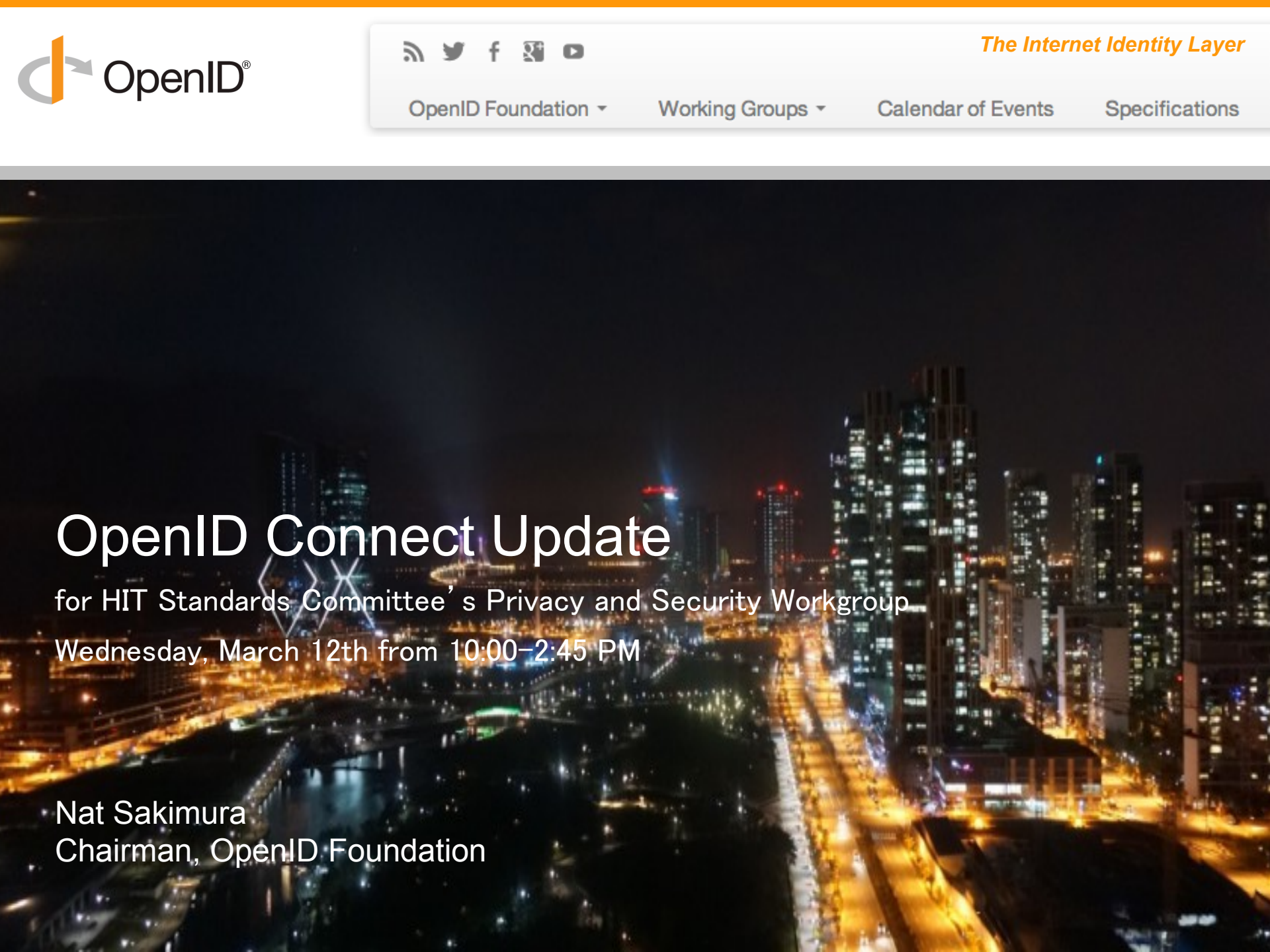

OpenID®
The Internet Identity Layer
OpenID Foundation
Working Groups
Calendar of Events
Specifications
OpenID Connect Update
for HIT Standards Committee's Privacy and Security Workgroup
Wednesday, March 12th from 10:00-2:45 PM
Nat Sakimura
Chairman, OpenID Foundation

OpenID®

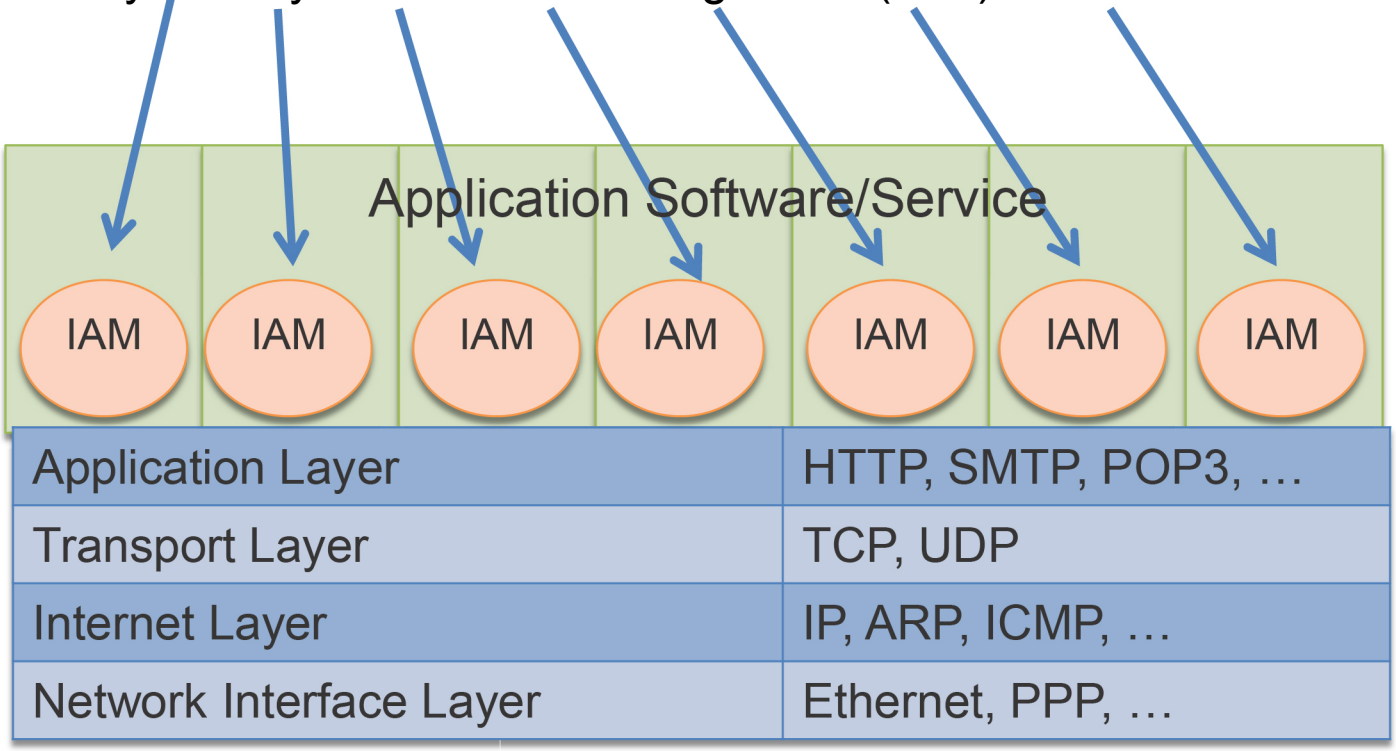
TCP/IP Reference Model

Application Layer	HTTP, SMTP, POP3, …
Transport Layer	TCP, UDP
Internet Layer	IP, ARP, ICMP, …
Network Interface Layer	Ethernet, PPP, …

OpenID®

Application Software/Service

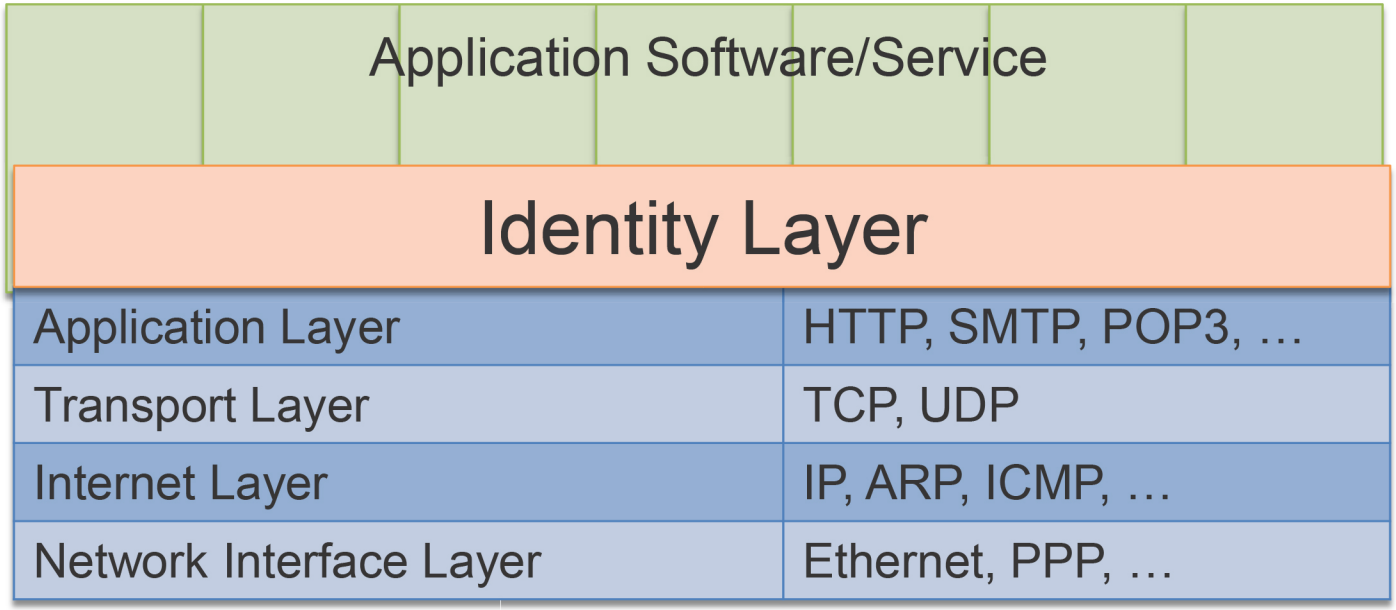
Over 95% of the internet security issues stems from lousy identity and access management (IAM).



OpenID®

Outsourcing to the Identity Layer

- enables application software / service to focus on what they are good at.



OpenID Connect is now a fully ratified international standard and is ready to be used

- OpenID Connect specifications:

- OpenID Connect Core
  - Defines the core OpenID Connect functionality: authentication built on top of OAuth 2.0 and the use of claims to communicate information about the End-User
  - http://openid.net/specs/openid-connect-core-1_0.html
- OpenID Connect Discovery
  - (Optional) Defines how clients dynamically discover information about OpenID Providers
  - http://openid.net/specs/openid-connect-discovery-1_0.html
- OpenID Connect Dynamic Registration
  - (Optional) Defines how clients dynamically register with OpenID Providers
  - http://openid.net/specs/openid-connect-registration-1_0.html
- OAuth 2.0 Multiple Response Types
  - Defines several specific new OAuth 2.0 response types
  - http://openid.net/specs/oauth-v2-multiple-response-types-1_0.html

OpenID®

An identity layer on top of OAuth 2.0

- Simple, REST based, yet secure;
- Authentication method agnostic and supports Authentication Context and step up authentication;
- Consent Framework Inside (explicit, implicit, revocation);
- Fair Information Practice Principles (FIPPs) friendly;
- Access Delegation (Access Granting) so that data can be accessed without user in presence;
- Distributed Claims model for dealing with multiple data sources;

Implementing OpenID Connect is “Simple & Easy” yet Secure

OpenID®

- Multiple open source implementations as well as commercial implementations are available.
- Options for digital signature and end to end encryption.

Open source implementations

Java
- MITREid Connect
- oleo
- OX OpenID Connect Platform

PHP
- phpOIDC

Python
- pyoidc

Ruby
- Ruby OpenID Connect

etc.

Has been looking at the NwHIN related use cases when coming up with requirements.

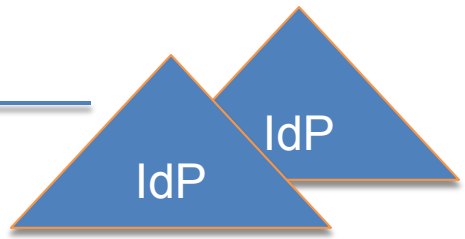
"Alice goes to a college use case"

The Internet Identity Layer

OpenID®

Alice

1.Alice downloads higher assurance authentication app and creates an account at an IdP. (May reuse her account if she has it already)



2. Consumer goes to doctor's office and have her existing health record bound to her IdP identity

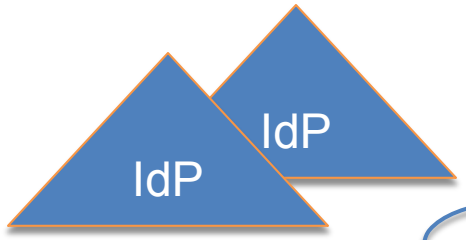
Chicago Clinic

The doctor knows Alice well so there is no issue in the identity binding.

OpenID®

"Alice goes to a college use case" (continued)

3. Now she moves to Boston to attend college. She fell sick after that.



Alice

4. Alice authorizes the access to her records at Chicago Clinic to Boston Clinic (ID Token format based structured token)

Chicago Clinic

5. Boston clinic presents the token to obtain Alice's record at the Chicago Clinic

Boston Clinic

Used in Blue Button+ & RHEx

- “Final Recommendations for RESTful Exchange Standards”
  - http://www.healthit.gov/facas/sites/faca/files/2013Aug_HITSC_NwHINPT_FINAL.pdf

Appendix: Useful Links

- OpenID Foundation
- OpenID Specifications
- OpenID Connect is here! – An Identity Layer on the internet
- OpenID Connect Stripped down to just “Authentication”
- Write an OpenID Connect server in three simple steps