Security - mHealth and FHIR:
mobile health applications and other Internet uses
Security in HL7 Standards

HL7 Security Working Group
John Moehrke
Agenda

- Basic mHealth security
- Communications security
- User Authentication
- Authorization
- Relationship to Privacy Consent
- Audit Logging and reporting
Overall view of mobile device security

- Functional, Operational, Physical, Procedural, Network, User, etc..
- NIST 800-53 - Security and Privacy Controls for Federal Information Systems and Organizations
- NIST 800-124 - Guidelines on Cell Phone and PDA Security
- **NIST 800-101**: Guidelines on Mobile Device Forensics
## NIST 800-53 Control Families

### 18 Families related to Security

<table>
<thead>
<tr>
<th>Access Control</th>
<th>Media Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Awareness and Training</td>
<td>Physical and Environmental Protection</td>
</tr>
<tr>
<td>Audit and Accountability</td>
<td>Planning</td>
</tr>
<tr>
<td>Security Assessment and Authorization</td>
<td>Personnel Security</td>
</tr>
<tr>
<td>Configuration Management</td>
<td>Risk Assessment</td>
</tr>
<tr>
<td>Contingency Planning</td>
<td>System and Services Acquisition</td>
</tr>
<tr>
<td>Identification and Authentication</td>
<td>System and Communications Protection</td>
</tr>
<tr>
<td>Incident Response</td>
<td>System and Information Integrity</td>
</tr>
<tr>
<td>Maintenance</td>
<td>Program Management</td>
</tr>
</tbody>
</table>

### 8 Families related to Privacy

<table>
<thead>
<tr>
<th>Authority and Purpose</th>
<th>Individual Participation and Redress</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accountability, Audit, and Risk Management</td>
<td>Security</td>
</tr>
<tr>
<td>Data Quality and Integrity</td>
<td>Transparency</td>
</tr>
<tr>
<td>Data Minimization and Retention</td>
<td>Use Limitation</td>
</tr>
</tbody>
</table>
Risk – Scalable Security

- Risk Assessment is a general and natural process
- Risk Assessment is applicable to many levels of design and deployment
  - Standards development – Security Cookbook
  - Software design – Medical Device ISO 14971
  - Network design
  - Deploying systems onto network – IEC 80001
  - Organizational – beyond network scope – ISO 27001
  - Nationwide Exchanges – IHE Affinity Deployment
In this scenario:

- The vulnerability is the hole in the roof
- The threat is the rain cloud
- Rain could exploit the vulnerability

The risk is that the building and equipment in the building could be damaged as long as the vulnerability exists and there is a likely chance that rain will fall.
Risk Management (ISO13335)
Risks – Resource protection

- Wrong people get access
- Right people get denied proper access
- Right people see too much (consent)
- Unauthorized Create/Update/Delete allowed
- Right people get wrong data
- Perception that wrong people got access
# NIST 800-53 Control Families

## 18 Families related to Security

<table>
<thead>
<tr>
<th>Access Control</th>
<th>Media Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Awareness and Training</td>
<td>Physical and Environmental Protection</td>
</tr>
<tr>
<td>Audit and Accountability</td>
<td>Planning</td>
</tr>
<tr>
<td>Security Assessment and Authorization</td>
<td>Personnel Security</td>
</tr>
<tr>
<td>Configuration Management</td>
<td>Risk Assessment</td>
</tr>
<tr>
<td>Contingency Planning</td>
<td>System and Services Acquisition</td>
</tr>
<tr>
<td>Identification and Authentication</td>
<td>System and Communications Protection</td>
</tr>
<tr>
<td>Incident Response</td>
<td>System and Information Integrity</td>
</tr>
<tr>
<td>Maintenance</td>
<td>Program Management</td>
</tr>
</tbody>
</table>

## 8 Families related to Privacy

<table>
<thead>
<tr>
<th>Authority and Purpose</th>
<th>Individual Participation and Redress</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accountability, Audit, and Risk Management</td>
<td>Security</td>
</tr>
<tr>
<td>Data Quality and Integrity</td>
<td>Transparency</td>
</tr>
<tr>
<td>Data Minimization and Retention</td>
<td>Use Limitation</td>
</tr>
</tbody>
</table>
mHealth = Security layers

RESTful Resources
- IHE MHD
- Continua
- HL7/OMG hData
- HL7 FHIR
- DICOM WADO

Secure RESTful HTTP Transport
- IHE IUA (2013)

Internet
- TCP/IP + DNS
Basic HTTP security

- Using HTTPS – Server side TLS/SSL
  - No impact on resource content and encoding
  - Authenticated server
  - Encrypts and Integrity protects communication
  - Does Not authenticate client
    - Use Client Authentication → Hard to manage
  - Does not authenticate user (see next slide)
User Authentication

- Using HTTP Authentication
  - Basic – username/password → Not scalable
  - Form – username/password → Not plugable tech
  - Kerberos → Doesn’t work well outside organization
  - SAML – SSO profile → okay if enterprise focused
  - OAuth → best if internet focused
Healthcare - Access Control

- Healthcare needs are more complex
  - But leverage concepts: RBAC, Policy, Tags,

- Enforce Privacy Consents
  - special consent rules, episodic, expired, revoked

- Data not simply classifiable into Role
  - Leverage clinical types but need Security Tags

- Policies point at data characteristics
  - Sensitive Health Topics, Care-Team

- Break-Glass – safety medical judgement

- Residual Rules → Obligations
 HL7 PASS – Access control

Request for Service/ Credentials

Policy Decision Point (PDP)

Access Request ADI

Access Control Decision Information (ADI)

Access Control Information (ACI)

Security & Privacy Policy Rules

Contextual Information

Resource ACI

Subject ACI

Policy Administration/Security Management

Privacy Policies

Privacy Management

Interface 1

Interface 2

Interface 3

Interface 4
Access Control Engine

Context
- Break-Glass
- PurposeOfUse
- Workflow

FHIR API

User
- Role
- Authz
- Facility

Patient
- Consent
- Care-team
- Deligates

Resource
- Sec Tags
- Class
- Dates

Policies
mHealth Access Control Deployment Models
Internet User Authorization (IUA)

- Sub-Authorizations user would otherwise have
- Use-Case: Simple browser app, mobile application, embedded device, and third party service
- Enables separation of concerns: User Identity, User Authentication, User Delegation of their Rights...
- Authenticable claims: user identity, user authentication mechanism, roles asserted, purpose of use asserted, policy pointers, ..
- OAuth 2.0: JWT/SAML token - Can be proxied to SAML
- Authorization is from user perspective and may not be same as resource perspective authorization
Resource – Security Tags

- Developing story – stay tuned
- Leveraging existing work
  - Security/Privacy DAM / Ontology / HCS
  - DS4P – Metadata use
  - IHE XD* metadata model
  - Vocabulary (HL7, OASIS, ISO, etc)
- Access Control engine – Uses FHIR API too
  - FHIR resources have Provenance
  - FHIR resources have Security Tags
User Management

- Best Practice: Use federated identity
  - Leverage security layer,
  - abstract healthcare specifics from user management
  - Internet or Corporate – OAuth or SAML

- FHIR Servers need to be careful which Identity Providers they trust, and for what reason

- Might be added to FHIR – for those that really want it, it should be there in a consistently usable way
The Role of the HL7 Security WG

- HL7 Security Risk Assessment Process
- Provides training on the HL7 Risk Assessment process
- Gives direct assistance to WGs during the risk assessment process
- Liaison to mHealth
- Liaison to FHIR
Conclusion

- Building off of advancements in general Internet Security Standards (HTTPS, OAuth, SAML, Dir)
  - pluggable authentication
- Building off of healthcare standards
- Layering Security in a way that is usable for many Healthcare projects (Continua, DICOM, IHE, HL7)
- Embedding Security Tags into FHIR Resources
- FHIR – Security Audit Log Resource
Resources

HL7
* mHealth http://wiki.hl7.org/index.php?title=Mobile_Health

IHE
* web http://www.ihe.net/
* IHE Wiki http://wiki.ihe.net/

DICOM http://medical.nema.org/standard.html

My blog http://healthcaresecprivacy.blogspot.com/