A Comprehensive and Flexible Security Concept for CDNs in Heterogeneous Environments

Rainer Falk, Anja Jerichow, Manfred Schäfer

***Abstract*—A major goal of the European project "mCDN" is the enhancement of Content Delivery Networks (CDNs) for secure multimedia content discovery and delivery that is very well suited for converged fixed-mobile environments. This is achieved by introducing specific Web service components such as personalization, optimal content placement and discovery, peer-to-peer solutions, and comprehensive security services.**

In this paper, a flexible security concept for CDNs developed currently by the mCDN project is presented. CDNs deal with an arbitrary mix of wired and wireless network technologies, heterogeneous devices, and diverse usage environments. An integrative, all-embracing, scalable, and centralising security approach has been designed allowing to protect various shapes of CDNs with varying demands for security.

***Index Terms*—Security, Content Delivery Networks, CDN, Web Services, AAA**

I. Motivation

A. Functionality of a CDN and Security Concerns

The initial idea behind Content Delivery Network (CDN) concepts is to boost the traffic efficiency of content. This is realised by replicating content in caches or edge servers, and re-directing the end user to a close edge node to obtain the content from there instead of a central origin server.

The basic functionality of a CDN is shown in Fig. 1, addressing content and metadata distribution, retrieval, search, and request, pointing out the enhancements developed by the European project mCDN [1]. When realising these features in future networks, the increasing convergence of fixed and mobile communication must be considered. For example, content may need to be adapted for mobile devices, bandwidth limitations must be considered. Essential security concerns of CDN comprise:

– The correct operation of the CDN, i.e. to insert and maintain content or metadata in the CDN system and to administer CDN nodes only by agreed and allowed processes.

This work is supported by the European Commission. We would like to express our gratitude for the financial support and sponsoring of the mCDN project, which is part of the 6th IST Framework Program.

Rainer Falk, Anja Jerichow, Manfred Schäfer are with Siemens, Corporate Technology, 81730 Munich, Germany (e-mail: rainer.falk@siemens.com, anja.jerichow@siemens.com, manfred.schaefer@siemens.com).

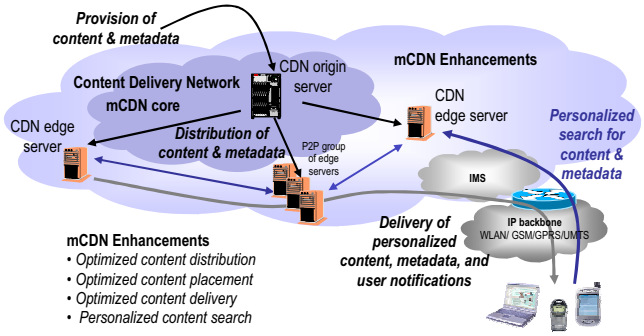

Fig. 1. Principal Architecture and Functionality of a CDN

– The proper delivery of desired content or metadata to prevent that a user gets delivered different data than the one requested.

– The prevention from any fraudulent use, e.g. obtaining content without having required subscription.

B. Security in the European Project mCDN – A flexible Approach suitable for heterogeneous Environments

The main goal of the mCDN project is enhancing traditional CDNs for multimedia content discovery and delivery in mobile and fixed environments by introducing Web service components for personalisation, optimal content placement and discovery, and peer-to-peer solutions and therefore optimizing the process for content distribution and content retrieval. Open solutions based on open interfaces are developed that enable the interaction of the different components at network and service layers and will therefore allow a faster reaction to changing market demands and developments. The novel inter-layering approach of mCDN improves the services that CDN platforms can offer.

Specifically, networks with an arbitrary mix of wired and wireless network technologies, various devices such as PDAs, PCs, and mobile terminals, and diverse usage environments as a closed enterprise CDN or a public operator-provided CDN have different, challenging security implications. Reflecting this, we present a flexible security approach for mCDNs that realises an all-embracing, scalable, and centralising security concept suitable to protect a variety of mCDN types satisfying their diverse demands for security.

C. Overview

This paper summarises the related results achieved during the first year of the EU project mCDN [2]. In Sect. II, we briefly describe the state of the art in CDN security. Sect. III introduces the components of the mCDN architecture. Sect. IV presents mCDN security requirements and Sect. V discusses the security concept. Sect. VI concludes.

II. State of the Art Security in CDNs

From the security point of view, the main focus of current CDNs is on authentication, authorization, and accounting (AAA). The AAA requirements for a CDN are driven by the need to ensure authorization of the client (user), publishing server or administrative server, and to perform accounting. Though the AAA aspect of security is considered important, security recommendations are barely given since the implementation of a balanced end-to-end security architecture is difficult, expensive, and time consuming [3]. However, since security solutions are an increasingly central concern of many sites, CDN providers such as Akamai [4] and Speedera [5] now start to offer security as a proprietary value-added service [6].

Authentication and authorisation are two crucial aspects. Though e.g. the use of digital certificates provides an authentication solution, in addition an appropriate authorisation infrastructure is required. Additionally, privacy aspects must be taken into account. This applies in particular if personalised and localised content adaptation services are offered. [7] proposes a certificate-based framework for secure content adaptation as well as authentication and authorisation to allow end-points to delegate authority to content distributors and to securely handle personal user information.

III. mCDN Architecture and Components

Usually, a complete CDN solution is offered by a single CDN provider. In contrast, mCDN offers open solutions for components and their seamless inter-working as well as for "opening" the isolated layers of legacy CDNs.

To offer the functionality of an open architecture capable to provide secure, personalised, user-friendly, and optimised content distribution and retrieval, new components are necessary and their mutual interactions must be based on open APIs. The term "open" usually refers to a publicly available API. In addition, we couple the term "open" with the inter-layered structure of the envisioned architecture and the different roles and responsibilities of the involved actors.

Fig. 2 shows the functionality of a mCDN as an interlayer architecture. Personalization, optimised content placement, distribution and retrieval can be structured into layers, while security will affect all the different layers [8].

The components of the mCDN architecture relevant for the understanding of the security concept are listed according to the inter-layered framework as follows.

– Content service layer: Aggregator (AGG), Personalisation and Profiling System (PPS), Security Server (SEC), and other

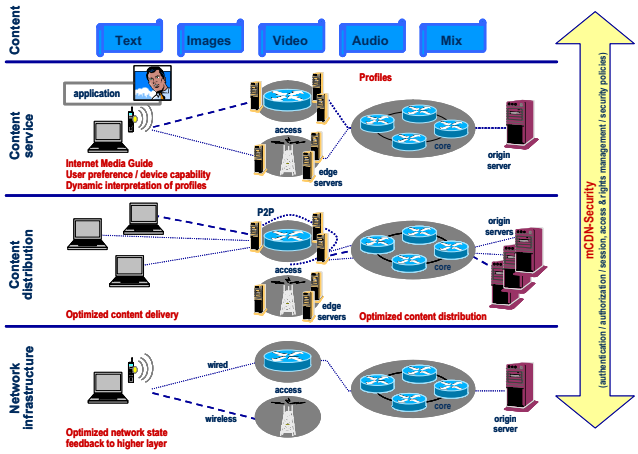

Fig.2. mCDN Interlayered Architecture

services are present at this layer. AGG acts as gate and multiplexer for mCDN users and components. All interactions are intercepted by the AGG and (re-)directed to other mCDN components. PPS provides all functionality for explicit and implicit personalisation. SEC represents a logical component to provide requested security functions. It can be regarded as a conceptual component that may be realised either centrally or distributed.

– Content distribution layer: Edge Server (EDS), Origin Server, Internet Media Guide (IMG), and the Optimal Content Placement (OCP) component are located at this layer. As the names suggest, Origin is the basis of all content and EDS the physical location of the content at the edge of the mCDN. IMG provides search, look up, subscription for metadata/content. OCP stores and locates the content at the optimal EDS.

– Network infrastructure layer: hosts network services such as Network Feedback Services and Optimal Route Selection.

IV. Security Requirements

The mission of security is taking control over desired and undesired, in particular malicious, actions. Security deals with the identification of actions that are permitted for authorised entities and with services and mechanisms that ensure that actions not allowed cannot take place.

On a single, central content server, security objectives can be satisfied by user authentication, enforcing access control to content, and protecting cryptographically the communication channel and/or the content itself. The more challenging case of distributed, open, and heterogeneous CDN technology as specified in the mCDN project includes personalisation according to user preferences and profiles and network feedback, the distribution of more valuable content, and the delivery to heterogeneous devices, but also peer-to-peer, CDN federation and DRM integration. This results in challenging security requirements. It requires a flexible federated user management and user identification, appropriate session management, consideration of privacy aspects, service and content specific access management as well as integrity and content protection for a distributed CDN with scalable,

adaptive security. Beside the interface to the end user, further interfaces have to be protected, e.g. the interface towards content provider or for CDN administration. Providing an adequate security concept for the technology investigated as part of the mCDN project is an area where so far not much specific work has been published.

Fundamental security objectives focused in the following sections are confidentiality, integrity, authenticity and non-repudiation. Other important security objectives are availability and accounting. For a real mCDN system, some of these objectives may not be relevant, depending on the particular usage environment and risk situation. This is taken into account by the scalable mCDN security concept.

V. The mCDN Security Concept

A. Assumptions

In many cases, mCDN security will not be deployed from the scratch, but an already existing security infrastructure shall be re-used. To deal with these demands, a modular and scalable approach is needed for security that can be applied to different usage environments. The centralising solution as introduced here offers unified and harmonised security services that are specific to the mCDN environment. In case of CDN federation, the security components of the involved CDNs cooperate to map in particular (user) identifiers and granted rights.

It is assumed that there exist trust relationships between servers, cashes, firewalls, proxies, network administration, etc. whereas many security requirements can be mapped onto the managed infrastructure hosting the mCDN. In contrast, mCDN users (end-users and content providers) and federated mCDNs are not part of the trusted mCDN part. Users may have unknown equipment and they may connect to the managed mCDN from any location. In particular, user clients are not part of the managed (i.e. trusted) mCDN and the client interface may be threatened by unauthorised access and even by eavesdropping attacks.

B. mCDN Security Architecture

Fig. 3 shows the architectural view concerning security services and related interactions with the Security Server being part of the managed mCDN, thus it is located within a 'trusted' part of the mCDN environment.

The aggregator plays an important role for the security services as typically AAA (or other security related) requests and responses are passed through it. It acts as a mediator to the mCDN core network and to the SEC component and to clients and has two security interfaces: The External Security Interfaces (ESI) interacting with the client site and the Internal Security Interface (ISI) talking with the SEC Security Server.

Depending on the scenario attackers may threaten the ESI communication. Via ISI no additional communication security is required since it is part of the trusted mCDN environment.

AGG acts as an enforcement point for security related interactions with internal mCDN network elements, such as

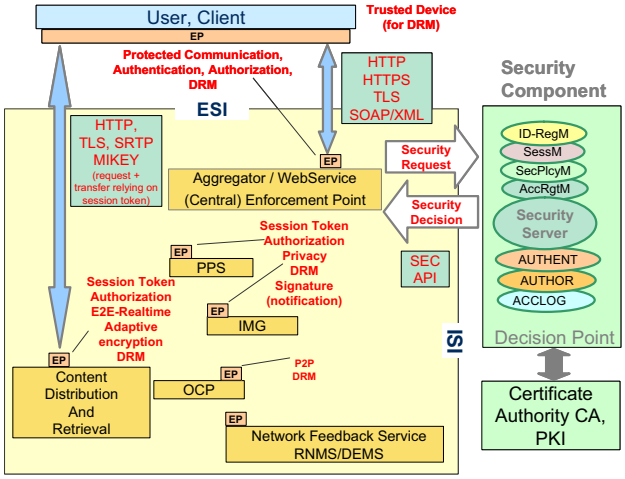

Fig. 3. Security Interactions

IMG, PPS, and content distribution and retrieval procedures. It has to transform internal requests (e.g. those requiring AAA decisions) into security requests and sends them to SEC, which acts as the decision point accepting or refusing the initiating requests. In case that security requests come directly from mCDN elements, AGG transmits them transparently.

The security related control of AGG's behaviour follows higher-order security policies (e.g. crypto protocols, formats, and parameters to be used). The other network elements may also be 'locally' involved in security interactions, depending on the distributed security policies. For that reason they may have to implement an (entity specific) enforcement point (EP) as well.

SEC itself will autonomously interact with other security entities, e.g. a CA for PKI integration or for federation and will be "invisible" at the ISI interface, i.e. for the mCDN core network.

C. External Security Interface (ESI)

The ESI corresponds to the interface to mCDN clients where AGG handles the communication security and security protocols to receive the client request, to interact with SEC via the ISI-Interface, and to respond to the client. Security interactions with the client handled by the Aggregator are authentication and authorisation (e.g. with HTTP, HTTPS, using credentials such as passwords, or PKI certificates), enforcement of AAA decisions by transmission of requests to the SEC security server via the internal ISI protocol, and communication protection to the clients (e.g. with SRTP, TLS). The 'API' of the ESI interface is defined by the security protocols selected and used depending on the security level that should be reached.

Following the requirements introduced in Section IV, within the user client device some security functionalities have to be implemented. These may provide mechanisms for: PKI/CA interaction to manage own certificates (user, device), verification of mCDN including PKI/CA interaction (mutual authentication: client checks the validity of mCDN server certificates), processing of authentication protocols (e.g. TLS, HTTP- or form-based authentication) and encryption protocols

(TLS, HTTPS, SRTP), verification of content authenticity (check digital signature of content provider / author), realisation of DRM (e.g. OMA DRM v2.0), and mechanisms as demanded for 'trusted device' operation, e.g. for TCG/TPM or OMA compliance.

D. Internal Security Interface (ISI)

The ISI transforms internal requests by AGG or another mCDN component that require security decisions into security requests and sends it to SEC that acts as central decision point. SEC processes the request and sends the answer (mostly a decision, but on demand also service answers such as digital signatures for origin content) back to AGG, which is responsible for the further 'mCDN' processing. In particular, AGG must enforce the decision, i.e. it has to take care for proper realisation and for controlling associated behaviour. If it is necessary, enforcement can be delegated to dedicated network elements. AGG, as well as SEC must be trusted entities.

Apart from basic AAA processing, SEC has additional security responsibilities comprising user registration (ID, credentials, PKI integration), session management, access rights management (controlling roles, rights, permissions and related assignments), security policies (e.g. for controlling security related behaviour/enforcement of trusted mCDN entities) and provision of extended security services (token, keys, signatures).

It is also possible to use SEC services across untrusted networks but in these cases ISI protocol messages need additional protection, e.g. by use of TLS.

E. mCDN Operation and Administration Security Interfaces

Further interfaces to the mCDN system exist that are needed for the operation of the CDN so that content providers, administrators (CDN provider, CDN operator), and federation partners (CDN composition) can access the CDN system. These interfaces have to be protected, ensuring authentication of authorised communication partners, session management and enforcement of corresponding access rights by using mechanisms for identity and access management.

In particular, for communication security suited mechanisms (e.g. IPsec-based VPN, TLS, SFTP, SCP/SSH, HTTPS) have to be provided if components (e.g. a content management Web GUI, an origin server, administration interfaces) have interfaces outside of the trusted infrastructure. The communications security mechanisms depend on the needs and the possibilities of the deployed hardware and software. The identity and access management can be addressed similar to the case for end users accessing content. Entries have to be stored in the Security Server allowing to authenticate as provider and to store respective permissions. For reasons of uniformity and consistency, we propose that the same SEC hosts also the security information needed for protecting mCDN operation interfaces. However, when required, these could also be hosted on a separate Security Server (respectively on an independent or shared security information base, holding accounts and permissions).

Many of the mechanisms provided for identity and access management are relevant also for mCDN administrators. If the mCDN is not managed and administered centrally, security related processes, duties and responsibilities have to be distributed and submitted to delegated administrators.

F. Security Building Blocks

The security architecture defines the security mechanisms that are in place to achieve the security requirements. Important security building blocks to realise the mCDN security architecture are related to the areas communication security, web service security, authorisation and access control, key management and public key infrastructure. They use basic cryptographic concepts such as symmetric and asymmetric cryptography, and cryptographic hash functions (see [9] for details on cryptography). In the following, these building blocks are shortly explained as they are the basis to realise the security concept.

Communication Security involving confidentiality, authentication of communication partners, and protecting the integrity and authenticity of exchanged messages can be achieved at different layers: Especially wireless systems (GSM, UMTS, DECT, IEEE 802.11 WLAN, Bluetooth, see [10] for details) include means to protect the wireless link. At higher layers, IPsec and SSL/TLS are available. SRTP is available for the UDP-based protection of real-time and multimedia data streams. Other mechanisms at higher layers are CMS for content protection and HTTP- or form-based authentication.

Secure Web Services communicate by exchanging over HTTP SOAP (RFC3288) [11, 14] messages using XML encryption and signatures that provide message integrity, authentication, and confidentiality. XML integrity and encryption can be applied flexibly on the complete SOAP header and/or body or on parts of them [12]. Example credentials are username/password, SAML assertions [13], digital certificates, and session tokens.

Authorisation and Access Control ensure that only permitted actions can take place. Authorization determines which actions are allowed, whereas access control ensures that only authorized actions can be performed.

Authorization for mCDN actors advantageously can be built on a role based access control (RBAC) concept. Administrative and basic user tasks and permission are central and 'static' and therefore largely independent from individual 'personal' characteristics. The administration of RBAC policies is organized by first defining permissions required for relevant functional positions, and in a second step assigning users (subjects) to the roles required to perform their function. The XML-based eXtensible Access Control Markup Language (XACML) [15] describes RBAC policies and requests to be checked against such a policy.

One of the most challenging problems in managing large networks is the complexity of security administration. RBAC has become the predominant model for advanced access

control because it reduces the complexity and cost of security administration in large networked applications.

In addition to role based access control for global tasks, content and user specific access control is rule and subscription based. Also, reusing DRM paradigms may be required to complement authorisation issues, in particular in peer-to-peer content distribution.

Key Management is the set of techniques and procedures supporting the establishment and maintenance of keying relationships between authorized parties [16]. It plays a fundamental role in cryptography as the basis for securing cryptographic techniques providing confidentiality, entity authentication, data origin authentication, data integrity, and digital signatures. The keys must initially be established by non-cryptographic, out-of-band techniques (e.g., in person, by a trusted courier or an administrator). For secret keys, confidentiality and authenticity must be ensured, whereas for public keys confidentiality is not required.

Key management usually involves some form of infrastructure called **Public Key Infrastructure** to distribute initial keys (e.g. stored on a SIM card) and to provide infrastructure services (e.g. certificates, certificate repositories, or Security Servers as the authentication centre in GSM).

Perimeter Protection: It is common practice to use firewalls to protect a network at its perimeter in order to control the network traffic passing the border between networks, trusted to different degrees. Firewalls are used in particular at the boundary of a corporate network and the public Internet. But they are also used to protect sensitive parts of an internal network requiring special protection. The purpose of perimeter security is to provide a single "choke" point that needs careful security design. Perimeter protection allows separating the trusted, managed infrastructure from untrusted parts of the network. Although using firewalls is common state of the art, they do not replace host-based security and are considered as being one level of an overall security concept.

VI. Summary and Conclusion

In the security concept presented for mCDN, the security objectives for the required security level must be identified examining the trust model, risks, and threats for the specific mCDN usage environment. In this paper, possible mechanisms to achieve these objectives at the different interfaces identified are described. The services provide much more than pure AAA functionality, including management processes for identities, credentials and rights, as well as integration of PKI/CA, DRM paradigms, and federation. Internal interfaces and APIs are defined, that have to be used by mCDN components that require related security interactions.

When the mCDN system comprises components belonging to different administrative domains (CDN federation, peer-to-peer content distribution between user devices), additional security issues need to be addressed. During the second project year, the security concept presented here will be extended accordingly, and the required security technology will be evolved in further detail. Security for different CDN federation scenarios will re-use federation concepts known from Web service security, making the security infrastructure of one CDN usable by another CDN. To protect content in the case of peer-to-peer content distribution between end users, but being under control of the managed part of the mCDN, the security enforcement will be complemented with DRM-like mechanisms operating on the content instead of the communication link.

Acknowledgment

We would like to thank the EU for sponsorship, and all partners (Fraunhofer FOKUS, INTRACOM, Intrasoft, Nat. Technical Univ. of Athens, Siemens AG, Siemens Mobile Comm., TNO, Univ. College London, Univ. of Kassel, VTT, Wunder-Media) in the mCDN project for their fruitful and successful cooperation. They all contributed to the open mCDN architecture and to component development, which is the basis for the security concept to come to reality.

References

[1] FP6 http://europa.eu.int/comm/research/fp6/p2/index_en.html and the Information Society Technology (IST) program, see http://dbs.cordis.lu/

[2] Eckert K. P. et al, 2004, mCDN Deliverable 2.2, Initial specification of the Interlayer APIs and the initial security concept.

[3] Telematica Institut, Content Distribution Networks (State of the art), TI/RS/2001/027, June 1, 2001 https://doc.telin.nl/dscgi/ds.py/Get/File-15534/cdnsota.pdf

[4] http://www.akamai.com/en/html/business/site_protection.html

[5] http://www.speedera.com

[6] The HTRC Group: 'A street-wise guide to choosing a CDN Service Provider' and 'Securing your business: Costly threats to web sites (Speedera's secure solutions)'; available at www.htrcgroup.com

[7] Bob Hulsebosch: Framework for Secure personalised Content Delivery, Technical Report, Telematica Institut TI/RS/2001/095, Jan 2002. https://doc.telin.nl/dscgi/ds.py/Get/File-19930/Framework.pdf

[8] Sokol J., et al., 2004, mCDN Deliverable 2.1, mCDN - Interlayer Issues in CDNs and initial mCDN architecture.

[9] Bruce Schneier; Applied Cryptography: Protocols, Algorithms, and Source Code in C; 2nd Edition, Wiley 1995.

[10] Andrew Tanenbaum, Computer Networks; 4th Edition, Prentice Hall PTR 2002.

[11] http://www.ietf.org/rfc.html

[12] http://www.w3.org/TR/xmldsig-core/ and ../xmlenc-core/

[13] http://www.oasis-open.org/committees/download.php/10624/sstc-saml-conformance-2.0-cd-03.pdf

[14] http://www.w3.org/TR/soap/

[15] http://www.oasis-open.org/committees/tc_home.php\wg_abbrev=xacml

[16] A. Menezes, P. Oorschot, and S. Vanstone: Handbook of Applied Cryptography; CRC Press 1996.