Using Smart Cards to Protect Against Advanced Persistent Threat

Smart Cards in Government

Oct 30, 2014

Chris Williams

leidos

Export Approval #
14-leidos-1016-1281

Agenda

- Who is Leidos?
- The Identity Challenge and PIV
- PIV Technology at Leidos (formerly SAIC)
- Advanced Persistent Threat (APT)
- The APT Attack Sequence
- The Failure of Endpoint Security
- Systems Administration Under Fire
- Mazes versus Minefields
- Fighting APT with Smart Cards
- Cyber Castles
- True Defense in Depth
- The Top 10 Features of a Next-Gen Defense
- Conclusion
- Closing Thought

 Acronyms and Trademarks on last slide

leidos

Who is Leidos?

- Formerly part of Science Applications International Corporation (SAIC)
- Fortune 500® solutions leader with over $5 billion annual revenue
- About 22,000 employees
- Businesses: National Security, Health, Engineering

National Security

Engineering **Health** **Cybersecurity**

leidos

The Identity Challenge

Let's consider Get Smart (2008):

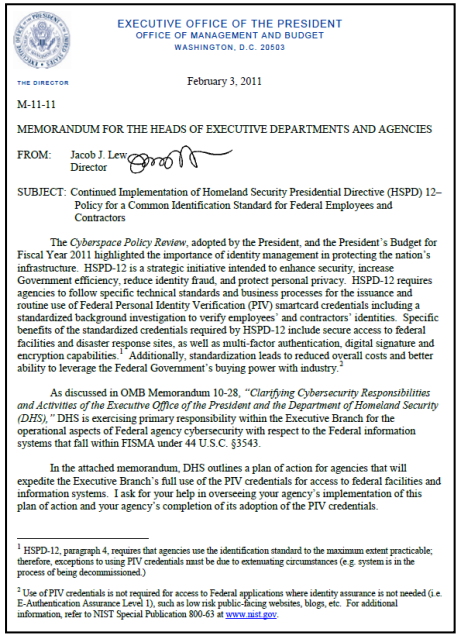
- **Siegfried**: How do I know you're not Control?
- **Maxwell Smart**: If I were Control, you'd already be dead.
- **Siegfried**: If you were Control, you'd already be dead.
- **Maxwell Smart**: Neither of us is dead, so I am obviously not from Control.

Good authentication is critically important.
It's also really hard to do well over a network.

leidos

PIV and OMB Memo 11-11

- **Office of Management and Budget Memo 11-11**
- Directs agencies to use *"PIV credentials as the common means of authentication for access to that agency's facilities, networks and information systems."*
- PIV an open standard specified by NIST in FIPS 201 and SP 800-73



EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

THE DIRECTOR

February 3, 2011

M-11-11

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Jacob J. Lew
Director

SUBJECT: Continued Implementation of Homeland Security Presidential Directive (HSPD) 12– Policy for a Common Identification Standard for Federal Employees and Contractors

The *Cyberspace Policy Review*, adopted by the President, and the President's Budget for Fiscal Year 2011 highlighted the importance of identity management in protecting the nation's infrastructure. HSPD-12 is a strategic initiative intended to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy. HSPD-12 requires agencies to follow specific technical standards and business processes for the issuance and routine use of Federal Personal Identity Verification (PIV) smartcard credentials including a standardized background investigation to verify employees' and contractors' identities. Specific benefits of the standardized credentials required by HSPD-12 include secure access to federal facilities and disaster response sites, as well as multi-factor authentication, digital signature and encryption capabilities.[1] Additionally, standardization leads to reduced overall costs and better ability to leverage the Federal Government's buying power with industry.[2]

As discussed in OMB Memorandum 10-28, *"Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and the Department of Homeland Security (DHS),"* DHS is exercising primary responsibility within the Executive Branch for the operational aspects of Federal agency cybersecurity with respect to the Federal information systems that fall within FISMA under 44 U.S.C. §3543.

In the attached memorandum, DHS outlines a plan of action for agencies that will expedite the Executive Branch's full use of the PIV credentials for access to federal facilities and information systems. I ask for your help in overseeing your agency's implementation of this plan of action and your agency's completion of its adoption of the PIV credentials.

[1] HSPD-12, paragraph 4, requires that agencies use the identification standard to the maximum extent practicable; therefore, exceptions to using PIV credentials must be due to extenuating circumstances (e.g. system is in the process of being decommissioned.)

[2] Use of PIV credentials is not required for access to Federal applications where identity assurance is not needed (i.e. E-Authentication Assurance Level 1), such as low risk public-facing websites, blogs, etc. For additional information, refer to NIST Special Publication 800-63 at www.nist.gov.

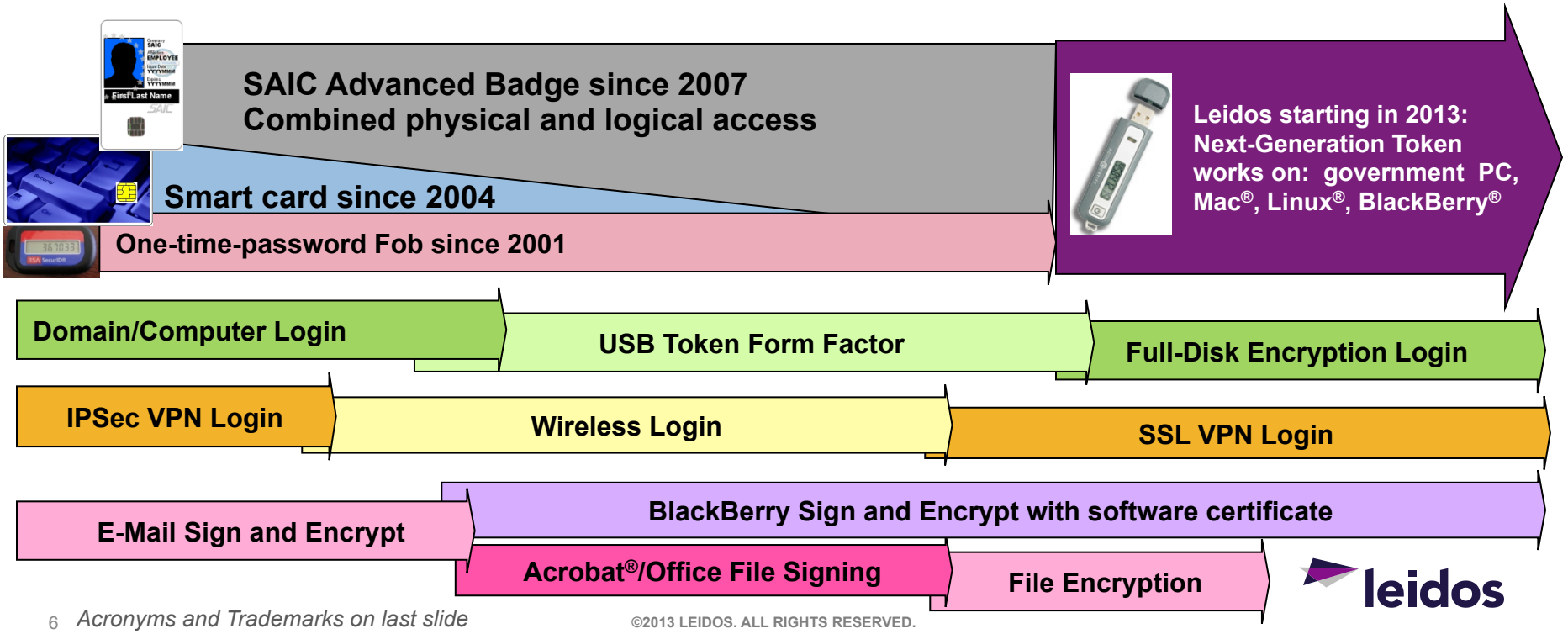
PIV provides a standard for badging and badge technology across the Federal government and DoD

 Acronyms and Trademarks on last slide

leidos

Ten Years of Smart Cards at Leidos (formerly SAIC)

- 2004: SAIC starts using smart cards
- 2007: SAIC Advanced badge modeled on CAC/PIV
- 2013: Leidos PIV-compatible Next-Generation Token
- Enterprise applications and capabilities enabled throughout
- Actively used by over 50% of employees



 Acronyms and Trademarks on last slide

Advanced Persistent Threat (APT)

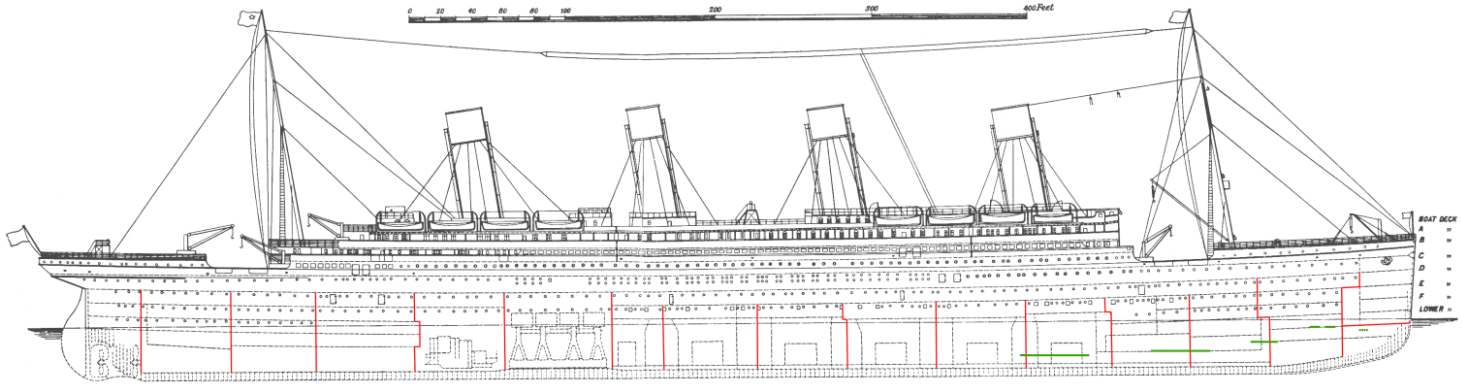
- **Sophisticated cyberattacks targeting governments and enterprises:**
  - **Advanced:** Uses advanced tools, techniques and procedures (TTPs) to penetrate the enterprise and gain control of infrastructure.
  - **Persistent:** Seeks to gain a foothold in the enterprise and maintain that foothold using stealth and flexibility.
  - **Threat:** Gains administrative control over the target so that they can copy, modify or delete data at will.
- **APT campaigns being widely conducted:**
  - By professional cyber-criminals to steal retail, banking and healthcare data for financial gain.
  - By intelligence operatives seeking to steal trade and national secrets from those who hold them.
  - By nation-state attackers seeking to gain political leverage against their adversaries.
- **This is not a hypothetical threat; it is real and it is upon us.**

 Acronyms and Trademarks on last slide

leidos

The APT Attack Sequence

1. **Use Malware to gain a foothold in the enterprise**
   - Exploit vulnerable servers, e-mail phishing, malicious web sites
2. **Establish command and control communications**
   - Use web server shells (webshell), reverse browsing, protocol tunneling
3. **Escalate privileges to gain control over target data**
   - Credential harvesting, keylogging, pass-the-hash
4. **Move laterally to find target systems and data**
   - Use mapping, remote shell, desktop, system administration tools
5. **Complete the Mission**
   - Exfiltrate, modify or destroy data on target systems



Acronyms and Trademarks on last slide

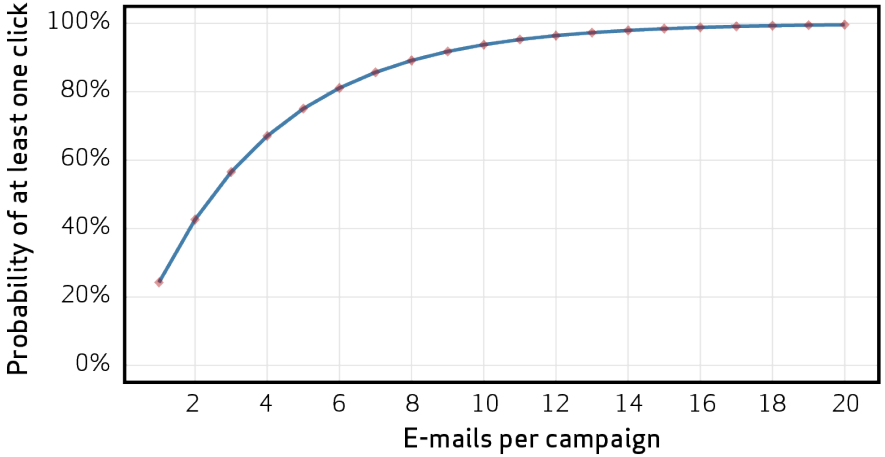
leidos

The Failure of Endpoint Security

- **The reality is that endpoints are *always* compromised:**

Home PCs	Enterprise PCs	Enterprise Servers
1 / 10	**1 / 100**	**1 / 1,000**

- **One cause is the "Inevitability of the Click":**



Source: Verizon
2013 Data Breach
Investigations Report

- **You can reduce these numbers but CANNOT eliminate them**

leidos

 Acronyms and Trademarks on last slide

Systems Administration Under Fire

- In the datacenter, technologies are stacked and interdependent
- More often than not, the administrator credentials are just passwords on the network
- Attackers can always go “lower in the stack” and bypass your security altogether
- Don’t need to find and exploit a vulnerability if you can steal the administrator credentials

Technology Stack	*Administration Stack*
End-User	User Credentials
Application	Application Admin
Database	Database Admin
Network & Net Security	Network Admin
Operating System	Operating System Admin Storage Area Network Admin
Drivers, Storage	
Virtualization (if present)	Virtualization Admin
Firmware / BIOS	Integrated Lights Out & Keyboard Video Mouse Admin
Hardware	Physical Access
Hardware Security Module / Crypto	Crypto Access

Acronyms and Trademarks on last slide

leidos

Mazes versus Minefields

Which is Scarier?

A Maze?

Or a Minefield?

Why are we building Mazes, then?

 Acronyms and Trademarks on last slide

Image sources: wikipedia.org; culturalmountains.org

leidos

Fighting APT with Smart Cards

- **Smart Cards are critical to APT defense:**
  1. Strong authentication for enterprise access from the Internet
  2. Strong authentication for privileged systems administration
  3. Encrypted e-mail capability while fighting incidents
- **To protect systems administration:**
  - Network isolation for servers and infrastructure
  - VPN or bastion hosts for system admins to get into isolated networks
  - Automated system rotates administrator passwords ***AT LEAST DAILY***
  - Two-factor authentication for all access and to get “password of the day”
  - Audit trails and alerts on system administrator activities
- **You can’t fight modern APTs without strong authentication**
  - Two-factor authentication for sysadmins even more important than two-factor authentication to the desktop

 Acronyms and Trademarks on last slide

leidos

Cyber Castles

- **We can learn from history by looking at medieval towns:**
  - Most of the productivity is in the undefended fields and village
  - The town is lightly defended, but the castle is heavily defended
  - To take the town, you have to control the castle

Tower = Authentication Systems

Castle = Security Systems

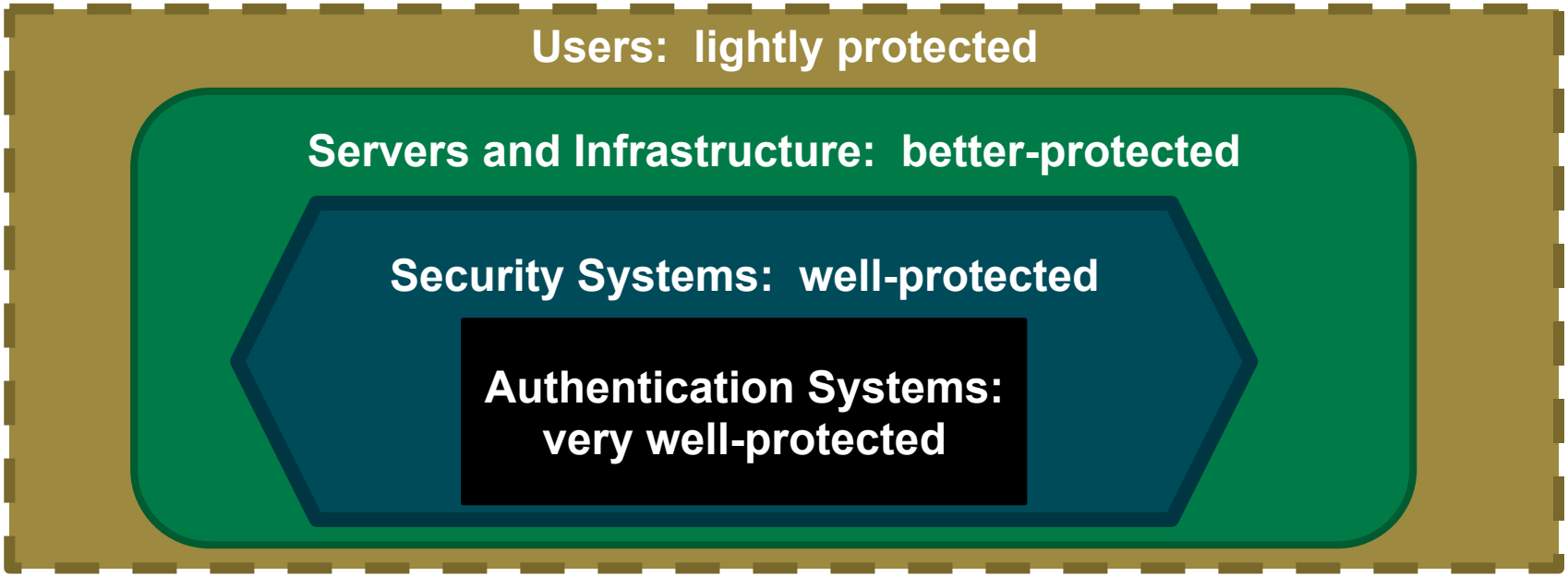
Town = Business Servers

Fields = Regular Users

leidos

True Defense in Depth

- Each layer gives defenders an opportunity to detect and repel attack
- Each layer's defense can be somewhat porous – perfection not required
- Defenses get stronger as attackers penetrate further inside
- Goal is to give defenders 2 or more opportunities to catch the attack



leidos

The Top 10 Features of a Next-Gen Defense

1. **Emphasis on detection** rather than protection
2. **Less reliance** on endpoint protection
3. **Network segmentation** to provide defense in depth
4. **Two-factor authentication** for system administrators
5. **Application whitelisting** for critical systems and assets
6. **Log aggregation** and security information and event management (SIEM)
7. **24x7 security monitoring** to detect incidents
8. **Forensics tools** to track down attacks when they occur
9. **Incident rapid response** to repel attacks in real time
10. **Security incident metrics** tracking activities and threats

leidos

Conclusion

- **PIV capabilities deliver significant business benefits**
  - Implementation is tricky, but cost-effective success is achievable
- **Strong Authentication is a critical part of APT defenses:**
  1. Multifactor authentication for access to enterprise from the Internet
  2. Multifactor authentication for systems administration
  3. E-mail encryption for incident response
- **APT protection depends on the 4 D's of Cyberdefense:**
  - **Disrupt** attacks from the Internet to keep casual and random attacks out
  - **Detect** attacks that successfully penetrate initial layers of defenses so that defenders can react
  - **Delay** attacks that are in-progress so that defenders have time to respond effectively
  - **Defeat** the attacks and send attackers back to their starting points

 Acronyms and Trademarks on last slide

leidos

Closing Thought

With a legacy cyber defense, the defender has to do everything perfectly to protect the enterprise.

With a next-generation cyber defense, the attacker has to do everything perfectly to attack it.

Which would you rather have?

leidos

Thanks!

Chris Williams
Chris.k.williams@leidos.com

Export Approval #
14-leidos-1016-1281

Acronyms and Trademarks

- AES = Advanced Encryption Standard
- BYOD = Bring Your Own Device
- CAC = Common Access Card
- CIV = Commercial Identity Verification
- DES = Data Encryption Standard
- ECA = External Certificate Authority
- FIPS = Federal Information Processing Standard
- FiXs = Federation for Identity and Cross-Credentialing Systems
- GSC-IS = Government Smart Card Interoperability Standard
- IT = Information Technology
- MD5 = Message Digest #5
- PC = Personal Computer
- NFC = Near Field Communication
- OTP = One Time Password
- PIV = Personal Identity Verification
- PIV-I = Personal Identity Verification – Interoperable
- PKI = Public Key Infrastructure
- RSA = Rivest Shamir Adleman
- SHA = Secure Hash Algorithm
- SSL = Secure Socket Layer
- TCO = Total Cost of Ownership
- TLS = Transport Layer Security
- UICC = Universal Integrated Circuit Card
- USB = Universal Serial Bus
- VPN = Virtual Private Network

- SecurID is a registered trademark of RSA, Inc.

leidos