PacketCable™ 2.0

Security Technical Report

PKT-TR-SEC-C01-140314

CLOSED

DISCLAIMER

Document Status Sheet

Document Control Number:	PKT-TR-SEC-C01-140314
Document Title:	Security Technical Report
Revision History:	V01 – Released April 6, 2006
	V02 – Released October 13, 2006
	V03 – Released September 25, 2007
	V04 – Released November 06, 2007
	V05 – Released April 25, 2008
	C01 – Closed March 14, 2014
Date:	March 14, 2014

Trademarks:

Abstract

This technical report describes the PacketCable security architecture, components, and reference points. The following information is included:

- Overview of PacketCable alignment with 3GPP IP Multimedia Subsystem (IMS) specifications;
- Description of threats to PacketCable architecture and data flows;
- Security architecture description;
- Explanation and description of PacketCable enhancements to 3GPP IMS requirements.

Table of Contents

Figures

Tables

1 INTRODUCTION

1.1 PacketCable Overview

PacketCable is a CableLabs specification effort designed to extend cable's IP service architecture and to accelerate the convergence of voice, video, data, and mobility technologies. PacketCable defines a modular architecture and a set of interoperable interfaces that leverage emerging communications technologies, such as SIP, Presence, and IM, to support the rapid introduction of new IP-based services onto the cable network.

PacketCable is based on the IMS as developed by the 3rd Generation Partnership Project (3GPP). The IMS is a SIP-based architecture for providing multimedia services. PacketCable defines enhancements to the IMS when necessary in order to ensure PacketCable addresses requirements that are not addressed by the IMS.

For more information, refer to the PacketCable Architecture Framework Technical Report [ARCH-FRM TR].

1.2 PacketCable Security Architecture Motivation and Goals

The PacketCable Security Architecture protects the data, interfaces, and components that make up the PacketCable architecture. This Technical Report describes the security relationships between the elements in the PacketCable architecture.

Design goals for the PacketCable security architecture include:

- Support for confidentiality, authentication, integrity, and access control mechanisms;
- Protection of the network from denial of service, network disruption, theft-of-service attacks;
- Protection of the UEs (i.e., clients) from denial of service attacks, security vulnerabilities, unauthorized access (from network);
- Support for end-user privacy through encryption and mechanisms that control access to subscriber data such as presence information;
- Mechanisms for device, UE, and user authentication, secure provisioning, secure signaling, and secure software download;
- Leverage and extend the IMS security architecture in furtherance of the previously stated goals.

2 REFERENCES

2.1 Normative References

There are no normative references in this specification.

2.2 Informative References

[ARCH-FRM TR]	PacketCable Architecture Framework Technical Report, PKT-TR-ARCH-FRM-C01-140314, March 14, 2014, Cable Television Laboratories, Inc.
[HSS TR]	PacketCable Home Subscriber Server Technical Report, PKT-TR-HSS-C01-140314, March 14, 2014, Cable Television Laboratories, Inc.
[ID SIP-OUTBOUND]	IETF Internet-Draft, Managing Client Initiated Connections in the Session Initiation Protocol (SIP), draft-ietf-sip-outbound-10, July 2007, work in progress.
[PKT 24.229]	PacketCable SIP and SDP Stage 3 Specification, 3GPP TS 24.229, PKT-SP-24.229- C01-140314, March 14, 2014, Cable Television Laboratories, Inc.
[PKT 33.203]	PacketCable Access Security for IP-Based Services Specification, 3GPP TS 33.203, PKT-SP-33.203-C01-140314, March 14, 2014, Cable Television Laboratories, Inc.
[RFC 2246]	IETF RFC 2246, The TLS Protocol Version 1.0, January 1999.
[RFC 2617]	IETF RFC 2617, HTTP Authentication: Basic and Digest Access Authentication, June 1999.
[RFC 3261]	IETF RFC 3261, SIP: Session Initiation Protocol, June 2002.
[RFC 3268]	IETF RFC 3268, Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS), June 2002.
[RFC 3280]	IETF RFC 3280, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, April 2002.
[RFC 3310]	IETF RFC 3310, Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA), September 2002.
[RFC 3329]	IETF RFC 3329, Security Mechanism Agreement for the Session Initiation Protocol (SIP), January 2003.
[RFC 3414]	IETF STD 62 (RFC 3414), User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3), December 2002.
[RFC 3415]	IETF STD 62 (RFC 3415), View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP), December 2002.
[RFC 3489]	IETF RFC 3489, STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs), March 2003.
[RFC 4086]	IETF RFC 4086, Randomness Requirements for Security, June 2005.
[SEC]	PacketCable 1.5 Security Specification, PKT-SP-SEC1.5-I03-090624, June 24, 2009, Cable Television Laboratories, Inc.

[SIP TR] PacketCable SIP Signaling Technical Report, PKT-TR-SIP-C01-140314, March 14, 2014, Cable Television Laboratories, Inc.

[TS 23.002] 3rd Generation Partnership Project; Technical Specification Group Services and Systems Aspects; Network architecture (Release 7); June 2007.

[TS 33.210] 3rd Generation Partnership Project; Network Domain Security Specification, IP network layer security (Release 7) September 2007.

[ID TURN] IETF Internet-Draft, Obtaining Relay Addresses from Simple Traversal Underneath NAT (STUN), draft-ietf-behave-turn-04, July 2007, work in progress.

2.3 Reference Acquisition

- 3rd Generation Partnership Project: www.3gpp.org
- Cable Television Laboratories, Inc., 858 Coal Creek Circle, Louisville, CO 80027;
  Phone +1-303-661-9100; Fax +1-303-661-9199; Internet: http://www.cablelabs.com
- Internet Engineering Task Force (IETF), Internet: http://www.ietf.org/

  Note: Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt

3 TERMS AND DEFINITIONS

This Technical Report uses the following terms and definitions:

ISIM	IM Services Identity Module - the collection of IMS security data and functions on a UICC; may be a distinct application.
PacketCable Multimedia	An application-agnostic QoS architecture for services delivered over DOCSIS networks.
Private Identity	See Private User Identity.
Private User Identity	Used, for example, for Registration, Authorization, Administration, and Accounting purposes. A Private User Identity is associated with one or more Public User Identities.
Public User Identity	Used by any user for requesting communications to other users or applications.
Server	A network element that receives requests in order to service them and sends back responses to those requests. Examples of servers are proxies, User Agent servers, redirect servers, and registrars.
SIP User Agent	As defined by [RFC 3261], a logical entity that can act as both a user agent client and user agent server, meaning that it can generate requests and manage the resulting transaction, and it can generate responses to incoming requests and manage the resulting transition.
Subscriber	An entity (comprising one or more users) that is engaged in a Subscription with a service provider.
Subscription	A contract for service(s) between a user and a service provider.
User	A person who, in the context of this document, uses a defined service or invokes a feature on a UE.
User Agent (UA)	A SIP User Agent.

4 ABBREVIATIONS AND ACRONYMS

This Technical Report uses the following abbreviations and acronyms:

3GPP	3rd Generation Partnership Project
AKA	Authentication and Key Agreement
CMS	Call Management Server
CMTS	Cable Modem Termination System
CSCF	Call Session Control Function
DDOS	Distributed Denial Of Service Attack
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DNSSEC	DNS Security
DOCSIS®	Data-Over-Cable Service Interface Specifications
DOS	Denial of Service
EMS	Element Management System
E-MTA	Embedded Multimedia Terminal Adapter
ESP	Encapsulating Security Payload
FQDN	Fully Qualified Domain Name
FW	Firewall
HSS	Home Subscriber Server
HTTP	Hyper Text Transfer Protocol
I-CSCF	Interrogating Call Session Control Function
IDS	Intrusion Detection System
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IPsec	Internet Protocol Security
MG	Media Gateway
MGC	Media Gateway Controller
MitM	Man in the Middle
MSO	Multi-System Operator: A company that owns and operates more than one cable system
MRF	Multimedia Resource Function
NA(P)T	Network Address and Port Translation; used interchangeably with NAT
NAT	Network Address Translation
NMS	Network Management System
P-CSCF	Proxy Call Session Control Function
PKI	Public Key Infrastructure
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RTP	Real-time Transport Protocol
SA	Security Association

S-CSCF	Serving Call Session Control Function
SDP	Session Description Protocol
SG	Signaling Gateway
SIP	Session Initiation Protocol
SLF	Subscription Location Function
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
STUN	Simple Traversal of UDP Through NAT
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TR	Technical Report
UA	User Agent
UDP	User Datagram Protocol
UE	User Equipment
UICC	Universal Integrated Circuit Card
URI	Uniform Resource Identifier

5 PACKETCABLE SECURITY

The PacketCable Security Architecture describes the reference points and logical components and the data flows between these components.

This section provides:

- A description of the relationship between PacketCable and 3GPP IMS releases;
- An overview of the PacketCable architecture;
- A description of the threats to the PacketCable architecture;
- A description of the PacketCable security mechanisms.

5.1 Relationship with 3GPP IMS

PacketCable is based on the IMS as defined by the 3rd Generation partnership Project (3GPP). 3GPP is a collaboration agreement between various standards bodies. The scope of 3GPP is to produce Technical Specifications and Technical Reports for GSM and 3rd Generation (3G) Mobile System networks.

Within the overall PacketCable goal to leverage existing industry standards whenever possible, there is a specific objective to align with the IMS architecture and specifications being developed by 3GPP. Specifically, PacketCable will reuse many of the basic IMS functional entities and interfaces. Although this Technical Report discusses IMS, the main goal is to describe the enhancements and modifications to 3GPP specifications. Refer to [TS 23.002] for additional information on the 3GPP IMS architecture.

5.2 PacketCable Reference Architecture

An overview of the PacketCable architecture elements and functional groupings is illustrated in Figure 1.

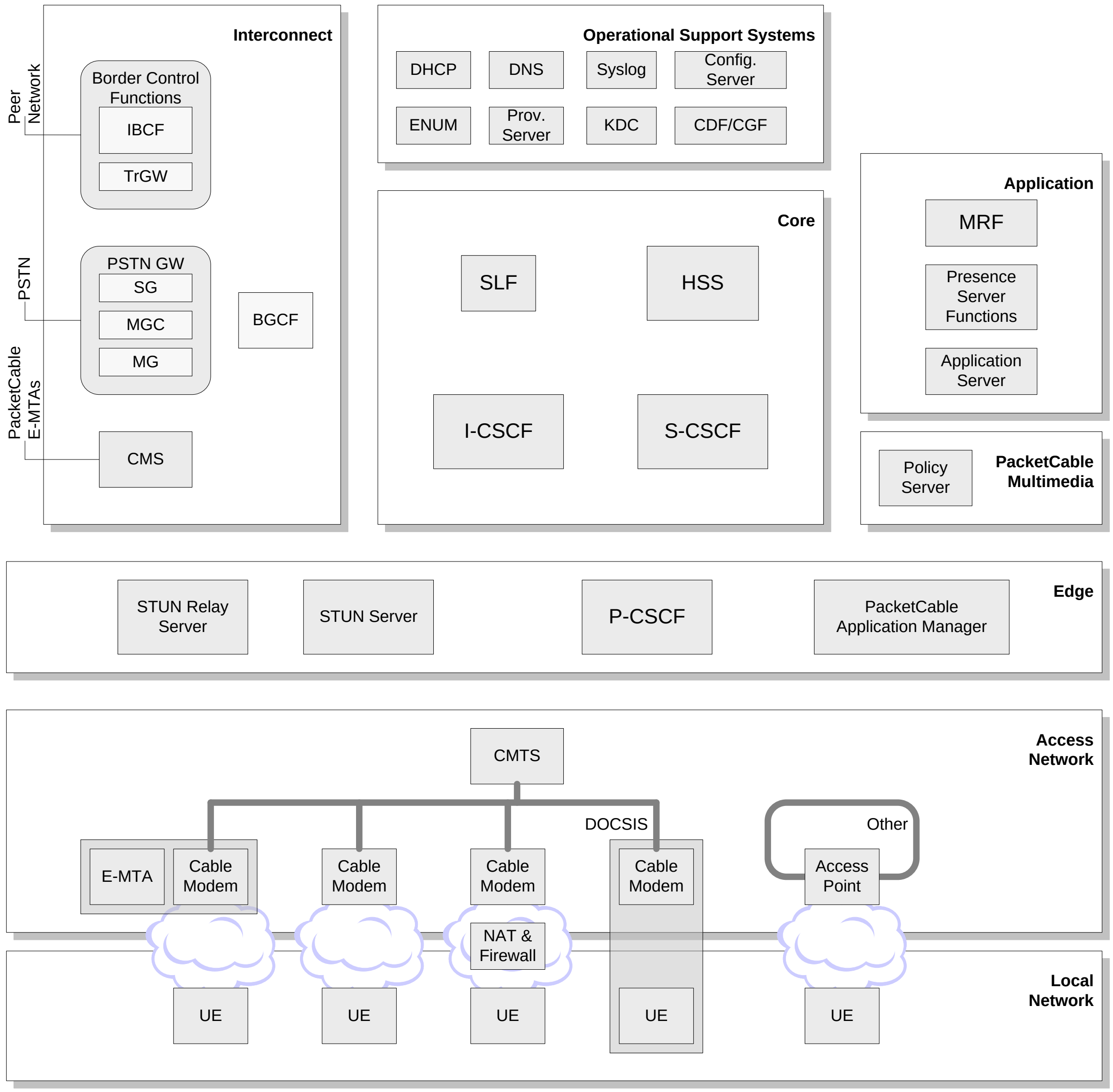

Figure 1 - PacketCable Reference Architecture

The PacketCable architecture is based on the IMS architecture, with the addition of some incremental extensions to support cable networks. These extensions include the use of additional or alternate components, as well as enhancements to capabilities provided by IMS functional components.

Some of the major PacketCable enhancements to the IMS include:

- Support for Quality Of Service for IMS-based applications on cable access networks, leveraging the PacketCable multimedia architecture;
- Support for signaling and media traversal of Network Address Translation (NAT) and Firewall (FW) devices, based on IETF mechanisms;

- Support for the ability to uniquely identify and communicate with an individual when multiple UEs are registered under the same Public Identity;
- Support for additional access signaling security and UE authentication mechanisms for PacketCable UEs;
- Support for provisioning, activation, configuration, and management of PacketCable UEs.

PacketCable includes both the existing IMS logical components and reference points, and logical elements and reference points added to support PacketCable requirements.

For more information refer to the PacketCable Architecture Framework Technical Report [ARCH-FRM TR].

5.3 PacketCable Security Threats

5.3.1 General Threats: Classification and Analysis

Following is an overview of the general threats in the context of a generic IP multimedia communications architecture.

5.3.1.1 Trust Domain Threats

A Trust Domain is a logical grouping of network elements that are trusted to communicate in a manner consistent with a set of relevant security policies. Trust domains can be demarcated by physical or logical boundaries. Communication across trust domains must always be reviewed for authentication and authorization. Interfaces of interest for an IP multimedia infrastructure are:

- Intra-network domain interfaces, which connect network elements within a service provider's domain. A compromise to any network element can be detrimental to the proper functioning of the network itself. Threats involve almost all the ones mentioned in this section.
- Inter-network domain interfaces, which connect two domains. The domains can be different service providers, or the same provider. Inter-domain trust levels can dictate the level of trust one can have within a domain (intra-domain), and hence, it is imperative that such interfaces be secured. Further, the security of two domains connected in such a manner relies on all the other connections established by each individual domain.
- Access domain interfaces, which allow UEs to connect to a service provider. This set of interfaces is highly vulnerable to a multitude of security threats, largely due to the fact that access domains typically contain trusted as well as un-trusted UEs and network elements. Strong authentication for any kind of network access would be vital for a service provider. If authentication is to be foregone, the services offered and the network elements to which such an unauthenticated access is provided should be minimized.

5.3.1.2 Theft of Service

"Theft of Service" refers to a multitude of threats, including but not limited to:

- Manipulation of the UE – UEs, especially software UEs, are vulnerable to Trojan attacks and manipulation of behavior. Mitigation techniques include signed code and embedded UEs.
- Protocol weakness exploitation – Exploitation of weak cryptographic measures can have a large impact, as it typically involves major redeployment. Mitigation techniques include defense in depth architecture.
- Identity spoofing – the act of impersonating another user in order to gain access to services. This can lead to loss of credibility and revenue. Mitigation includes the use of strong authentication and user education.

- UE cloning – the act of imitating a legitimate UE. This is typically an issue when UE identities are deemed sufficient to offer services, such as in architectures without the distinction of a 'user' and a 'client'. The recommendation would be to require UE credentials, to authenticate users before offering services, and to build infrastructures that can identify cloning and mitigate threats.
- Subscription fraud and non-payment of services – subscriptions established with falsified information and detection of non-payment are beyond the scope of this specification.

5.3.1.3 Disruption and Denial of Service

General DoS attacks aim to cause service interruption by crippling some or all service providing entities in the network. These attacks occur at layer 2 through layer 4 of the OSI reference model. Denial of service attacks focus on rendering a particular network element unavailable, using one of several different mechanisms. DoS attacks include:

- Malformed message attacks - an attacker issues malformed messages that attempt to exploit a weakness in the robustness of a stack. Weaknesses include buffer overflows, or insufficient corner case and error handling. Mitigating this attack requires well-designed software protocol stacks and robustness testing.
- Layer four depletion attacks - an attacker causes excessive state information to be consumed on a victim device, often in the context of state-aware protocol stacks. An example is a TCP-level attack such as a SYN flood, used to exhaust stack resources that keep track of session state. These attacks can be mitigated by Intrusion Detection Systems (IDS) and firewalls, and by well-designed software protocol stacks and robustness testing.
- Bearer-level flooding attacks - denial of service attacks that focus on rendering a particular network element unavailable, usually by directing an excessive amount of media network traffic at its interfaces. Preventing this attack requires state-aware firewalls that open pinholes for media only if the trusted side of the firewall initiates the connection first. Flooding attacks often make use of spoofed source addresses to open firewall pinholes. Source address verification through 3-way handshakes can mitigate this threat. Quality of Service (QoS) can also prevent excessive flows through a router.

Flooding attacks generally make use of IP packets with spoofed source addresses. By preventing packets with spoofed addresses, some flooding attacks can be mitigated. There are several mechanisms to prevent address spoofing:

- Use a challenge/response mechanism such as STUN or STUN Relay;
- Use of TCP makes source address verification easier (3-way handshake);
- Unicast reverse path forwarding (uRPF) - uses routing tables to determine whether the route to the source of the packet (the reverse path) is pointing to the interface the packet came in on.

Zombie attacks consist of any type of denial of service attack that is launched from an authenticated endpoint. In addition, most zombie attacks make use of many zombies, resulting in a distributed denial of service attack (DDOS). Typically, a Trojan compromises an endpoint in order to leverage the endpoint's authentication. It is very difficult to defend against a zombie attack, because the endpoint is authenticated and authorized. Zombie attacks can be thwarted by detecting anomalous traffic behavior and filtering malicious traffic.

5.3.1.4 Signaling Channel Threats

In a multimedia environment such as a SIP architecture, signaling messages include data pertaining to identity, services, routing, and other sensitive and critical data. Multimedia components such as proxies exist in the access domain, exposing them to a greater number of threats.

Attacks on signaling security include:

- Compromise of confidentiality - Signaling information, such as the caller identity and the services to which a customer subscribes may be vulnerable to discovery. The caller's identification information may also be used to locate the caller even if the caller wished to keep their location private.
- Man in the middle (MitM) attacks – attacks resulting from the interception and possible modification of traffic passing between two communication parties. These attacks are successful if the communicating parties can't distinguish communications with the intended recipient from those of the attacker. Attacks, some of which are described in other sections, include impersonating a proxy, undesired redirection, and loss of privacy due to MitM intervention.
- Denial of service attacks – DOS attacks in the signaling channel range from the creation of bogus requests resulting in amplification attacks to falsifying routing headers. The use of multicast to transmit SIP requests greatly increases the potential for DOS attacks.

Many of these threats can be mitigated by requiring mutual authentication, identity assertion, confidentiality, and integrity on the signaling plane.

5.3.1.5 Bearer Channel Threats

Threats to the bearer channel relate to the media traffic transferred between communicating parties.

Attacks on Bearer security include:

- Compromise of confidentiality – confidentiality in this sense is protection of the media messages themselves, which could be an audio session, instant messaging, or other multimedia message transfer. Depending on the security mechanism negotiated, end-to-end confidentiality may not be under the control of the sender.
- Compromise of integrity – modification, deletion, and replay are all possible attacks to the bearer channel.
- Disruption attacks – as with any media technology, the ability of parties to communicate introduces unwanted communications. This category includes all the "normal" Public Switched Telephone Network (PSTN) attacks such as harassment, as well as some new threats relating to degradation and disruption of service in the IP model.

Bearer channel attacks are mitigated by requiring mutual authentication, confidentiality, and integrity on the bearer plane to prevent manipulation of data on the bearer plane, and ensuring privacy of sensitive information.

5.3.1.6 Reconnaissance

Well-planned attacks on Service Providers normally start with gaining reconnaissance on a network. Reconnaissance threats can be mitigated by using topology hiding mechanisms, including the introduction of border elements. Enforcing filtering techniques in the access domain allows for traffic policy enforcement at the edge of the network.

5.3.1.7 Roaming Model Considerations

Roaming models can minimize or add to security threats. UEs accessing services through alien environments can expose both the UE and the home network to greater risks. The trust relationship between the home and visited networks is enforced at the inter-domain security boundary.

5.3.2 Protocol Specific Security threats

The following sections highlight threats to multimedia protocols. While this list does not include every multimedia protocol, it includes the major protocols discussed in the architecture and in later sections.

5.3.2.1 SIP

Examples of attacks that can be performed from information gained by capturing SIP messages on the network include:

- Tampering with message bodies (e.g., sending malformed SIP messages to disrupt a SIP network element; sending fake REGISTER messages to cause signaling messages to be redirected, rendering the hijacked UE unable to initiate or accept sessions);
- Tearing down sessions (e.g., sending BYE or CANCEL messages to end a session prematurely);
- Impersonating a server (e.g., sending false INVITEs);
- Masquerading and faking server responses leading to service unavailability or Denial of Service (e.g., Flooding the network with 302 Redirect or 401 Unauthorized messages).

Some of the important vulnerabilities are explained in the following subsections.

5.3.2.1.1 Registration Hijacking

Registration hijacking involves a malicious endpoint that changes the registration of a different, existing endpoint, to point either back to the attacker or to a different location. Registration hijacking can take several forms:

- SIP endpoint cloning - an attacker User Agent (UA) may attempt to register as an existing victim UE. The attacker UE becomes a "clone" of the victim UA, stealing the victim's identity.
- Exploitation of weak identity - if a registrar assesses the identity of a UA, the 'From:' header of a SIP request can be arbitrarily modified and hence open to malicious registration.
- Attackers could de-register some or all users in an administrative domain, thereby preventing these users from being invited to new sessions, resulting in a type of DoS attack.

Refer to section 26.1.1 in [RFC 3261] for more information about Registration Hijacking. The general method to prevent registration hijacking is to use secure identity assertion.

5.3.2.1.2 Faking User Identity

Unless authenticated, SIP messages are vulnerable to identity spoofing. Fields such as 'From:' are not required to be filled and 'P-Asserted-Identity', unless populated by a trusted element securely, can be manipulated.

Possible solutions to mitigate such a threat include:

- Use strong credentials and establish secure tunnels for message flows.
- Use appropriate SIP Identity mechanism like "SIP identity" that supports cryptographically verifiable assertions.

5.3.2.1.3 Malformed SIP Messages

An attacker can issue malformed SIP messages that attempt to exploit a weakness in the robustness of a SIP stack or the protocol itself. Weaknesses include unwarranted DoS initiation, buffer overflows, or insufficient corner case handling. Mitigating this attack requires stack robustness testing. Specific scenarios that lead to DoS attacks include:

- Using falsified Via header fields identifying a targeted host as the originator of the request and then sending these requests to a large number of SIP network elements.
- Using falsified Route headers in a request that identify the target host and then sending such messages to forking proxies that will amplify messaging sent to the target.

SIP proxy servers by nature accept requests from varied IP endpoints and are consequently exposed to an increased number of threats.

5.3.2.1.4 SIP Message Storms

SIP message storms can consist of sending random SIP messages so that memory or processing power is exhausted by exhausting state storage or requiring encryption steps, respectively. SIP message storms can happen either from within a network or from the outside. Mitigation techniques to thwart such attacks include:

- Debugging stacks for resource depletion;
- Use of anti-replay countermeasures;
- Avoiding multiple responses to a single event (e.g., multiple 401 messages for authentication challenge);
- Detecting storms and using appropriate filters to shutdown misbehaving UEs.

Message storms may arise from registration floods, where a large number of endpoints attempt to register, but fail authentication at the edge of the network and bog down the edge proxies. In addition, edge proxies may allow endpoints to register without authentication, and then defer the UE challenge to servers internal to the network, in which case the internal servers are susceptible to DoS floods. There are several ways to mitigate these types of attacks:

- Require authentication at the edge proxies to spread the load of authentication and better defend against registration DoS floods;
- Impose flood-control measures – provide a nonce to UEs that authenticate for the first time, which can be used later, under less strict rate limiting;
- Allow the P-CSCF to prioritize signaling, based on previously successful challenges from the same UE.

5.3.2.1.5 Session Hijacking

Methods of launching a session hijacking attack include the following:

- Modification of SDP information;
- Using messages like "301 moved permanently" to redirect INVITEs to another location (assuming the attacker knows Call-ID, To, From, Cseq fields).

The general method to prevent session hijacking is to require authentication of all SIP messages.

5.3.2.1.6 Impersonating a Server

SIP servers may be impersonated in the network by an attacker. SIP server impersonation can result in a DoS or privacy breach. It presents a possibly greater problem when SIP mobility is considered. The general method to prevent impersonation is server authentication by UAs.

Refer to section 26.1.2 in [RFC 3261] for more information.

5.3.2.1.7 Tampering with Message Bodies

Refer to section 26.1.3 in [RFC 3261] for more information.

5.3.2.1.8 Tearing Down Sessions

Refer to section 26.1.4 in [RFC 3261] for more information.

5.3.2.1.9 Reconnaissance Threats

Certain SIP messages and fields facilitate reconnaissance threats. Mitigation of such threats can be facilitated by preventing the usage of certain fields (e.g., OPTIONS) in messages.

5.3.2.2 STUN

In general, attacks on STUN can be classified into denial of service attacks and eavesdropping attacks. Denial of service attacks can be launched against a STUN server itself or against other elements using the STUN protocol.

Many of the attacks require the attacker to generate a response to a legitimate STUN request, in order to provide the UE with a faked MAPPED-ADDRESS. The attacks that can be launched using such a technique include:

- DDOS Against a Target
- Silencing a UE
- Assuming the Identity of a UE
- Eavesdropping

More detailed information on these attacks and how the threats are addressed by the STUN protocol itself can be found in [RFC 3489].

5.3.2.3 STUN Relay

A STUN Relay server acts as a redirector to funnel media streams through a NAT to a destination. A STUN Relay server therefore has the potential to become a source for a DoS attack that utilizes high-bandwidth media streams. Critical to preventing misuse of a STUN Relay server is a cryptographically verifiable way of establishing an authentication and authorization mechanism to allow recipients of media streams to authorize the STUN Relay server to forward media.

5.3.2.4 TLS

Because Transport Layer Security (TLS) is hop-by-hop, it may be compromised within a server that terminates and re-originates signaling.

TLS also relies on a mechanism to establish trust between two communicating entities, such as a Public Key Infrastructure (PKI) within an administrative domain. TLS establishment between servers should involve mutual authentication.

TLS generally relies on transitive trust for hop-by-hop security. If each endpoint has its own local server, and the servers trust each other, then the endpoints can assume through transitive trust that the end-to-end communication is secure.

5.3.2.5 HTTP Digest

The primary threat posed to HTTP-Digest authentication involves a MitM (man in the middle) attack. HTTP Digest operates by verifying that a user has a pre-shared password. After the UE requests access to a resource, the server challenges the UE for a password. In the challenge, the server sends down a nonce in the clear that should be used by the UE to generate a securely formed hash of the password. The hashed password is sent to the server in the clear. This method of authentication is susceptible to a MitM using a dictionary attack, in an attempt to find a password that results in the same secure hash as the value sent back to the server. Consequently, HTTP Digest should be used over secure data paths.

5.3.2.6 DNS

The Domain Name Service in general is insecure without the use of DNSSEC. Possible security threats include manipulation of request or response queries leading to redirection or denial of service, and usage of Dynamic DNS functionality, if enabled, to manipulate DNS Servers and reflect incorrect topologies.

To mitigate some of these threats, DNS should only be used for general information and other configuration mechanisms, such as authentication, used to validate network elements.

5.3.2.7 Software-based UEs

PacketCable support software-based UEs to authenticate and use network services. Software-based UEs present challenges that lead to vulnerabilities:

- Even though software-based UEs may have a provision to connect to a secure hardware keystore, such as a smart card, they generally store credentials in unprotected storage;
- The software image on a soft UE is not tamper-proof;
- Applications on software-based UEs may store a user's password for later automated entry.

5.4 PacketCable Security Architecture Overview

This section describes the PacketCable Security Architecture, including enhancements to the IMS. The trust domains described in Section 5.3 are used to decompose the PacketCable architecture. Each trust domain is discussed in further detail in the following sections.

5.4.1 Access Domain

UEs connect to the network through the Access domain. Interfaces and components present in the Access domain are shown in Figure 2.

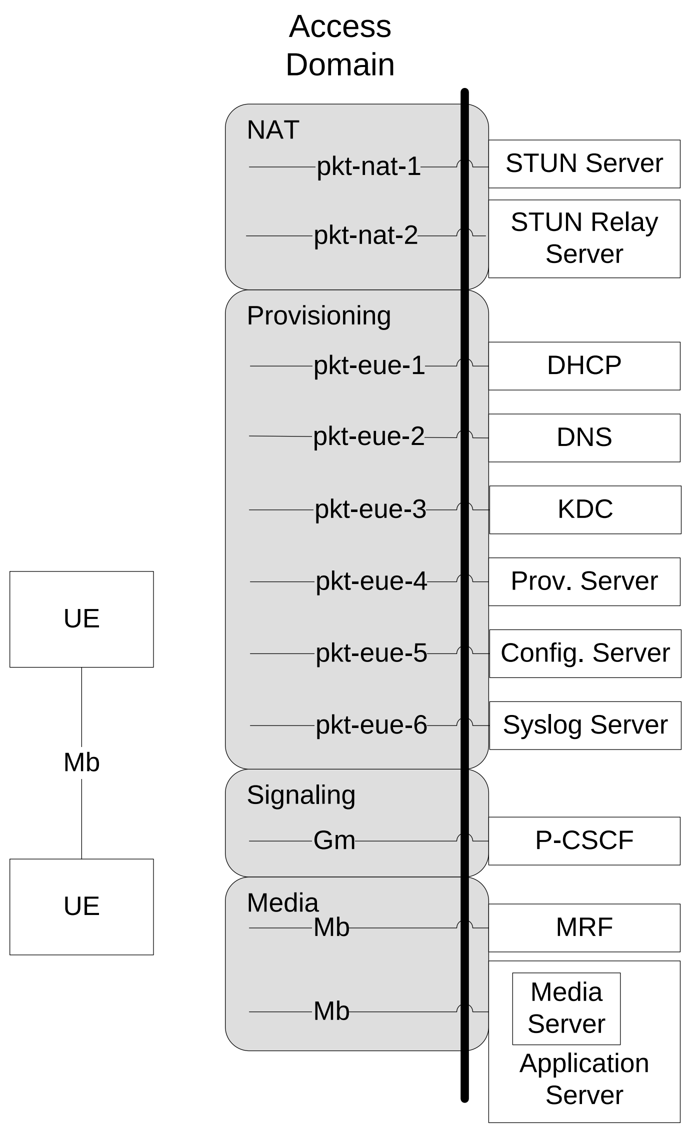

Figure 2 - Access Domain Reference Points

UE interactions with the network occur in the Access domain. Access methods are varied, and include DOCSIS and wireless. Due to these characteristics, the access domain is home to a multitude of threats, as described in Section 5.3.

Table 1 provides a high-level overview of the security architecture that results from the PacketCable enhancements to IMS. Each Access domain reference point, along with the security mechanism employed for that interface, are included.

Table 1 - Access Domain Reference Points Description

Reference Point	PacketCable Network Elements	Reference Point Security Description
pkt-nat-1	UE<->STUN Relay Server	STUN Relay: STUN Relay requests are authenticated and authorized within the STUN Relay protocol itself.
pkt-nat-2	UE – External STUN Server	STUN: Message integrity is provided by STUN mechanisms.
pkt-eue-1	eUE – DHCP	DHCP: Security for this interface is out-of-scope. Security threats are mitigated via follow-on Kerberos procedures in the Secure Provisioning Flow.
pkt-eue-2	eUE – DNS	DNS: Security for this interface is out-of-scope. Security threats are mitigated via follow-on Kerberos procedures in the Secure Provisioning Flow.
pkt-eue-3	eUE – KDC	Kerberos: Authentication, message integrity, and privacy are provided within the Kerberos protocol.
pkt-eue-4	eUE – Provisioning Server	Kerberos, SNMP: Authentication, message integrity, and privacy (optional in SNMPv3) are provided within the Kerberos and SNMP protocols in the Secure Provisioning Flow only.
pkt-eue-5	eUE – Configuration Server	TFTP, HTTP (optional): Message integrity of the configuration file contents, and optional privacy, is provided via pkt-eue-4 signaling in the Secure Provisioning Flow only.
pkt-eue-6	eUE – Syslog Server	Syslog: Security for this interface is out-of-scope.
Mb	UE - UE UE - Media Server UE - MG UE – E-MTA UE - MRF	RTP: Media security is out of scope for this specification.

5.4.2 Intra-Network Domain

Intra-domain reference points and components are contained within a service provider's network, and consequently, a holistic security policy.

IMS defines the security of intra-domain connections with the Zb interface, as described in [TS 33.210]. Within IMS, integrity is required and confidentiality is optional when the Zb interface is implemented. IPsec ESP is used to provide security services for the Zb interface between intra-domain components.

PacketCable Provisioning also requires an interface between the KDC and the Provisioning Server to map the eUE's Mac Address to the assigned IP address and the Fully Qualified Domain Name. Message integrity, authentication, and privacy for this interface is provided within the Kerberos protocol.

Refer to [ARCH-FRM TR] for a description of the varied intra-domain reference points and components.

5.4.3 Inter-Network Domain

Inter-domain reference points connect the operator security domain with external partners and networks. These connections provide interworking between the operator's network and other service providers and networks, including the PSTN. Figure 3 shows the Inter-domain trust boundary.

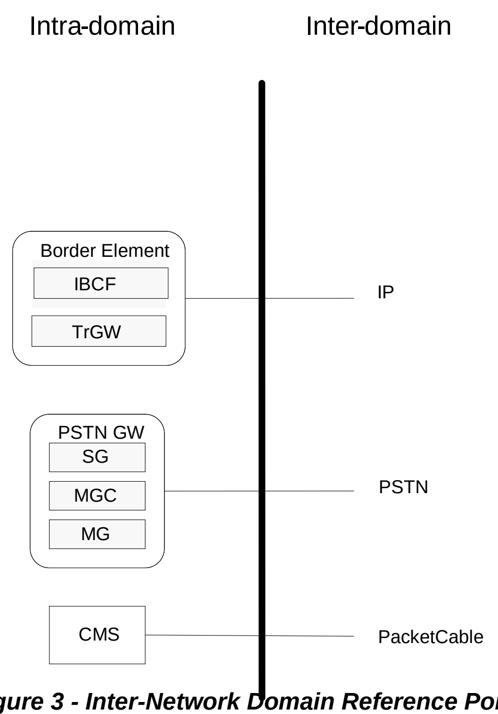

Figure 3 - Inter-Network Domain Reference Points

IMS defines the security of inter-domain connectivity with the Za interface, as described in [TS 33.210]. Both integrity and confidentiality are required for the Za interface, based on IPsec ESP. Inter-domain traffic in IMS is required to pass through a Security Gateway (SEG). The SEG terminates reference point Za IPsec tunnels and enforces security policy on inter-domain traffic flows. Figure 3 shows an architecture including the SEG functionality in the Border Element, but the SEG may be a separate element.

The PSTN Gateway to PSTN reference point is secured using PSTN security mechanisms.

PacketCable adds support for inter-networking to PacketCable networks. The Call Management Server (CMS) provides translation for PacketCable messaging. Security for the CMS reference point is detailed in [SEC].

6 PACKETCABLE SECURITY REQUIREMENTS

The following sections describe the PacketCable enhancements to the IMS security architecture.

6.1 User and UE Authentication

3GPP IMS relies completely on credentials stored in a Universal Integrated Circuit Card (UICC) for access security. The UICC is a platform for security applications used for authentication and key agreement. PacketCable has a requirement to support multiple types of UEs, such as software UEs, that will not contain or have access to UICCs.

[PKT 33.203] describes the IMS approach to authentication and establishing transport security between the UE and the P-CSCF. The IMS uses a combination of IPsec for integrity and optional confidentiality, and IMS-AKA for authentication. To meet the IMS requirements of minimal round trips, the security elements of the negotiation "piggy-back" on the SIP register messaging flow. [RFC 3329] is used to negotiate security between the UE and the P-CSCF, and IMS-AKA [RFC 3310] is used between the UE and the S-CSCF to perform mutual authentication. [RFC 2617] is extended to pass authentication data from the UE to the S-CSCF. The communications between the UE and the P-CSCF and the communications between the UE and the S-CSCF are related in that the keying material for the security associations between the UE and the P-CSCF are computed from the long-term shared secret stored in the Home Subscriber Server (HSS) and the UICC in the UE. Figure 4 shows the high-level message flows for authentication during registration. Some elements and messages are not displayed in order to simplify discussion.

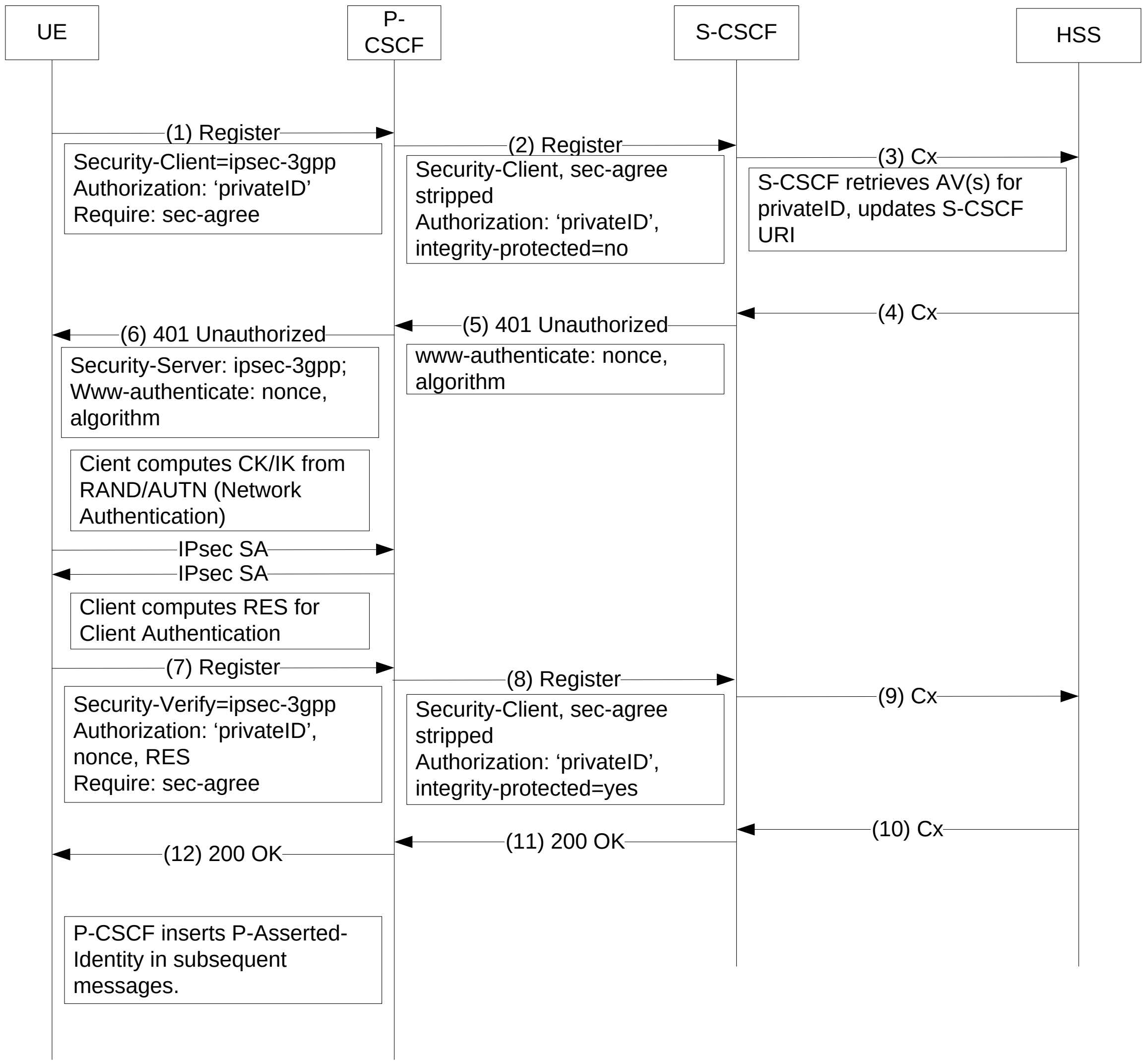

Figure 4 - IMS Registration Message Flow

For authentication during registration, the following basic steps occur:

1. The UE sends a register request to the P-CSCF. The message includes an RFC 3329 Security-Client header, which includes the security mechanisms the UE supports. IMS mandates 'ipsec-3gpp'. The message also includes an authorize header which includes the private identity of the subscriber.

2. The P-CSCF strips the security agreement headers, inserts 'integrity-protected=no' in the authorized header, and forwards the register request to the appropriate I-CSCF, which forwards the request to the appropriate S-CSCF of the subscribers home network.

3. The S-CSCF contacts the HSS to update the S-CSCF URI for that user, and if necessary, request one or more authentication vectors.

4. The HSS returns one or more authentication vectors if requested. The authentication vectors provide the necessary data for the S-CSCF to create a www-authenticate header and challenge the user.

5. The S-CSCF creates and sends a SIP 401 (Unauthorized) response, containing a www-authenticate header that includes a challenge. This response is routed back to the P-CSCF.

6. The P-CSCF strips the integrity key (IK) and the confidentiality key (CK) from the 401 response to use for IPsec SAs between the P-CSCF and the UE, and sends the rest of the response to the UE.

7. Upon receiving the challenge message, the UE determines the validity of the received authentication challenge. The UE sets up security associations with the P-CSCF using the IK and CK that was derived from the data sent by the HSS, utilizing the long-term shared key in its UICC. The UE then calculates a response (RES) and sends a second register request with an Authorization header including the challenge response. This message includes Security-Verify headers as per [RFC 3329].

8. The P-CSCF strips the security agreement headers, inserts 'integrity-protected=yes' in the authorize header, and forwards to the appropriate I-CSCF, which forwards to the appropriate S-CSCF.

9. The S-CSCF compares the authentication challenge response received from the UE with the expected response received from the HSS. If they match, the S-CSCF updates HSS data using the Cx interface.

10. The HSS provides the S-CSCF with subscriber data over the Cx interface, including service profiles, which contain Initial Filter Criteria.

11. The S-CSCF forwards a 200 OK response to the UE. The 200 OK contains a P-Associated-URI header, which includes the list of public user identities that are associated to the public user identity under registration.

12. The P-CSCF forwards the 200 OK to the UE. Because the user has now been authenticated and there is an existing security association between the P-CSCF and the UE, the P-CSCF inserts a P-Asserted-Identity header in all subsequent messages from that UE.

PacketCable has requirements to support UEs and authentication schemes not considered in the IMS architecture, as well as additional transport security mechanisms. PacketCable enhances the IMS specifications in several areas in order to support these requirements.

6.1.1 Description

The PacketCable architecture supports the following authentication mechanisms:

- IMS AKA
- SIP Digest Authentication
- Certificate Bootstrapping

The architecture must also accommodate UEs with multiple authentication credentials. For example, a UE may have a certificate for accessing services while on a cable network, and a UICC for accessing services while on a cellular network.

A subscriber may have multiple credentials. A subscriber may have multiple UEs, with different capabilities related to those credentials. For example, a subscriber may have an MTA with a certificate for home use, and a UICC-based UE for traveling.

6.1.1.1 IMS AKA

IMS AKA authentication with UICC credentials will continue to operate as described in 3GPP specifications.

6.1.1.2 SIP Digest Authentication

IMS also supports SIP authentication, which is also described in [PKT 33.203]. SIP authentication uses a challenge-response framework for authentication of SIP messages and access to services. In this approach, a user is challenged to prove their identity, either during registration or during other SIP dialogues initiations.

SIP authentication is handled in a similar manner to IMS AKA, and follows [RFC 3261] and [RFC 2617]. This approach minimizes impact to the existing IMS authentication flow by maintaining existing headers and round trips. Unlike IMS AKA, however, challenges are not precomputed. In order to maximize the security of SIP Digest authentication, cnonces and qop "auth" directives are used, which requires challenges to be computed in real-time at the S-CSCF.

Figure 5 shows the message flow for SIP-based authentication during a registration.

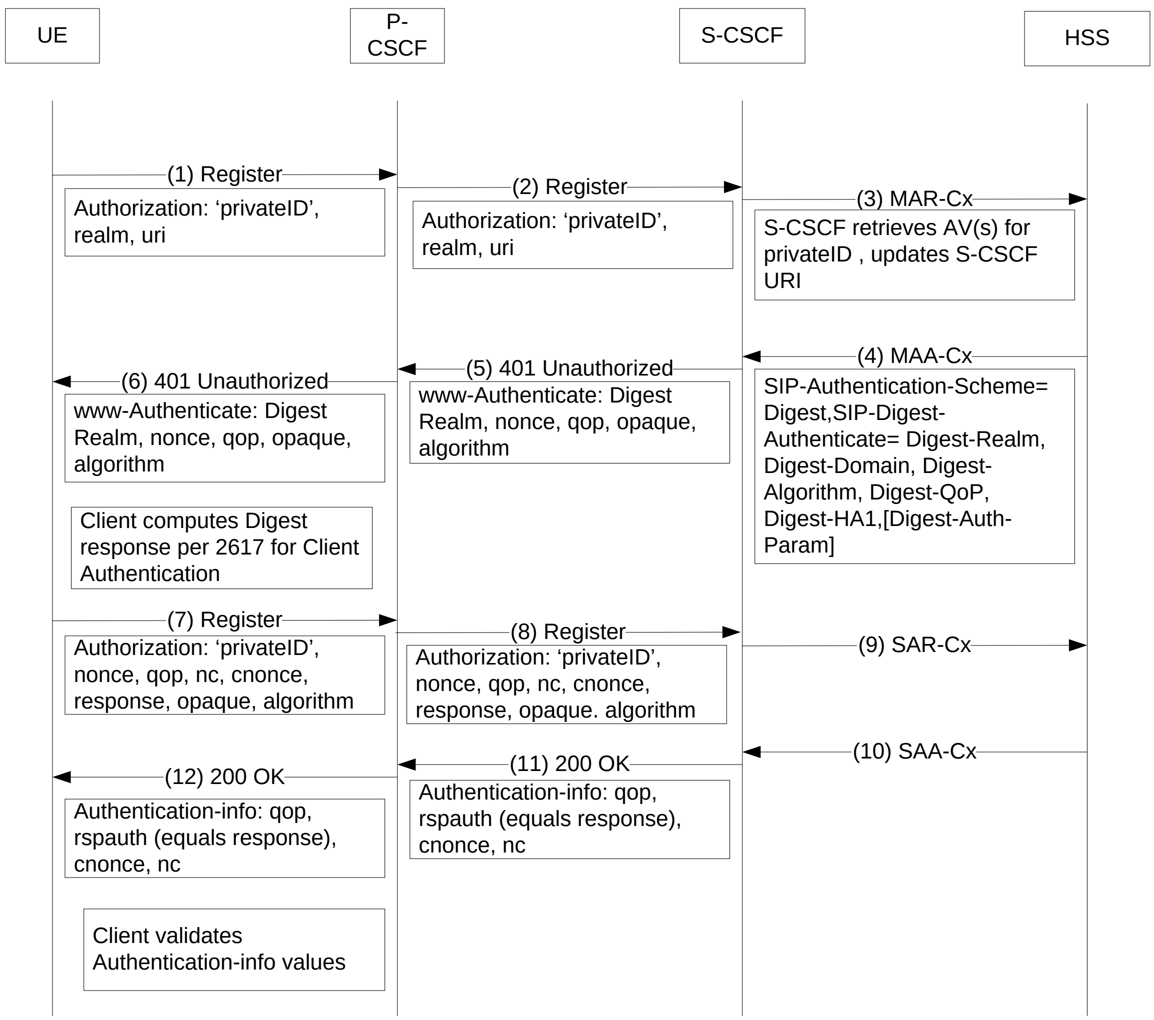

Figure 5 - SIP Digest Authentication

For SIP Digest authentication during registration, the following basic steps occur. [RFC 3329] headers and other SIP header content is not shown for simplicity.

1. The UE sends a register request to the P-CSCF. The message includes an Authorization header, which includes the private identity of the subscriber. An example authorization header is shown below:

```
REGISTER sip:home.atlanta.com SIP/2.0
Authorization: Digest username="alice_private@atlanta.com",
      realm=" atlanta.com", nonce="", uri="sip:home.atlanta.com",
      response=""
```

2. The P-CSCF forwards the register request to the appropriate I-CSCF, which forwards the request to the appropriate S-CSCF of the subscriber's home network.

3. The S-CSCF contacts the HSS using a MAR command towards the HSS on the Cx interface. The MAR message includes the private identity of the subscriber, the S-CSCF information, and the number of authentication vectors requested. This information is used by the HSS to update the S-CSCF URI for the private identity and to deliver the correct authentication vector information to the S-CSCF.

4. The HSS returns an MAA message on the Cx interface. The MAA message includes the public identities and authentication vectors for that subscriber. The contents of the authentication vector for SIP Digest are detailed in a later section. The main differences are the lack of a CK and IK, and the contents of the SIP-Authenticate data element. Instead of AKA data, the SIP-Authenticate AVP contains data the S-CSCF requires for computing a Digest response, primarily HA1.

5. The S-CSCF creates a SIP 401 (Unauthorized) response, which includes a challenge in the www-authenticate header field and other [RFC 3261] fields. An example header is shown below:

```
SIP/2.0 401 Unauthorized
      WWW-Authenticate: Digest realm="atlanta.com",
        nonce="CjPk9mRqNuT25eRkajM09uTl9nM09uTl9nMz5OX25PZz==",
        qop=auth, opaque="5ccc069c403ebaf9f0171e9517f40e41",
              algorithm="MD5"
```

6. This response is routed back to the I-CSCF, then the P-CSCF, and then to the UE.

7. Once the UE receives the challenge, the UE calculates the response based on items in the WWW-Authenticate header and additional items (e.g., cnonce) generated by the UE. The values in the Authorize header are calculated as per [RFC 3261] and thus [RFC 2617]. The UE sends a second register request with the Authorization header. An example Authorization header is shown below:

```
REGISTER sip:home.atlanta.com SIP/2.0
      Authorization: Digest
              username="alice_private@atlanta.com", realm="atlanta.com",
              nonce="CjPk9mRqNuT25eRkajM09uTl9nM09uTl9nMz5OX25PZz==",
              uri="sip:home.atlanta.com", qop=auth, nc=00000001,
              cnonce="0a4f113b", response="6629fae49393a05397450978507c4ef1",
              opaque="5ccc069c403ebaf9f0171e9517f40e41", algorithm="MD5"
```

8. The P-CSCF forwards the message to the appropriate I-CSCF, which forwards to the appropriate S-CSCF.

9. Upon receiving the second register from the UE, the S-CSCF calculates the challenge in the same manner as the UE, in order to compare the two results and thus authenticate the subscriber. Using parameters from the HSS such as HA1, and the parameters from the Authorization header such as cnonce, the S-CSCF computes the challenge response as per [RFC 3261] and thus [RFC 2617]. The computation is performed in a manner consistent with the qop parameter with the value of 'auth'.

   If the two challenge results are identical, the S-CSCF performs a SAR procedure on the Cx interface, informing the HSS the user is registered and requesting the user profile.

10. The HSS returns a SAA message to the S-CSCF containing the user profile, which includes, among other things, the collection of all the Public User Identities allocated for authentication of the Private User Identity, as well as the initial filter criteria.

11. The S-CSCF sends a 200 OK response to the register request. The response includes an Authentication-Info header, which allows the UE to authenticate the network, or S-CSCF. The rspauth value is calculated per [RFC 2617]. The 200 OK message is forwarded to the UE. An example Authentication-Info header is shown below:

```
SIP/2.0 200 OK
        Authentication-Info:
        qop=auth, rspauth="7729fae49393a05397450978507c4ef1",
        cnonce="0a4f113b",nc=00000001,
        nextnonce="8829fae49393a05397450978507c4ef1"
```

12. The 200 OK is routed to the appropriate P-CSCF, and then to the UE.

13. The UE validates the rspauth value, to authenticate the network, or S-CSCF.

Because the user has now been authenticated and there is an existing security association between the P-CSCF and the UE, the P-CSCF inserts a P-Asserted-Identity header in all subsequent messages from that UE. In the case that signaling security is disabled, the S-CSCF inserts P-Asserted-Identity after successful authentication.

Adding support for SIP digest impacts the IMS specifications in the following ways:

- New digest algorithms are allowed to be present in the www-authenticate and Authorization headers.
- The HSS must compute and store new types of data elements.
- UEs must be able to support and compute new types of digest responses.
- The home network (or S-CSCF) authenticates to the UE by including an Authentication-Info header in the 2xx response following a successful authentication of the UE.

Impacts to specific components are discussed in Section 6.1.2.

6.1.1.3 Certificate Bootstrapping

PacketCable embedded UEs (eUEs) contain digital certificates, however SIP [RFC 3261] does not define an authentication solution for certificates. PacketCable defines procedures for the UE to bootstrap IMS credentials using an X.509 certificate. This is termed Certificate Bootstrapping.

The eUE connects to a Certificate Bootstrapping Server and performs mutually authenticated TLS procedures. Once completed, the eUE is provided with IMS Credentials. The eUE can then authenticate through normal registration procedures using the bootstrapped credentials.

6.1.2 Impacted Components

The following sections describe the impacts to IMS components in order to accommodate PacketCable authentication requirements.

6.1.2.1 UE

PacketCable UEs supporting Digest authentication must conform to [RFC 3261], and thus RFC [RFC 2617]. Upon receiving a challenge from the S-CSCF in a 401 Unauthorized message, UEs must create an Authorization header including a challenge response as described in [RFC 2617] based on the algorithm parameter in the www-Authenticate header. Cnonce and nc parameters must be included in the challenge response. UEs must be able to validate Authentication-Info header values returned from the S-CSCF with the 200 OK message.

UEs must be able to securely store usernames and passwords in a manner that minimizes risk. UEs may optionally prompt users for username and password input.

6.1.2.2 S-CSCF

In order to support SIP Digest, the S-CSCF must be able to calculate Digest responses as described in [RFC 3261] and [RFC 2617]. The S-CSCF will receive HA1 from the HSS over the Cx interface, and the S-CSCF must use this HA1 value to create the digest response for this private identity. This response is compared to the response received by the UE, so it must be calculated in the same manner. If the S-CSCF calculated response is identical to the response received from the UE, the S-CSCF sends a 200 OK containing an Authentication-Info header per [RFC 2617].

Based on local policy, the S-CSCF should:

- Accept a previously used nonce with a valid nonce-count, for example, to allow for PRACK and other types of requests received before a 2xx response.
- Only accept a previously used nonce for a specific period of time. It is recommended to use a time value of 10 minutes or less.
- Only accept a previously used nonce for a specific number of times. It is recommended to use a value of 5 times or less.
- Accept an old nonce based on the above policy rules even if nextnonce was sent.

The above policy rules are mainly related to the case where signaling security is disabled in the network.

6.1.2.3 HSS

In order to support new authentication schemes, the Cx interface and procedures must be extended. Digest authentication adds new parameters to the Cx interface, specifically the SIP-Auth-Data-Item AVP present in both MAR and MAA procedures. The authentication vector provides the S-CSCF with HA1 and other elements to allow the S-CSCF to compute responses. For further details, see [HSS TR].

6.1.3 Signaling Security

The IMS defines IPsec and TLS for the secure signaling between UEs and edge proxies. The UICC provides credentials for authentication and IPsec. The security mechanism is negotiated using [RFC 3329] SIP Security Agreement. TLS as an option for signaling security between the UE and the P-CSCF. The use of TLS by the UE is optional, and is based on the following advantages:

- TLS is the recommended security mechanism specified in [RFC 3261].
- There is a general shift towards the use of TCP to better handle longer messages.
- TLS supports NAT traversal at the protocol layer.
- TLS is implemented at the application level instead of the kernel level, which provides some advantages such as easier support in multiple environments.

Adding support for TLS for signaling leads to the consideration of TLS credentials.

- Mutually Authenticated TLS - UE and server both provide certificates when establishing signaling security. The server must validate the UE certificate, and the UE must validate the server certificate. Mutual authentication provides a high degree of security.
- Server Side Authentication – Only the sever provides a certificate when establishing signaling security. This approach avoids the extra computational overhead of a PKI operation on the UE. Provides a medium level of security, with lower CPU requirements on the UE. May be used to secure HTTP Digest sessions.

Both of these models require the P-CSCF and the UE to support PKI features, such as certificate validation and certificate management. As not all UEs utilize certificates, only server-side authentication is supported in PacketCable.

Adding support for TLS also leads to the consideration of TLS port assignments and TLS connection management. PacketCable will use the standard SIP ports for UDP, TCP, and TLS as defaults. UEs negotiating TLS connect to the SIPS port of 5061. Otherwise, UEs use the standard SIP UDP/TCP port of 5060. Operators may configure other ports for requests. Requests and responses are performed according to procedures in [ID SIP-OUTBOUND].

Figure 6 shows signaling security negotiation during a successful register dialogue. Only signaling security headers are shown for simplicity.

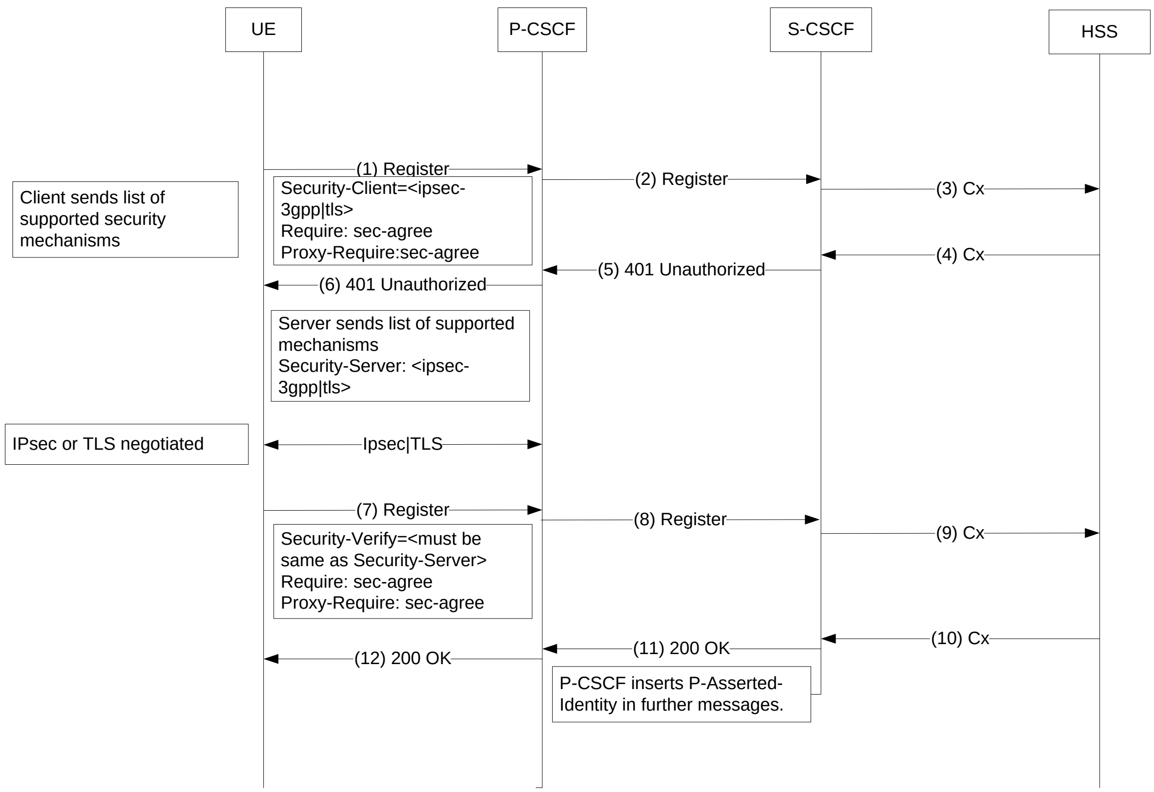

Figure 6 - Transport Security

To support TLS for signaling security between the UE and the P-CSCF, the IMS specifications must be enhanced to allow TLS as an optional SIP security mechanism to be negotiated. [RFC 3329] includes TLS as a security mechanism that can be negotiated; thus the only change is to IMS specifications.

At a high-level, the impacts to IMS components are:

- UE must support the ability to negotiate TLS using [RFC 3329];
- P-CSCF must support the ability to negotiate TLS using [RFC 3329].

6.1.3.1 Impacted Components

The following sections describe the impacts to IMS components in order to negotiate signaling security.

6.1.3.1.1 UE

In order to support the negotiation of signaling security, PacketCable UEs must support TLS as defined in [RFC 2246].

UEs must support the construction and interpretation of [RFC 3329] headers containing the mechanism-name of 'tls'.

6.1.3.1.2 P-CSCF

The P-CSCF must be able to establish TLS sessions based on a request from a UE. The P-CSCF must not request UE certificates, as not all UEs will have certificates. If TLS is established, the P-CSCF must set integrity-protected=tls-pending in Authorization headers for the second REGISTER of an initial registration, and integrity-protected=tls-yes in Authorization headers for re-registrations performed over existing TLS sessions. If TLS is not established, the P-CSCF does not include an integrity-protected header. These rules are in addition to the existing rules for IPsec establishment.

The P-CSCF must support the [RFC 3329] mechanism-name of 'tls'. The same rules for assigning integrity-protected values apply as above.

Certificates should be validated according to [RFC 3280].

6.1.3.1.3 S-CSCF

The S-CSCF can challenge any SIP message. Messages containing Authorize headers with no integrity-protected parameter should be challenged, as this flag indicates the lack of signaling security between the UE and the P-CSCF on non-initial register requests. If the S-CSCF successfully challenges a subscriber, the S-CSCF must insert the P-Asserted-Identity header in subsequent messages from that subscriber if the P-Asserted-Identity header does not exist.

6.1.3.2 Disabling Signaling Security

While not recommended, signaling security may be disabled at the P-CSCF. By disabling signaling security, UEs and the network are exposed to many of the threats described in Section 5.3, especially when combined with a weaker form of authentication, such as SIP Digest.

When TLS is not used with SIP Digest, the P-CSCF creates an IP association, which maps the IP address and port used during registration to the public identities provided by the S-CSCF. This information is used to police subsequent requests (e.g., INVITEs) to ensure only authorized SIP identities are used.

The PacketCable SIP Signaling Technical Report [SIP TR] and the PacketCable [PKT 24.229] delta specification contain detailed information on the procedures for disabling signaling security. The major difference in procedures for disabling signaling security is non-register dialog requests should be challenged and IP associations are used to add an additional layer of security.

6.2 Identity Assertion

PacketCable environments require a way for trusted network elements to convey the identity of subscribers to other elements or services, and to remove the identity when communicating with untrusted networks. Identity assertion is the mechanism by which elements and services can trust the identity of a user.

As described in [PKT 24.229], IMS assigns the task of identity assertion to P-CSCFs for all SIP messages, based on the strict flow described in Section 6.1. Once the IPsec Security Associations (SA) are established and the subscriber is authenticated, the P-CSCF asserts the identity of the subscriber. By monitoring SIP messaging towards the UE, the P-CSCF observes the 200 OK message from the subscribers S-CSCF. This information, plus the presence of SAs to the UE, allow the P-CSCF to substantiate successful authentication of the UE.

PacketCable enhances IMS with the following requirements:

- A P-CSCF with an established TLS session or IP association with a UE that observes a 200 OK response from the S-CSCF for that subscriber can assert the identity of the public identity used by that UE.

6.3 NAT Traversal Security

The following sections describe STUN and STUN Relay security.

6.3.1 STUN

The STUN protocol [RFC 3489] defines the countermeasures for the attacks described in Section 5.3.2.2. These include network architecture recommendations as well as message integrity mechanisms provided by STUN itself. No additional mechanisms are proposed for this version of the Technical Report.

6.3.2 STUN Relay

The STUN Relay server represents a network resource that is utilized for the duration of a connection, therefore security for this resource is an important consideration.

The STUN Relay protocol [ID TURN] defines the countermeasures for the attacks described in Section 5.3.2.3. These include network architecture recommendations as well as message integrity mechanisms provided by STUN Relay itself. No additional mechanisms are proposed.

Note: Security for STUN Relay is being updated. Details will be provided once the STUN Relay draft becomes available.

6.4 Configuration Security

Configuration Security for embedded UEs is provided only in the Secure Provisioning Flow. It is accomplished by establishing SNMPv3 via the Kerberos protocol with PacketCable-specific PKINIT extensions. This provides authentication, message integrity, and optionally privacy.

6.5 Management Security

In order to provide security protection for management information for devices that are not behind NATs, the User-based Security Model (USM) [RFC 3414] and the View-based Access Control Model (VACM) [RFC 3415] features of SNMPv3 are supported. USM provides authentication, integrity, and privacy services for SNMP through the specification of two cryptographic functions: authentication and encryption. VACM provides further security protection to management information by controlling access to managed objects.

6.6 Secure Software Download

Secure software download is out-of-scope for this version of the Technical Report.

6.7 Media Security

Media security is out-of-scope for this version of the Technical Report.

6.8 Certificate Validation

[RFC 3280] should be used for guidance on validation of certificates.

6.9 Certificate Revocation

Certificate revocation is out-of-scope for this version of the Technical Report.

Appendix I Open Issues

- STUN Relay security needs to be updated when new STUN Relay draft is issued.
- Secure Software Download and Media Security sections need to be updated.

Appendix II Acknowledgements

This Technical Report was developed and influenced by numerous individuals representing many different vendors and organizations. CableLabs hereby wishes to thank everybody who participated directly or indirectly in this effort.

CableLabs wishes to recognize the following individuals for their significant involvement and contributions to the V01 Technical Report:

Sumanth Channabasappa - CableLabs

Scott Firestone - Cisco

Wassim Haddad - Ericsson

Louis LeVay - Nortel

Nhut Nguyen - Samsung

Jim Stanco - Siemens

Steve Dotson - CableLabs

Stuart Hoggan - CableLabs