisments from FAs are always given ingress.
    - If colocated addresses are used, filtering is done on the encapsulated packet.
    - Registration Replies are filtered statefully.
  - MIPv6:
    - Binding Acknowledgements/Errors are filtered statefully.
    - Route optimization and return routability not supported yet (awaiting proposed enhancements to MIPv6).

# Thank you for your time...

Questions?