

Workshop on States Security: Identity, Authentication, and Access Control

March 27-28, 2002

www.security.scs.cmu.edu

Robert Thibadeau, Ph.D.
CMU Security Research Workshop Series
School of Computer Science and the Heinz School
Carnegie Mellon University
Pittsburgh, Pennsylvania

Workshop Sponsored By
AMS (www.ams.com)
Wave Systems, Inc. (www.wave.com)

Contents

Executive Summary	2
Presentations and Discussion	4
Appendix I: Full Text of Gov. Howard Dean's Address	10
Appendix II: Full Text of the Agenda	16
Appendix III: Roster of Participants	18



Gov. Mark Schweiker, Gilles Lisimaqu

Lark Allen, Robert Thibadeau, Phillip Hallam-Baker, Gov. Howard Dean

Executive Summary

On March 27 and 28 an invited group of experts assembled to address issues of States security with two themes:

1. A Computer Emergency Response Team (CERT) for States, and
2. Interoperability of drivers licenses

This white paper is the report from that workshop. The conclusions of the workshop are:

1. A separate CERT for States would be highly desirable based on the experiences of the CERT coordination center and based on the experiences and expectations of the security experts assembled.
 - a. Experience with over 100 CERTs suggests that CERTs need to have focused constituents/memberships and that the “States” level appears to be a level which is highly promising.
 - b. Gubernatorial support in a CERT for States is justified because of the implications for states security, and because there are so many information technology departments which will directly and materially benefit. NASCIO, the National Association of State CIOs and AAMVAnet are just two examples of the important information technology groups that should be involved. Without the interest of the highest levels of the state governments, participation by key beneficiary groups may not occur.
 - c. The direct cost of such a center (estimated at \$3-7M a year to support all 50 states) was deemed highly justified by the expected benefits. Equally important is the need to provide the information technology departments and interstate associations with the resources they need to participate in the CERT.
1. The process of developing next generation interoperable drivers licenses is well in hand

by the AAMVA. Recommendations included:

- a. Strong support for open and public discussion on all the issues based on the need to establish a robust system. Open and public discussion is the best way to insure a secure, strong and long-lasting result as well as achieving a result that will be accepted by the various constituencies for driver's licenses.
- b. It was suggested that state leaders should consider asking for a drivers license solution that can last for at least some number of years. Certainly this number should be more than 20 and reasonably no more than 50 years.
- c. Separate advisory teams of unbiased experts should be convened to provide expert guidance on the following areas.
 - i. Privacy Technologies because of the potential for privacy abuse.
 - ii. Pattern Recognition / Biometrics Technologies because biometrics are error prone and therefore highly subject to over-optimistic misrepresentation. The group recommends the wise use of multiple biometrics.
 - iii. Security, because of the high degree of expertise needed to evaluate security threats.
 - iv. Public Policy and Law from all levels, International, National, State, Local because of the widespread accepted uses of driver's licenses.
 - v. Interactions / Secondary Driver's License Applications (e.g., using a driver's license to establish identity and age). Possibly just a directive to groups i. (Privacy), iii. (Security), and (iv.) Public Policy. In particular, there is a concern to make sure that foreign national identity methods and national identity methods have interoperability and comparable utility in security, privacy, and authentication. Note this requirement may be outside the scope of the AAMVA but should be within the scope of other National and State constituencies.
 - vi. Large scale, pervasive, evolving systems. The information systems needed to support interoperable, functional, secure, and privacy-safe driver's licenses will be among the largest scale systems ever constructed. As in the other areas, great expertise is highly desirable both with regard to managing change and designing robust, reliable, and sustainable systems.

Presentations and Discussion

Welcome

Jared L. Cohon, President, Carnegie Mellon University

Jared Cohon noted the importance of a convocation of this form on States Security. The workshop was established in the security workshop series. Each workshop in this series focuses on a different problem of security where computers are involved. He mentioned that of the 19 terrorists on 9-11 there were 63 valid drivers licenses. The group assembled included a small diverse assortment of technical and public policy experts in order to engage in open and unfettered discussion of important issues of states security.

Workshop Organization and Themes

Robert Thibadeau, Principal Research Scientist, School of Computer Science,
Carnegie Mellon University

Robert Thibadeau introduced the major themes of a CERT for States and Driver's License Interoperability. He noted that the New York Times had published a recent report from a Boston Bar that was using the Magnetic Stripe information on the back of most Driver's Licenses to gather personal information about people coming to the bar as well as the more expected use of determining if the cardholder was of legal age to drink. He showed a system which can provide identity information tailored to publicly acceptable rights to information. The system would be highly secure against fraud, identity theft, tampering, and counterfeiting while simultaneously dramatically improving on personal privacy. It could also be anticipated to be useful by law enforcement in saving lives. This system is practical in the sense that we have the technical know-how to implement it. However, it would be relatively expensive, it would require detailed coordination with the law making bodies on both a federal and state level, and it would require national centers to tie together key data and support for the information technology infrastructures. Among these a CERT for States would be highly desirable.

Technologies for Identity Tokens

Gilles Lisimaque, VP, Gemplus

Gilles Lisimaque is one of the founders of the largest Smart Card company and has over a dozen years of direct experience in identity cards. Over 4 million smart cards are manufactured everyday worldwide. Gilles emphasized that the card-format is the most common because it can be printed for human reading, is convenient for wallets and for envelopes. He pointed out that the solution path suggested by Robert Thibadeau (and others) could be largely met by inexpensive smart cards but that the full solution would require relatively expensive smart cards (i.e., a dollar or two compared to twenty or thirty dollars per card). However, experience dictates that the readers for smart cards is the area where the most careful planning needs to be done. The readers need to recognize existing needs and future needs as well. Standards are very important.

Keynote

Governor Howard Dean, Vermont

Governor Dean provided an important address directed at the information technology community in support of smart cards and their careful use so as to protect privacy while improving security. Among the many insightful and important observations was this one.

“We are attacked by **individuals** --- united not by a ***national*** cause --- but by cell phones, computer networks, exploding shoes and box cutters. Therefore, our security systems must account for this reality. Security must adapt to the threat of individuals --- not just nations --- while still protecting our fundamental civil liberties.”

The threat to security today, is a threat from small groups of individuals. States have much of opportunity and obligation in establishing security to the individual level. Driver’s licenses are currently the de-facto identification device and therefore need state support and attention, and local and state law enforcement need the tools to accurately determine identity and accountability without interfering with the privacy and rights of the individual. The technical and vendor community is needed to educate all the players as to the opportunities that exist for improvement in national security through state action.

Managing Privacy and Identity - Issues at the State Level

David Chaum, Privacy Technology Innovator

David Chaum emphasized that security and privacy is not a balancing act. More security does not mean less privacy as many people naively think. Instead, security and privacy can be simultaneously improved if attention is given to improving both. Security only damages privacy when security is addressed without simultaneously addressing privacy. David showed a number of technical mechanisms. In one surprising observation, he observed that while security usually demands there should be no ‘backdoor,’ with privacy you need a ‘backdoor.’ Gaining detailed information about an individual should always be possible with suitable authorization even though most of the time this information may be kept perfectly hidden.

Authentication and Access Control for Networks

Jeremy Stieglitz, Group Product Manager,
Cisco’s Identity Management Solutions

Jeremy Steiglitz covered the product offerings of Cisco including the product offerings that provide authenticated access control to network resources. Cisco equipment represents an important and pivotal source of the infrastructure that is participating in securing the Internet.

Welcome to Pennsylvania and Call for Participation

Governor Mark Schweiker, Pennsylvania

Governor Schweiker emphasized that the states groups, technical experts, and policy experts need to assume personal and direct responsibility for taking action to improve homeland security. He emphasized that we must not forget the events of 9-11 because it was clear, for many reasons, that these events are just an example of what can and will happen in the future without the active participation of these groups.

CERT for the States? A CERT Perspective

Richard D. Pethia, Director CERT Centers

Richard Pethia laid out what was generally recognized as a tour-de-force on why a CERT for States is not just desirable but is essential. Richard directs the CERT Coordination Center, which is both the first CERT and also the CERT that coordinates the activities of over 100 other CERTS globally. He pointed out that the CERT Coordination Center alone received over 52,000 incident reports in 2001 and has a catalogue of current system vulnerabilities in excess of 2,500. The vulnerability list is doubling every year. No single IT department can even hope to keep up with this. A CERT can function to interpret the deluge of information about threats for its specific constituency but must be independent of its constituency and the vendor community in order to provide the highest quality service to both. Trust is everything. The CERT must provide its services quietly both to maintain the trust necessary to gain access to security problems that may exist and to stimulate improvements without finger pointing.

A CERT’s main function is incident handling. Other services include alerts and announcements,

vulnerability analysis, cyber-forensics, practices and facilities security training, intrusion detection, risk analysis and auditing. It can be used to outsource security testing of products so as to eliminate redundancy. A CERT must also explicitly coordinate with other CERTs. Most important, the best CERTs are those that know their community. CERT's experience shows that you cannot expect the national CERT to handle states problems. CERTs are appropriate to communities of trust and responsibility. Since a single CERT with only a few dozen people effectively handles national problems, a similar sized CERT could handle states problems. However, these people have to be selected not just for their technical skills but also, and equally, for their communication skills.

CERT for the States? General Discussion

The main discussion was why States seemed to be "right sized" for a CERT. It was recognized this is a preliminary judgment call, and that only the state organization with appropriate state leadership can, in the end, make this determination with the assistance of the experts.

Risk Assessment in Large Scale PKI

Don Beaver, Ph.D. Harvard, Cryptology, Security Architectures, Seagate Research

Don Beaver focused on methods for estimating risk. He drew on extensive experience in the banking industry to show how banks control risk from information threats. In the case of the financial community, risk is mitigated by making sure that no single individual can, acting alone, do too much damage. As one example, no person who can issue a driver's license should be able to issue too many too fast. By careful attention to what one person can do, risk can be mitigated well enough that insurance companies can and will come in to provide insurance protection on infrastructure. Without careful attention to setting up systems with risk management designed in, the threats can become unbounded.

International Security Trust and Privacy Alliance (ISTPA), Framework

Michael Willett, Ph.D. UNC, Cryptology, Strategist, Wave Systems, Inc.

Michael Willett pointed out that the trade organization of the ISTPA has created the first framework for outlining the technologies needed to manage personal information privacy in the digital age. This framework can provide guidance to designers of identity, authentication, and access systems who wish to incorporate privacy considerations. The ISTPA Framework emphasizes techniques for handling the "life cycle of personal information" throughout the information infrastructure.

Federal/State Relations

Jeffrey Hunker, Dean, Heinz School of Public Policy

Jeffrey Hunker brought his experience as the head of cyber security for the National Security Council during the Clinton Administration to the problem of states security. He pointed out that there is general recognition that an Information Coordination Center, much like the one that handled Y2K, is where we are going with much of the security stuff. He emphasized that such a coordination center requires the voluntary involvement of people from state, local, and corporate organizations. He pointed out that there are legal hurdles, policy hurdles, as well as the technical hurdles. For example, it is generally recognized that information attacks may require triage – when you can't fix everything at once. How do you decide to help problems in one state perhaps at the expense of not helping in another state. The only solution is that the states are involved actively in deciding on policy. A national center is also the place where risk can be managed. For many reasons such a national center for the states needs to be run by the states. Finally, he emphasized that our tort system need to incentivize appropriate behavior and in that regard is woefully inadequate today.

Sustainable Computing

Bill Scherlis, Principal Research Scientist, School of Computer Science

Bill Scherlis focused on high dependability and sustainable computing. You cannot build an ROI (return on investment) model for dependability if you don't have a way to measure the R. How do we value, for example, the benefit of new technologies such as those for security and identity? Part of the security picture is improving and assuring various dependability attributes of the underlying systems. Despite much talk, there is still no consensus on how to achieve our dependability goals. Obtaining such a consensus requires us to consider together technological factors, including improvement, measurement, and assurance, as well as economic, market, legal, and regulatory factors. The term "sustainability" refers to the comprehensive treatment of these factors. CMU is undertaking an effort to bring the various stakeholders together to explore the interrelationships among these factors and achieve meaningful approaches to IT risk management. The States face particular challenges as they develop solutions that must embrace the rapidly moving targets of commercial technologies and standards, along with the architectures for other state systems, as well as linked federal and municipal systems. What technology management approaches can be defined to support this process effectively?

PKI Practice: Addressing the Issues of Scale, Complexity, Interoperability

Phillip Hallam-Baker FBCS C.Eng., Principal Scientist, VeriSign Inc.

Phillip Hallam-Baker pointed out important industry initiatives in Public Key Infrastructure, one of the Trust Infrastructures seen to be essential in lifting both security and privacy. Verisign handles all .com traffic routing, much of the authentication for finance, and lately telephony routing. He emphasized there are three major standards initiatives that need to be carefully studied: X.509 (ISO/ANSI), XKMS and SAML as being highly relevant to states security concerns about identity and authentication.

NIST Security Initiatives

Timothy Grance, Manager of Network Security Research, NIST

Timothy Grance emphasized the role of NIST in supporting the national information infrastructure. NIST is an organization that focuses on measurement. They currently support over 52,000 organizations in public safety. NIST can be called on to help in tailoring assurance technologies based on information valuations and cost of ownership. He mentioned that Intrusion Detection Systems, though sexy, do not have measurable benefit. Rather than focusing on band-aids to patch systems that are vulnerable, he suggested that focus is most cost effectively placed on the proper design of systems built to last. There is a great deal of expertise available nationally in security architectures, embedded systems, evaluation, composability, sociology and security and avoiding the tyranny of the installed base. In effect, it is never too late to design the system correctly. NIST also can help in raising awareness about possible operating systems, database, PKI, smart card, biometric, firewall, and wireless security technologies. They represent probably the best objective single source nationally on desirable, and feasible, security attributes in these technologies. They function in strong support of the vendor community as well as the user community.

Trusted Input Devices - Distributed Strong Authentication

Lark Allen, Executive VP, Wave Systems

Lark Allen introduced several new devices for strong authentication and strong trust. These use islands of strong trust that are supported by silicon so as to insure that the client side of consumer transactions can be trusted. He showed a new keyboard where the key strokes cannot be intercepted by a hacker intent on stealing passwords or other critical information. Both the keyboard and a USB-attached device contain the Wave EMBASSY security chip, which can be programmed for client-side support of sensitive applications. He also showed a European FinRead (financial reader) device where stronger authentication and authorization is required because the authorization is for moving real money. Similar systems will in all likelihood be needed at points of contact between states and their employees and their constituencies in order to secure the systems.

State DMV as Interoperable Identity Credentials

Jay Maxwell, President, COO, AAMVAnet

Jay Maxell presented a comprehensive overview of the AAMVA and AAMVAnet activities in drivers licenses. The AAMVA represents 100% of all the state motor vehicle associations in the United States and Canada. This represents 68 jurisdictions.

The drivers license (DL) is the de-facto primary identification document in the US. 68 jurisdictions means 68 unique systems. There are no current standardized security features. The system is currently based on reciprocity meaning that one state just recognizes the DL from another. However, reciprocity is not ideal. Also, people can easily download templates for DLs in all states and make credible counterfeits. There are over 6,000 valid forms of birth certificates. No DMV official can hope to know whether a particular proof of identity is real, so this means that DLs have a weak basis. There is only limited federal oversight. The national system also includes:

1. Truck driver licenses are coordinated nationally for the 10.5 million truck drivers.
2. 30 Million Revoked or Suspended licenses are in a national database.
3. Every DMV has a link to social security for validation that a particular name goes with a particular social security number and a particular birth date.

The system needs first to be improved to guarantee that of the 250 million people with driver's licenses they cannot have a drivers license in more than one state – as is the mandate with truck drivers. The reason is that criminal records are associated with drivers licenses and people will get new drivers licenses in order to get by limits on the number of traffic convictions.

In the next year the goal of the AAMVA is to develop the specifications for the next general drivers license. Since drivers licenses are commonly used for ID purposes it is unreasonable to assume that the new drivers licenses will not be used for ID purposes beyond determining that you can drive a car. The next year will also implement a photo exchange program and the electronic state-to-state check of licenses. Also in the next year there will be the preliminary design of the new DRIVeRS (Driver Record Information Verification System). Finally, after this year, the AAMVA intends to provide for new interoperable DL card designs that can meet all the needs of the many stakeholders.

The AAMVA is committed to open public discussion as evidenced clearly by Jay Maxwell's active and open participation in the Workshop and by the involvement of others from the AAMVA and DMVs. This was deemed as essential if we are to arrive at secure and privacy preserving solutions going forward which meet the mandates outlined by Governor Dean, Governor Schweiker and other state and national leaders.

Enterprise Identification Objectives

Barry Goldman, AMS

Barry Goldman emphasized that insider threats are among the biggest threats for the DMVs. Furthermore, DMVs are like many other large and geographically diffuse State and Local government organizations. State and local governments almost universally need to focus on insider threats precisely because of the many touch points with the population. Therefore the devices and software systems that register membership and identity must take account of what a malicious insider can do. He demonstrated a new system, Identicate, which cross-correlates to detect any of numerous kinds of fraud that may exist for systems such as driver's license issuance systems.

Framework for Non-repudiation

Gary Daemer, Senior Principal, AMS Center for Advanced Technologies

Gary Daemer introduced the CMU Practicum Team sponsored by AMS for providing a component of the Identicate system. The Practicum Team demonstrated a method for PKI signing of documents from remote

terminals and also demonstrated the architecture for PKI Middleware that could support the activities of knowing who is being authenticated and who is authenticating the authenticatee.

Identity Credential Authentication

Bruce Monk, President and COO, AssureTec Systems, Inc.

Bruce Monk pointed out that there are 400-600 Official Government identity documents in use in the US. The verification supplied by the ID document should be as good as the original enrollment and the original enrollment for all the types of documents needs to be secured. As such, Bruce was pointing out that the driver's license problem is only one of hundreds of others that similarly need to be secured both against threats and to preserve privacy. AMS is one vendor committed to providing a comprehensive, correct-by-design, solution.

Driver License General Discussion

William Scherlis and Robert Thibadeau, Principal Research Scientists,
School of Computer Science, Carnegie Mellon University

The discussion resulted in the executive summary presented at the beginning of this white paper. One observation that was made which is very pertinent is that we need to coordinate our activities not only with states and nationally, but with the International community. Governor Dean's observation that the threat now is from the individual, means that an individual in a foreign country can now substantially threaten state and locality security. If we do not intend to make sure that foreign identity documents and methodologies are properly integrated with our systems, then the threat is actually not diminished by our own activities. Thanks to Peter Sprague for this observation.

Appendix I : Full Text of Gov. Howard Dean's Address

CARNEGIE MELLON UNIVERSITY ADDRESS GOV. HOWARD DEAN STATE OF VERMONT

Wednesday, March 27, 2002

Workshop on States Security : Identity, Authentication, and Access Control
School of Computer Science and the Heinz School
Carnegie Mellon University

Good morning and thank you for the opportunity to meet with you today.

Not so long ago---when my grandparents were about the age I am now --- television came onto the scene.

It's hard to believe, but there were those who honestly thought that while you watched people on TV --- the people on TV could watch you right back. Right there in your living room!

We laugh. But as you all know -- probably better than most Americans -- technology has advanced to the point that we *can* watch people in their own living rooms.

You can track me on the computer as I surf the Internet, or make purchases with my credit card, or look for just about anything on-line.

Even in a password-protected network, an individual can install a "worm" on your computer that can read every key stroke as it is typed -- without the PC user ever knowing. This makes password theft a breeze.

You can send me a disastrous virus. Or as EDS head Richard Brown warned recently, you could do a lot worse. Here's his fear:

"... a crippling new wave of attacks might come next, puncturing the nation's underbelly and disabling the networks that keep nuclear missiles in their silos, the lights on in hospitals, and ATM's belching out cash."

What about global financial transfers, electricity grids -- even local traffic lights and airport controller tools?

As Brown says, "we are as vulnerable to an electronic Pearl Harbor now as we were on September Eleventh..."

Without knowing it, our desktop computers can be used in an attack on our networks.

The viruses, the worms, and the other attacks we've already seen are nothing next to what might happen if we don't act today to secure our network infrastructure.

Our data infrastructure has become vital to the functioning of the nation. Without it, we can't communicate, we can't work and we can't be safe.

While our grandparents thought the only kind of "cookie" was something to be dipped in milk, they still had the right instincts about the downside of technology's future.

Their worst technological nightmare is now electronically possible. People on the Internet really CAN watch us right back --- whether we want them to or not.

Things have changed. Today, our children carry around more computing power in their Game Boys than NASA had at their disposal when *Sputnik* was launched.

In a very short time, we have made an electronic revolution so pervasive and accessible that we have completely reversed the old definition of power.

We have empowered **the individual** in almost unimaginable ways.

This is, quite simply, the greatest democratizing fact in world history.

At the same time, this change has taken away something comforting. Our grandparents knew who the enemy was and where they lived.

We don't.

Modern technology has empowered individuals... all kinds of individuals ... including individuals who want to destroy us.

The thought of being attacked by the *nation* of Afghanistan is laughable. The very idea of the nation-state is being challenged by the borderless networks of crime syndicates, drug empires and terrorists.

There are no boundaries anymore.

We are attacked by **individuals** --- united not by a **national** cause --- but by cell phones, computer networks, exploding shoes and box cutters.

Therefore, our security systems must account for this reality. Security must adapt to the threat of individuals --- not just nations --- while still protecting our fundamental civil liberties.

Denying this would be like saying we don't want to re-enforce cockpit doors because it will restrict pilot movement.

We have recognized and begun addressing some of the threats posed by terrorists. No longer can we board a plane without a thorough screening; our borders are tighter; we have to produce identification to enter certain buildings.

But how do we protect ourselves from the cyber-threat, knowing that the personal computers sitting on our desks today were never designed with security in mind?

Security used to mean locking your front door or getting a dog. Today, powered by the Internet and driven by browsers, anyone can be a cyber-terrorist and anyone can be a victim--- often without realizing it.

With a growing sense of concern, governments and businesses have invested billions to secure their servers at the core of the system ---

--- but little has been spent to secure the most vulnerable part of the network --- the PC, the laptop, the government and corporate desktop computers – all at the perimeter of the computer network system.

This is a mistake because the computing power at that perimeter can be used --- Napster style --- to take the entire network down.

And any PC or desktop can anonymously be used to launch an attack with far more devastating consequences than we've ever witnessed.

September Eleventh was a wake-up call to increase the level of security at critical points in our public infrastructure such as airports.

Now we must focus on the perimeter -- the desktop, the laptop and the PC.

This cannot wait. In recent weeks, even Microsoft has declared that the security of the PC is a critical issue --- **right now**. Thousands of Microsoft engineers have been re-assigned from other projects to the PC security detail.

It is time to take a serious look at hardware and smart-card based solutions.

I believe that the states -- and therefore *you* -- will lead the way in the discovery and implementation of greater digital security. Some of you have already begun this process.

States can move faster than the federal government to ensure that employees accessing the state's network are indeed who they say they are – and that they are doing legitimate business.

But it would be shortsighted to imagine that your work is limited to solving these problems only for state employees.

State Chief Information Officers, and each of you here today, have tremendous power to forge a solution that will set the standards for securing devices for all of us, not just those accessing state resources.

We must develop flexible solutions that will likely require the use of Smart Cards and some form of hardened security in a reader or desktop device.

For example, one state's Smart Card driver's license must be identifiable by another state's card reader. It must also be easily commercialized by the private sector and included in all PCs over time -- making the Internet safer and more secure.

In an age where identity and trust are paramount, the fact remains that the only viable form of universal identity in the U.S. today is the state-issued driver's license.

Think about it: When you entered the airport or the train station to travel to this conference, how many times did you use your driver's license to prove your identity?

Remember -- this is the same driver's license that teenagers alter in order to get into a club or buy cigarettes. Terrorists do it all the time. They did it on September Eleventh.

As you know, states have made great strides in developing drivers licenses that are difficult to counterfeit --- even by ingenious teenagers.

But the question remains --- how does an airline agent at the Pittsburgh airport know what an Alaska or Florida license is supposed to look like, let alone identify a counterfeit?

It is clear that the state issued driver's license is the current identification standard. It is also clear that this is certainly an inadequate way to go through this uncertain world.

Many in private and public life have called for a national identification card. In spite of Larry Ellison's offer to provide the necessary software for free --- this has raised a public outcry concerning privacy and sharing too much private information with the government.

We can't let this become our briar patch. I'm from Vermont and believe me, government is kept at a respectful but very conscious distance.

Reality demands that we understand ---First --- that the rise of empowered individuals whose single mission is to destroy Americans means that we have to fight them at an INDIVIDUAL level and...

...Second --- that we have already ceded our private information to faceless credit card companies and direct marketers who then sell it for a profit.

Now --- I believe that our nation has the technological capacity to protect both our privacy **and** our way of life.

And I am convinced that these complex solutions rest in a successful partnership between private enterprise and government --- led by state governments.

As we stand here today, please accept the vital challenge I offer each of you.

The solutions you create to protect your state's networks must be implemented in a complimentary manner, allowing interaction between every state of the Union.

We must tighten driver's license standards among the states. Fortunately, this work has already begun, led by the American Association of Motor Vehicle Administrators' Task Force on ID Security.

Beyond that, we must move to smarter license cards that carry secure digital information that can be universally read at vital checkpoints.

And we must include new security features to provide ever-greater protection against counterfeiting.

Issuing such a card would have little effect on the privacy of Americans.

I understand that you will be discussing privacy issues at a later workshop in this important conference --- but let's take a moment to look at privacy in America today.

In many ways, privacy is the new urban myth.

Your credit card company knows every flight you've taken; they know your rental car, your hotel, the movies you watched, and where you had breakfast. Credit card companies have a

stake in knowing everything about you because it's a marketer's dream. The information for sale regarding your private life is detailed -- and lucrative.

When it comes to the Internet, every web page you have ever visited, every e-mail you have ever sent, every word you have ever typed, is stored somewhere and can be accessed by someone with the right skills. And as you well know, it's not just the Good Guys who possess these skills.

What's the fastest growing crime in the U.S.? Identity theft --- stealing individuals' identities -- not just their credit card numbers but their very existence.

So, is the answer to create an Orwellian Ministry of Information? No. It's about creating safe passage through a free but threatened life.

We will not, and should not, tolerate a call to erode privacy even further --- far from it. Americans can only be assured that their personal identity and information are safe and protected when they are able to gain more control over this information and its use.

Again, this points to Smart Card adoption and development of card readers that limit information access but also confirm it --- when appropriate.

The same Smart Card that confirms that a person is a registered voter can also be used to validate age in a liquor store.

The Smart Card owner may decide to put her medical information into the card database, which can be accessed by an Emergency Medical Technician with a universal authorization code. That EMT can learn the blood type and complete medical history of an unconscious accident victim.

The beauty of the Smart Card is that the liquor store doesn't know anything but age, and the hotel doesn't know about non-hotel purchases, and the state knows nothing about any of it.

On the Internet, this card will confirm all the information required to gain access to a state network -- while also barring anyone who isn't legal age from entering an adult chat room, making the internet safer for our children, or prevent adults from entering a children's chat room and preying on our kids.

A Smart Card reader at the airport, adapted to a universal standard perhaps designed by those in this very room, could match the ticket and the baggage with the card presenter.

Recently, Sen. Dick Durbin of Illinois and Rep. Jim Moran of Virginia introduced legislation to provide funding to states to increase the security features of driver's licenses. The Moran Bill provides additional and specific funding to states to develop Smart Card capabilities.

I strongly support these efforts and urge you to do the same.

The European Union is ahead of us because they adopted Smart Card technology long ago. The EU has ambitious plans to deploy Smart Cards and Smart Card readers throughout the continent -- and to securely deliver electronic government services, electronic banking, and electronic commerce.

Hong Kong is using Smart Card technology with biometrics at security check points.

My view is that the technology is here but that Americans are reluctant to adopt it. It's time to overcome our fears. It's time to get interested.

The American resistance to the Smart Card also came from the private sector, which was initially the only card issuer. It costs \$15 to produce a chip-bearing card versus 80 cents to issue a card without the security chip. Costs have now gone down dramatically.

Many new computer systems are being created with card reader technology. Older computers can add this feature for very little money.

These are relatively new issues to me -- and to most Americans. And while I certainly do not have all the answers, there are some things I *do* know after running a state for 11 years.

* **STATES must lead** --- I believe that the federal government cannot --- and will not --- be able to enact these changes in time to protect us adequately. STATES must forge partnerships with private enterprise and perhaps join with other states for wider reach.

* **States have more to do with establishing digital security standards than any other entity.** Therefore, you must think big while also focusing on inter-operability and flexibility.

* **States must work together to create a universal system to protect all Americans.** I want to applaud the work of the National Association of State Chief Information Officers, and encourage that organization to continue focusing on these critical issues. I also thank Carnegie Mellon for hosting the CERT Coordination Center, and for your fine work that serves as a resource for all of us "out there" at the state and local level.

* **Lastly, know that your work is urgently important.** I know --- as sure as I'm standing here --- that time is not on our side.

Cyber-terrorism could turn our economy upside down with more dangerous effectiveness than any violent act of which terrorists are now capable.

Thanks to you --- and others like you --- we have the means and the talent to accomplish our goals. The real question is whether we have the public **will** to act in time to matter.

Therefore, we must all accept the critical challenge of making the cyber threat real and immediate to Americans everywhere. We have a tremendous learning curve to conquer.

We live in a new world that we cannot allow to be more dangerous than brave -- in a world our Founding Fathers could never have imagined.

We must honor their vision --- not by allowing it to be hijacked ---

But by protecting it ... and extending it around the globe.

That is my call to action today.

I thank you for letting me share it...

... and above all, I thank you for being on the front lines.

Appendix II : Full Text of the Agenda

Workshop on States Security:

Identity, Authentication, Access Control

March 27-28, 2002
Carnegie Mellon University
Pittsburgh PA

Program Agenda

Wednesday, March 27, 2002

- 8:15** *Welcome*
Jared L. Cohon, President, Carnegie Mellon University
- 8:20** *Workshop Organization and Themes*
Robert Thibadeau, Principal Research Scientist, School of Computer Science,
Carnegie Mellon University
- 8:45** *Technologies for Identity Tokens*
Gilles Lisimaque, VP, Gemplus
- 9:30** *Introduction to Governor Dean*
Jared L. Cohon, President, Carnegie Mellon University
- 9:35** *Keynote*
Governor Howard Dean, Vermont
- 10:00** **Break**
- 10:15** *Managing Privacy and Identity - Issues at the State Level*
David Chaum, Privacy Technology Innovator
- 11:00** *Authentication and Access Control for Networks*
Jeremy Stieglitz, Group Product Manager,
Cisco's Identity Management Solutions
- 12:00 pm** *Introduction to Governor Schweiker*
Jared L. Cohon, President, Carnegie Mellon University
- 12:05** *Welcome to Pennsylvania*
Governor Mark Schweiker, Pennsylvania
- 12:30** **Lunch**
- 1:30** *CERT for the States? A CERT Perspective*
Richard D. Pethia, Director CERT Centers

- 2:45** *CERT for the States? General Discussion*
- 4:00** **Break**
- 4:10 – 4:30** *Risk Assessment in Large Scale PKI*
Don Beaver, Ph.D. Harvard, Cryptology, Security Architectures, Seagate Research
- 4:30 – 5:00** *International Security Trust and Privacy Association, Framework*
Michael Willett, Ph.D. UNC, Cryptology, Strategist, Wave Systems, Inc.
- 6:30 – 8:30** *Cocktails & Dinner, Wyndham Garden University Place*
Sponsored by AMS

Thursday, March 28, 2002

- 8:30** *Federal/State Relations*
Jeffrey Hunker, Dean, Heinz School of Public Policy
- 9:00** *Sustainable Computing*
Bill Scherlis, Principal Research Scientist, School of Computer Science
- 9:30** *PKI Practice: Addressing the Issues of Scale, Complexity, Interoperability*
Phillip Hallam-Baker FBCS C.Eng., Principal Scientist, VeriSign Inc.
- 10:15** **Break**
- 10:30** *NIST Security Initiatives*
Timothy Grance, Manager of Network Security Research, NIST
- 11:30** *Trusted Input Devices - Distributed Strong Authentication*
Lark Allen, Executive VP, Wave Systems
- 12:15 pm** **Lunch**
- 1:15** *State DMV as Interoperable Identity Credentials*
Jay Maxwell, President COO, AAMVAnet
- 2:15** *Framework for Non-repudiation*
Gary Daemer, Senior Principal, AMS Center for Advanced Technologies
Identity Credential Authentication
Bruce Monk, President and COO, AssureTec Systems, Inc.
Enterprise Identification Objectives
Barry Goleman, AMS
- 3:00 – 3:30** *Hard Problems and Next Steps*
William Scherlis and Robert Thibadeau, Principal Research Scientists,
School of Computer Science, Carnegie Mellon University

Appendix III: Roster of Participants

Please note that the white paper is the work product of the authors who have attempted to represent consensus views. However, individuals and organizations below may disagree with any and all of the substance and content in the white paper.

1. Allen,Lark,Executive Vice President,Wave Systems Corp.
2. Apt,Jay,Distinguished Service Professor,Carnegie Mellon University
3. Arunachalam,V.,Distinguished Service Professor,Carnegie Mellon University
4. Barkeloo,Jason,Director of Research and Development,ACEtek Research
5. Beaver,Donald,Research Staff Member,Seagate Research
6. Bhagavatula,Vijayakumar,Professor,Carnegie Mellon University
7. Blair,Mary Ann,Director, Administrative Computing,Carnegie Mellon University
8. Bourgein ,John,CEO,"Location Dynamics, Inc."
9. Brinker,Rex,IA Project Manager,CERT/CC - Software Engineering Institute
10. Buntz,Robert,Consultant,Office for Information Technology
11. Camden,Tom,"Director, StatePointPlus Technology",Westinghouse Electric Co.
12. Chaum,David,Privacy Consultant,"Chaum, LLC"
13. Chu,Yang-hua,Graduate Student,Carnegie Mellon University
14. Cohon,Jared ,President,Carnegie Mellon University
15. Connelly,Anita,,Carnegie Mellon University
16. Daemer,Gary,Senior Principal,AMS Center for Advanced Technologies
17. Dean,Howard,Governor,State of Vermont
18. DeBroff,Hilary ,VP Marketing and Communications,"Bright Plaza, Inc."
19. Eppinger,Jeffrey,Senior Systems Scientist,Carnegie Mellon University
20. Foley,John,President,VigilantMinds Inc
21. Goleman,Barry,Vice President,AMS
22. Grance,Timothy,Manager, Systems and Network Security Group,National Institute of Technology and Standards
23. Hallam-Baker,Phillip ,Principal Scientist,VeriSign Inc.
24. Harrison,John,Associate Computer Scientist,RAND
25. Higgins,Helen,,Carnegie Mellon University
26. Hunker,Jeffrey,"Dean, Heinz School of Public Policy",Carnegie Mellon University
27. Johnson,Kevin,CERT Support Specialist,North Central Information Operations Center
28. Keating ,Wick,Vice President,AMS
29. Keton,James,CEO,Palladin Inc.
30. Khalaf,James,Director of Advanced Technology,Rainbow Technologies
31. Lisimaque,Gilles,Senior Vice President,Gemplus
32. Maxwell,Jay,President & COO,"AAMVAnet, Inc."
33. McCarthy,Michael,Senior Lecturer,Carnegie Mellon University
34. Monk,Bruce,President and COO,AssureTec Systems Inc.
35. Moore,Maryann,Assistant Vice President for Relationship Marketing,Carnegie Mellon University
36. Nace,William,PhD Candidate,ISRI, Carnegie Mellon University
37. Nicolai,Frank,Executive Vice President,AMS
38. Owens,Dawn,Contracts Specialist,CMU Software Engineering Institute
39. Padman,Rema,Associate Professor,"The Heinz School, CMU"
40. Peha,Jon,Associate Director, Center for Wireless and Broadband Networks,Carnegie Mellon University
41. Pethia,Richard,"Director, Networked Systems Survivability Program",Carnegie Mellon University
42. Regan,Rock,CIO,"State of Connecticut, National Chairman of NASCIO"
43. Root,Nathan,Standards Program Director,AAMVA
44. Sadeh,Norman,Associate Professor,Carnegie Mellon University
45. Sanders,Joseph,,Department of Motor Vehicles - State of New York
46. Scherlis,William,Principal Research Scientist, School of Computer Science,Carnegie Mellon

- University
47. Schweiker, Mark, Governor, State of Pennsylvania
 48. Shaw, Mary, AJ Perlis Professor of Computer Science, Carnegie Mellon University
 49. Shovlin, Peter, InterTECH Security LLC
 50. Sibert, Olin, Founder, Silicon Keep, LLC
 51. Siegel, Mel, Senior Research Scientist, Carnegie Mellon University
 52. Skalko, Ed, Director of Exploratory Technology, Seagate Technology
 53. Sprague, Peter, Chairman, Wave Systems Corp.
 54. Sprague, Steven, President & CEO, Wave Systems Corp.
 55. Stephan, Edgar, C.T.O., Tempest Computers
 56. Stieglitz, Jeremy, Group Product Manager, Cisco's Identity Management Solutions, Cisco Systems
 57. Sweeney, Latanya, Assistant Professor of Computer Science & Public Policy, Carnegie Mellon University
 58. Thibadeau, Robert, Principal Research Scientist, School of Computer Science, Carnegie Mellon University
 59. Townsend, Tahlia, Carnegie Mellon University
 60. Turner, Paul, Chief Technology Officer, AMS
 61. Veil, Len, CTO, Wave Systems Corp.
 62. Wells, Harry, Managing Director, Winslow Asset Management
 63. Willett, Michael, Security Architect, Wave Systems
 64. Zobel, Rosalie, Director of European E-Commerce Program, European Commission