

Identity, Privacy & Security

Michael Pomerleau

State of Maine

Office of Information Technology

Policy & Strategic Planning

Identity, Privacy & Security

- The digital age has brought about a level of convenience and access to services that were never before imagined.
- Unfortunately, it has also opened the door to a whole new set of challenges in privacy and confidentiality, including identity theft and identity fraud.
- What is the responsibility of government in safeguarding confidential information?
- What other Internet policy issues must be confronted?

The Global Threat

- Information security is not just a paperwork drill...
- There are dangerous adversaries out there capable of launching serious attacks on our information systems that can result in severe or catastrophic damage to the nation's critical information infrastructure and ultimately threaten our economic and national security...

Very Threatening World for IT

- Internet, broadband & wireless make connectivity easier and expose IT systems
- Identity & data theft via phishing are replacing spam as our prime security concern
- Threats and known vulnerabilities to IT systems are increasing
- Security incidents involving our systems, our partners and our neighbors are occurring more frequently

Balance Greater Access & Security

- IT is essential to providing nearly all government services across all branches of government - Federal, State, & local
- Re-balance Confidentiality and Integrity against Availability
 - Availability currently outweighs security
- Federal & State regulations are requiring more secure IT systems

Key Security Principals

- Data Classification is an underlying principal for all security activities
- VALUE - What do I need to protect?
- RISK - What is the exposure to the loss?
- VULNERABILITY - What are my security weaknesses?
- THREAT - What is the likely-hood?

Evaluate Security Risks

- Business owners must be involved
- Risk assessment is fundamental
- Only data owners can assess the true value of their data assets
 - Social security numbers and credit card information are extremely high-value targets for identity theft
 - All personal information has value

Managing Enterprise Risk

- Key activities in managing enterprise-level risk resulting from the operation of an information system:
 - Categorize the information system (criticality/sensitivity)
 - Select and tailor minimum (baseline) security controls
 - Supplement the security controls based on risk assessment
 - Document security controls in system security plan
 - Implement the security controls in the information system
 - Assess the security controls for effectiveness
 - Determine agency-level risk and risk acceptability
 - Authorize information system operation
 - Monitor security controls on a continuous basis

Vulnerabilities

- To servers and other network devices
 - Unnecessary services left active
 - Unnecessary privilege levels granted
 - Default profiles in use
- To applications and databases
 - Vulnerabilities to automated and manual hacking, including SQL injections and buffer overflows
- Via social engineering
 - Compromised systems can include data that can be used to further exploit the environment

Security Bad & Good News

- Data breach is the sum of all vulnerabilities
- Defenses against existing and future threats are defenses against data breach vulnerabilities
- OIT staff are already engaged in providing a network of interlocking strategies to reduce risk
- Harden servers + examine application code + educate staff on good security practices =
Reduced risk of data breach

Maine Defines "security breach"

- Unauthorized acquisition of an individual's computerized data that compromises security, confidentiality or integrity of personal information of the individual
- Maintained by an individual, partnership, corporation, limited liability company, trust, estate, cooperative, association or other entity, including agencies of State Government, and colleges and universities
- Attorney General Office will take measures to inform affected parties, so they can take steps to protect their identities
- If more than one thousand accounts are affected, the Attorney General Office will also give notice to credit reporting agencies

Consequences of Security Breaches

- Costs to Businesses & individuals:
 - Lost productivity
 - Legal
 - Financial
 - Public relations

We Have Skills & Resources

- We have talented people who are protecting our data on state enterprise systems
- We have systems and processes available
- IT partners have tools to assist us
- IT industry has experience to help us deliver
- We need to make IT Security a priority goal

So, Why Aren't We Secure?

- Culture of operational expediency has put planning, risk management, sound policies and procedures on back burner (OPEGA)
- Written policies and procedures are either non-existent, inadequate or inconsistent across Executive branch in a number of IT areas (OEGA)
- Security was not a priority

The Challenge is Employing Appropriate Security Consistently

- Use IT security policies, standards and best practices
- Use IT automation to employ a consistent security configuration to applications, network infrastructure, servers and clients
- Use IT tools to self assess and report security status
- Audit & validate security compliance

Trade-offs - Disciplined Security & Outsourcing Efficiencies

- Security must be extended to include outsourcers and interfaces with networks that are managed by others
- Federal government imposes strict regulations & procedures for sharing data with states
 - FBI, IRS, FDA, FDIC, Medicare & Medicaid (HIPA) = Security requirements for sharing information
- State governments must require vendors & business partners to implement strong security practices

Federal Information Security Management Act (FISMA)

- Protecting the Nation's Critical Information Infrastructure
- Standards for categorizing information and information systems by mission impact.
- Standards for minimum security requirements for information and information systems.
- Guidance for selecting appropriate security controls for information systems.
- Guidance for assessing security controls in information systems and determining security control effectiveness
- Guidance for certifying and accrediting information systems.

Secure Configuration Settings

- *The linkage between security controls and the information system...*
- Configuration settings are critically important in the implementation of selected security controls to ensure the full security capability of the controls can be obtained.
- Mandatory configuration settings, agency established and agency enforced, are a key provision of FISMA.

US Gov Protection of Sensitive Information - OMB Directive June 2006

- Encrypt all data on mobile computers/devices
- Allow remote access only with two-factor authentication
- Use a “time-out” function for remote access and mobile devices requiring user re-authentication after 30 minutes inactivity
- Log all computer-readable data extracts from databases holding sensitive information
 - Verify each extract including sensitive data has been erased within 90 days

The REAL ID Act

- REAL ID Act of 2005 stipulates that after May 11, 2008, "a Federal agency may not accept, for any official purpose, a driver's license or identification card issued by a State to any person unless the State is meeting the requirements" specified in the REAL ID Act

The Maine Notice of Risk to Personal Data Act (PL 583 1/31/2007)

- Expands the existing requirement that information brokers notify consumers of a security breach of personal information to apply to a broader range of persons and businesses including colleges, universities and state government
- State Employees - If you become aware of a security breach of the information you are maintaining, or suspect the potential of it being lost or misused, you are required to notify your agency's leadership.
- Creates a private cause of action for certain violations of the requirement to notify consumers.

Maine Defines “personal information”

- An individual's first name, or first initial, and last name in combination with anyone or more of the following data elements, when either the name or the data elements are not encrypted or redacted:
 - Social security number;
 - Driver's license number or state identification card number;
 - Account number, credit card number or debit card number, if circumstances exist wherein such a number could be used without additional identifying information, access codes or passwords;
 - Account passwords or personal identification numbers or other access codes

Maine IT Application Certification Policy

- Applications must not allow unauthorized access, or compromise data or workflow
- All personal, medical and financial data, in motion, must be encrypted end-to-end, inside and outside the State firewall
- Data resident in portable computing devices must be encrypted
- Full vulnerability assessment and penetration tests:
 - Must be performed on the application, including all relevant client devices, and web, application & database servers
 - Testing includes: hardware & software configurations + password cracking + auditing + integrity checks + buffer overflow, cross-site scripting, and denial of service tests
- All applications enforce standard best practices

Maine OIT Enterprise Security

- Multi-layered Check Point Firewall
- Intrusion Prevention System
- Managed routers & networks (WebNM)
- Email Anti-Virus & Spam control
- Managed desktop & server Anti-Virus
- Enterprise vulnerability patch system
- Remote Access via SecurID
- Secure Wireless networking

Maine OIT Enterprise Initiatives

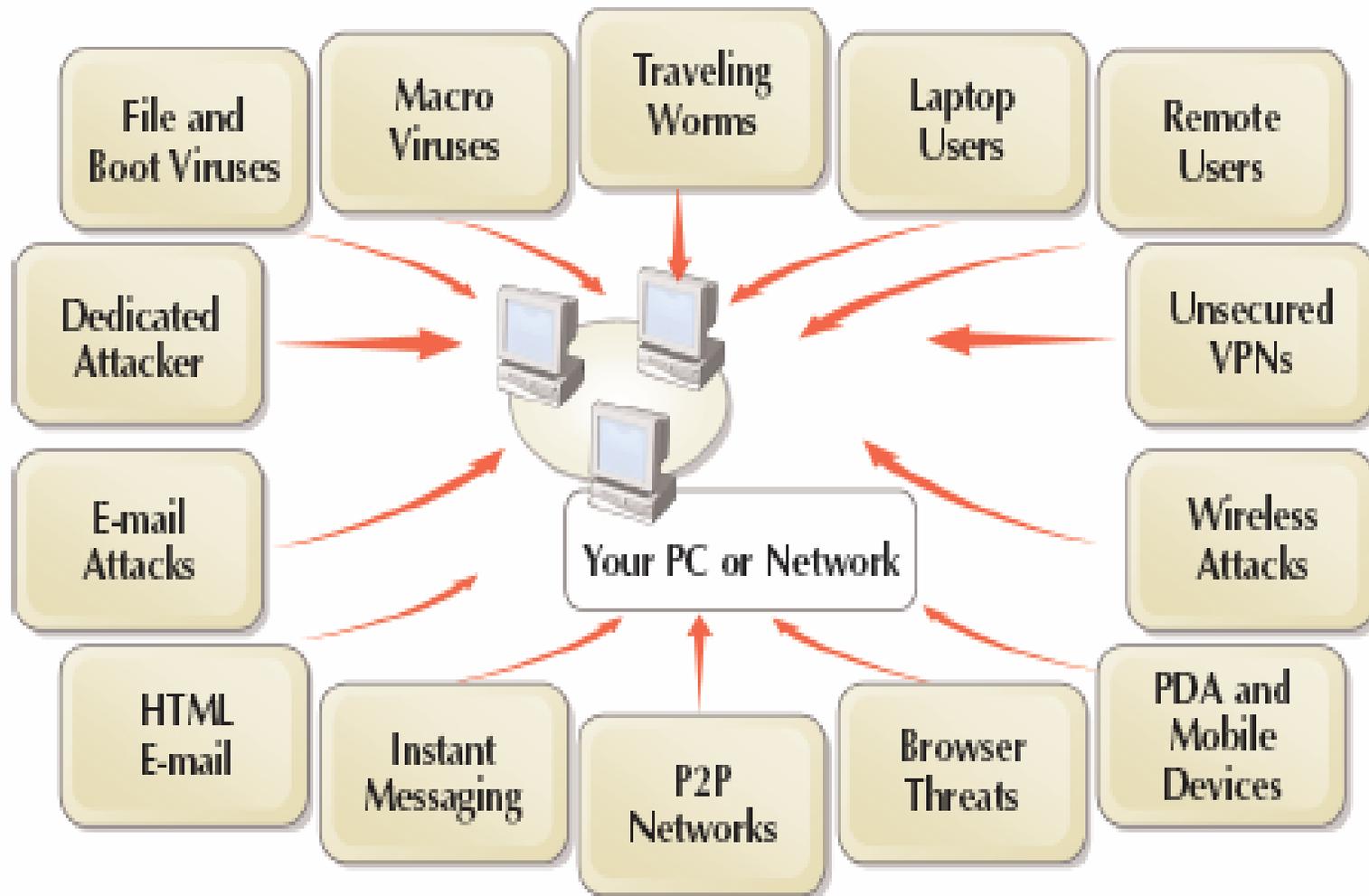
- State Certificate Services & Identity Mgmt PKI
- Enterprise Security Policy
- Secure single sign-on w/password recovery
- Enterprise data backup
 - disaster recovery & archival
- Records management system
- Single Active Directory to manage PCs
- Consolidate file servers
- DHCP, DNS, Radius & LDAP services

Certificates Help Provide Security

- Secure e-mail - encryption & digital signatures
- Secure Web sites - minimize spoofing
- Secure Web & FTP communications - encryption
- Custom security solutions for applications - authentication, confidentiality, integrity, & non-repudiation
- Identity management (Smart card)
- Secure logons - biometrics Network layer encryption - Internet Protocol Security (IPSec)
- 802.1x wireless encryption - WPA & 802.11i
- Encrypting File System (EFS) - protect data (Laptops, PCs, Servers)
- Software code signing - Trojans & spyware prevention

Threats to PCs and Networks

Potential attack vectors



Operating System & Application Exploits

- Microsoft Windows & Internet Explorer
- Email exploits - SPAM & malicious mail
- Malicious web sites
- Instant messaging
- File sharing & downloads
- Remote access threats
- FTP & Telnet, no protection credentials & data

Information Worker Security

- Information workers depend on computers
- Networking & the Internet has connected us to the world
- Peer-to-peer or workgroup networking isn't secure enough by itself to protect us from the world
- Most of us are aware of risks in using a networked computer - viruses & malicious code, intrusions, and hacking.
- Unfortunately individual computer users do not know how to consistently protect themselves.

Help Safeguard Your Personal Information Online

- Phishing attacks
 - Luring someone to a spoofed Web site
- Spoofing attacks
 - Spoofed site is usually designed to look like the legitimate site, using components from the real site
- Always verify the security certificate issued to a site before submitting personal information
- Secure site lock icon
 - Double-click the lock icon to display the security certificate
 - Issued to should match the site you think you are on

From: Billing@walmart.com
To: mindyp@fairpoint.net
Cc:
Subject: IMPORTANT: Online WALMART survey! Important for you!

Sent: Wed 9/27/2006 3:07 AM



Dear Customer,

CONGRATUALIONS!!

You have been chosen by WAL*MART online department to take part in our quick and easy 5 question survey.

In return we will send \$35 to your confirmed Credit Card - Just for your time!

This survey has been sent only to a few people from our random generator!

Helping us better to understand how our customers feel, benefits everyone. With the information collected we can decide to direct a number of changes to improve and expand our online services.

This information you provide to us is all non-sensitive and anonymous - No part of it is handed down to any third party groups.

We kindly ask you to spare two minutes of your time in taking part with this unique offer!

To Continue click on the link below:

<https://www.walmart.com/cservice/survey?customersurvey=546>

<http://www.revo-gilde.de/walmart/>

Sincerely,
Wal*Mart Online Service

Official State of Maine Web Site?

Welcome MOSES - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Refresh Print Mail Stop

Address <https://www.informe.me.uk/moses/> Go Links



Welcome to MOSES

MOSES is the Maine Department of Inland Fisheries and Wildlife's online hunting & fishing licensing system. With MOSES, you can purchase licenses any time of the day or night, and print your license out in your home or office in just minutes.

Here's what you need to know before getting started:

- Licenses are delivered by email, so be very careful when entering your email address, to ensure you receive your license.
- Visa, MasterCard and Discover are accepted.
- Lifetime and Complimentary licenses are not available online at this time.

Begin by selecting your status and then the item you wish to purchase.

Please Select:

This is my first time buying a license online through MOSES

A. I am a repeat user of the MOSES online system

What would you like to purchase? Select one:

B.



Hunting/Fishing Combo Fishing License Hunting License

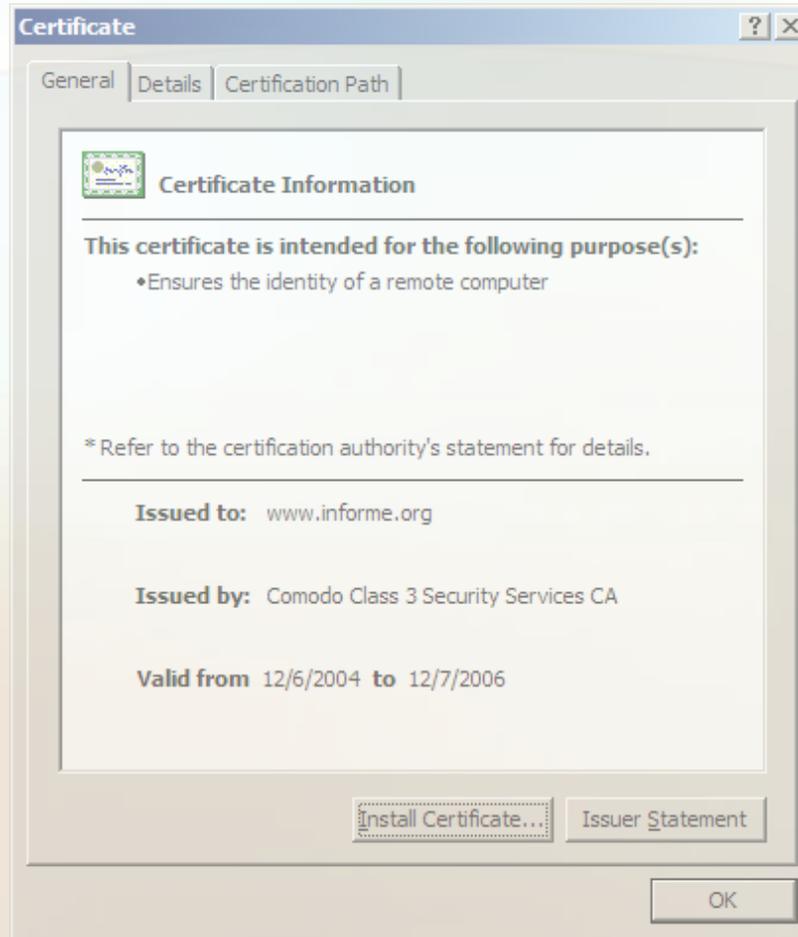
Done

Internet

Start | The Dell Online Store: Bu... | Techbargains.com - Buy ... | Welcome MOSES - Mic... | Microsoft PowerPoint - [...]

10:16 PM

Official State of Maine Certificate?



Problems with Web Site Certificates

Security Alert [X]

 Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

- The security certificate is from a trusted certifying authority.
-  The security certificate has expired or is not yet valid
-  The name on the security certificate is invalid or does not match the name of the site

Do you want to proceed?

Security Alert [X]

 Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

-  The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.
- The security certificate date is valid.
- The security certificate has a valid name matching the name of the page you are trying to view.

Do you want to proceed?

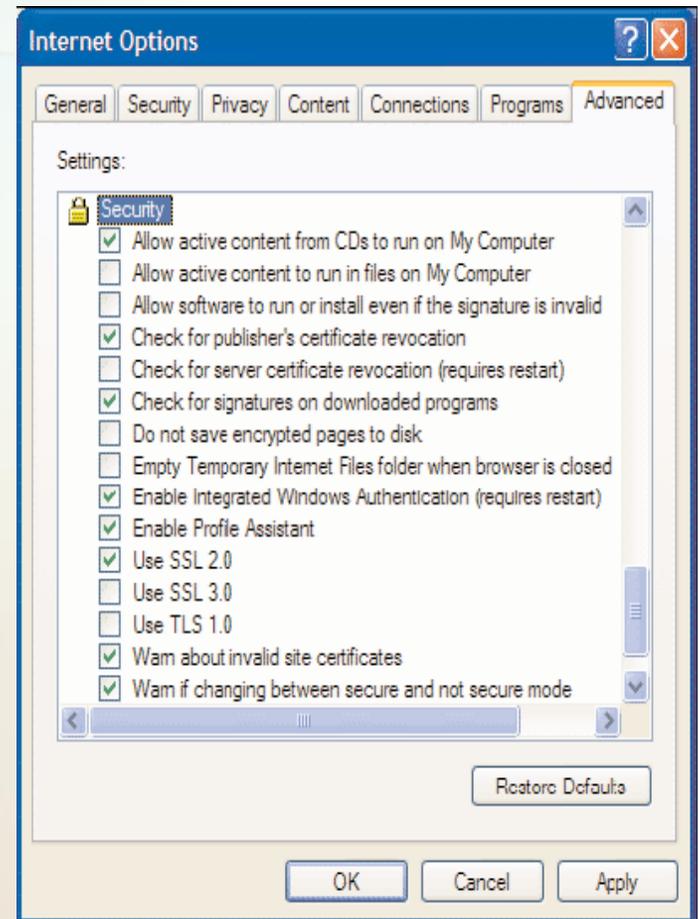
Secure Socket Layer & Transport Layer Security (SSL & TLS)

SSL with Mutual Authentication (TLS) allows a user to authenticate to the server using a certificate and private key.

TLS a.k.a. Client Authenticated SSL

Due to the vulnerabilities inherent in SSL 2.0, the only reasonable protocols to consider for deploying transport layer security are SSL 3.0 or TLS 1.0.

Because SSL 3.0 is not approved for use in the protection of Federal information, (Section 7.1 of [FIPS140Impl]), TLS must be properly configured to ensure that the negotiation and use of SSL 3.0 never occurs when Federal information is to be protected



Maine State Government Needs a Consistent Integrated Approach to IT Security Services

- Educate a combined State business & IT management team
- Collect business requirements
- Guide the strategy
- Help IT select the appropriate approach
- Use the resulting security services