doi: 10.7690/bgzdh.2016.02.007

美国海事信息共享环境安全架构研究

徐 飞[1,2]，戴剑伟[1]，王永瑞[3]，郭 璇[2,4]

（1. 国防信息学院一系，武汉 430010；2. 国防信息学院八系，武汉 430010；
3. 中国人民解放军 75737 部队，广州 510800；4. 武警警官学院信息工程系，成都 610213）

摘要：针对美国海事信息共享环境（maritime information sharing environment，MISE）面临的主要安全问题，对其安全架构进行研究。分析 MISE 安全需求，探讨美国海事信息共享环境安全架构的组成，介绍 MISE 运用安全属性、安全断言标记语言和可信结构文档等技术的方法和原理。结果表明：该架构能有效解决海事信息跨组织跨机构共享的问题，对于实现跨领域信息的安全交换具有重要的借鉴价值。

关键词：海事信息共享环境；安全架构；信息交换

中图分类号：TP391 **文献标志码**：A

Research on Security Architecture of USA Maritime Information Sharing Environment

Xu Fei[1,2], Dai Jianwei[1], Wang Yongrui[3], Guo Xuan[2,4]

(1. *No*. 1 *Department*, *PLA Academy of National Defense Information*, *Wuhan* 430010, *China*; 2. *No.* 8 *Department*, *PLA Academy of National Defense Information*, *Wuhan* 430010, *China*; 3. *No*. 75737 *Unit of PLA*, *Guangzhou* 510800, *China*; 4. *Department of Information Engineering*, *Armed Police College of CAPF*, *Chengdu* 610213, *China*)

Abstract: Based on the main security problems of maritime information sharing environment (MISE), research on its security architecture. The security requirements of the MISE are analyzed, discus the security architecture of MISE, and introduce method and principle of MISE security attribute, security assertion markup language and trust structure document. The results show that the architecture can effectively solves the problems of marine information across organization and mechanism sharing, it has important reference value for implementing the information exchange security across different domains.

Keywords: maritime information sharing environment; security architecture; information exchange

0 引言

为了维护美国海上利益、实现海上安全战略目标，2004 年 12 月，时任美国总统布什签署了第 41 号国家安全总统令、第 13 号国土安全总统令（national security presidential directive-41/homeland security presidential directive-13），要求美国国土安全部、国防部、司法部对获取到的态势信息进行共享，融合集成情报、监测、侦察、导航系统及其他信息源，形成海上综合态势图，尽早并尽可能远地发现海上安全威胁，及时采取应对措施。为此，美国政府成立了海上安全政策协调委员会，督促海上安全国家战略和相关计划的实施，并启动了海域态势感知国家计划（national plan to achieve maritime domain awareness，MDA Plan）。

根据海域态势感知国家计划的安排，美国海军情报部门、海岸警备队、海军舰队和运输部等机构于 2006 年 2 月联合组建了海域态势感知利益共同体（maritime domain awareness community of interest，MDA COI），采用统一的海事信息交换模型标准，构建了海事信息共享环境（maritime information sharing environment，MISE）[1]。MISE 是一个数据交换环境。通过 MISE，海事信息的提供者和使用者采用统一的数据定义管理和共享海事信息，为联邦、州、地方政府、当地部落、领地、私营部门和合作伙伴提供基于互联网的、非机密信息共享能力[2]。该项目有效提升了信息交换共享的范围和程度，迅速得到了推广，并被美国国家信息交换模型（national information exchange model，NIEM）管理办公室评为 2013 年最佳 NIEM 应用奖[3]。

可信系统及用户、基于属性的访问控制机制构成了 MISE 安全架构的主要基础，数据交换标准为可信系统间的信息交换提供了有效途径，同时还考虑到信息安全交换的需求。MISE 面临的主要安全问题是用户身份的认证和信息的安全交互。为了有

收稿日期：2015-10-19；修回日期：2015-11-28

基金项目：国防预研基金项目（9140A15090112JB93180）

作者简介：徐 飞（1982—），男，江苏人，在读博士，讲师，从事数据工程和计算机研究。

效应对这些问题的挑战，在 MISE 的架构中，全面强化了基于属性的访问控制、身份验证等方面的措施，形成了一整套操作流程清晰、安全管控严格的安全保障措施；因此，笔者从安全架构的组成、实现安全架构的关键技术 2 个角度进行分析。

1 MISE 的整体逻辑结构

MISE 的整体逻辑结构如图 1 所示，主要包括 4 个部分：

1) 可信系统及用户。参与 MISE 信息交换的系统称为可信系统，可信系统既可以是信息提供者，又可以是信息使用者，还能同时扮演这 2 种角色。用户是可信系统的操作和管理者。

2) 信息共享基础设施(information sharing infrastructure，ISI)。ISI 是 MISE 的核心，为参与信息交换的可信系统提供共享服务。可信系统间不直接进行信息交换，所有信息交互必须通过 ISI。

3) 数据交换标准。MISE 中的可信系统需遵守统一的数据交换标准，通常基于美国国家信息交换模型(national information exchange model，NIEM)。

4) 基于属性的访问控制机制。MISE 为数据、用户和实体定义了各类安全属性，实现对交换的信息进行访问控制管理。

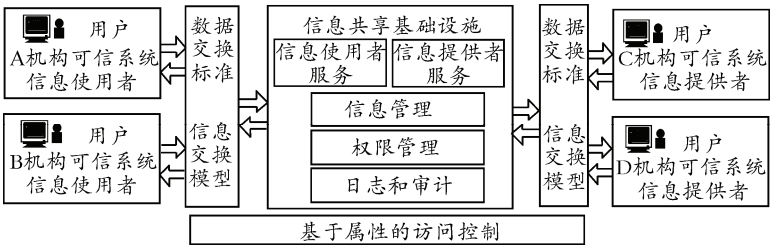

图 1 MISE 逻辑结构

2 MISE 安全需求分析

在 MISE 中，参与信息交换的系统可能归属不同的组织机构，每个组织机构都有其信息安全保障机制。各信息系统参与 MISE 的信息交换时，不能破坏系统原有的安全机制，同时还要考虑来自其他组织机构的跨领域跨系统用户访问请求时的各种安全问题，具体的安全需求包括：

1) 跨信任域的安全。MISE 必须能够提供一个信任模型，可以跨不同的信任域进行服务调用和信息交换。

2) 安全策略的制定。在传统安全域，往往有一套统一的安全保障机制，在跨领域信息交换时，信息提供者的要求可能会有所不同。如某个安全域对用户的身份认证采用 X.509 证书，另一个安全域中则采用了用户名和密码的方式；因此，MISE 中的安全策略必须能够根据具体需要进行调整。

3) 与现有信息安全解决方案的整合。MISE 中信息交换的安全架构并不取代现有的安全基础设施，相反，还应充分利用现有的 IT 资源，与现有的安全工具和应用程序无缝集成。

4) 安全体系的不可见性。MISE 的安全体系不应影响其他服务的实现。具体来说，新的安全体系结构的部署不应给服务提供者带来以下问题：① 要求使用任何一个特定的编程语言；② 向一个特定的硬件平台进行服务迁移；③ 针对任何特定供应商的 API 接口修改现有的服务实现；④ 重新编译或重建已有的代码。

传统的信息系统安全架构往往采用防火墙和入侵检测技术实现基于边界的安全控制，阻止安全威胁。在跨领域信息交换时，数据要跨越系统边界进行传输，传统的安全模型不能满足信息交换的安全性需求。基于以上分析，MISE 需要采用基于属性的访问控制模型、安全断言标记语言等开放、可扩展的安全技术安全架构的搭建。

基于属性的访问控制(attribute-based access control，ABAC)模型以实体属性为最小粒度，特别适合开放式环境，能够进行细粒度访问控制。“属性”作为访问控制中的最小单位，主要包括主体属性、资源属性和环境属性。其中：“主体”是指请求对某种资源执行某些操作的请求者，在 MISE 中，“主体”是可信系统的用户，主体属性主要定义主体的身份和特性，包括身份、角色、职位和年龄等；“资源”是指系统提供给请求者使用的数据、服务和系统组件，资源属性包括资源的身份、URL 地址、大小和类型等，在 MISE 中，“资源”是进行交换的数据资源；“环境”是指访问发生时，可操作的、技术层面的环境或上下文，包括当前的时间、日期、网络的

安全级别等，在 MISE 中，“环境”是参与交换的可信系统和信息基础设施。

安全断言标记语言(security assertion markup language，SAML)提供了一种信任与授权的标准架构，与具体的实现无关，允许对实体、特权及权限进行申明，通过 XML 文档来定义服务对象的鉴别、授权、权限和会话信息。基于 SAML 构建信息交换环境，能够以更加便捷灵活的方式来处理信息安全问题。

3　MISE 安全架构视图

在 MISE 中，主要通过建立安全套接字层(security socket layer，SSL)连接、身份验证、基于属性的访问控制等措施来确保共享信息的安全。可信系统之间的数据发布和使用都通过 SSL 协议进行安全交互[4]。身份证书和权限信息的存储、安全属性的传输都采用开放的、标准的 SAML 元数据来描述，有效解决了动态环境中不确定用户之间信息共享的安全问题。MISE 安全架构视图如图 2[1]所示。

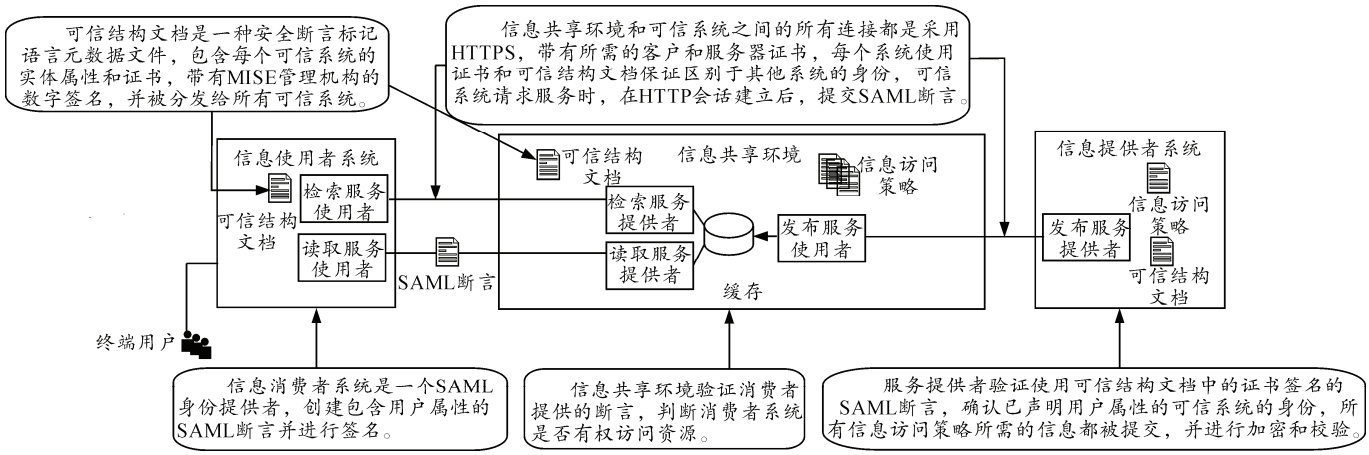

图 2　MISE 安全架构视图

在 MISE 中，信息使用者通过 ISI 来获取信息提供者系统发布的信息，信息使用者和提供者通过 HTTPS 与 ISI 进行连接。

MISE 信息使用者系统、ISI 和信息提供者系统均采用可信结构文档，实现身份认证和访问控制。可信结构文档是一种 SAML 元数据文件，包含每个可信系统的实体属性和证书，带有 MISE 管理机构的数字签名，并被分发给所有的可信系统。信息使用者系统创建包含用户属性的SAML断言并对其进行签名；信息提供者系统对 SAML 断言进行验证，确认可信系统的身份；ISI 对信息使用者提供的断言进行验证，判断其是否有权访问共享基础设施中的信息资源。MISE 综合运用以上多种安全手段，确保信息交换的安全性。

4　MISE 安全架构实现关键技术

MISE 安全架构的作用是确保共享信息能够得到有效保护，信息提供者发布的信息仅能被满足一定权限规则的用户访问。搭建 MISE 安全架构，需综合运用安全属性、SAML 和可信结构文档等技术。

4.1　安全属性

MISE 通过定义用户属性、数据属性和实体属性，确保信息的安全访问。信息提供者发布信息时，为发布到ISI中的每一条信息设置合适的数据属性，当可信系统按照用户的意愿请求信息时，共享基础设施将信息使用者的用户属性与信息的数据属性进行比对，只有访问权限相匹配时，信息才能被访问。

MISE 定义的实体属性、用户属性和数据属性 3 类安全属性如图 3[1]所示。

图 3　MISE 定义的安全属性

1) 用户属性。

授权用户登录到信息使用者系统，根据用户的行为使用服务架构中的服务，以便从共享基础设施获取信息，由于多个信息使用者系统授权的用户可能访问由多个不同信息提供者系统共享的信息，信息提供者必须对用户的访问权限进行验证。尽管掌握全部用户和信息使用者系统的信息不现实，但可以用标准化的方法对用户信息进行描述，便于对用户身份进行验证。

MISE 定义了一个通用的用户属性集，用于描述可信系统某个用户的详细信息，用来确保用户只能访问所请求的、有资格访问的信息。

用户属性及说明如表 1 所示。其中“Citizenship Code”“Law Enforcement Indicator”“Privacy Protected Indicator”“COI Indicator”是授权用户属性，用于信息访问策略的实施。“Full Name”“Electronic Identity Id”是审计属性，用于 ISI 的审计管理，将被记录在审计日志中[1]。

表 1 用户属性

属性名称	属性含义	数据类型	属性值举例
Citizenship Code	用户国际代码	ISO3166-1 规定的国家代码	USA, GBR, FRA
COI Indicator	利益共同体指示符	Boolean	True, False
Electronic Identity ID	用户身份电子标志码	Text	DOE.JOHN.A.2370295257
Full Name	用户姓名	Text	JOHN Doe, Jim Q.public
Law Enforcement Indicator	法律保护指示符	Boolean	True, False
Privacy Protected Indicator	隐私保护指示符	Boolean	True, False

2) 数据属性。

每条共享的数据都由信息提供者设定信息访问策略。信息访问策略是一个规则集，定义了用户访问数据应具备的权限属性，信息访问策略的实施使得 MISE 能够控制用户完全或部分地访问某条数据。数据属性及说明如表 2[1]所示。

表 2 数据属性

属性名称	属性含义	数据类型	属性值举例
COI Indicator	利益共同体指示符	Boolean	True, False
Scope	数据范围	Text	HurricaneKatrina
Law Enforcement Indicator	法律保护指示符	Boolean	True, False
Privacy Protected Indicator	隐私保护指示符	Boolean	True, False
Releasable Indicator	公开发布指示符	Boolean	True, False
Releasable Nations Code List	可公开发布国家	ISO3166-1 规定的国家代码	USA, GBR, FRA

3) 实体属性。

正如用标准方法来描述用户属性一样，MISE 也需要对可信系统的属性进行统一规范描述。MISE 管理机构有责任对可信系统进行审查，确保加入 MISE 的可信系统满足其制定的规则，并保证可信系统的实体属性准确。实体属性及说明如表 3[1]。

表 3 实体属性

属性名称	属性含义	数据类型	属性值举例
Administrative Point of Contact Email AddressText	管理机构联系方式电子邮箱	Text	John.Doe@company.com
Administrative Point of Contact Fax Number	管理机构联系方式传真号码	Text	(555)555-5555
Administrative Point of Contact Full Name	管理机构联系方式姓名	Text	John Doe
Administrative Point of Contact Telephone Number	管理机构联系方式电话号码	Text	(555)555-5555
Certificate	数字证书	64 位编码	MIICJzCCAZ……Plf4+VzegRM
COIIndicator	利益共同体指示符	Boolean	True, False
Entity Abbreviation	实体名称缩写	Text	MAGNET, MSSIS
Entity ID	实体标志	Text	MSSIS:123, MISE:TIB:MAGNET
Entity Name	实体名称	Text	Maritime Analysis Global Network
Law Enforcement Indicator	法律保护指示符	Boolean	True, False
Owner Agency Country Code	机构所属国家代码	ISO3166-1 规定的国家代码	USA, GBR, FRA
Owner Agency Name	可信系统所属机构名称	Text	NORAD-USNORTHCOM
Owner Agency WebSite URI	可信系统所属机构网址	Text	http://website.company.com
Privacy Protected Indicator	隐私保护指示符	Boolean	True, False
Technical Point of Contact Email Address Text	技术支持人员电子邮箱	Text	John.Doe@company.com
Technical Point of Contact Fax Number	技术支持人员传真号码	Text	(555)555-5555
Technical Point of Contact Full Name	技术支持人员姓名	Text	John Doe
Technical Point of Contact Telephone Number	技术支持人员电话号码	Text	(555)555-5555

4.2 SAML 断言

SAML 是一个 XML 框架，可用于在不同的安全域间传递身份信息。MISE 运用 SAML，使来自不同可信系统的用户，能够突破系统异构的壁垒，

跨系统跨领域进行信息交互。

在 MISE 中，为确保信息安全，调用如信息检索和信息获取等服务时，需要以 SAML 的方式提交用户属性。从 SAML 角度来看，信息使用者系统是身份提供者，它在按照用户行为调用服务之前，需要产生 SAML 断言。这个 SAML 断言包含某些用户属性，该 SAML 断言被 ISI 认证后，所有符合这些用户属性的用户或用户组在后续的服务调用中即可访问该用户请求的信息。信息使用者系统将使用可信结构文档中“MISE Consumer Descriptor”元素指定的证书私钥对该 SAML 进行数字签名。

提交断言、验证数字签名及验证断言文档的内容需要较大系统开销；因此，断言只在一系列服务调用的开始发送一次，不需每次服务调用都发送，这种方式可以大大减少系统开销。请求和响应消息体只简单地包含与服务相关的信息，不需要在每个接口都容纳 SAML 断言文档的内容。

SAML 断言处理过程如图 4 所示。

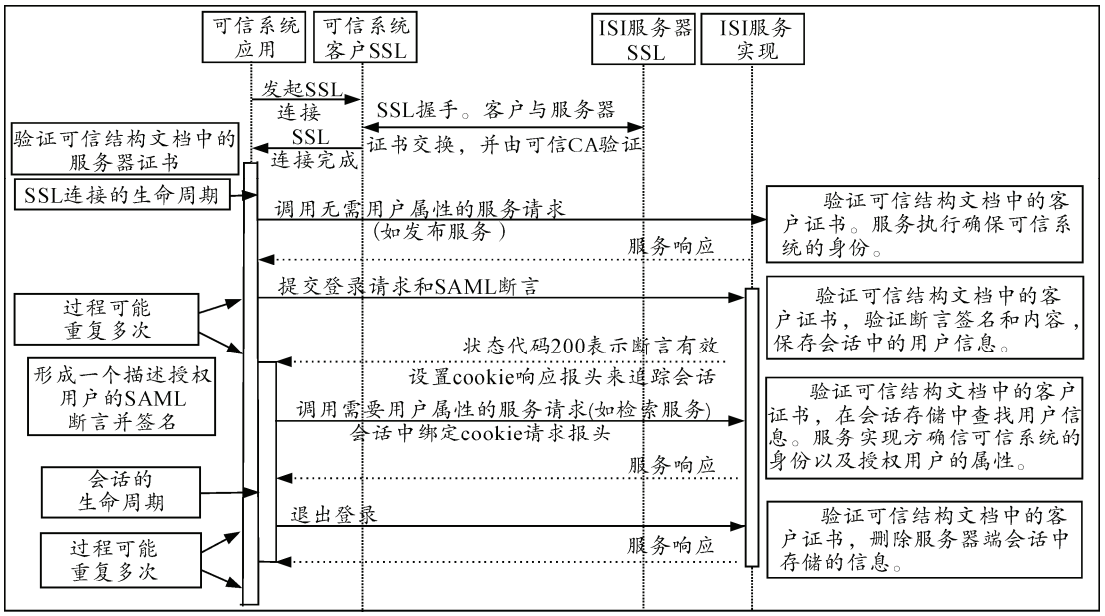

图 4　SAML 断言处理过程

从图 4 可知，用户可调用的服务可以分为 2 类：一是如信息发布等无需 ISI 提供数据的服务。调用该类服务时，无需 ISI 提供数据；因此，用户不需要提供自己的身份信息，此时不会创建 SAML 断言。二是如信息检索等需要使用 ISI 数据的服务。调用此类服务时，用户必须创建 SAML 断言，提交自己的身份信息供 ISI 验证，只有满足权限要求的用户才被允许访问 ISI 中的数据，否则将返回错误代码。SAML 的使用，有效保证了信息交互的安全。

4.3　可信结构文档

可信结构文档是一个符合 SAML 元数据格式的 XML 文件，它对参与 MISE 的可信系统进行了描述。可信结构文档由 MISE 证书验证中心（CA）进行签名后，分发到所有的可信系统中，作为数据加密操作的依据[1]。

可信结构文档在 MISE 的安全架构中扮演了重要角色。MISE CA 的电子签名保证了可信结构文档难以被篡改；因此它包含的参与 MISE 的各可信系统的证书都是可信的，从而保证了可信系统交换信息时 SSL 安全连接的成功创建[5]。

如图 4 所示，ISI 中的服务被调用前，可信系统应用必须与 ISI 服务器进行握手，建立 SSL 连接，在此过程中即包含了客户端和服务器端的证书交换及验证操作，连接双方的证书由各自的可信结构文档提供。

1) 可信结构文档格式定义。

可信结构文档组成结构如表 4[1,6]所示。可信结构文档的顶层标签为“EntitiesDescriptor”，该标签下包含一个或多个“EntityDescriptor”标签，分别对应某个实体（ISI 或可信系统）。每个“EntitiesDescriptor”标签包含一个“RoleDescriptor”标签，标志对应实体的安全证书、实体属性等信息，用于建立 SSL 连接或用作安全审计。“RoleDescriptor”标签指明了该实体在信息交换过程中扮演的角色，如 ISI、信息使用者或信息提供者。

表 4 可信结构文档组成结构

标签名称	含义
EntitiesDescriptor	可信结构文档根标签
>Signature	数字签名
>>SignedInfo[1]	数字签名相关信息
>>>CanonicalizationMethod	标准化算法
>>>SignatureMethod	签名算法
>>>Reference	定义了摘要算法或摘要值
>>>>Transforms	转换算法集合
>>>>>Transform	具体的转换算法
>>>>>>InclusiveNamespace	包含的命名空间
>>SignatureValue	基于 64 位加密的签名信息
>>KeyInfo	密钥信息
>>>X509Data	X509 数据信息
>>>>X509Certificate	基于 64 位加密的证书
>EntityDescriptor	实体描述符
>>RoleDescriptor	角色描述符
>>>KeyDescriptor	密钥描述符
>>>>KeyInfo	密钥信息
>>>>>X509Data	X509 相关信息
>>>>>>X509Certificate	X509 基于 64 位加密的证书
>>>MISELoginService	MISE 登录服务地址
>>>MISELogoutService	MISE 退出服务地址
>>>MISESearchService	MISE 检索服务地址
>>Organization	实体的机构信息
>>>OrganizationName	机构名称
>>>OrganizationDisplayName	机构显示名称
>>>OrganizationURL	机构 URL 地址
>>ContactPerson	联络人信息
>>>Company	联络人所属公司
>>>GivenName	联络人名字
>>>SurName	联络人姓氏
>>>EmailAddress	联络人 Email 地址
>>>TelephoneNumber	联络人电话号码

2) 可信结构文档生命周期。

拥有可信系统的各个机构与 MISE 管理机构共同设置描述可信系统的“EntityDescriptor”元素的信息。“EntityDescriptor”元素的信息设置完成，而且验证了其准确性，确定满足所有 MISE 规则，MISE 管理机构就把它并入可信结构文档，并且用 MISE CA 的私钥进行签名，然后将修改过的可信结构文档分发给所有可信系统。当任一可信系统的“EntityDescriptor”元素的信息被修改后，都要重复上述过程。可信结构文档的生命周期包括创建、分发、修改和使用 4 个阶段[7]。

① 创建阶段。

创建一个新的可信结构文档包括 2 个基本步骤：一是修改文档使之能反映策略的变化(如新的可信系统加入 MISE)；二是用 MISE 证书验证中心的私钥对新的文档进行数字签名[1]。具体如下：

a. 以最近的可信结构文档为基础，编辑修改需要发生变更的内容；

b. 复制已编辑的可信结构文档到移动存储介质；

c. 将存储未签名的可信结构文档的移动存储介质连接到执行签名操作的计算机上，同时将存储 CA 私钥的移动存储介质也连接到计算机上；

d. 利用 CA 私钥，对可信结构文档执行加密签名操作，在加密签名操作过程中，不能将 CA 私钥从移动存储介质复制到其他介质上，也不要将进行签名操作的计算机连接任何网络；

e. 将已签名的可信结构文档复制到存储未签名的可信结构文档的存储介质上。

② 分发阶段。

当一个可信结构文档被创建、修改、签名后，新的可信结构文档必须分发到所有可信系统，具体步骤如下：

a. 将新的可信结构文档发布到一个已知的 URL 上；

b. 通过事先提供的联系方式，通知所有的可信系统下载最新的可信结构文档。

MISE 的安全不依赖于可信结构文档内容，而是由 MISE CA 的证书确保其正确性；因此，可信结构文档可被公开访问，也无需对文档本身进行加密。

③ 修改阶段。

可信结构文档需要重新生成和重新发布的情况包括：

a. 新的可信系统加入 MISE；

b. 原有的可信系统离开 MISE；

c. 某个可信系统的配置发生变化(如证书过期、迁移到新的服务器、密钥泄露等)；

d. MISE CA 的公钥证书过期；

e. MISECA 的私钥被泄露。

④ 使用阶段。

当可信系统向 MISE 发起连接或收到 MISE 管理机构的变更通知时，可信系统必须从已知的 URL 获取可信结构文档。可信系统应当能够在线重新装载可信结构文档，能自动地、周期性地获取和激活最新的可信结构文档。

为了确保系统使用的可信结构文档是由 MISE 管理机构创建和签发的官方版本，在解析和装载可信结构文档时，系统必须对其进行验证，具体要求包括：

a. 包含在可信结构文档内的数字签名必须是有效的；

b. 用来对可信结构文档进行签名的证书必须与 MISE CA 的证书一致；

c. 从已知的 URL 获取可信结构文档需要采用 HTTPS 连接，不需要客户证书；

d. 必须验证被 MISE CA 签名的服务器证书。

5　结束语

美国政府采用基于 NIEM 的信息交换新思路，通过构建 MISE，提供了一个可通过因特网访问的，非保密的信息共享架构。通过综合运用基于属性的访问控制、SAML 断言和可信结构文档等一系列方法措施，有效解决了海事信息跨组织跨机构安全共享的问题，对于实现跨领域信息的安全交换具有重要的借鉴价值。

参考文献：

[1] Navy's Data Engineering Services Center. The National Maritime Domain Awarness Architecture Plan(Version 2.0, Release 3)[EB/OL]. 2013[2015.5.20]. https://mise.mda.gov/drupal/sites/default/files/MDA_Arc-h_MDA_Arch_Plan_V_2.0_Release3_Full.pdf.

[2] Office of Global Maritime Situational Awareness. Maritime Domain Awareness (MDA) Concept of Operations[EB/OL]. 2007[2015.6.5].https://www.ise. gov/sites/default/files/National%20MDA%20CONOPS%202007.pdf.

[3] NIEM Program Management Office. The 2013 Best of NIEM Winners[EB/OL]. 2014[2015.6.10]. https://www.niem.gov/aboutniem/best-of-niem/Pages/2013-Winners.aspx.

[4] Navy's Data Engineering Services Center. MISE Implementation[EB/OL]. 2015[2015.5.25]. https://mise.mda.gov/drupal/node/21.

[5] 王志海. OpenSSL 与网络信息安全: 基础、结构和指令[M]. 北京: 清华大学出版社, 2007: 11-13.

[6] Navy's Data Engineering Services Center. .NET Client Toolkit[EB/OL]. 2013[2015.5.15]. https://mise.mda.gov/drupal/dotnet.

[7] 戴剑伟. 跨领域信息交换方法与技术[M]. 北京: 电子工业出版社, 2014: 263-265.

****

（上接第 13 页）

5　结论

1) 根据GPS接收机的通信和GPS帧数据协议，编写了与之相应的关键控制的程序，在程序运行中删除可能出现的数据传输错误，并对接收机状态进行实时反应，最后完成对接收机星历的装订。

2) 该装订系统使用 FRAM 存储模块、键盘模块和液晶模块，不仅能协调、快速地控制 GPS 数据的接收，而且能无遗漏地保存 GPS 数据。

3) 户外实验结果表明，GPS 数据的发送和接收控制能为智能弹药的研制和设计打下可靠的基础。

参考文献：

[1] 王丹丹, 陈小军, 侯雄, 等. 一种利用初始装订实现GPS 快速定位的方法[J]. 上海航天, 2009(3): 62-65.

[2] 秦丽, 祖静, 李永红. 窄脉冲信号的弹载存储测试技术[J]. 测试技术学报, 1994, 8(2): 103-106.

[3] 黄建军, 张志安, 陈俊, 等. 基于铁电存储器的弹载数据高速存储系统研究[J]. 测试技术学报, 2013, 27(1): 50-55.

[4] 刘大杰, 施一民, 过静珺. 全球定位系统(GPS)的原理与数据处理[M]. 上海: 同济大学出版社, 1996: 32-47.

[5] 蔡桂祥, 薛质, 侯育炜. 双频实时动态 GPS 接收机的设计与研制[J]. 光学仪器, 2007, 29(2): 73-77.

[6] 胡立志, 董莲, 陆福敏, 等. 基于 GPS 模拟器的接收机测试方法研究[J]. 电子测量技术, 2009, 32(6): 127-130, 147.

[7] 史金光, 王中原, 常思江, 等. 二维弹道修正弹修正方法[J]. 海军工程大学学报, 2010, 22(4): 87-92.