Fifth National HIPAA Summit

October 31, 2002

Implementing an Enterprise Security System for Internet Authentication and Authorization

Ken Patterson, CISSP
Information Security Officer
Harvard Pilgrim Health Care

Harvard Pilgrim Health Care

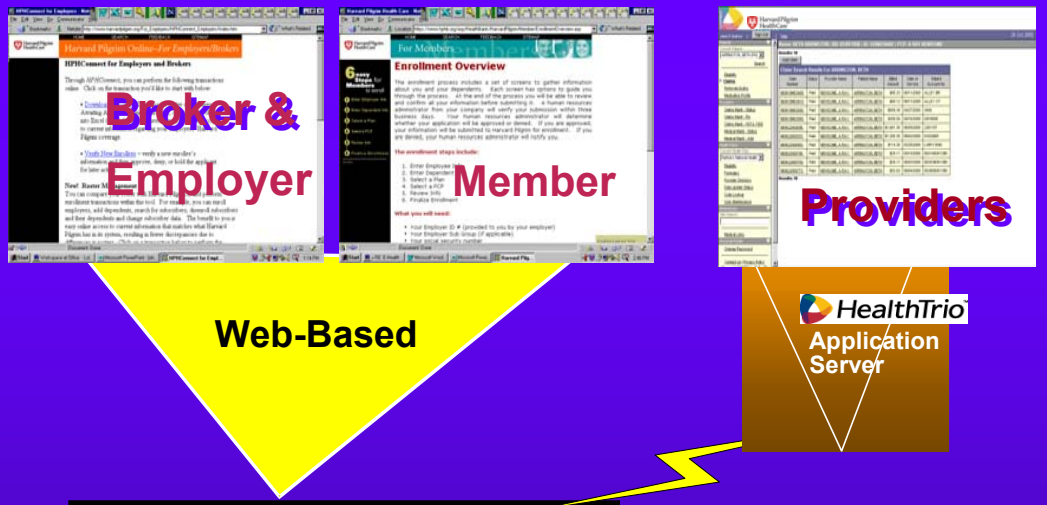
Harvard Pilgrim Health Care

- Medium size health plan serving MA, NH, and ME
- 750,000 members
- 20,000 Providers
- As a Multiple Function Covered Entity, HPHC must comply with HIPAA as a(n):
  - Health Plan – HMO, PPO, Medicare+Choice
  - Employer
  - Self Insured Health Plan
  - Provider – Nashua Medical Group
  - TPA – we provide this function for some of our Self insured groups

eHealth Program

- Leverage the web to meet demands for data and transaction simplicity
  - Better tools, better data, better decisions to create value
  - Internet may help with customer service - In response to plans offering Internet access, growing numbers of consumers access benefits info online

HPHConnect


Broker &
Employer
Member
Providers
Web-Based
HealthTrio
Application
Server
Harvard Pilgrim
HealthCare

Access Control Review

- Security Standard - Access Control
  - Context, Role Based or User Based Access
  - Emergency Access
- Security Standard - Authorization control
  - Role Based Access;
  - User Based Access
- Privacy Rule
  - Role-based access is required
  - Identify person needing access to what

Authentication Rule Review

- Entity authentication
  - Auto logoff
  - Unique user identification
- At least one of the following:
  - Biometric identification system
  - A password system
  - A personal identification number (PIN)
  - Telephone callback
  - A token system

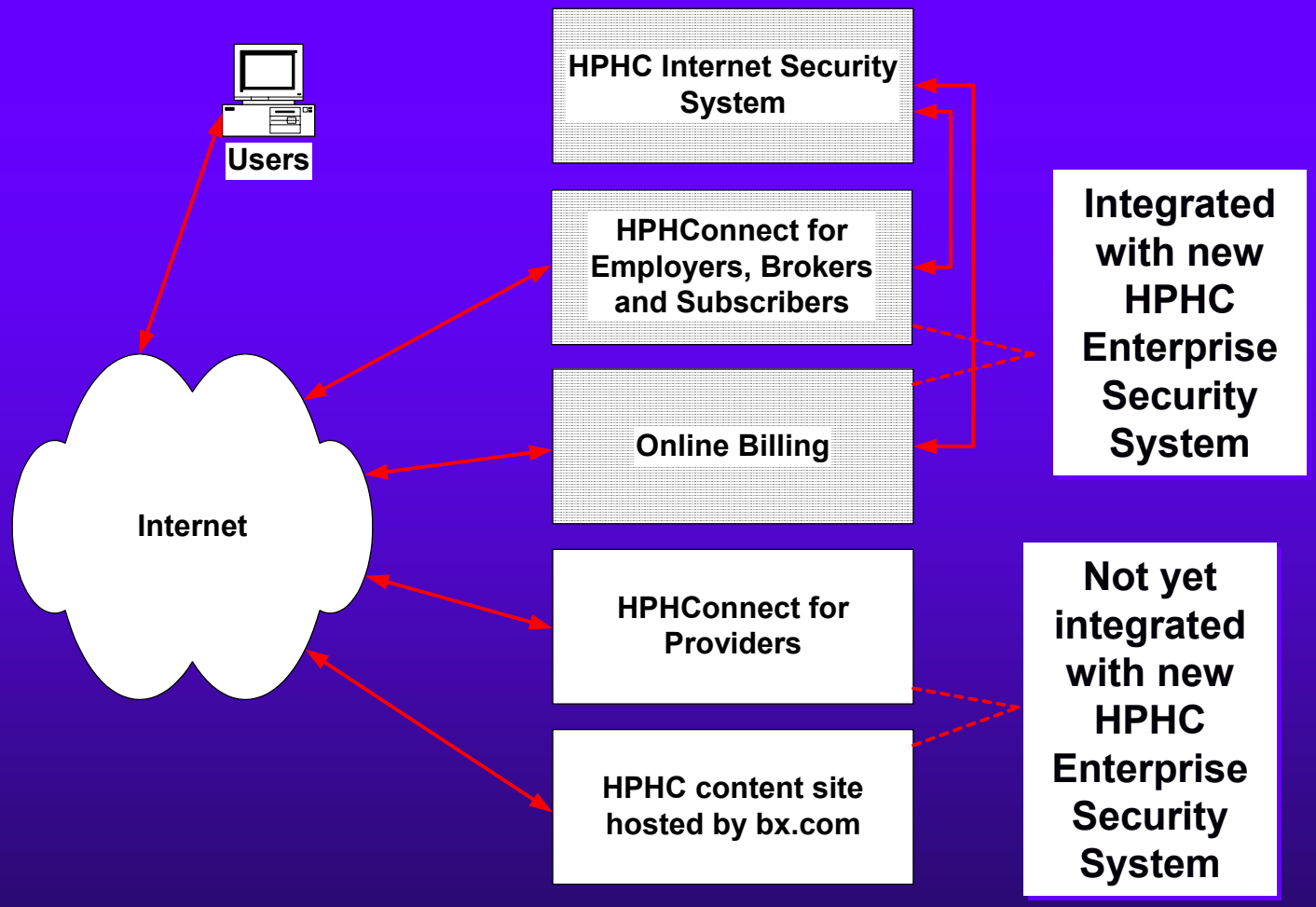
What's the Problem

- Multiple security models and tools used for authentication and authorization
- High cost of support
- Different systems = different roles and different identification
- Multiple logins using Intranet & Internet
- Policy change = changing many systems

Solution

- Implement an Internet Authentication and Authorization Project
  - Centralize management and administration of the external user access to we applications
  - Select commercial software and hardware
  - Migrate users of web applications for **Subscribers**, Employers, Brokers, and online billing.
- Continue as HPHC Enterprise Security System
  - Extend to Providers & **Member** model
  - Require all new web applications to use
  - Add Federated Services for web affiliations
  - Legacy systems integration later on

Initial Adoption Plan



Component Definitions

- Netegrity
  - Site Minder - overall operational and development environment
  - Web Agent – Protects secured resources
  - Policy Server – Maps user roles, security policies, and data to determine privileges
  - Policy Store – data store for Policy information
  - Advance Password Services (APS) – complex password rules for specific policies
  - Identity Management Services (IMS) – User administration delegation - Planned for FY 2003

Component Definitions

- Novell
  - eDirectory – end user data store, LDAP structure
- Why Netegrity & Novell
  - Industry Leaders in respective functions

If the user requests a secured service and is authenticated access to the web site is permitted. The Web Security Agent adds the user's identity and access information to the request.

Web Site configured to have pages/transactions secured by HPHC Enterprise Security System

User

Web Security Agent (Netegrity)

User Request
Web Site Response

Web Application Business Logic

Look up

Application Access Rules

The application takes the access rights from the request and uses its application specific rules to determine the specific response.

If the user requests a secured service and is not authenticated a login screen is presented by the Agent which upon user entry communicates with the Policy server to validate authentication credentials and request access information.

ID & Password
User Access Rights

HPHC Enterprise Security System

Policy Server (Netegrity)

ID/Password Check
Returns User Role & Org.

Directory Services (Novell)

The language of this communication is LDAP

The policy server uses policies (rules) to turn user profile data into a users access information.

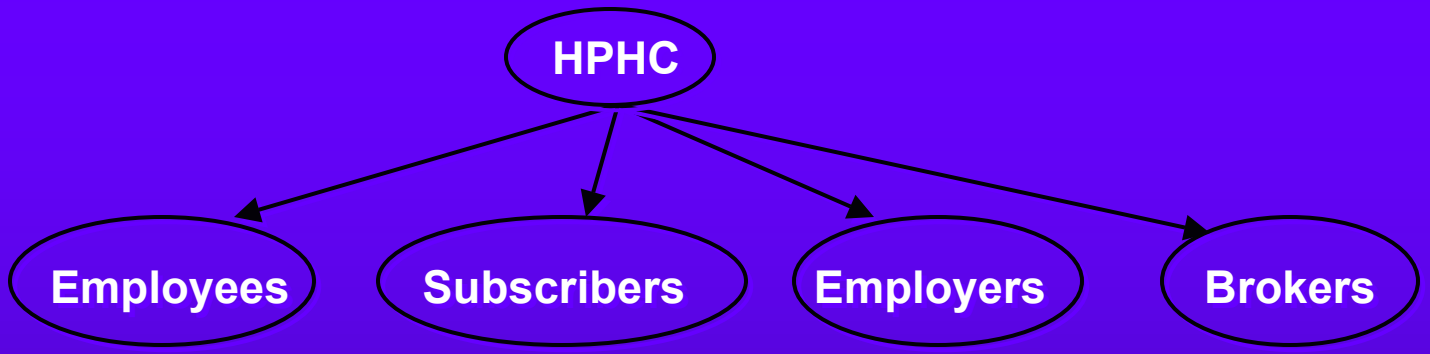
Look up

Policies

Look up

User security data (ID, Password, Role)

Directory Structure



- Flat structure allows for different security policies and better performance
- Different Ids - Business decision to bound user environments

Advanced Password Services

- Different rule by constituent
- Minimum 8 characters
- Can not use username, first name, or last name combinations
- Must use at least 1 numeric & 1 alpha
- Can not use dictionary word
- Can not use strings
- Password lockout
- Password change & aging

Subscriber vs. Member Model

- Subscriber – owner of the health plan account
  - One account for subscriber that contains all family members
  - Self-service account creation
  - Supply the following to create an account
    - Social Security Number
    - Date of Birth
    - HPHC Member Number
  - Re-enter if password is forgotten

Subscriber vs. Member Model

- Members are individuals identified on a health plan account that have a relationship to a valid subscriber
- Member model
  - Each adult member has own account with health information
  - Self-service member registration
  - Send letter with one-time password
  - Member creates ID & password

Federated Identity

The ability to correlate user names between different security infrastructures, is the core technology behind Internet single sign-on (I-SSO), and it also applies to secure Web Services and to SSO solutions within an enterprise.”

Giga 2002

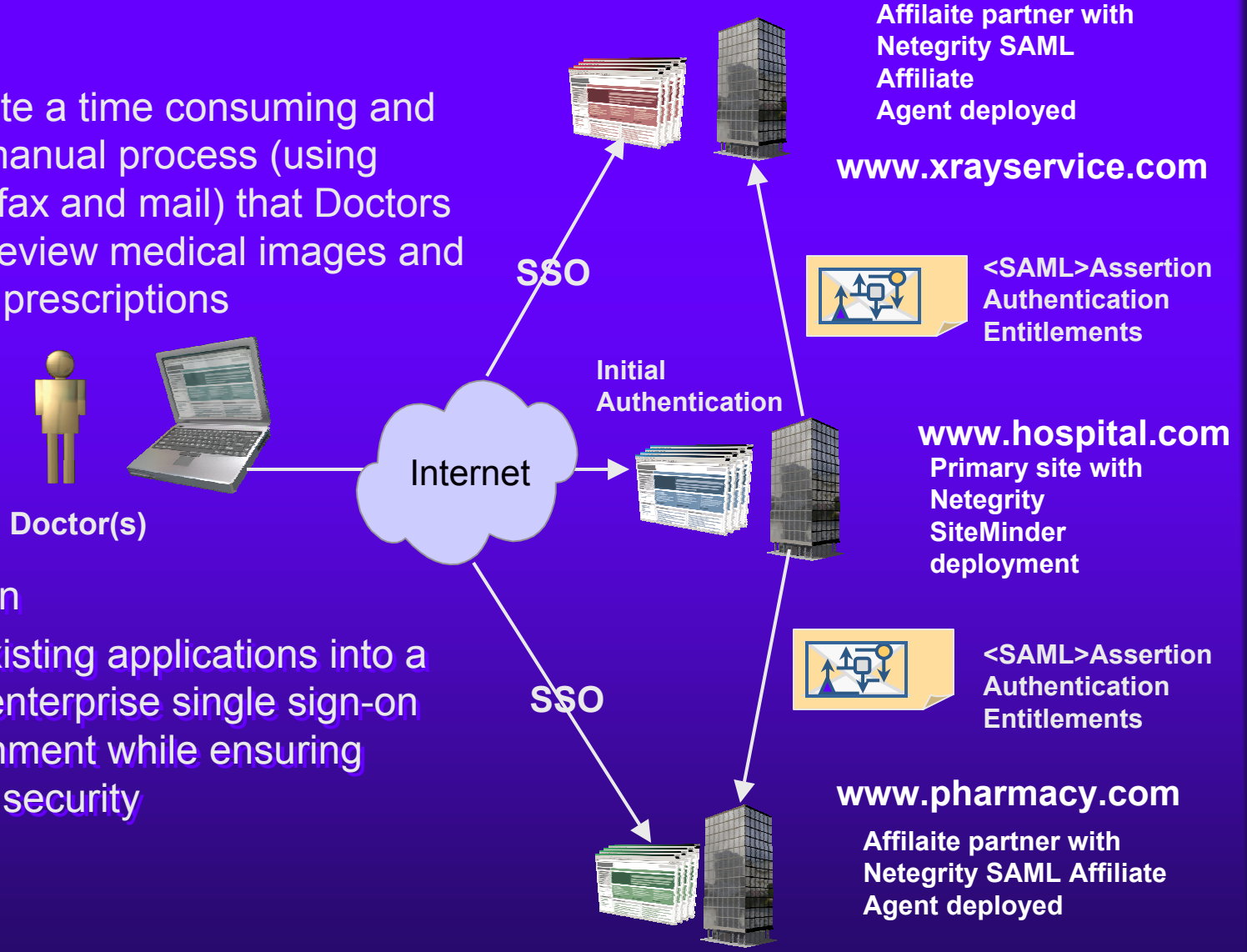
Protocol and Security Standards

- SSL (Secure Socket Layer)
  - Data encryption (SAML assertions are communicated over bilateral SSL)
- SOAP (Simple Object Access Protocol)
  - Provides an envelope for the SAML messages exchanged between a portal and its affiliates
- SAML (Security Assertion Markup Language)
  - Standard way to describe Web access-control with an open framework for sharing security information on the Internet through XML documents

Federated Identity Service for eHealthcare

Goal

Automate a time consuming and costly manual process (using phone, fax and mail) that Doctors use to review medical images and send in prescriptions

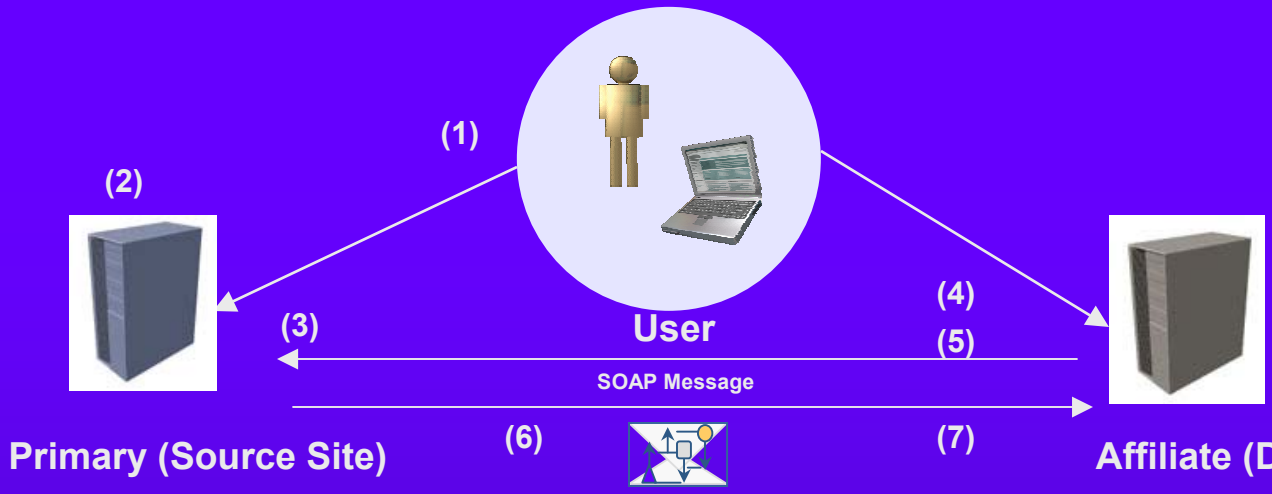


Solution

Link existing applications into a cross enterprise single sign-on environment while ensuring proper security

Harvard Pilgrim Health Care

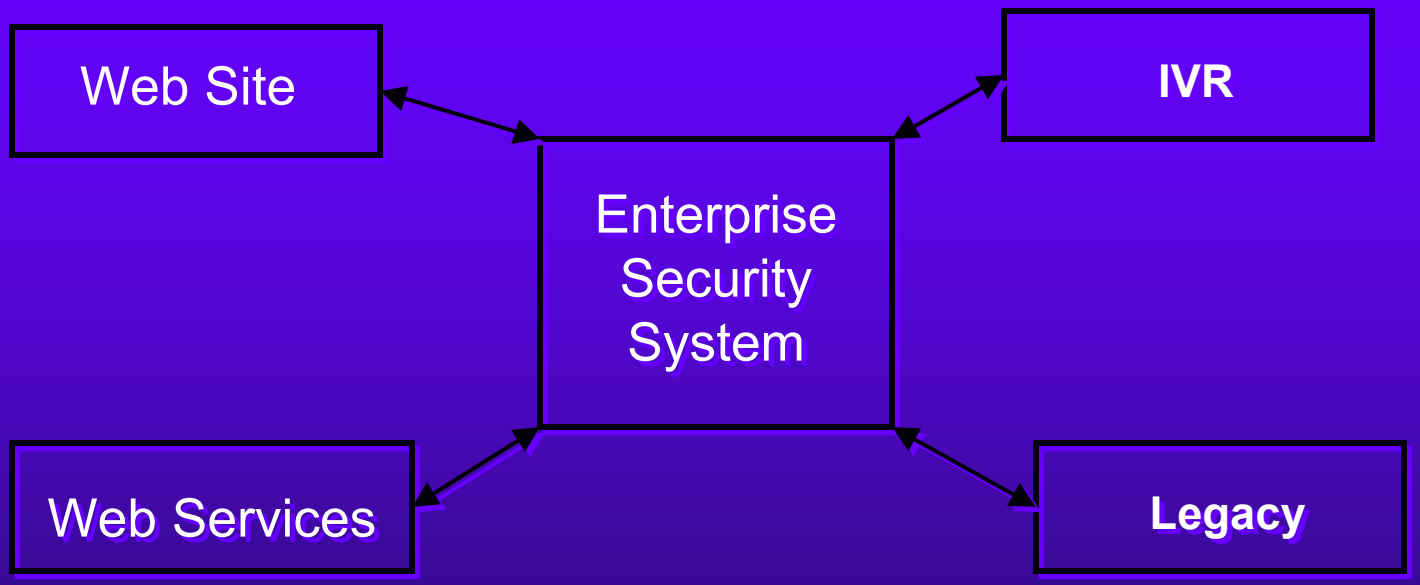
Federated Services Scenario



1. User authenticates at Primary Site directly or through redirection from Affiliate.
2. Primary Site generates SAML authN assertion, stores it in session server, creates SAML artifact.
3. When user clicks on Affiliate link, Primary Site puts SAML artifact on URL query string, followed by target Affiliate resource, e.g.,
   https://www.AffiliateSite.com?SAMLArtifact=<hexNum>&target=<affiliateResource>
4. Affiliate intercepts request and determines source site's information from SAML artifact.
5. Affiliate requests full-fledged SAML assertion from Portal thru SOAP message.
6. Portal fetches SAML assertion and sends it to Affiliate thru SOAP message.
7. Affiliate extracts SAML assertion from SOAP message and creates Affiliate's session.

Future

- Web services and web sites managed by one security resources



Interactive Voice Response (IVR)

- An electronic system
- Do you disclosure PHI?
- If yes, must use authentication
- Can be integrated with Netegrity as part of the Enterprise Security System

Budgeting For Security:

Questions?