IDS WG Meeting Minutes
March 23, 2023

This IDS WG Meeting was started at approximately 3:00 pm ET on March 23, 2023.

Attendees

Graydon Dodson	Lexmark
Jeremy Leber	Lexmark
Alan Sukert	
Brian Volkoff	Ricoh
Steve Young	Canon

Agenda Items

1. The topics to be covered during this meeting were:
    - Latest status on the HCD iTC
    - Special topics on ETSI TR 103 305-1 V2.1.1 and a comparison between ETSI TR 103 305-1 V2.1.1 and the NIST Cybersecurity Framework.
    - Round Table
2. Meeting began by stating the PWG Anti-Trust Policy which can be found at https://www.pwg.org/chair/membership_docs/pwg-antitrust-policy.pdf and the PWG Intellectual Property Policy which can be found at https://www.pwg.org/chair/membership_docs/pwg-ip-policy.pdf.
3. Al gave a quick status of the HCD iTC.
    - NIAP and ITSCC are still reviewing the documents. ITSCC indicated that they should complete review of the HCD SD v1.0 by Oct 2023. Kwangwoo will check the current status with the ITSCC and Jonghong to follow up the SD approval by the next CCDB meeting (Target date: 11th April 2023)
    - There was a CCDB-CCUF Joint Session Update as part of the CCUF Workshop held Mar 8-9. Al missed the workshop because he was on vacation. However, Kwangwoo Lee will share the CCDB/CCUF Joint Session recording to the HCD iTC members (Youtube channel). Al indicated he will share the link with IDS members as soon as he gets the recording from Kwangwoo.
    - The detailed Transition Policy and guidance of transitioning from CC3.1R5 to CC:2022 will be published by Q2, Q3 2023. This is under the voting process by the CCDB/CCMC, so it could take a while.
    - Kwangwoo indicated that the EC Cybersecurity Implement Act is under legal review at the current time.
    - The next HCD iTC Meeting is scheduled for 10 April 2022 / US 19:00 – 20:00; 11 April 2023 08:00-09:00 / KST, JST
    - Al indicated he will have a meeting of the HIT next week. Al then asked Graydon about Lexmark's plans to certify one or more MFPs in Canada against the HCD cPP v1.0 now that Canada has posted an Endorsement Statement for the HCD cPP. Graydon indicated that Lexmark plans to do the certifications as soon as they can, although the fact that Lexmark is using a new lab and a new cPP will slow things done a little bit.

      During the discussion Graydon indicated that Lexmark had found a disconnect in the HCD cPP KeyWrap SFRs with the TPM Standard. Specifically, the TPM Standard allows CFB mode but the KeyWrap SFR in the HCD cPP does not allow this mode. Lexmark found a work-around for this issue, but this disconnect does need to be addressed.

      Al indicated that this is the kind of issue that needs to be brought to the HIT to determine whether to address in v1.0 or pass it on to the full HCD iTC to address in v1.1. Graydon indicated that once he has time to put the full facts together he will submit the Request for Interpretation to the HIT.

4. Al presented the first of this week's special topics on ETSI TR 103 305-1 V2.1.1 CYBER; Critical Security Controls for Effective Cyber Defence; Part 1: The Critical Security Controls. The slides Al used can be found at https://ftp.pwg.org/pub/pwg/ids/Presentation/ETSI TR 103 305-1.pdf.

   The main items covered in the presentation were:

   - ETSI TR 103 305-1 V2.1.1 was published in August 2016 and can be found at https://www.etsi.org/deliver/etsi_tr/103300_103399/10330501/03.01.01_60/tr_10330501v030101p.pdf.

     It was developed and maintained by the Center for Internet Security (CIS) and describes a specific set of technical measures available to detect, prevent, respond, and mitigate damage from the most common to the most advanced of cyber attacks

     The Security Controls in the Technical Report are designed to:

     - Block the initial compromise of systems
     - Address detecting already-compromised machines and preventing or disrupting attackers' follow-on actions
     - Reduce the initial attack surface by hardening device configurations
     - Identify compromised machines to address long-term threats inside an organization's network
     - Disrupting attackers' command-and-control of implanted malicious code
     - Establish an adaptive, continuous defence and response capability that can be maintained and improved
     - The five critical tenets of an effective cyber defence system as reflected in the Critical Security Controls are:
     - Offense informs defence: Use knowledge of actual attacks that have compromised systems to provide the foundation to continually learn from these events to build effective, practical defences. Include only those controls that can be shown to stop known real-world attacks
     - Prioritization: Invest first in Controls that will provide the greatest risk reduction and protection against the most dangerous threat actors, and that can be feasibly implemented in a computing environment
     - Metrics: Establish common metrics to provide a shared language for executives, IT specialists, auditors, and security officials to measure the effectiveness of security measures within an organization so that required adjustments can be identified and implemented quickly

       Al noted that the EU is very big on metrics and measures.
     - Continuous diagnostics and mitigation: Carry out continuous measurement to test and validate the effectiveness of current security measures, and to help drive the priority of next steps
     - Automation: Automate defences so that organizations can achieve reliable, scalable, and continuous measurements of their adherence to the Controls and related metrics

       Al noted that the EU is also very big on automation and that will be visible throughout this TR.

   - The only definition included in the TR was:

     Critical Security Control (CSC): Specified capabilities that reflect the combined knowledge of actual attacks and effective defences of experts that are maintained by the Center for Internet Security

     Al noted that this really wasn't much of a definition.

   - The following 20 Critical Security Controls are defined in ETSI TR 103 305-1:

- **CSC 1: Inventory of Authorized and Unauthorized Devices**: *Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access*

  This is managing the hardware devices one has on the network
- **CSC 2: Inventory of Authorized and Unauthorized Software**: *Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution*

  This is managing the software on the network
- **CSC 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers**: *Establish, implement, and actively manage (track, report on, correct) the security configuration of laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings*

  This is ensuring that there is a known secure configuration for every device that in continuously managed
- **CSC 4: Continuous Vulnerability Assessment and Remediation**: *Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers*
- **CSC 5: Controlled Use of Administrative Privileges**: *The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications*

  This is managing admin privileges to all devices and network. Note this is different from managing admin credentials which is what we do for HCDs.
- **CSC 6: Maintenance, Monitoring, and Analysis of Audit Logs**: *Collect, manage, and analyze audit logs of events that could help detect, understand or recover from an attack*

  This is similar to the audit log SFRs in the HCD cPP
- **CSC 7: Email and Web Browser Protections**: *Minimize the attack surface and the opportunities for attackers to manipulate human behavior though their interaction with web browsers and email systems*

  Email and web browser protection is something that Al hasn't seen in similar cybersecurity frameworks or controls
- **CSC 8: Malware Defenses**: *Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defense, data gathering, and corrective action*

  Similar to CSC 7, this is something that AL Hasn't specifically seen in other cybersecurity controls
- **CSC 9: Limitation and Control of Network Ports, Protocols, and Services**: *Manage (track/control/correct) the ongoing operational use of ports, protocols, and services on networked devices in order to minimize windows of vulnerability available to attackers*

  Al indicated this is something important that he was glad was in here and should be in similar cybersecurity control schemes
- **CSC 10: Data Recovery Capability**: *The processes and tools used to properly back up critical information with a proven methodology for timely recovery of it*

  Al indicated that from his experience at Xerox backups are very important
- **CSC 11: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches**: *Establish, implement, and actively manage (track, report on, correct) the security configuration of network infrastructure devices using a rigorous configuration management*

and change control process in order to prevent attackers from exploiting vulnerable services and settings

Similar to CSC7 and CSC8 this is something Al has not seen in similar cybersecurity control schemes

- **CSC 12: Boundary Defense**: *Detect/prevent/correct the flow of information transferring networks of different trust levels with a focus on security damaging data*

  This is something unique
- **CSC 13: Data Protection**: *The processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information*

  It is interesting that this is stated at such a high level rather than protecting data at rest or data in transit
- **CSC 14: Controlled Access Based on the Need to Know**: *The processes and tools used to track/control/prevent/correct secure access to critical assets (e.g., information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification*

  Al noted that this CSC applies not only to data but also to documents
- **CSC 15: Wireless Access Control**: *The processes and tools used to track/control/prevent/correct the security use of wireless local area networks (LANs), access points, and wireless client systems*

  Al felt it was important that wireless was specifically separated out given how widespread it is being used
- **CSC 16: Account Monitoring and Control**: *Actively manage the life cycle of system and application accounts - their creation, use, dormancy, deletion - in order to minimize opportunities for attackers to leverage them*

  The key of this CSC is that it is monitoring and control user accounts themselves and not the user credentials associated with those accounts
- **CSC 17: Security Skills Assessment and Appropriate Training to Fill Gaps**: *For all functional roles in the organization (prioritizing those mission-critical to the business and its security), identify the specific knowledge, skills, and abilities needed to support defense of the enterprise; develop and execute an integrated plan to assess, identify gaps, and remediate through policy, organizational planning, training, and awareness programs*

  This CSC is fairly straightforward
- **CSC 18: Application Software Security**: *Manage the security life cycle of all in-house developed and acquired software in order to prevent, detect, and correct security weaknesses*

  This is very similar to what is required for EAL3 and above
- **CSC 19: Incident Response and Management**: *Protect the organization's information, as well as its reputation, by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications, management oversight) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and systems*

  Similar to what most other control schemes have
- **CSC 20: Penetration Tests and Red Team Exercises**: *Test the overall strength of an organization's defenses (the technology, the processes, and the people) by simulating the objectives and actions of an attacker*

  Unusual to explicitly require penetration testing

- For each Critical Security Control there are one or more controls presented in the slides. They will not all be included in these notes (see the slides for the full list for each CSC); only the specific ones that Al pointed out during the discussion at the meeting will be included in the minutes.

  CSC 1: Inventory of Authorized and Unauthorized Devices

  - Deploy an automated asset inventory discovery tool and use it to build a preliminary inventory of systems connected to an organization's public and private network(s).
  - Ensure that all equipment acquisitions automatically update the inventory system as new, approved devices are connected to the network.
  - Maintain an asset inventory of all systems connected to the network and the network devices themselves, recording at least the network addresses, machine name(s), purpose of each system, an asset owner responsible for each device, and the department associated with each device. The inventory should include every system that has an Internet protocol (IP) address on the network, including but not limited to desktops, laptops, servers, network equipment (routers, switches, firewalls, etc.), printers, storage area networks, Voice Over-IP telephones, multi-homed addresses, virtual addresses, etc. The asset inventory created should also include data on whether the device is a portable and/or personal device. Devices such as mobile phones, tablets, laptops, and other portable electronic devices that store or process data should be identified, regardless of whether they are attached to the organization's network.
  - Deploy network level authentication via 802.1x to limit and control which devices can be connected to the network. The 802.1x should be tied into the inventory data to determine authorized versus unauthorized systems

  As stated earlier, the use of automation is very important to the EU as is automatic update of inventory. The key is to maintain the asset inventory of all systems connected to the network and the network devices themselves and keep it up-to-date and accurate.

  CSC 2: Inventory of Authorized and Unauthorized Software

  - Devise a list of authorized software and version that is required in the enterprise for each type of system, including servers, workstations, and laptops of various kinds and uses. This list should be monitored by file integrity checking tools to validate that the authorized software has not been modified.
  - Deploy software inventory tools throughout the organization covering each of the operating system types in use, including servers, workstations, and laptops. The software inventory system should track the version of the underlying operating system as well as the applications installed on it. The software inventory systems should be tied into the hardware asset inventory so all devices and associated software are tracked from a single location.

  Again, list for CSC 1 the key is to maintain a list of authorized software and version and keep it up-to-date and accurate.

  CSC 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

  - Establish standard secure configurations of operating systems and software applications. Standardized images should represent hardened versions of the underlying operating system and the applications installed on the system. These images should be validated and refreshed on a regular basis to update their security configuration in light of recent vulnerabilities and attack vectors.
  - Follow strict configuration management, building a secure image that is used to build all new systems that are deployed in the enterprise. Any existing system that becomes compromised should be re-imaged with the secure build. Regular updates or exceptions to this image should be integrated into the organization's change management processes. Images should be created for workstations, servers, and other system types used by the organization.

- Store the master images on securely configured servers, validated with integrity checking tools capable of continuous inspection, and change management to ensure that only authorized changes to the images are possible.
- Perform all remote administration of servers, workstation, network devices, and similar equipment over secure channels. Protocols such as telnet, VNC, RDP, or others that do not actively support strong encryption should only be used if they are performed over a secondary encryption channel, such as SSL, TLS or IPSEC.
- Implement and test an automated configuration monitoring system that verifies all remotely testable secure configuration elements, and alerts when unauthorized changes occur.

Note again the heavy reliance on automation and the importance, like CSC 1 and CSC 2, of establishing and maintaining the standard secure configurations of operating systems and software applications.

CSC 4: Continuous Vulnerability Assessment and Remediation

- Run automated vulnerability scanning tools against all systems on the network on a weekly or more frequent basis and deliver prioritized lists of the most critical vulnerabilities to each responsible system administrator along with risk scores that compare the effectiveness of system administrators and departments in reducing risk. Use a SCAP-validated vulnerability scanner that looks for both code-based vulnerabilities (such as those described by Common Vulnerabilities and Exposures entries) and configuration-based vulnerabilities (as enumerated by the Common Configuration Enumeration Project).
- Correlate event logs with information from vulnerability scans to fulfil two goals. First, personnel should verify that the activity of the regular vulnerability scanning tools is itself logged. Second, personnel should be able to correlate attack detection events with prior vulnerability scanning results to determine whether the given exploit was used against a target known to be vulnerable.
- Subscribe to vulnerability intelligence services in order to stay aware of emerging exposures, and use the information gained from this subscription to update the organization's vulnerability scanning activities on at least a monthly basis. Alternatively, ensure that the vulnerability scanning tools used are regularly updated with all relevant important security vulnerabilities.
- Deploy automated patch management tools and software update tools for operating system and software/applications on all systems for which such tools are available and safe. Patches should be applied to all systems, even systems that are properly air gapped.
- Establish a process to risk-rate vulnerabilities based on the exploitability and potential impact of the vulnerability, and segmented by appropriate groups of assets (example, DMZ servers, internal network servers, desktops, laptops). Apply patches for the riskiest vulnerabilities first. A phased rollout can be used to minimize the impact to the organization. Establish expected patching timelines based on the risk rating level

These controls are the type of controls one would expect for vulnerability assessment and remediation. Al especially liked the “Subscribe to vulnerability intelligence services…” control because it is important to keep on top of what the current vulnerabilities are for the software ant system has.

CSC 5: Controlled Use of Administrative Privileges

- Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.
- Use automated tools to inventory all administrative accounts and validate that each person with administrative privileges on desktops, laptops, and servers is authorized by a senior executive.

- Before deploying any new devices in a networked environment, change all default passwords for applications, operating systems, routers, firewalls, wireless access points, and other systems to have values consistent with administration-level accounts.
- Use multi-factor authentication for all administrative access, including domain administrative access. Multi-factor authentication can include a variety of techniques, to include the use of smart cards, certificates, One Time Password (OTP) tokens, biometrics, or other similar authentication methods.
- Where multi-factor authentication is not supported, user accounts should be required to use long passwords on the system (longer than 14 characters)

As Al stated above the focus here is on the admin accounts themselves rather than on the admin privileges that HCDs focus on. The control to "change all default passwords for applications, operating systems, routers, firewalls, wireless access points, and other systems" when deploying a new device is interesting but might be difficult to implement for an enterprise which large numbers of network devices. Similarly, the requirement to use multi-factor authentication for admin access is a good idea but might again be difficult to implement for enterprises with large numbers of network devices. Finally, Al wondered why the requirement in case no multi-factor authentication was possible was for a long password rather than for a strong password like we required for HCDs.

CSC 6: Maintenance, Monitoring, and Analysis of Audit Logs

- Include at least two synchronized time sources from which all servers and network equipment retrieve time information on a regular basis so that timestamps in logs are consistent.
- Validate audit log settings for each hardware device and the software installed on it, ensuring that logs include a date, timestamp, source addresses, destination addresses, and various other useful elements of each packet and/or transaction. Systems should record logs in a standardized format such as syslog entries or those outlined by the Common Event Expression initiative. If systems cannot generate logs in a standardized format, log normalization tools can be deployed to convert logs into such a format.
- Ensure that all systems that store logs have adequate storage space for the logs generated on a regular basis, so that log files will not fill up between log rotation intervals. The logs should be archived and digitally signed on a periodic basis.
- Deploy a SIEM (Security Information and Event Management) or log analytic tools for log aggregation and consolidation from multiple machines and for log correlation and analysis. Using the SIEM tool, system administrators and security personnel should devise profiles of common events from given systems so that they can tune detection to focus on unusual activity, avoid false positives, more rapidly identify anomalies, and prevent overwhelming analysts with insignificant alerts.

The control to include two synchronized time sources is different; it would be interesting to see if such a requirement should be applied to HCDs. Validation of audit log settings is something that we don't think about but should be done. If audit logs are to be stored on an HCD, which is allowable per the HCD cPP, it is important to make sure there is sufficient storage space on the HCD to store the audit log. Finally, one of the issues that the HCD iTC will likely look at for HCD cPP 1.1 is requirements for integrating the audit log with SIEM tools, so this control is very timely in that context.

CSC 7: Email and Web Browser Protection

- Ensure that only fully supported web browsers and email clients are allowed to execute in the organization, ideally only using the latest version of the browsers provided by the vendor in order to take advantage of the latest security functions and fixes.
- Uninstall or disable any unnecessary or unauthorized browser or email client plugins road-on applications. Each plugin should utilize application / URL whitelisting and only allow the use of the application for pre-approved domains.

- Deploy two separate browser configurations to each system. One configuration should disable the use of all plugins, unnecessary scripting languages, and generally be configured with limited functionality and be used for general web browsing. The other configuration should allow for more browser functionality but should only be used to access specific websites that require the use of such functionality.
- Scan and block all email attachments entering the organization's email gateway if they contain malicious code or file types that are unnecessary for the organization's business. This scanning should be done before the email is placed in the user's inbox. This includes email content filtering and web content filtering

The controls for emails and web browsers seem reasonable, especially the ones to only allow fully-supported web browsers and email clients and to Uninstall or disable any unnecessary or unauthorized browser or email client plugins road-on applications. The control to deploy two separate browser configurations to each system is interesting to see how it would be implemented in practice. Finally, it is always good practice to block email attachments if they are from an unknown source.

CSC 8: Malware Defenses

- Employ automated tools to continuously monitor workstations, servers, and mobile devices with anti-virus, anti-spyware, personal firewalls, and host-based IPS functionality. All malware detection events should be sent to enterprise anti-malware administration tools and event log servers.
- Employ anti-malware software that offers a centralized infrastructure that compiles information on file reputations or have administrators manually push updates to all machines. After applying an update, automated systems should verify that each system has received its signature update.
- Limit use of external devices to those with an approved, documented business need. Monitor for use and attempted use of external devices. Configure laptops, workstations, and servers so that they will not auto-run content from removable media, like USB tokens (i.e., "thumb drives"), USB hard drives, CDs/DVDs, FireWire devices, external serial advanced technology attachment devices, and mounted network shares. Configure systems so that they automatically conduct an anti-malware scan of removable media when inserted
- Use network-based anti-malware tools to identify executables in all network traffic and use techniques other than signature-based detection to identify and filter out malicious content before it arrives at the endpoint.

These four controls are ones one would expect for malware – use automated tools to continuously monitor for malware, limit use of external devices to only those needed and filter out malware in executables.

CSC 9: Limitation and Control of Network Ports, Protocols, and Services

- Ensure that only ports, protocols, and services with validated business needs are running on each system.
- Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.
- Perform automated port scans on a regular basis against all key servers and compare to a known effective baseline. If a change that is not listed on the organization's approved baseline is discovered, an alert should be generated and reviewed.
- Place application firewalls in front of any critical servers to verify and validate the traffic going to the server. Any unauthorized services or traffic should be blocked and an alert generated.

Like CSC 8, these controls are the ones one would expect – ensure only requires ports, protocols, and services are running, run automated port scans on a regular basis, make sure only allowed services and ports pass through filters and validate traffic going through servers.

CSC 10: Data Recovery Capability

- Ensure that each system is automatically backed up on at least a weekly basis, and more often for systems storing sensitive information. To help ensure the ability to rapidly restore a system from backup, the operating system, application software, and data on a machine should each be included in the overall backup procedure. These three components of a system do not have to be included in the same backup file or use the same backup software. There should be multiple backups over time, so that in the event of malware infection, restoration can be from a version that is believed to predate the original infection. All backup policies should be compliant with any regulatory or official requirements.
- Test data on backup media on a regular basis by performing a data restoration process to ensure that the backup is properly working.
- Ensure that backups are properly protected via physical security or encryption when they are stored, as well as when they are moved across the network. This includes remote backups and cloud services

Al indicated that from his experience at Xerox the three main things for data recovery are (1) make sure you have backups, (2) make sure the backups ae physically protected and secure and (3) make sure your backups are tested.

CSC 11: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches

- Compare firewall, router, and switch configuration against standard secure configurations defined for each type of network device in use in the organization. The security configuration of such devices should be documented, reviewed, and approved by an organization change control board. Any deviations from the standard configuration or updates to the standard configuration should be documented and approved in a change control system.
- All new configuration rules beyond a baseline-hardened configuration that allow traffic to flow through network security devices, such as firewalls and network-based IPS, should be documented and recorded in a configuration management system, with a specific business reason for each change, a specific individual's name responsible for that business need, and an expected duration of the need.
- Use automated tools to verify standard device configurations and detect changes. All alterations to such files should be logged and automatically reported to security personnel.
- Manage network devices using two-factor authentication and encrypted sessions
- Install the latest stable version of any security-related updates on all network devices.
- Network engineers should use a dedicated machine for all administrative tasks or tasks requiring elevated access. This machine should be isolated from the organization's primary network and not be allowed Internet access. This machine should not be used for reading email, composing documents, or surfing the Internet.

The key is to have a standard configuration, document it and then track all changes to it. Also, make sure it is up-to-date with the latest security-related changes. This last control is interesting in requiring network engineers to have a dedicated machine for admin tasks; this would not be practical for HCDs.

CSC 12: Boundary Defense

- Deny communications with (or limit data flow to) known malicious IP addresses (blacklists), or limit access only to trusted sites (whitelists). Tests can be periodically carried out by sending packets from bogon source IP addresses (non-routable or otherwise unused IP addresses) into the network to verify that they are not transmitted through network perimeters. Lists of bogon addresses are publicly available on the Internet from various sources, and indicate a series of IP addresses that should not be used for legitimate traffic traversing the Internet.
- Deploy network-based IDS sensors on Internet and extranet DMZ systems and networks that look for unusual attack mechanisms and detect compromise of these systems. These

network-based IDS sensors may detect attacks through the use of signatures, network behavior analysis, or other mechanisms to analyze traffic.

- Network-based IPS devices should be deployed to complement IDS by blocking known bad signatures or the behavior of potential attacks. As attacks become automated, methods such as IDS typically delay the amount of time it takes for someone to react to an attack. A properly configured network-based IPS can provide automation to block bad traffic. When evaluating network-based IPS products, include those using techniques other than signature-based detection (such as virtual machine or sandbox based approaches) for consideration.
- Require all remote login access (including VPN, dial-up, and other forms of access that allow login to internal systems) to use two-factor authentication.

This CSC is looking at protecting the boundary, so controls that look at implementing IDS sensors and IPS devices make sense. The first control is a reasonable one to limit data flow to known trusted sites and block untrusted sites. Finally, the use of multi-factor authentication here for remote login is consistent with other controls in other CSCs.

CSC 13: Data Protection

- Perform an assessment of data to identify sensitive information that requires the application of encryption and integrity controls.
- Deploy approved hard drive encryption software to mobile devices and systems that hold sensitive data.
- Deploy an automated tool on network perimeters that monitors for sensitive information (e.g., personally identifiable information), keywords, and other document characteristics to discover unauthorized attempts to exfiltrate data across network boundaries and block such transfers while alerting information security personnel.
- Monitor all traffic leaving the organization and detect any unauthorized use of encryption. Attackers often use an encrypted channel to bypass network security devices. Therefore, it is essential that organizations be able to detect rogue connections, terminate the connection, and remediate the infected system.

Notice that the first control is to perform as assessment to identify information that requires the use of encryption rather than, like we did in the HCD cPP, actually require encryption of specific sensitive data. The second control involving encryption of sensitive data stored on mobile devices is something that should be in the mobile device cPPs if it is not already. The last two controls emphasize the trends of use of automations and monitoring of traffic that are consistent throughout this TR.

CSC 14: Controlled Access Based on the Need to Know

- All communication of sensitive information over less-trusted networks should be encrypted. Whenever information flows over a network with a lower trust level, the information should be encrypted.
- Sensitive information stored on systems should be encrypted at rest and require a secondary authentication mechanism, not integrated into the operating system, in order to access the information.
- All information stored on systems should be protected with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principal that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.
- Enforce detailed audit logging for access to nonpublic data and special authentication for sensitive data.

It is interesting that the “sensitive information…” controls above appear here, because one would expect that to appear under CSC 13: Data Protection. Similarly, one would expect the audit logging control to be under CSC 6: Maintenance, Monitoring, and Analysis of Audit Logs.

Normally, controls involving access control lists typically come under a separate Access Control category that includes more additional access-related controls. The fact that this is the only access-related control in the entire TR is surprising.

CSC 15: Wireless Access Control

- Ensure that each wireless device connected to the network matches an authorized configuration and security profile, with a documented owner of the connection and a defined business need. Organizations should deny access to those wireless devices that do not have such a configuration and profile.
- Ensure that all wireless traffic leverages at least Advanced Encryption Standard (AES) encryption used with at least Wi-Fi Protected Access 2 (WPA2) protection.
- Ensure that wireless networks use authentication protocols such as Extensible Authentication Protocol-Transport Layer Security (EAP/TLS), which provide credential protection and mutual authentication.
- Disable peer-to-peer wireless network capabilities on wireless clients
- Disable wireless peripheral access of devices (such as Bluetooth), unless such access is required for a documented business need

It is important the wireless networks use authentication protocols like EAP/TLS, that Bluetooth and peer-to-peer wireless networks are disabled, and that AES encryption with WPA2 protection is use on wireless traffic. Finally, following a consistent theme in this TR make sure the wireless devices connected to the network have a documented security configuration.

CSC 16: Account Monitoring and Control

- Review all system accounts and disable any account that cannot be associated with a business process and owner.
- Ensure that all accounts have an expiration date that is monitored and enforced.
- Establish and follow a process for revoking system access by disabling accounts immediately upon termination of an employee or contractor. Disabling instead of deleting accounts allows preservation of audit trails.
- Regularly monitor the use of all accounts, automatically logging off users after a standard period of inactivity.
- Use and configure account lockouts such that after a set number of failed login attempts the account is locked for a standard period of time.
- Configure access for all accounts through a centralized point of authentication, for example Active Directory or LDAP. Configure network and security devices for centralized authentication as well.
- Require multi-factor authentication for all user accounts that have access to sensitive data or systems. Multi-factor authentication can be achieved using smart cards, certificates, One Time Password (OTP) tokens or biometrics.
- Where multi-factor authentication is not supported, user accounts should be required to use long passwords on the system (longer than 14 characters).
- Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels

The above controls are all reasonable for managing user accounts. The ones that were most interesting were (1) requiring multi-factor authentication for all user accounts that have access to sensitive data or systems – that would be impractical for enterprises with large numbers of network devices or HCDs unless biometrics are implemented, (2) the requirement for ling passwords father than strong passwords in the case multi-factor authentication is not supported (see above discussion) and (3) the lockout and logging off controls ae both ones that are SFRs in the HCD cPP. Finally, the control to ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels – it Is surprising it didn't require the use of secure protocols instead.

CSC 17: Security Skills Assessment and Appropriate Training to Fill Gaps

- Perform gap analysis to see which skills employees need to implement the other Controls, and which behaviors employees are not adhering to, using this information to build a baseline training and awareness roadmap for all employees.
- Deliver training to fill the skills gap. If possible, use more senior staff to deliver the training. A second option is to have outside teachers provide training onsite so the examples used will be directly relevant. If there are small numbers of people to train, use training conferences or online training to fill the gaps.
- Implement a security awareness program that:1) focuses on the methods commonly used in intrusions that can be blocked through individual action;2) is delivered in short online modules convenient for employees;3) is updated frequently (at least annually) to represent the latest attack techniques;4) is mandated for completion by all employees at least annually;5) is reliably monitored for employee completion; and6) includes the senior leadership team's personal messaging, involvement in training, and accountability through performance metrics.

Al didn't say much about these controls; the unique aspect here is performing the gap analysis to determine the skills needed and then deliver the training to fill the gaps identified.

CSC 18: Application Software Security – Controls

- For all acquired application software, check that the version used is still supported by the vendor. If not, update to the most current version and install all relevant patches and vendor security recommendations.
- Test in-house-developed and third-party-procured web applications for common security weaknesses using automated remote web application scanners prior to deployment, whenever updates are made to the application, and on a regular recurring basis. In particular, input validation and output encoding routines of application software should be reviewed and tested.
- Maintain separate environments for production and nonproduction systems. Developers should not typically have unmonitored access to production environments.
- Ensure that all software development personnel receive training in writing secure code for their specific development environment.

Al pointed out that the last control is something that is checked for in EAL3 and is something that is very important to maintain. The first control above is very important also, especially to ensure that the application software has the latest security patches to address any detected vulnerabilities. It is important to make sure all in-house and 3rd party applications are continuously checked for vulnerabilities. Finally, Al noted that while at Xerox he tried to implement secure coding guidelines but had limited success in do it; however, it is still important to ensure that developers know how secure coding practices.

CSC 19: Incident Response and Management

- Ensure that there are written incident response procedures that include a definition of personnel roles for handling incidents. The procedures should define the phases of incident handling.
- Devise organization-wide standards for the time required for system administrators and other personnel to report anomalous events to the incident handling team, the mechanisms for such reporting, and the kind of information that should be included in the incident notification. This reporting should also include notifying the appropriate Community Emergency Response Team in accordance with all legal or regulatory requirements for involving that organization in computer incidents.

- Assemble and maintain information on third-party contact information to be used to report a security incident (e.g., maintain an email address of security@organization.com or have a web page http://organization.com/security).

The control to devise organization-wide standards for the time required for system administrators and other personnel to report anomalous events is interesting because it only deals with the time to report an incident but says nothing about the time to resolve the incident, which many controls in the US strive to deal with. The control to gather information on third-party contact information to be used to report a security incident is unique and very inciteful.

CSC 20: Penetration Tests and Red Team Exercises

- Conduct regular external and internal penetration tests to identify vulnerabilities and attack vectors that can be used to exploit enterprise systems successfully. Penetration testing should occur from outside the network perimeter (i.e., the Internet or wireless frequencies around an organization) as well as from within its boundaries (i.e., on the internal network) to simulate both outsider and insider attacks.
- Any user or system accounts used to perform penetration testing should be controlled and monitored to make sure they are only being used for legitimate purposes, and are removed or restored to normal function after testing is over.
- Include tests for the presence of unprotected system information and artifacts that would be useful to attackers, including network diagrams, configuration files, older penetration test reports, emails or documents containing passwords or other information critical to system operation.
- Plan clear goals of the penetration test itself with blended attacks in mind, identifying the goal machine or target asset. Many APT-style attacks deploy multiple vectors-often social engineering combined with web or network exploitation. Red Team manual or automated testing that captures pivoted and multi-vector attacks offers a more realistic assessment of security posture and risk to critical assets.

The fact that there is a CSC specifically for penetration testing is unique as stated earlier. The fact that regular external and internal penetration tests are required, and that the controls specific specify what types of tests and goals these penetration tests should include is also unique. The use of controlled accounts to do penetration testing is reasonable.

- Slides 40 - 42 list the attack types that were used to generate the 20 CSCs and the controls for each CSC. Al noted that the attack types are things like “Attackers gain access to internal enterprise systems and gather and exfiltrate sensitive information without detection by the victim organization” or “Attackers exploit weak default configurations of systems that are more geared to ease of use than security”.

  They are completely different from the attack types that form the basis for the threats like ‘An attacker may access (read, modify, or delete) User Document Data or change (modify or delete) User Job Data in the TOE through one of the TOE’s interfaces” used to generate the Security Problem Definition in the HCD cPP.

5. The second of this week’s special topics was a Comparison of Cybersecurity Security Controls between the NIST Cybersecurity Framework and ETSI TR 103 305-1 V2.1.1. The slides Al used can be found at https://ftp.pwg.org/pub/pwg/ids/Presentation/Cybersecurity Controls Comparison.pdf. However, the slides were just a PowerPoint version of the following table:

Security Control	NIST Cybersecurity Framework	ETSI TR 103 305-1
Asset Management	√	
Business Environment	√	
Governance	√	
Risk Assessment	√	

Security Control	NIST Cybersecurity Framework	ETSI TR 103 305-1
Risk Management Strategy	√	
Supply Chain Risk Management	√	
Identity Management, Authentication and Access Control	√	√
Awareness and Training	√	√
Data Security	√	√
Information Protection Processes and Procedures	√	
Maintenance	√	
Protective Technology	√	
Anomalies and Events	√	√
Security Continuous Monitoring	√	√
Detection Processes	√	√
Analysis	√	√
Mitigation	√	√
Improvements	√	
Recovery Planning	√	√
Improvements	√	
Communications	√	
Inventory of Authorized and Unauthorized Devices		√
Inventory of Authorized and Unauthorized Software		√
Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers		√
Controlled Use of Administrative Privileges		√
Maintenance, Monitoring, and Analysis of Audit Logs		√
Email and Web Browser Protections		√
Malware Defenses		√
Limitation and Control of Network Ports, Protocols, and Services		√
Secure Configurations for Network Devices such as Firewalls, Routers, and Switches		√
Boundary Defense		√
Controlled Access Based on the Need to Know		√
Wireless Access Control		√
Account Monitoring and Control		√
Application Software Security		√

Security Control	NIST Cybersecurity Framework	ETSI TR 103 305-1
Penetration Tests and Red Team Exercises		√

Al’s point was that although there are some areas where the two sets of controls have some common CSCs, the comparison shows that NIST and the EU are emphasizing two different types of things in their cybersecurity controls. NIST cybersecurity controls are focused mainly on management-related controls like governance, risk management, and areas related to the Cybersecurity Executive Order such as supply chain security. The EU cybersecurity controls are focused are more “hands-on” issues like secure configurations, inventory control, email and browser protection and application software security.

Neither is right or wrong; it’s just that the comparison showed the clear difference in emphasis between NIST (and therefore the US perspective on cybersecurity controls) and the EU perspective on cybersecurity controls.

6. There was no Round Table at today’s meeting.
7. **Actions:** None

Next Steps

- The next IDS WG Meeting will be April 20, 2023 at 3:00P ET / 12:00N PT because April 6th, which would have been the date for our next regularly scheduled meeting, is the 1st day of Passover and Al will be getting ready for the Passover Seder that night. Main topics will be the latest status of the HCD iTC and a special topic to be determined.