This paper was presented at : **International Conference on Emerging of Networking, Communication and Computing Technologies (ICENCCT 2014)** Co-jointed **with International Conference on Emerging Trends of Computer Science with Educational Technology (ICETCSET 2014)** – Zurich, Switzerland on February 22-23, 2014 – Organized by : **Institute of Information System and Research Center (IISRC)**

Applying Systems Thinking to Adjudicate Privacy and Trust Concerns in Identity and Access Management Systems

Jonathan M. Branker, Dr. Shahryar Sarkani, Dr. Timothy Eveleigh, Dr. Thomas Holzer
Department of Engineering Management and Systems Engineering
The George Washington University
Washington DC, USA
JB_for2D@gwu.edu, Emseor2003@yahoo.com, Eveleigh@gwu.edu, Holzert@gwu.edu

Abstract :

Identity and Access Management (IdAM) Systems evolved as autonomous systems but the need for sharing of Personal Identity Verification (PIV) information and the collection, retention, use, and disposal of credentialing information has led to privacy and trust issues. This lack of trust has resulted in law enforcement personnel and first responders being denied access to facilities during emergency situations. This research seeks to investigate the privacy concerns and the utilization of trusted sources that IdAM systems require to adjudicate data. The papers further outlines the author's research goals to incorporate systems thinking into IdAM designs, identify gaps in current design methodologies and proposes a system dynamics (SD) approach that begins to suggest how to mitigate privacy and trust concerns. SD is selected since real world complex system problems and system behaviors over time can be modeled using combinations of feedback loops, causal loop diagrams to illustrate interdependencies, stocks and flows, and temporal delays. Artifacts of the research include initial SD models and recommendations for infrastructure enhancements to support future designs.

Keywords-component; *Access Control, Infrastructure Design, Privacy, System Dynamics, Systems Engineering, Systems Thinking, Trust.*

I. INTRODUCTION

Personnel identification has evolved from the simple photo identification badge to credit card size computing platforms with integrated storage memory. These cards require an embedded memory module and computer chips to support the increasing amount of information storage and processing necessary to perform verification and validation of the individual and their unique credentials. As the level of sophistication of IdAM credentials increases, so has the need for systems to track the issuance of credentials for persons requiring access to computer systems, services, and facilities[1]. Digital identity management is ubiquitous in this information age but comes with a number of consequences due to the increase in credential tampering and the compromise of personal identification information, both resulting in the need for risk assessment, risk mitigation strategies, and privacy concerns[2]. The collection, storage, verification, validation, and use of personal information to generate Personal Identity Verification (PIV) credentials has also led to the ancillary privacy concerns on how the information is stored, used, and disposed should the individual no longer be part of a facility or system[3]. This need for PIV credentials resulted in increased requirements for Personal Identified

Information (PII) to verify and validate the identity of individuals, thus increasing privacy concerns due to unauthorized leaks. PII also drove the need for additional levels of security and additional training for those persons whose job is to access and verify PII information[4].

The need to share user PII information has led to the requirement to integrate IdAM systems from multiple platforms into a common platform. Personnel are no longer tied to a single work facility and credentialing portability is ubiquitous in today's working paradigm. The lack of integration and trust amongst IdAM systems has led to several incidents over the years and a recent loss of life. An incident at the Delta Airlines terminal at John F. Kennedy International Airport in New York City resulted in the death of a passenger waiting to board a flight because the Emergency Medical Technicians (EMTs) and a Law Enforcement Officer (LEO) dispatched to assist in an apparent heart attack did not have their credentials adjudicated to access the security doors in the terminal [5]. The lack of integration is a recognized problem at the federal level and the Federal Identify, Credential, and Access Management (FICAM) implementation guidance document identifies gaps with the First Responder's Access Cards (FRAC) due to lack of integration between IdAM systems and their adjudication databases [6]. The scenario could be the destruction of a building resulting in sensitive documents being scattered in the immediate area. FRACs must be adjudicated to ensure that only those with suitable clearances are allowed to enter the area. Both the EMTs and the first responders required to clean up the sensitive documents illustrate the gaps in the IdAM systems since access could be denied if there is no trust established among the organizations responsible for addressing the incident and assigning the right personnel.

In IdAM systems, accountability and responsibility for the information contained within is delegated to different functional organizations[7]. IdAM systems need to be architected in such a manner that they support information sharing while protecting the integrity of personal data as well as promoting the release of information only to authorized users[8]. Prior IdAM research has focused on the technology used in access control systems[9], architectural alternatives for IdAM[10], and the security and privacy concerns associated with the use of biometrics[11]. This research builds on the prior focus but introduces a systems engineering approach incorporating systems thinking.

II. OVERVIEW

Personal Identifiable Information (PII) for use by individuals and systems has evolved from the simple photo identification as a quick means of matching the individual to the credential, to the use of computer-chip enabled smart credentials incorporating multiple biometrics and a personal identification number (PIN) to authenticate and validate the user to the Identity and Access Management (IdAM) system[12]. IdAM systems are identified as the combination of an Identity Management and Credential Issuance System (IdM-CIS) and a Physical Access Control System (PACS)[13]. The IdM-CIS requirements include enrollment capture equipment (camera for photo capture, biometric sensors for fingerprint capture, iris scanning, etc.), Identity and Credential Management software, card production equipment, and storage devices. Recommendations and guidance for the issuance process are outlined in the National Institute of Science and Technology (NIST) Special Publication (SP) 800-63.

The IdM-CIS collect personal attributes of the individual for verification, usually by a third-party Certificate Authority (CA) that issues a digital certificate via a Public Key Infrastructure (PKI) management infrastructure[14]. Credentials issued to users are presented to the IdAM which validates that the person presenting the credential is the authorized holder of the credential and can access the facility or resource. The IdM-CIS is also responsible for the full life-cycle of the PII information, i.e., from the acquisition of information during the enrollment process through the storage and use of the identity, and ending with the proper disposal of the information when the individual is no longer part of the organization[10]. Figure 1 illustrates the biometrics enrollment process for credential issuance of the Transportation Worker Identification Card (TWIC) for Maritime workers under the direction of the Transportation Security Administration (TSA)[15]. The enrollment and credential issuance process steps include:

- Biographical and Biometric information
- Enrollment and Adjudication of candidate
- Background check(s)
- Credential Issuance
- Validation of user and credential
- Privilege granted for access control

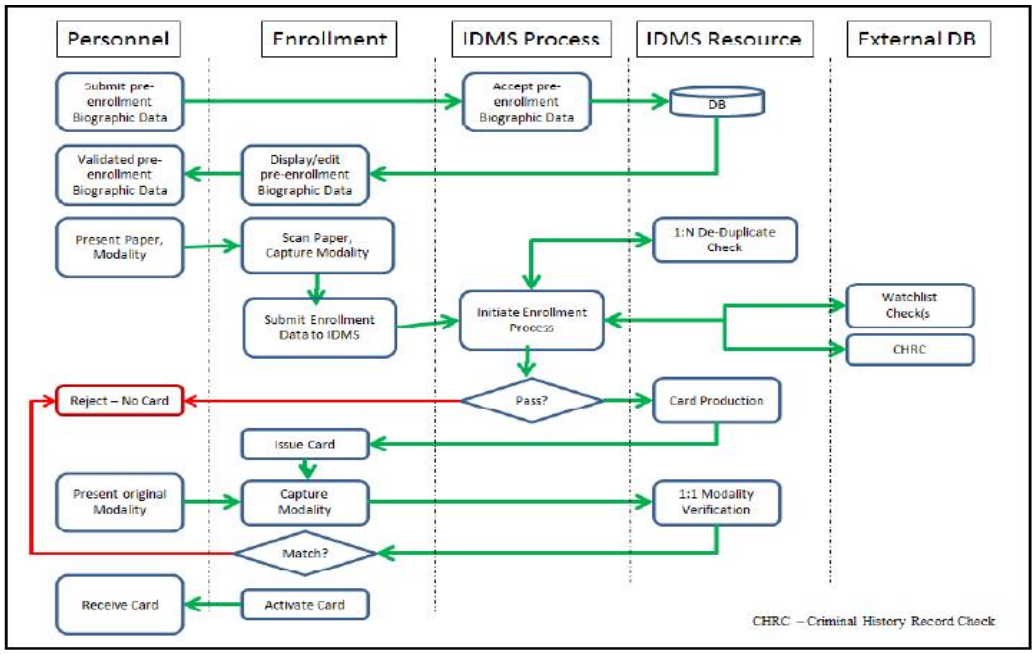

Figure 1. Pre-Enrollment thru Credential Issuance

The act of presenting biographical and biometric information for the enrollment process raises privacy issues as third parties are required for adjudication which ultimately can lead to the chain of trust issues that are inherent in most IdAM systems[10]. The IdAM validation process requires the user to present their credentials in the form of an identified token that was issued to them, a biometric or something that is unique to the user (such as a photo or fingerprint), and something that is known only to the user such as a PIN or special password[16]. In the TSA use-case, privacy and trust concerns raised during the enrollment process are

adjudicated differently from those raised during the subsequent use of the TWIC for access control purposes[15]. Trust concerns can come in the form of impersonating an individual as a result of identity theft or the abuse of the implicit trust relationship between the IdAM and its third parties adjudicator[10]. It is therefore a mandatory process step that the individual returns to the enrollment station and presents the original biographic and biometric information as part of the credential issuance process as the means of verifying their identity. This facilitates the issuance and activation of the reference credential into the IdAM for use during the deny/grant challenge process.

Figure 2 shows the credential interactions with a physical access management component of a generic biometric access control system[17]. PACS requirements include biometric sensors (similar to the enrollment equipment), a PACS management and control system, and networking equipment for system integration based on the number of devices and access points.

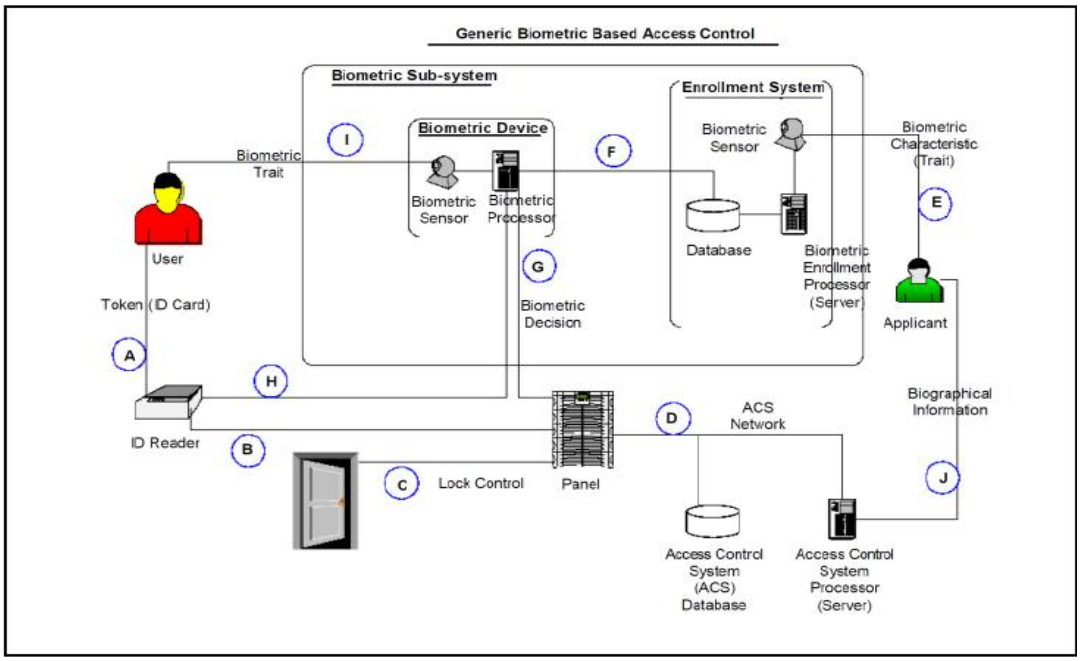

Figure 2. Generic Biometric-based Access Control

The details for the user access control process are as follows:

A. User presents a credential to the access control reader to verify an identity.

B. User information (ID code, card number, etc.) read from the credential is sent to the PACS Panel to determine access privilege for the user.

C. Signal path to the door portal to grant/deny access or initiate emergency override based on verification results.

D. Communication networks to facilitate data exchange between the access control database and processor to the PACS panel.

E. Biometric characteristic (e.g., picture, fingerprint, etc.) presented during the enrollment process to the identity management processor stored as a template.

F. Biometric template transferred to biometric processor for registered users (either pre-loaded or per access request).

G. Grant/Deny access indication sent to the PACS panel based on the results of the verification transactions.

H. Based on the implementation (biometric template on card), user information read from the credential is sent to the Biometric processor to 'claim the identity' for the user.

I. Biometric characteristic (e.g., picture, fingerprint, etc.) presented to the biometric sensor at the portal during the access request.

J. Applicant-specific information (name, address, etc.) obtained during PACS enrollment via the PACS processor (used in some legacy PACS implementations).

The TSA, TWIC, and the Common Access Card used by the Department of Defense (DOD) for active duty military personnel, selected reserve personnel, civilian employees, and eligible contractors follow similar enrollment, issuance, and access control methods. These credentials identify and authenticate personnel and a trusted source determines whether or not to grant/deny them access based on the privileges setup for each user[18]. The Federal Information Processing Standards (FIPS) 201 and NIST SP 800-63 documents are used by DOD, TSA, and other government agencies but different trusted sources are used for user authentication which amplifies privacy and trust issues among federal agencies [6]. Along with NIST, the International Telecommunications Union Telecommunications Standardization Section (ITU-T) Working Groups (WG) 4 & 5 are focused on Security Controls, Identity Management and Privacy technologies, and providing guidance in documentation in the form of ITU-T 24760/ISO 29115.

III. PREVIOUS RESEARCH

The need for IdAM exploded rapidly in the late 1990s as airport operators found themselves with a multitude of competing technologies required to support various areas of their operations. The need for integrated IdAM was apparent as these airports had to interface with their standalone Intrusion Detection Systems and closed circuit television systems[19, 20]. The Federal Aviation Administration (FAA) accelerated its focus on access control systems after the September 11, 2001 attacks by outlining the limitations in the legacy badging systems and the need to integrate various biometrics such as hand geometry and facial recognition into the employee verification process[9]. The FAA research was further expanded to recommend risk based approaches to access control systems[21]. Additional research reports were published on the shortcomings of access control systems, the need for integration, data sharing, and the fusion of individual systems[22, 23]. Alston and Campbell introduced the systems engineering approach for security system design[24] and influenced the direction of this research to incorporate systems thinking into IdAM designs through the use of SD modeling.

IV. PROBLEM DESCRIPTION AND GAPS

Identity and Access Management requires a framework built around architectures focused on privacy and trust for enrollment, authentication of users to their credentials, and the interfaces to IdAM systems. This framework requires the establishment of trust for PII information used in the enrollment and vetting process with an IdM-CIS authority; the transfer of trust in the operating paradigm when requested by the access control system to grant/deny access for an individual; and the verification of the user to the access control system during the verification process. IdAM processes and technology have advanced but privacy and trust issues associated with the adjudication of credentialing attributes in PII information remain the dominant problem. Some of the gaps in the IdAM process and technology include[7]:

- Lack of a common credentialing registration, enrollment, issuance, and revocation process
- No common set of data elements that define the identity criteria of the user
- The inability to establish a common trust authority for identity verification
- No authoritative source to collect and exchange identity data
- No reciprocity of biographic information between agency investigations
- Lack of common guidance on what constitutes privacy data in credentialing systems.

The IdM-CIS needs to be robust and account for the security and privacy concerns associated with the collection, storage, retention, and destruction of PIV information collected as part of the enrollment process. For example, a biometric template is generated as part of the enrollment process and stored for later use by the IdAM when the issued credential is presented. The enrollment process requires the establishment of a set of criteria that the IdAM designer should consider for their system[2]. The establishment of identity clearance processes for document verification and the separation of duties safeguard the processes of identity proofing and registration. These actions ensure that issuance does not fall on a single department or individual. Criteria needs to be established for the credential registration information used during the enrollment process, how and when information is shared between agencies, how trust is established between organizations, and the adherence to established privacy objectives of the IdAM [2]. Additional criteria gaps also include:

- What identity source documentation would be acceptable for enrollment?
- What documentation exists to codify what information would be collected, what would be authorized for disclosure (including usage duration), and the disposal methods for this information upon credential revocation?
- What are the enrollment requirements and what process will be used to examine source documents?
- With respect to access to PII information, how are legitimate needs represented?
- What processes are in place to report system violations of privacy policies or when privacy and trust is compromised?

V. RESEARCH GOALS AND APPROACH

The research goal of this work is to investigate Identity and Access Management credentialing and Access Management architectures, identify gaps in the current approaches, and propose a framework improvement through the use of systems engineering principles. Using a SD model, a secondary goal of the research is to establish a framework based on the mitigation of privacy concerns and the establishment of a trust framework whereby organizations can exchange credentialing information to facilitate the granting or revocation of access control privileges. The research will highlight the benefits of using systems engineering and SD principles in IdAM designs to mitigate privacy and trust concerns. IdAM systems will be evaluated and modeled by the SD framework based on the privacy and trust concerns raised in the gap analysis. The research focus is in the transportation modality with emphasis on the aviation and maritime domains but the resulting framework could be expanded to other modalities.

The research approach will analyze the process and technology used in Figures 1 & 2 to develop a conceptual SD model. This approach will utilize a descriptive qualitative strategy based on a case study of privacy and trust concerns in access control systems. The SD model will identify the users or customers that require credentials; the actors who will use the processes of the IdAM; various system owners assigned to either the IdM-CIS or PACS; the inputs and outputs of the transformation processes; privacy restrictions and environmental constraints based on trust; and the world view of the model[25]. The SD model will represent what activities are associated with the IdAM and the flow of information from the enrollment phase to the granting or denial of access based on the issued credential.

VI. RESEARCH METHODOLOGY AND CONCEPTUAL FRAMEWORK

The research methodology approach and the development of the conceptual framework was influenced by Checkland's Systems Thinking, Systems Practice[25]. This methodology utilizes Checkland's four activities, 'systems thinking' model approach that: a) defines the problem statement, b) formulates the relevant activity models, c) debates changes that could improve the situation, and d) proposes what actions could be taken to improve the situation. This allows the perceived research problem to be expressed in terms of various system interactions and relationships, i.e., a conceptual model framework. However, this only shows the linear relationship of the IdAM and there needs to be a shift from this linear approach to a systems thinking model. As Peter Senge explained, "the essence of the discipline of systems thinking lies in a shift of the mind: seeing interrelationships rather than linear cause-effect chains, and seeing processes of change rather than snapshots" [26].

Figure 3 shows the flowchart of a conceptual model flowchart and the area of this research focus. In the IdAM enrollment process, biometric and biographic information is captured and adjudicated by various trust authorities and once verified, the information is stored for later use. Various collection, capture, and storage methods are used for these processes along with a number of trusted 'trust' authorities that can adjudicate the information presented as valid for use during the IdAM enrollment process. Information privacy and trust are

major concerns for IdAM systems that perform these functions. Once verified, the user is once again asked to present their biometric and biographic reference information and this is checked against the verified information and a determination is made to issue authorized credentials or deny the issuance (mismatch).

The authorized credential is presented to an IdAM Access Control system and a determination needs to be made to deny or grant access to the individual based on the information presented and the response received from a trust authority. The authorized trust authority used by the IdAM Access Control System may not be the same as the one used in the IdAM enrollment process. Mutual agreements between the parties must be in place before information exchange between these subsystems is possible.

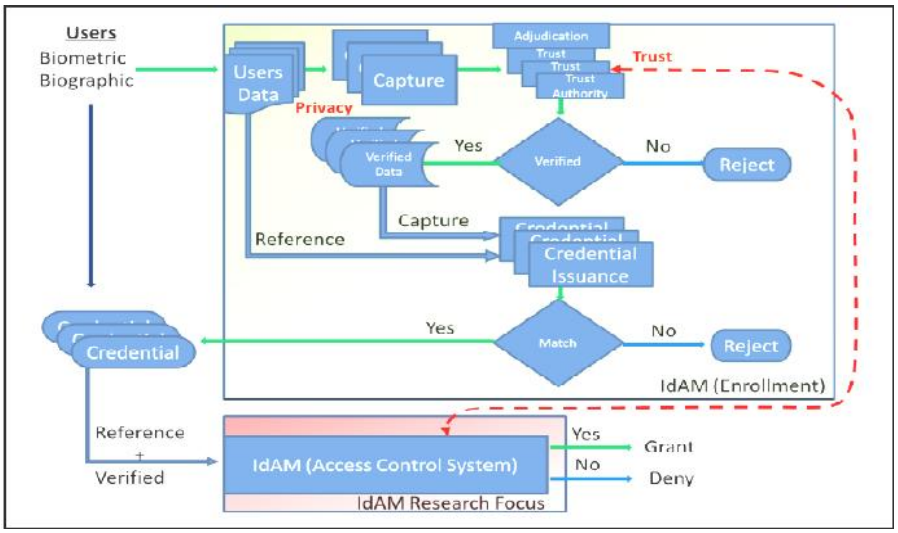

Figure 3 IdAM Conceptual Model Flowchart

This research applies systems thinking to the IdAM access control process and utilizes an SD model to mitigate inherent privacy and trust issues. The IdAM conceptual model flowchart is being adapted to a real world transportation modality problem as depicted in Figure 4. It shows the model applied to United States Postal Service (USPS) drivers. The USPS employs drivers for pickup and drop-offs using various vehicles ranging from small vans to heavy trucks. At any given time, drivers will deliver mail and packages to airports, seaports, and international border points. In the case of an airport destination, the driver is required to have their USPS credentials and may require a Commercial Drivers' License (CDL) depending on the type of vehicle required for the load. A Secure Identification Display Area (SIDA) credential is required since special training and identification is required to drive onto an airport tarmac. For these credentials to be acceptable, trust relationships must exist among all parties to facilitate credentialing information among the IdAM systems to deny/grant access to the drivers.

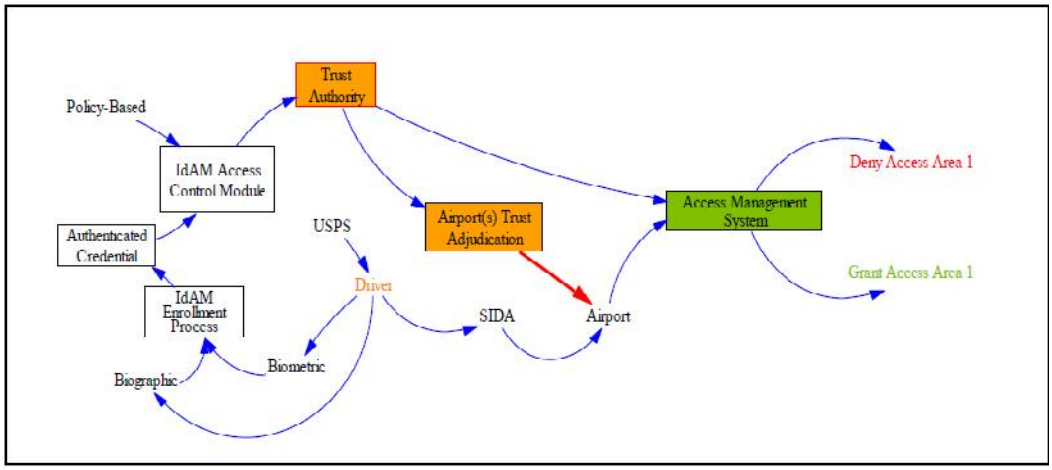

Figure 4 USPS Drivers Standalone Airport Use Cases

As a result of their possible destination locations, access control requirements necessitate multiple credentials to be issued from their biographic and biometric information but adjudicated and authenticated by different IdAM systems based on their operating modality. In today's environment, drivers are required to carry multiple credentials if they have to access multiple airports since most IdAM are standalone and dedicated to that specific airport. To access a sea-port, the driver would require their USPS credentials, a Transportation Worker Identification Card (TWIC) along with their Commercial Driver's License (CDL), and their biographic and biometric information in the maritime adjudication system. If the same driver was scheduled to transit an international border point, that driver would require the Free and Secure Trade – International (FAST-Intl) credential and depending on the cargo, could also require the Hazardous Material Endorsement. Using the SD approach as outlined in Figure 5 below, the model flowchart could be analyzed using causal relationships.

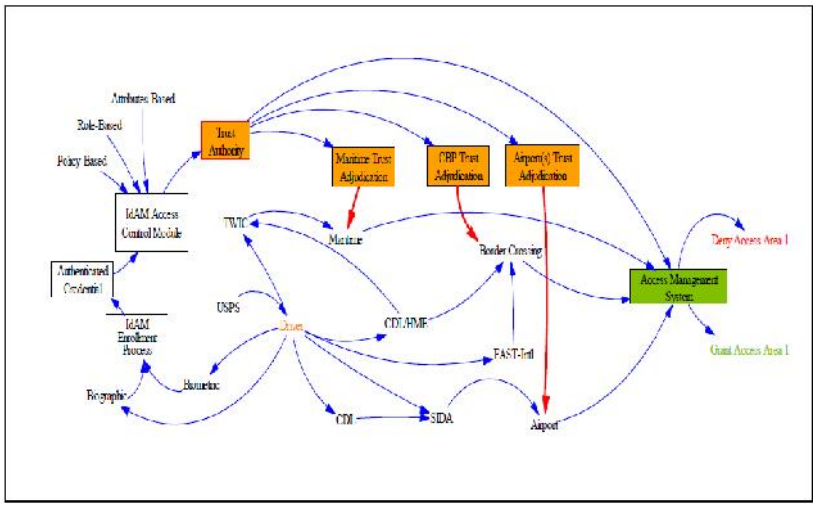

Figure 5 Driver Causal Relationships

This SD model is being enhanced to address the trust issues with credentialing attributes and will propose an improved process to mitigate the need for multiple credentials based on which modality the driver needs to visit.

In addition, the issue of privacy would also be addressed as the proposed solution would include steps to protect the integrity of the data at rest (when used in the IdAM) and in transit (between the trust authorities and the IdAMs). Preliminary modeling results indicate the promise of improvements in the re-use of credentialing information across multiple IdAMs by addressing the inherent privacy and trust gaps.

VII. RESEARCH QUESTIONS

This research will investigate the requirements to maintain data privacy and trusted sources for information adjudication in IdAM systems and propose how the use of system dynamics can mitigate these challenges. The research would generate an SD causal loop model of the IdAM to study the system interactions and use the results to propose system changes in IdAM designs. This research will address the following questions:

Q1: Does the application of systems thinking improve trusted sources selection in IdAM systems?

Q2: Does systems thinking help adjudicate privacy concerns in IdAM systems?

Q3: How would credential interoperability improve through the application of systems thinking to mitigate privacy and trust in IdAM systems?

Q4: How does the application of systems thinking eliminate the need for multiple access control credentials in IdAM systems?

Q5: How does the exchange of privacy data between trusted sources and IdAM systems improve through the use of systems thinking?

VIII. CONCLUSION

Our research is focused on the transportation domain since it is one of the most difficult areas to secure due to its diverse modalities. The transient nature of its operations and personnel increases the challenges of maintaining updated credentials in this environment[27]. NIST and ITU-T have study groups actively pursuing IdAM. However, the existence of these standards and adjudication of credentialing information for identity verification used in IdAM systems will continue to be problematic unless solutions are developed for the trusted sources and privacy concerns of information sharing. This research hopes to prove that the application of systems thinking and a SD framework will improve the processes and technological choices for IdAM while mitigating their privacy and trust issues. The expected contribution to the body of knowledge is an expanded understanding of the benefits of using systems engineering principles, the use of SD (especially in the design of access control systems), and a framework that will apply to access control systems across multiple domains.

ACKNOWLEDGMENT

Special thanks to my George Washington University advisors Dr. Timothy Eveleigh, Dr. Thomas H. Holzer, and Dr. Shahryar Sarkani for their research guidance.

REFERENCES

[1] Libin, P., *Defogging Identity-Based Access Control*, in *Security Technology & Design*. 2006, Cygnus Business Media, Inc: Park Ridge, United States, Park Ridge. p. 20-22.

[2] Palmer, A.J., *Criteria to Evaluate Automated Personal Identification Mechanisms.* Computers & Security, 2008. **27**(7–8): p. 260-284.

[3] Bryan, C., *Privacy Impact Assessment (Amended) for the Security Threat Assessment for Airport Badge and Credential Holders.* Report, 2006: p. 9.

[4] Chen, J., et al., *Differentiated security levels for personal identifiable information in identity management system.* Expert Systems with Applications, 2011. **38**(11): p. 14156-14162.

[5] Gastaldo, E. *Man Dies as Airport Security Doors Keep EMTs Away*. 2013 [cited 2013 July 19, 2013]; Airport Security Doors deny access to EMT personnel resulting in the death of a passenger]. Available from: http://www.newser.com/story/171184/man-dies-as-airport-security-doors-keep-emts-away.html?utm_source=syn&utm_medium=goognews&utm_campaign=chan3_feed.

[6] CIO. *Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance*. 2011 December 2, 2011; v2:[478]. Available from: http://www.idmanagement.gov/sites/default/files/documents/FICAM_Roadmap_and_Implementation_Guidance_v2%200_20111202_0.pdf.

[7] Palmer, A.J., *Approach for selecting the most suitable Automated Personal Identification Mechanism (ASMSA).* Computers & Security, 2010. **29**(7): p. 785-806.

[8] Farroha, B. and D. Farroha. *Architecting dynamic privileges in protected systems through hardening Identity and Access Management*. in *Systems Conference (SysCon), 2012 IEEE International*. 2012.

[9] Lazarick, R., *Applications of Technology in Airport Access Control.* IEEE, 2001: p. 11.

[10] Chehab, M.I. and A.E. Abdallah. *Architectures for identity management*. in *Internet Technology and Secured Transactions, 2009. ICITST 2009. International Conference for*. 2009.

[11] Prabhakar, S., S. Pankanti, and A.K. Jain, *Biometric recognition: security and privacy concerns.* Security & Privacy, IEEE, 2003. **1**(2): p. 33-42.

[12] Gunter, C.A., D.M. Liebovitz, and B. Malin, *Experience-Based Access Management: A Life-Cycle Framework for Identity and Access Management Systems.* Security & Privacy, IEEE, 2011. **9**(5): p. 48-55.

[13] SC-207, *Integrated Security System Standard for Airport Access Control Systems.* 2008, RTCA DO-230B: USA.

[14] D'Agostino, S., Engberg, D., Sinkov, A., Bernard, R, *The Roles of Authentication, Authorization and Cryptography in Expanding Security Industry.* SIA Quarterly Technical Update, 2005.

[15] Tilton, C. *Use Case Specification: Transportation Worker Identification*. 2006 July 11, 2012; 8]. Available from: https://www.oasis-open.org/committees/download.php/20952/TWIC%20Use%20Case%20v1-0.pdf.

[16] Kuklinski, T. and B. Monk. *The Use of ID Reader-Authenticators in Secure Access Control and Credentialing*. in *Technologies for Homeland Security, 2008 IEEE Conference on*. 2008.

[17] TSA. *Guidance Package - Biometrics for Airport Access Control*. 2005 [cited 1, 2, 3; 140]. Available from: http://www.acconline.org/documents/biometrics_guidance.pdf.

[18] David, M.W., G.A. Hussein, and K. Sakurai. *Secure identity authentication and logical access control for airport information systems.* in *Security Technology, 2003. Proceedings. IEEE 37th Annual 2003 International Carnahan Conference on*. 2003.

[19] Redpath, G. and G. McClure. *The role of electronic security systems integration in airport management*. in *Security and Detection, 1997. ECOS 97., European Conference on*. 1997.

[20] O'Mara, D.L., *Multi-year Upgrade Focuses on CCTV.* Security: Solutions for Enterprise Security Leaders, 2000. **37**(8): p. 42.

[21] Wilson, D.L., *Airport information systems security.* Aerospace and Electronic Systems Magazine, IEEE, 2003. **18**(4): p. 25-27.

[22] O'Bryon, J., et al, *Fusion of Security System Data to Improve Airport Security.* The National Academies, National Research Council, 2007: p. 83.

[23] Riley, J., *Airport Access Control and Tracking, and the Aviation and Transportation Security Act.* White Paper, 2008: p. 8.

[24] Alston, I. and S. Campbell. *A Systems Engineering Approach for Security System Design*. in *Emerging Security Technologies (EST), 2010 International Conference on*. 2010.

[25] Checkland, P., *Systems Thinking, Systems Practice: includes Soft Systems Methodology: a 30-year Retrospective*. 1 ed. 1999, West Essex, England: John Wiley & Sons Ltd. 424.

[26] Senge, P.M., *The Fifth Discipline: The Art & Practice of the Learning Organization*. 2006, USA: Doubleday. 446.

[27] Diedam, J., *Access control: The process of securing a transportation site*. Journal of Airport Management, 2009. **3**(3): p. 263-273