2010

New pathways in identity management

Clark, Paul C.; Cook, Glenn R.; Fisher, Edward L.; Fulp, John D.; Linhoff, Valerie; Irvine, Cynthia E.

Copublished by the IEEE Computer and Reliability Societies, 2010, November/December 2010, pp. 64-67.
http://hdl.handle.net/10945/41127

Editors: Matt Bishop, bishop@cs.ucdavis.edu
Cynthia Irvine, irvine@nps.edu

New Pathways in Identity Management

Paul C. Clark, Glenn R. Cook, Edward L. Fisher, John D. Fulp, Valerie Linhoff, and Cynthia E. Irvine
Naval Postgraduate School

Historically, people established identity using simple attributes. They determined group membership through factors such as language, dress, ethnicity, and behavior, as well as referrals by other group members. Globalization and heterogeneity have dramatically affected our ability to identify individuals solely on the basis of such evidence. As one dog said to the other in a *New Yorker* cartoon, "On the Internet, nobody knows you're a dog."[1] How do you establish identity before granting access to the premises or to protected information? In addition, establishing whether a person has been involved in unlawful behavior is sometimes useful. For example, if a weapon is left at a crime scene, can investigators compare the fingerprints on the weapon to those of known criminals and suspects?

A major challenge in computer-enabled systems and networks is binding the identity of the person outside the computer to the logical entities executing on the person's behalf. Increased user mobility combined with a variety of platforms for conducting work has raised concerns regarding the nature of the devices that deliver and manage information. Furthermore, autonomous devices, such as those in embedded or sensor systems, must be identified. To address identity in the federal sector, requirements have been levied throughout the US government. Most notable of these is Homeland Security Presidential Directive 12, which calls for "a mandatory, government-wide standard for secure and reliable forms of identification issued by the federal government to its employees and to the employees of federal contractors."[2] The US government has extended similar requirements to encompass things—for example, computers, laptops, mobile devices, and sensors.

Identification and authentication of individuals accessing computer systems have always been components of cybersecurity. What's new is the complex technology required for both personal-identity verification[3] and our growing ability to rapidly identify and possibly link individuals with other evidence. The introduction of "things," more transitory than the people using them, creates additional technical complexity. Ample opportunity exists for misunderstandings, confusion, and the construction of costly but ineffective systems.

A clear need exists to appreciate the requirements and supporting technologies for, as well as the use of, identity management (IDM) systems. In response, the US Naval Postgraduate School (NPS) has established a comprehensive IDM education program that includes training and awareness, executive education, graduate-degree programs, and the centerpiece of our IDM education activities: a certificate program.

Determining What to Cover

We wanted the certificate program to be accessible to those without a deep technical background and to be available to part-time students. Our first task was to determine the material that the courses would cover for the certificate. Biometrics was an obvious choice; it provides a way to bind an identity to a physical person. Another easily determined area was the infrastructure required to provide highly distributed, efficient use of identities to support various functions.

In addition, people involved in practical IDM must understand the laws and policies pertaining to the collection, storage, and management of identity information. Because IDM is an emerging area in which some of our graduates might develop policy, we wanted students to not only know about existing policies but also be able to reason about policy concepts from both national and international perspectives.

Finally, IDM involves collecting and managing identity information in the field. Some scenarios are obvious—for example, when someone applies for a government-issued identifier, various kinds of identity information, such as birth records, are required. More challenging might be the correlation of fingerprints from an individual with those obtained from a crime scene or an improvised explosive device (IED). To

address these topics, we needed to discuss IDM's operational aspects.

These considerations led to a six-month program comprising four graduate-level courses.

Motivation for IDM Topics

IDM technology both enables and constrains policy and operations, and vice versa. We decided that by examining the things that could go wrong without IDM, our courses would provide a strong motivation.

Biometrics

First, we examined biometrics. Over the past two millennia, multiple societies independently invented biometrics to solve common problems. How can you prove someone's claim of identity? How can you determine whether this person has been seen before? Modern biometrics uses technology to keep up with the size of the populations and to make quicker, cheaper decisions.

For thousands of years, people have also been using passwords to prove identity by establishing a shared secret in advance. Modern technology incorporates passwords to solve the verification problem, but they have various disadvantages:

- They must be memorized.
- They can be written down to solve the memorization problem, which leaves them vulnerable for others to find.
- They can be shared on purpose, but perhaps in violation of policy.
- They can be observed while being entered.
- They can be guessed.
- They can be calculated if the password database is compromised.
- People are somehow supposed to remember a different password for each computer account.

The most common problem for IT help desks is forgotten passwords, which translates into a large administrative expense. So, using passwords for verification gives only low confidence that it proves a claimed identity, yet incurs high organizational support costs. If passwords protect sensitive data, their disadvantages can have disastrous effects, whether personal (identity theft) or national (state secrets).

Exacerbating the problems passwords pose for verification, they can't begin to solve the identification problem because often an uncooperative person, a nonpresent person (for example, a latent fingerprint), or a corpse must be identified quickly and reliably. Without biometrics, the wrong prison inmate might be released,[4] the wrong suspect in a crime might be identified,[5] or someone's remains might not be identified to give closure to a grieving family.[6] Balanced use of biometrics, including the careful management of biometric information, lets us solve the verification and identification problems without adding the difficulty of managing secrets. Of course, biometrics depends on a sound infrastructure.

Infrastructure

Often, a flaw in identification or authentication lies at the core of network vulnerabilities. When IDM has been applied to devices, many potential, and realized, failures have (or could have) led to attacks. Such attacks can target information confidentiality, integrity, or availability. Additionally, because some physical infrastructure (for example, power, water, and transportation) components might be monitored and controlled via the Internet, attacks on their process control systems can lead directly to physical damage or disruption.

We now describe seven motivating IDM infrastructure issues.

DNS cache poisoning. This attack delivers fallacious IP addresses associated with server names (fully qualified domain names) to Domain Name System (DNS) servers. DNS servers accepting these "updates" facilitate the attacker's goal of redirecting traffic to a computer of the attacker's choosing. Because most DNS information isn't authenticated, anyone can impersonate a DNS server and provide false name-to-IP address mappings.

Dynamic routing protocols. Most routers run protocols that support the collective sharing of route table information. This information influences the path that packets traverse. Because most routers don't authenticate route information received from other routers, an attacker can create false route information and deliver it to legitimate routers.

Specious equipment. Recently, criminals placed legitimate Cisco Systems serial-number placards on networking gear manufactured in China, then sold the gear to unwary buyers.[7] This subverted supply-chain integrity and increased the risk of intentionally installed hardware or software artifices.

RFID-enabled payment systems. Because most RFID implementations for payment systems (for example, in toll booths) employ passive chips, processing power is extremely limited, and inclusion of any authentication protocol is rare. So, an attacker can capture and replay payment account data, causing unauthorized charges.

RFID-enabled passports. The combination of RFID and ID documents potentially facilitates identification, tracking, and targeted cueing of electronic IDs. This example highlights a case in which anonymity might be desired in an IDM implementation.

"IP-enabled" process control. Some process control sensors and actuators (for example, distributed control systems and supervisory control and data acquisition systems) are accessible over public net-

works, including the Internet. The potential for attacks is greatly exacerbated when no authentication is required before device access.

EMV chips and PINs. Implementation of card-to-ATM authentication by EMV (Europay, MasterCard, and Visa) has proven vulnerable to a relatively simple man-in-the-middle attack that subverts the authentication.[8] This allows any PIN to be accepted as valid.

Identity Management 101

Before the courses start, we give a three-hour lecture called Identity Management 101 to introduce the students to IDM's many dimensions.

The lecture begins with an overview of six core IDM topics. First, we define IDM. We present two example definitions based only on persons, then expand the definition to address nonhuman entities.

Next, we introduce a 2 × 2 matrix. On one dimension are identification and verification; on the other are humans and nonhuman entities. Both "human quadrants" are easily understood; however, verification of a nonhuman entity often challenges students with less technical backgrounds. We explain this quadrant by illustrating a logon based on the Common Access Card (CAC), showing the two constituent authentications: CAC to cardholder and server to CAC. The CAC and server are clearly nonhuman. Identification of a nonhuman entity is the least familiar quadrant. We explain it with two examples: metallurgical analysis of IED fragments to help identify the manufacturer, and bit string analysis of binary code to identify a known computer virus.

Our third topic centers on security services enabled by IDM mechanisms. For identification, this is simply the removal of anonymity. For verification, the resulting proof of an identity claim enables the spectrum of security controls dedicated to access control and audit. When the underlying protocol employs asymmetric cryptography and time stamps, nonrepudiation can also be supported at the technical level.

The fourth topic is subject enrollment. Given the relative ease of forging "breeder" documents, such as birth certificates, some consider enrollment to be IDM's weakest link. A "Bob Old versus Bob New" scenario facilitates thoughtful discussion. A man "legally" named Bob Old presents specious documents identifying himself as Bob New, which the registrar accepts. If his new credential entails biometric binding, he is now and forever associated with this new name. Furthermore, the enrollment date is on record, so any association of that identity with this person's history before that date remains open to question.

The fifth topic contrasts biometric and secret-based authentication. Students learn that biometric information is unique to a person, is always with that person, and can't easily be changed. In typical use, biometric verification is optimal in local applications in which the user is physically present and provides the "raw" analog biometric information directly to the verifier. Otherwise, a risk of a replay attack exists. For remote applications or local applications that haven't been biometrically enabled, proof of possession of a secret is the basis for verification. We examine secret-based verification's strengths and weaknesses: its scalability and flexibility versus insufficient bit entropy and implementation flaws that can leak information related to the secret.

The last topic names the principle IDM roles. Once the *subject* registers, he or she becomes a *subscriber*. A subscriber engaging in a transaction becomes a *claimant*. The party with a stake in a claim's veracity is the *relying party*. The *verifier* checks a claim's veracity. The *credential service provider* binds identity attributes to an identity credential. We use various scenarios to illustrate these roles.

Course Content

Each of the four courses covers one of the areas we mentioned in the section "Determining What to Cover."

Biometrics

This course reviews the technical details of biometric identification and verification. It covers the major approaches (for example, fingerprints and irises) with respect to acquisition of biometric data, matching techniques, antispoofing techniques, and current standards. The course also covers biometrics' uses and limitations.

Identity Management Operations

This course addresses using IDM in real-world settings and the largely managerial and social aspects of IDM related to actual implementations. It provides an operational overview of the tactical and strategic advantages derivable from a properly designed and operated IDM program. It presents generic descriptions of both identification and verification use cases, followed by the review of several specific fielded IDM programs. The course addresses repositories for identity information and the use of open standards for exchanging that information. It also analyzes using context, error probabilities, and other factors as components of IDM applications in various operational environments.

Identity Management Infrastructure

This course covers the technologies necessary to support e-authentication and the secure transfer of biometric information. It also addresses the identity of platforms, devices, sensors and other "things." It covers a broad range of topics related to the standards, protocols, technolo-

gy, and management infrastructure necessary to field an enterprise-level IDM solution. Lecture and reading assignments span the gamut of IDM issues, from low-level authentication protocol mechanics to high-level identity federation initiatives.

Identity Management Policy

This course addresses the overarching guidelines, standards, and laws influencing IDM implementations. It assesses any given IDM program's life cycle (provision, distribution, operation, and deprovision) against policy, laws, and regulations pertinent to the establishment, collection, distribution, and maintenance of identification credentials. Of particular interest is the proper scoping of IDM organizational and technical policy so as to balance the often conflicting goals of security and privacy protection while maintaining and exchanging personally identifiable information.

Hybrid Course Delivery

We loosely modeled our program on an existing NPS program, despite our fewer resources. We teach the courses in a hybrid delivery mode that lets students meet ongoing work responsibilities while enrolled in classes. This mode combines traditional classroom lectures and labs with Web-based instruction. The on-campus instruction acclimates students to graduate studies and builds a feeling of team membership that creates a sense of obligation to complete the course work.

The first week of course work is onsite. Activities include Identity Management 101, invited talks and presentations, and extensive lectures and exercises for the first two courses (Biometrics and Identity Management Operations). Approximately nine weeks of asynchronous Web-based instruction follow. Then, students return to the classroom for more lectures, presentations, lab exercises, and final exams. We've arranged the schedule so that students segue into the next two courses (Identity Management Infrastructure and Identity Management Policy) in the following week with a full slate of classroom work. This, again, is followed by Web-based instruction. After another nine weeks, the students return for more on-location study and completion of the certificate program.

A Web-based content management server linked to the course website supports both course management and instruction. The server includes tools to support group discussions, access to course materials, and quizzes.

We launched the certificate program in September 2008. Cohorts of between 20 and 25 students convene quarterly. Participants come from a range of US Department of Defense and federal agencies, many with locations across the US and overseas. By September 2010, 143 students in nine cohorts had enrolled, and seven cohorts (114 students) had completed all four courses. The attrition rate was 10 percent, which compares favorably to the attrition rates of 43 percent or higher in traditional distance-learning programs. We attribute the program's success to a combination of engaging material and the hybrid delivery model. To continue with a degree program that builds on the IDM certificate, students can enroll in the NPS Master of Arts in Identity Management and Cybersecurity program. □

References

1. P. Steiner, "On the Internet, Nobody Knows You're a Dog," cartoon, *New Yorker*, 5 July 1993, p. 61.
2. "Policy for a Common Identification Standard for Federal Employees and Contractors," Homeland Security Presidential Directive 12, Office of the Press Secretary, The White House, 27 Aug. 2004.
3. "Personal Identity Verification (PIV) of Federal Employees and Contractors," *Federal Information Processing Standards Publication 200-1*, US Nat'l Inst. Standards and Technology, Mar. 2006.
4. B. Nuckols, "MD Revises Procedures after Wrong Inmate Released," *Washington Times*, 3 Mar. 2010.
5. S. Greene, "Evidence Proves Innocence after 24 Years," *Denver Post*, 25 July 2007.
6. F.N. Rasmussen, "Unknown Soldier—but Not Forgotten Honor," *Baltimore Sun*, 14 Nov. 1998.
7. "Fake Cisco Serial Numbers in $1 Million Chinese Computer Parts Scheme," *Homeland Security Newswire*, 4 Dec. 2009.
8. S.J. Murdoch et al., "Chip and PIN Is Broken," *Proc. 2010 IEEE Symp. Security and Privacy*, IEEE Press, 2010, pp. 433–446.

Paul C. Clark *is a research associate in the Naval Postgraduate School's Department of Computer Science. Contact him at pcclark@nps.edu.*

Glenn R. Cook *is a senior lecturer in the Naval Postgraduate School's Department of Information Sciences. Contact him at grcook@nps.edu.*

Edward L. Fisher *is a lecturer in the Naval Postgraduate School's Department of Information Sciences. Contact him at elfisher@nps.edu.*

John D. Fulp *is a senior lecturer in the Naval Postgraduate School's Department of Computer Science. Contact him at jdfulp@nps.edu.*

Valerie Linhoff *is a special-projects coordinator at the Naval Postgraduate School's Department of Computer Science. Contact her at vllinhof@nps.edu.*

Cynthia E. Irvine *is a professor in the Naval Postgraduate School's Department of Computer Science and the director of the school's Center for Information Systems Security Studies and Research. Contact her at irvine@nps.edu.*