



The Security of Security

Information, Cyber, and Physical Security Convergence

Agenda



- Information Security
- Cyber Security
- Embedded Systems
- Integrated Security
- Security Information Event Management (SIEM)
- Conclusions

- Individual or Computer Clubs/ Groups
- Manual efforts with Social Engineering
- Success = Badge Of Honor
- Personal Monetary Gain or to pay for / fund hacking activity
- War Protesting and Civil Disobedience
- Anti-Establishment Rhetoric
- Social Rebels and Misfits
- Initially viewed as mostly a nuisance growing into Criminal Acts
- Telco, University and some Government sites primary focus



- Automated / Sophisticated Malware
- **Hactivism** –Freedom of Speech, Statements to Influence Change, Sway Public Opinion and Publicize Views
- **Criminal** –Drug Cartels, Domestic and Foreign Organized Crime for Identity Theft and Financial Fraud
- **Espionage** –IP, Business Intelligence, Technology, Military / Political Secrets
- **Terrorism** –Sabotage, Disruption and Destruction
- **Nation-State** –Intelligence Gathering, Disruptive Tactics, Clandestine Ops, Misinformation, Warfare Strategies, and Infrastructure Destruction

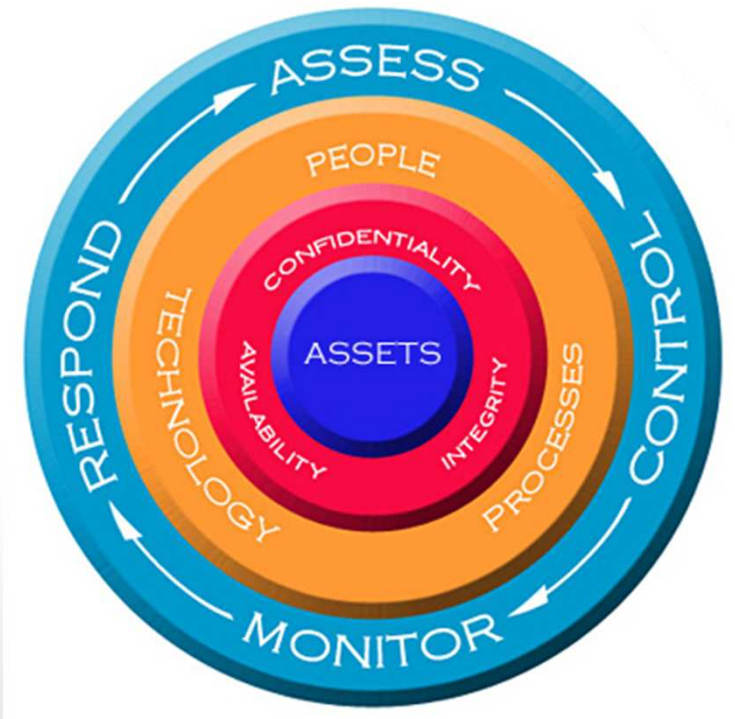


INFORMATION SECURITY

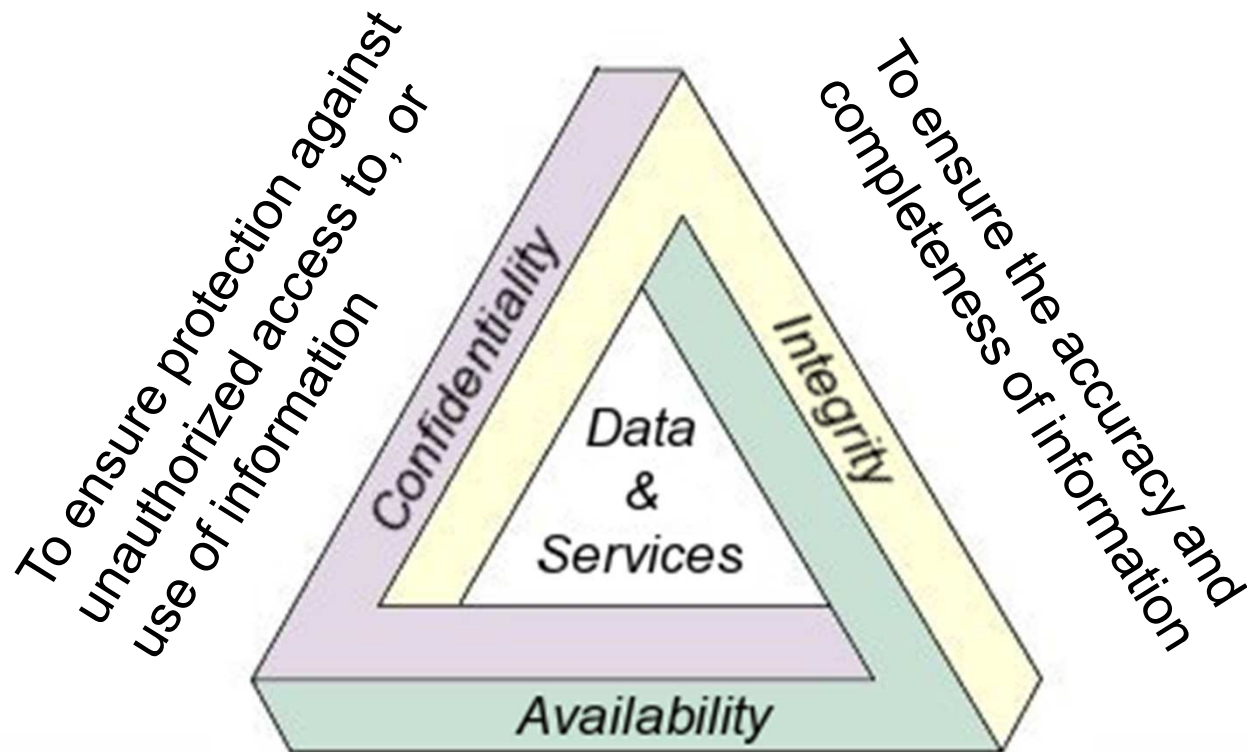
Information Security



- Programmatic Effort to Reduce Risks
- Ongoing Processes (not on project completion)
- Ever-changing Landscape
 - Threats (Agents/Actors)
 - Technologies
 - Countermeasures
- Never 100% Secure



InfoSec Goals: The CIA Triad

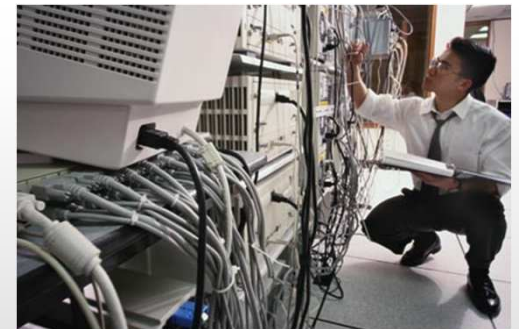


To ensure that information and vital services are useable when required

ISO / IEC 27001



- Can be used by any organization
- Aids in securing information in an appropriate manner relevant to the business
- Monitor and control security, minimizing residual business risk
- Helps organization protect proprietary information, common basis for security standards development, enhances security management practice and increases confidence and trust in inter-organizational dealing



<http://site.ul.com/asiaonthemark/as-en/2006-Issue17/page6.htm>

Information Security Domains (27001:2005)



ISO 27001 Control Domain	Objectives	Controls
Security policy	1	2
Organization of information security	2	11
Asset management	2	5
Human resources security	3	9
Physical and environmental security	2	13
Communication and operational management	10	33
Access control	7	25
Systems development and maintenance	6	16
Information security and incident management	2	5
Business Continuity Plan	1	5
Compliance	3	10
	39	134

<http://site.ul.com/asiaonthemark/as-en/2006-Issue17/page6.htm>

Regulatory Field



- PCI DSS – Payment Card Industry Data Security Standard
- HIPAA – Health Insurance Portability and Accountability Act
- GLBA – Gramm–Leach–Bliley Act
- SOX – Sarbanes–Oxley Act
- FERPA – Family Educational Rights and Privacy Act
- FISMA – Federal Information Security Management Act
- NERC – North American Electric Reliability Corp.



<http://www.educause.edu/ero/article/unified-approach-information-security-compliance>

<http://www.csoonline.com/article/632218/the-security-laws-regulations-and-guidelines-directory>

The Basics of Data Retention



- Types of companies
- Types of data retained
 - Retention of IP address allocations
 - Retention of traffic data
 - Retention of location data
 - Retention of the content of communications
- Length of retention period
- Financial burden
- Restrictions on access to retained data
- The volume of data mandated to be retained
- Disclosure rules



Additional Info: <http://msdn.microsoft.com/en-us/library/aa480484.aspx>

Data Retention Law



- Federal awards data “for three years”. Uhhhh.....
 - OMB Circular A-110: retention period is three years from the date the final financial report is submitted
 - NIH: Grants Policy Statement includes “three years”
 - NSF General Grant Conditions (2005) that records must be retained for three years after the submission of all required reports (research and other special reports)

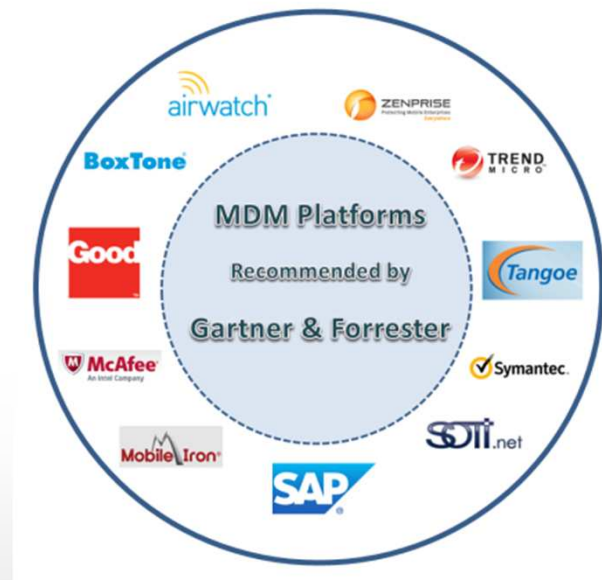


- Retention Schedule for Records of Public Safety Agencies
 - <https://www.tsl.state.tx.us/slrn/recordspubs/ps.html>
 - 30 days, 90 days, 120 days, AV (as long as administratively valuable), 2 years

MDM – Mobile Device Management



- Mobile device security is an imperative
- IDC report from smart phone sales outpaced PC sales for first time in 2010
- BYOD policies will become norm as show business advantage
- Issues
 - Malware
 - Eavesdropping
 - Access
 - Theft and loss
 - Applications



Learning guide: Mobile device protection

<http://searchmobilecomputing.techtarget.com/guides/Mobile-device-protection-and-security-threat-measures>



CYBER SECURITY

Vulnerabilities and Penetration Testing

Understanding Vulnerabilities



Common Vulnerabilities and Exposures (CVE)

<http://cve.mitre.org/>

The screenshot shows the CVE website in a web browser. The browser's address bar displays 'http://cve.mitre.org/'. The page features a navigation bar with links for 'CVE LIST', 'COMPATIBILITY', 'NEWS - JANUARY 24, 2013', and 'SEARCH'. Below the navigation bar, the CVE logo is prominently displayed. The main content area is titled 'Common Vulnerabilities and Exposures' and includes a subtitle 'The Standard for Information Security Vulnerability Names'. A green banner indicates 'TOTAL CVEs: 54297'. The page is organized into several sections: 'About CVE' (Terminology, Documents, FAQs), 'CVE List' (About CVE Identifiers, Search CVE, Search NVD, Updates & RSS Feeds, Request a CVE-ID), 'CVE In Use' (CVE-Compatible Products, NVD for CVE Fix Information, CVE Numbering Authorities), 'News & Events' (Calendar, Free Newsletter), 'Community' (CVE Editorial Board, Sponsor, Contact Us), and 'Search the Site'. A central section titled 'Widespread Use of CVE' lists various organizations and standards that utilize CVE, including NVD (National Vulnerability Database), US-CERT Bulletins, CVE Numbering Authorities (CNAs), Recommendation ITU-T X.1520 Common Vulnerabilities and Exposures (CVE), ITU-T CYBEX Series, Vulnerability Management, Patch Management, Vulnerability Alerting, Intrusion Detection, and Security Content Automation Protocol (SCAP). A 'Related Efforts' section highlights the Vulnerability Scoring System (CVSS), Assessment Language (OVAL), Software Weakness Types (CWE), and Making Security Measurable. A 'Focus On' section titled 'Requesting CVE Identifier Numbers' explains the process of obtaining a CVE Identifier (also called 'CVE-IDs,' 'CVE numbers,' 'CVE names,' and 'CVEs') before publicizing a new vulnerability. It provides two primary ways to obtain a CVE Identifier: 1. Contact one of the official CVE Numbering Authorities (CNAs), which will then include a CVE-ID number in its initial public announcement about your new vulnerability. 2. Contact the CVE project to Request a CVE-ID and we will provide you with our 'CVE Identifier Reservation Guidelines for Researchers' and work with you to assign a CVE-ID number while you work through the process of publicly disclosing the vulnerability. On the right side of the page, there are sections for 'Latest News' (Call for Public Feedback on Upcoming CVE ID Syntax Change, MITRE Announces Initial 'Making Security Measurable' Calendar of Events for 2013, 2 Products from Huawei Technologies Now Registered as Officially 'CVE-Compatible', Opcon Technology Makes 3 Declarations of CVE Compatibility, Mozilla and Symantec Added as CVE Numbering Authorities (CNAs)) and 'Upcoming Events' (CVE/Making Security Measurable booth at RSA Conference 2013, February 25 - March 1). The browser's status bar at the bottom shows the time as 2:29 PM on 1/30/2013.

CVE LIST



64,267 entries on 25Sep2014

59,390 on 17Jan2014

58,306 on 08Nov2013

The screenshot displays the CVE Mitre website interface. The top section shows a list of vulnerabilities, including CVE-2013-0012 through CVE-2013-0001. Below this, a detailed view of CVE-2012-1240 is shown, describing an unspecified vulnerability in the RECRUIT Dokodemo Rikunabi 2013 via unspecified vectors. The right sidebar contains a 'National Vulnerability Database' section with a 'Vulnerability Summary for CVE-2012-1240' and a 'National Cyber-Alert System' section with a 'Vulnerability Summary for CVE-2012-1240'.

does not properly handle encrypted packets, which allows man-in-the-middle attackers to conduct SSLv3 downgrade attacks against (1) SSLv3 sessions or (2) TLS sessions by intercepting handshakes and injecting content, aka "Microsoft SSL Version 3 and TLS Protocol Security Feature Bypass Vulnerability."

CVE-2013-0012 *** RESERVED *** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.

CVE-2013-0011 The Print Spooler in Microsoft Windows Server 2008 R2 and R2 SP1 and Windows 7 Gold and SP1 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted print job, aka "Windows Print Spooler Components Vulnerability."

CVE-2013-0010 Cross-site scripting (XSS) vulnerability in Microsoft System Center Operations Manager 2007 SP1 and R2 allows remote attackers to inject arbitrary web script or HTML via crafted input, aka "System Center Operations Manager Web Console XSS Vulnerability," a different vulnerability than CVE-2013-0009.

CVE-2013-0009 Cross-site scripting (XSS) vulnerability in Microsoft System Center Operations Manager 2007 SP1 and R2 allows remote attackers to inject arbitrary web script or HTML via crafted input, aka "System Center Operations Manager Web Console XSS Vulnerability," a different vulnerability than CVE-2013-0010.

CVE-2013-0008 win32k.sys in the kernel-mode drivers in Microsoft Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, Windows 7 Gold and SP1, Windows 8, Windows Server 2012, and Windows RT does not properly handle window broadcast messages, which allows local users to gain privileges via a crafted application, aka "Win32k Improper Message Handling Vulnerability."

CVE-2013-0007 Microsoft XML Core Services (aka MSXML) 4.0, 5.0, and 6.0 does not properly parse XML content, which allows remote attackers to execute arbitrary code via a crafted web page, aka "MSXML XSLT Vulnerability."

CVE-2013-0006 Microsoft XML Core Services (aka MSXML) 3.0, 5.0, and 6.0 does not properly parse XML content, which allows remote attackers to execute arbitrary code via a crafted web page, aka "MSXML Integer Truncation Vulnerability."

CVE-2013-0005 The WCF Replace function in the Open Data (aka OData) protocol implementation in Microsoft .NET Framework 3.5, 3.5 SP1, 3.5.1, and 4, and the Management OData IIS Extension on Windows Server 2012, allows remote attackers to cause a denial of service (resource exhaustion) via a crafted request, aka "Microsoft OData IIS Extension Denial of Service Vulnerability."

CVE-2013-0004 Microsoft .NET Framework 1.0 SP3, 1.1 SP1, 2.0 SP2, 3.0 SP2, 3.5, 3.5.1, 4, and 4.5 allows remote attackers to execute arbitrary code via (1) a crafted XAML browser application (XBAP) or (2) a .NET assembly, aka ".NET Framework XBAP Remote Code Execution Vulnerability."

CVE-2013-0003 Buffer overflow in a System.DirectoryServices.Protocols (S.DS.P) namespace method allows remote attackers to execute arbitrary code via (1) a crafted XAML browser application (XBAP) or (2) a .NET assembly, aka "S.DS.P Buffer Overflow Vulnerability."

CVE-2013-0002 Buffer overflow in the Windows Forms (aka WinForms) component in Microsoft .NET Framework 1.0 SP3, 1.1 SP1, 2.0 SP2, 3.0 SP2, 3.5, 3.5.1, 4, and 4.5 allows remote attackers to execute arbitrary code via (1) a crafted XAML browser application (XBAP) or (2) a .NET assembly, aka "WinForms Buffer Overflow Vulnerability."

CVE-2013-0001 The Windows Forms (aka WinForms) component in Microsoft .NET Framework 1.0 SP3, 1.1 SP1, 2.0 SP2, 3.0 SP2, 3.5, 3.5.1, 4, and 4.5 allows remote attackers to obtain sensitive information via (1) a crafted XAML browser application (XBAP) or (2) a .NET assembly, aka "WinForms Buffer Overflow Vulnerability."

CVE-2012-1240 Unspecified vulnerability in the RECRUIT Dokodemo Rikunabi 2013 via unspecified vectors.

CVE-2011-1240 Integer overflow in the TCP/IP implementation in Microsoft Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, Windows 7 Gold and SP1, Windows 8, Windows Server 2012, and Windows RT allows remote attackers to execute arbitrary code by sending a sequence of crafted UDP packets to a closed port, aka "Microsoft TCP/IP Integer Overflow Vulnerability."

CVE-2010-2013 Cross-site scripting (XSS) vulnerability in cp/edit_email.php in USK CMS 4.4 allows remote attackers to inject arbitrary web script or HTML via a crafted request, aka "USK CMS 4.4 XSS Vulnerability."

CVE-2009-2013 SQL injection vulnerability in bin/aps_browse_sources.php in Frontis 3.9.01.24 allows remote attackers to execute arbitrary code via a crafted request, aka "Frontis 3.9.01.24 SQL Injection Vulnerability."

CVE-2008-2013 Cross-site scripting (XSS) vulnerability in index.php in the pNFlashGames 1.5 through 2.5 mod allows remote attackers to inject arbitrary web script or HTML via the id parameter in a display action, aka "pNFlashGames 1.5 through 2.5 mod XSS Vulnerability."

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1240

National Vulnerability Database

automating vulnerability management, security measurement, and compliance checking

Vulnerabilities | Checklists | SCAP Validated Tools | Product Dictionary | SCAP Events | Impact Metrics | Data Feeds | Contact | Vendor Comments | Statistics

Vulnerability Summary for CVE-2012-1240

Original release date: 06/29/2012
Last revised: 07/02/2012
Source: US-CERT/NIST

Overview

Unspecified vulnerability in HP System Management Homepage (SMH) before 7.1.1 allows remote attackers to cause a denial of service, or possibly obtain sensitive information or modify data, via unknown vectors.

Impact

CVSS Severity (version 2.0):
CVSS v2 Base Score: 2.5 (HIGH) [AV:N/A/C:U/Au:N/C:P/R/A:P] (legend)
Impact Subscore: 6.4
Exploitability Subscore: 10.0
CVSS Version 2 Metrics:
Access Vector: Network exploitable
Access Complexity: Low
**NOTE: Access Complexity scored Low due to insufficient information
Authentication: Not required to exploit
Impact Type: Allows unauthorized disclosure of information; Allows unauthorized modification; Allows disruption of service

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST website. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to: comments@nist.gov

Computer Emergency Response Team and...



- <http://www.cert.org/>
- <http://www.us-cert.gov/>
 - DHS' National Cybersecurity and Communications Integration Center (NCCIC)
- <http://nvd.nist.gov/home.cfm>
- <http://www.dhs.gov/office-cybersecurity-and-communications/>
- The Common Vulnerability Reporting Framework (CVRF)
 - <http://www.icaso.org/cvrf>
- <http://www.stopthinkconnect.org/>
- <https://buildsecurityin.us-cert.gov/>
- <https://ics-cert.us-cert.gov/Standards-and-References>
- http://en.wikipedia.org/wiki/Cyber_security_standards
- DIACAP (Department of Defense Information Assurance Certification and Accreditation)
 - http://www.prim.osd.mil/Documents/DIACAP_Slick_Sheet.pdf



STOP | THINK | CONNECT™

Types of Penetration Tests



- Social Engineering
- Application Security Testing
- Physical Penetration Test
- Penetration Testing Techniques
 - Manual penetration test
 - Using automated penetration test tools
 - Combination of both manual and automated process



<http://www.softwaretestinghelp.com/penetration-testing-guide>
hackersthirst.com

<http://www.ipost.com/blog/data-breaches/social-engineering-how-a-simple-phone-call-can-ruin-your-business/>
<http://magazine.thehackernews.com/images/Social-Engineering.JPG>

Penetration Testing



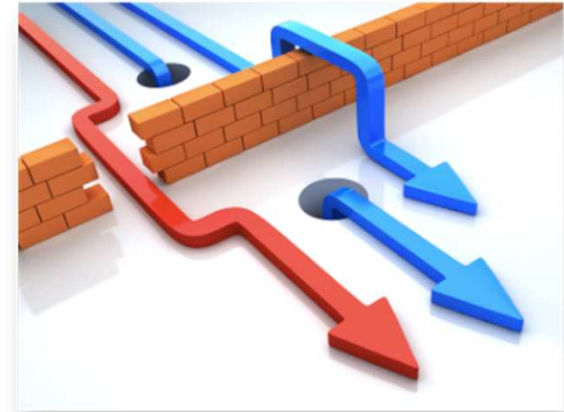
- Phase I – **Scanning** to determine the attack surface
- Phase II – **Vulnerability Assessment**, or verification of true weakness and selection of attack vectors
- Phase III – **Penetration Test**
- Methods:
 - Data collection
 - Vulnerability Assessment
 - Actual Exploit
 - Result analysis and report preparation



Causes of Vulnerabilities



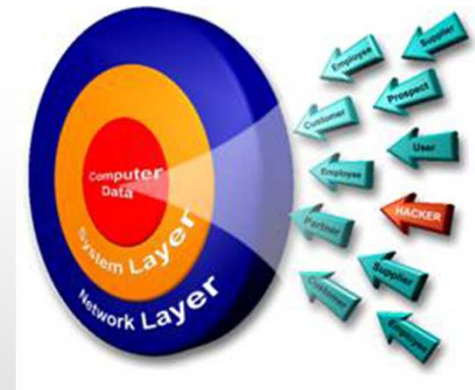
- Design and development error
- Poor system configuration
- Human errors

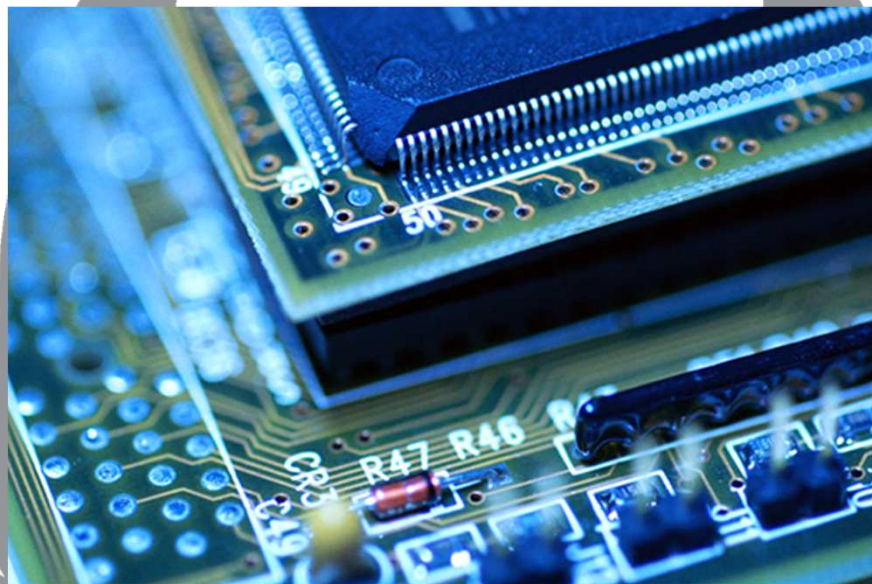


Pen Testing Standards



- PCI DSS (Payment Card Industry Data Security Standard)
 - https://www.pcisecuritystandards.org/security_standards/
- OWASP (Open Web Application Security Project)
 - <https://www.owasp.org>
- ISO/IEC 27002 (Information technology – Security techniques – Code of practice for information security management)
 - http://en.wikipedia.org/wiki/ISO/IEC_27002
- OSSTMM (The Open Source Security Testing Methodology Manual)
 - <http://www.isecom.org/mirror/OSSTMM.3.pdf>





EMBEDDED SYSTEMS

Why and How Attack?



- Why
 - Harder to perform forensics
 - Custom firmware can be developed
 - Host based IDS (intrusion detection system) does not usually exist
- How
 - No or simple default password
 - Classic Programming Mistakes
 - Input validation
 - Format strings
 - Buffer overflows
 - Cross Site / CSRF Scripting



Project SHINE (SHodan INtelligence Extraction)



- Development started mid-2008 and began ingesting raw data in mid-April 2012.
- Initiated to determine a baseline of just how many SCADA/ICS devices and software products are directly connected to the Internet

Medical devices	Power regulators/UPSs
Traffic management systems	Security/access control (includes CCTV and webcams)
Automotive control	Serial port servers
HVAC/environment control	Data radios (point-to-point 2.4/5.8/7.8 GHz direct-connected radios)

<http://www.shodanhq.com/>

<http://www.tofinosecurity.com/blog/project-shine-1000000-internet-connected-scada-and-ics-systems-and-counting>

Critical IO Project



- HD Moore's (Metasploit) Critical IO (Internet-Wide Scan Data Repository) project:
 - Little in the way of authentication
 - Critical infrastructure or corporate network
 - > 95,000 exposed over mobile connections (3G or GPRS)
 - 13,000 root shells, system consoles and admin interfaces that did not require authentication or were pre-authenticated
 - Undetectable access is able to capture or manipulate data moving through the serial port
 - Console connections, HVAC, SCADA, etc.
 - Project Sonar (NEWER): a community effort to improve security through the active analysis of public networks

Universal Plug and Play (UPnP) Protocol



- Numbers from January 2013
 - 40 and 50 million networked devices
 - > 81 million different IPs responded to UPnP discovery requests
- 6,900 different products from 1,500 vendors
- Enabled by default
 - printers, routers, network-attached storage, IP cameras, media players, smart TVs, etc.
- Open to attack over the Internet via flaws
- Portable UPnP SDK has been patched (> 1.6.18) and issue in question fixed more than two years ago: even so, some 330 vendors still run older versions of that software
- Embedded baseboard management controllers (BMCs) in June 2014 using Intelligent Platform Management Interface (IPMI)

<https://community.rapid7.com/docs/DOC-2150>

<http://www.tripwire.com/state-of-security/vulnerability-management/supermicro-ipmibmc-vulnerability-analysis/>

IP Cameras



- Default or no password
- Firmware bugs (authentication not needed)
- Issues:
 - Access to video stream
 - Access to network
 - Credentials (WiFi, ftp, email, etc)
 - Firmware exploits
 - CSRF (cross-site request forgery) exploits



“Hack of the Insulin Pump”



- A major problem with embedded devices
- Most were not designed to be easily updated
- Where is target?
 - A growing number of vulnerabilities being found
 - Fixing flaws in the field is not easy (no easy way to patch)

“Smart” Home Appliances



- Sent 750,000 malicious emails between December 23, 2013 and January 6, 2014
- No more than 10 messages sent from a single device
- 25% of those messages from appliances
- 100,000 gadgets (TV, multimedia center, router, refrigerator)
- Internet of Things
 - Nest (recent google acquisition for \$3.2 B)
 - Large botnets
 - Embedded systems
- Gartner expects 26 billion Internet “things” by 2020 (was 2.5 B in 2009)

Even Toilets Aren't Safe



- Hijacked Robotoilet
 - Open or close the lid
 - Squirt a stream of water
- Where are we going? Your smartphone will be able to:
 - lock your house
 - turn on the air conditioning
 - check whether the milk is out of date
 - heat up your iron
 - What else?



<http://www.bloomberg.com/news/2014-06-10/even-toilets-aren-t-safe-as-hackers-target-home-devices.html>

What can they do with access?



- Replace firmware
- Remote commands
- Remote management
- DNS
- Starting point on network
- DDoS (distributed denial-of-service) attack
- Brick device (printer exploit few years ago)
- Exploit video



<http://rocketdock.com/images/screenshots/Hacker.png>

What can you do?



- Change default passwords
- Update firmware
- Disable services not in use
- Restrict access (login and ports) using ACL
- Use https/ssh
- Remote logging (and review)
- Network design (subnets for embedded devices)
- SNMP read/write communities
- Stay on top of vendors



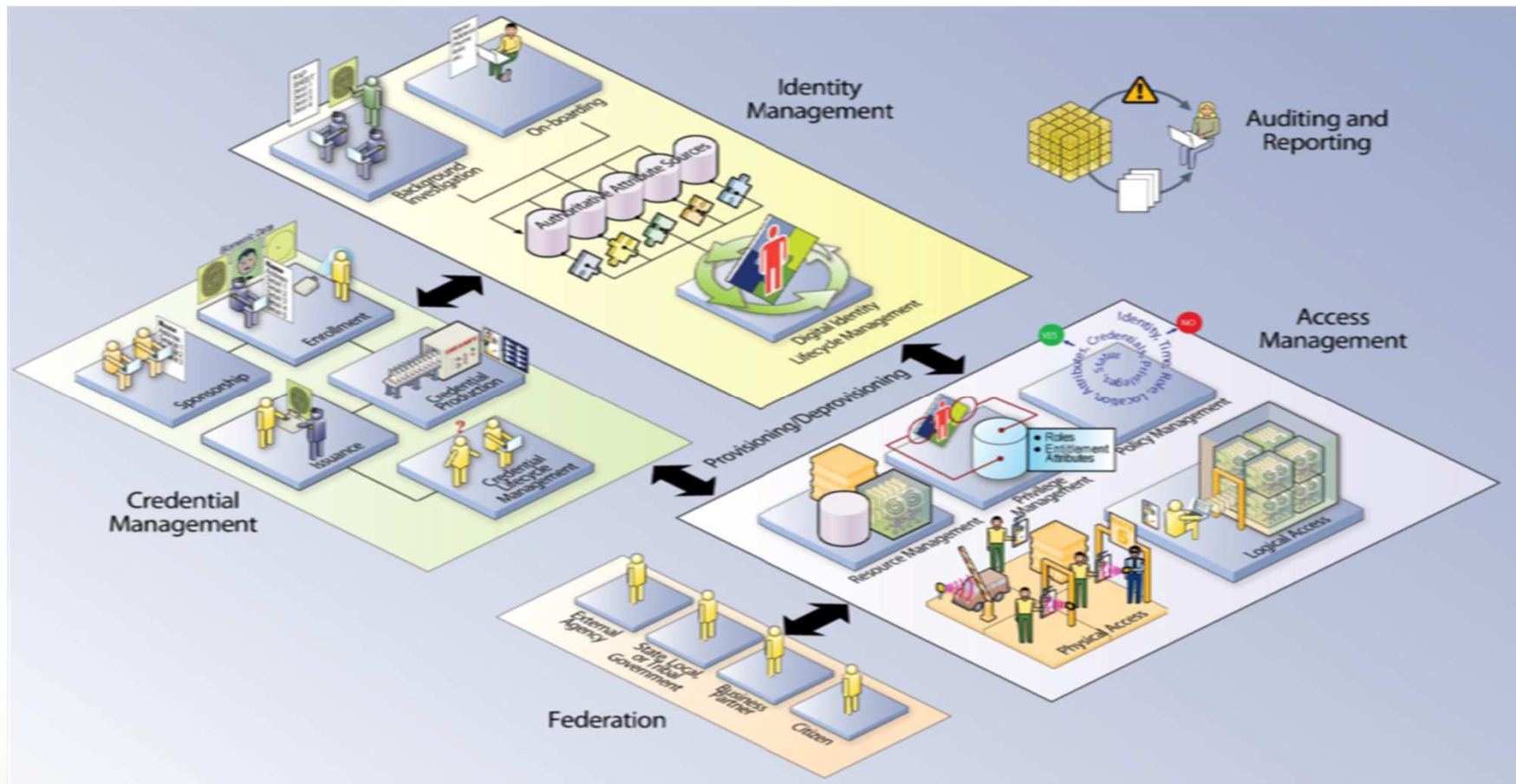
<http://techologic.com/images/security.jpg>



INTEGRATED SECURITY

Convergence of PACS and LACS

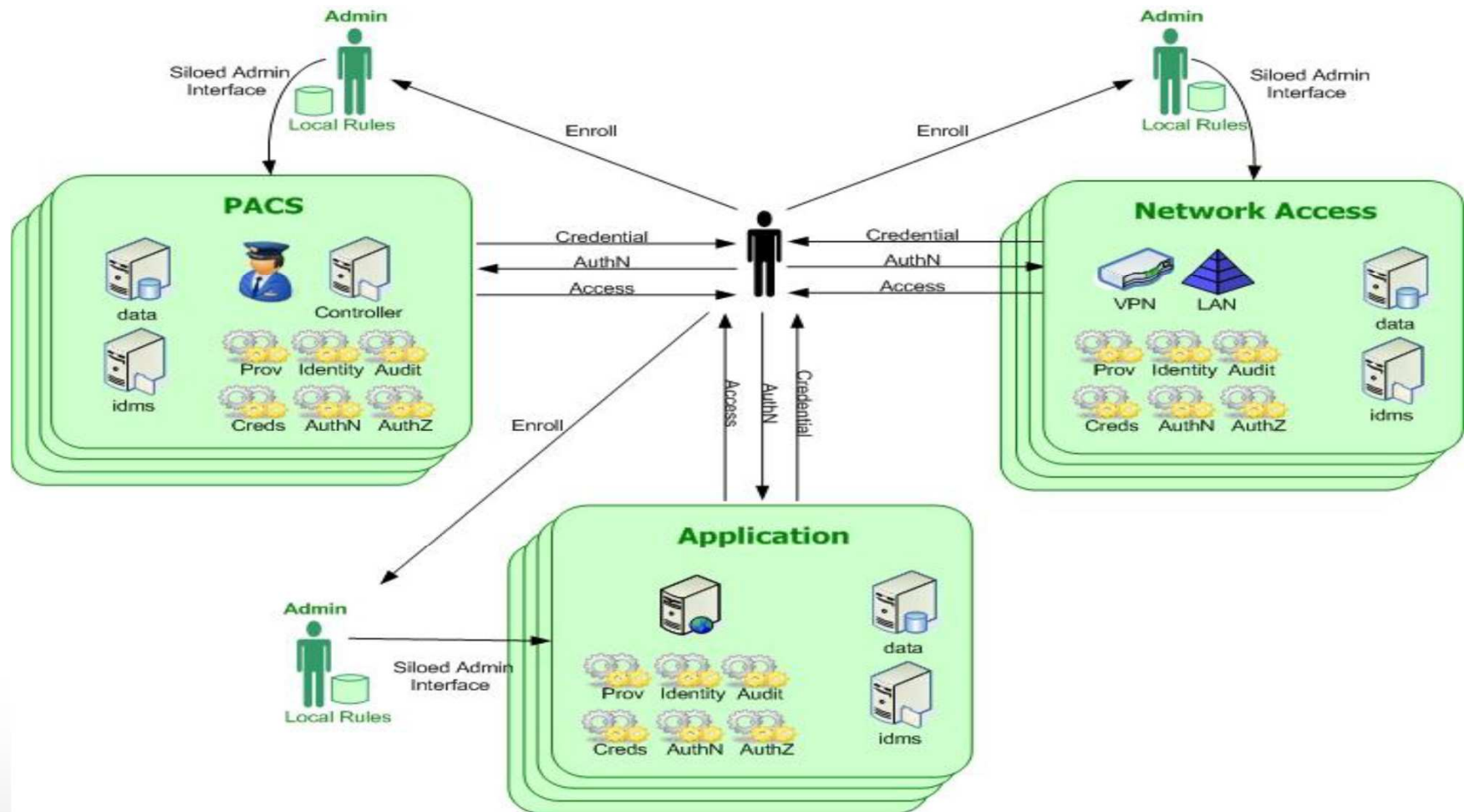
Conceptual View



www.idmanagement.gov

<https://federation.nih.gov/ppt/JudySpencerTrust20091210.ppt>

Current State – Parallel Systems

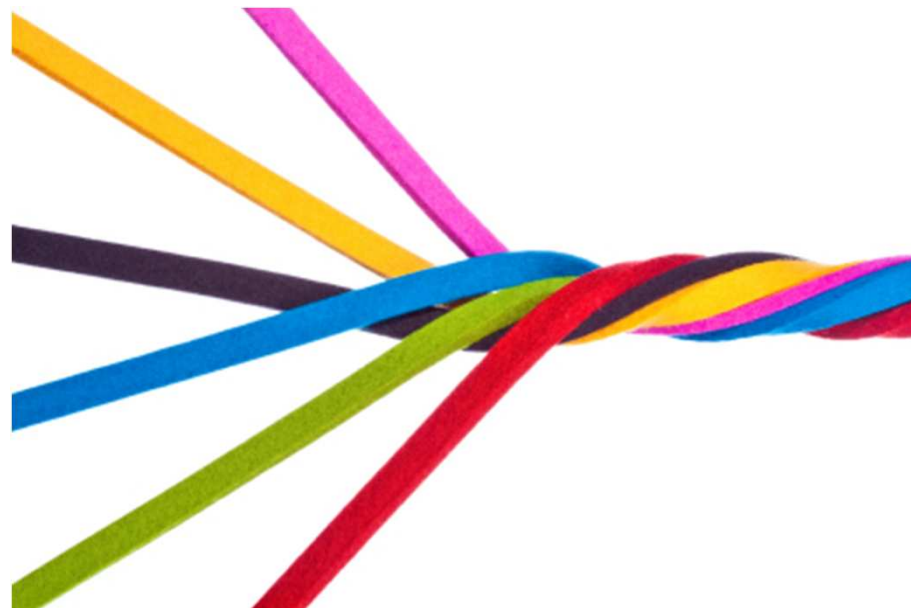


PACS and LACS operate in silos

Convergence



- Securing the Network
 - Outside-In
 - Inside-Out
 - Inside
- Protecting the People
- Securing the Data
- Securing the Facility

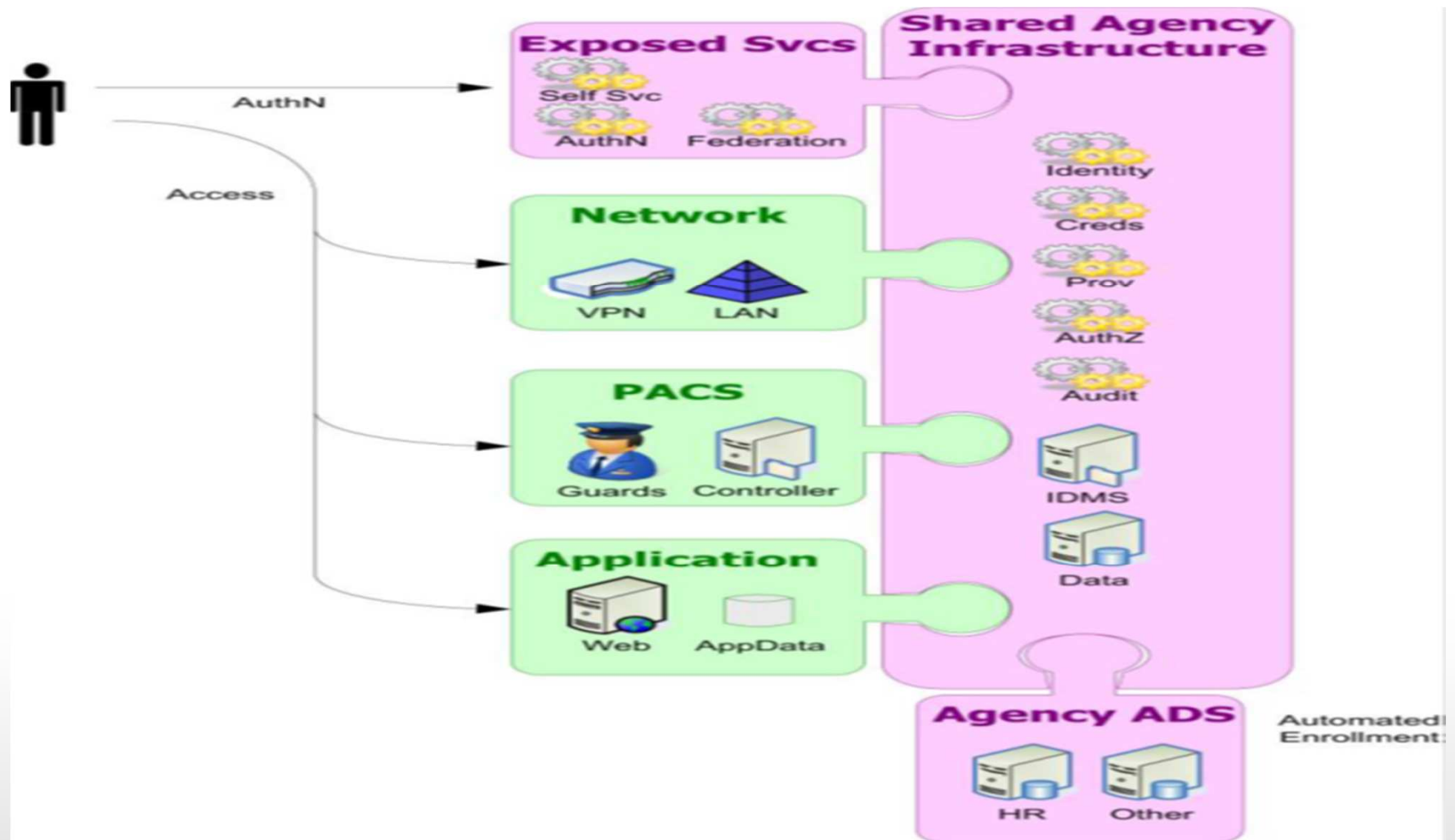


http://www.csrandthelaw.com/uploads/image/iStock_000014777263XSmall.jpg

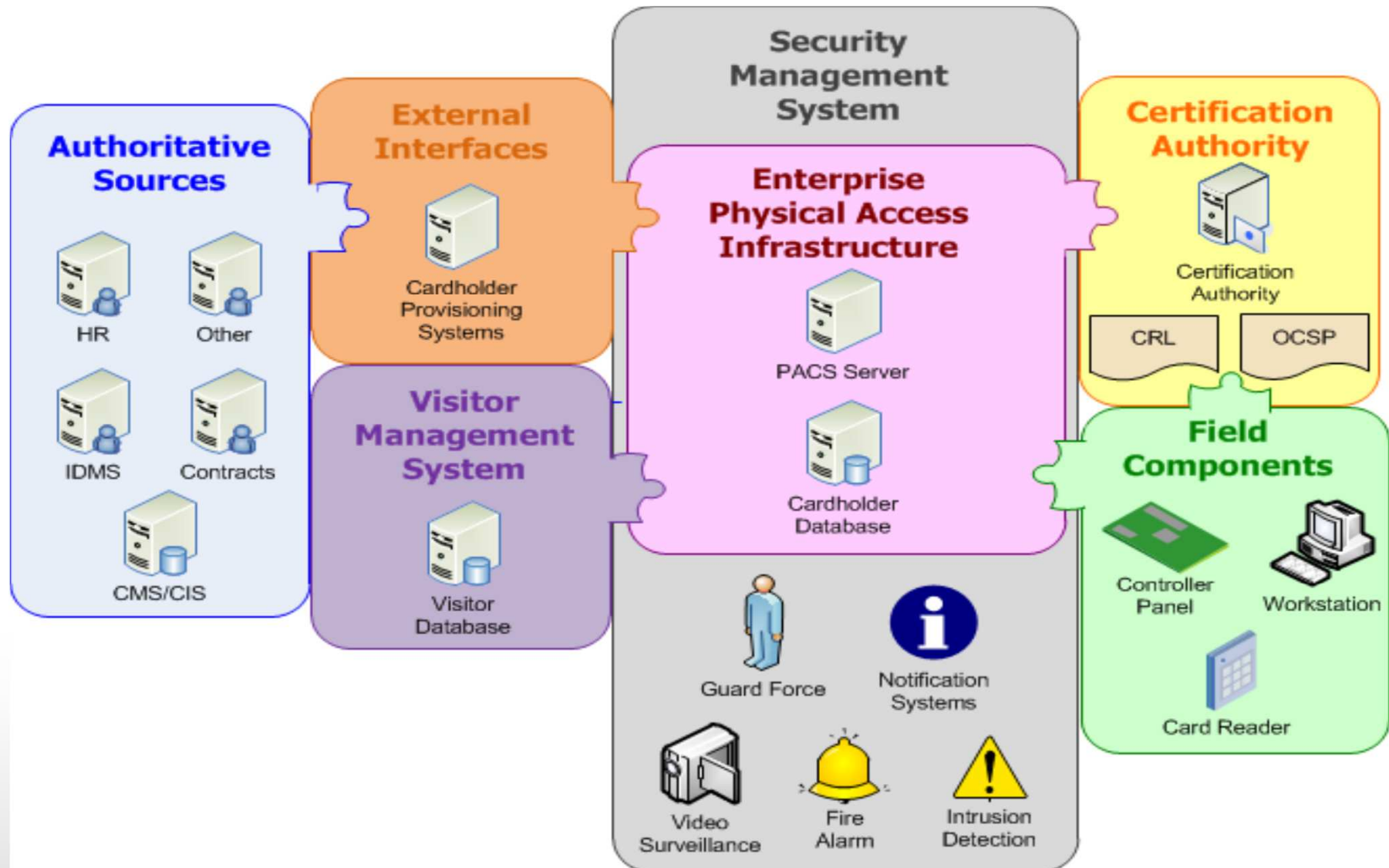
Future State – Common Services



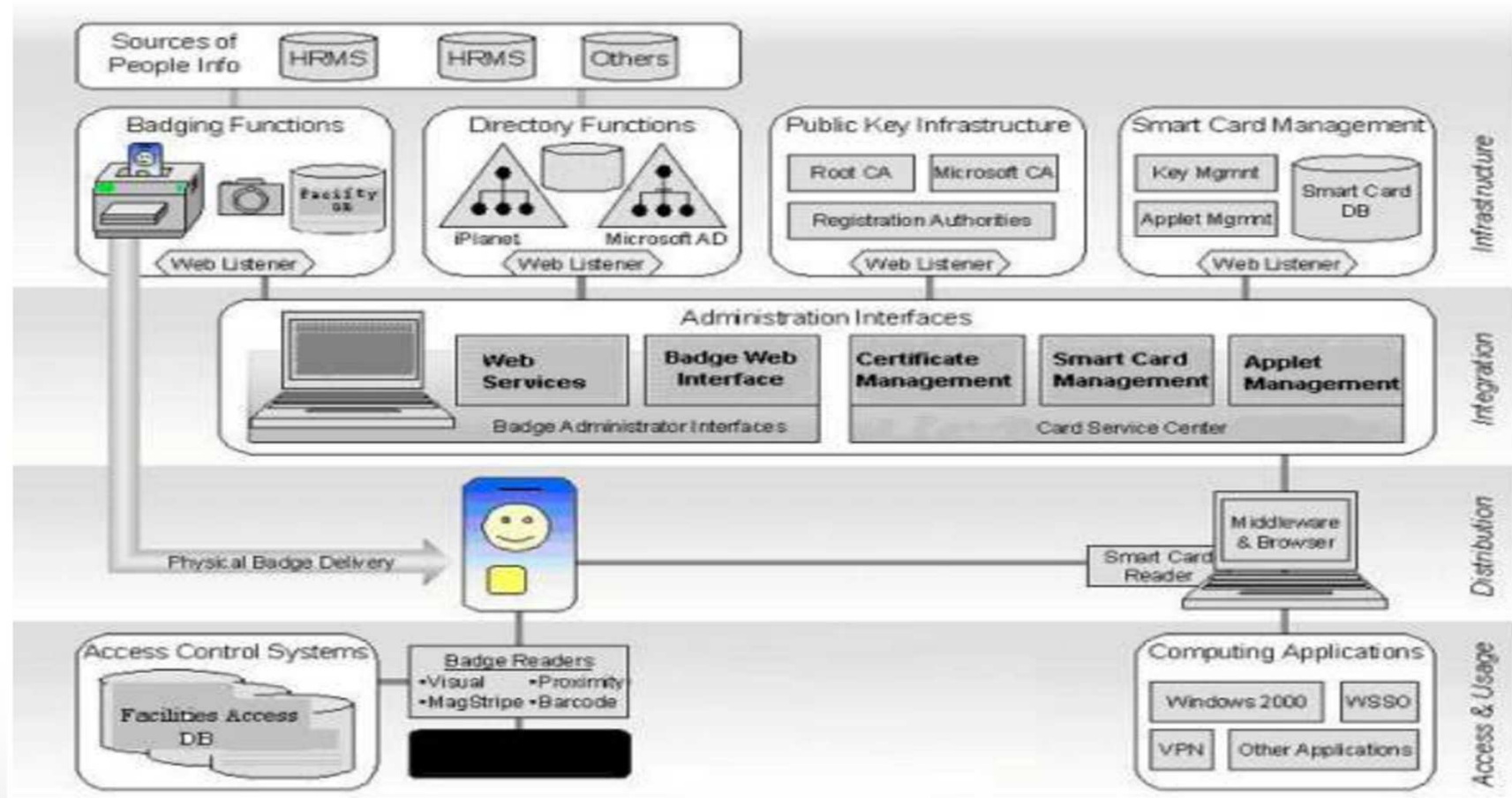
One Set of Services



Physical Security Context



Convergence of Logical and Physical Security



<http://www.sans.org/reading-room/whitepapers/authentication/convergence-logical-physical-security-1308>



SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)

What can be done to Protect Data?



- Review Access Policy
- Secure Perimeter
- Review Logs
- 2FA
- Data Masking
- Encryption
- Cloud Compliance Solutions
 - Governance, Risk and Compliance (GRC) framework
 - Secure bridge between cloud and enterprise
- USB device connectivity
- Systematic Approach



http://cdn.business2community.com/wp-content/uploads/2013/04/depositphotos_3622965_original.jpg

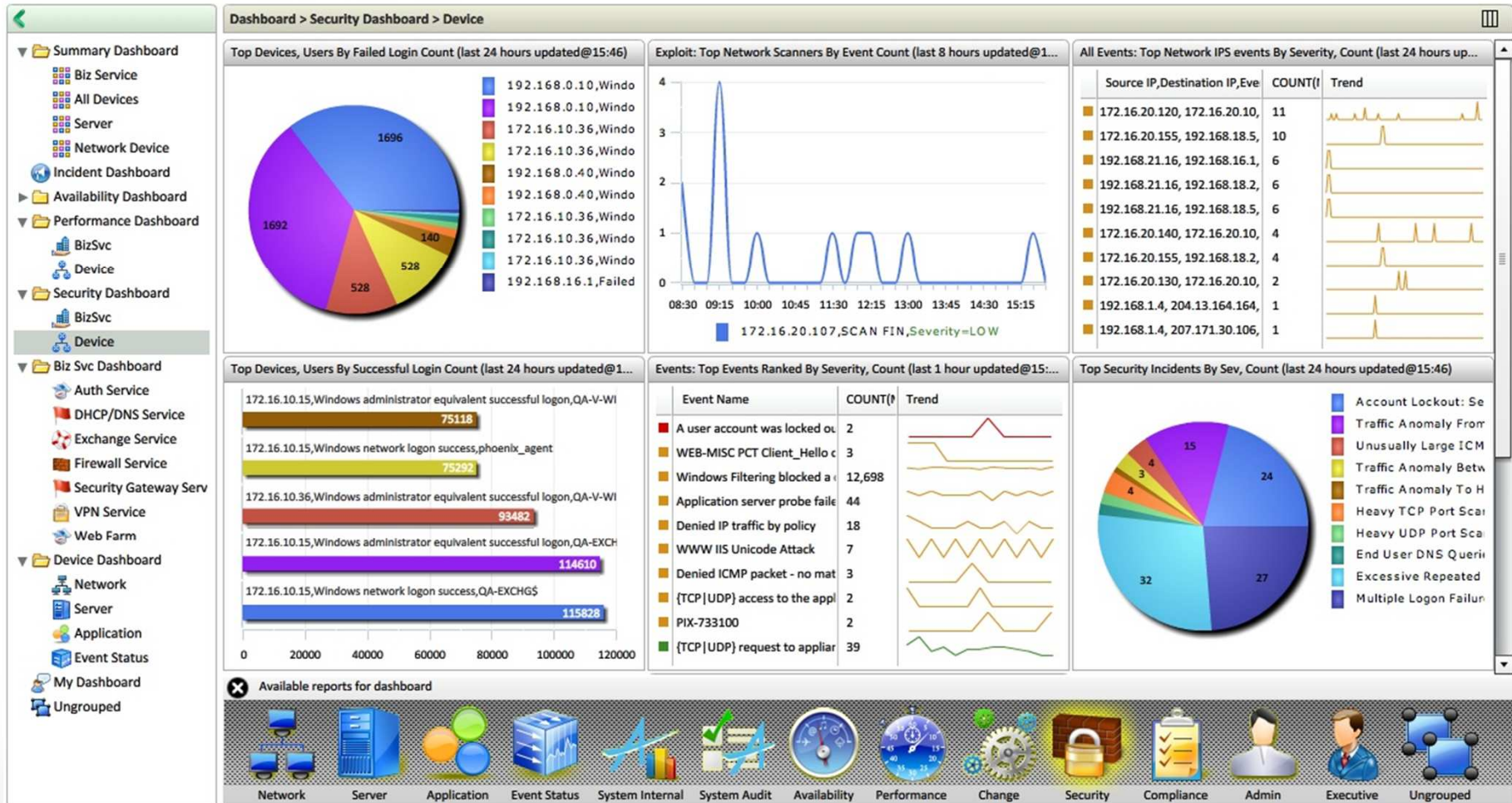
Security Information & Event Management (SIEM)



- Security information management (SIM)
- Security event manager (SEM)
- Real-time analysis of security alerts generated by network hardware and applications
 - Information from network and security devices
 - Identity and access management applications
 - Vulnerability management and policy compliance tools
 - Operating system, database and application logs
 - External threat data

http://en.wikipedia.org/wiki/Security_information_and_event_management

Sample SIEM Screen



<http://www.accelops.com/images/product/siem-security-dashboard-full.jpg>



CONCLUSIONS

Conclusions



- Information Security
- Cyber Security
- Embedded Systems
- Integrated Security
- Security Information Event Management (SIEM)

Discussion



Contact Information:

Chris Peckham, Ph.D., P.E.

Senior Vice President, Chief Technology Officer and Special Projects

chris.peckham@KratosPSS.com