



IT'S JUST A PRINTER...

LESSONS LEARNED OVER TEN YEARS OF CC EVALUATIONS

Lachlan Turner, CSC Labs Technical Director
Alan Sukert, Xerox Product Security Specialist

International Common Criteria Conference
September 2013



MFDs are complex, embedded network devices

- MFDs have:
 - One or more operating systems
 - Network controller and firmware
 - One or more hard disk drives
 - Web server
 - Hardware ports
 - Page Description Language interpreters (PS & PCL)
 - Fax
 - Network Interfaces



...multiple points of vulnerability

Which have been exploited....

AMERICAN BANKER | Risk Management
Wednesday, August 7, 2013
Today's Paper | Magazine | Video | Web Seminars | White Papers | Women in Banking | FinTech
MERGERS & ACQUISITIONS | REGULATION & REFORM | COMMUNITY BANKING | CONSUMER FINANCE | BANK TECHNOLOGY | BANKTHINK
SIGN ME UP NOW FOR FULL ACCESS | SUBSCRIBE | TAKE A FREE TRIAL (INCLUDING EMAIL ALERTS)

SECURITY WATCH
Wells Fargo Blames Statement Data Breach on Buggy Printer

Forbes - New Posts (+1 posts this hour) | Most Popular (What 20-Year-Olds Don't Get) | Lists (America's Top Colleges)

Get 2 FREE Issues of Forbes

CIO NETWORK
INSIGHTS AND IDEAS FOR TECHNOLOGY LEADERS.
+ Follow (524)
TECH | 2/07/2013 @ 7:07PM | 5,071 views

infosecurity
EUROPE
News

The Hidden IT Security Threat: Multifunction Printers

VIAFORENSICS
advancing mobile security
viaForensics » Security » Exploiting printers via Jetdirect vulnerabilities
by Sebastián | in Security | January 14, 2013
Exploiting printers via Jetdirect vulnerabilities

CRN NEWS, ANALYSIS, AND PERSPECTIVE FOR VAR'S AND TECHNOLOGY INTEGRATORS
LATEST ISSUE | SUBSCRIBE TODAY!
HOME | NEWS | SLIDE SHOWS | VIDEO | BLOGS | BUZZ | REVIEWS | HOW-TO | RESEARCH | LISTS | EVENTS | LEARNING CENTERS | INTERNET
NETWORKS | SECURITY | CLOUD | STORAGE | APPS | DATA CENTER | MOBILITY | VIRTUALIZATION | MANAGED SERVICES | COMPONENTS
Like 1 | Share 1 | Tweet 1 | Follow 13.2K followers | +1 0 | Submit

US-CERT: Samsung Printer Vulnerability Opens Backdoor To Admin Rights

Printer-related security breaches affect 63% of enterprises

14 March 2013

Data Protection
News | Blogs | Tools & Templates | Security Jobs | Basics | Data Protection | Identity & Acc

Home » Data Protection » Network Security

NEWS

Printers join fray in network vulnerability landscape

Even Xerox have reported vulnerabilities...

CVE Details

The ultimate security vulnerability datasource

[Log In](#) [Register](#) [Reset Password](#) [Activate Account](#)

[Home](#)

Browse :

[Vendors](#)

[Products](#)

[By Date](#)

[By Type](#)

Reports :

[CVSS Score Report](#)

[CVSS Score Distribution](#)

Search :

[Vendor Search](#)

[Product Search](#)

[Version Search](#)

[Vulnerability Search](#)

[By Microsoft References](#)

Top 50 :

[Vendors](#)

[Vendor Cvss Scores](#)

[Products](#)

[Product Cvss Scores](#)

[Versions](#)

Other :

[Microsoft Bulletins](#)

[Bugtraq Entries](#)

[CWE Definitions](#)

[About & Contact](#)

Xerox » Workcentre : Security Vulnerabilities

CVSS Scores Greater Than: [0](#) [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#)

Sort Results By : [Cve Number Descending](#) [Cve Number Ascending](#) [CVSS Score Descending](#) [Number Of Exploits](#)


[Copy Results](#) [Download Results](#) [Select Table](#)

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gain
1	CVE-2009-1656			Exec Code	2009-05-16	2009-06-09	10.0	
Xerox WorkCentre and WorkCentre Pro 232, 238, 245, 255, 265, 275; and WorkCentre 5632, 5638, 5645, 5645, 5645 commands via unknown attack vectors, aka "command injection vulnerability."								
2	CVE-2008-6436	79		XSS	2009-03-06	2009-04-02	4.3	
Cross-site scripting (XSS) vulnerability in the Web Server in Xerox WorkCentre 7132, 7228, 7235, and 7245								
3	CVE-2008-2825	79		XSS	2008-06-23	2009-04-14	4.3	
Cross-site scripting (XSS) vulnerability in the embedded Web Server in Xerox WorkCentre M123, M128, and script or HTML via unspecified vectors.								
4	CVE-2008-2824	264			2008-06-23	2009-04-14	10.0	
Unspecified vulnerability in the Extensible Interface Platform in Web Services in Xerox WorkCentre 7655, 7655, 7655								
5	CVE-2006-6473				2006-12-11	2008-09-05	10.0	
Multiple unspecified vulnerabilities in Xerox WorkCentre and WorkCentre Pro before 12.050.03.000, 13.x before 13.050.03.000 related to (1) an Immediate Image Overwrite (IIO) error message at the Local User Interface (LUI) if overwrite failure when the overwrite is greater than 2 Gb.								
6	CVE-2006-6472				2006-12-11	2008-09-05	10.0	
The httpd.conf file in Xerox WorkCentre and WorkCentre Pro before 12.050.03.000, 13.x before 13.050.03.000 has unspecified impact and remote attack vectors.								


No vulnerabilities reported for the 9700...



The Xerox Security Model

	Network Security		Document Security	
	<ul style="list-style-type: none">• IP/MAC Address Filtering• SSL/TLS• Network ports On/Off• IPv6• Digital Certificate• SNMPv3• 802.1X (Wire/wireless)• Firewall• Fax/Network separation		<ul style="list-style-type: none">• Secure Print• Encrypted PDF• Fax Forwarding to Email and Network• Fax Destination Confirmation• Digital Signatures• Glossmark• Check 21• Resource Security	
	Data Security		Authentication	
	<ul style="list-style-type: none">• HD Overwrite• Data Encryption• Volatile and Non-volatile Memory• Secure Fax• Scan to Mail Box Password Protection• S/MIME for Scan to Email• Job Log Conceal• Hard Disk Removal Program		<ul style="list-style-type: none">• Network Authentication• Role Based Access• SMTP Authentication• Microsoft Active Directory Services• Smart Card, including Common Access Card, Personal Identity Verification (PIV) card, .Net, proximity card	

The Xerox Security Model – evaluated functionality



Network Security		Document Security	
<ul style="list-style-type: none">• IP/MAC Address Filtering• SSL/TLS• Network ports On/Off• IPv6• Digital Certificate• SNMPv3• 802.1X (Wire/wireless)• Firewall• Fax/Network separation	<ul style="list-style-type: none">• Secure Print• Encrypted PDF• Fax Forwarding to Email and Network• Fax Destination Confirmation• Digital Signatures• Glossmark• Check 21• Resource Security		
Data Security		Authentication	
<ul style="list-style-type: none">• HD Overwrite• Data Encryption• Volatile and Non-volatile Memory• Secure Fax• Scan to Mail Box Password Protection• S/MIME for Scan to Email• Job Log Conceal• Hard Disk Removal Program	<ul style="list-style-type: none">• Network Authentication• Role Based Access• SMTP Authentication• Microsoft Active Directory Services• Smart Card, including Common Access Card, Personal Identity Verification (PIV) card, .Net, proximity card		

Xerox Common Criteria Evaluations



WorkCentre 4250/4260



WorkCentre 7120



WorkCentre 5135/5150



WorkCentre 5225/5230



WorkCentre 5700 series



Xerox 4112/4127
Copier/Printer



ColorQube 9200 series
(undergoing evaluation)



Xerox Color 550/560 Printer



WorkCentre 7700 series
(undergoing evaluation)



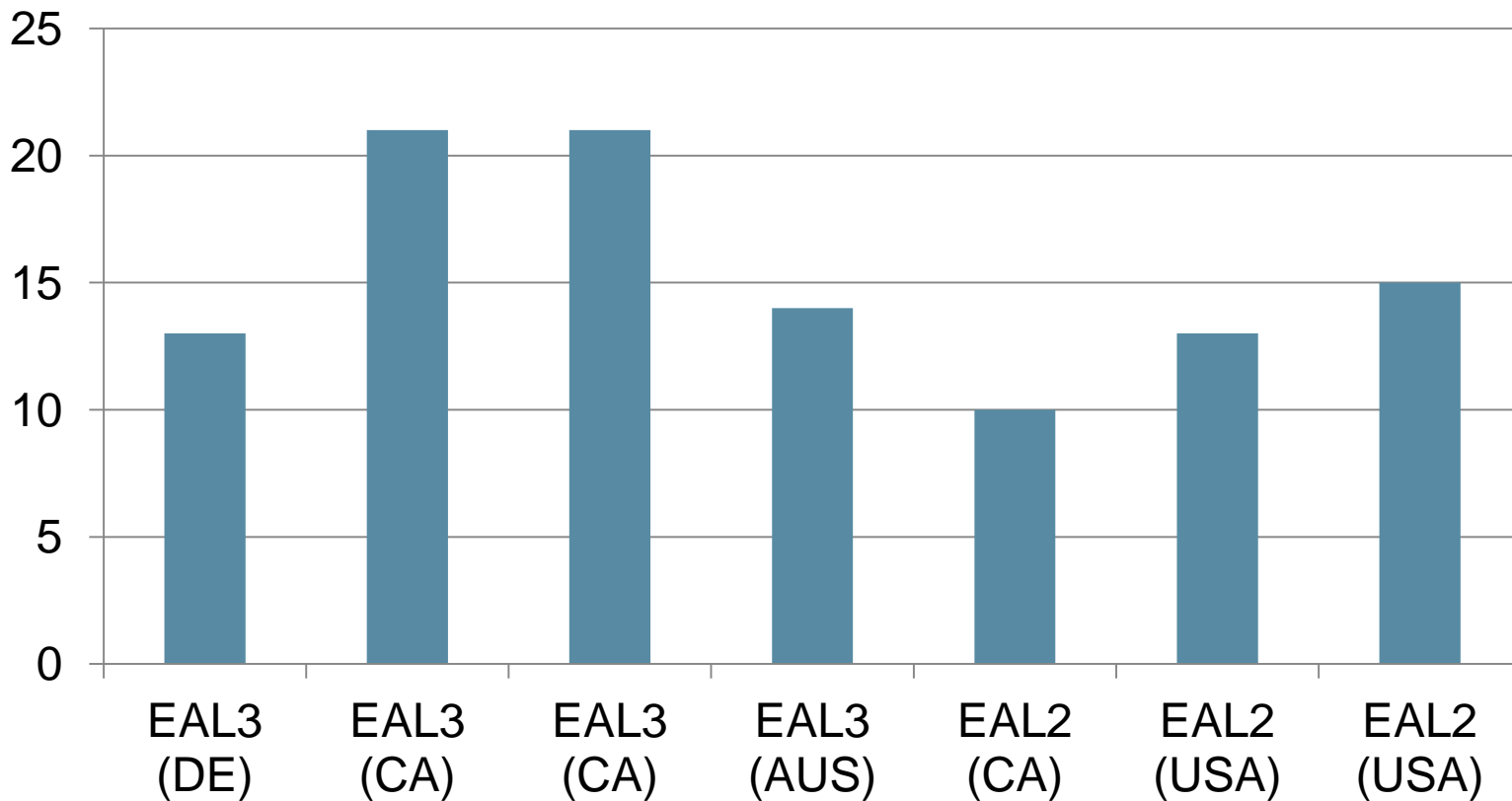
WorkCentre 7500 series



WorkCentre 5300 series

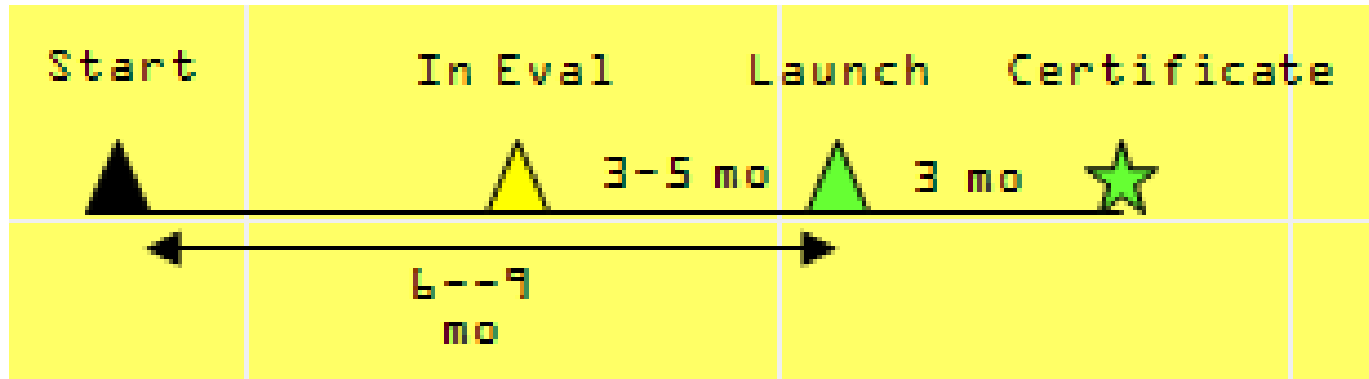
Xerox Evaluation History (subset)

Time to Evaluate (months)



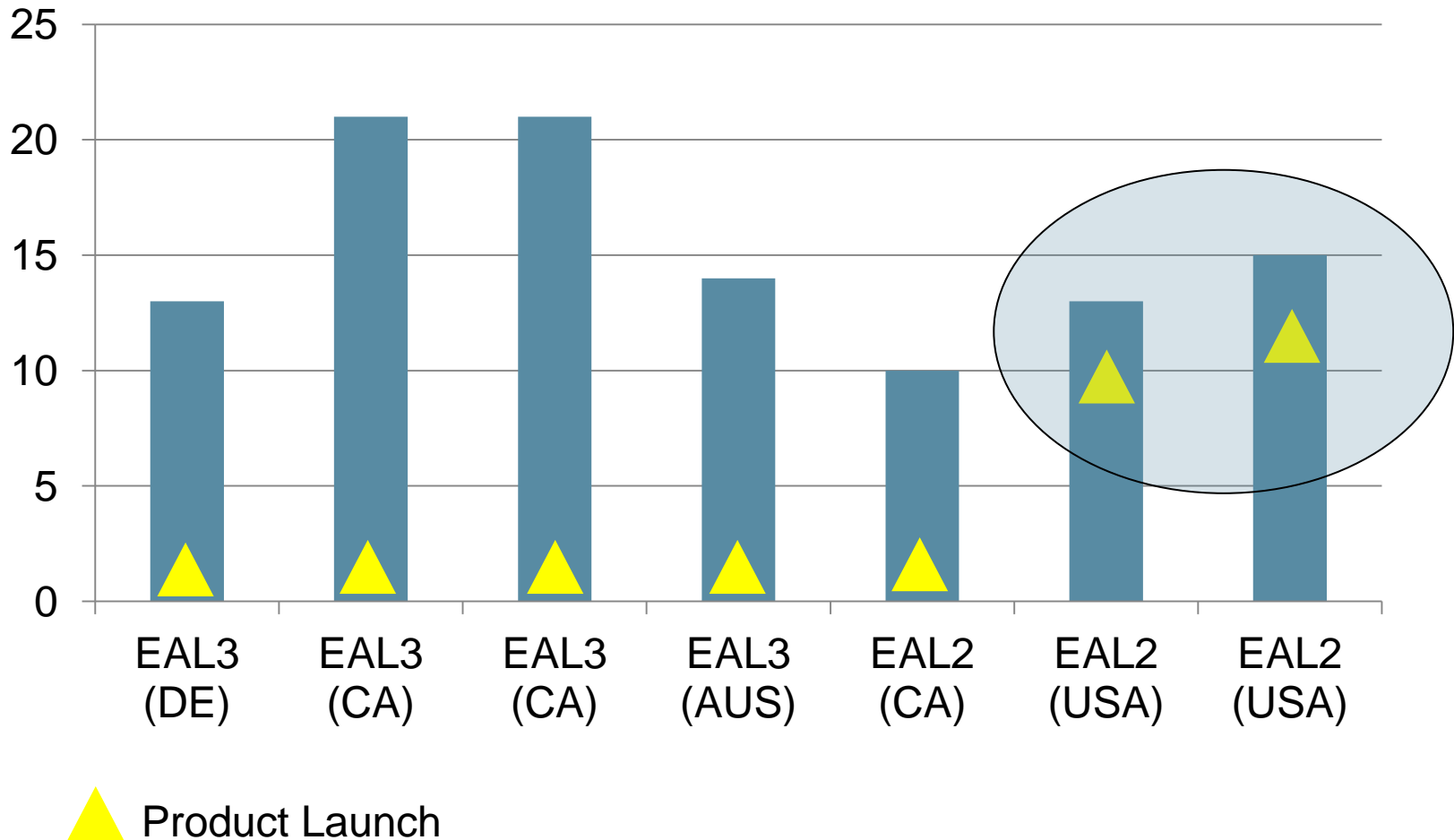
Xerox wanted a smarter approach

- Certification within 3 months of product launch
- Achieved by:
 - Strategic plan / schedule for products to be certified
 - Starting CC process before product launch
 - Better communication between Development and Security teams
 - Leverage strong lab relationship




Xerox Evaluation History – Process Improvements

Time to Evaluate (months)




Reducing Cost of Evaluation by 40%

- Xerox and CSC have reduced evaluation/certification cost by 40%
- Common platform across machines / strategic ST development
 - Enable more machines per evaluation



National Information Assurance Partnership
Common Criteria Certificate
is awarded to
Xerox Corporation
for
**WorkCentre 5845, 5855, 5865, 5875, 5890, 7220, 7225, 7830, 7835, 7845,
7855 & ColorQube 9301, 9302, 9303**



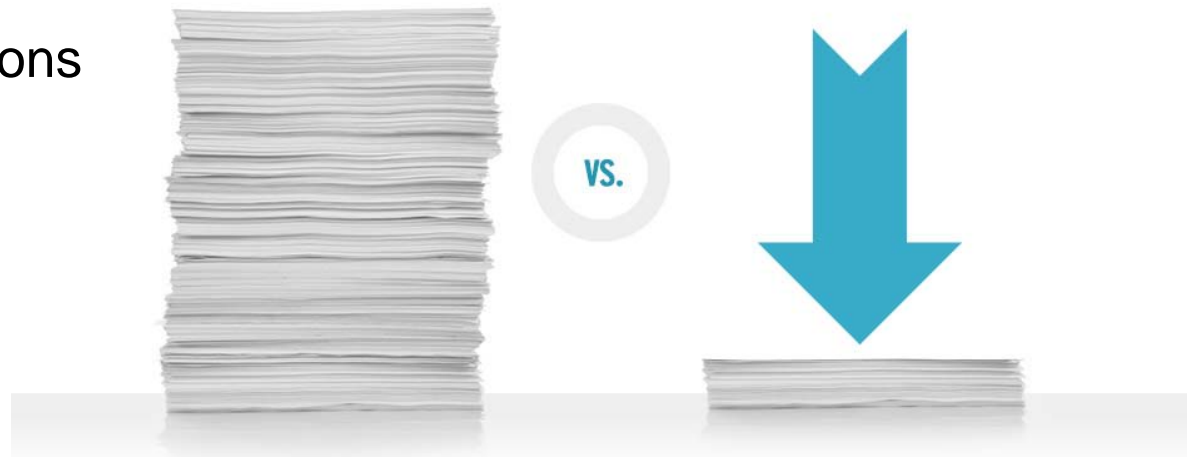
The IT product identified in this certificate has been evaluated at an accredited testing laboratory using the Common Methodology for IT Security Evaluation (Version 3.1) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1). This certificate applies only to the specific version and release of the product in its evaluated configuration. The product's functional and assurance security specifications are contained in its security target. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by any agency of the U.S. Government and no warranty of the IT product is either expressed or implied.

Date Issued: 2013-05-29
Validation Report Number: CCEVS-VR-VID10499-2013
CCTL: Computer Sciences Corporation

Assurance Level: EAL2 Augmented with
ALC_FLR3
Protection Profile Identifier:
U.S. Government Protection Profile for Hardcopy Devices Version
1.0 (IEEE Std. 2600.2™-2009)

Reducing Cost of Evaluation by 40%

- Simplification of CC evidence
 - **Development (ADV)**. Re-align to CEM and remove unnecessary detail.
 - **Functional Specification (FSP)** 500 pages to 200 pages
 - **TOE Design (TDS)** 100 pages to 30 pages
 - **Life Cycle (ALC)**. Replace source process documents (30+) with CC specific documents (3).
 - **Testing (ATE)**. Reduce test traceability from 30 pages to 8 pages (due to simplified FSP).
- Re-use across evaluations



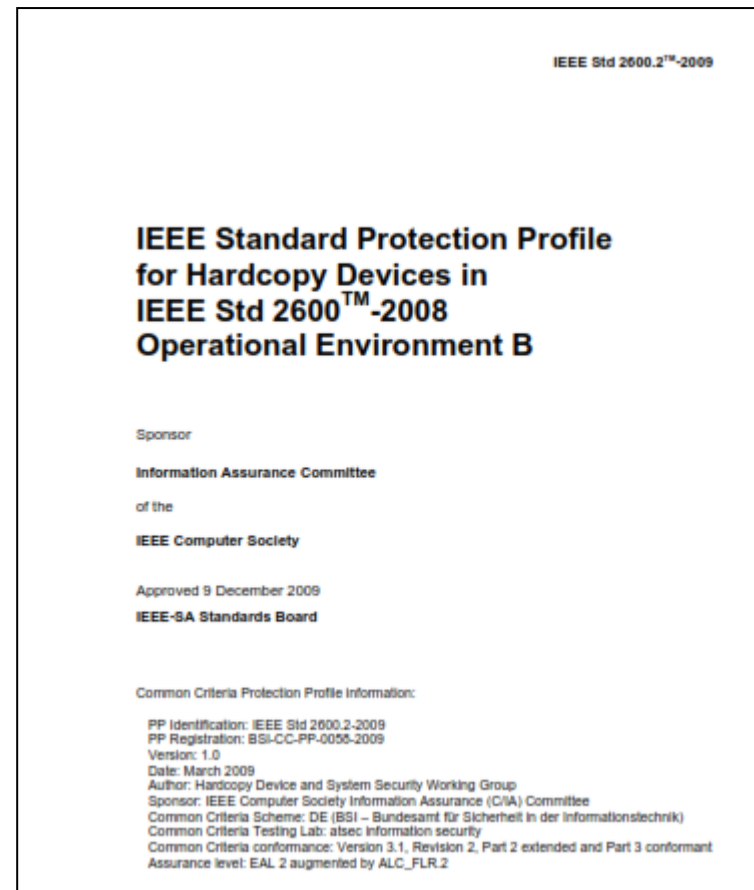
Reducing Cost of Evaluation by 40%

- Close engagement with CC consultant / advocate
- Continuity of evaluation team / lab
 - Xerox and CSC have been working together for over 10 years
 - Test team product familiarity
 - POC familiarity (Xerox / CSC working relationships)
- Continuity of scheme (NIAP)
 - Request same certifiers / validators (not always possible)
 - Process awareness



Protection Profiles?

- Xerox heavily involved in MFD PP development (IEEE 2600)
 - Multi-vendor collaboration
 - Adopted by NIAP in 2010
 - EAL2 + ALC_FLR.2
 - “...great but lengthy experience”
 - “Takes a lot of work and discussions..”



Protection Profiles?

- Xerox involved in development a new MFD PP
 - Collaboration between IPA (Japan) and NIAP (USA)
 - Multi-vendor collaboration (same as IEEE 2600)
 - EAL0? (similar to NDPP)
 - *“...Original schedule was way optimistic;it will take a couple of years to do this”*
- Motivation for involvement?
 - Drive what will be in the PP
 - Align product features to what will be in the PP

What is next for Xerox?

- Continue working with CSC
- Certify as many MFDs as business case support
- Expand into product lines that have not been evaluated
- Hints on new features?
 - WebDAV
 - Tablet / smartphone support



Predictions for the future of CC?

- Relevance will depend on the policy drivers that require CC
- Realization that it is very hard to achieve and maintain a set of Collaborative PPs
- Gap between vision and reality
- Splintering of evaluation markets (e.g. Europe, Asia stay with EALs / others chase cPP)
 - Vendors back to performing multiple evaluations?
- Reconsideration of PP only policies





THANK YOU

Lachlan Turner, CSC Labs Technical Director, lturner28@csc.com

Alan Sukert, Xerox Product Security Specialist, alan.sukert@xerox.com





BUSINESS SOLUTIONS
TECHNOLOGY
OUTSOURCING