Extending the Cybersecurity Digital Thread with XForms

Joshua Lubell
Balisage Markup Conference
August 2015

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

engineering laboratory

Disclaimer

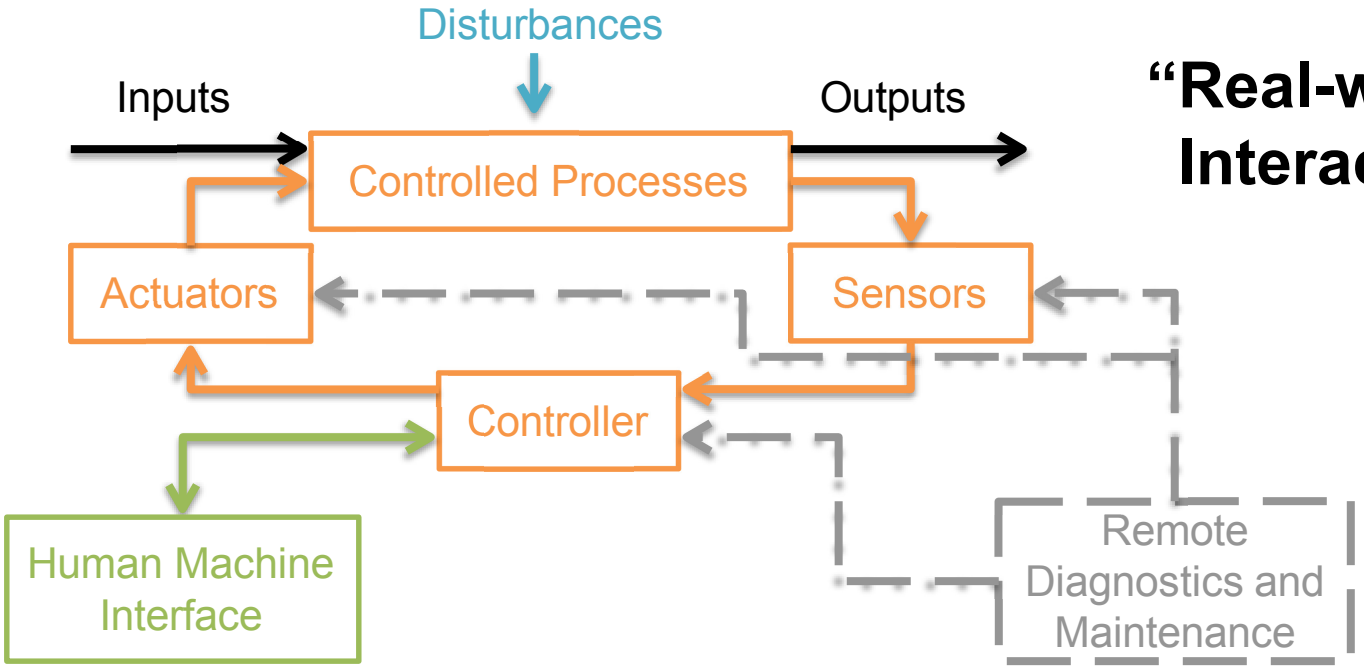
Certain commercial products are identified to help explain the research. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the products identified are necessarily the best available for the purpose.

Outline

- Cybersecurity digital thread and security control selection gap
- Existing guidance
- Security automation example
- Closing the gap
  - Technical approach
  - Demo!
- Conclusion and future work

Examples motivated by Industrial Control Systems security requirements

Industrial Control System



"Real-world" Interaction




Source: Victoria Yan Pillitteri, FCSPM Forum, June 2013

Critical Infrastructure

- US government definition*: "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."

* Executive Order no. 13636, *Improving Critical Infrastructure Cybersecurity*, DCPD-201300091, February 12, 2013. http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf

Some Recent Headlines

‘Car hacking’ just got real: In experiment, hackers disable SUV on busy highway

Topics: Cybersecurity | Networks, Datacenters &

Cyber attacks against industrial control systems, retailer point-of-sale systems see surge in 2014

April 13, 2015 | By Dibya Sarkar

Hacking the planet

The internet of things is coming. Now is the time to deal with its security flaws

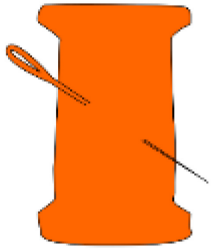
Jul 18th 2015 | From the print edition

Timekeeper Like 239 Tweet 158

- **ICSA-15-006-01** : **Eaton’s Cooper Power Serie Vulnerability**
  This advisory was originally posted to the US-CE released to the ICS-CERT web site. This advisor vulnerability in Eaton’s Cooper Power Systems F
  07/16/2015 - 11:54
- **ICSA-15-195-01** : **Siemens SICAM MIC Authen**
  This advisory provides mitigation details for an a device.
  07/14/2015 - 17:32
- **ICS-MM201506** : **May-June 2015**
  The NCCIC/ICS-CERT Monitor for May - June 2015 is a summary of ICS-CERT activities for that period of time.
  07/07/2015 - 10:52

A CYBERATTACK HAS CAUSED CONFIRMED PHYSICAL DAMAGE FOR THE SECOND TIME EVER

Cybersecurity Digital Thread



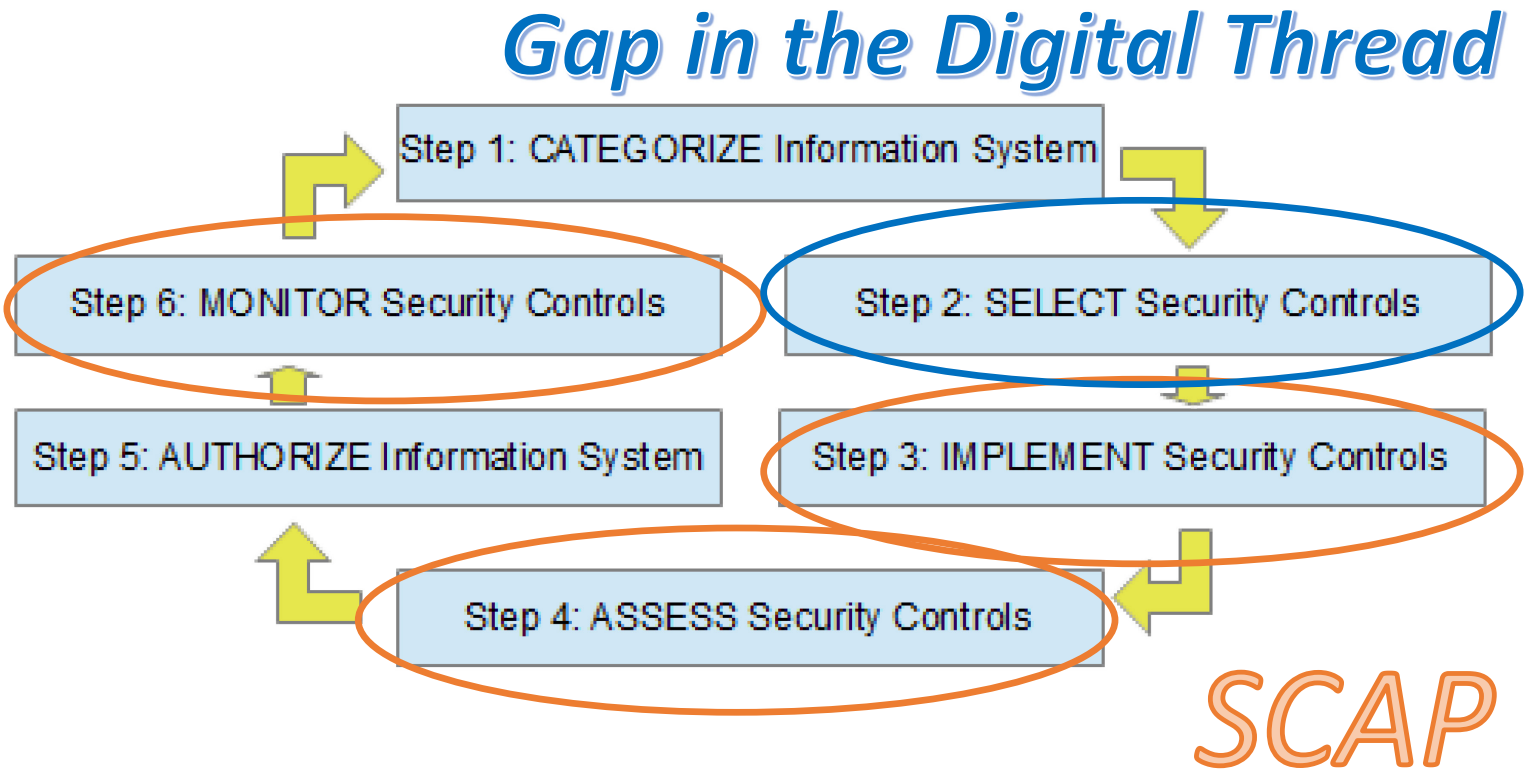
- Conveys the data flow between cyber-risk management activities
- Consists of standardized languages, data formats, taxonomies, metrics
- Requires infrastructure
  - Integration framework
  - Recommended practices
  - Reference data

} *SCAP*

SCAP (pronounced “ess-cap”)

- **S**ecurity **C**ontent **A**utomation **P**rotocol (scap.nist.gov)
- Provides order, infrastructure for an array of existing and emerging security content standards
  - Languages
  - Enumerations
  - Metrics
- Components
  - SCAP Specification, usage guide, and XML schema
  - National Vulnerability Database (nvd.nist.gov)
  - Validation program (scap.nist.gov/validation)

Cybersecurity Risk Management



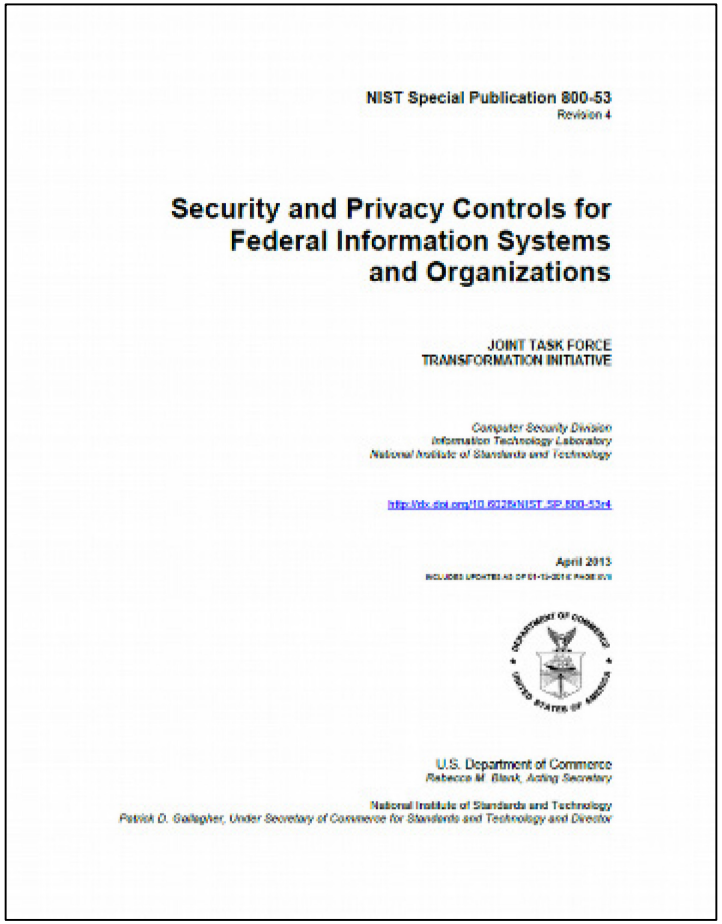
Outline

- Cybersecurity digital thread and security control selection gap
- Existing guidance
- Security automation example
- Closing the gap
  - Technical approach
  - Demo!
- Conclusion and future work

NIST SP 800-53, Revision 4

- Security and Privacy Controls for Federal Information Systems and Organizations
- Foundation of FISMA (Federal Information Security Management Act of 2002)
- Used in public and private sectors

Provides a comprehensive catalog of customizable, ***technology-neutral*** *security controls for organizations to manage cyber-risk*


NIST Special Publication 800-53
Revision 4

Security and Privacy Controls for Federal Information Systems and Organizations

JOINT TASK FORCE
TRANSFORMATION INITIATIVE

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology

http://dx.doi.org/10.6028/NIST.SP.800-53r4

April 2013

U.S. Department of Commerce
Rebecca M. Blank, Acting Secretary

National Institute of Standards and Technology
Patrick D. Gallagher, Under Secretary of Commerce for Standards and Technology and Director

SP 800-53 Security Control Baselines

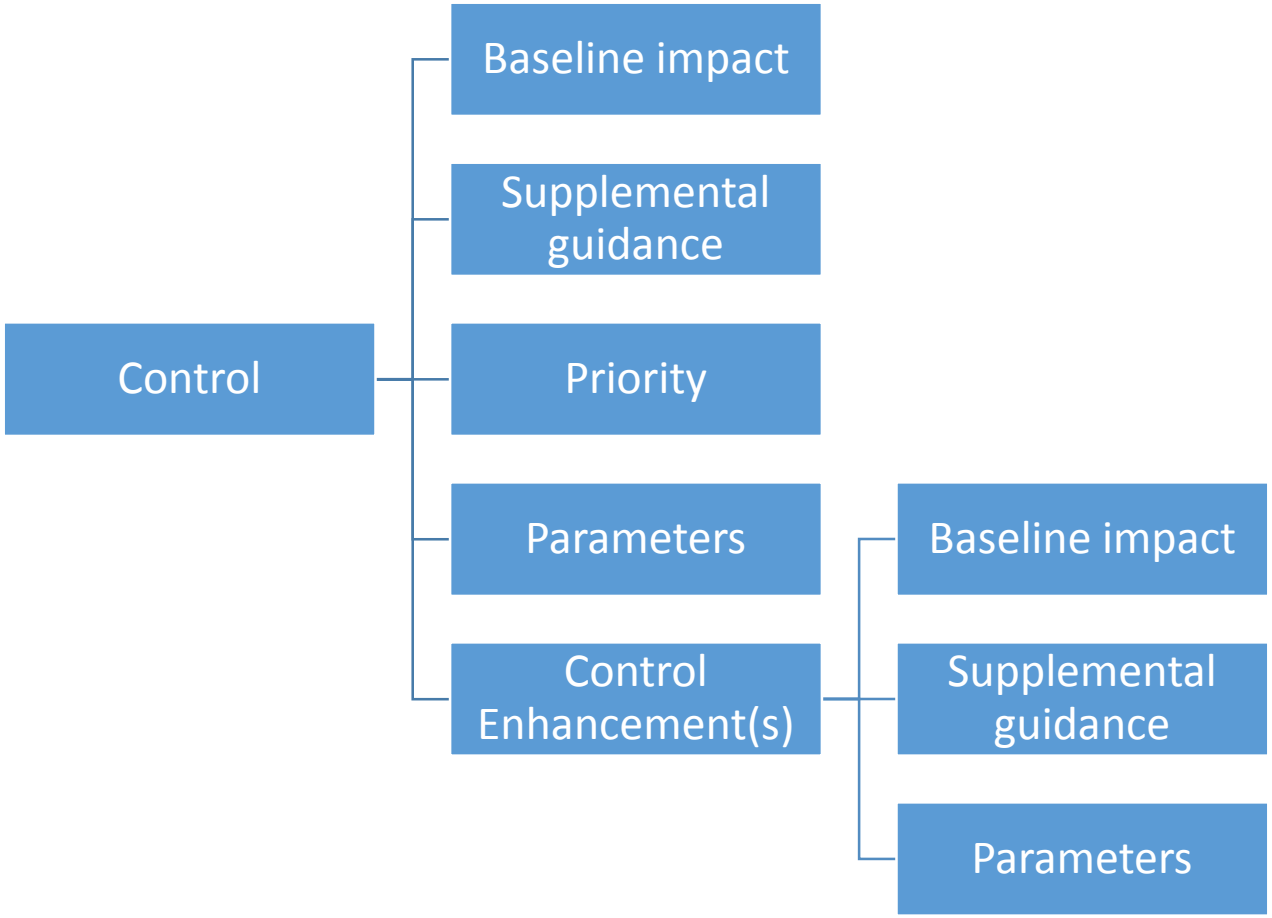
- Suggested “traditional” IT system defaults for Step 2 (SELECT Security Controls)
- For LOW, MODERATE, and HIGH impact systems
  - Impact determined in Step 1 of risk management process (CATEGORIZE Information System)
  - Based on consequences of loss of **confidentiality**, **integrity**, **availability**
- Organizations tailor baselines as appropriate
  - Confidentiality/integrity/availability requirements influence tailoring decisions
    - Example: Industrial Control Systems (ICS) often prioritize availability over confidentiality
  - LOW baseline (i.e., baseline for LOW impact systems) a typical starting point

Threat to Integrity *and* Availability

Security Control Families

ID	FAMILY	ID	FAMILY
AC	Access Control	MP	Media Protection
AT	Awareness and Training	PE	Physical and Environmental Protection
AU	Audit and Accountability	PL	Planning
CA	Security Assessment and Authorization	PS	Personnel Security
CM	Configuration Management	RA	Risk Assessment
CP	Contingency Planning	SA	System and Services Acquisition
IA	Identification and Authentication	SC	System and Communications Protection
IR	Incident Response	SI	System and Information Integrity
MA	Maintenance	PM	Program Management

Security Control Structure



Baselines for IA Family

ID	Control Name	LOW	MODERATE	HIGH
IA-1	Identification and Authentication Policy and Procedures	IA-1	IA-1	IA-1
IA-2	Identification and Authentication (Organizational Users)	IA-2 (1) (12)	IA-2 (1) (2) (3) (8) (11) (12)	IA-2 (1) (2) (3) (4) (8) (9) (11) (12)
IA-3	Device Identification and Authentication	Not Selected	IA-3	IA-3
IA-4	Identifier Management	IA-4	IA-4	IA-4
IA-5	Authenticator Management	IA-5 (1) (11)	IA-5 (1) (2) (3) (11)	IA-5 (1) (2) (3) (11)
IA-6	Authenticator Feedback	IA-6	IA-6	IA-6
IA-7	Cryptographic Module Authentication	IA-7	IA-7	IA-7
IA-8	Identification and Authentication (Non-Organizational Users)	IA-8 (1) (2) (3) (4)	IA-8 (1) (2) (3) (4)	IA-8 (1) (2) (3) (4)

Example: Tailoring IA-3

IA-3	Device Identification and Authentication	**Added**	IA-3	IA-3

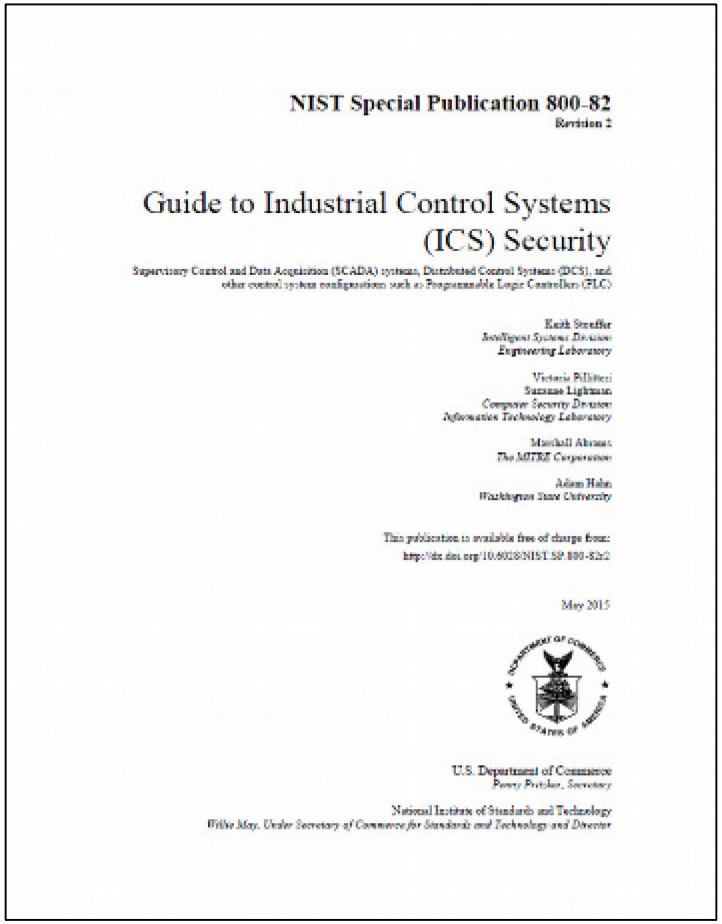
- IA-3 pertains to identifying and authenticating devices before connecting to them
- Default assumption: low-impact systems do not connect directly to devices external to the organization
- But an ICS may need to connect directly to devices belonging to and authorized by business partners
- **Rationale for changing LOW baseline**: these external devices require proper identification and authentication

Other Tailoring Operations

- Assign/select parameter values
  - From IA-3 description: "The information system uniquely identifies and authenticates [Assignment: organization-defined specific and/or types of devices] before establishing a [Selection (one or more): local; remote; network] connection."
- Add additional supplementary guidance
  - ICS Example (IA-3): "The organization may permit connection of devices, also known as non-person entities (NPE), belonging to and authorized by another organization (e.g., business partners) to their ICS. Especially when these devices are non-local, their identification and authentication can be vital. Organizations may perform risk and impact analysis to determine the required strength of authentication mechanisms. Example compensating controls for devices and protocols which do not provide authentication for remote network connections, include implementing physical security measures."

Overlays

- Set of control customizations applicable to a group of organizations with common security requirements
- Example: NIST SP 800-82 (Guide to ICS Security) overlay
  - Source of previous IA-3 tailoring
- Other overlays
  - Cloud computing
  - Mobile devices
  - Smart Grid



NIST Special Publication 800-82
Revision 2

Guide to Industrial Control Systems (ICS) Security

Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC)

Keith Stouffer
Intelligent Systems Division
Engineering Laboratory

Victoria Pillitteri
Suzanne Lightman
Computer Security Division
Information Technology Laboratory

Marshall Abrams
The MITRE Corporation

Adam Hahn
Washington State University

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-82r2

May 2015

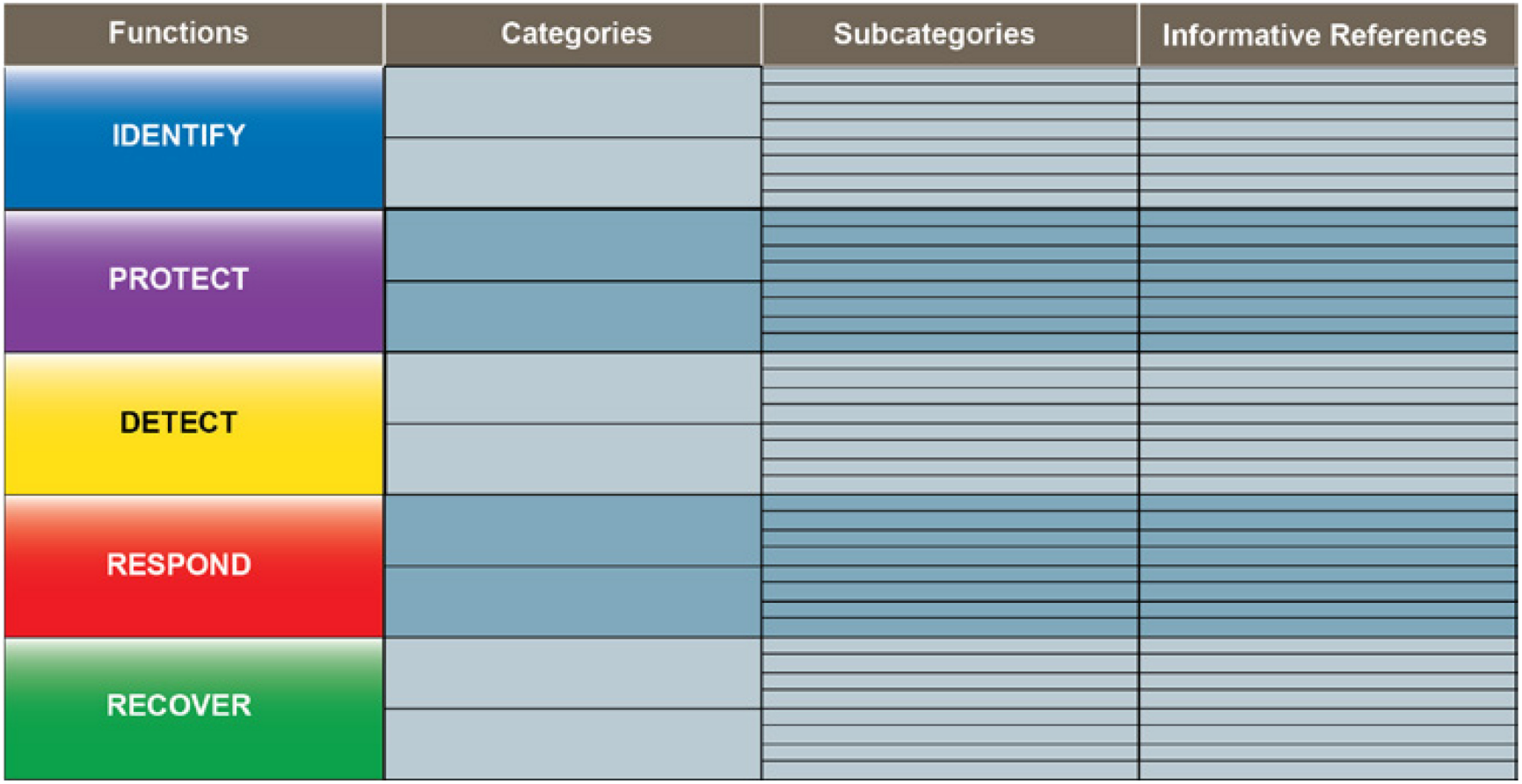
U.S. Department of Commerce
Penny Pritzker, Secretary

National Institute of Standards and Technology
Willie May, Under Secretary of Commerce for Standards and Technology and Director

US Cybersecurity Framework

- "Framework for Improving Critical Infrastructure Cybersecurity," Version 1.0 (February 2014)
- Provides mechanism for organizations to:
  - Describe current cybersecurity posture and target state
  - Identify opportunities for improvement
  - Assess progress
  - Communicate with stakeholders
- Used by large and small businesses, organizations, governments – domestic and international
- Core: set of cybersecurity activities and references common across critical infrastructure sectors and organized around particular outcomes

Framework Core Structure

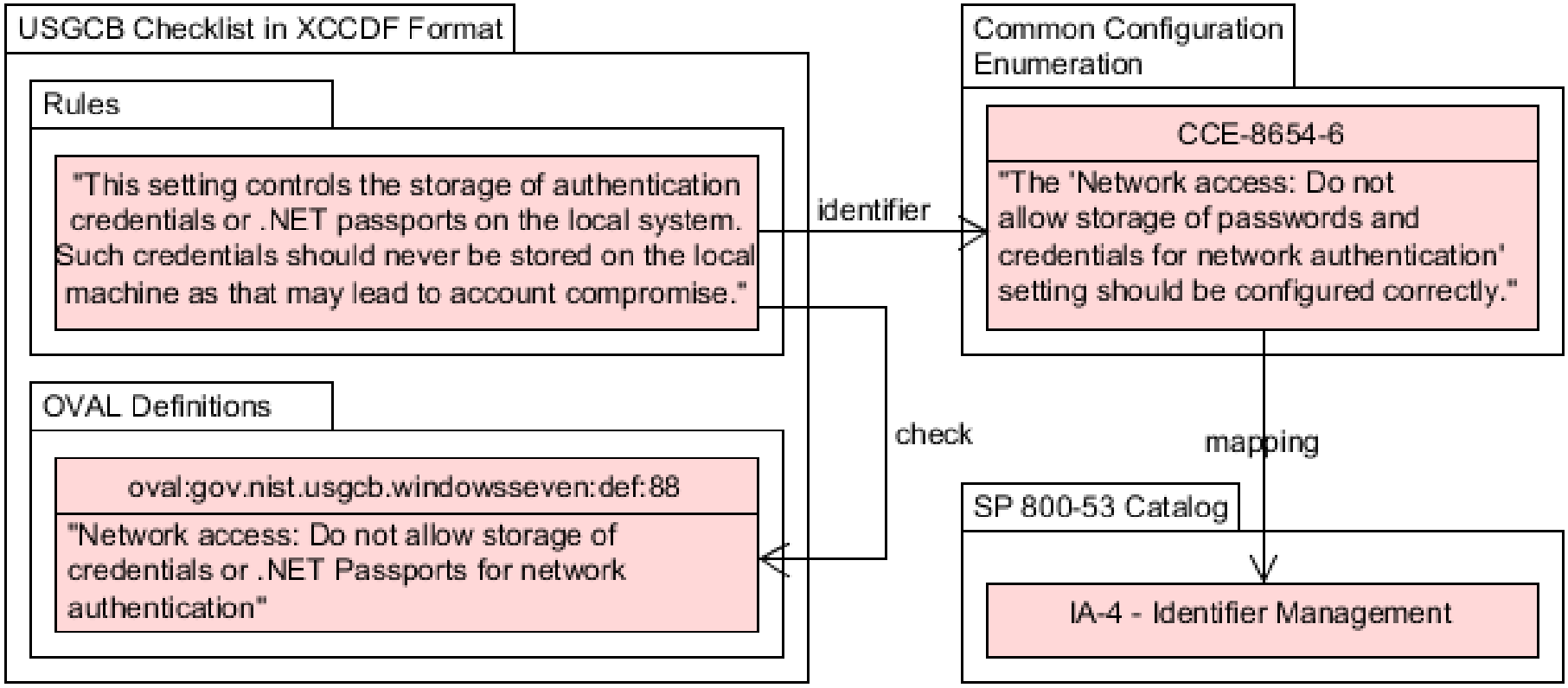


Outline

- Cybersecurity digital thread and security control selection gap
- Existing guidance
- Security automation example
- Closing the gap
  - Technical approach
  - Demo!
- Conclusion and future work

- Repository of SCAP-based vulnerability data
- Vulnerability severity scoring calculator
- Searchable SP 800-53 security control catalog in XML format
- Repository of checklists (benchmarks)
- Data feed mapping system configurations to relevant security controls

Example: Automated Security Check



Common Configuration Enumeration entry mapping to IA-4

```
<entry xmlns="http://scap.nist.gov/schema/feed/configuration/0.1"
  xmlns:config="http://scap.nist.gov/schema/configuration/0.1"
  xmlns:scap-core="http://scap.nist.gov/schema/scap-core/0.3"
  id="CCE-8654-6">
  <config:cce-id>CCE-8654-6</config:cce-id>
  <config:published-datetime>...</config:published-datetime>
  <config:last-modified-datetime>...</config:last-modified-datetime>
  <config:summary>...</config:summary>
  <scap-core:control-mappings>
    <scap-core:control-mapping system-id="http://csrc.nist.gov/..."
      source="http://nvd.nist.gov/" last-modified="...">
     <scap-core:mapping published="...">IA-4</scap-core:mapping>
    </scap-core:control-mapping>
  </scap-core:control-mappings>
</entry>
```

Checklist rule mapping to CCE-8654-6

```
<xccdf:Rule xmlns:xccdf="http://checklists.nist.gov/xccdf/1.2">
  <xccdf:title>Network access: Do not allow storage...</xccdf:title>
  <xccdf:description>This setting controls the...</xccdf:description>
  <xccdf:reference>...</xccdf:reference>
  <xccdf:ident system="http://cce.mitre.org">CCE-8654-6</xccdf:ident>
  <xccdf:check system="http://oval.mitre.org/...">...</xccdf:check>
</xccdf:Rule>
```

Takeaways

- Executable checklists enable automated security checking
- National Vulnerability Database provides SCAP checklists, reference data, online tools
- Mappings from common OS configurations to SP 800-53 security controls provide compliance evidence, traceability

Takeaways: Cyber Framework

- Multiple levels of abstraction make it useful for CEOs and cybersecurity experts alike
- Informative references guide application of standards and provide traceability to requirements
- ***But the Cyber Framework lacks an SCAP-friendly computer-readable format***

Takeaways: SP 800-53

- Tailorable security controls are essential to accommodating diverse requirements
- Security control catalog has a hierarchical structure
- Tailored baselines and overlays require additional structure
- XML representation of catalog enables navigation, search, cross-referencing
- ***But no XML format exists for tailored baselines or overlays***

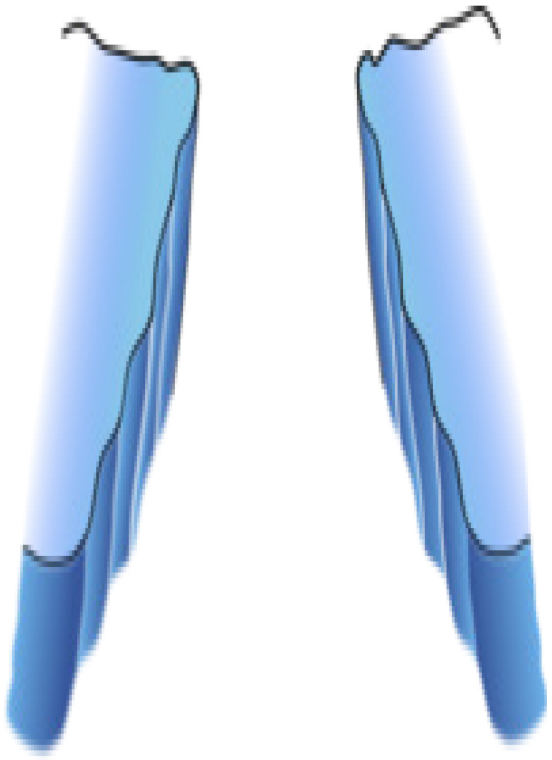
Incompatible Representations

- NIST SP 800-82 Industrial Control System overlay documented as a series of tables
- Tailored baselines for mobile devices and cloud computing services each documented as spreadsheets
- All use divergent documentation conventions
- None are easy for cybersecurity practitioners to navigate or for software developers to implement with SCAP

Outline

- Cybersecurity digital thread and security control selection gap
- Existing guidance
- Security automation example
- Closing the gap
  - Technical approach
  - Demo!
- Conclusion and future work

Closing the Gap: It's All About the Data



- XML formats for Small Arcane Nontrivial Datasets (SANDs)
  - Tailored security control
  - Framework Core
- XML technologies
  - XSLT – make existing data more useful
  - XForms – implement user interfaces for SANDs
- Guiding principles
  - Minimize maintenance
  - Keep it simple
  - Minimize IT requirements

SANDs

- They're everywhere
  - But most noticeable to people who deal with a particular SAND on a regular basis
- Cumbersome to navigate without specialized software
  - But optimal software often lacking for access and editing
  - Weak business case for developing killer app
- Excel often used
  - Fine if data is naturally tabular
  - Suboptimal for handling cross-references, hierarchies, inheritance
- For more details
  - Lubell, J. "XForms User Interfaces for Small Arcane Nontrivial Datasets." In *Proceedings of Balisage: The Markup Conference 2014*. Balisage Series on Markup Technologies, vol. 13 (2014). doi:10.4242/BalisageVol13.Lubell01.

XForms

- W3C XML language for specifying forms for the Web
- Great if data natively in XML, or easily convertible to XML
- Declarative – no scripting required
- Minimizes browser and OS dependencies
- Promotes software longevity
- Adopts model-view-controller (MVC) software pattern
- Well-suited for specifying user interfaces for SANDs

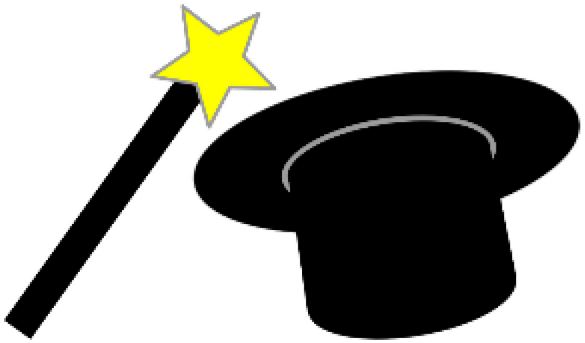
New XML Formats Developed

- Tailored security control
  - Represents modifications to NIST SP 800-53 baselines when combined with National Vulnerability Database security control catalog XML data
  - Generated via XForms user interface
- Framework Core
  - Hierarchically represents information content from table in Cyber Framework document
  - Generated via XSLT 2.0 from Filemaker Pro runtime database output*

* http://www.nist.gov/cyberframework/csf_reference_tool.cfm

XForms User Interface: “Baseline Tailor”

- Navigate Framework Core and SP 800-53 cross references
- Tailor security controls for inclusion in baselines and/or overlays
- Generate tailored security control XML output in accordance with SP 800-53

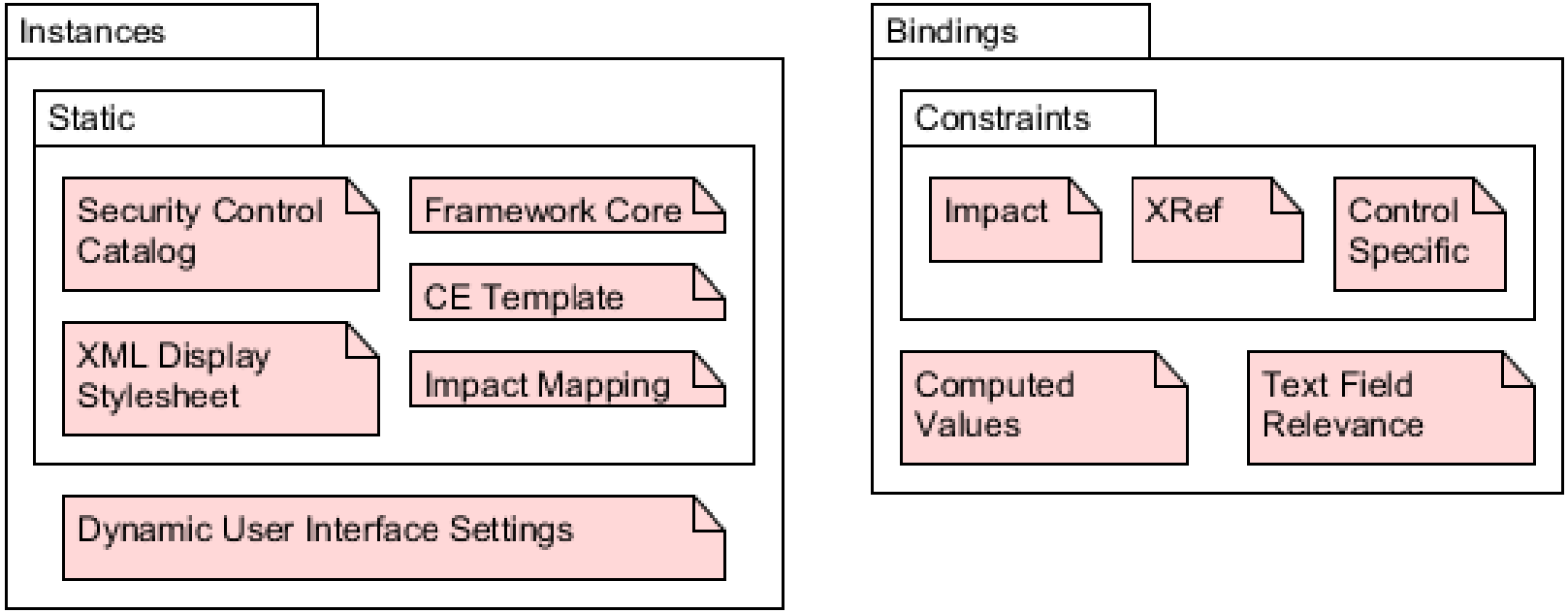


Demo

Baseline Tailor Implementation

- Source code is 100% XML (XForms, XSLT, XHTML)
- Uses XSLTForms XForms processor (http://www.agencexml.com/xsltforms)
- All processing client side
- Runs in common browsers (Chrome, Firefox, Safari, IE, …)
- Can be run from local file system without HTTP server

Baseline Tailor XForms Model



Outline

- Cybersecurity digital thread and security control selection gap
- Existing guidance
- Security automation example
- Closing the gap
  - Technical approach
  - Demo!
- Conclusion and future work

Summary

- SCAP enables cybersecurity digital thread
- Lack of software support for SP 800-53 security control selection is a gap in the digital thread
  - Barrier to implementation of tailored baselines, overlays
- Software-friendly structured data formats for framework core and tailored controls can help close the gap
- Baseline Tailor software tool
  - Provides a specialized user interface for tailoring security controls
  - Enforces NIST SP 800-53 tailoring guidelines
  - Generates XML content suitable for automated processing by other cybersecurity tools

Limitations of Baseline Tailor

- Lack of ability to import an existing tailored control
  - Needed for composability (e.g., tailoring an overlay)
- Lack of support for NIST SP 800-53 assignment and selection parameters
  - Example from IA-3 description: "The information system uniquely identifies and authenticates [Assignment: organization-defined specific and/or types of devices] before establishing a [Selection (one or more): local; remote; network] connection."

Ongoing and Future Efforts

- Industrial Control Systems cybersecurity testbed
  - Will use XML generated by Baseline Tailor to represent ICS overlay
  - Will use SCAP-represented checklists
- Alternatives to XForms
  - Recent advances in HTML5 single-page application technologies show promise
  - But handling mixed content such as parameters embedded in descriptive text could be challenging
  - NIST developing prototype implementation using AngularJS