Identity Professionals Recommend

An annotated bibliography

Updated and Issued from Time to Time

Contributions by the membership of IDPro

compiled by
The Body of Knowledge Committee

January 16, 2019

Preface

Beginnings aren't simple; they take courage and curiosity. Courage to try something new is applauded, whether what is new is a new profession, such as identity management, or a new discipline, such as learning federation after already mastering access certification. Regardless, setting out to do something new requires the curiosity to figure out how to do it.

A consistent challenge in our profession is finding the resources from which to learn that new thing. IDPro's mission is to help do just that: connecting professionals to learn from one another, providing opportunities to learn from experts, and building resources from which professionals can learn. And this biblio is one such resource.

The collation of suggestions from identity professionals, this biblio hopes to provide a needed resource for people with the courage and curiosity to begin something. The books, blogs, and articles referenced within span a wide range of topics and a wide range of approaches. And more that than, it offers a glimpse as to why your peers suggested the resource in the first. Knowing why someone read something is a useful clue as to the value you'll get from reading the same thing.

This biblio represents a beginning in and of itself. It is the first, of what will be many resources, that our Body of Knowledge Committee has created. I applaud the group for their courage and curiosity to begin and hope you find a gem or two in here that helps you on your beginning!

January 10, 2019
Ian Glazer
Founder and President, IDPro

Introduction

This document is intended as an a way to convey some of the accumulated wisdom and knowledge of the members of IDPro. It is in the form of an annotated bibliography, where the references may be books or any other form of knowledge transfer.

The selections are voluntarily submitted by members of IDPro and are expected accumulate over time.

The contributors' biographic details, likenesses and annotations are subject to only to light editing by the Body of Knowledge Committee.

A selection of fonts is intended to create a sense of light-heartedness and the annotations are intended to be likewise fresh and friendly.

Additional contributions are more than welcome. Please contact @bok for the best method to contribute.

The Contributors

George Dobbs

Hartford, Connecticut, USA area

Although my day job is not currently involved directly with identity, I continue my long involvement with the subject in my role as chair of the IDPro body of knowledge committee. I also am a current board member IDPro.

In previous roles I have had extensive experience in the corporate world designing and implementing both worker and customer identity systems. My most recent was in the area of so called "proofing" - how to recognize someone at a distance. I am concerned with methods of sharing knowledge and know-how.

Recommendations

1. Hoffman, *Modern Methods for Computer Security and Privacy*
2. Cameron, *The Laws of Identity*

Ian Glazer

Washington, DC, USA

I am the Vice President for Identity, Privacy, and Data Governance Product Management, at Salesforce. I look after the product management team, product strategy and identity standards work. I am also involved with major customer initiatives, briefing C-level executives, and coordinating industry-wide identity efforts.

I used to be a research vice president and agenda manager on the Identity and Privacy Strategies team at Gartner, where I oversaw the entire team's research. I got to Gartner by way of Gartner's acquisition of the Burton Group. I led the team's coverage for authorization and privacy; topics within these two main areas included externalized authorization management, XACML, federated authorization, privacy by design, and privacy programs. Other topics I researched include user provisioning, identity and access governance, access certification, role management, identity data quality, and national identity programs.

My other work experience includes program management at a financial controls and governance, risk and compliance startup, director of identity strategy at a network-based admissions control company, and product management at IBM.

I am the founder and president of IDPro, the professional organization for digital identity management. I have previously served as the Editor for the Identity Relationship Management Working Group at the Kantara Initiative. I was a founding member of the Man-

agement Council and Board of Directors for the US Identity Ecosystem Steering Group (IDESG) - the private-sector lead body described in the US National Strategy for Trusted Identities in Cyberspace.

During my decade-plus time in the identity industry I have co-authored a patent on federated user provisioning, co-authored the Service Provisioning Markup Language (SPML) Version 2 specification, contributed to the System for Cross Domain Identity Management (SCIM) Version 2 specification, and am a noted blogger, speaker, and photographer of my own socks.

I graduated from the University of Pennsylvania cum laude with a Bachelors of Applied Science in Computer Science. I studied artificial intelligence at the University of Edinburgh. I currently reside in Washington DC.

Recommendations

1. Richer and Sanso, *OAuth 2 in Action*
2. Clippinger, *A Crowd of One*

Salman (Shaq) Haq

Mclean, Virgina, USA area

A digital identity technologist currently working at a major financial institution as a CIAM product manager. In my current role I am responsible for providing a secure and intuitive authentication experience for our customers. Previous stints include an identity platform startup and a registry services provider.

Recommendations

1. Windley, *Digital Identity*

Steve Hutchinson

Richmond, Virginia, USA area

I am the Principal Cybersecurity Architect for GE Digital. After cutting my teeth in C/C++ software development and network engineering, I spent a decade as an enterprise architect in the healthcare sector focused on security and network technologies. In my current role at GE, I am responsible for strategy of one of the largest corporate identity infrastructures in the world and I oversee its evolution to provide the next generation of identity services required for GE's "Industrial Internet." I am a founding member of IDPro and honored to sit on the inaugural Board focused on

community development which has always been one of my passions. If you're ever in Richmond, VA on a Wednesday night, drop me a note for an invite to our biweekly backyard get-together.

Recommendations

1. Birch, *Identity is the New Money*
2. Hardjono, Shrier, and Pentland, *Trust::Data*
3. Richer and Sanso, *OAuth 2 in Action*
4. Nayyar, *Borderless Behavior Analytics*

André Koot

Amsterdam, Netherlands area

André is IAM and Security Consultant at Nixu Benelux and is the IAM Internal Practice Lead within Nixu.

My IAM experience comes from my financial accounting and auditing background. This background of anti-fraud detection and prevention business processes lead to research in the area of authorization principles. Currently I am working with different customers on federated identity and access architectures, both for internal and external identities (B2C, B2B, B2E and T2B - Things to Business). My motivation to participate in the IDPro BoK project stems directly from my need to share knowledge as a lecturer, author, blogger and social media activist. And from my mission to take infosec out of the realm of IT.

Recommendations

1. Cameron, *The Laws of Identity*
2. Harper, *Identity Crisis*
3. Hardt, *Identity 2.0 Keynote*

Corey Scholefield

Victoria, British Columbia, Canada area

I work in the area of public-sector digital identity management, designing access management solutions that meet requirements for information security, ease of use, and privacy. I am currently working on identity systems renewal projects for the University of Victoria, related to systems that provide accounts-provisioning, access certification, and identity life-cycle management functions. I am also working in the area of identity feder-

ation with higher-Ed colleagues connected to BCNet, CANARIE, and the Canadian Access Federation.

Recommendations

1. Windley, *Digital Identity*
2. Prasad and Rajbhandari, *Identity Management on a Shoestring*
3. Hazelton and Walker, *The CIC Cloud Services Cookbook*

Sarah Squire

Seattle, Washington, USA area

Sarah Squire is a Senior Technical Architect at Ping Identity. She is a co-author of NIST Special Publication 800-63C Digital Identity Guidelines, which outlines federated authentication standards for all US federal agencies. She serves on the Board of Directors for IDPro and the OpenID Foundation. She has been named one of the top 100 influencers in identity. Sarah holds a Bachelor of Science in Physics and a Master of Science in Information Management from the University of Washington where she was a NASA Space Grant Scholar. She is also a Certified Information Security System Professional (CISSP).

Recommendations

1. *National Strategy for Trusted Identities in Cyberspace*
2. Richer and Sanso, *OAuth 2 in Action*
3. Gilman and Barth, *Zero Trust Networks*
4. Hardt, *Identity 2.0 Keynote*

Graham Williamson

Brisbane, Queensland, Australia

Graham Williamson is an IAM consultant working with commercial and government organisations for over 20 years with expertise in identity management and access control, enterprise architecture and services-oriented architecture, electronic commerce and public key infrastructure as well as ICT strategy development and project management. Graham has undertaken major projects for commercial organisations such as Cathay Pacific in Hong Kong and Sensis in Melbourne, academic institutions in Australia such as Monash University and Griffith University and government agencies such as Queensland Government CIO's office and the Northern Territory Government in

Australia and the Ministry of Home Affairs in Singapore. Graham holds an electrical engineering degree from the University of Toronto and a Master of Business Administration from Bond University. This initiative will provide the definitive body of knowledge for the sector.

Recommendations

1. Various, *NIST Special Publication 800-63C, Digital Identity Guidelines*
2. Digital Transformation Agency, *Trusted Digital Identity Framework*
3. Williamson, *Identity Management: A Business Perspective*

Bibliography

Birch, David. *Identity is the New Money*. London Publishing Partnership, 2014, 140 pages.

I purchased this book shortly after its release after reading one of David Birch's online posts about the rise of social identity in parallel to the decline of cash in our modern world. He begins with a synopsis of how broken our definitions of 'identity' are and focuses on three primary types: personal individual identity, social identity, and legal identity. Of these, he singles out social identity (which he differentiates from social media) with the observation that "identity is returning to a concept built on networks, rather than index cards in a filing cabinet." The book is also loaded with real-world case studies to highlight and support David's conclusions. Even those seasoned professionals who feel that there's little more to learn from a book will find important insights here that have certainly shaped my own view on the future of identity, identity systems, and the frameworks that support them.
– Steve Hutchinson

Cameron, Kim. *The Laws of Identity*. 2005. URL: http://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf (visited on 12/01/2018).

It is such a fundamental piece of writing, that major topics are now part of GDPR.
– André Koot

Love the careful use of language. For example, distinguishing between claims and assertions based on the connotation or note of doubt. How sad that 2005 era vision of user control and consent has not yet been universally accepted in 2018. In 2018 this document still provides a powerful framework for thought about identities.
– George Dobbs

Clippinger, John Henry. *A Crowd of One: The Future of Individual Identity*. PublicAffairs, 2007, 240 pages.

Less on the pragmatic and more on the philosophical end of the spectrum, Clippinger's work lays highlights some of a questions our industry must face. Although a bit dated, A Crowd of One is still worth a read, if only to help trigger "big thoughts" on identity.
– Ian Glazer

Digital Transformation Agency, Australian Government. *Trusted Digital Identity Framework*. 2018. URL: https://www.dta.gov.au/our-projects/digital-identity/join-identity-federation/accreditation-and-onboarding/trusted-digital-identity-framework (visited on 01/07/2019).

The TDIF defines the requirements for a complete identity and access management deployment. It is over-the-top for most organizations but provides useful reference material.
– Graham Williamson

Gilman, Evan and Doug Barth. *Zero Trust Networks: Building Secure Systems in Untrusted Networks*. O'Reilly Media, June 2017, 240 pages.

This is an excellent primer on strong authentication techniques. Don't let the word "networks" in the title fool you. This is about securing systems using methods other than networks - namely, identity, device, and application management.
– Sarah Squire

Hardjono, Thomas, David Shrier, and Alex Pentland, eds. *Trust::Data: A New Framework for Identity and Data Sharing*. VisionaryFuture, 2016, 312 pages.

A wonderful academic discussion on the need for our identity and data security systems to adapt to a world that has moved from a physical document-based culture to one built on digital transactions. The book includes in-depth examinations of user centricity, data privacy, distributed trust authorities, universal access, and many other topics. It also includes some possible solutions (such as MIT's OPAL/ENIGMA systems). The solutions presented are more reliant on blockchain than I care for but followers of UMA will see much in here familiar and well presented. You may not agree with everything in the book but it superbly researched and documented. The 20-page bibliography alone is worth the price of admission as it allows you to delve deeper into specific topics with the source material.
– Steve Hutchinson

Hardt, Dick. *Identity 2.0 Keynote*. 2005. URL: https://www.youtube.com/watch?v=RrpajcAgR1E (visited on 12/01/2018).

Although an old video, still worthwhile: the keynote about "Identity 2.0". This presen-

tation (great style, by the way) shows that we still have a long way to go to enable access.
– André Koot

This keynote has inspired a generation of identity professionals, and highlights many deep problems with current identity infrastructure (like a lack of pervasive zero-knowledge proofs) that still exist today.
– Sarah Squire

Harper, Jim. *Identity Crisis: How Identification is Overused and Misunderstood*. Cato Institute, May 19, 2006, 250 pages.

I really love the subtitle. We should care more about Access, than about Identity. Especially in federated contexts, identity is no longer the bearer of authorizations.
– André Koot

Hazelton, Keith and David Walker. *The CIC Cloud Services Cookbook*. 2015. URL: https://carmenwiki.osu.edu/display/CICIDM/The+CIC+Cloud+Services+Cookbook (visited on 12/01/2018).

A great reference coming from the higher-Ed space on SAML SSO integrations, written in a very compelling DO and DON'T format. Many great lessons-to-learn from this one, on many topics in the identity and access management space.
– Corey Scholefield

Hoffman, Lance J. *Modern Methods for Computer Security and Privacy*. Prentice-Hall, Inc., 1977, 234 pages.

It is interesting how much the world has changed since this book came out. And it is also interesting how much is still relevant. Sure, you can smirk at some of the examples, such as a line speed of 600 characters per minute! However, the text does a good job of the basics on Authentication and Authorization - many of the considerations have remained the same. Although, to be fair, this book predates public key technology and packet switched networks were not yet widely adopted. Chapter 5 is an excellent introduction to ciphers leading up to the P-boxes and S-boxes used Data Encryption Standard. Good background for more modern crypto! There is also a long bibliography of historical interest.
– George Dobbs

National Strategy for Trusted Identities in Cyberspace. 2011. URL: https://www.nist.gov/sites/default/files/documents/2016/12/08/nsticstrategy.pdf (visited on 01/02/2019).

This paper was produced by the US Government during the Obama administration and outlines in basic English why the United States does not want to have a central government directory or a central government identity provider. It speculates as to how government could enable the private sector to fill that gap in very smart and innovative ways that protect citizen privacy and prevent government overreach.
– Sarah Squire

Nayyar, Saryu. *Borderless Behavior Analytics: Who's Inside? What're They Doing? 2nd Edition*. Ankur Chadda, 2018, 424 pages.

This is one of my new favorite books in the identity and cybersecurity space. Saryu has brought together insights from over a dozen CISOs and CIOs give their views on the state of cybersecurity in the age of zero trust. The common thread in all of their perspectives is "the amplified view of the value of identity and access." I love the book not only because it covers a wide array of identity topics but because it is visionary in its view of what's important now and in the immediate future. I particularly appreciate that, in the end, Saryu takes the input of those contributing security professionals and uses them to provide clear requirements and use cases for what's next: such things as Predictive Security Analysis, Identity Analytics, and User and Entity Behavior Analytics. A fantastic read for any security and/or identity professional.
– Steve Hutchinson

Prasad, Ganesh and Umesh Rajbhandari. *Identity Management on a Shoestring*. 2012. URL: `https://www.infoq.com/minibooks/Identity-Management-Shoestring` (visited on 12/01/2018).

In some contexts, IDAM middleware doesn't get much love. And sometimes, not much budget. In those cases, take some tips from these authors as they assemble an admirable collection of open-source technologies, and an identity-management architecture (IMA) for enterprise. A great read, recommended to me by a respected IDAM colleague.
– Corey Scholefield

Richer, Justin and Antonio Sanso. *OAuth 2 in Action*. Manning Publication, Mar. 2017, 360 pages.

OAuth is a very powerful tool. Its power comes from its flexibility. Flexibility often means the ability to not only do what you want to do, but also the ability to do things in an unsafe way. Because OAuth governs access to APIs, which in turn gates access to your important data, it's crucial that you do use it in a safe way by avoiding antipatterns and using best practices. Stated differently, just because you have the flexibility to do anything and deploy in any way, doesn't mean that you should.

Thankfully, Justin and Antonio provide pragmatic guidance on what to do and what not to do. They acknowledge both the "I just want to get this done" and the "I want to make sure this is secure" mindsets you have.
(Full disclosure... I wrote the Foreword for the book)
– Ian Glazer

This is not only the most comprehensive book available about OAuth but it is also the most accessible, which is a neat trick to pull off. Justin and Antonio expertly guide the reader by providing an overview of what OAuth is by talking about why it came to be and what it was meant to solve. They describe the flow between all of the different players in the framework followed by dedicated chapters for each one of those participants before presenting the reader with more advanced topics. One of those is easily the best description ever written about dynamic client registration, which I have referred to many times in our own implementation. As a cybersecurity architect, I particularly appreciate the 50 pages of detailed discussion about common vulnerabilities of different parts of the system. It's a fantastic resource that you'll not only refer to again and again, but also a resource to lend to those new identity professionals that you're trying to grow.
– Steve Hutchinson

This is a textbook on the theory and intent behind OAuth and OpenID Connect. It includes not only history and reasoning behind the development of these standards, but also easy tutorials and sample code allowing the reader to build his own providers and clients in an afternoon. Highly recommended.
– Sarah Squire

Various. *NIST Special Publication 800-63C, Digital Identity Guidelines*. 2017. URL: `https://pages.nist.gov/800-63-3/sp800-63c.html` (visited on).

NIST provides a succinct summary or access control issues and is considered a seminal publication to guide IAM strategy and deployment.
– Graham Williamson

Williamson, Graham. *Identity Management: A Business Perspective*. MC Press Online, Boise, ID, 235 pages.

It was written to help business people understand IAM, the trends and the responsibilities of those collecting, using and storing identity data.
– Graham Williamson

Windley, Phillip J. *Digital Identity: Unmasking Identity Management Architeture (IMA)*. O'Reilly Media, 2005, 266 pages.

I've used Phil's resource before in several contexts, including: a) Course textbook for an online course in enterprise identity management b) Selecting some chapters as "homework assignments" for newcomers to our IDAM Team c) Educating decision-makers on the governance aspects of identity management in enterprise.
His chapter 15 example of an Identity Management Maturity (IMM) model is outstanding.
– Corey Scholefield

This book starts with the basics of digital identity - what you know, what you have, what you are. From there it provides a broad overview of many important concepts. It is an accessible book and caters to beginner and expert readers alike and best of all, it can be read cover to cover in one sitting.
– Salman (Shaq) Haq