



# Security in Mac OS X

John Hurley, Ph.D.

Manager, Data Security

Apple Computer, Inc.



# Introduction

- ◆ Mac OS X is a great platform to implement security features on
- ◆ Apple is in a unique position for security
- ◆ We have some great features to help developers implement their security solutions
- ◆ Configurability gives us some exciting off-the-shelf possibilities



# Contents

- ◆ Overview of OS X
- ◆ Darwin Kernel
- ◆ Open Source
- ◆ Keychain
- ◆ Authorization
- ◆ CDSA
- ◆ Smartcards
- ◆ NIST Security APIs
- ◆ [STOS] Consortium
- ◆ More resources



# Overview of Mac OS X

- ◆ New Apple OS based on BSD Unix & Mach
- ◆ Great graphical user interface
- ◆ Version 10.0 shipped 3.24.01
- ◆ Now shipping with all Macintoshes
- ◆ Don't think UNIX think Mac OS X



# Mac OS X Components

- ◆ Aqua    new look
- ◆ Classic/Java/Carbon/Cocoa
- ◆ Quartz/OpenGL/QuickTime
- ◆ BSD Kernel
  - File system, networking, POSIX
- ◆ Mach Kernel
  - IOKit & Drivers, tasks, threads, memory



# Mac OS X Opportunities

- ◆ Protected memory
- ◆ Multitasking
- ◆ BSD infrastructure
- ◆ Fresh start
- ◆ Draw on open source movement



# The Darwin Kernel

- ◆ BSD sits on top
  - File system layer
  - Network stack
  - POSIX functionality
- ◆ I/O Kit owns the driver model
- ◆ Mach sits underneath
  - Tasks and threads
  - Memory
  - Manages the processor



# BSD Kernel

- ◆ Based on BSD 4.4
- ◆ Integrated with Mach and I/O Kit
- ◆ Provides OS Personality APIs and Services
  - Process model
  - Basic security policy
  - File system architecture
  - Networking architecture



# Security Policy

- ◆ Users
- ◆ Super user vs. everyone else
- ◆ File system access
  - Users
  - Groups
- ◆ Not capabilities based
- ◆ Examining Mandatory Access Controls (MAC)



# Core OS Security

- ◆ Mac OS X ships with most services off
- ◆ Root account disabled by default but can be re-enabled
- ◆ File permissions are designed to work with Mac OS 9
- ◆ UNIX security knowledge is helpful



# Open Source

- ◆ We are open sourcing many components of the Apple Data Security Architecture!
- ◆ All subprojects of Security.framework
- ◆ Allows for peer review
- ◆ Easier export compliance
- ◆ We value your contributions



# Open Source Components

- ◆ Sub-projects of Security.framework:
  - Authorization, SecureTransport, Keychain and SecurityServer
- ◆ Default plugin modules and utility frameworks
  - AppleDL (DL), AppleCSP (CSP), AppleCSPDL (CSP/DL), AppleX509CL (CL), AppleX509TP (TP), SecuritySNACCRuntime, SecurityASN1, and cdsa\_utilities



# Keychain

- ◆ Every user on Mac OS X has a Keychain
- ◆ Unlocked with login password
- ◆ If you need to save a password somewhere, use the Keychain!
- ◆ Usually totally transparent to users
- ◆ Available through Carbon



# Authorization API

- ◆ Authorization vs. Authentication

- Authorization is yes/no for operation

- Do I have the ability to do something?

- ◆ Authentication

- May establish identity

- Who you are, what you know, what you have

- Optionally produces some sideband info

- May succeed trivially



## Authorization API (Cont.)

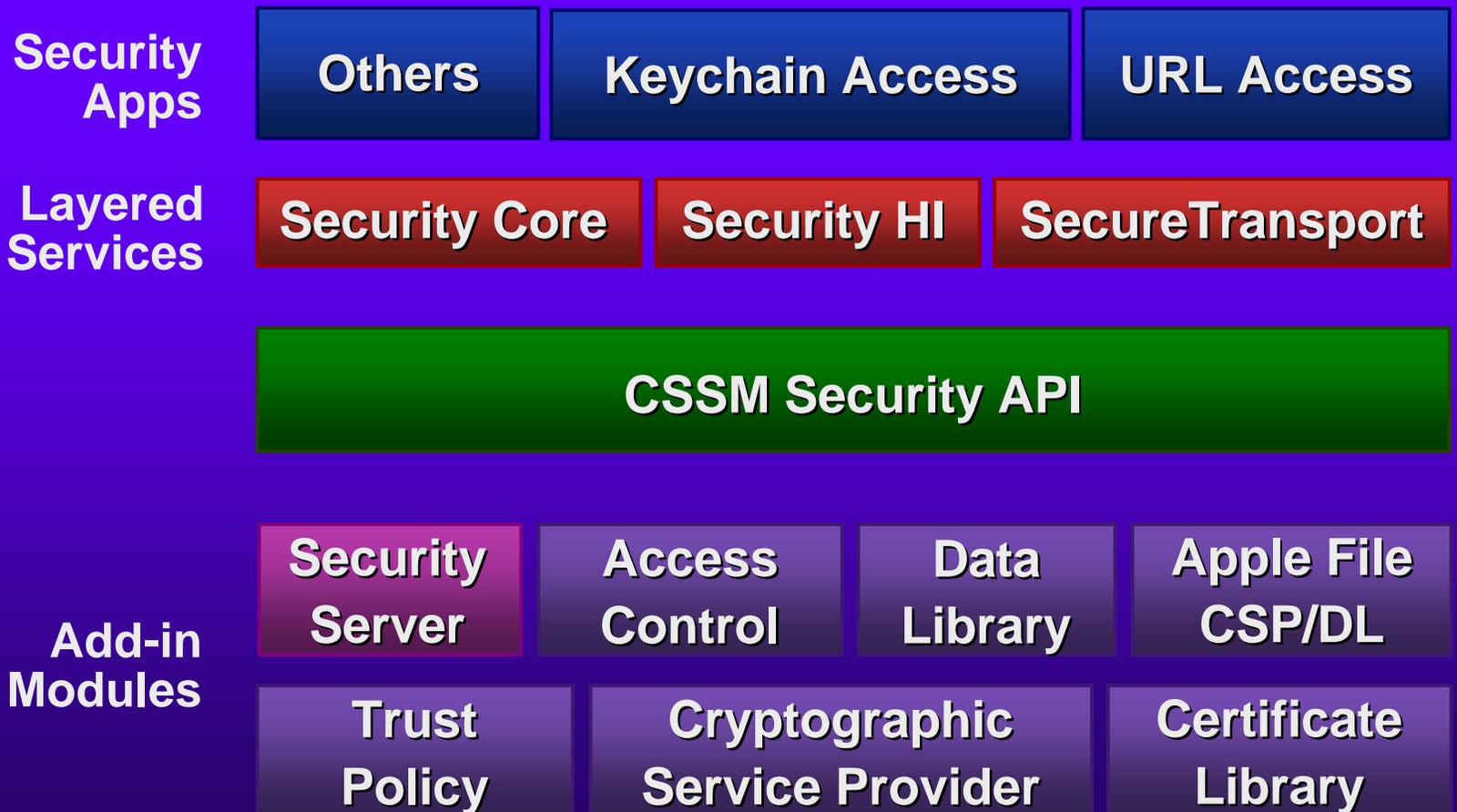
- ◆ Operation: log in at console
  - Authentication steps could include:
    - Type user name and password
    - Insert smartcard
    - Fingerprint
    - Voice recognition
- ◆ Examples of operations
  - Unlock screensaver
  - Play a CD
  - Format a disk



# CDSA

- ◆ Common Data Security Architecture
- ◆ OpenGroup standard
- ◆ Uses plugin modules
  - Data Library (DL)
  - Cryptographic Service Provider (CSP)
  - Certificate Library (CL)
  - Trust Policy (TP)

# Apple Security Architecture





# Data Library Modules (DLs)

- ◆ Store information used by other CDSA modules
- ◆ Apple File CSP/DL
  - A combination CSP/DL (encrypts and stores)
  - Keychains are flat files maintained by this CSP/DL
- ◆ Other Examples
  - LDAP DL



# Certificate Library Modules (CLs)

- ◆ Interpret public key certificates
- ◆ Examples
  - Apple CL interprets X.509 v3 certificates
  - PGP CL
  - Attribute CL



# Trust Policy Modules (TPs)

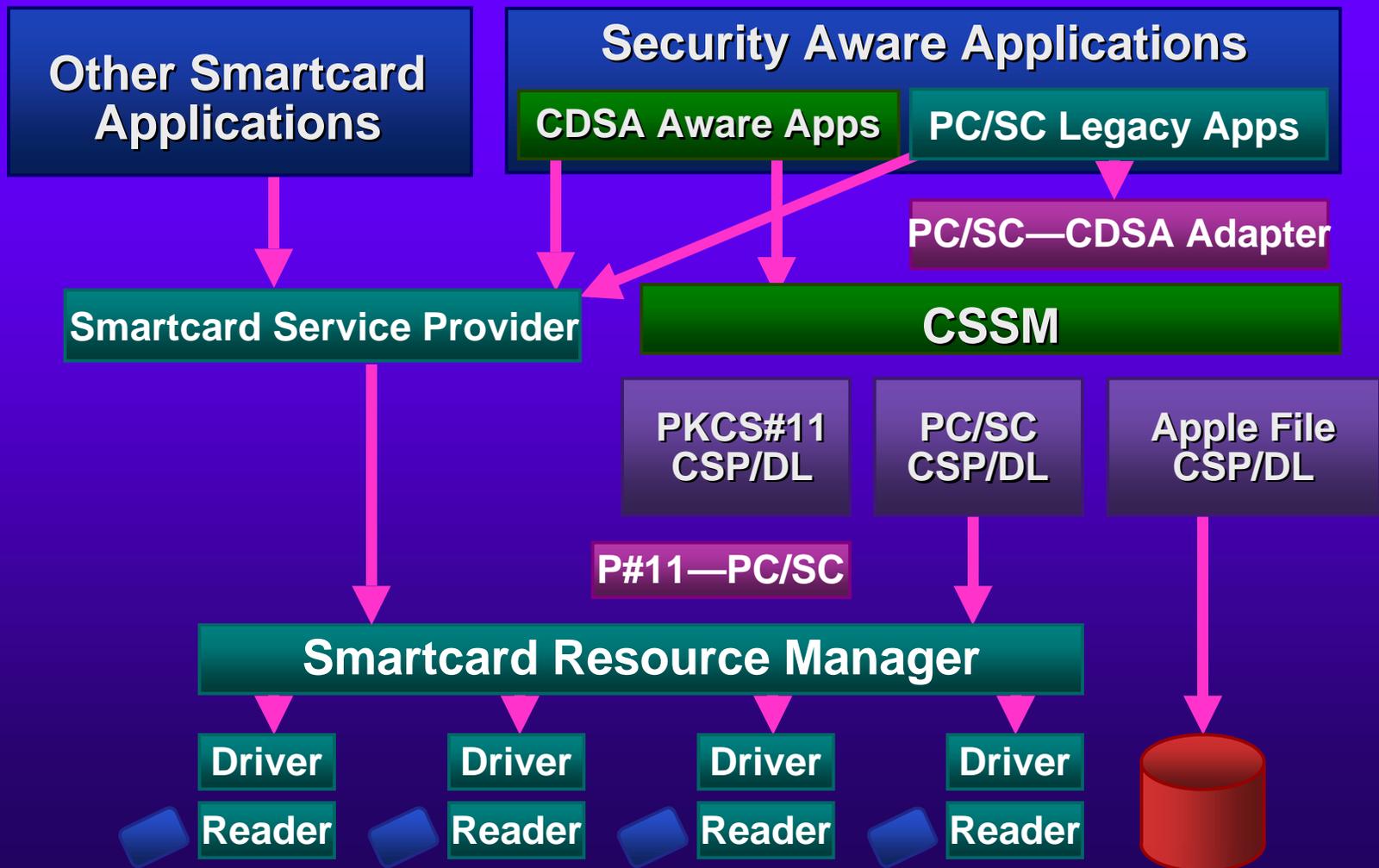
- ◆ Encapsulate how certificates should be evaluated for trust decisions
- ◆ Examples
  - A corporate TP could reject any certificate chain that did not contain the corporate certificate in the chain
  - Could implement web-of-trust instead of chain of trust



## Smartcards with PC/SC

- ◆ Allow easy access to CDSA APIs
- ◆ Current applications using PC/SC
- ◆ Apple will try to minimize coding impact for:
  - Hardware developers writing drivers for readers
  - Applications written to PC/SC on other platforms
  - Card developers writing CSPs for cryptography

# Apple PC/SC Architecture





# NIST Security APIs

- ◆ signBuffer
- ◆ signFile
- ◆ verifyBuffer
- ◆ verifyFile
- ◆ encryptBuffer
- ◆ CSSM\_Sign\_Data
- ◆ CSSM\_Digest\_Data
- ◆ CSSM\_Verify\_Data
- ◆ Digest then verify
- ◆ CSSM\_Encrypt\_Data

<http://csrc.nist.gov/pki/pkiapi/welcome.htm>

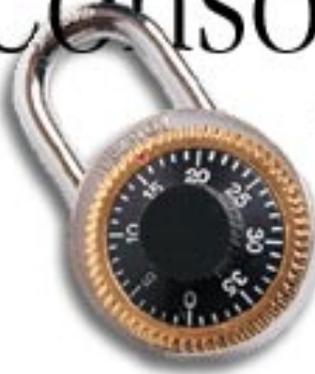


# Product Security Web Page

- ◆ <http://www.apple.com/support/security>
- ◆ Report incidents
- ◆ Security tips
- ◆ Work closely with CERT, FIRST and FreeBSD
- ◆ Internal rapid response team
- ◆ Low key



# [STOS] Consortium



Secure  
Trusted  
Operating  
System

*Shawn Geddis*  
*Chairman, co-founder*  
*[geddis@apple.com](mailto:geddis@apple.com)*

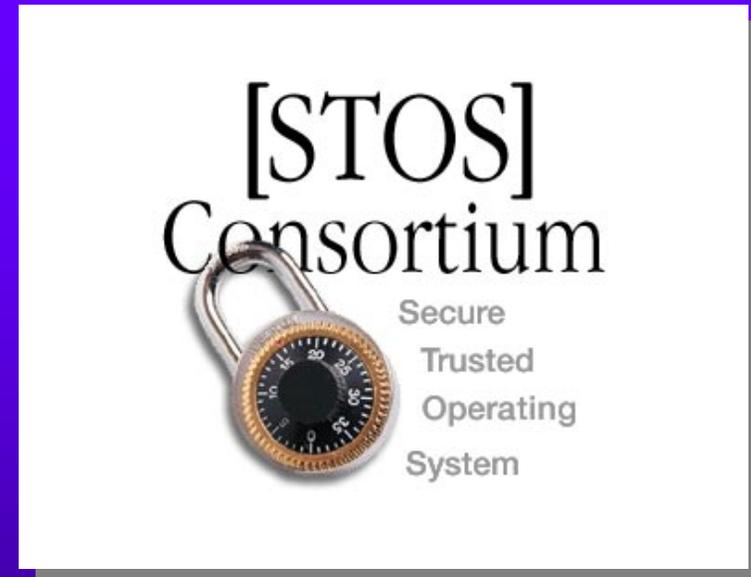
# Overview

- ◆ What it is
- ◆ Who we are
- ◆ What we are doing
- ◆ How to get involved



# [STOS] Consortium

**S**ecure  
**T**rusted  
**O**perating  
**S**ystem





# [STOS] Consortium

A **cooperative** and **collaborative**  
arrangement to:

*Build a high volume, secure, trusted operating system through open and collaborative research, development and deployment based on the Darwin Open Source Project.*



# [STOS] Consortium

A **cooperative** and **collaborative**  
arrangement among:

- ◆ Federal Agencies
- ◆ Intelligence Contractors
- ◆ Industry
- ◆ Academia



# Organizational Structure



# Quarterly Meetings

August 9, 2000

**Consortium Kickoff** *(Reston, VA)*

November 9, 2000

**Security Direction** *(Reston, VA)*

February 2001

**- postponed -**

May 22, 2001

**State of the Union** *(San Jose, CA)*

August 27-29, 2001

**Power & Progress** *(Cupertino, CA)*



# Federal Representation

- ◆ National Security Agency
  - ◆ Defense Advanced Research Projects Agency
  - ◆ Department of NAVY
  - ◆ Office of the Secretary of Defense
  - ◆ Executive Office of the President
  - ◆ National Security Council
  - ◆ Department of Energy
    - SNL, LLNL, LANL, PNL,
- and more



# DoD Contractor Representation

- ◆ General Dynamics
- ◆ SAIC
- ◆ Raytheon
- ◆ Logicon
- ◆ FGM
- ◆ TRW

and more



# Academia Representation

- ◆ University of Michigan
- ◆ MIT
- ◆ Ohio State Supercomputer Center
- ◆ University of Colorado

and more



# Active Projects

- ◆ Darwin / DTOS kernel Comparison (Sandia)
- ◆ SNMP v3 / NetInfo (iServices)

## Related Projects

- ◆ CHATS (DARPA)  
*Composable High Assurance Trusted Systems*
  - \$55M / 5 yrs - Focus on all Open Source OS initiatives
  - Dr. Doug Maughan DARPA/ITO - Core [STOS] Member
- ◆ Security Extensions to FreeBSD (NAI Labs)
  - \$1.2M funding from DARPA
  - CVS sync submission to Darwin
  - Robert Watson NAI Labs/TrustedBSD - Core [STOS] Member



# Consortium Status

Growing, building upon core group

We have taken off  
and are starting to gain momentum !



# How to Get Involved

- ◆ Join [STOS] Consortium

- Web site for content collaboration and registration

- For Contact: Shawn Geddis [geddis@apple.com](mailto:geddis@apple.com)

- ¥ Submit Membership Request Form

- ◆ Next Quarterly [STOS] Consortium Meeting

Power & Progress

August 27 - 29, 2001

Cupertino, CA



# How to Get Involved

- ◆ Collaborate on proposed projects
- ◆ Participate on Group Mailing Lists
- ◆ Submit Project Proposals
- ◆ Perform funded research

-----

- ◆ Develop from Darwin Open Source
- ◆ Read and inspect - Code Review
- ◆ File and fix bugs



# Resources

---

## Security

Specifications and SDKs for developers

<http://developer.apple.com/macos/security.html>

---

## CDSA 2.0

Specifications

<http://www.opengroup.org>

---

## PC/SC

Specifications

<http://www.pcscworkgroup.com>

---

## Open Source

Apple's open source repository

<http://opensource.apple.com/>

---

## Product Security

Apple's security information and reporting page

<http://support.apple.com/security>

---



# Who to Contact

---

## Apple Federal Systems

Shawn Geddis

Federal Senior Systems Engineer

**geddis@apple.com**

---

## Worldwide Developer Relations

Craig Keithley

Security & Cryptography Technology Manager

**keithley@apple.com**

---

## Software Engineering

John Hurley, Ph.D.

Manager, Data Security

**jhurley@apple.com**

---



# Q&A