A Distributed Security Announcement Authoring System with CAIF Support

Anselm R. Garbe, Oliver Goebel

Stabsstelle DV-Sicherheit (RUS-CERT)

Universitaet Stuttgart

garbe@cert.uni-stuttgart.de, goebel@cert.uni-stuttgart.de

Abstract: Many Security Teams issue *Security Announcements* (aka *Advisories*) to their constituencies to provide them with up-to-date information about security problems in soft- or hardware and their mitigation by applying workarounds or patches. To be able to use the benefits of advanced document formats designed for this task, like the Common Announcement Interchange Format (CAIF), powerful software, that also implements an authoring process, is is a prerequisite. This article describes the architecture of and the authoring process implemented by a distributed authoring system based on but not limited to CAIF. It presents the parts of the system API to adapt, further develop, and integrate existing authoring systems, like the SIRIOS[4] System into the distributed authoring process, based on web-service and classic RPC technology.

1 Preface

A main task of many Security Teams is the issuing of security announcements crafted for their constituency and providing it with tailored information.

Security announcements are documents describing security problems in software, hardware or other technical systems. Almost all issuers, including vendors, use their own document formats and terminologies to describe security issues in their announcements. These formats differ in structure, layout, content and channels of distribution. Most announcements are published as plain text files to be distributed via mail. Some of the issuers also provide RSS feeds and HTML-rendered announcements.

Although there is still no commonly used standard established, most formats feature a very basic set of information in only slightly differing form. Besides a problem description (in heavily differing level of detail), they usually provide information about solutions such as patches or workarounds to the problems described. Other valuable information, e.g. about the attack vector which could be used to produce problem mitigations by configuring a firewall that is preventing the use of the vector by outsiders, is provided in the rarest cases.

The fact, that there are still so many formats in so many differing quality levels makes the use of the information provided in the announcements a hard and time-consuming job and co-operation between issuers inefficient. Currently the main target group of security announcements are system administrators and network coordinators. Other target groups like technically lesser qualified users or managers who usually need a different view on the information about a problem are not served by almost all currently issued announcements. Providing these target groups with tailored information can be a promising market and would increase the effectiveness of announcement services, since the information carried would potentially get through to may more users of affected IT-infrastructure.

This situation was one of the key reasons for the development of CAIF[1][3] during the last years, based on the expertise gained running RUS-CERT's announcement service[2].

2 Authoring System

The authoring process implemented in the software described in this document tries to be as generic as possible. It is based on the process currently in use in RUS-CERT's announcement service.

The terminology, authoring process, technology, and architecture implemented by the authoring system is described in the following.

2.1 Terminology

To fully understand the authoring process of security announcements, the existing terminology is clarified in the following.

Security Announcement A published security announcement is a formatted CAIF-document containing information about security issues in software, hardware or a technical system.

Draft An unpublished security announcement.

Reader A reader is a person who reads a security announcement. Such a person can be anyone, such as a system administrator, a student or a random visitor of the site providing a security announcement.

Constituency The constituency is the fraction of readers that belong to a specific organization. E.g. RUS-CERT's constituency are the members of Stuttgart University.

Target Group/Audience A target group/audience is the fraction of the readership, that has a specific technical background knowledge, organizational overview, and native language. Note, that the target group is not a subset of a constituency in general, although a constituency usually can be devided into several target groups. A target group in general is a group of readers that share these characteristics. They usually can be found in most constituencies.

Author An author is a person who writes, or reviews security announcements.

Originator An originator is an author originally writing a new security announcement or starting to extend an already published (issued) announcement.

Issuer An issuer is an author or authoring organization who publishes (issues) or republishes (re-issues) security announcements.

Review A review is the quality assurance phase in the authoring process. Reviewing announcements can be implemented differently according a policy to be defined.

Reviewer A reviewer is an author who reviews drafts of security announcements which are going to be published.

2.2 Authoring Process

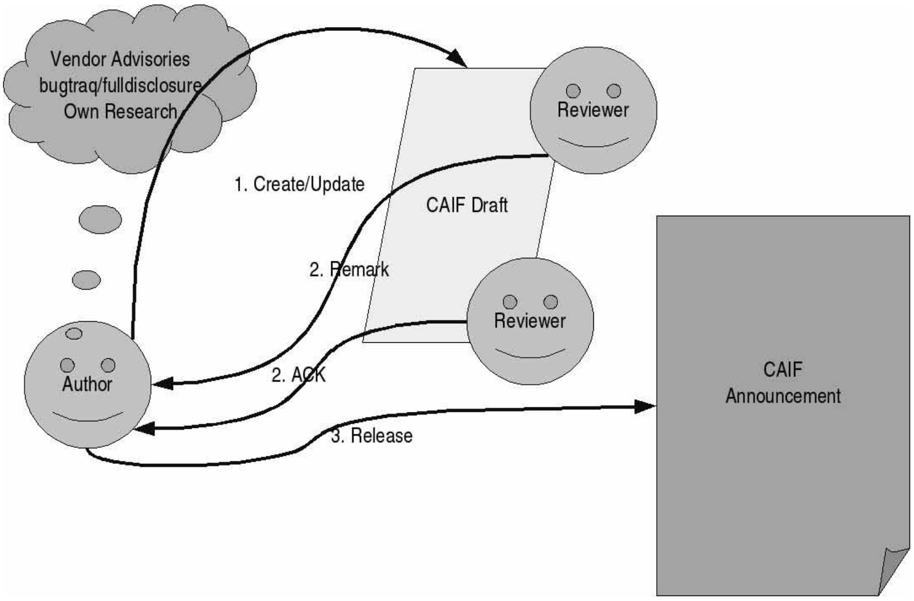


Figure 1: Authoring Process

The basic authoring process for security announcements is very simple. Each author is specialized in specific subjects of security issues and reads associated security announcements of various vendors several times per week.

Besides generic research on vulnerabilities and flaws the process of writing security announcements in most cases is based on the investigation of information provided by vendors, security organizations and teams. If a piece of information is recognised relevant, an author decides about the importance of the subject and then issues a summary or a full announcement describing the problem.

If an author decides that a specific problem is relevant for his constituency, he (the originator) creates a new security announcement. Sometimes, an originator decides to update an existing announcement with new information instead of creating a new one, because new information on the problem described in the already issued announcement is available. Typically this is the case if security patches have been published for a specific security hole, or when exploits are spreading.

If the security issue is of low importance, the originator may wish to write a summary that contains a link pointing to the original security announcement. Otherwise an originator usually writes a fully qualified security announcement for his constituency.

After finishing an initial draft of the announcement, an originator is releasing it to be reviewed by other authors in the communication channel of the review process.

Mostly, reviewers comment semantic and syntactic mistakes in the announcements to be reviewed. Often, they also provide links pointing to additional information about the problems. When a reviewer approves a draft, he is asked to send his acknowledgement to the originator, or to the communication channel.

Often, authors are allowed to change an announcement under review, however this should never be done without notifying the originator.

Since any quality assurance process requires a great deal of discipline from the reviewers and since publishing security announcements is time critical, it must be possible to omit the reviewing process.

Sometimes the originator may want to ask other authors to write specific sections for a security announcement, e.g. background information about a specific problem. In such a case, those authors are originators as well. Seldom, originators pass complete drafts to different authors, e.g. if the originator is leaving for vacation, before the announcement can be published.

The complete review process can take several iterations until an a document is in a state the originator wants to issue (publishes) it to the readers of his constituency.

If an originator issues an announcement, it is distributed through all configured information channels, e.g. RSS feeds, mailing lists, web sites, etc, to the constituency. Afterwards, readers are able to read the published security announcement. In special cases, it may be necessary to distribute a document to be issued via a subset of the channels available.

Through sharing the storage of announcements and author-specific data between issuers, the basic authoring process is extended to form a distributed authoring process. The storage can be mirrored by all participants for reliability reasons.

2.3 Technologies

The system is implemented as a web application in a Web Service environment and uses J2EE, CAIF, XML, XSL, WSDL, SOAP, and RSS technologies. It is assumed that those technologies are known, however the most important ones are described in the following.

2.3.1 Common Announcement Interchange Format (CAIF)

CAIF is an XML format for security related documents – especially announcements – that has been developed to meet generic requirements of issuers like security teams and product vendors.

An extensive set of high-level mark-up elements enables authors and issuers to increase document readbility independently from a rendering policy. Besides the basic elements for text emphasis in several levels, code, and preformatted text, CAIF provides elements to mark-up program names, services (like daemons), file names and contents of various types, terminal interaction, various menus, and vendor names.

The format provides mechanisms that allow to include information that is specific to a given constituency – a concrete IT-infrastructure and their users, operators, and adminsitrators – within the announcement in a way that it can be selectively treated. Such handling could be its deletion before the announcement is issued outside the constituency or the production of constituency-specific renderings.

Since CAIF is an XML-based format the documents allow the selective production of different renderings of announcements for the intended target groups addressing one, a sub-set, or all problems multi- or mono-lingual in the languages provided.

2.3.2 Web Services

Web Services are a new server technology to access specific software services based on web technologies. They are addressed by an URI and its interfaces are defined in the WSDL (Web Service Description Language). To dynamically announce Web Services, UDDI directory services are used.

Web Services provide the three key mechanisms for interoperability: finding a service, binding to its interface and interchanging data (communicate) based on standard Web technologies.

Web Services are oriented on the Service Oriented Architecture paradigm, thus they combine object-oriented and distributed programming concepts to form business applications.

2.4 Architecture

The system consists of a *persistence layer*, a *middleware*, and a web-based *front-end*.

The *persistence layer* and *middleware* are implemented as APIs, which can be easily extended and integrated into existing systems, like SIRIOS.

All top-level elements of CAIF documents are persisted in separate tables, the database creates separate tables for each element.

The middleware achieves permission and announcement management through storing authentication and announcement history information in a special database, which can be shared among issuers.

The web-based front-end is implemented as a web application for an arbitrary web application server, like Apache Jakarta. It provides a web-based user interface for *readers* and *authors*. It is based on the middleware and persistence layer APIs.

2.5 Web Service extension

The system provides a Web Service to access the functionality implemented by the middleware, such as retrieving all published announcements, creating new announcements and

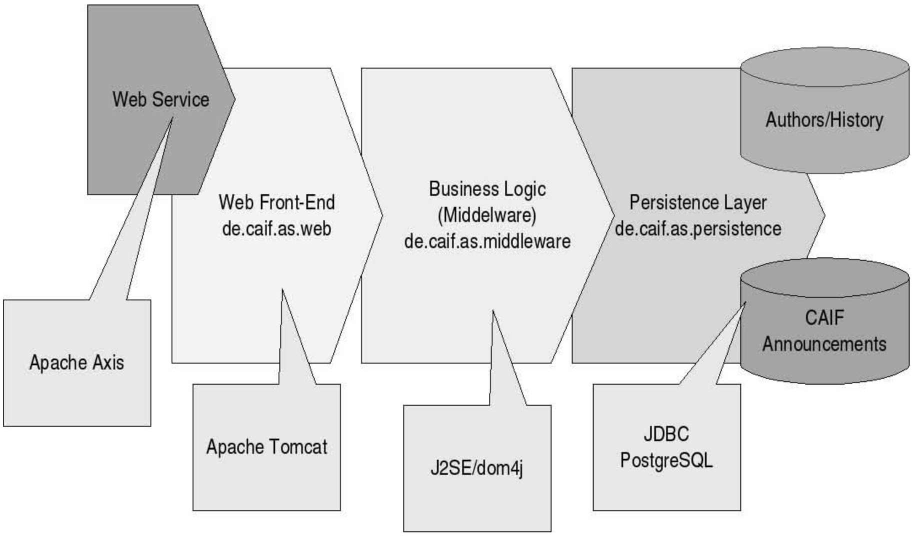
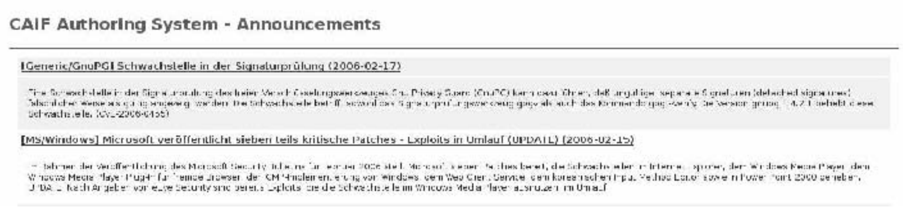


Figure 2: Architecture

publishing drafts.

The Web Service interface of the system allows to be accessed by different kinds of clients. For example, through retrieving all CAIF documents an RSS feed can be generated easily.



CAIF Authoring System - Announcements

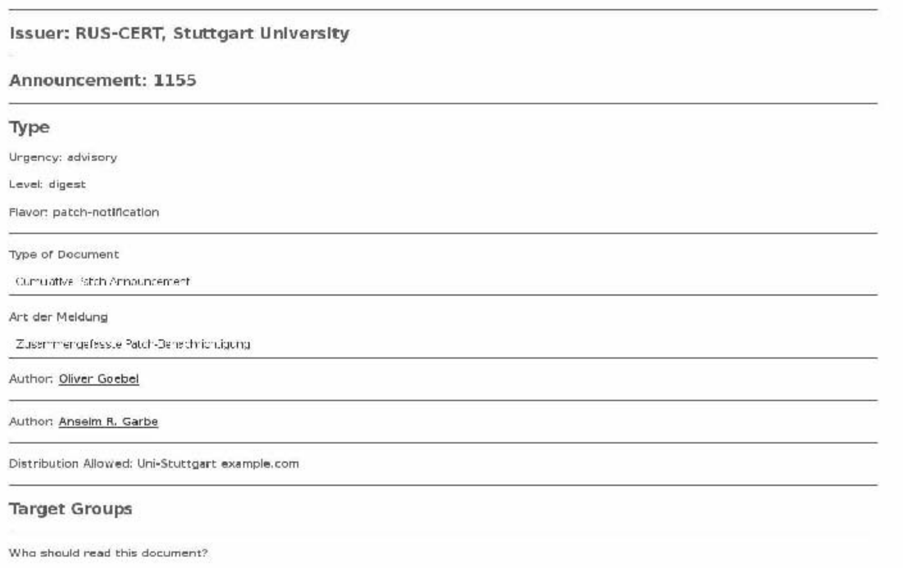
[Generic/GnuPG] Schwachstelle in der Signaturprüfung (2006-02-17)

Eine Schwachstelle in der Signaturprüfung des freien Verschlüsselungswerkzeuges Gnu Privacy Guard (GnuPG) kann dazu führen, daß ungültige separate Signaturen (detached signatures) fälschlicher Weise als gültig angezeigt werden. Die Schwachstelle betrifft sowohl das Signaturprüfungswerkzeug gpgv als auch das Kommandozeilen-Werkzeug. Die Version gnupg 1.4.2.1 behebt diese Schwachstelle. (CVE-2006-0455)

[MS/Windows] Microsoft veröffentlicht sieben teils kritische Patches - Exploits in Umlauf (UPDATE) (2006-02-15)

Im Rahmen der Veröffentlichung des Microsoft Security Bulletins für Februar 2006 stellt Microsoft sieben Patches bereit, die Schwachstellen im Internet Explorer, dem Windows Media Player, dem Windows Media Player Plugin für fremde Browser, der TCP/IP-Implementierung von Windows, dem Web Client Service, dem koreanischen Input Method Editor sowie in PowerPoint 2000 beheben. UPDATE: Nach Angaben von eEye Security sind bereits Exploits, die die Schwachstelle im Windows Media Player ausnutzen, im Umlauf.

Figure 3: List of announcements



Issuer: RUS-CERT, Stuttgart University

Announcement: 1155

Type

Urgency: advisory

Level: digest

Flavor: patch-notification

Type of Document

Cumulative Patch Announcement

Art der Meldung

Zusammengefasste Patch-Benachrichtigung

Author: Oliver Goebel

Author: Anselm R. Garbe

Distribution Allowed: Uni-Stuttgart example.com

Target Groups

Who should read this document?

Figure 4: Announcement details

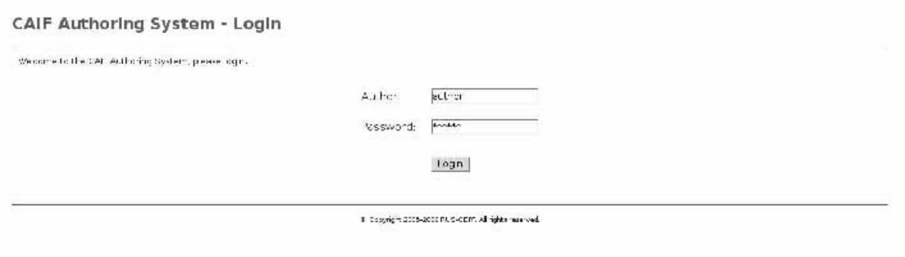
2.6 User Interface

The user interface of the systems web front-end for *readers* and *authors* is presented in the figures 3 - 7 .

3 Conclusion

To support collaboration among issuers in the autoring process, either the APIs of the middleware and persistence layer, or the Web Service interface can be adapted and integrated into existing authoring systems.

Accessing the Web Service allows to form a distributed authoring system even based on different technologies and authoring systems in use. This is a big advantage of the Web



CAIF Authoring System - Login

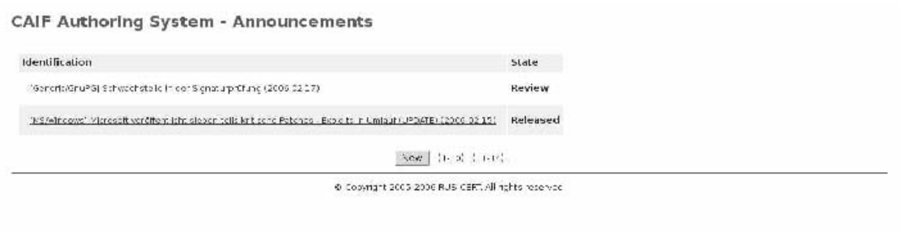
Welcome to the CAIF Authoring System, please login.

Author: [illegible]

Password: ******

© Copyright 2005-2006 RUS-CERT. All rights reserved.

Figure 5: Login

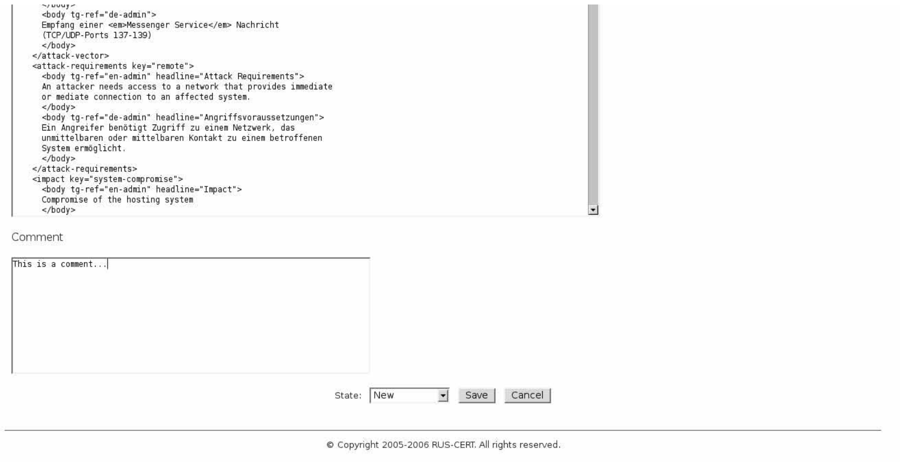


CAIF Authoring System - Announcements

Identification	State
[Generic/GnuPG] Schwachstelle in der Signaturprüfung (2006-02-17)	Review
[MS/Windows] Microsoft veröffentlicht sieben teils kritische Patches - Exploits im Umlauf (UPDATE) (2006-02-15)	Released

© Copyright 2005-2006 RUS-CERT. All rights reserved.

Figure 6: List of drafts



```
      </body>
      <body tg-ref="de-admin">
      Empfang einer <em>Messenger Service</em> Nachricht
      (TCP/UDP-Ports 137-139)
      </body>
    </attack-vector>
    <attack-requirements key="remote">
      <body tg-ref="en-admin" headline="Attack Requirements">
      An attacker needs access to a network that provides immediate
      or mediate connection to an affected system.
      </body>
      <body tg-ref="de-admin" headline="Angriffsvoraussetzungen">
      Ein Angreifer benötigt Zugriff zu einem Netzwerk, das
      unmittelbaren oder mittelbaren Kontakt zu einem betroffenen
      System ermöglicht.
      </body>
    </attack-requirements>
    <impact key="system-compromise">
      <body tg-ref="en-admin" headline="Impact">
      Compromise of the hosting system
      </body>
```

Comment

This is a comment...

State: New

© Copyright 2005-2006 RUS-CERT. All rights reserved.

Figure 7: Edit an announcement

Service technology to classical RPC technology used in the systems APIs. However, for performance-critical tasks classical RPC technology like J2EE should be used, instead of Web Service technology.

Besides this, there is no need that a collaborative issuer uses the CAIF format to persist his announcements internally, he can use a different format, but he only has to be able export and import CAIF[1].

4 Future Work

The authoring system as it is described is the starting point for further developments and the optimisation of the distributed authoring process. It also serves as a reference implementation for CAIF 1.2[3].

The system is currently being deployed RUS-CERT. In the pilot phase, it will be operated in co-operation with CERT-VW, ComCERT, dCERT, GN-CERT, and the University of Constance. Talks with the Royal British Cabinet Office and SAP AG to join the evaluation team are currently taking place. The purpose of the evaluation phase is to optimise the processes for the collaborative creation of announcements, and identify requirements that arise during production. This phase also helps to identify new possibilities of collaboration and resulting optimisations.

References

[1] Common Advisory Interchange Format (CAIF) - Requirements, F. Weimer and Goebel O., `http://www.caif.info/draft-weimer-goebel-caif-requirements.html`

[2] RUS-CERT Ticker, `http://cert.uni-stuttgart.de/ticker`

[3] Common Announcement Interchange Format (CAIF) – Format Specification, Version 1.2, O. Goebel, `http://www.caif.info/draft-goebel-caif-format.html`

[4] SIRIOS - Incident Response Module, `http://www.cert-verbund.de/sirios/`

[5] Web Services - Concepts, Architectures and Applications, G. Alonso, F. Casati, H. Kuno, V. Machiraju, 2002, Springer, ISBN 3-540-44008-9

[1] Although CAIF can be used to store data, its main purpose is the interchange of data.