



center for applied identity
management research

An Applied Research Agenda for Confronting Global Identity Management Challenges



**Report of the CAIMR Identity
Management Research
Agenda Workshop
May 2009**

An Applied Research Agenda for Confronting Global Identity Management Challenges

About CAIMR

The Center for Applied Identity Management Research (CAIMR) is a non-profit corporation comprised of representatives from government, corporate, and academic institutions who share a common interest in the multi-faceted aspects of identity management. CAIMR is a trusted public-private partnership bringing together cross-disciplinary experts in criminal justice, financial crime, biometrics, cyber crime and cyber defense, data protection, homeland security, risk management and national defense. CAIMR is an applied research organization that studies identity issues, their social implications, and the processes, technologies and polices designed to deal with them. The emphasis is on discovering real world solutions to the challenging identity management problems faced by society.

CAIMR's partners are:

- **Academic:** Indiana University and The University of Texas at Austin
- **Corporate:** LexisNexis, IBM, Intersections, Cogent Systems, Visa, Equifax, Symantec Corporation, Lockheed Martin, Fair Isaac, Wells Fargo & Company, Dragnet Solutions, and ID Experts
- **Government & Law Enforcement:** The Department of Defense, United States Secret Service, and United States Marshals Service.
- **Non-Profit:** Identity Theft Assistance Corporation (ITAC), Information Technology Association of America (ITAA), and National Center for Missing and Exploited Children (NCMEC)

The Authors

Gary R. Gordon, Ed.D.
Executive Director, CAIMR
Senior Scholar in Identity Management, Indiana University

Suzanne Barber, Ph.D.
Director, Center Excellence in Distributed Global Environments (EDGE)
AT&T Endowed Professor, Electrical and Computer Engineering
The University of Texas at Austin

Fred H. Cate, J.D.
Director, Center for Applied Cybersecurity Research
Distinguished Professor, School of Law
Indiana University

CAIMR and the authors express their sincere gratitude to the subject matter experts who generously shared their time and knowledge at the workshop. The participants are listed in the appendix. This report reflects the discussion and conclusions reached during the workshop, without identifying particular participants or their organizations. The authors of the report are solely responsible for its content.

Acknowledgements: The following individuals assisted in the documentation of the event and contributed to the final report: Shiu-Kai Chin, Syracuse University, Richard Scott, The University of Texas at Austin, Thomas Regan, CAMIR, and L. Richard Fischer, Partner, Morrison & Foerster LLP.

Introduction

Identity management, while not a new issue, has been exacerbated by our rapidly expanding digital world and the challenges it presents both domestically and globally. The universality of the Internet has led to the ready availability of personal identifier information. While this has had a positive impact on the economy and has allowed unprecedented access to data necessary for decision-making, it has also provided criminals and terrorists with access to data that they can use to harm individuals, commerce, and government. Criminals and terrorists are migrating to the digital world as it is more profitable and has less risk. They know that personal identifier information is a valuable commodity, so are willing to steal it and eager to sell it for profit. The resultant escalation of cyber crimes and cyber attacks has resulted in the need for improved cyber investigations, security and cyber defense.

As is apparent from the breadth of CAIMR's partners and the participants in the workshop, all sectors of society, as well as individual citizens, are grappling with these challenges. Individuals must protect their identities by paying close attention to their financial statements, by using only trusted online services that employ strong authentication, and by guarding their personal identifying information online, in print, and during telephone and face-to-face interactions. In the commerce arena, knowing the true identity of a person or entity is essential for trusted transactions. The financial services industry depends in large part on identity management in order to sustain online banking, online investment management, card-not-present credit transactions, and the like. The health care industry cannot operate without a secure identity management system, as they are responsible for sensitive medical information that must be shared between and among physicians, health facilities, and health insurers. Identity management is essential to government on many levels. Federal and state government entitlement programs and local, state, and federal agencies which issue personal identification documents, e.g. Social Security cards, passports, drivers' licenses, depend on accurate personal identifier information and authentication processes. Agencies which grant security clearances, permission to enter government facilities, and access to government computer systems and databases are all dependent on identity management.

Because identity management is tantamount in our society, it is a major focus for criminals and organized crime groups, both domestic and international. This, in turn, has created a significant challenge for law enforcement at all levels as they work to prevent, detect, investigate, and prosecute the many crimes which are facilitated by identity theft and crime in both the physical and cyber worlds. Many of the crimes facing society have identity components. Registered sex offenders often mask their identities to hide in plain sight and lead "normal" lives. Individuals with poor credit assume the identities of others, often within

their families, to open new accounts and to obtain mortgages and other loans. Illegal immigrants are able to assume or create an identity in order to gain legal status. Cyber criminals prey on individuals or organizations to gain access to personal identifier information. Cyber criminals work individually or in organized groups. They may attack from outside a company or be insiders working alone or in concert with others. Data breaches that occur as a result of criminal activity (as opposed to those which are a result of lost hardware and software) are extremely lucrative, as the personal identifying information can both be used to commit identity fraud and sold to others who will do the same.

Cyber attacks also pose threats to the critical infrastructure and require new cyber defense strategies. Protection of assets such as telecommunications, public health, and the power grid, are necessary for the functioning of society. In combat zones, war fighters must be able to identify people and determine if they are friend or foe, as well as if and how much of a risk they present. The challenge is to provide the war fighter with accurate information in real time.

Since identity management problems impact all aspects of our society, there is a need for more collaborative effort to mitigate or solve them. In general, most sectors work on the problems they face within their own space. Opportunities to work together have been few and are themselves fraught with issues. Corporations and government agencies may not be willing to disclose the amount of fraud with which they are faced, for fear of economic repercussions. They may not be willing to share the data they have, especially that containing personal identifier information for fear of it being used for nefarious purposes or "falling into the wrong hands," or because there is no mechanism by which it can be shared securely. However, because the opportunity for identity management-related crime is growing exponentially, no one sector can mitigate or solve it alone. Instead, individuals from many different corporate, government, and academic institutions with expertise in varied disciplines, including information technology, informatics, computer and electrical engineering, information assurance, and security, policy and regulation formation, business, criminal justice, and law, must work collaboratively.

The mission of the Center for Applied Identity Management Research is to meet current and future identity management challenges through a multi-disciplinary applied research agenda aimed at providing pragmatic solutions and incorporating the perspectives of key academic, governmental, and commercial entities.

CAIMR's objectives are:

- ❖ Establish a trusted public/private partnership that brings together identity management thought leaders representing all sectors of society to

- marshal their resources to solve the key challenges in identity management. This includes the required academic disciplines.
- ❖ Leverage CAIMR organizational structure to facilitate best practices for information sharing, as well as protection of the data owner's intellectual property. This will enable data for research purposes to be shared through agreements that articulate the understanding of how it will be used, accessed, shared, and communicated. This allows the data owner's to comply with legal, regulatory, and best practices.
 - ❖ Using this collective expertise and experience, define the key challenges and a strategic applied research agenda to address them.
 - ❖ Leveraging trusted relationships, identify the resources necessary to conduct the research, including access to relevant data sets, expertise of those faced with the challenge and those providing solutions, and access to the software and hardware to conduct the research.
 - ❖ Through the academic partners, bring together the necessary disciplines to conduct independent applied research.
 - ❖ Use the organizations that help define the research agenda and specific projects to review the results, disseminate them, and encourage implementation.

To that end, CAIMR held the Identity Management Research Agenda Workshop in December 2008. It brought together thought leaders (see Appendix) to define the current and near future challenges in identity management and to build a research agenda to address those challenges. This report reflects the seminal discussions that helped shape the findings and provide the basis for the first phase of an applied research agenda for confronting the global identity management challenges we face.

Current and Near Future Identity Management Challenges

In the beginning of an interview after the launch of CAIMR in October 2008, an astute reporter asked what appeared to be a simple question, "With all of the advanced technologies and the efforts by various groups over the last ten years, why haven't we solved the identity management problem?" The complexities discussed in the introduction section provide part of the answer. The key challenges discussed at the workshop provide the rest. What is needed is a holistic approach that focuses on the societal challenges posed by identity management that goes beyond the current symptoms approach.

A pre-workshop survey was sent to all participants asking about the top three identity management challenges faced by their organizations, a description of a threat scenario for each challenge, current capabilities of their organizations to mitigate the threat and desired new ones, and what research studies they feel would meet the challenges. A compilation of the surveys was presented at the

beginning of the workshop. The ensuing discussion focused on threat scenarios, the existing capabilities to mitigate the threats, and the needed capabilities. Based on the results of the survey and the ensuing discussion, it became clear that a portfolio of requirements, capabilities, customers, and roadmaps is necessary to:

- identify a benchmark of requirements
- track requirements as threats change and new threats appear
- assess how well current capabilities address current requirements
- determine the gaps where no capability exists to satisfy requirements
- identify and compare priorities and roadmaps of various customers to satisfy requirements.

The key challenges listed below provide insight into the problem and point the way to potential solutions. These challenges cannot be dealt with in isolation, as there is considerable overlap. For example, in focusing on a particular cyber issue for research purposes, it may be necessary to address information sharing hurdles, ensure the protection of the information, understand the policy implications, and determine privacy concerns and address them.

The Cyber Challenge

The most discussed identity management challenges during the workshop were those posed by current and emerging cyber threats. These threats impact trusted transactions in online commerce, cyber investigations, authentication of individuals or organizations who want to gain access to services, systems, and facilities, the authentication of entities communicating in a network, the protection of personal identifier information, information sharing for cyber defense purposes, and protection of the critical infrastructure. While this challenge was discussed the most, two other areas of major concern were mortgage and healthcare fraud. These three constituted the top societal challenges where identity management plays a major role.

The Information Protection Challenge

Every sector of our society, from individuals to business to the public sector, faces the challenge of protecting personal identifier information. It is readily apparent that solutions are needed. Data is “leaking” – through insecure data systems, by insiders, through breaches, by theft -- across all sectors. Every organization and individual has a need to protect some sort of data – personal, financial, government, medical -- from being used for nefarious purposes. Criminals are eager to acquire such data as it facilitates their access to financial gain, credit, medical services, and government entitlements, and provides the information needed for economic espionage and terrorist acts against the critical

infrastructure and the homeland. It also allows them to mask their communications and remain anonymous.

Besides protecting the existing data, it is essential to improve authentication systems, so that it is possible to verify a person or entity claiming an identity is actually that person or entity. Better authentication will make it more difficult for criminals to gain access to data and will render that which they do access useless. It will begin to inhibit the criminal and terrorist activities that personal identifying information facilitates.

The Information Use and Sharing Challenge

Since 9/11, there has been much discussion, especially within the federal government, of the need for information sharing among entities and across sectors. However, it still remains a major challenge. Inhibiting information sharing causes system vulnerabilities and threats to the critical infrastructure, and makes it easier for criminals to operate, as they know that what they do within one organization will not be revealed to others.

Without information sharing, the large amounts of information held by organizations and entities cannot be fused. Fused data -- particularly biometric, biographic, and digital -- would provide faster decision-making powers for those who are authenticating identities. Many programs have been attempted, but have failed as they have required various public and private sectors to share relevant information. Such sharing is difficult given policy, regulatory, and privacy requirements.

The Policy and Privacy Challenge

As alluded to above, a number of technologically sophisticated government sponsored programs that held promise for solving some major security problems have not been successful. Their demise was, in part, a result of omitting policies addressing the use and protection of the data. Technological solutions, no matter how elegant, are not feasible without the incorporation of proper policies from the very beginning. However, some policies and regulations are overly restrictive, making it difficult for information to be shared. The ongoing debate over security and privacy – utilizing personal identifier information for decision-making vs. restricting the use of data to protect an individual's privacy – is counterproductive. Increasing security at the expense of privacy or the reverse will not make these programs work. Rather, the responsible and productive use of information may enhance the privacy of the individual. Realistic and pertinent laws, policies, and regulation are needed to allow the necessary information sharing that can accomplish this. In order for this to occur, solutions must be

based on empirically based results to assuage the concerns of all stakeholders including legislators, citizens, and privacy advocates.

Threats and Mitigations

Workshop participants identified over one hundred scenarios including threat scenarios (describing how identity can be compromised) and threat mitigation scenarios (describing how identity can be protected).

Identified threat scenarios span every industry, government agency and personal use for the Internet. Examples include:

- Account take-over fraud against bank/retailer/healthcare provider
- Attack on an identity database
- Cyber threat to enterprise attribute-based controls
- Insider misuse of corporate assets/information
- Gain access to credit/financial data by fraud
- Using Zombie networks to extort or hijack identity
- Identity fraud in thin file situations
- Relating real-world identities to 2nd life identities

To remain sufficiently “ahead of the threat curve,” it is necessary to envision the threat Scenarios and offer capabilities for implementing threat protection and mitigation scenarios in response to anticipated threats.¹ At the workshop, it was agreed that the United States, as a nation and industrial leader, is failing to anticipate the threat and to drive new solutions in response to anticipated threats. CAIMR members are committed to changing this equation.

Existing Capabilities

A wide range of solutions exist to (1) declare identity and (2) protect the digital representation of that declaration of identity, and (3) guard against identity theft and misuse.

Two primary types of solutions were identified as capabilities to *declare identity*:

- Biometric, which are capable of recognizing entities and establishing identities (for individuals or equipment) based on physical or behavioral traits.
- Biographic or information-based, which use information about entities to establish identity (e.g. SSN, drivers license, date of birth, security question, URL, IP address, etc).

¹ CAIMR employed the AWAREness Suite™ to capture, relate and analyze Threat Scenarios, Threat Protection Scenarios, Solutions, Customers with Identity Management Requirements, and Customer Roadmaps to anticipate and satisfy Identity Management requirements.

Solutions identified as capabilities to *protect the digital representation of identity* included:

- Data encryption, which transforms information to make it unreadable without special information to decrypt the data.
- Database security measures, which guard data repositories (e.g. firewalls)
- Digital rights management, which provides access controls on the use of identity information.

Solutions identified as capabilities to *guard against identity theft and misuse* include:

- Policy management, which relies on legislation and business policies to guard against identity theft.
- Breach detectors, which monitor unauthorized system intrusions and/or data acquisition and provide alerts.
- Auditing, which monitor behavior and use of identities to detect unauthorized use
- Authentication solutions, which establish that those using an identity actually own the particular identity.

Even with all of these solutions, the battle to establish identity, protect identity, and guard against theft and misuse is being lost. New solutions are not arriving fast enough and are not sophisticated enough to stop (even thwart) those aiming to falsify, take and use the identity of others.

What happens to a nation when the identity of individuals, organizations and resources is no longer trusted? Can any interaction with the nation and its people, organizations, and resources be trusted and consequently valued? Identity management is a serious problem requiring serious recognition and investment.

Needed Capabilities

The data in the AWAREness Suite™ (capturing, relating and analyzing threats, solutions, and customer roadmaps to meet threats) shows that between 20% and 50% of the identified threat scenarios are being addressed (to some degree or another) with the available solutions. However, new solutions must evolve and advance faster than these threat scenarios to anticipate and defeat the threat.

CAIMR will identify and seek investments for these needed future capabilities. Solutions considered at the workshop include:

- Assuming an offensive, proactive mode instead of the typical passive, reactive mode. Examples include agent technology at The University of

Texas Center for Excellence in Distributed, Global Environments which is capable of proactively, continually, and in real-time keeping trustworthiness assessment values on entities offering data and exhibiting behaviors on the Internet.

- Combining the strengths of biographic data and biometrics (e.g. combining the retinal scan and the SSN).
- Education to discourage, not assist, identity theft.

Framing the Research Agenda

An overarching research agenda will evolve as CAIMR serves as an authoritative source for (1) what is required to define and protect identity, (2) available solutions to meet those requirements and (3) means to measure requirements, solutions and roadmaps to successful Identity Management. In this iterative process, CAIMR will:

- Define, disseminate, and advocate a common, agreed-upon set of terms and definitions to support a national dialogue about identity management challenges and solutions. The need for commonly agreed uniform definitions was raised several times during the workshop. Connotations and definitions of the terms *identity*, *identity management*, and *identity theft and fraud* vary greatly among organizations and within particular contexts. While it may be difficult to gain universal consensus on these and other key terms, any effort to work toward this end, and develop at the least a set of definitions to apply to the various aspects of identity management, would enhance the research effort and clarify issues that are being discussed in the community. This is crucial, especially as the concept of a digital identity continues to expand.
- Provide a model for the use of data for identity management research. It was noted in all the sessions that gaining access to relevant data sources is imperative in order to conduct applied research projects whose ends are actionable results. Several barriers, some real and some perceived, have made data unavailable for identity management research. Even where there is a recognized need and desire to share data for research purposes, problems arise to thwart the cooperation. The workshop attendees discussed how a trusted public/private partnership, such as CAIMR, provides a model that will allay concerns, encourage participation, and demonstrate how this task is compatible with current regulatory compliance. This structure allows for the sharing of data in a neutral, non-competitive, secure, and confidential environment.
- Create and maintain a portfolio of evolving requirements and solutions across industry, government, and academia.

- Provide gap analysis of
 - ❖ Identity management threats in order to determine what capabilities are required.
 - ❖ Current solutions to provide direction for R&D projects and commercialization opportunities.
 - ❖ The identity management roadmaps employed by key industries and customers, so that specific action plans can be formulated.
- Help individuals and organizations to manage identity by
 - ❖ Establishing best practices (business process and tools) in identity management and benchmarks by which to measure their effectiveness.
 - ❖ Establishing identity management scorecards (business processes and tools) to measure the degree of compliance to identity management best practices.

The Agenda

Many ideas for research projects to meet the challenges in the areas outlined which evolved from the workshop discussions. Combined with the iterative process above, they will help frame CAIMR's applied research agenda.

The Cyber Challenge

- Cyber crime investigations including advanced processes, methods, and tools to determine digital identities and to link them back to physical ones
- Cyber security (Preventions and detection, data protection, attack vectors)
- Cyber defense (increased information sharing)

The Information Protection Challenge

- Current and future attack vectors: vulnerabilities and how they can be eliminated
- Data breaches: analysis of the characteristics of the breaches, the amount of identity theft and fraud associated with the stolen data, the risks posed by different types of breaches, and how the breaches occurred

The Information Sharing Challenge

- Assessment of information sharing and collaboration models that incorporate strong policy and privacy components for enhancing identity management across large government organizations
- Collaboration models for the sharing of information in order to protect the critical infrastructure

- Test-bed environments to study the impact of fusing shared data sets such as biometric and biographic information to improve authentication

The Policy and Privacy Challenge

- Assess the effectiveness of implemented policies (legislation or regulation) to address identity management issues such as credit freezes to protect future harm from identity theft or Red Flag Regulations
- Assess the impact of proposed identity management policies

Call for Action

The consensus of the workshop participants is that a bold, comprehensive, and innovative applied research agenda is required to solve the identity management challenges faced by society today and in the future. To that end, the following recommendations are offered:

Recommendation 1: Create and maintain an identity management portfolio that identifies threats, current capabilities, and needed capabilities.

This process began prior to the workshop through a short survey of the participants, discussed during the workshop, and expanded in this report. It is a first step to mapping the current landscape and the future needs. CAIMR will continue to work on this iterative process and will reach out to other groups for their input and assistance. The target date for completion of this initial review is June 2009.

Recommendation 2: Identify and prioritize the gaps on an on-going basis.

Building on the work in Recommendation 1, the gaps will be identified and prioritized. Identifying the gaps will enable understanding of the evolving threats, indicate areas where solutions need to be developed, and provide direction to organizations to address “red flag” areas in their identity management roadmaps. Prioritizing the gaps will lead to CAIMR defining explicit research goals and objectives, which will provide direction for the research agenda. This process will be completed shortly after the data is available from Recommendation 1.

Recommendation 3: Address research impediments, including the need for agreed upon definitions of key terms and the limited access to relevant data.

While it may be difficult to gain universal consensus on key terms, any effort to work toward this end, and develop at the least a set of definitions to apply to the various aspects of identity management, will enhance the research effort and clarify issues that are being discussed in the community.

Gaining access to relevant data sources is imperative in order to conduct applied research projects whose ends are actionable results. CAIMR is committed to developing models for data sharing.

Both of the above efforts are in progress and will be made available as soon as completed.

Recommendation 4: CAIMR should conduct a review on an annual basis to insure its research agenda continuously addresses the current and most significant identity management challenges faced by society.

CAIMR is committed to conducting an annual workshop similar to the December 2008 one. The next one will be scheduled towards the end of 2009. It is also considering workshops and meetings that will address some of the issues raised above in greater detail.

Conclusion

CAIMR's first workshop brought together experts from all the key stakeholders to address the identity management challenges faced by society. It was evident the participants believed that the stakes are high and that dealing with this complex problem will require a deliberate investment of time, intellect, and treasure.

The consensus is that there is a strong need for an organization such as CAIMR, as it brings together the essential stakeholders and ingredients for success. CAIMR's partners and its organizational model place it in the unique position of being a leader in identity management research and serving as a national resource for: (1) facilitating a dialogue on identity management, (2) developing a portfolio of requirements and solutions, (3) establishing benchmarks and scorecards, and (4) setting the applied research agenda to fill identified gaps. The Identity Management Research Agenda Workshop was an important first step in meeting these objectives and was significant in that the stakeholders pledged their full participation in moving forward.

APPENDIX

CAIMR Identity Management Workshop Participants

Suzanne Barber, Ph.D.
Director
Professor
University of Texas at Austin

Mark Grantz
Special Agent
Criminal INTEL Section - CID
United States Secret Service

Ben H. Bell III
Special Advisor to the President
Cogent Systems

Diana Greenhaw
Information Security Specialist
Corporate Risk & Compliance
Visa U.S.A. Inc.

Shiu-Kai Chin, Ph.D.
Professor, Engineering and Computer
Science
Syracuse University

Bob Gregg
CEO
ID Experts

Joanna P. Crane
Division of Privacy and Identity
Protection
Federal Trade Commission

Dennis Groseclose
Vice President, Strategic Development
and Advanced Programs
Lockheed Martin

Tom Dee
Director, Defense Biometrics
Office of the Secretary of Defense

Gregory C. Hall
Chief, Identity & Access Management
Division
Office of the National Director of
Intelligence Programs

Shawn Elliott
DoD Biometrics Task Force
Office of the Secretary of Defense

John "Jack" Hermansen
CTO, Global Name Recognition
IBM

Steve Emmert
Director, Government and Industry
Affairs
Reed Elsevier

Michael Higgins
Chief Security Officer
LexisNexis

Rick Fischer
Partner
Morrison & Foerster LLP

Andrew Jennings
Chief Research Officer
Fair Isaac

Gary R. Gordon, Ed.D.
Executive Director
Center for Applied Identity
Management Research

Douglas "Scott" Johnson
Deputy Assistant Director
Office of Investigations
United States Secret Service

Rick Kam
President
ID Experts

Steve Myers
Assistant Professor
School of Informatics
Indiana University

Thomas Regan
Senior Policy Advisor
CAIMR

Rick Scott
Assistant Director, EDGE
University of Texas at Austin

Merle Sharick
VP-Manager
Mortgage Research Asset Institute

Todd Sherman
Lead Engineer
Lockheed Martin

Allen Shoaff
Project Manager
Nationwide Strategy to Prevent &
Respond to Identity Crime
International Association of Chiefs of
Police

Robert Thompson
Chairman
Thompson Advisory Group

George "Chip" Tsantes
EVP & CTO
Intersections Inc.

Staca Urie
Program Manager, Special Analysis
Unit
National Center for Missing and
Exploited Children

Tomas Vagoun, PhD
CSIA and SDP Technical Coordinator
National Coordination Office for
Networking and Information
Technology R&D

Anne Wallace
President
Identity Theft Assistance Corporation

Tim Walston
SVP, E-commerce & Product
Development
Intersections Inc.

Norm Willox
Chairman
CAIMR
CBO
LexisNexis