



Radiology Option for Audit Trail and Node Authentication

Andrei Leontiev

Dynamic Imaging



- **Defines basic security features for an individual system for use as part of the security and privacy environment for a healthcare enterprise.**
 - Provides host level authentication, which is used in conjunction with the user authentication from EUA and XUA.
 - Provides audit trail mechanism for monitoring activities related to security and patient privacy

- **Protect Patient Privacy and System Security:**
 - Meet ethical and regulatory requirements
- **Enterprise Administrative Convenience:**
 - Unified and uniform auditing system
 - Common approach from multiple vendors simplifies definition of enterprise policies and protocols.
 - Common approach simplifies administration

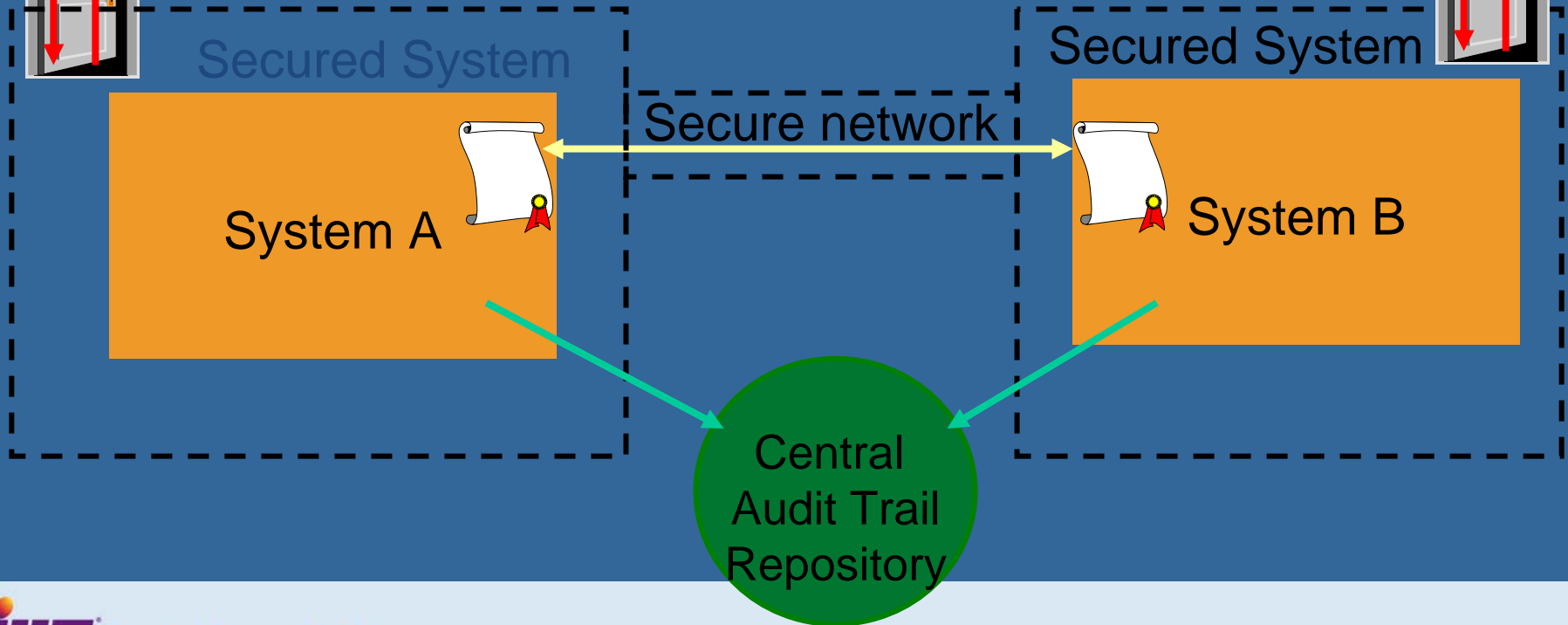
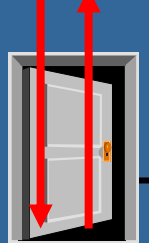
- **Development and support cost reduction through Code Re-use:**
 - Allows vendors to leverage single development effort to support multiple actors
 - Allows a single development effort to support the needs of different security policies and regulatory environments.

- **Reasons: Clinical Use and Privacy**
 - authorized persons must have access to medical data of patients, and the information must not be disclosed otherwise.
 - Unauthorized persons should not be able to interfere with operations or modify data
- **By means of procedures and security mechanisms, guarantee:**
 - Confidentiality
 - Integrity
 - Availability
 - Authenticity

- **IHE makes cross-node security management easy:**
 - Only a simple manual certificate installation is needed, although more sophisticated systems can be used
 - Separate the authentication, authorization, and accountability functions to accommodate the needs of different approaches.
 - Enforcement driven by ‘a posteriori audits’ and real-time visibility.

ATNA *Integrating Trusted Nodes*

- Local access control (authentication of user)
- Strong authentication of remote node (digital certificates)
 - network traffic encryption is not required, it is optional
- Audit trail with:
 - Real-time access
 - Time synchronization



- X.509 certificates for node identity and keys
- TLS for node authentication, and optional encryption
- Secure handshake protocol of both parties during Association establishment:
 - Identify encryption protocol
 - Exchange session keys
- Actor must be able to configure certificate list of authorized nodes.
- ATNA presently specifies mechanisms for HTTP, DICOM, and HL7

- **Designed for surveillance rather than forensic use.**
- **Two audit message formats**
 - IHE Radiology interim format, for backward compatibility with radiology
 - IETF/DICOM/HL7/ASTM format, for future growth
- **Both formats are XML encoded messages, permitting extensions using XML standard extension mechanisms.**

ATNA *Auditable Events*

Actor-start-stop	<i>The starting or stopping of any application or actor.</i>
Audit-log-used	<i>Reading or modification of any stored audit log</i>
Begin-storing- instances	<i>The storage of any persistent object, e.g. DICOM instances, is begun</i>
Health-service-event	<i>Other health service related auditable event.</i>
	<i>The query for instances of persistent objects.</i>
Instances-deleted	<i>The deletion of persistent objects.</i>
Instances-stored	<i>The storage of persistent objects is completed.</i>

ATNA - Radiology Option

- Radiology Option for ATNA defines radiology specific trigger events (in two main categories)
- Security Events:
 - “The access permissions for Dr. Kildare were changed on the PACS”
- Patient Privacy Events:
 - “Dr. Welby looked at Mrs. Smith’s MR images and report on 6/29/05” or “Bob Jones’ Renal US study was exported to a CD on 6/30/05”.

- **ATNA + Radiology Option is backward compatible with Basic Security**
- **Integration Statements should change support claim from “Basic Security” to “Radiology Option for ATNA”**

What it takes to be a secure node

- The entire host must be secured, not just individual actors.
- The entire host must have appropriate user access controls for identification, authentication, and authorization.
- All communications that convey protected information must be authenticated and protected from interception. This means every protocol, not just the IHE transactions.
- All health information activities should generate audit trails, not just the IHE actors.

What it takes to be a secure node

- **The Secure node is not a simple add-on of an auditing capability. The complete work effort includes:**
 - Instrumenting all applications to detect auditable events and generate audit messages.
 - Ensuring that all communications connections are protected.
 - Establishing a local security mechanism to protect all local resources.
 - Establishing configuration mechanisms for:
 - Time synchronization using Consistent Time (CT) profile
 - Certificate management
 - Network configuration
- **Implement the audit logging facility**



iHE[®] *changing the way healthcare*
www.ihe.net *connects*

WWW.IHE.NET