



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

### Organization and Themes

[www.security.scs.cmu.edu](http://www.security.scs.cmu.edu)

Bob Thibadeau  
School of Computer Science  
rht@cs.cmu.edu



## Workshop Format

- **Technical Know-How**
- **Hard Problems**
  - Security is always a *delicate* combination of
    - » Practice/Policy/Law/Forensics/Enforcement
    - » Technology/Know-How
- **White Paper and Video**



## Sponsors

- **AMS, Inc.**

**\$1 billion international business and information technology consulting firm**

**customers include 43 state and provincial governments, most federal agencies, and hundreds of companies in the Fortune 500.**

- **Wave Systems, Inc.**

**The leading designer and developer of platforms, infrastructure and services**

**that enable trusted, secure and reliable relationships, digital exchange and commerce over the Internet.**



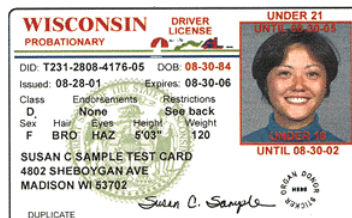
## Grounding -- facilitation --

- **A CERT for States**

- That Friendly Phone Call about a problem ...
- What should a CERT for States be?

- **Interoperable Driver's Licenses**

- Re: New York Times 3/21/02 article Boston Bar Scanning DLs: Privacy?
- How do we secure a system so it becomes difficult to misuse?



## CERT Computer Emergency Response Team



- Study Internet Security Vulnerabilities
- Handle Incidents
- Publish Security Alerts
- Research long-term changes in networked systems.
- Develop Information and Training to improve security on your site.
  
- Work With You and With Vendors to facilitate the best solutions possible.

Robert Thibadeau, Copyright 2002

5

## CERT for States



- 63 Valid Drivers Licenses for 19 Terrorists : We need to tie systems together somehow.
  
- Tens of Thousands of State and Local Gov't Web Sites (and other exposure points).
  
- E.g., Data Storage so only authorized users have access to authenticated data.

Robert Thibadeau, Copyright 2002

6



## Grounding in Interoperable Drivers Licenses

- Consider a How-To Straw Man
- To Solve the Hard Problem : Security Versus Personal Privacy

Robert Thibadeau, Copyright 2002

7



## Strawsylvania

**Accepted to Idealized Statehood : 2020**

**Population : 20,000,000**

**Gov't Web Sites : 30,000**

**Drivers : 14,000,000**

**Innocent Hackers (includes kids and people just making mistakes) : 500,000**

**CyberCrooks, Terrorists, and Intentionally Evil Hackers : 200**

Robert Thibadeau, Copyright 2002

8

## The Driver's License from Strawsylvania



The License is **Information**

that

Asserts the explicit License

Authenticates an individual (biometrics)

Can't be altered (tamperproof)

Can't be counterfeited (provably authorized)

Manifestation (need not be 'just a card')

Physical:

Individual : Smart Card, a computer terminal, ring ...

Reader/Verifier : Black Box, Computer terminal ...

Signal: Wired, Wireless (Proximity)

Robert Thibadeau, Copyright 2002

9

## Strawsylvania Authenticates People by



- **What you have** : A token that holds the certificate that is a provably authorized token.
- **What you are** : Biometric proof that the holder of the token is the right holder
- **What you know** : Questions that can be asked that you should be able to answer.

Robert Thibadeau, Copyright 2002

10



## Strawsylvania uses Biometrics

- **Digital Picture**
  - Includes Face Features for Automatic Recognition
- **Fingerprint**
  - Includes Fingerprint Features for Automatic Recognition
- **Voice Verification**
  - Includes Voice Features for Automatic Recognition
- **DNA**
  - Includes Features for Forensics

Robert Thibadeau, Copyright 2002

11



## Strawsylvania uses Public Key Technology

- **Public Key Infrastructure**
- **What is Public Key? (Tamperproofed, Non-Counterfeitable, & Authorized Licenses)**
  - One Key Marks it
  - One Key Reveals.
  - Make One Key Public
  - To Assure All Your Deals!
- **Hierarchical**
  - Nation
    - » State 1
      - Person 1
        - » License
      - Person 2 ..
    - » State 2 ..

Robert Thibadeau, Copyright 2002

12

## Strawsylvania is Interoperable and Privacy Preserving



- **Only authorized, role-based, inquiries of Drivers License Information are possible**
  - DMV : Only Agent that can Change License Information
  - Police
  - National Data Center
  - Public
- **Only limited information is available for inquiry by a specific inquirer**
  - Yes/No : This is his fingerprint, this is his face
  - Public : Yes/No : He is over 21/18/16
  - Police : This is his Age
  - National Data Center : Yes/No This License is Valid in the State of Strawsylvania, USA

Robert Thibadeau, Copyright 2002

13

## Uses



- **Bar**
  - Can ask Drivers License if this person is old enough and see a picture of his/her face. That's all.
- **Check Cashing/Ticket Buying**
  - Card Confirms a name, address, a 'public DL Number' and shows a picture. That's all.
- **Airport/Other Security**
  - Card provides forensic record pointer (DL Number and State, Recognition and Picture). That's all.
- **Extended : Voting Card**
  - Can see picture of face and test fingerprint with yes/no as to correct voting precinct and anonymized voter ID Number. That's all.

Robert Thibadeau, Copyright 2002

14



## Extended Uses : Smart Car

Car reads the radio signals of your license, figures that is good enough, and starts.

- **Privacy: Car is not authorized for further information**
- **Car tells Drivers License what Drivers can Drive it, and Driver's License proves it is held by one of these Drivers but never discloses persons name or other personally identifiable information.**
- **Car buying sets master Driver's License**
- **Parking Attendant Button (on/off only by Licensed Driver)**



## Uses : Police

- **Car Reveals Licensed Occupants from Safety of Police Car**
  - Police Station gets Forensic Quality Data
  - Policeman Gets Data Necessary only to Him
- **Policeman can ask where the car has just been with the present driver?**

## Strawsylvania Smart License



### Information Available

Authority	DL #	Name	Picture	Face Recog	Yes/No Valid	Finger Print	Age
DMV	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Police - Beat	No	Yes	Yes	No	Yes	No	Yes
Car	No	No	No	No	Yes	No	No
Bar	No	No	Yes	No	Yes	No	Yes +21
Tickets & Check Cash	Yes	Yes	Yes	No	Yes	No	No
Security Check Point	Yes	Yes	Yes	Yes	Yes	Yes	No

Robert Thibadeau, Copyright 2002

17

## Managing the Interoperable Drivers License Infrastructure



- A CERT for States?
- Acting as a resource to keep this system reliably functioning and secure.

Robert Thibadeau, Copyright 2002

18



## Back to Kansas!

There's no place like home!

## Agenda - Wednesday



1. 8:45 *Technologies for Identity Tokens* Gilles Lisimaque, VP, Gemplus
2. 9:30 *Introduction to Governor Dean* Jared L. Cohon, President, Carnegie Mellon University
3. 9:35 *Keynote* Governor Howard Dean, Vermont
4. 10:00 Break
5. 10:15 *Managing Privacy and Identity - Issues at the State Level* David Chaum, Privacy Technology Innovator
6. 11:00 *Authentication and Access Control for Networks* Jeremy Stieglitz, Group Product Manager, Cisco's Identity Management Solutions
7. 12:00 pm *Introduction to Governor Schweiker* Jared L. Cohon
8. 12:05 *Welcome to Pennsylvania* Governor Mark Schweiker, Pennsylvania
9. 12:30 Lunch
10. 1:30 *CERT for the States? A CERT Perspective* Richard D. Pethia, Director CERT Centers
11. 2:45 *CERT for the States?* PANEL
12. 4:00 Break
13. 4:15 – 5:00 *Risk Analysis* Don Beaver, Ph.D. Harvard, Cryptologist, Security Architectures, Seagate Research
14. 6:30 – 8:30 *Cocktails & Dinner, Wyndham Garden University Place* Sponsored by AMS

## Agenda - Wednesday



1. 7:30 am Continental Breakfast
  2. 8:30 *Federal/State Relations* Jeffrey Hunker, Dean, Heinz School of Public Policy\
  3. 9:00 *Sustainable Computing* Bill Scherlis, Principal Research Scientist, School of Computer Science
  4. 9:30 *PKI Practice: Addressing the Issues of Scale, Complexity, Interoperability* Phillip Hallam-Baker  
FBCS C.Eng., Principal Scientist, VeriSign Inc.
  5. 10:15 Break
  6. 10:30 *NIST Security Initiatives* Timothy Grance, Manager of Network Security Research, NIST
  7. 11:30 *Trusted Input Devices - Distributed Strong Authentication* Lark Allen, Executive VP, Wave  
Systems
  8. 12:15 pm Lunch
  9. 1:15 *State DMV as Interoperable Identity Credentials* Jay Maxwell, President COO, AAMVAnet
  10. 2:15 *Framework for Non-repudiation* Gary Daemer, Senior Principal, AMS Center for Advanced  
Technologies
  11. *Identity Credential Authentication* Bruce Monk, President and COO, AssureTec Systems, Inc
  12. *Enterprise Identification Objectives* Barry Goleman, AMS
- 3:00 – 3:30 *Hard Problems and Next Steps* William Scherlis and Bob Thibadeau

Onward to Gilles!

