Digital Identity

L. JEAN CAMP

DIGITAL VISION

The word, "identity" refers to an increasing range of possible nouns – from a set of personality-defining traits to a hashed computer password.

The lack of conceptual clarity reflected by the overload of the word is confounding the ubiquitous practice of risk management via identity management. Thus this article clarifies the nature of identification in a digital networked world, as opposed to a paper-based world. The examples and the context are identification as used in law enforcement in the United States. Together the definitions and the examples illustrate the importance of developing policies with recognition of the social implications of technical change.

Authentication, Identity, and Access

The problems of authentication, identity, and access are difficult individually. Identification requires authentication of identity; access to data must often be preceded by authentication. The difficulty of these problems is further exacerbated by the subtleties of authentication, identity, and access in law enforcement because of privacy concerns unique to matters of justice.

Identification is a necessary element of transactions-based digital government [9]. While citizen interaction with and access to government is increasingly remote and computer mediated, identification systems used by citizens remain firmly grounded in the age of print. Understanding how digital networked identification is different from paper-based identification systems is a critical and often overlooked element in appropriate design of identification systems.

In this discussion, we begin by offering rigorous definitions of identity and related terms. These illuminate the core problem in modern identity systems – the assumptions about the functioning of identification are based on assumptions built on centuries of experience with paper. The failure of identity in the law enforcement cases discussed here can be understood as stemming from mental models of paper-based identity management mapped onto digital networked systems. The policies and organizational models of paper-based identification system create dangerous failure modes when applied to digital networked identities. The most widely known failure mode is identity theft. These assumptions are discussed in some detail in the section on paper identities.

Applying rigorous definitions to the case of an officer stopping a citizen who may or may not be a suspect in a crime illustrates that unverified assertions of identity can, in fact, undermine rational risk management. Digitizing these falsifiable claims of identity results in less security, not more.

An identity system is useful for threat management in a high-risk situation only if there is no effective opportunity for falsification during enrollment and verification. Just as completely unverified assertions of identity have less than no value, faulty identity systems have similar risks. Therefore, the use of identity management systems as risk management systems creates a situation in which security is reduced, as the genuinely dangerous will be presented or authenticated as having apparently benign identities.

Definitions

Consider a passport. A passport includes an identifier, the passport number. It lists some attributes, including nationality, sometimes height and weight. It includes personal identifiers, including date of birth and name. It includes a biometric[1] method of identification – a photograph [5]. Passports are used, therefore for both identification ("I am me") and identity authentication ("My government authenticates that I am me."). A passport links attribute authentication (citizenship) with identity authentication (name) to enable off-line identification (photograph and data). All of these elements are combined in a single document, and that document must be shown in whole to provide authentication. This binding of attribute to identity for the purpose of authentication is made necessary by the power and limits of paper.

A few decades ago, the immigration official reviewing a passport was not expected to calculate the exponentials needed to make a public key system work – this required computers. That official also could not check whether an attribute identified only by a number was valid in a highly dynamic system - this required a network and highly available data.

The aggregation of elements of identity, identifiers, and authentication that inherently occurs with a paper-based system does not necessarily exist in digital systems. Clarity requires breaking a traditional paper system into its functional components and understanding the interaction of those components in a digital networked environment. Without that clarity, digital systems can be designed with vulnerabilities, concepts of identity, and authentication.

In order to further develop the core argument, the consideration of definitions is the next order of business.[2] Each of these describes a function or element of an identity system.

Identifier. An identifier distinguishes a distinct person, place or thing within the context of a specific namespace. For example, an automobile, account, and a person each have identifiers. The automobile has a license plate and the account has a number. The person may be associated with either auto or account through additional information, e.g., a serial number, or a certificate. One person, place, or thing can have multiple identifiers. A car has a permanent VIN and temporary license plate. Each identifier is meaningful only in the namespace, and only when associated with the thing being identified. Therefore, each identifier can reasonably be thought of as having a <thing identified, identifier, namespace> set, e.g., <car, license plate, state motor vehicle database>.

Attribute. An attribute is a characteristic associated with an entity, such as an individual. Examples of persistent attributes include eye color, and date of birth. Examples of temporary attributes include address, employer, and organizational role. A Social Security Number is an example of a long-lived attribute in the American governmental system. Passport numbers are long-lived attributes. Some biometric data are persistent, some change over time or can be changed, (e.g., fingerprints versus hair color).

Personal identifier. Persistent identifiers consist of that set of identi-

[1] A biometric is a physical , biological feature or attribute that can be measured. Examples of unique biometrics are fingerprints, iris patterns, and DNA sequences. Other biometrics are not unique and therefore not useful for authentication or identification, e.g., hair color, nose length, and height .

[2] The following definitions were developed cooperatively in preparation for the KSG Identity Civic Scenario by participants of this event. For more information please see: http://www.ksg.harvard.edu/digitalcenter/conference.

fiers associated with an individual human that are based on attributes that are difficult or impossible to alter. For example, human date of birth and genetic pattern are all personal identifiers. Notice that anyone can lie about his or her date of birth, but no one can change it. Personal identifiers are not inherently subject to authentication.

Identification. Identification is the association of a personal identifier with an individual presenting attributes, e.g., "You are John Doe." Examples include accepting the association between a physical person and claimed name; determining an association between a company and a financial record; or connecting a patient with a record of physical attributes. Identification occurs in the network based on both individual humans and devices. Identification requires an identifier (e.g., VIN, passport number).

Authentication. Authentication is proof of an attribute. Identity as it is constructed in modern systems is an attribute, e.g., "Here is my proof of payment so please load the television onto my truck." A name is an attribute and an identifier, but it usually is not used to provide authentication.

Identity Authentication. Authentication of identity is proving an association between an entity and an identifier: the association of a person with a credit or educational record; the association of an automobile with a license plate; or a person with a bank account. Essentially this is verification of the <thing identified, thing> claim in a namespace. Notice, "You are John Doe." is identification while "Your documents illustrate that you are John Doe." is identity authentication.

Attribute Authentication. Authentication of an attribute is proving an association between an entity and an attribute; e.g., the association of a painting with a certificate of authenticity. In an identity system this is usually a two-step process: identity authentication followed by authentication of the association of the attribute and identifier. The automobile is identified by the license plate; but it is authenticated as legitimate by the database of cars that are not being sought for enforcement purposes. Of course, the license plate check may find an unflagged record in the database yet fail identity authentication if the license plate is visibly on the wrong car; e.g., a license plate issued to a VW bug on a Hummer. The person is identified by the drivers' license and the license simultaneously authenticates the right-to-drive attribute. Notice the difference between "Your documents illustrate that you are John Doe." and "Your documents illustrate that you are a student registered at the University and have access rights in this building."

Authorization. Authorization is a decision to allow a particular action based on an identifier or attribute. Examples include the ability of a person to make claims on lines of credit; the right of an emergency vehicle to pass through a red light; or a certification of a radiation-hardened device to be attached to a satellite under construction.

Identity. In an identity management system identity is that set of permanent or long-lived temporal attributes associated with an entity.

Anonym (as in anonymous). An anonym is an authenticated attribute that is not linked to an identifier. An identifier associated with no personal identifier, but only with a single-use attestation of an attribute is an anonym. An anonymous identifier identifies an attribute, once. An anonymous identifier used more than once becomes a pseudonym.

Pseudonym. An identifier associated with attributes or set(s) of transactions, but with no permanent identifier.

The most commonly used anonyms are the dollar and the euro. The most familiar anonyms self-authenticate. Paper money is authenticated by the users. The right to spend the paper money is authenticated simply by the fact that it is presented. To hold a euro is to have an anonym that authenticates the right to spend that euro. These dollars, euros, and shillings are anonymous tokens. In contrast, credit cards and debit cards authenticate an identity, use that identity to authenticate the attribute. The attribute in this case is the right to make charges. Credit cards are identity-based payment systems. Cash is token-based anonymous payment.

Identity options exist in more than money. Disney World offers season tickets, where a season ticket holder can authenticate by hand geometry. Alternatively, Disney World offers tickets where the ticket itself authenticates the right to enter the park – anonyms that verify the right to enter the park. Disney stores offer insured tickets, where the ticket is linked to the identity via payment mechanism. These tickets look like anonymous tickets. However, if the ticket is lost, the purchaser can go to the Disney store or office, cancel the previously purchased ticket, and obtain a new valid ticket by presenting proof of identity. The insured ticket has an identifier that is linked, by Disney, to the payment process.

In contrast, passports explicitly reject the possibility of providing anonymity. A pseudonymous passport that simply identifies you as a citizen is not available. In the digital world, in theory, a passport could present a citizenship claim, then add a biometric to authenticate the citizenship/body claim and even enable a search of known criminals. In such a transaction the person remains anonymous assuming there is no match between the unique biometric and the list of those sought by law enforcement. The binding between the citizenship authentication and the person physically present is much stronger than in the case with the paper passport, yet the role of identity is minimized. There is no need to store the exact biometric for this system to function. Privacy-enhancing biometric systems, such as those that depend on one-way hashes of biometrics, are more secure in the long term than systems that depend on predictable and thus more easily forged data.

Identity systems must be trustworthy to be useful. The more critical the context or namespace in which identities are authenticated, the more robust the attribute authentication must be. Making certain that no one is holding explosives requires stronger attribution than making certain that everyone in the plane purchased a ticket. Adding identity into attribute authentication can weaken an identity system by creating a possible attack because it adds an extra step. When identity is added to authentication attribution then the authentication becomes as strong as the <identity, thing identified> link. If the authentication has two steps (identity authentication, then <identity, attribute authentication>) this creates another opportunity to subvert the authentication by subverting the first stage.

As an example, consider "criminal identity theft" as it occurs in the United States. First, the arrested individual presents false identification information. Those false identifiers are entered into the national fingerprint database under the claimed name. The fingerprints are not compared with those already in the database because the system is keyed on claims of identity (name and date of birth) rather than the persistent attribute (fingerprint). The criminal identity theft victim discovers the theft after being arrested for another person's crime. At that time the criminal identity theft victim's fingerprints are compared to the criminal's. Then the criminal's fingerprints are compared with all other fingerprints in the national fingerprint database, often but not always yielding a match. When the difference is discovered, the criminal identity theft victim obtains a document that verifies that the person's identity is an alias of a criminal. The bearer of this certificate can then present the certificate to law enforcement officials to attest to his or her innocence. The initial dependence on the constructed identity rather than the biometric attribute allows an attack on the law enforcement system, allowing wanted criminals to escape from police custody by whitewashing their criminal records with others' good names.

Compare the entering of names (identities) with the direct entering of fingerprints (biometric attributes). The entering of a name asks the question, "Is this claimed identity in the system?" The attribute authentication question, "Are the fingerprints of this body in the database of criminals?" offers a more reliable response.

Criminal identity theft illustrates that biometrics can deliver the wrong answer more quickly and with a greater degree of precision than paper-based identity systems. Biometrics are only as reliable as the process of enrollment.[3]

Direct attribute authentication ("Do you have a euro?") is more reliable than identity-based attribute authentication ("Do you have a euro credit?") in any case where it is easier to create a fraudulent identity than it is to create a false attribute. If dollars were easier to counterfeit than identities to steal, identity theft would arguably not be the fastest growing crime in the United States. If the process of arrest and enrollment in the American criminal justice system relied on personal attribute (i.e., fingerprint) first, before identity authentication (i.e., name and ID), then criminal identity theft would not be useful.

Fingerprints are not validated against an arrested person's assertion of identity during the arrest procedure. This failure to verify identity allows high-risk multiple-offense felons to be classified as the low-risk single-arrest identities they present. The failure to verify every fingerprint against possible identity theft not only puts law enforcement personnel inappropriately processing dangerous multiple offenders at risk; this failure also increases the value of stolen identities of the innocent.

Identity in the Law Enforcement Context

Currently in the United States there is considerable debate about appropriate responses to an ill-defined terrorist threat and an increasing crime rate. In seeking to provide security, multiple identification mechanisms are being implemented.

At the Federal level in the U.S., there is a Transportation Security Administration (TSA) "no fly list" and also a Computer Assisted Passenger Screening System (CAPSS) list. Without addressing the widely cited possibility that the no-fly list is used to limit efficacy of political opponents of the Bush Administration [1], [11], CAPSS can be addressed in terms of its efficacy in its stated goal. A similar list, the Computer-Assisted Passenger Pre-Screening System (CAPPS II), is being developed by the TSA and the Department of Homeland Security. Note that no system is perfect and in every system there will be failures, even in theory [4], [10].

The CAPPS II and CAPSS systems embody the perfect failures of static lists of identities [7]. Static lists provide identifiers associated with people who have proven to be untrustworthy in the past, or who are expected to be untrustworthy in the future.

With a static list of identities, an individual knows that some rating is associated with an identity. A serious attack requires first avoiding security scrutiny. To implement the attack, the first round is to deter-

[3] Enrollment is the process of entering initial records with biometrics. A biometric is only useful if it is associated with attributes (e.g., criminal records). The creation of a biometrics: attribute record is enrollment.

mine if the identity used for the attack is one that will result in scrutiny. Therefore, the obvious first effort is to determine a set of identities that will certainly not result in being subject to scrutiny. The less random the scrutiny, the easier it is to avoid.

Currently the no-fly and security check lists are static [7]. In addition, there are well-known factors that determine security scrutiny. Buying one-way tickets and having no frequent flyer number result in certain scrutiny. Having a frequent flyer number, buying a round trip ticket, and flying coach results in no scrutiny. These well-known flags create a brittle system of security that is deterministic and therefore easy to subvert.

The use of static lists of identities for security without randomization and comprehensive security requires a flawless identity system and perfect knowledge of who will commit the next crime.

The identity system must be flawless or at least less subject to flaw than the security implemented against untrusted adversaries. Otherwise, an attacker can obtain a false identity and escape the security net.

Consider the case of the no-fly list. If that were the sole protection, then by definition everyone who flies can be trusted. Of course, this is not the case. Every passenger is examined for metal and some for explosive residue. If the existence of an untrusted (and thus by default a more trusted) list decreases the overall scrutiny of each passenger or person not on the list, overall security is decreased. The least trusted person could obtain a false identifying information offering verification as the most trusted.

An identity-based security management system must be able to predict the source of the next attack. Otherwise, a person who has not yet implemented an attack but intends to do so can pass through the security system unchecked. A failure to predict the identity of the next attacker causes a failure in an identity-based system.

Compare one example of an identity-based list of trustworthy people to a list of specific threats that could be posed by any person. One list would check the identities of all drivers in an area; another approach would refuse to allow any vehicle large enough to be a significant car bomb into an area. The Kennedy School of Government allows any vehicle to enter the parking area, but has installed large concrete "planters" that prevent any car from driving into the pedestrian or building areas. In contrast, during 2004 graduation, cars were allowed into Harvard Yard lots based on the appearance of the driver. A female clad in academic robes (the author) was able to drive into parking areas with drivable access to the pavilion. The KSG approach is to protect against car bombs; the Harvard approach is to identify untrustworthy drivers. Thus under the Harvard College approach the driver must get past identity scrutiny only.

The university example, CAPSS, and CAPPS II illustrate the risks of using identity as a security management tool. In the U.S., there is currently a court case about the more generic use of identity in security management.

Unauthenticated Assertions of Identity in Risk Management

If only individuals who are known current or future threats are subject to scrutiny, then any unknown future criminal will escape security examination. This is a general observation, and applies to traffic stops as well as airline travel.

In the United States, there is currently no legislation or case law requiring identification in order to travel by air, and the courts are not hearing cases that assert the right to travel without identification.

However, there was a recent court case on the right of a police officer to demand identification of any individual he or she approaches, Hiibel vs. Nevada. [118 Nev. 868, 59 P. 2d 1201, affirmed., U.S. Supreme Court No. 03-5554. Argued March 22, 2004 – Decided June 21, 2004]. In this case the state claimed that the ability to demand an unauthenticated claim of identity increased officer safety. In the summer session of 2004, the U.S. Supreme Court upheld the state's position and effectively reasoned that only an innocent person has to provide information. A guilty party has a Fifth Amendment right not to incriminate themselves; however, the innocent has no such right. The Court did not address how a person would know they were innocent of the crime being committed, or if guilt of any crime conveys the Fifth Amendment protection. This case became an excellent illustration of the misuse of identity in risk management.

In order for there to be a need for identification of a subject at the beginning of interrogation to be useful there must be three conditions. First, the identification must be accurate. Second, the identification must immediately correspond to useful information. Third, the identification and information must address an identified threat, thereby providing guidance for the officer that will immediately enhance his or her safety.

Without an authenticated identity leading to the corresponding appropriate response to the specific potential threat, identification does not decrease risk. False identities, if believed, lull officers into believing that there is a low level of risk in a high-risk situation. If assertions of low-risk identities cannot be believed, then the officer must always assume he or she is in a high-risk situation. The information cannot be trusted, and cannot be used in risk management. False identities used by dangerous suspects, and the resulting false sense of security by officers, may lead to an increase in risk.

Without identity management as

a risk tool, the implication is that every officer should treat every traffic stop and every encounter as potentially dangerous.

Any identity system that is not one hundred percent accurate will result in an officer lowering his or threat level and acting accordingly. In order to explain why the implementation of such an identity system will create rather than reduce threats, it is necessary to clarify the distinctions between identification, authentication, and verification.

Demanding a claim of identity is demanding an identifier. The claim of identity is simply a claim of a label. There is little or no direct way in which to confirm a simple claim of a name. In order to confirm the claim it will be necessary for the investigating officer to demand a list of associated claims that might authenticate the identity. For example, the officer would need to obtain date of birth and current address to confirm a claim of a name with driver's license records. In fact, the officer may need the drivers' license number itself depending upon the database access provided by the motor vehicle provider to confirm the claim.

Asking for a name is either asking for a completely unverified and therefore useless label from a potentially hostile party, or asking for a data set that verifies any claim of identity. A completely unverified claim of identity is of no use in a criminal situation. An innocent party will provide correct information, while any suspicious party would misidentify. Criminal aliases were used before identity management systems in law enforcement, and their value to criminals in fraud and detection is well documented.

First, consider false identification. In this case, an officer evaluates his or her investigation, and indeed his or her personal safety, based on false information. A name is accepted from a potential suspect as a valid identifier. A criminal identifies him- or herself as a person with no criminal record. The officer may significantly decrease his or her wariness in a potentially dangerous situation.

Second, consider that the person is innocent indeed. In this case, the officer has required that an innocent person provide information. If every inquiry is reported, then an innocent person may have a record created on the basis of nothing but a traffic stop. Innocent individuals may find themselves tagged as suspicious simply as a result of being innocently stopped multiple times. Given the current racial disparities in traffic stops, so common as be referred to as "DWB" or "driving while black," this possibility is particularly troublesome.

Imagine that an unchangeable biometric, such as fingerprints, is embedded on the driver's license. Once fingerprints are available in a driver license database, those data are then available for theft and misuse. If the stolen information is from a person with no previous criminal record then any possible record could be added – there will be no extant data and the goal of the criminal will simply be to have a match. Utilizing real time biometrics requires highly available networked technology. The officer would have to be able to observe the collection of the fingerprint. Then a database search would reveal identity if there was a match. With current field technology, innocent individuals will be arrested, and criminals will escape, as data capture technologies have not evolved to the point where those who are not technologists will have reliable, consistent reads. If the technology were to ever be so mature, then there would be a possible trade of privacy for security. Under current social, organizational, and technical conditions, privacy is lost and security is decreased.

Even given the ideal technologies, the treatment of all traffic stops as potentially dangerous is the best possible practice for the police officer for the same reason that the treatment of all patients as bearing infectious disease is the best possible medical practice. In both cases, those identified as previously benign may suddenly change to hazardous. In both cases, professional practice of self-protection and wariness is the best defense for the professional on the front lines.

In contrast to a traffic stop that elicits the suspect's name (claimed identity), a fingerprint-based authentication of identification is the verification of a claimed identity using specific attributes. It enables the appropriate application of long-practiced and well-understood risk management in handling prisoners. Note that traffic stop identification is not verified; is not used to evaluate specific attributes; and should the attributes be identified would not bring into play specified practices. Traffic stop identification increases risks to law enforcement personnel by substituting flawed information for best practices, and violates citizen privacy, in order to obtain this potentially dangerous outcome. In short, the two examples of fingerprints interacting with criminal identity theft and unverified claims of identity in traffic stops illustrate the strength and weaknesses of identity management.

Paper Identity

"Where are your papers?"

Why is it the case that law enforcement professionals, experts in risk by definition, are using identifiers in a consistently counter-productive manner, enabling criminal identity theft? Why do system designers that understand the malleability of information begin to think that entering a password creates all the implications of an identity, instead of the access required by a particular role? Both the risk expert and the technical elite translate narrow digital techniques of authentication into ancient human concepts of identity. This is because paper-based centuries-old concepts of identity are being stapled into the digital age.

Paper is itself a technology, one that has been so long embedded in Western culture that it is often no longer identifiable as technology [8], [12]. Paper has distinct characteristics, and paper-based identification systems build on those characteristics to create distinct modes of failure. Paper identifiers create bindings between identification, and attributes that are optional or even hazardous in digital systems. Yet the mental model of the designers and law enforcement is that of paper.

Paper credentials must be human-readable. Paper credentials must be long lived, because their creation and distribution is so expensive. Paper credentials need to be self-proving because there is by definition no option to go on-line and confirm credentials.

Papers are physical self-confirming documents. Without computer databases and networks, the paper has to stand on its own. The papers are physical, they are usually carried by the person asserting their association with the documents. In the paper-based environment, transactional histories were sparse and accessible to few. A single sharing of data does not result in multiple copies distributed across multiple databases. Personal histories were verified by community networks, community centers, or common recollection, with little documentation. The classic example of this is the personal letter of reference. Physical skills and craftsmanship can be illustrated at the moment when a person applies for work, there is no need for a degree and the related certifications.

In the paper world the physical person is inherently linked to the action. Theft or fraud requires showing up to take the money. A transaction requires presence of a body in the physical environment. Thus the body and the identity are linked. In particular this enables an enforcement system that depends in the extreme on bodily enforcement (such as imprisonment).

The individual data that together form a ‘proof’ of identity are hard to locate or extract in a paper-based system. Consider the difficulty of locating a mother’s maiden name and a Social Security Number (SSN) for a stranger before networked digital information. Access to that information would require access to paper records, records that could be managed and secured. In a computerized and networked environment such individual data are difficult to conceal. Once each individual datum is located, the access data can be created by a simple combination. When such data are identifiable, availability threatens privacy [2], [3], and when the data are authenticating data, their availability threatens security.

Anonymity in a paper system implies the simple absence of papers: no papers, no credential, and thus no accountability. Yet anonymity in a digital system means rather that the credential stands alone, can be confirmed during use, and thus does not depend on a network of personal information. Anonymous credentials can be long-lived (e.g., confirmation of date of birth) or short-lived (confirmation of a ticket to an event). Note that the ability to subvert that network of personal information is exactly what makes the paper model of credentials weak in the digital networked world. Confirming date of birth without additional information enables secure attribute verification and decreases overall risk. The clerk can answer the critical question (“Are you old enough to buy beer?”) without information leakage (“This attractive person lives at 37 Noan Rd and here is her phone number”; or, “This well dressed person has this date of birth and this social security number.”).

In contrast, consider cryptographic keys and codes used as session keys. Session keys were the domain of the military, with codebooks distributed at great cost to treasury and life. Now every user of Internet commerce generates a session key for each purchase, real time, and uses it only for the single transaction. Digital networked systems and modern cryptography solved the cost of generating keys and distributing them.

When concepts of paper authentication are used in digital networked systems the nature of paper documents (persistent, self-authenticating information) creates serious risks. The same information - called identity - that links the achievement of a college degree, credit worth, health insurance risk, or a promotion is connected to emails and on-line purchase records at on-line merchants. The record of each web view can be traced to the login at a specific machine. Information entered into forms may remain on the machines in the users’ profile or password manager. These identifiers were built for paper systems: names, social security numbers, and other human-readable persistent identifiers.

Anonymous/Pseudonymous Attribute Systems: Greater Security and Privacy

With automated face recognition, ubiquitous video, and widespread digital authentication systems based on identity, many actions that were traditionally hidden in the faces of the crowd are becoming easily associated with identity. Many times security is given as the reason for this association. These claims of security and the value of identity must be subject to clear and critical scrutiny. Sometimes privacy is lost and security is subverted by the use of identity as a substitute for attribute-based risk management.

Identity systems that function best in law enforcement are those that identify an individual through an unforgeable biometric (the capture of which is observed by law enforcement and processed appropriately) that is linked to a specific attribute. The use of other identity management tools has abetted criminals in committing fraud, escaping justice, and evading surveillance. Identity systems are best used only when the threat is one of misidentification, rather than for attribute forgery.

Paper-based identity systems link attribute, identity, and authentication into a single stand-alone document. The availability of networked data opens entire new vistas of possible systems. Simultaneously, networked data are undermining the assumptions of "secret" information on which paper systems depend.

Identity in government is sufficiently critical that an identity system is to some degree inevitable. However, an identity system that builds upon biometric-confirmed pseudonyms can provide privacy and enhance security. Current identity management systems increasingly harm privacy and security, rather than enhancing either. Anonymous and pseudonymous attribute systems should be used whenever feasible, as imperfect attribute authentication is often weakened, not strengthened, by the addition of imperfect identity authentication.

Author Information

L. Jean Camp is Associate Professor of Informatics at Indiana University, 901 East 10th St., Bloomington, IN 47408-3912; email: ljeanc@gmail.com. An earlier version of this paper was presented at ISTAS'03, Amsterdam, The Netherlands.

References

[1] LA Times Editors, "'No Fly' list traps innocent," *LA Times*, Apr. 14, 2004.

[2] E. Alderman and C. Kennedy, *The Right to Privacy*. New York, NY: Knopf, 1995.

[3] R.E. Anderson, D.G. Johnson, D. Gotterbarn, and J. Perrolle, "Using the ACM Code of Ethics in decision making," *Commun. ACM*, vol. 36, pp. 98-107, 1993.

[4] T. Aslam, I. Krsul, and E. H. Spafford, "A taxonomy of security vulnerabilities," in *Proc. 19th Nat. Information Systems Security Conf.,* Baltimore, MD, Oct. 6, 1996, pp. 551-560.

[5] K. Bowyer, "Face recognition technology: Security versus privacy," *IEEE Technology & Society Mag.*, vol 23, no. 1, pp. 9-19, 2004.

[6] L. Camp, *Trust and Risk in Internet Commerce*. Cambridge MA: M.I.T. Press, 1999.

[7] S. Chakrabarti and A. Strauss, "Carnival booth: An algorithm for defeating the computer-assisted passenger screening system," *First Monday*, vol. 7, no. 10, Oct. 2002; http://www.firstmonday.org/issues/issue7_10/chakrabarti/index.html.

[8] E. L. Eisenstein, *The Printing Press as an Agent of Change*. Cambridge, U.K.: Cambridge Univ. Press, 1979.

[9] J. Fountain, *Building the Virtual State: Information Technology and Institutional Change*. Brookings, 2001.

[10] C. Landwhere, Bull, McDermott & Choi,, "A taxonomy of computer program security flaws, with examples", *ACM Computing Surveys*, vol. 26, pp. 3-39, Sept. 1994.

[11] Lindorff "Is a federal agency systematically harassing travelers for their political beliefs?" *In These Times*, Issue 27, No 2, Nov 22, 2002.

[12] H. M. McLuhan, *The Gutenberg Galaxy: The Making of Typographic Man*. Toronto, CN: Univ. of Toronto Press, 1962.

[13] E. M. Newton,. and J. D. Woodward, "Biometrics: A technical primer," adapted from J.D. Woodward, K.W. Webb, E.M. Newton et al., "Biometrics: A technical primer," *Army Biometric Applications: Identifying and Addressing Sociocultural Concerns*, App. A, RAND/MR-1237-A. Santa Monica, CA: RAND, 2001.

[14] B. Yee and R. Blackley, "Trusting code and trusting hardware," *Digital Identity Civic Scenario*, Harvard Univ., Apr, 2003; available at http://www.ksg.harvard/edu/digitalcenter/conference/references/htm.

Creating Moral Buffers in Weapon Control Interface Design *(Continued from page 33)*

of this paper was presented at ISTAS'03, Amsterdam, The Netherlands.

References

[1] P. Brey, "The politics of computer systems and the ethics of design," in *Computer Ethics: Philosophical Enquiry*, J.v.d. Hoven, Ed. Rotterdam, The Netherlands: Rotterdam Univ. Press, 1998.

[2] B. Friedman and P.H. Kahn, "Human agency and responsible computing: Implications for computer system design," in *Human Values and the Design of Computer Technology*, B. Friedman, Ed. Stanford, CA: CSLI Publications, 1997, pp. 221-235.

[3] B. Friedman and L.I. Millet, "Reasoning about computers as moral agents: A research note," in *Human Values and the Design of Computer Technology*, B. Friedman, Ed. Stanford, CA: CSLI Pubs., 1997, pp. 205.

[4] D. Grossman, *On Killing*. Boston, MA: Little Brown & Co, 1995.

[5] D. Grossman, "The morality of bombing: Psychological responses to "distant punishment," presented at the Center for Strategic and International Studies, Dueling Doctrines and the New American Way of War Symp., Washington, DC, 1998.

[6] D. Grossman, "Evolution of weaponry," *Encyclopedia of Violence, Peace, and Conflict*. Academic Press. 2000.

[7] P.R. Helft, M. Siegler, and J. Lantos, "The rise and fall of the futility movement," *New England J. Medicine*, vol. 343, no. 4, pp. 293-296, 2000.

[8] D.G. Johnson, *Computer Ethics*, 3 ed. Upper Saddle River, NJ: Prentice Hall, 2001.

[9] H. Jonas, *The Imperative of Responsibility: In Search of an Ethics for the Technological Age*. Chicago, IL: Univ. of Chicago Press, 1979.

[10] S. Milgram, *Obedience to Authority*. New York, NY: Harper and Row, 1975.

[11] K.L. Mosier and L.J. Skitka, "Human decision makers and automated decision aids: Made for each other?," in *Automation and Human Performance: Theory and Applications,* R. Parasuraman and M. Mouloua, Eds. Mahwah, NJ: Lawrence Erlbaum Assoc., 1996, pp. 201-220.

[12] C. Nass, J. Steuer, and E.R. Tauberm, "Computers are social actors," presented at the CHI'94: Human Factors in Computing Systems, Boston, MA, 1994.

[13] W.V. O'Brien, *The Conduct of Just and Limited War.* New York, NY: Praeger, 1981.

[14] R. Parasuraman, and V. Riley, "Humans and automation: Use, misuse, disuse, abuse," *Human Factors*, vol. 39, no. 2, pp. 230-253, 1997.

[15] R. Parasuraman, T.B. Sheridan, and C.D. Wickens, "A model for types and levels of human interaction with automation," *IEEE Trans. Systems, Man, and Cybernetics*, vol. 30, no. 3, pp. 286-297, 2000.

[16] B. Reeves and C. Nass, *The Media Equation: How People Treat Computers,Television and New Media Like Real People and Places*. Stanford, CA: CSLI Pubs., and New York. NY: Cambridge Univ. Press, 1996.

[17] T.B. Sheridan, "Speculations on future relations between humans and automation," in *Automation and Human Performance*, M. Mouloua, Ed Mahwah, New Jersey: Lawrence Erlbaum Assoc., 1996, pp. 449-460.

[18] L.J. Skitka, K.L. Mosier, and M.D. Burdick, "Does automation bias decision-making?" *Int. J. Human-Computer Studies*, vol. 51, no. 5, pp. 991-1006, 1999.

[19] D.L. Wells, "Opening remarks," presented at the Swarming: Network Enabled C4ISR, McLean, VA, 2003.