# Threat Assessment and Remediation Analysis (TARA)

# Training Workshop

February 2020



© 2020 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited, Case 20-0272.

# TARA Training Agenda (1-Day Workshop)

- 0830 0900 Admin, Introductions
- 0900 0945 TARA Overview
- 0945 1000 Break
- 1000 1015 Catalog demonstration
- 1015 1045 Cyber Threat Modeling
- 1045 1130 Cyber Threat Susceptibility Analysis
- 1130 1200 Exercise #1: Creating a shopping cart
- 1200 1230 Lunch
- 1230 1330 Cyber Risk Remediation Analysis
- 1330 1400 Exercise #2: Exporting catalog data
- 1400 1430 Catalog Content Management
- 1430 1500 Exercise #3: Updating the catalog
- 1500 1515 Break
- 1515 1545 TARA Risk and Cost Scoring Tools
- 1545 1600 Exercise #4: Using a risk calculator
- 1600 1615 Recap
- 1615 Adjourn

The MITRE Corporation

# **TARA Overview**



© 2020 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited, Case 20-0272.

# **Objectives**

Provide an overview of the TARA methodology

- Discuss the TARA data model support for vector groups, taxonomies, attack vectors, countermeasures and mappings
- Discuss application of TARA in Systems Security Engineering (SSE) contexts



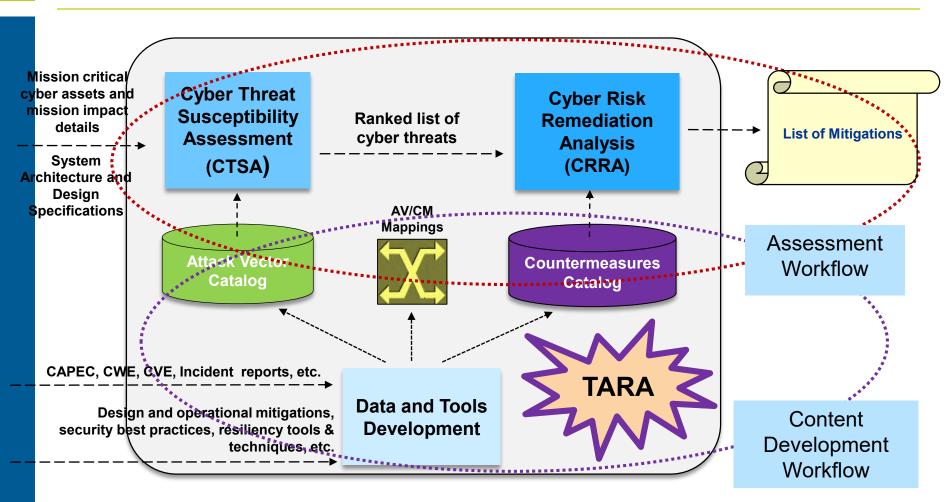
# **Threat Assessment & Remediation Analysis (TARA)**

- Methodology to identify and assess cyber threats and select countermeasures effective at mitigating those threats
  - Leverages catalog of Attack Vectors (AVs), Countermeasures (CMs), and associated mappings
    - Use of catalog ensures that findings are consistent across assessments

5

- Uses scoring models to quantitatively assess AVs and CMs
  - AVs ranked by risk, providing a basis for effective triage
  - CMs ranked by cost-effectiveness, providing a basis for identifying optimal solutions
- Delivers recommendations
  - Allows programs to make informed choices on how best to improve a system's security posture and resilience
- Can be performed separately or as follow-on to a Crown Jewels Analysis (CJA)
  - CJA results can inform TARA scope and assessment of risks

# **TARA Methodology Workflows**

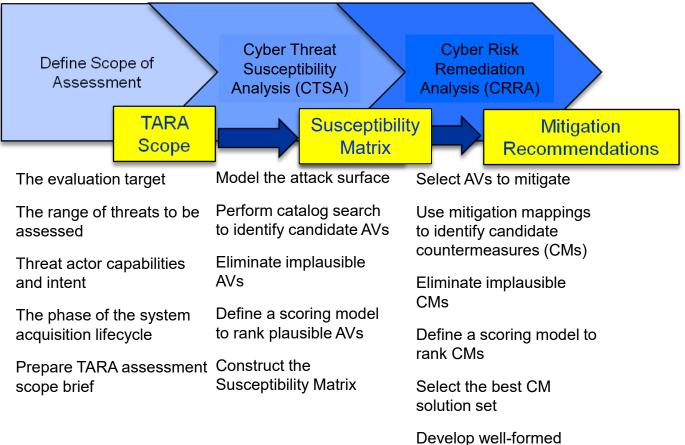


*Workflow* – Sequence of connected activities that produce useful work



# **Phases of a TARA Assessment**

Objective to identify and assess cyber threats and select countermeasures effective at mitigating those threats



### **MITRE**

# **TARA Assessment Products**

### **Susceptibility Matrix**

Provides a ranked list of cyber threats, mapped to components of the evaluation target

	Attack Vectors	Risk		Shopp	oing cart	
AV ID	AV Name	Score	Browser	Database	Web Server	Email App
T000049	Buffer Overflow	High	Х	Х	Х	х
T000014	Accessing, Intercepting, and Modifying HTTP Cookies	Moderate	Х			х
T000050	Forced Integer Overflow	Moderate		Х		
T000071	SOAP Array Overflow	Moderate			Х	
T000052	Inducing buffer overflow to disable input validation	Low		Х		х
T000170	Attack through shared data	Low	Х		Х	

Answers the questions: Where and how is my system most susceptible?

### **Solution Effectiveness Table**

Provides a ranked list of countermeasures, mapped to cyber threats, and identifies the preventative or mitigating effect each countermeasure provides

	Countermeasure (CM)	Scoring	Effect (by Attack Vector ID)					
CM ID	Name	U/C Ratio	T000014	T000049	T000050	T000052	T000071	T000170
C000134	Select programming languages that minimize software defects	75		PM	PM	PM		
C000117	Apply principle of least privilege	67					RM	RM
C000093	Merge data streams prior to validation	50				PM		
C000096	Use vetted runtime libraries	50		PH			PH	
C000047	Encrypt session cookies	33	PH					
C000051	Use digital signatures/checksums	33	PH					
C000132	Use sandboxing to isolate running software	25						PM
	TOTALS	333	2	2	1	2	2	2

Answers the questions: How are my threats mitigated and where are the gaps?



# **TARA Toolset**

Web-based tools supporting TARA assessments and catalog development

### **Catalog Search Tools**

	Mission Assurance Engineering : Threat Assessment and Remediation Analysis
ds Loaded	TIPS
	earches: Select Search Run Search Modify Search Delete Search
	Stde: C Full & Moinal Mission Assurance Engineering a Threat Assessment and Remediation
h Home	
Records Loaded	TTPs Loaded AC IDs in [328]
ts Asset Classes	Apply Filter TTP/CM Mapping
TTPS	
Countermeasures	Filter TTP ID TTP Name
Search for	T000010 HTTP Request Smuggling
TTPs	T000014 Accessing, Intercepting, and Modifying HTTP Cookies
Countermeasures	T000016 Simple Script Injection
nt Reports PALMA Reports	T000023 Cross Site Tracing
PALMA Reports     Catalog Maintenance	
Asset Classes	T000039 Exploitation of Session Variables, Resource IDs and other Trusted Credentials
TTPs	T000066 Web Server/Application Fingerprinting
Countermeasures	T000073 HTTP Response Splitting
Admin Functions	T000076 HTTP Verb Tampering
Account Managment	T000078 Flash Parameter Injection
Catalog Merge Tool	T000081 HTTP Response Smuggling
Data Schemas Spreadsheet Template	T000084 Web Logs Tampering
Converter/Importer	T000088 Modifying filename extensions to misclassify content
TTP-CM Mapping Tools	TO00096 Poison Web Service Registry
	T000100 Forceful Browsing
	indows Internet Explorer provided by MITRE
Pie Edit View Favorit	226-sendou mitre org 2020(lapache-sch-1,4.2)adminifium, jep 🗙 🕂 🛠 Une Sex ch
😭 🕸 🖂 Solt when p	
Solr Adm	nin (example)
g026-sandbox:8080	Colr
cwd=/asrlocal/spache	-tomcat-6.0.20/bin SolrHome=home/jwynn/Desktop/solr
Solr/Lucene	101*
Statement	
Filter Query	-1d:CVE-* -1d:CHE-*
Start Row	0
Maximum Rows	1000
Returned Fields to Return	id. name. desc
Query Type	id, name, desc standard
Output Type	standard
Debug: enable	Note: you may need to "your source" in your browser to see explain() correctly indented
Debug: explain	Apply original query scoring to matches of this query to see how shey
others Enable Highlighti	compane.
Enable Highlighti Fields to Highlighti	
i inter to ingringing	Search,
	tes the most common query options available for the built in Query Types. Please consult the
	ter the most common guery options available for the built in Query Types. Please consult the ad Query Parameters. * disat research

### **Catalog Update Tools**

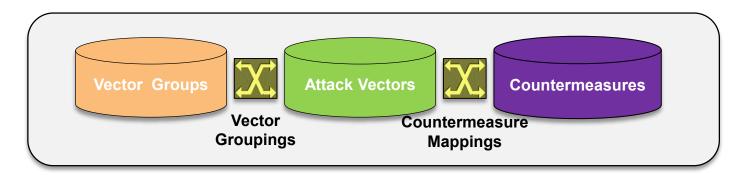
Asset Cla faces	iss Managment Interfac	e							
ermeasures Classes	et Class by ID: Get AG				Class from file				
is Loaded Des (aug		2			Ment AC			_	
	Mission Assurance	Engineering & Threat Asses	sment and Ren	nediation Ar	alysis				
	ics, Techniques, and Proce	edures (TTP) Management Inter	face						
terfaces		Test.	ort TTP from file:						
rPs suntermeasures Get 1	TTP by ID:	Get TTP	Browse.						
set Classes	The by ab. ]		et TTP from file						
ecords Loaded Pr	revious TTP		Next TTP						
TPs									
ountermeasures					ategories:				
sset Classes Tool earch for (Edi		njection	1	Social	Engineering cric Warfare		_		
TPs (Edi	iting)				are/Firmware				
	Niccion Are	surance Engineering : Thr	ant Arcore	int and De	modiation	Analycic			
CALCER & HALLSHELMS & D.B.	Mission As	surance Engineering : Thr	eat Assessme	int and Ke	mediation	anaiysis			
Home	Countermeasure Man	agement Interface							
Interfaces			-						
TTPs	Get CM by ID:	Get CM Import C	M from file:		Brows	e Gi	at CM from file		
Countermeasures									
Asset Classes	Previous CM					lext CM			
Records Loaded	CM ID:	CM Name:			Sc	ope:			
TTPs	C000133	Design to avoid SQL in	ection attacks		2-	4 -			
Countermeasures	(Editing)				-1				
Asset Classes Search for		1				turity: idespread			
TTPs	Description:					idestriead			
Countermeasures		is using prepared statements, hese features should accept				st:			
Misc. Tools	support strong typin	g. Do not dynamically constr				rer 💌			
Spreadsheet Template	using "exec" or sind	lar functionality.					and the		
Converter/Importer						issification 1 Inclassified	evel:		
TTP-CM Mapping Tools									-
	Goals:	Forms:			Ke	ferences:	Add	145	
	Limit	Requirements					1 110		1
	Detect Recover	Fielding							
	Neutralize	Disposal Operation							
		Implementation			-				1
1	-	Design				Remove Ref.			
	Olars From 1	Delete Make this a						/Update	
	Clear Form	Delete Make this a	new GM				1400	Opeare	
	and a strange of the strange of the strange								
	This Countermeasure spp	lies to the following TTPs:							
		TP ID - Name	Detect	Neutralize	Limit	Recover	Classification		
	-	on through SOAP Parameter	N/A	Medium	N/A	N/A	Unclassified	Edit	Delet
		en	N/A	Medium	N/A	N/A	Unclassified	Edit	Delet
	T000064 - SOL Injecti T000065 - Blind SOL Is		N/A N/A	Medium	N/A N/A	N/A N/A	Unclassified	Edit Edit	Delet







# **Objectives of the TARA Catalog**



- Provide a repository of Attack Vector (AV) and Countermeasure (CM) data used in TARA assessments
- Support mappings and groupings used to integrate and traverse catalog data
- Implement an XML-based data model to represent AVs and CMs
- Help establish consistency from one TARA assessment to the next

# **Navigating the TARA Catalog**

### **Vector Groups (VGs)**

Home	All Asset	Classes Loade	d
TTPs	AC ID	AC Name	Keywords
Countermeasures Asset Classes	A000223	Applications	antivirus   browser   excel   MS project   MS word   Outlook   pdf reader   powerpoint   visio   vpn   internet explorer   firefox
Records Loaded	A000036	authentication	credential   password   account   authentication   certificate   username   authenticate   user   SAML token   credentials
Countermeasures	A000187	Data	DOM   html   parse   schema   Unicode   XHTML   XML   cookie   token
Asset Classes	A000037	database	database   Oracle   SQL   schema   DBMS   JDBC   MS access   ODBC
Search for	A000201	email	email   IMAP   POP   SMTP   Outlook   Thunderbird
Countermeasures	A000057	firmware	BIOS   firmware   IOS
Misc. Tools Spreadsheet Template	A000267	mobile	3G   4G   802.11   access point   cell   cellular   hotspot   mobile   WEP   wi- if   wimax   wireless   WIPA
Converter/Importer	A000098	network service	IDS   IPS   proxy
TTP-CM Mapping Tools	A000235	os	android   IOS   linux   OS   unix   windows
	A000128	OSI - Application Layer	BGP   DHCP   DNS   FTP   http   HTTPS   IMAP   LDAP   POP   SIP   SMTP   SNMP   SSL
	A000140	OSI - Data Link Layer	ARP   OSPF   VLAN
	A000136	OSI - Network Layer	ICMP   IP   IPv4   IPv6
	A000131	OSI - Transport Layer	TCP   UDP
	A000251	PKI	certificate   CRL   keystore   PKI   revocation   root   self-signed   X.509   X509   CA   certificate authority
	A000051	platform	bridge   cloud   firewall   gateway   hub   router   server   switch   thick client   thin client   wireless
	A000228	Remote access	IPsec   SSH   telnet   vpn
	A000179	Scripting	CGI   JavaScript   Perl   PHP   Python   flash   bash
	A000172	Security	access matrix   ACL   AES   biometric   certificate   CHAP   DES   digital signature   EAP   encryption   firewall   hash   IPsec   kerberos   L2F   L2TP   MDS   packet fiter   password   PKI   PPTP   radius   security   SHA   SSH   7aanan   MTA   MTA   MTA   MTA   STA

Named collection of attack vectors, e.g., architectural components, technologies, shopping carts, intrusion sets etc.

### Attack Vectors (AVs)

Home	All TTPs	Loaded
Records Loaded	-	
TTPs	TTP ID	TTP Name
Countermeasures	<u>T000001</u>	Malicious BIOS code allows unsigned updates
Asset Classes Search for	<u>T000002</u>	Secure BIOS update bypassed via buffer overflow
TTPs	<u>T000003</u>	User installs malicious BIOS image on device
Countermeasures	<u>T000004</u>	Malware reflashes device with malicous BIOS
Catalog Maintenance	<u>T000005</u>	System is rolled back to an authentic but vulnerable system BIOS
TTPs	<u>T000006</u>	Compromised update server distributes malicious BIOS
Countermeasures	<u>T000007</u>	SNMP community strings transmitted in the clear
Asset Classes	T000008	SNMP Community String Name is Guessable
My Account	T000009	Session Credential Falsification through Prediction
Change password Admin	<u>T000010</u>	HTTP Request Smuggling
Functions	T000011	Lifting Data Embedded in Client Distributions
Account Managment	T000012	Postfix, Null Terminate, and Backslash
Catalog Merge	T000013	Exploiting Trust in Client
Data Schemas	T000014	Accessing, Intercepting, and Modifying HTTP Cookies
Spreadsheet	T000015	Cross Site Request Forgery (Session Riding)
Template Converter/Importe	T000016	Simple Script Injection
TTP-CM Mapping	T000017	Subvert Code-signing Facilities
	T000018	Using Unicode Encoding to Bypass Validation Logic
	T000019	Using Escaped Slashes in Alternate Encoding
	T000020	Xquery Injection
	T000021	Man in the Middle Attack
	<u>T000022</u>	Cryptanalysis
		Cross Site Tracing
	T000024	Malicious Software Update
		Accessing Functionality Not Properly Constrained by ACLs
		Manipulating Input to File System Calls

# Adversary approaches to compromise a cyber asset

### **Countermeasures (CMs)**

	Assula	nce Engineering : Threat Assessment and Remediation Analysis
Home A	Il Count	termeasures Loaded
Records Loaded		
TTPs	CM ID	<u>CM Name</u>
	000001	Verify secure BIOS update non-bypassability
Asset Classes	000002	Verify BIOS image write protection
	000003	Verify recovery process to restore last-known-good BIOS image
Countermeasures	000005	Institute secure BIOS update capabilities using RTU
Catalog Maintenance	000006	Perform source code review of BIOS to identify software defects and potential vulnerabilities
	000007	Perform test and evaluation (TandE) of BIOS update mechanism
Countermeasures	000010	Restrict admin access to device
Asset Classes	000012	Enforce the 2-man rule when performing critical administrative functions
	000013	Conduct independent verification of software image once installed
Change password –	000015	Verify BIOS implemented security controls after BIOS image update
Functions	000018	Use checksums to verify the integrity of downloaded BIOS image updates
Account Managment	000020	Restrict access to the BIOS update server
Catalog Merge	000021	Use latest version of SNMP protocol
	000022	Isolate network management traffic to internal network
Spreadsheet Spreadsheet	000023	Change default SNMP community string values
Converter/Importer	000024	Restrict SNMP community string value reuse
TTP-CM Mapping Tools	000025	Configure web servers to utilize strict parsing
9	000027	Terminate client sessions after each request
2	000028	Mark all sensitive web pages as non-cacheable
5	000030	Conduct threat modeling
9	000034	Reduce attack surface
\$	000039	Convert input data
2	C000041	Use same character encoding
5	000045	Utilize high quality session IDs
2	2000047	Encrypt session cookies
2	000049	Enforce client authentication
9	000051	Use digital signatures

Approaches for mitigating attack vectors





# **Vector Groups and Taxonomies**

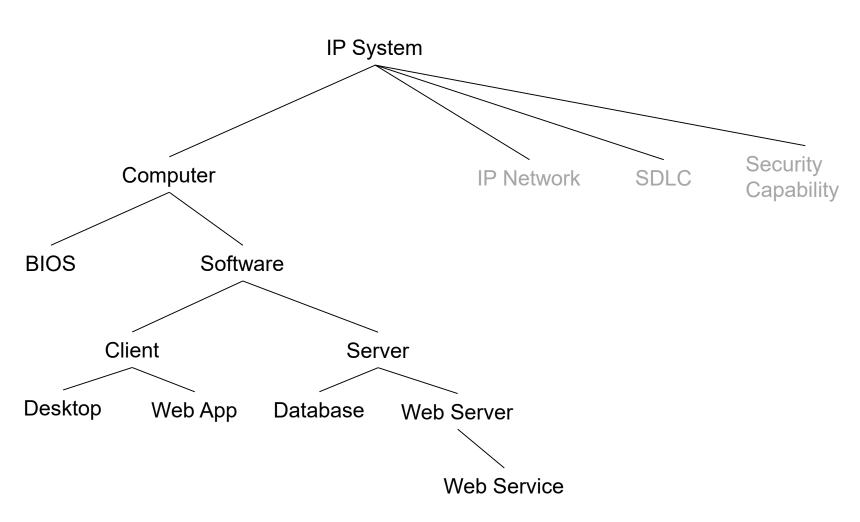
### Vector Group – Named collection of attack vectors

**Taxonomy** – Hierarchically structured collection of vector groups

p leve	Missio	on Assur	ance Engine	eering : Threat Assessment and Remediation Analysis		
p leve			and the second	eening i filleat Assessment and Kemediation Analysis		
•	l Vector	Groups				
Cor	mposite Lis	st of Attack	Vectors	Intersection of Attack Vectors		
ect 1 o	or more v	ector grou		a to your composite list of attack vectors.		
elect	<u>VG ID</u>	<u>Children</u>	and the second se	Description	Туре	Attacks
	1000 (00	10				(22)
	4000422	<u>10</u>	ATT&CK		Poot	<u>122</u>
					NOOL	
	1000387	16	CADEC		-	120
	4000387	10	CAFEC	provides a publicly available catalog of common attack patterns.	Root	120
	4000384		CM Practices	Groups of Countermeasures (CMs)	Root	Z
		-			7.000	-
	4000493	3		Organizational taxonomy representing ICS/SCADA Systems	Root	
	1000474	4			<b>D</b>	
	4000471	4	IP System	Organizational taxonomy representing IP-based, distributed systems	ROOT	
	4000409		Institute	Attack vector collection used in MITRE Institute TARA workshop	Shopping	<u>57</u>
					Cart	
	ect 1     c       /ect     ////////////////////////////////////	ect 1 or more v       vect     VG ID       A000422       A000387       A000384       A000493       A000471	A000422       10         A000387       16         A000493       3         A000471       4	Vector GroupVector GroupA00042210ATT&CKA00038716CAPECA000384CM PracticesA0004933ICS/SCADA A0004714IP System	VG ID       Children       Vector Group       Description         A000422       10       ATT&CK       Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK <sup>TM</sup> ) is a framework for describing post-compromise adversary behavior within an enterprise network.         A000387       16       CAPEC       Common Attack Pattern Enumeration and Classification (CAPEC <sup>TM</sup> ) provides a publicly available catalog of common attack patterns.         A000384       CM Practices       Groups of Countermeasures (CMS)         A000493       3       ICS/SCADA System       Organizational taxonomy representing ICS/SCADA Systems         A000471       4       IP System       Organizational taxonomy representing IP-based, distributed systems	A000422       16       CM Practices         A000422       10       ATT&CK       Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK <sup>TM</sup> ) is a framework for describing post-compromise adversary behavior within an enterprise network.       Root         A000387       16       CAPEC       Common Attack Pattern Enumeration and Classification (CAPEC <sup>TM</sup> ) provides a publicly available catalog of common attack patterns.       Root         A000384       CM Practices       Groups of Countermeasures (CMs)       Root         A000493       3       ICS/SCADA System       Organizational taxonomy representing ICS/SCADA Systems       Root



# Taxonomy Example: IP System





# Attack Vectors (AVs)

A sequence of steps performed by an adversary in the course of conducting a cyber attack

### Sources of Attack Vector data

- Open source info on attack patterns (CAPEC<sup>™</sup>), adversary TTPs (ATT&CK<sup>™</sup>), software weaknesses (CWE<sup>™</sup>), and vulnerabilities (CVE<sup>™</sup>)
- National Institute of Science and Technology (NIST) publications
- Reported security incidents from the commercial sector
- Published security research
  - Includes exploits presented at hacker conferences, e.g., Blackhat, DEFCON, ShmooCon, etc.



# **Common Attack Pattern Enumeration and Classification (CAPEC)**

### MITRE open source repository of cyber attack patterns

- Includes postulated attacks and real world security incidents
- DHS-hosted, Community-contributed, MITRE-moderated
- Updated quarterly

### CAPEC catalog includes 400+ attack patterns

- Attack patterns contributed by the security research community at large, subject to MITRE review for quality and completeness
- Patterns conform to XML schema and include fields that characterize the sophistication and resources required
  - CAPEC patterns provide analysis of underlying design weaknesses, which is key to follow-on mitigation engineering activities



# **CAPEC Taxonomy: Mechanisms of** Attack

🔿 🔤 http://capec	:.mitre.org/data/definitions/1000.html		) दे (i
Edit View Favorites			
My Mil Home 🛎 Rem	note Access Portal 🖲 TRS-Web		
	Common Attack Pattern Enumeration and Classification		
	A Community Resource for Identifying and Understanding Attacks		
me > CAPEC List	> CAPEC-1000: Mechanisms of Attack (Version 2.8) Search by	ID:	Go
ocuments	CAPEC VIEW: Mechanisms of Attack		-
ossary	View ID: 1000 Structure: Graph	Status: Draft	
Qs			
APEC List	View Objective		ι
view	This view organizes attack patterns hierarchically based on mechanisms that are frequently employed when exploiting a vulnerability. T		
wnloads	es that are members of this view represent the different techniques used to attack a system. They do not represent the consequence f the attacks.	s or goals o	£ .
cumentation lease Notes	The attacks.		
chive	✓ Relationships		
ibmit Content	Expand All   Collapse All		
mmunity			
alated Activities	1000 - Mechanisms of Attack		
scussion List	<ul> <li></li></ul>		
ontact Us	$\blacksquare \blacksquare \text{ Injection - (152)}$		
ompatibility ogram	B Deceptive Interactions - (156)		
equirements	■ Manipulate Timing and State - (172)		
irticipants	<ul> <li>              € Abuse of Functionality - (210)      </li> <li>             € Probabilistic Techniques - (223)         </li> </ul>		
ake a Declaration	$\mathbb{E}$ Exploitation of Authentication - (225)		
ews & Events alendar	$\blacksquare \oplus Exploitation of Authorization - (232)$		
ee Newsletter	Me Manipulate Data Structures - (255)		
earch the Site	■ Manipulate Resources - (262)		
	⊕ <u>Analyze Target</u> - (281)     ⊕ Gain Physical Access - (436)		
	$\mathbb{E} \subseteq \underline{Sain} = \underline{Code} = (430)$		
	B Alter System Components - (526)		

http://capec.mitre.org/

MITRE

# **Example CAPEC Attack Pattern**

	ote Access Portal TRS Web	
	Common Attack Pattern Enumeration and Classification	
<i>i</i> ape	A Community Resource for Identifying and Understanding Attacks	
> CAPEC List	> CAPEC-100: Overflow Buffers (Version 2.8)	Search by ID:
CAPEC	CAPEC-100: Overflow Buffers	
ry	Attack Pattern ID: 100 Abstraction: Standard	Status: Draft Completeness: Complete
C List	Presentation Filter: Basic	
v	▼ Summary	
ads	Buffer Overflow attacks target improper or missing bounds checking on buffer operations, typically trigg	acred by input injected by an
entation e Notes	attacker. As a consequence, an attacker is able to write past the boundaries of allocated buffer regions	
2	crash or potentially redirection of execution as per the attackers' choice.	,, 5 , 5
t Content	✓ Attack Prerequisites	
nunity Citations		
d Activities	Targeted software performs buffer operations.  Targeted software inadequately performs bounds sheeting on buffer operations	
sion List	<ul> <li>Targeted software inadequately performs bounds-checking on buffer operations.</li> </ul>	
t Us atibility	Attacker has the capability to influence the input to buffer operations.	
m	Solutions and Mitigations	
ements	Use a language or compiler that performs automatic bounds checking.	
pants	Use secure functions not vulnerable to buffer overflow.	
a Declaration & Events	If you have to use dangerous functions, make sure that you do boundary checking.	
lar	Compiler-based canary mechanisms such as StackGuard, ProPolice and the Microsoft Visual Studio /GS	flag. Unless this provides
ewsletter	automatic bounds checking, it is not a complete solution.	5
h the Site	Use OS-level preventative functionality. Not a complete solution.	

https://capec.mitre.org/data/definitions/100.html

MITRE

# Adversary Tactics, Techniques, and Common Knowledge (ATT&CK)

- Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK™) is a model for describing the actions an adversary may take while operating within an enterprise network
  - Can be used to characterize post-Exploit adversary behavior
    - Focuses on Control, Execute, and Maintain steps within the cyber attack lifecycle<sup>1</sup>
  - Can be used to help prioritize network defense against advanced persistent threat (APT) threat actors operating within the network
  - TTPs provide technical descriptions, indicators, targeted platforms, sensor data, detection analytics, and potential mitigations

http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf



# ATT&CK Taxonomy of Post Exploit Adversary TTPs

Persistence	Privilege Escalation	Defense Evasion	Credential Access	Host Enumeration	Lateral Movement	Execution	C2	Exfiltration
Leg	itimate Credenti	als	Credential	Account	Application	Command	Commonly	Automated
Accessibilit		Binary	Dumping	enumeration	deployment	Line	used port	or scripted
AddMo	-	Padding	Credentials	File system	software	File Access	Comm	exfiltration
DLL Search (		DLL Side- Loading	in Files	enumeration	Exploitation	PowerShell	through removable	Data compressed
Edit Default F	•	Disabling	Network	Group	of Vulnerability	Process	media	Data
New Se		Security	Sniffing	permission	Logon	Hollowing	Custom	encrypted
Path Inte		Tools	User	enumeration	scripts	Registry	application	Data size
Schedule	•	File System	Interaction		Pass the	Rundli32	layer	limits
Service File		Logical	Credential	Local network	hash Pass the	Scheduled	protocol	Data staged
Service File Weak		Offsets	manipulation	connection	ticket	Task	Custom	Exfil over C2
Shortcut Me		Process Hollowing	manipulation	enumeration	Peer		encryption	channel Exfil over
		Rootkit			connections	Service	cipher Data	alternate
Webs				Local	Remote	Manipulation	obfuscation	channel to
BIOS		s UAC		networking enumeration	Desktop Protocol	Third Party	Fallback	C2 network
Hypervisor		jection Indicator				Software	channels Multiband	Exfil over
Rootkit	Exploitation	blocking on		Operating		nanagement	comm	other
Logon Scripts	of	host		system		entation	Multilayer	network
	Vulnerability	Indicator		enumeration		s remote	encryption Péer	medium
Master Boot		removal from		Owner/User		gement	connections	Exfil over
Record		tools		enumeration	Remote Services		Standard app	physical
Mod. Exist'g		Indicator		Process	Replication		layer	medium
Service		removal from host		enumeration	through		protocol	From local
Registry Run		Masquerad-		Security	removable		Standard	system
Keys		ing NTFS		software	media		non-app	From
Serv. Reg. Perm.				enumeration	Shared		layer	network
Weakness		Extended		Service	webroot Taint shared		protocol Standard	resource
Windows Mgmt		Attributes Obfuscated		enumeration	content		encryption	From
Instr. Event		Pavload		Window	Windows		cipher	removable
Subsc.		Rundll32		enumeration	admin		Uncommonly	media
Winlogon Helper DLL		Scripting			shares	J	used port	Scheduled
		Software					•	transfer
		Packing	http:/	//attack.mitre.or	'n		l	

http://attack.mitre.org

Timestomp



# **An Example ATT&CK Technique**

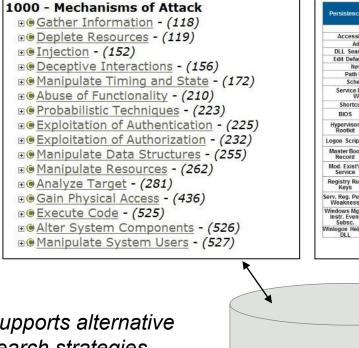
Edit View Favorites Tools		ー ロ > erability ×
ATT&CK.		v form View source View history Search Q
Main page Help Contribute References Tactics Persistence Privilege Escalation Defense Evasion Credential Access Discovery Lateral Movement	Exploitation of a software vulnerability occurs when an adversary takes advantage of programming error in a program, service, or within the operating system software or kernel itself to execute adversary-controlled code. Exploiting software vulnerabilities allow adversaries to run a command or binary on a remote system for lateral moven escalate a current process to a higher privilege level, or bypass security mechanism Exploits may also allow an adversary access to privileged accounts and credentials example of this is MS14-068, which can be used to forge Kerberos tickets using dor user permissions. <sup>[1][2]</sup>	or Exploitation of Vulnerability es may ment, ID T1068 ms. Tactic Credential Access, Defense Evasion, Lateral Movement, Privilege Escalation Blatform Windows Search 2008
Execution Collection Exfiltration Command and Control	2 Mitigation 3 Detection 4 References Examples	System Unpatched software or otherwise vulnerable Requirements target. Depending on the target and goal, the system and exploitable service may need to be remotely accessible from the internal network. In the case of privilege escalation, the adversary likely already has user permissions on the target system.
All Techniques Technique Matrix Groups All Groups	<ul> <li>FIN6 has used tools to exploit Windows vulnerabilities in order to escalate privile The tools targeted CVE-2013-3660, CVE-2011-2005, and CVE-2010-4398, all o which could allow local users to access kernel-level privileges.<sup>[3]</sup></li> </ul>	leges. Permissions User, Administrator, SYSTEM

https://attack.mitre.org/wiki/Technique/T1068

# **Catalog support for Multiple Search Taxonomies**

### TARA attack vectors mapped into alternative taxonomy structures

### **CAPEC Mechanisms of Attack**



### **ATT&CK** Tactics

Persistence	Privilege Escalation	Defense Evasion	Credential Access	Host Enumeration	Lateral Movement	Execution	62	Exfiltration
Legitimate Credentials		Credential	Account	Application	Command	Commonly	Automated	
		Binary	Dumping	enumeration	deployment	Line	used port	or scripted
AddMonitor		DLL Side-	Credentials in Files	File system enumeration	software Exploitation of Vulnerability	File Access	Comm through removable media	exfiltration Data compressed Data
DLL Search Order Hijack						PowerShell Process		
		Loading Disabling	Network	Group				
New S	ervice	Security	Sniffing	permission	Logon	Hollowing	Custom	encrypted Data size
Path Interception		File System Logical	User Interaction	enumeration	Pass the hash Pass the	Registry	application layer protocol Custom	limits Data staged
Scheduled Task				Local		Rundll32		
Service File Permission		Offsets				Scheduled		Exfil over C2
Weak		Process		connection	ticket	Task	encryption	channel
Shortcut M	Shortcut Modification			enumeration	connections	Service	cipher	Exfil over
BIOS	Bypas	IS UAC		Local	Remote Desktop	Manipulation	Data	alternate channel to C2 network
	DLL In	jection		networking		Third Party	obfuscation Fallback	
Hypervisor Rootkit	Exploitation	xploitation Indicator		enumeration	Protocol	Software		Exfil over
Logon Scripts	of Vulnerability	blocking on host Indicator		system ins	Windows m instrum	nanagement entation	Channels Multiband Comm Multilayer	other
Master Boot		removal from			Windows remote management		encryption Peer connections Standard app layer	medium
Record		tools	Owne	Owner/User				Exfil over physical medium
Mod. Exist'g		Indicator		enumeration	Continue			
Service		removal from		Process				
Registry Run		host Masguerad-		enumeration	through		protocol	From local
Keys				Security			Standard	system
erv. Reg. Perm.		NTES		software enumeration	media		non-app layer protocol Standard encryption cipher	From network resource
Weakness		Extended			Shared			
Vindows Mgmt		Attributes Obfuscated		Service	webroot Taint shared Content Windows admin			
Instr. Event Subsc.		Payload		enumeration				From removable
Jinlogon Helper		Rootkit		Window enumeration				
DLL		Rundli32				Uncommo	Uncommonly	media
		Scripting			shares	1	used port	Scheduled
		Software						transfer
		Packing						

### Supports alternative search strategies

taxonomies

Can be extended to support sponsor-defined

**Attack Vectors** 



# Other Sources of Catalog Data: Common Weakness Enumeration (CWE)

### MITRE open source repository of software weaknesses

- Over 800 weaknesses currently identified
- Updated quarterly

🏉 CWE - CWE-289: Au	thentication Bypass by Alternate Name (1.8.1) - Windows Internet Explorer provi	ided by MITRE	
🔆 🖓 🗸 🖓 http://c	we.mitre.org/data/definitions/289.html	🖌 🖌 🔛 Live Search	- 9
File Edit View Favori	tes Tools Help		
🛠 🏘 🥼 cwe - cwe	-289: Authentication Bypass by Alternate	🙆 • 📾 · 🖶 • 🔂	Page 🔹 🎯 Tools 🔹 🎇
CU	Common Weakness Enumeration		
Home > CWE List > 0	WE- Individual Dictionary Definition (1.8.1)	Search by II	): <u>60</u> =
CWE List	CWE-289: Authentication Bypass by Alter		
Development View	Authentication Bypass by Alternate	Name	
Research View	Weakness ID: 289 (Weakness Variant)	Status: I	ncomplete
About	▼ Description		
Sources	Description Summary		
Process Documents	The software performs authentication based on the name or the name of the actor performing the access, but it doe possible names for that resource or actor.	of a resource being ac s not properly check a	ccessed, all
Related Activities	<ul> <li>Time of Introduction</li> </ul>		
Discussion List			
Research CWE/SANS Top 25 CWSS	Architecture and Design     Implementation		
News	✓ Applicable Platforms		
Calendar	Languages		
Free Newsletter	All		
Compatibility	▼ Observed Examples		
Requirements	Reference Description		
Declarations Make a Declaration	CVE-2003-0317 Protection mechanism that restricts URL a URL encoding.	ccess can be bypasse	d using
Contact Us Search the Site	CVE-2004-0847 Bypass of authentication for files using "\" 5C" (encoded backslash).	" (backslash) or "%	~
		Internet	€ 100% ·

# **Uses for TARA**

- Cross-reference CWE and CAPEC to identify a range of attack patterns for a given set of software weaknesses
  - Example: Top 25 SANS/CWE weaknesses
- CWE entries identify mitigations intended to correct software weaknesses, which can be viable remediation alternatives

#### http://cwe.mitre.org/



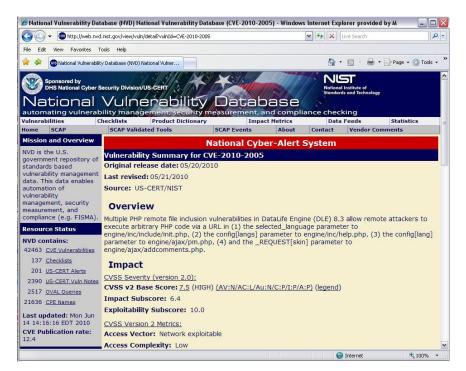
# Other Sources of Catalog Data: Common Vulnerabilities and Exposures (CVE)

# Open source repository of software vulnerabilities

- Over 79000 CVEs reported across commercial software products
- Weekly release cycle

# **Uses for TARA**

- Cross reference CVE with CAPEC attack patterns that can exploit a given software vulnerability
- Can be used to correlate vulnerabilities with specific technologies
  - Example: SNMP related attack vectors added to TARA catalog based on CVE vulnerabilities reported for SNMP agents



http://cve.mitre.org/



# **Countermeasures (CMs)**

"Actions, devices, procedures, or techniques that meet or oppose (i.e., counters) a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken." Source: CNSS 4009

### Sources of countermeasure data

- Open source info on adversary TTPs (ATT&CK), attack patterns (CAPEC), and software weaknesses (CWE) often includes mitigation details
- DoD and NIST publications, e.g., NIST SP 800-53, etc.
- Industry recognized security best practices
- Published security research
  - Journal articles detailing new approaches for detecting anomalous behavior, malware, etc.

# **Example: Software Vector Group (1/2)**

0	
File Edit View Favorites Tools	nitre.org/ACInput.aspx?ACID=A0( $\mathcal{P} \neq \mathcal{O}$ @ MAE Tools × @ Exploitation of Vulnerability  CAPEC CAPEC 100: Overflo @ New tab $\Omega \cong \Theta$
My MII Home Remote Acc	
	Mission Assurance Engineering : Threat Assessment and Remediation Analysis
Home	Vector Group Managment Interface
Records Loaded	
Vector Group Attack Vectors	VG ID: A000271 Name [editing] Created By: Software
Countermeasures	Description:
Search for	Group of attack vectors that exploit generic software vulnerabilities
Attack Vectors	Broup of attack vectors that exploit generic software vulnerabilities
Countermeasures	
Reports	Add/Update
Catalog Maintenance	Type
Vector Group	Sub-tree 🗸 Sub-tree
Attack Vectors	Keyword: Add Keyword Make subgroup of:
Countermeasures	· · · · · · · · · · · · · · · · · · ·
Admin Functions	Add Group
Catalog Export/Import	Child Of:
Account Management	□ A000476 - Computer - Parent Group(s)
Catalog Merge Tool	
Data Schemas	Remove Related Group(s)
Spreadsheet Template Converter/Importer	Parent of:
AV-CM Mapping Tools	• A000403 - API
	• A000235 - OS
	• A000330 - Web 2.0 - Subgroup(s)
	• A000357 - VM
	• <u>A000035 - XML</u>



# **Example: Software Vector Group (2/2)**

### **Attack Vectors**

<u>AV ID</u>	AV Name	<u>CM ID</u>
<u>T000019</u>	Using slashes, escaped slashes, or UTF-8 encodings to bypass input validation	<u>C000152</u>
<u>T000020</u>	Xquery Injection	<u>C000187</u>
<u>T000024</u>	Malicious Software Update	<u>C000235</u>
<u>T000026</u>	Accessing Functionality Not Properly Constrained by ACLs	<u>C000090</u>
<u>T000027</u>	Manipulating Input to File System Calls	<u>C000117</u>
<u>T000028</u>	Manipulating User-Controlled Variables	<u>C000242</u>
<u>T000030</u>	JSON Hijacking (aka JavaScript Hijacking)	<u>C000248</u>
T000032	XPath Injection	<u>C000091</u>
<u>T000036</u>	Log Injection-Tampering-Forging	<u>C000051</u>
<u>T000037</u>	Accessing, modifying or executing executable files	<u>C000234</u>
<u>T000038</u>	Manipulation of resources loaded by a software application	<u>C000238</u>
<u>T000041</u>	Exploit race conditions and/or deadlock conditions in software	<u>C000253</u>
<u>T000049</u>	Buffer Overflow	<u>C000121</u>
<u>T000055</u>	Target Programs with Elevated Privileges	<u>C000118</u>
<u>T000058</u>	Manipulating Writeable Terminal Devices	<u>C000244</u>
<u>T000067</u>	XML Ping of Death	<u>C000144</u>

### Countermeasures

<u>CM ID</u>	<u>CM Name</u>
<u>C000152</u>	Conduct penetration testing
<u>C000187</u>	Configure COTS hardware/software to disable unnecessary features and functions
<u>C000235</u>	Isolate network segments to limit exploitation of vulnerabilities
<u>C000090</u>	Validate input fields use of NULL, escape, backslash, meta, and control characters
<u>C000117</u>	Apply principle of least privilege
<u>C000242</u>	Regulate remote or external access through DMZs
<u>C000248</u>	Harden IT assets
<u>C000091</u>	Apply blacklist and whitelist validation in combination
<u>C000051</u>	Use digital signatures/checksums to authenticate source of changes
<u>C000234</u>	Design to log securely
<u>C000238</u>	Enforce software quality standards and guidelines that improve software quality
<u>C000253</u>	Establish a verifiable software update / patch management process
<u>C000121</u>	Verify input sources
<u>C000118</u>	Enforce default-deny access policies
<u>C000244</u>	Restrict network traffic
<u>C000144</u>	Encrypt sensitive data persistently stored



#### Entries are a partial listing, in no particular order

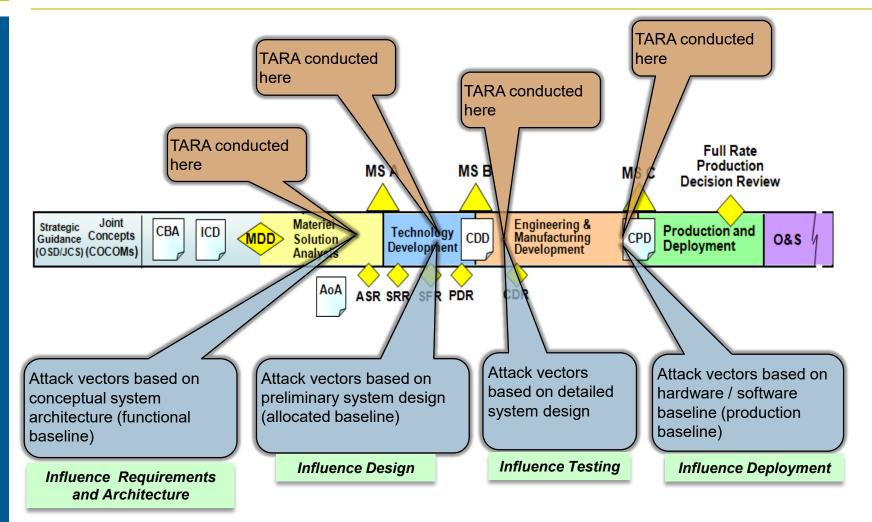
© 2020 The MITRE Corporation. All rights reserved.

Approved for Public Release; Distribution Unlimited, Case 20-0272.

# Applications of TARA



# **Threat-Informed Systems Analysis for Acquisition Programs**





# **Applications of TARA**

### Threat Model Development

 TARA can be used to develop cyber threat models that identify plausible cyber attacks for specified cyber threat actors

### Cyber Risk Remediation

TARA can be used to identify and select countermeasures that mitigate risks from identified cyber attacks

### Cyber Resiliency Assessment

 TARA can be used to select resilience techniques to reduce the risk from identified cyber attacks

### Vulnerability Assessment / Penetration Test Planning

 TARA assessment recommendations can be recast as vulnerability or penetration test objectives

# Supply Chain Risk Management (SCRM) Analysis

 TARA can be used in conjunction with specialized catalog of supply chain threats and countermeasures



# **Risk Management Framework (RMF)**

RMF is a United States federal government policy and standards for securing information systems (computers and networks) developed by National Institute of Standards and Technology

### Applications of TARA within RMF include

### - Tailoring 800-53 controls

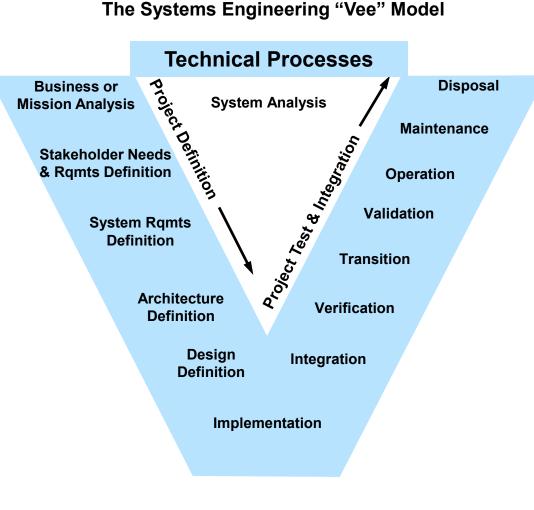
 The Risk Management Framework (RMF) supports program tailoring of security controls based on cost/benefit and risk tradeoffs. TARA has been applied in a limited context to the selection of 800-53 controls.

### Development of threat models

 Specific NIST 800-53 controls call for use of threat modeling "to identify use cases, threat agents, attack vectors, and compensating controls and design patterns to mitigate risk." TARA is used to develop cyber threat models that identify attack vectors, assesses their risk, and identifies mitigating countermeasures.



# **System Life Cycle Processes**



#### ISO/IEC/IEEE 15288, System life cycle processes, 2015-05-15

### Agreement Processes

- Acquisition
- Supply

### Organizational Project-Enabling Processes

- Life Cycle Model Mgmt
- Infrastructure Mgmt
- Portfolio Mgmt
- Human Resource Mgmt
- Quality Mgmt
- Knowledge Mgmt

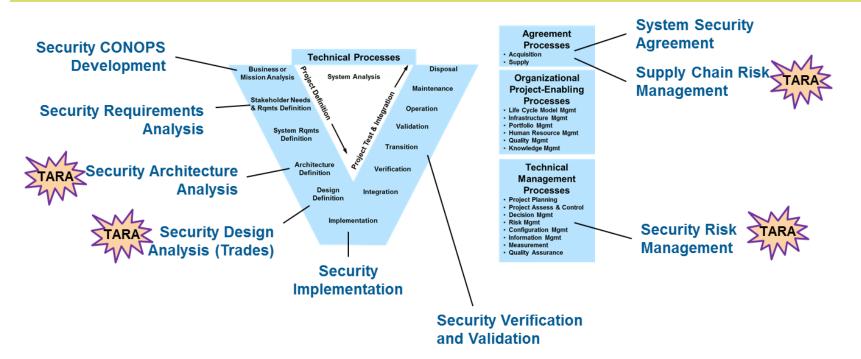
### Technical Management Processes

- Project Planning
- Project Assess & Control
- Decision Mgmt
- Risk Mgmt
- Configuration Mgmt
- Information Mgmt
- Measurement
- Quality Assurance

32



# Systems Security Engineering (SSE) Framework

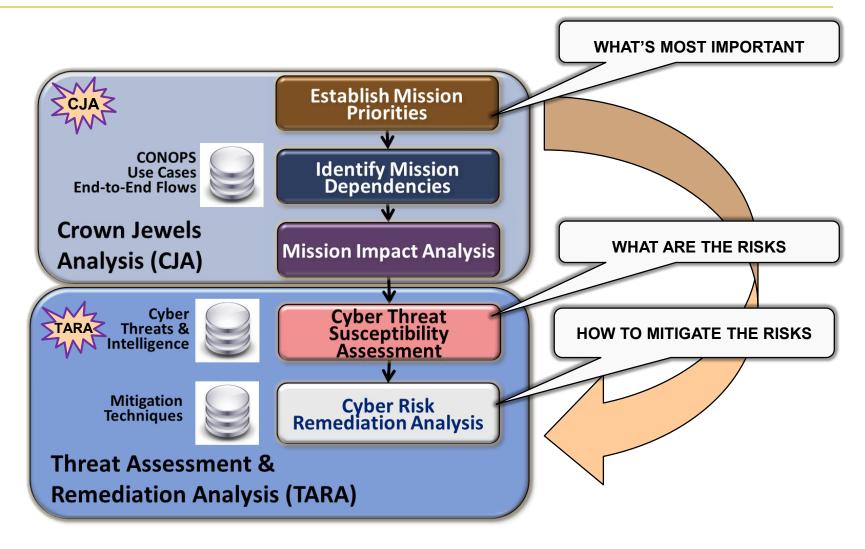


# **Applications of TARA in the SSE Framework**

- Security architecture analysis and threat model development
- Countermeasure selection (trade)
- Cyber risk assessments
- SCRM assessments



# MITRE Mission Assurance (MA) Process Framework





# **CJA and TARA**

### Crown Jewel Analysis (CJA)

 CJA is a process for identifying mission-critical cyber assets, enabling us to focus risk mitigation measures where they will be most effective

### CJA and TARA can be performed separately or together

When performed together, CJA and TARA support identification, assessment, and mitigation of cyber risk to mission critical assets

### TARA use of CJA results

- Identified mission critical cyber assets (crown jewels) can be the focus of a TARA assessment
- Mission impact used in assessment of attack vector risk
  - TARA performs triage on large lists of attack vectors based on risk
- CJA mission impacts used in TARA assessment recommendations
  - A compelling TARA recommendation uses potential mission impacts to justify implementation of selected countermeasures



# **Summary**

- TARA is an engineering approach that is rigorous and repeatable, provides traceability, identifies gaps, and develops defense-indepth
- TARA's objective is to influence programs early in the acquisition lifecycle where the cost of change is less
- TARA applies model-based systems engineering and tradeoff analysis to system security engineering
- TARA maintains and utilizes catalogs of attack vector and countermeasure data that incorporates data from a variety of sources including CAPEC, CWE, and CVE
- The TARA approach is flexible and can be tailored to meet the needs of users
- TARA has been applied to over 2 dozen Army, Navy, Air Force, and DoD acquisition programs

**The MITRE Corporation** 

# **TARA Cyber Threat Modeling**



© 2020 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited, Case 20-0272.

### **Objectives**

- Discuss elements of a cyber threat model
- Discuss attack surface modeling
- Discuss cyber threat scenarios



## **Cyber Threat Models**

TARA can be used to develop cyber threat models that identify plausible cyber attacks for specified cyber threat actors

### Key Elements

- Cyber Threat Actor Profiles
  - Used to represent adversary capability and intent
- Exploitable Attack Surface features
  - Used to identify attack vectors and associated effects

#### Optional Elements

- Assessed Risk
- Plausible Countermeasures



## **Cyber Threat Actors**

- Cyber threat actors include organizations or individuals that have the motivation, intent and capability to cause harm
  - Common examples include nation state actors, transnational actors, criminal organizations, trusted insiders, etc.
- Some Definitions (courtesy of Merriam Webster)
  - Motivation
    - The reasons for acting or behaving in a particular way
  - Intent
    - A determination (resolve) to act in a certain way
      - Motivation leads to Intent
  - Capability [cyber]
    - The facility for use or deployment [of disruptive cyber effects]

Threat actor motivations, intentions, and capabilities continuously change



### **Example Threat Actor Intentions**

- Discover system architecture, network topology, security capabilities, etc.
  - Motivation: To identify ways to exploit the system

#### Monitor system utilization

- Motivation: To provide early indications and warnings (I&W)

#### Exfiltrate sensitive or classified data

Motivation: Intelligence collection

#### Establish durable, persistent access

- Motivation: To provide quick and stealthy penetration
- Disrupt: Momentary loss of use
- Deny: Longer term loss of use
- Destroy: Permanent loss of use
- Degrade: Reduced capacity or performance
- Deceive: Loss of data integrity and/or situational awareness
  - Motivation: To achieve disruptive cyber effects on mission critical and mission essential systems or components (when necessary)



## **Example Threat Actor Cyber Capabilities**

#### Reconnaissance

- Use of open source intelligence (OSINT) to identify targets
- Exfiltration of system data from cleared defense contractors (CDCs)
- Identification of key system users via social media

#### Weaponization

- Develop injects that exploit known, unpatched vulnerabilities
- Use of open source rootkits
- Use of vulnerability analysis to identify zero-day exploits in commercial products
- Weaponization of zero-days purchased on the dark web
- Use of reverse engineering to develop new malware variants

#### Delivery

- Use of commercial penetration testing / vulnerability scanning tools
- Use of TOR to stage attacks anonymously
- Exploitation of supply chain vulnerabilities to deliver implants
- Use of air-gap malware
- Co-opting / recruitment of trusted insiders

#### C2

- Use of encrypted C2 to manage implants and for bulk exfiltration of data



## **Cyber Threat Actor Profile**

# A Cyber Threat Actor Profile provides comparative analysis of threat actor motivation, intent, and capability

- Threat actor motivation, intent, and capabilities vary widely
  - Motivation and intent of a regional threat actor may be significantly higher for regionally deployed systems
- Projected adversary cyber capabilities for 2020, 2025, etc. can be especially useful for acquisitions programs

			1														1
Threat Actor	Motivation	Intent	Finances (Annual)	Use of OSINT	Exfiltration through CDCs	Use of Social Media	Exploits unpatched vulnerabilities	Open source rootkits	Develops new zero- days	Purchases zero-days	Malware reverse engineering	Commercial scanning tools	Custom scanning tools	Use TOR to stage attacks	Supply chain implants	Recruits trusted insiders	Uses encrypted C2
Nation State Actor X	твр	тво	>1B	Demo'd	Demo'd	Demo'd	Demo'd	Demo'd	Demo'd	Likely	Demo'd	N/A	Demo'd	Likely	Likely	Demo'd	Demo'd
Nation State Actor Y	твр	тво	>500M	Demo'd	Possible	Demo'd	Demo'd	Demo'd	Likely	Possible	Likely	Demo'd	Possible	Unlikely	Unlikely	Possible	Demo'd
Crime Syndicate A	Steal money	Deny use of systems	>200M	Possible	Unlikely	Possible	Demo'd	Likely	Possible	Possible	Possible	Demo'd	Possible	Possible	Possible	Possible	Likely
Transnational Group 1	TBD	TBD	>50M	Possible	Unlikely	Likely	Likely	Likely	Unlikely	Unlikely	Unlikely	Possible	Unlikely	Unlikely	Unlikely	Possible	Likely
Disgruntled Employee	Perceived unfair treatment	Revenge	N/A	N/A	Possible	N/A	Likely	N/A	N/A	N/A	Unlikely	Demo'ed	N/A	N/A	Possible	Unlikely	Possible
Careless User	Minimal effort; lazy	Non malicious	N/A	N/A	N/A	N/A	Unlikely	N/A	N/A	N/A	N/A	Possible	N/A	N/A	Unlilkely	Unlikely	N/A

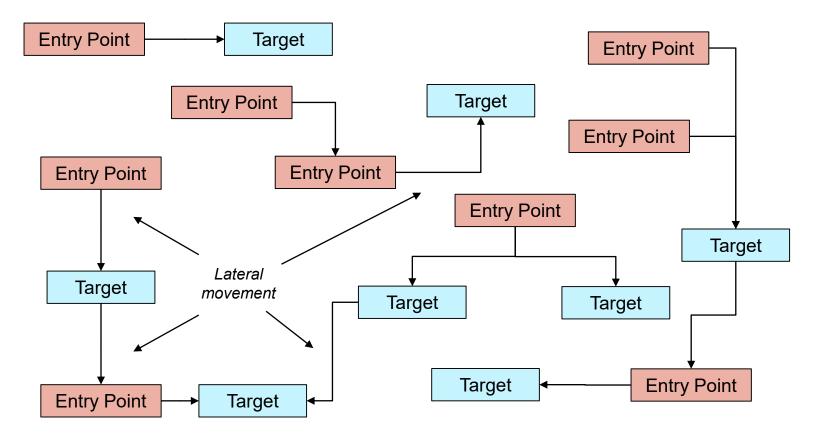
#### Threat Actor Cyber Capabilities

#### **Example Cyber Threat Actor Profile**



### **Exploitable Attack Surface Features**

"Attack surface is the set of ways in which an adversary can enter the system and potentially cause damage."\*



\*Manadhata, P.,. "An Attack Surface Metric", Carnegie Mellon University, CMU-CS-08-152, November 2008.

### **Attack Vectors Redefined**

- Originally: A sequence of steps performed by an adversary in the course of conducting a cyber attack
- Redefined: A sequence of steps performed by an adversary to get from an Entry Point to an Intended Target
  - Entry Points and Targets are attack surface features
    - Both compromised by exploiting a known or unknown vulnerability
  - Lateral Movement is the adversary's means (tradecraft) to get from an Entry Point to an intended Target
    - There can be multiple paths between an Entry Point and a Target
    - The same Entry Point can get to multiple Targets
    - Multiple Entry Points can get to the same Target
    - An Intended Target (once compromised) can become an Entry Point

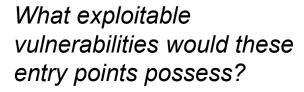


### **Example Entry Points**

- User accounts
- Hidden backdoors
- USB ports
- Database query fields
- Unsecured web applications or web pages
- Email attachments, downloads, etc.
- Processes for system upgrades or maintenance
- Modem connections (Remember the movie Scanners?)
- Temporary network connections
- Vendor or partner connections

An entry point can be structural, permanent, temporary, and can exist at any point in the system lifecycle

Approved for Public Release: Distribution Unlimited. Case 20-0272.





### **Example Targets**

- Mission critical and mission essential subsystems, components and assets
- System interfaces, APIs, etc. used to access and manage mission and system configuration data

47

- Special purpose algorithms
- System security features and perimeter access capabilities
- Critical Program Information (CPI)
- Baseline system configuration data
- IP network infrastructure / topology
- Data storage capabilities
- Supporting SCADA infrastructure, e.g., power distribution, HVAC, etc.
- Key development and testing facilities
- Critical component supply chains
- Key personnel
- Key locations

## **Cyber Threat Scenarios**

A cyber threat scenario is a narrative description that extends the attack vector with contextual information to better frame the cyber threat

Scenario Details	Description
Motivation	Reason(s) that drive an adversary's intent
Threat actor	The adversary initiating an attack
Effect(s)	1st order (component), 2nd order (system), and 3rd order (mission) effects
Vulnerability	The underlying vulnerability to be exploited (in the target)
Perimeter entry point	Weakness through which adversary gains access to target
Targeted component	Component being targeted for effect
Indicator [of compromise]*	Observable (detectable) characteristics that the attack has occurred (is occurring)
Likelihood*	Probability the attack will be successful
Impact*	Magnitude of harm caused by a successful attack
Risk*	The assessed risk
Mitigation(s)*	Countermeasure(s) that reduce the likelihood or impact of a successful attack

#### \*Denotes optional scenario details



### **Example Cyber Threat Scenario**

#### Narrative Description

In conjunction with military operations, nation state X intends to disrupt plant operations by exploiting cyber vulnerability ICSA-14-079-01 in the Siemens SIMATIC S7-1200 Programmable Logic Controller (PLC) that regulates circulation of pressurized coolant within the Boiler Level / Pressure Control System. Disruption of the pressure control system may result in unscheduled plant shutdown. Indicators of this attack include specially crafted packets sent to the PLC on port 102/TCP (ISO-TSAP). This attack vector poses a low likelihood, moderate impact risk

#### Scenario Elements

- Motivation: In conjunction with military operations
- Threat Actor: nation state X
- Effect(s): 1<sup>st</sup> order: disable PLC; 2<sup>nd</sup> order: disrupt pressure control system; 3<sup>rd</sup> order: trigger plant shutdown (deny)
- Vulnerability: ICSA-14-079-01
- Targeted component: Siemens SIMATIC S7-1200 PLC
- System impacted: Boiler Level / Pressure Control System
- Indicator(s): crafted packets on port 102/TCP (ISO-TSAP)
- Risk: low likelihood, moderate impact

Reference: https://ics-cert.us-cert.gov/advisories/ICSA-14-079-01

## **Cyber Threat Scenario Development**

- Identify threat actors
- Evaluate attack surface entry points and targets
- For each target
  - Identify potential entry points
    - The most plausible scenario(s) tend to use the most accessible entry point(s) and the least lateral movement
  - Evaluate first, second, third order effects
    - CJA results will inform effects analysis
  - Identify indicators that an attack has occurred or is occurring
    - Indicators include observables associated with lateral movement and component disruption
  - Assess risk
  - Identify potential mitigations



### Summary

This brief discusses cyber threat actor profiles and attack surface modeling

- Cyber threat actor profiles represent capability and intent of cyber threat actors
  - Different threat actor profiles for different systems, capabilities, regions of the world, etc.
- Attack surface modeling identifies plausible attack vectors that target system components with disruptive effects, e.g., disrupt, deny, destroy, etc.
  - The vector model considers adversary lateral movement from an initial (exposed) system entry point to an intended target
- Cyber Threat Scenarios develop narrative descriptions by adding contextual information to attack vectors
  - 1<sup>st</sup>, 2<sup>nd</sup>, and 3<sup>rd</sup> order effects derived from CJA results
  - Exploitable vulnerability
  - Indicators of compromise, assessed risk, and mitigations (optional)



**The MITRE Corporation** 

# TARA Cyber Threat Susceptibility Analysis



© 2020 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited, Case 20-0272.

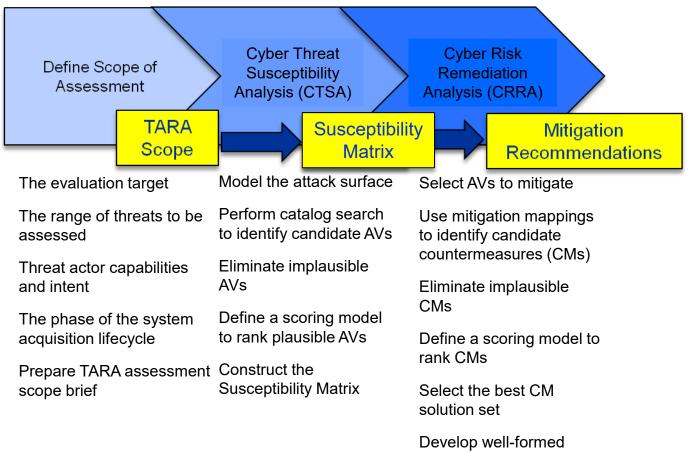
### **Objectives**

- Discuss TARA scoping considerations
- Discuss Cyber Threat Susceptibility Analysis (CTSA)
- Exercise #1: Creating a shopping cart



### **Phases of a TARA Assessment**

Objective to identify and assess cyber threats and select countermeasures effective at mitigating those threats



recommendations

#### **MITRE**

## **TARA Scoping Considerations**

#### Evaluation target

CJA results can help scope a TARA assessment to focus on mission critical systems and components

#### Threat actor capability and intent

- Identify key adversary capabilities to assess threat actors
- Attack surface analysis
  - Develop a representative, i.e., not exhaustive, set of plausible attack vectors

#### Staffing is critical

- Need experienced SSEs who can *think like the adversary* 

#### Schedule and funding constraints

- Level of effort estimate 10 14 staff weeks (ballpark)
  - Additional time may be needed to produce assessment reports
- Large assessments can be performed incrementally

#### Deliverables may be classified

- Executive Order (EO) 13526 may apply
- Logistics for handling classified data



### Work Breakdown Structure (WBS)

Notiona	I TARA Work Breakdown Structure (WBS)	Level of Effort (LO			
NOtiona	TIARA WORK BIEAKOOWITSTRUCTURE (WBS)	Staff Weeks	Staff Hours		
1	Threat Susceptibility Analysis				
1.1	Develop Cyber Threat Model	3	120		
1.2	Identify Plausible Attack Vectors	1	40		
1.3	Perform Risk Assessment	1	40		
2	Risk Remediation Analysis				
2.1	Identify Plausible Mitigations	2	80		
2.2	Assess Mitigation Utility and Cost	1	40		
2.3	Perform Mitigation Selection	1	40		
3	Knowledge Management				
3.1	Prioritize Information Needs	1	40		
3.2	Identify and Evaluate External Data Sources	2	80		
3.3	Update Catalog	1	40		
	LOE Totals	13	520		

## 13 staff weeks (~500 staff hours) is a ballpark estimate for a TARA assessment *(your mileage may vary)*



## Information Used in a TARA Assessment

Technical details about the system are needed in order to model its attack surface and identify plausible attack vectors

- Mission capabilities, system logical and physical architecture, external interfaces, management interfaces, types of mission data stored and processed, critical program information, security capabilities, security perimeters, user roles and permissions, use of COTS, etc.
- There is no laundry list of data, no minimum. However more is not always better...
  - Availability of data depends on the lifecycle phase of the acquisition program and on what contractor data/deliverables are on contract
    - Previous TARA assessments have found use of CONOPS, system architecture documents, Crown Jewels Analysis (CJA) results, operating manuals, DODAF views, hardware and software baseline info, DIACAP package details, etc.
    - TARA is often conducted in the PDR to CDR timeframe when much of this data is likely to exist



# WARNING!

### Make sure you obtain the Security Classification Guide (SCG) <u>prior</u> to conducting a TARA assessment

The SCG will specify the classification level of information collected and developed during the assessment

The SCG will identify the clearance level required for staff conducting the assessment, and whether classified processing is required



### **TARA Scope Brief Outline**

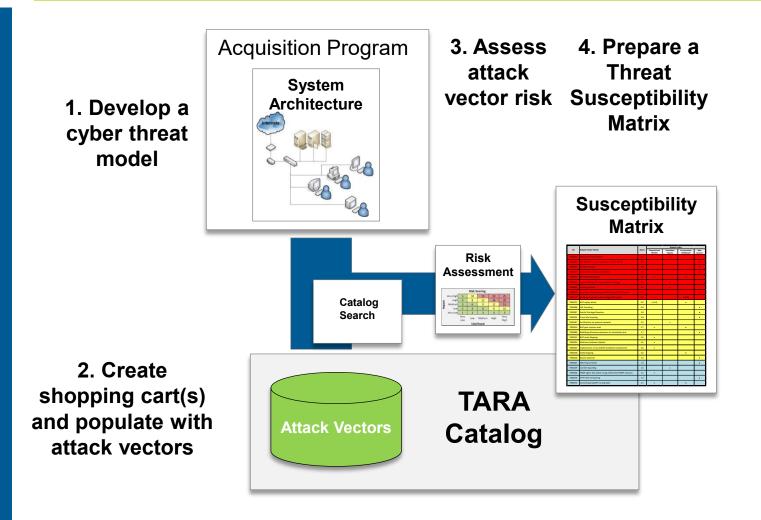
- Purpose
  - Details the plan to conduct a TARA assessment
- Audience
  - MITRE project management; program/project sponsor

#### Content

- The system being assessed, i.e., evaluation target
- The range of threat actors and capabilities
- Network diagrams, DODAF views, etc.
- Aspects of the system that are in scope and out of scope
- System technical information requirements
- The range of countermeasures being considered
- The types of recommendations
- Staffing and schedule
- Data classification and processing requirements



### **Cyber Threat Susceptibility Analysis (CTSA)**





### **CTSA Workflow Details**

#### Develop a cyber threat model

 Based on threat actor range of capabilities, exploitable attack surface of entry points and targets, and known attack patterns

#### Create shopping cart(s) and populate with attack vectors

- New and existing (catalog) attack vectors added to shopping cart(s)
- Multiple shopping carts can be used to organize the work

#### Assess attack vector risk

 Compute a risk score for each attack vector that will be used to rank vectors in the Susceptibility matrix

#### Prepare Susceptibility Matrix

 TARA artifact used to transition from CTSA step Cyber Risk Remediation Analysis (CRRA) activity



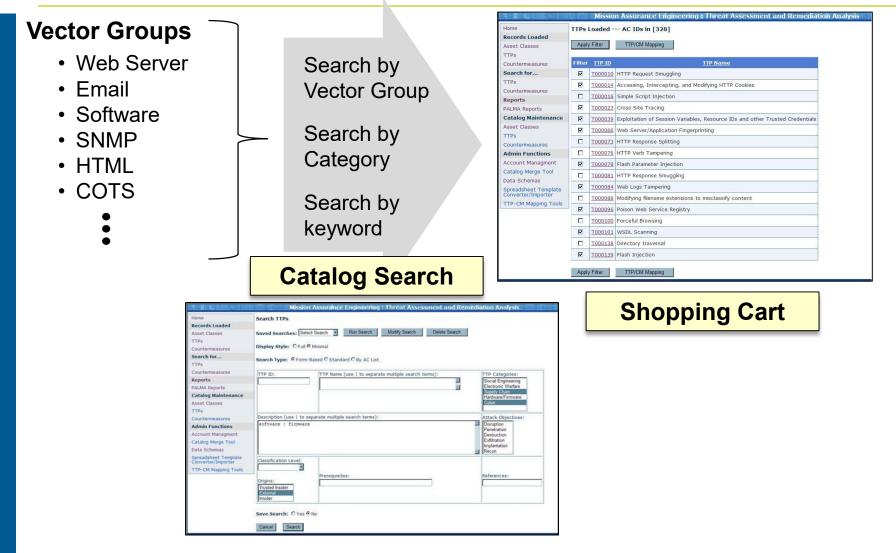
## **Developing the Cyber Threat Model**

- Cyber Threat Actor Profile used to identify adversary intent and range of capabilities
  - Discussed previously
- Exploitable attack surface features and known attack patterns used to identify plausible attack vectors
  - Attack vectors based on Entry Points and Targets
    - Discussed previously
  - Attack vectors based on known attack patterns and TTPs, e.g., CAPEC, ATT&CK, etc.
    - Over 400 attack vectors are currently stored in the TARA catalog and discoverable using catalog search tools

# TARA cyber threat models can leverage open source attack pattern data stored in TARA catalog



## **Populating a Shopping Cart**





## **Shopping Cart Example**

Filter	AV ID	AV Name
ঘ	<u>T000004</u>	Malware reflashes device with malicous BIOS
P	<u> 1000006</u>	Insider uploads malicious BIOS to update server for enterprise-wide distribution
4	T000031	Choosing a Message/Channel Identifier on a Public/Multicast Channel
4	<u>T000040</u>	File System Function Injection, Content Based
4	<u>T000085</u>	Cache Poisoning
4	<u>T000091</u>	Router DoS using TCP protocol messaging
4	<u>T000095</u>	Exploitation of built-in back doors
d	<u>T000113</u>	Router configuration access via crafted HTTP request
4	<u>T000114</u>	Route forwarding misconfigured using multicast join messaging
ব	<u>T000126</u>	MITM attacks on KVM switch
न	<u>T000128</u>	Router DoS using malformed IP packets
4	<u>T000134</u>	Using malware signature generation capabilities to conduct a DDoS attack, aka allergy attacks
ব	<u>T000145</u>	Cisco IOS Software TCP Denial of Service Vulnerability
d	<u>T000151</u>	Gain access using default usernames and passwords
व	<u>T000153</u>	Scanning for default ports to identify installed COTS software
q	<u>T000160</u>	Compromised automated software installation processes
4	<u>T000167</u>	IDS/IPS not configured to detect adversary reconnaissance or penetration attempts
ব	<u>T000168</u>	DoS attack on IDS/IPS disrupts network connectivity
q	<u>T000173</u>	Message traffic to disable or bypass IDS/IPS filters
ব	<u>T000174</u>	Using crafted content to disable or bypass antivirus capabilities
ন	<u>T000175</u>	TCP SYN packets used for host discovery and to bypass misconfigured firewalls
ব	<u>T000176</u>	UDP pings used for host discovery and to bypass misconfigured firewalls
ব	<u>T000177</u>	Use of TCP ACK segments to gather information about deployed firewalls
ব	<u>T000178</u>	Stateless firewalls ineffective against certain port scanning techniques
R	<u>T000179</u>	Malware targets PKI readers
d	<u>T000181</u>	Malicious software implantation through 3rd party bundling
a	<u>T000228</u>	Virtual Machine (VM) embedded malware
ব	<u>T000257</u>	Router stack overflow arbitrary code execution
न	<u>T000261</u>	Malware Attacks

- Example includes attack vectors from the firewall, IDS/IPS, malware, and network appliance vector groups
- Catalog search tools can be used to add additional attack vectors to the shopping cart
- There will always be unknown risks – objective is to identify a representative NOT exhaustive list of attack vectors to assess using TARA

### **Assessing Attack Vector Risk**

#### Sometimes the shopping cart contains too many vectors

 More than 25 attack vectors can be difficult to evaluate in a single TARA assessment

#### Risk scoring used to rank attack vectors

 Lower risk attack vectors can be omitted from CRRA step, i.e., treated as residual risk or deferred to follow on assessment

#### Different risk assessment approaches can be used

- Approaches include risk cubes, weighted sums, multi-attribute utility analysis (MAUA), etc.
  - CJA results can help calibrate risk based on mission impacts when a system or component is compromised



### **Risk Calculators**

Risk score calculated for each attack vector as a weighted sum of risk factors:

Risk Score ~  $\Sigma$  ( (risk factor value)<sub>*i*</sub> \* (factor weighting)<sub>*i*</sub> )

Risk Factor	Q	ualitative Efi ر		Factor Neigh		Ris	k Fac	tor Va	lues	]
Factors for assessing TTP Risk	Factor	Attack Vectors								
Factor Range	Low = 1	Medium = 2	High = 3	Weight	T000001	T000008	T000016	T000021	T000049	T000105
Locality: How localized are the effects posed by this TTP?	isolated to single unit	external networks potentially impacted	all units globally and associated infrastructure	0.2	1	2	1	2	2	3
Impact: How serious an impact is loss of data confidentiality resulting from successful application of this TTP?	no impact from TTP	limited impact requiring some remediation	Data spills routinely exercised	0.2	2	1	1	1	2	3
Impact: How serious an impact is loss of system availability resulting from successful application of this TTP?	no impact from TTP	limited impact requiring some remediation	Simulated system outages routinely exercised	0.2	1	1	2	2	1	2
Prior Use: Is there evidence that this TTP has been successfully used before?	no evidence of TTP use	confirmed evidence of TTP use	widespread use of TTP reported	0.3	2	3	3	1	2	1
Stealth: How detectable is this TTP when it is applied?	TTP obvious without monitoring	detection likely with routine monitoring	undetectable	0.1	2	2	1	1	1	2
			Score	1.0	1.6	1.9	1.8	1.4	1.7	2.1

#### Alternative risk calculators discussed later in the training



## **Susceptibility Matrix Example**

				Shopp	ing Carts	
ID	Attack Vector	Risk Score	External Router	Internal Router	Web Server	Workstation
T000259	Malicious email content	2.7				x
T000040	File System Function Injection, Content Based	2.6			x	
T000261	Malware attacks	2.6			x	
T000019	Alternate Encoding combination	2.2			x	
T000250	BGP route disruption	2.1	x	x		
T000015	Cross Site Request Forgery (Session Riding)	2.1				x
T000260	Phishing Attacks	2.1				x
T000014	Accessing, Intercepting, and Modifying HTTP Cookies	2.1			x	
T000128	Malformed packet used to trigger DoS attack	2.0	x	x (1.3)		
T000253	BGP replay attack	2.0	x (1.4)	x		
T000098	URL Encoding	2.0			x	
T000097	Restful Privilege Elevation	2.0			x	
T000105	Cross Site Scripting	2.0			x	
T000187	Ex-filtration via external network	1.9				x
T000254	BGP peer session reset	1.7	x	x		
T000088	Modifying filename extensions to misclassify content	1.7			x	
T000255	BGP route flapping	1.6	x			
T000024	Malicious Software Update	1.6	x			
T000163	Implantation of counterfeit hardware components	1.6	x			
T000258	VLAN Hopping	1.6		x		
T000020	Xquery Injection	1.5			x	
T000067	XML Ping of Death	1.4			x	
T000169	Content Spoofing	1.3				x
T000046	SNMP agent DoS attack using malformed SNMP requests	1.3	x			
T000076	HTTP Verb Tampering	1.3			x	
T000252	Eavesdropping BGP routing data	1.1	x	x		

- Produced during CTSA
- Details attack vectors assigned to different shopping carts
  - Separate column for each shopping cart
- Lists top 20 25 highest risk attack vectors across all shopping carts
  - Highest risk vectors on top
- Risk scores depends on scoring model used
  - May be qualitative or quantitative
- Vector risk scores may be different for each shopping cart
  - Conflict resolution: highest risk score used with lower score noted

## **Exercise #1: Creating a Shopping Cart**

- 1. Go to the vector group maintenance page by clicking on Vector Group under Catalog Maintenance
- 2. Enter a vector group name, provide a description, Add/Update
- 3. Find your new vector group on the vector groups page under Records Loaded
- 4. Open it
- 5. Use the selection box at the bottom to add 3-4 attack vectors to the vector group (Use the Add New button to add the entry)
- 6. Go to the attack vectors search form under Search for...
- 7. Perform a keyword search in the description field (your choice of keywords)
- 8. Select 1-2 attack vectors and add them to your vector group
- 9. Perform a filtered search on the attack objectives field
- **10**. Select 1-2 attack vectors and add them to your vector group



### Your Turn...

#### Create a shopping cart titled (your name)

 Add 7 – 10 attack vectors to your shopping cart for an evaluation target consisting of a web application running on a web server

#### Discussion

- Did you find everything that you were looking for?
- How do your shopping carts compare?
- How did you model the target, e.g., interfaces, perimeters, etc.?
- What information about the evaluation target would be useful?
- What filtered and keyword searches do you perform?
- How to distinguish between what's plausible and what's not?



### **Summary**

#### Establishing the Assessment Scope

- Range of threats and countermeasures, schedule, staffing, etc.
- Scoping brief

#### Cyber Threat Susceptibility Analysis (CTSA)

- Develops attack vectors based on system attack surfaces and evaluates catalog attack vectors based on CAPEC attack patterns
- Uses shopping carts to construct persistent lists of attack vectors
- Applies risk scoring to rank (select) vectors for remediation
- Susceptibility Matrix

#### Exercise #1: Creating a shopping cart



**The MITRE Corporation** 

# TARA Cyber Risk Remediation Analysis



© 2020 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited, Case 20-0272.

### **Objectives**

Discuss Cyber Risk Remediation Analysis (CRRA)

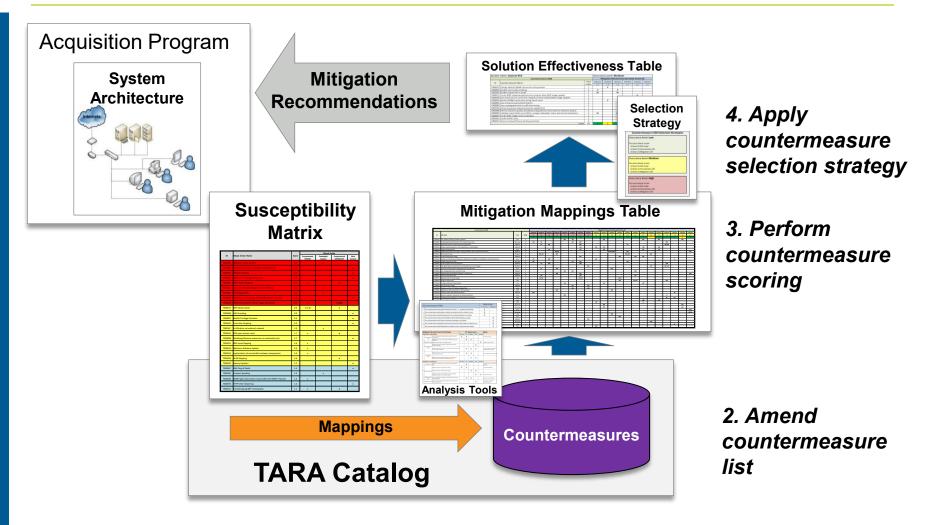
- Worked example: Apply countermeasure scoring and selection strategy to develop an optimized solution set
- Exercise #2: Exporting catalog data



### **Cyber Risk Remediation Analysis (CRRA)**

73

MITRE



### 1. Obtain initial list of countermeasures

© 2020 The MITRE Corporation. All rights reserved. Approve

# **CRRA Workflow Details**

### Obtain initial mitigation mapping table

 Countermeasure mapping data for attack vectors in Susceptibility Matrix used to obtain initial list of countermeasures

### Amend countermeasures list

 Add countermeasures and/or mappings to fill gaps and address scoping requirements; remove countermeasures that don't apply

### Perform countermeasure scoring

 Compute utility/cost (U/C) ratio for each CM; reorder mitigation mapping table to rank countermeasures based on U/C scores

### Apply a countermeasure selection strategy

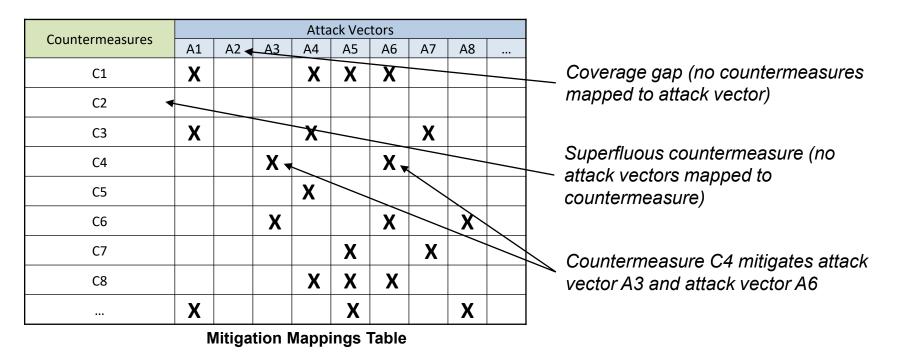
 Execute selection strategy to identify countermeasures for the Solution Effectiveness Table



# **Mitigation Mappings Table**

### A mitigation mapping table conveys the effects that countermeasures have over a range of attack vectors

- Attack vectors represented as columns in the mapping table
- Countermeasures represented as rows in the mapping table
- Matrix cells identify what effect a countermeasure has on an attack vector





# **Countermeasure Effects**

- A countermeasure can have 3 potential effects on an attack vector
  - Prevent (denoted by a 'P')
    - The countermeasure eliminates conditions that make the attack possible

### - Detect (denoted by a 'D')

 The countermeasure makes it possible to determine if the attack has occurred, is occurring, or potentially could occur

### Respond (denoted by a 'R')

The countermeasure reduces the likelihood that the attack will occur, or its impact will be significant

A countermeasure can have different effects on different attack vectors and multiple effects on the same attack vector



### **Countermeasure Effects and the Cyber** Attack Lifecycle

The **Cyber Attack Lifecycle**<sup>\*</sup> illustrates the stages that an adversary goes through to achieve its objectives and provides a framework for recognizing how attacks are structured

#### occurred, is occurring, or potentially could occur Deliver Control Maintain Recon Weaponize Exploit Execute Prevent Respond eliminate conditions reduce the likelihood that make the attack or impact of the possible attack

Detect

makes it possible to determine if the attack has

\*The cyber attack lifecycle is frequently referred to as the "cyber kill chain." See http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf



# **Assessing Countermeasure Effects**

# The following table provides guidance for assessing the effect a countermeasure has on a given attack vector

ID	Countermeasure Effect	Tei	nds to be	
		Prevent	Detect	Respond
1	The countermeasure disrupts the attack's sequence of activities	Х		
2	The countermeasure eliminates condition(s) necessary for the attack to occur	Х		
3	The countermeasure facilitates detection of conditions leading to an attack	Х	Х	
4	The countermeasure reduces the likelihood of the attack being successful			X
5	The countermeasure minimizes the extent of damage or disruption			X
6	The countermeasure facilitates rapid recovery/reconstitution after the attack occurs			X
7	The countermeasure facilitates forensic analysis and/or attribution following an attack		X	X



## **Effects Confidence**

 Estimates the certainty that a countermeasure effect will be realized

- High Confidence
  - Engineering verification confirms the effect, i.e., demonstration, inspection, testing, or analysis
- Moderate Confidence
  - Effect based on judgment of a cyber Subject Matter Expert (SME)
- Low Confidence
  - Plausible effect that has not yet been confirmed or substantiated

### Applications

- Can be used to establish priorities for mapping table validation and applied security testing
- Can be used to filter mapping table data, e.g., disregard all mappings with low confidence, etc.

79



# **Mitigation Mappings Table Example**

	Countermeasure (CM)		Ef	fect (by Att	ack Vector	ID)	
CM ID	Name	T000014	T000049	T000050	T000052	T000071	T000170
C000103	Match buffer size to data input size		PH	PH			
C000293	Disable file and printer sharing			RM	RL		PL
C000134	Select programming languages that minimize potential software defects		PM	PM	PM		
C000238	Enforce software quality standards and guidelines that improve software quality		PM	PM	PM		
C000117	Apply principle of least privilege					RM	RM
C000135	Avoid use of dangerous memory functions and operations		RM		RM		
C000039	Convert input data into the data format in which it is used				PM		
C000059	Enable use of the HTTP Referrer header field	RM					
C000093	Merge data streams prior to validation				PM		
C000096	Use vetted runtime libraries		PH			PH	
C000123	Design software to fail securely		PM		RM		
C000136	Utilize processor-based protection capabilities		PL				PM
C000045	Utilize high quality session IDs	RM					
C000047	Encrypt session cookies	PH					
C000051	Use digital signatures/checksums to authenticate source of changes	PH					
C000089	Validate the range of numeric input			PM			
C000095	Convert input to canonical form before validating				PM		
C000101	Verify buffer sizes		PH				
C000102	Verify message size data					DH; PH	
C000137	Use unsigned variables to represent whole numbers			PM			
C000094	Validate data exchanges across language boundaries				RM		
C000132	Use sandboxing to isolate running software						PM
C000146	Apply transport-level mechanisms such as TLS and or VPNs to protect sensitive content	PH					

#### **Countermeasure Effects**

- PH Prevent Effect / High Confidence
- RM Respond Effect / Moderate Confidence
- DL Detect Effect / Low Confidence

Mitigation mappings for attack vectors T000014, T000049, T000050, T000052, T000071, T000170





# **Countermeasure Scoring**

- Once the mapping table is constructed, countermeasures can be scored and ranked
- TARA uses a numeric scoring approach to calculate a utility-tocost (U/C) ratio for each countermeasure
  - Utility reflects the effectiveness of a countermeasure over the range of attack vectors being assessed
    - Computed as a weighted sum of P's and R's
  - Cost reflects the Life Cycle Cost (LCC) of ownership of a countermeasure
    - Cost scale used: [1...5] *This in* <u>NOT</u> a dollar cost estimate!

### Countermeasure U/C ratios reflect "bang for the buck" effectiveness



# **Countermeasure Cost Factors**

### Acquisition Costs

- Cost to develop
- Cost to test
- Cost to integrate into system

### Operational Costs

- Cost to staff
- Cost to train
- Cost to operate
- Cost to maintain
- Cost to dispose

Cost factors reflect the Lifecycle Cost (LCC) of a countermeasure



# A Life Cycle Cost (LCC) Calculator

Factors for assessing Mitigation Life Cycl	e Cost (LCC)					Factor Weighting	C000x	COOOX	C000x
Acquisition cost factors	Very Low = 1	Low = 2	Medium = 3	High = 4	Very High = 5	0.4	0.4	1.2	2
Maturity: How technically mature is the mitigation?	Proven technology	New to market product or technology	fielded operational prototype	fielded demonstration prototype	laboratory or research prototype	0.2	1	3	5
Development: Does the mitigation require specialized or hard to find hardware or software capabilities to install or operate?	minimal capabilities required to develop	limited capabilities needed to develop	some specialized capabililities required	wide range of specialized capabilities required	extensive specialized and hard-to-find capabilities required	0.2	1	3	5
Development: Does the mitigation have a limited shelf life, i.e., does its effectivness deminish over time?	90% effective after 10 years	75% effective after 8 years	60% effective after 5 years	40% effective after 1 year	10% effective after 6 months	0.2	1	3	5
Integration: Does the mitigation implement standard interfaces and/or protocols that would facilitate integration with other technologies?	Interoperable through industry standard interfaces	Limited interoperability with other vendor products	Proprietary interfaces and non standard protocols	Undeveloped external interfaces	Mitigation implemented as standalone capability	0.2	1	3	5
Integration: Would system hardware or software baselines require extensive change in order to adopt the mitigation?	Drop-in capability	Minor configuration changes to existing baseline	Major configuration changes to existing baseline	Requires changes to software baseline (recoding)	Requires changes to hardware baseline (retooling)	0.2	1	3	5
Utilization cost factors	Very Low = 1	Low = 2	Medium = 3	High = 4	Very High = 5	0.6	0.6	1.8	3
Training: Would the mitigation require extensive training in order to operate or apply?	no training required	minimal training require	some training required	regular training required	extensive training required	0.2	1	3	5
Operation: Does the mitigation require significant staff to operate?	no additional staff required	minimal staff required	some staff required	significant staff commitment	labor intensive activity	0.2	1	3	5
Operation: Does the mitigation require specialized or hard to find hardware or software capabilities to install or operate?	no special capabilities required to install or operate	limited capabilities needed to install and operate	some specialized capabililities required	wide range of specialized capabilities required	extensive specialized and hard-to-find capabilities required	0.2	1	3	5
Maintenance: Would the mitigation require periodic hardware or software upgrades in order to remain effective?	infrequent	occasional	regular	frequent	very frequent	0.2	1	3	5
Disposal: Would disposal of the mitigation involve handling of toxic or hazardous substances?	No toxic or hazardous substances involved	Minimal likelihood of contact with harzardous substances	Contact with hazardous substances possible	Contact with hazardous subtances likely	Extensive contact with hazardous substances	0.2	1	3	5
					LC	C Score	1	3	5

© 2020 The MITRE Corporation. All rights reserved.

83

# **Adding Scoring Data to Mapping Table**

	Countermeasure (CM)			fect (by Att	ack Voctor	n)	2       3       4       3       3       3       3       3       3       3       3					
CM ID	Name	T000014	1	T000050	T000052		T000170	Total Die	Tatal Dia		Cast	LL/C Datia
-		1000014	T000049	1000050		T000071	1000170	Total P S	Total R S	Utility		U/C Ratio
	Convert input data into the data format in which it is used				PM						_	H
	Utilize high quality session IDs	RM									Ŭ	H
	Encrypt session cookies	PH									-	H
	Use digital signatures/checksums to authenticate source of changes	PH									-	<b> </b>
C000059	Enable use of the HTTP Referrer header field	RM									2	ļ
C000089	Validate the range of numeric input			PM							3	ļ
C000093	Merge data streams prior to validation				PM						2	I
C000094	Validate data exchanges across language boundaries				RM						4	
C000095	Convert input to canonical form before validating				PM						3	I
C000096	Use vetted runtime libraries		PH			PH					4	
C000101	Verify buffer sizes		PH								3	
C000102	Verify message size data					DH; PH					3	
C000103	Match buffer size to data input size		PH	PH							2	
C000117	Apply principle of least privilege					RM	RM				3	
C000123	Design software to fail securely		PM		RM						4	
C000132	Use sandboxing to isolate running software						PM				4	
C000134	Select programming languages that minimize potential software defects		PM	PM	PM						4	
C000135	Avoid use of dangerous memory functions and operations		RM		RM						3	
C000136	Utilize processor-based protection capabilities		PL				PM				4	
C000137	Use unsigned variables to represent whole numbers			PM							3	
	Apply transport-level mechanisms such as TLS and or VPNs to protect sensitive content	PH									4	
	Enforce software quality standards and guidelines that improve software quality		PM	PM	PM						4	
	Disable file and printer sharing			RM	RL		PL				3	

New scoring section added

© 2020 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited, Case 20-0272.



# **Calculating a U/C Ratio**

	Countermeasure (CM)		Ff	fect (by Att	ack Vector	D)				Scoring		
CM ID	Name	T000014	T000049	T000050	T000052	T000071	T000170	Total P's	Total R's	Utility	Cost	U/C Ratio
C000039	Convert input data into the data format in which it is used				PM			1		1	2	50
C000045	Utilize high quality session IDs	RM							1	1	3	33
C000047	Encrypt session cookies	PH						1		1	3	33
C000051	Use digital signatures/checksums to authenticate source of changes	PH						1		1	3	33
C000059	Enable use of the HTTP Referrer header field	RM							1	1	2	50
C000089	Validate the range of numeric input			PM				1		1	3	33
C000093	Merge data streams prior to validation				PM			1		1	2	50
C000094	Validate data exchanges across language boundaries				RM				1	1	4	25
C000095	Convert input to canonical form before validating				PM			1		1	3	33
C000096	Use vetted runtime libraries		PH			PH		2		2	4	50
C000101	Verify buffer sizes		PH					1		1	3	33
C000102	Verify message size data					DH; PH		1		1	3	33
C000103	Match buffer size to data input size		PH	PH				2		2	2	100
C000117	Apply principle of least privilege					RM	RM		2	2	3	67
C000123	Design software to fail securely		PM		RM			1	1	2	4	50
C000132	Use sandboxing to isolate running software						PM				4	
C000134	Select programming languages that minimize potential software defects		PM	PM	PM						4	(
C000135	Avoid use of dangerous memory functions and operations		RM		RM						3	(
C000136	Utilize processor-based protection capabilities		PL				PM				4	
C000137	Use unsigned variables to represent whole numbers			PM							3	
C000146	Apply transport-level mechanisms such as TLS and or VPNs to protect sensitive content	PH									4	
C000238	Enforce software quality standards and guidelines that improve software quality		PM	PM	PM						4	
C000293	Disable file and printer sharing			RM	RL		PL				3	

### How the U/C ratio is computed

- 1. Total the number of P's and R's across all attack vector columns
- 2. Optional: Select a weighting scheme for P's and R's
- 3. Utility Score = (Total P's)\*Weighting(P) + (Total R's)\*Weighting(R)
- 4. Utility/Cost ratio = Utility Score / Cost Score \* 100

# **Reordering the Mapping Table**

	Countermeasure (CM)		Ef	foct (by Att	ack Vector	<u></u>				Scoring		
CM ID	Name	T000014	T000049	T000050	T000052	T000071	T000170	Total P's	Total D'a	Utility	Cost	U/C Ratio
	Match buffer size to data input size	1000014	PH	PH	1000052	1000071	1000170	2	TOLDIKS	2	2	100
	Disable file and printer sharing			RM	RL		PL	1	2	3	3	100
	Select programming languages that minimize potential software defects		PM	PM	PM		ΓL.	3	2	3	4	75
-			PIVI	PIVI	PIVI			3		3	4	75
	Enforce software quality standards and guidelines that improve software quality		PIVI	PIVI	PIVI	RM	514	5	2	3	4	-
	Apply principle of least privilege					RIVI	RM		2	2	3	67
	Avoid use of dangerous memory functions and operations		RM		RM				2	2	3	67
C000039	Convert input data into the data format in which it is used				PM			1		1	2	50
C000059	Enable use of the HTTP Referrer header field	RM							1	1	2	50
C000093	Merge data streams prior to validation				PM			1		1	2	50
C000096	Use vetted runtime libraries		PH			PH		2		2	4	50
C000123	Design software to fail securely		PM		RM			1	1	2	4	50
C000136	Utilize processor-based protection capabilities		PL				PM	2		2	4	50
C000045	Utilize high quality session IDs	RM							1	1	3	33
C000047	Encrypt session cookies	PH						1		1	3	33
C000051	Use digital signatures/checksums to authenticate source of changes	PH						1		1	3	33
C000089	Validate the range of numeric input			PM				1		1	3	33
C000095	Convert input to canonical form before validating				PM			1		1	3	33
C000101	Verify buffer sizes		PH					1		1	3	33
C000102	Verify message size data					DH; PH		1		1	3	33
C000137	Use unsigned variables to represent whole numbers			PM				1		1	3	33
C000094	Validate data exchanges across language boundaries				RM				1	1	4	25
C000132	Use sandboxing to isolate running software			_			PM	1		1	4	25
C000146	Apply transport-level mechanisms such as TLS and or VPNs to protect sensitive content	PH						1		1	4	25

### **Alternative Reordering Strategies**

Bang-for-the-buck – table ordered by descending U/C ratios

*Max-Utility* – table ordered by descending Utility scores

Least-Cost – table ordered by ascending Cost scores

Countermeasure selection always starts from the top, so reordering strategies <u>will effect the selection</u>



# **Countermeasure Selection Strategy**

- A countermeasure selection strategy defines success criteria for the set of countermeasures selected to mitigate each attack vector
- Attack vectors with the highest risk scores are solved first
  - A best practice is to order attack vectors (columns) from left to right by descending risk

### Countermeasures with the highest ranking are selected first

 A best practice is to order countermeasure (rows) from top to bottom using the preferred reordering strategy

### Once selected, the countermeasure applies to all attack vectors

 The goal is to select the minimum number of countermeasures that satisfy the selection strategy



# **2 Example Selection Strategies**

- Construct a solution set containing at least 3 countermeasures for each attack vector with high risk, at least 2 countermeasures for each attack vector with moderate risk, and at least 1 countermeasure for each attack vector with low risk
- Construct a solution set containing at least 1 preventative and 1 responsive countermeasure for each attack vector AND at least 3 countermeasures for attack vectors with high risk, at least 2 countermeasures for attack vectors with moderate risk, and at least 1 countermeasure for attack vectors with low risk



# **Countermeasure Selection Example (1/5)**

	T000010	T000011	T000013	T000014	T000016	T000023	T000030	T000036	T000060	T000066			
CM ID	High	High	Moderate	Moderate	Moderate	Moderate	Low	Low	Low	Very Low	Utility	Cost	U/C Ratio
C000112	Х		Х		Х	Х	Х				5	20	25
C000100		Х			Х				Х	Х	4	20	20
C000325	Х				Х		Х	Х		Х	5	30	17
C000102	X		Х			Х	Х	Х			5	40	13
C000313		Х				Х	Х		Х		4	40	10
C000326		Х	Х				Х		Х		4	40	10
C000324	Х		Х	Х							3	40	8
C000118	Х	Х			Х		Х				4	60	7
C000114				Х		Х		Х			3	50	6
C000116		Х	Х					Х		Х	4	80	5
Totals													



### The Countermeasure Selection Strategy

Construct a solution set containing at least 3 countermeasures for each attack vector with high risk, at least 2 countermeasures for each attack vector with moderate risk, and at least 1 countermeasure for each attack vector with low risk.



# **Countermeasure Selection Example (2/5)**

CIAID	T000010	T000011	T000013	T000014	T000016	T000023	T000030	T000036	T000060	T000066		Cast	
CM ID	High	High	Moderate	Moderate	Moderate	Moderate	Low	Low	Low	Very Low	Utility	Cost	U/C Ratio
1. C000112	Х		Х		Х	Х	Х				5	20	25
C000100		Х			Х				Х	Х	4	20	20
2. C000325	Х				Х		Х	Х		Х	5	30	17
3. C000102	Х		Х			Х	Х	Х			5	40	13
C000313		Х				Х	Х		Х		4	40	10
C000326		Х	Х				Х		Х		4	40	10
C000324	Х		Х	Х							3	40	8
C000118	Х	Х			Х		Х				4	60	7
C000114				Х		Х		Х			3	50	6
C000116		Х	Х					Х		Х	4	80	5
Totals												90	



# Applying the selection strategy to the first vector selects 3 countermeasures

- The selected countermeasures apply to all attack vectors that they are mapped to
- The total cost (so far) is 90



# **Countermeasure Selection Example (3/5)**

CNUD	T000010	T000011	T000013	T000014	T000016	T000023	T000030	T000036	T000060	T000066		Gast	
CMID	High	High	Moderate	Moderate	Moderate	Moderate	Low	Low	Low	Very Low	Utility	Cost	U/C Ratio
1. C000112	Х		Х		Х	Х	Х				5	20	25
4. C000100		Х			Х				Х	Х	4	20	20
2. C000325	Х				Х		Х	Х		Х	5	30	17
3. C000102	Х		Х			Х	Х	Х			5	40	13
5. C000313		Х				Х	Х		Х		4	40	10
6. C000326		Х	Х				Х		Х		4	40	10
C000324	Х		Х	Х							3	40	8
C000118	Х	Х			Х		Х				4	60	7
C000114				Х		Х		Х			3	50	6
C000116		Х	Х					Х		Х	4	80	5
Totals												190	



# Applying the selection strategy to the second vector selects 3 more countermeasures

- Note that 3 countermeasures have already been selected for the third vector, so no additional countermeasures are needed for that vector
- The total cost is now 190



# **Countermeasure Selection Example (4/5)**

CNUD	T000010	T000011	T000013	T000014	T000016	T000023	T000030	T000036	T000060	T000066	L LATINA .	Cast	
CM ID	High	High	Moderate	Moderate	Moderate	Moderate	Low	Low	Low	Very Low	Utility	Cost	U/C Ratio
1. C000112	Х		Х		Х	Х	Х				5	20	25
4. C000100		X			Х				Х	Х	4	20	20
2. C000325	Х				Х		Х	Х		Х	5	30	17
3. C000102	Х		Х			Х	X	Х			5	40	13
5. C000313		Х				Х	Х		Х		4	40	10
6. C000326		X	Х				X		Х		4	40	10
7. C000324	Х		Х	Х							3	40	8
C000118	Х	Х			Х		Х				4	60	7
8. C000114				Х		Х		Х			3	50	6
C000116		Х	Х					Х		Х	4	80	5
Totals												280	



# Applying the selection strategy to the fourth vector selects 2 countermeasures

- Only 2 countermeasures are needed to satisfy the strategy for moderate risk vectors
- The total cost is now 280



# **Countermeasure Selection Strategy (5/5)**

CMID	T000010	T000011	T000013	T000014	T000016	T000023	T000030	T000036	т000060	T000066	1 1+:1:+. /	Cost	
CM ID	High	High	Moderate	Moderate	Moderate	Moderate	Low	Low	Low	Very Low	Utility	Cost	U/C Ratio
1. C000112	Х		Х		Х	Х	Х				5	20	25
4. C000100		Х			Х				Х	X	4	20	20
2. C000325	X				Х		Х	X		X	5	30	17
3. C000102	X		Х			X	Х	X			5	40	13
5. C000313		Х				X	Х		Х		4	40	10
6. C000326		Х	Х				Х		Х		4	40	10
7. C000324	X		X	Х							3	40	8
C000118	Х	Х			Х		Х				4	60	7
8. C000114				Х		X		X			3	50	6
C000116		Х	Х					Х		Х	4	80	5
Totals	4	3	4	2	3	4	5	3	3	2		280	
Totals	4	3	4	2	3	4	5	3	3	2		280	





# Countermeasures selected so far are sufficient to satisfy the strategy for the remaining vectors in the mapping table

- The number of countermeasures selected is totaled for each column. Green indicates the strategy is satisfied.
- The total cost of this solution is 280



# **Finding an Optimal Solution**

l	CNUD	T000010	T000011	T000013	T000014	T000016	T000023	T000030	T000036	T000060	T000066	1 14:11:4	Cont	
	CM ID	High	High	Moderate	Moderate	Moderate	Moderate	Low	Low	Low	Very Low	Utility	Cost	U/C Ratio
	1. C000112	X		Х		X	X	Х				5	20	25
	4. C000100		Х			X				X	Х	4	20	20
	2. C000325	X				X		Х	Х		X	5	30	17
₹	3. C000102	Х		Х			Х	Х	Х			5	40	13
7	5. C000313		X				X	Х		X		4	40	10
$\left  \right\rangle$	6. C000326		Х	Х				Х		X		4	40	10
	7. C000324	X		Х	X							3	40	8
	C000118	Х	Х			Х		Х				4	60	7
	8. C000114				X		X		Х			3	50	6
	C000116		Х	Х					Х		Х	4	80	5
	Totals	3	3	3	2	3	3	4	2	3	2		240	



### An optimal solution will <u>minimize</u> the number of countermeasures selected while satisfying the strategy

- While selecting CMs is performed starting from the top, de-selecting CMs is performed starting from the bottom
- C0000102 is deselected, reducing the total cost by  $(280-240)/280 \sim 14\%$



# What if the strategy cannot be satisfied?

CMUD	T000010	T000011	T000013	T000014	T000016	T000023	T000030	T000036	T000060
CM ID	High	High	Moderate	Moderate	Moderate	Moderate	Low	Low	Low
C000112							R		
C000100		R							
C000325	Р							R	
C000102									
C000313		R					R		Р
C000326		Р							R
C000324	R		Р	R					
C000118	R				Р		R		
C000114				R				Р	
C000116			Р						
Totals	3	3	2	2	1	0	3	2	2

Green = satisfied Yellow = deficiency Red = gap

### Alternatives

- Add mappings
- Add countermeasures (and mappings)
- Adjust the strategy
- Recognize that there are deficiencies in the model

For bonus points: Can you deduce the selection strategy from this table?



# **Solution Effectiveness Table**

The solution effectiveness table represents a solution set. For each countermeasure it identifies the preventative or mitigating effect(s) it has over the range of attack vectors. The table also provides a cost summary and indicates whether the selection strategy is satisfied for each attack vector, or where gaps exist.

	Countermeasure (CM)			Effect (by Attack Vector ID)				
CM ID	Name	U/C Ratio	T000014	T000049	T000050	T000052	T000071	T000170
C000134	Select programming languages that minimize software defects	75		PM	PM	PM		
C000117	Apply principle of least privilege	67					RM	RM
C000093	Merge data streams prior to validation	50				PM		
C000096	Use vetted runtime libraries	50		PH			PH	
C000047	Encrypt session cookies	33	PH					
C000051	Use digital signatures/checksums	33	PH					
C000132	Use sandboxing to isolate running software	25						PM
	TOTALS	333	2	2	1	2	2	2

The solution effectiveness table is produced by removing unselected countermeasures from the mapping table and tabulating the totals

# **Exercise #2: Exporting Catalog Data**

- 1. Go to the vector group list
- 2. Select (check) your vector
- **3**. Generate a Composite List of Attack Vectors (button at top)
- **4.** Generate a Composite List of Countermeasures (button at top)
- 5. Export TARA Spreadsheet (button at top)
- 6. Save as.. On the desktop, call it TARA extract.xlsx



## Your Turn...

### Discussion

- Did you find everything you were looking for?
- Do you agree with the mappings?



## **Summary**

### Cyber Risk Remediation Analysis (CRRA)

- Extends initial mapping table with additional countermeasures and mappings
- Applies cost scoring to estimate lifecycle cost for countermeasures
- Computes U/C ratios for countermeasures
- Applies selection strategy to select countermeasures
- Produces a Solution Effectiveness table and associated recommendations

### Worked example

- Use of mapping table and U/C ratio scoring
- Use of a selection strategy to select countermeasures
- Solution set optimization
- Sensitivity analysis to develop and evaluate alternative solutions

### Exercise #2 : Exporting Catalog Data

### **MITRE**

**The MITRE Corporation** 

# **TARA Catalog Content Management**



© 2020 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited, Case 20-0272.

### **Objectives**

- Discuss Knowledge Management (KM) activities
- Discuss taxonomies
- Discuss catalog virtualization
- Exercise #3: Updating the catalog



# KM in TARA

### The TARA catalog is <u>never</u> complete and <u>never</u> up-to-date

- Numerous content gaps
- Constantly evolving cyber threat landscape
- Did you find everything you were looking for? Probably not.

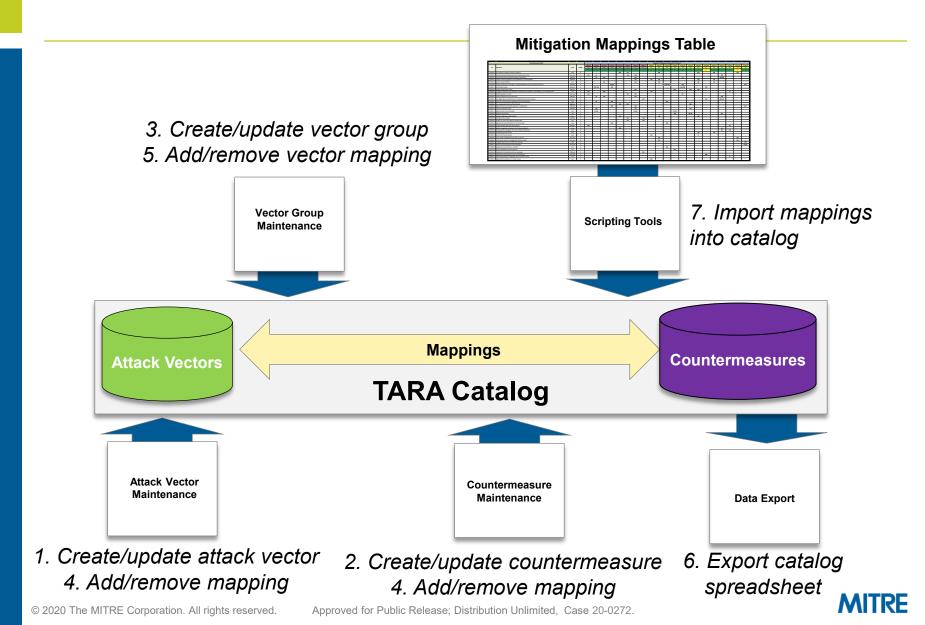
### No elves behind the scenes to maintain the catalog

- Catalog updates necessary for every assessment
  - Attack vectors, countermeasures, and mitigation mappings added depending on assessment needs

### Content added to the catalog is reused in subsequent assessments



### **KM Workflows**



# **KM Workflow Details**

- 1. Create / update attack vector
- 2. Create / update countermeasure
- 3. Create / update vector group
  - Used to create and manage attack vectors, countermeasures, and vector groups
- 4. Add / remove mapping
  - Used to manage mappings between attack vectors and countermeasures
    - Performed in the context of attack vector or countermeasure maintenance

### 5. Add / remove vector mapping

- Used to manage mappings between attack vectors and vector groups
  - Also used to manage contents of shopping carts
- Used to manage hierarchical relationships between vector groups
  - Support taxonomy development

### 6. Export catalog spreadsheet

Used to generate a TARA export spreadsheet containing attack vectors, countermeasure, and mapping details

### 7. Import mappings into catalog

Supports bulk importation of mappings from a mitigation mappings table (spreadsheet)



# Managing Attack Vectors and Countermeasures (1/3)

### **Catalog Menu**

#### Home Records Loaded Vector Group Attack Vectors Countermeasures Search for... Attack Vectors Countermeasures Reports **Catalog Maintenance** Attack Vectors Countermeasures -110/15 Catalog Export/Import Account Managment Catalog Merge Tool Data Schemas Spreadsheet Template Converter/Importer AV-CM Mapping Tools

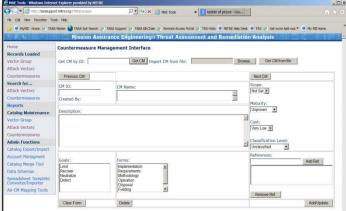
Requires maintainer privileges to access

### **Attack Vector Maintenance Screen**

🗃 💬 💌 🧭 http://tarasuppo	ort.mitre.org/TTPInput.aspx	D 🔹 +7 🗙 🥘 MAE Tools	× Reebler ell picture - Goo	() :
File Edit View Favorites To	ols Help			
🙀 🚳 MyME - Home 🍃 TAR	A Master 🎃 TARA Solt Search 🝃	TARA Support 🎒 TARA Kil Chain 🎒 Remote Access	Portal 🥃 TRS-Web 😬 METRE Help Desk	😕 TRS 🧔 Get more Add-ons 🕶 🧶 My HIL Home
	Mission Ass	Irance Engineering : Threat Ass	essment and Remediatio	n Analysis
Home	Attack Vector Mana	nement Interface		
Records Loaded				
Vector Group			oort AV from file:	
Attack Vectors	Get AV by ID:	Get AV	Browse	
Countermeasures			Get AV from file	
Search for	Previous AV		Next AV	
Attack Vectors				
Countermeasures	Attack Vector ID:	Attack Vector Name:		AV Categories:
Reports			2	Social Engineering Electronic Warfare
Catalog Maintenance	Created By:		2	Supply Chain
Vector Group				Hardware/Firmware Cyber
Attack Vectors				-/
Countermeasures	Description:			Attack Objectives:
Admin Functions			3	Disruption
Catalog Export/Import				Penetration
Account Managment				Extitration
Catalog Merge Tool				Implantation Recon
Data Schemas			-	2.4
Spreadsheet Template	Classification Level:	Prerequisites:		References: Add Ref
Converter/Importer	Unclassified		Add Pre.	700 100
AV-CM Mapping Tools	Origins:			
	Trusted Insider			
	External	Remove Pre.		La comen
	Insider	Foundve Fre.		Remove Ref.
	Clear Form	Delete		Add/Update

Screen used to create, modify, and delete an attack vector in the TARA catalog

### **Countermeasure Maintenance Screen**



Screen used to create, modify, and delete a countermeasure in the TARA catalog

# Managing Attack Vectors and Countermeasures (2/3)

### Attack Vector Maintenance Screen (Bottom)

Mapped Countermeasure(s):						
CM ID - Name	Prevent	Detect	Respond	Classification		
C000062 - Disable client side scripting	High	N/A	N/A	Unclassified	Edit	<u>Delete</u>
C000090 - Validate input fields use of NULL, escape, backslash, meta, and control characters	Medium	N/A	N/A	Unclassified	Edit	<u>Delete</u>
C000121 - Verify input sources	Medium	Medium	N/A	Unclassified	Edit	Delete
C000115 - Limit user functional roles	N/A	N/A	Low	Unclassified	Edit	<u>Delete</u>
C000132 - Use sandboxing to isolate running software	N/A	N/A	Medium	ledium Unclassified		Delete
C000194 - Disable hyperlinks in email	N/A	N/A	Low	Unclassified	Edit	<u>Delete</u>
C000197 - Automated attack signature detection and firewall update	N/A	Medium	Medium	Unclassified	Edit	<u>Delete</u>
C000220 - Supplement signature-based malware detection with anomaly-based capabilities	Medium	N/A	N/A	Unclassified	Edit	<u>Delete</u>
C000344 - Enforce use of pre-configured or well know redirection URIs	Medium	N/A	N/A	Unclassified	Edit	<u>Delete</u>
C000001 - Verify secure BIOS update non-bypassability	N/A 💙	N/A 💙	N/A 🗸	Unclassified V	Add New	

Screen also used to create, update, and delete mappings to countermeasures in the catalog

### **Countermeasure Maintenance Screen (Bottom)**

Threat Vector ID - Name	Prevent	Detect	Respond	Classification		
T000182 - Software defects hidden/obscured by code complexity	N/A	Low	N/A	Unclassified	Edit	Delete
T000189 - Adversary gains unauthorized access by exploiting software vulnerabilities	N/A	Medium	N/A	Unclassified	Edit	Delete
T000312 - Software assurance practices	N/A	N/A	N/A	Unclassified	Edit	Delete
T000269 - Spoofed authenticated router access	Medium	N/A	N/A	Unclassified	Edit	Delete
T000157 - Force Use of Corrupted Files	Medium	N/A	N/A	Unclassified	Edit	Delete
<u> T000290 - Using Leading 'Ghost' Character Sequences</u> to Bypass Input Filters	Low	N/A	N/A	Unclassified	<u>Edit</u>	Delete
T000001 - BIOS replaced with version that allows unsign	N/A 🗸	N/A 💙	N/A 🗸	Unclassified V	Add New	

Screen also used to create, update, and delete mappings to attack vectors in the catalog



# Managing Attack Vectors and Countermeasures (3/3)

N/A N/A	N/A N/A	N/A N/A	<u>Edit</u> Edit	<u>Delete</u> Delete
	N/A	N/A	Edit	Delete
N/A	N/A	N/A	Edit	Delete
N/A	N/A	N/A	Edit	Delete
N/A	N/A	N/A	Edit	Delete
N/A	N/A	N/A	<u>Edit</u>	Delete
	N/A N/A	N/A N/A N/A N/A N/A N/A	N/A         N/A         N/A           N/A         N/A         N/A           N/A         N/A         N/A	N/A     N/A     N/A     Edit       N/A     N/A     N/A     Edit       N/A     N/A     N/A     Edit

Screen used to create, update, and delete mappings of attack vector to vector groups.

Vector groups selected based on attack vector details.

Select all that apply.

A000035 - XML A000036 - Session Management A00037 - Database A000114 - Web Service A000179 - Scripting A000201 - Email A000223 - Desktop A000223 - Remote Access	^					
A000235 - OS A000251 - PKI Ass A000256 - Web Server A000266 - Web Application A000267 - Mobile		Confidentiality	Integrity	Availability		
A000271 - Software A000282 - Identification of CPI		N/A	N/A	N/A	Edit	<u>Delete</u>
A000308 - Crypto A000325 - Use of COTS		N/A	N/A	N/A	Edit	<u>Delete</u>
A000326 - BIOS A000330 - Web 2.0		N/A	N/A	N/A	Edit	<u>Delete</u>
A000334 - Passwords A000335 - IDS/IPS		N/A	N/A	N/A	Edit	Delete
A000336 - Firewalls A000350 - Malware		N/A	N/A	N/A	Edit	Delete
A000352 - HTML A000354 - IP Device A000357 - VM		N/A	N/A	N/A	Edit	<u>Delete</u>
A000357 - VM A000361 - publish-subscribe A000376 - IdAM A000381 - BGP A000387 - CAPEC	~	N/A 🔽	N/A 🔽	N/A	Add New	

© 2020 The MITRE Corporation. All rights reserved.

Approved for Public Release; Distribution Unlimited, Case 20-0272.



# **Guidance for Updating the Catalog**

- Use catalog search to verify that an attack vector or countermeasure is not already represented in the catalog
  - Duplicate entries effect performance and assessment quality

### Always cite external reference(s)

- Allows users to assess the veracity of the data and/or to locate additional details
- Add new attack vector to all taxonomy groups that apply
- An attack vector without a countermeasure is a problem without a solution; a countermeasure without an attack vector is a solution without a problem
  - Neither provide value in the TARA catalog



# WARNING !

#### **NEVER** store classified data in a TARA catalog

Always store classified data on a classified system TARA data can be exported in a spreadsheet and transferred to the classified system



## **Taxonomies**

#### Vector Group – Named collection of attack vectors Taxonomy – Hierarchically structured collection of vector groups

Taxonomies can be used to organize attack vectors based on technology, system architecture, attack vector properties, etc.

Taxonomies listed on the Top Level Vector Groups page with type "Root"



<u>VG ID</u>	<u>Children</u>	<u>Vector Group</u>	<u>Description</u>	Туре
<u>A000422</u>	<u>10</u>	ATT&CK	Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK™) is a framework for describing post-compromise adversary behavior within an enterprise network.	Root
<u>A000387</u>	<u>16</u>	CAPEC	Common Attack Pattern Enumeration and Classification (CAPEC™) provides a publicly available catalog of common attack patterns.	Root
<u>A000384</u>		CM Practices	Groups of Countermeasures (CMs)	Root
<u>A000493</u>	3	ICS/SCADA System	Organizational taxonomy representing ICS/SCADA Systems	Root
<u>A000495</u>	2	Indicators	Organizational taxonomy of Indicators of Compromise (IOCs)	Root
<u>A000471</u>	4	IP System	Organizational taxonomy representing IP-based, distributed systems	Root

# WARNING !

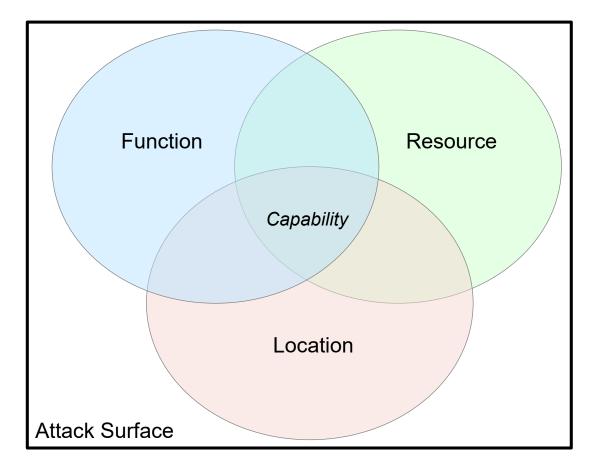
# Do <u>NOT</u> use system or program names for vector group names

For DoD systems, that association may be classified For National Security Systems (NSS), that association <u>will</u> be classified



111

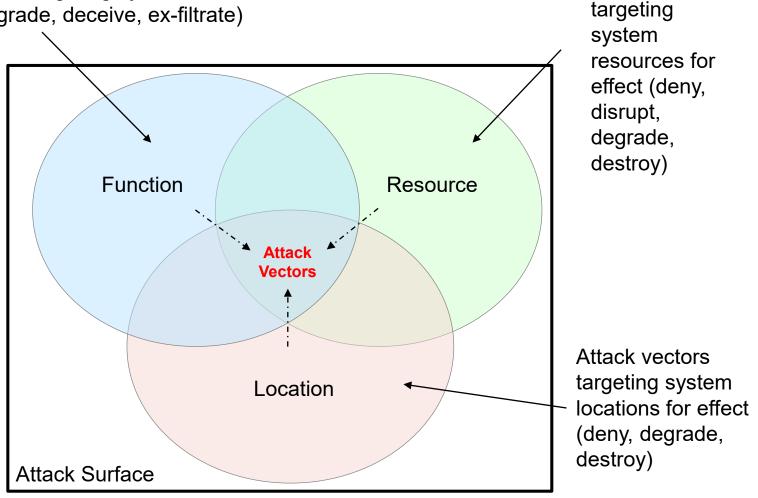
### **Taxonomy for Representing Attack Surfaces**





# **Targeting for Effect**

Attack vectors targeting system functions for effect (disrupt, degrade, deceive, ex-filtrate)



MITRE

Attack vectors

# **TARA Catalog as a Virtual Resource**

The TARA catalog is deployed as a virtualized resource within the MITRE Enterprise

- Several instances of the TARA catalog are currently hosted
  - Catalog content tailored to support specific acquisition lifecycle timeframes and/or program or sponsor specific requirements
  - Finesses multi-tenancy issues
- Catalog import/export can be used to share (exchange) catalog data between virtual catalog instances
  - Each catalog instance uses the same data representation format and software baseline
  - "Chunks" of the TARA master catalog can be imported into other catalog instances



# **Exercise #3: Updating the Catalog**

#### Create a Mapping

- 1. Open the attack vector (or countermeasure) you wish to create a mapping for
- 2. Find a countermeasure (or attack vector) you wish to map it to in the appropriate drop-down list
- 3. Select the mapping type press Add New

#### **Create an Attack Vector**

- 1. Perform a keyword search to verify the attack vector doesn't already exist
- 2. Under Catalog Maintenance open a new attack vector maintenance page
- 3. Enter name, description, reference, prerequisite(s)
- 4. Select category, attack objectives, origin
- 5. Select Add/Update
- 6. Create a mapping to at least one countermeasure

#### Create a Countermeasure

- 1. Perform keyword search to verify countermeasure doesn't already exist
- 2. Under Catalog Maintenance open a new countermeasure maintenance page
- 3. Enter name, description, reference
- 4. Select maturity, cost, goals, forms
- 5. Select Add/Update
- 6. Create a mapping to at least one attack vector

# Your Turn...

#### Create an Attack Vector

 Create an attack vector and add it to the shopping cart created in the previous exercise.

#### Create a Mapping

 Create a mapping to a countermeasure for the attack vector you created above. Use keyword search to locate a countermeasure to use for the mapping.

#### Create a Countermeasure

Create a new countermeasure and map it to your attack vector.

#### For BONUS Points..

- Re-export the spreadsheet to incorporate the updates.



# **Summary**

There are TARA catalogs available on the MII for conducting TARA assessments

- Periodically resynchronized with the Catalog master
- Read only access typically granted
- A separate catalog instance can be set up to support sponsor or program

117

 For projects that intend to use different catalog data and are willing to take responsibility for managing that data

#### Guidance for adding new attack vectors and countermeasures

- No duplicates
- Cite your sources
- Don't forget to add new attack vectors to applicable taxonomy structures

#### The value of TARA catalog data is in the mappings between attack vectors and countermeasures

- Without mappings, neither individually provides value

The MITRE Corporation

# **TARA Risk and Cost Scoring Tools**



© 2020 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited, Case 20-0272.

# **Objectives**

Discuss TARA risk and cost scoring tools

Example #4: Using a risk calculator



# **Risk and Cost Calculators**

- TARA provides spreadsheets for risk and cost scoring
  - Risk calculators used to score attack vectors
  - LCC calculator used to score countermeasure costs

#### Different risk calculators<sup>1</sup> use different risk factors

- Standard risk calculator
  - Risk factors are likelihood and impact, equally weighted
- CIA risk calculator
  - Impact: loss of confidentiality, integrity, and availability treated as separate factors (possibly different weightings)
- Mission risk calculator
  - Impact represented as impact to mission and/or mission readiness
- V x E risk calculator
  - Likelihood factor replaced with vulnerability and exposure
- Custom risk calculator
  - Supports customizable set of risk factors based on program or sponsor requirements



# **Standard Risk Calculator**

Factors for assessing Attack Vector Risk (Standard)								, j	
Factor Range	Very Low = 1	Low = 2	Medium = 3	High = 4	Very High = 5	Factor Weight	T000x	T000x	T000x
Likelihood: What is the likelihood that the attack will be successful?	Very unlikely	Unlikely	Possible	Likely	Very likely	1	1	3	5
Impact: What impact would result if the attack is successful?	Negligible impact	Minimal impact	Moderate impact	Serious impact	Catastrophic impact	1	1	3	5
Risk Score							1.0	9.0	25.0

#### Two risk factors: likelihood and impact, equally weighted

Note that the likelihood and impact scales used in the standard risk calculator align with the risk scales used in NIST 800-30

# Confidentiality, Integrity, Availability (CIA) Risk Calculator

Factors for assessing Attack Vector Risk (CIA Impacts)								¢	
Factor Range	Very Low = 1	Low = 2	Medium = 3	High = 4	Very High = 5	Factor Weight	T000x	T000x	T000x
Likelihood: What is the likelihood that the attack will be successful?	Very unlikely	Unlikely	Possible	Likely	Very likely	1	1	3	5
Impact: What impact to confidentiality would result if the attack is successful?	Negligible impact	Minimal impact	Moderate impact	Serious impact	Catastrophic impact	0.3	1	3	5
Impact: What impact to integrity would result if the attack is successful?	Negligible impact	Minimal impact	Moderate impact	Serious impact	Catastrophic impact	0.3	1	3	5
Impact: What impact to availability would result if the attack is successful?	Negligible impact	Minimal impact	Moderate impact	Serious impact	Catastrophic impact	0.4	1	3	5
Risk Score							1.0	9.0	25.0

#### Two risk factors: likelihood and impact, equally weighted.

# Note that impact is decomposed into separate factors (loss of confidentiality, integrity, and availability)



# **Mission Risk Calculator**

Factors for assessing Attack Vector Risk (Mission Impact)								~	v
Factor Range	Very Low = 1	Low = 2	Medium = 3	High = 4	Very High = 5	Factor Weight	T000x	T000x	T000x
Likelihood: What is the likelihood that the attack will be successful?	Very unlikely	Unlikely	Possible	Likely	Very Likely	1	1	3	5
Mission Impact: What would be the impact to the mission if the attack is successful?	Sporadic loss of mission capability	Intermittent loss of mission capability	Regular loss of mission impact	Extended loss of mission capability	Permanent loss of mission capability	1	1	3	5
Risk Score							1.0	9.0	25.0

#### Two risk factors: likelihood and impact, equally weighted.

Note that impact is defined in terms of impact to mission. This could be further decomposed into mission impact(s) for individual mission capabilities, as would be reflected in CJA results

### Vulnerability x Exposure (V x E) Risk Calculator

Factors for assessing Attack Vector Risk (V x E)									
Factor Range	Very Low = 1	Low = 2	Medium = 3	High = 4	Very High = 5	Factor Weight	T000x	T000x	T000x
Vulnerability: How vulnerable is the system to attack?	Negligible vulnerabilities	Limited vulnerabilities	Moderate vulnerabilities	Serious vulnerabilities	Extremely vulnerable	0.5	1	3	5
Exposure: How accessible is the system to malicious threat actors?	Negligible exposure	Limited exposure	Moderately exposed	Serious exposures	Extremely exposed	0.5	1	3	5
Impact: What impact would result if the attack is successful?	Negligible impact	Minimal impact	Moderate impact	Serious impact	Catastrophic impact	1	1	3	5
Risk Score							1.0	9.0	25.0

Two risk factors: likelihood and impact, equally weighted.

#### Note that likelihood is defined in terms of vulnerability and exposure



# **Custom Risk Calculator**

Factors for assessing Attack Vector R	J	¢	¢				
Factor Range	Low = 1 Medium = 2		High = 3	Factor Weight	T000x	T000x	T000x
Locality: How localized are the effects posed by this Attack Vector?	isolated to single unit	external networks potentially impacted	all units globally and associated infrastructure	0.2	1	3	5
Impact: How serious an impact is loss of data confidentiality resulting from successful application of this Attack Vector?	no impact from Attack Vector	limited impact requiring some remediation	COOP remediation activites routinely exercised	0.2	1	3	5
Impact: How serious an impact is loss of system availability resulting from successful application of this Attack Vector?	no impact from Attack Vector	limited impact requiring some remediation	COOP remediation activites routinely exercised	0.2	1	3	5
Likelihood: Has this attack vector been seen before in the wild?	unconfirmed indications	indications Attack Vector attempted previously	widespread use of Attack Vector apparent	0.3	1	3	5
Stealth: How detectable is this Attack Vector when it is applied?	Attack Vector obvious without monitoring	detection possible with specialized monitoring	undetectable	0.1	1	3	5
Risk Score							5.0

#### Multiple risk factors, individually weighted.

# Note that custom risk calculators can be developed using sponsor or program specified risk factors and weightings

© 2020 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited, Case 20-0272.

# Life Cycle Cost (LCC) Calculator

Factors for assessing Mitigation Life Cycl	e Cost (LCC)				-	Factor Weighting	C000×	C000×	C000×
Acquisition cost factors	Very Low = 1	Low = 2	Medium = 3	High = 4	Very High = 5	0.4	0.4	1.2	2
Maturity: How technically mature is the mitigation?	Proven technology	New to market product or technology	fielded operational prototype	fielded demonstration prototype	laboratory or research prototype	0.2	1	3	5
Development: Does the mitigation require specialized or hard to find hardware or software capabilities to install or operate?	minimal capabilities required to develop	limited capabilities needed to develop	some specialized capabililities required	wide range of specialized capabilities required	extensive specialized and hard-to-find capabilities required	0.2	1	3	5
Development: Does the mitigation have a limited shelf life, i.e., does its effectivness deminish over time?	90% effective after 10 years	75% effective after 8 years	60% effective after 5 years	40% effective after 1 year	10% effective after 6 months	0.2	1	3	5
Integration: Does the mitigation implement standard interfaces and/or protocols that would facilitate integration with other technologies?	Interoperable through industry standard interfaces	Limited interoperability with other vendor products	Proprietary interfaces and non standard protocols	Undeveloped external interfaces	Mitigation implemented as standalone capability	0.2	1	3	5
Integration: Would system hardware or software baselines require extensive change in order to adopt the mitigation?	Drop-in capability	Minor configuration changes to existing baseline	Major configuration changes to existing baseline	Requires changes to software baseline (recoding)	Requires changes to hardware baseline (retooling)	0.2	1	3	5
Utilization cost factors	Very Low = 1	Low = 2	Medium = 3	High = 4	Very High = 5	0.6	0.6	1.8	3
Training: Would the mitigation require extensive training in order to operate or apply?	no training required	minimal training require	some training required	regular training required	extensive training required	0.2	1	3	5
Operation: Does the mitigation require significant staff to operate?	no additional staff required	minimal staff required	some staff required	significant staff commitment	labor intensive activity	0.2	1	3	5
Operation: Does the mitigation require specialized or hard to find hardware or software capabilities to install or operate?	no special capabilities required to install or operate	limited capabilities needed to install and operate	some specialized capabililities required	wide range of specialized capabilities required	extensive specialized and hard-to-find capabilities required	0.2	1	3	5
Maintenance: Would the mitigation require periodic hardware or software upgrades in order to remain effective?	infrequent	occasional	regular	frequent	very frequent	0.2	1	3	5
Disposal: Would disposal of the mitigation involve handling of toxic or hazardous substances?	No toxic or hazardous substances involved	Minimal likelihood of contact with harzardous substances	Contact with hazardous substances possible	Contact with hazardous subtances likely	Extensive contact with hazardous substances	0.2	1	3	5
					LC	C Score	1	3	5

Same idea as risk calculator but replace risk factors with cost factors

LCC cost is the sum of acquisition costs and utilization costs

Weightings based on applicability of cost to program

LCC cost scores in range [1...5] used in U/C ratio calculation

# Custom LCC calculators utilize program or sponsor specified cost factors, scales, weighting schemes, etc.



# **Exercise #4: Using a Risk Calculator**

#### Using the Risk Calculator

- Open the TARA scoring models spreadsheet on the Desktop
- Go to the CIA Scoring model
- Select IDs of 3 attack vectors from your shopping cart
- For each attack vector:
  - Enter the ID into the spreadsheet
  - Find the attack vector description in the catalog (search or from the master list)
  - Follow the reference URL and review info about the vector
  - In the spreadsheet enter likelihood and impact estimates



# Your Turn...

#### Evaluating the risk scoring process and the results..

- Does the ranking surprise you?
- Is the ranking consistent with the level of risk reflected in the reference data?
- Did all of the risk factors apply equally?
- What additional risk factors would be relevant?
- Would more precise qualitative effects make analysis easier?
- Would adjusting the weightings improve the scores?



# Threat Assessment and Remediation Analysis (TARA)

Recap



© 2020 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited, Case 20-0272.

# **Summary of Material Covered**

- Provided an overview of the Threat Assessment and Remediation Analysis (TARA) methodology
- Discussed the TARA data model elements: vector groups, taxonomies, attack vectors, countermeasures, mappings
- Discussed application of TARA in Systems Security Engineering (SSE) contexts
- Discussed uses of open source data: CAPEC, ATT&CK, CWE, CVE, etc.
- Provided a TARA catalog demonstration
- Discussed cyber threat actor motive, intentions, capabilities, etc.
- Discussed modeling of attack surfaces
- Discussed cyber threat scenarios
- Discussed phases of a TARA assessment: Scoping, CTSA, CRRA
- Practiced creation of shopping carts
- Provided a worked example of applying countermeasure scoring and selection strategy to develop an optimized solution set
- Practiced exporting catalog data
- Discuss Knowledge Management (KM) activities
- Practiced catalog maintenance activities
- Discussed taxonomies for organizing attack vectors
- Discussed the TARA catalog as a virtual resource
- Discussed TARA risk and cost scoring tools
- Practiced using risk scoring tool

# **TARA Acronyms**

ΑΡΤ	Advanced Persistent Threat
ATT&CK™	Adversarial Tactics, Techniques, and Common Knowledge
AV	Attack Vector
C2	Command and Control
CAPEC™	Common Attack Pattern Enumeration and Classification
CDC	Cleared Defense Contractor
CDR	Critical Design Review
CJA	Crown Jewels Analysis
СМ	Countermeasure
CONOPS	Concept of Operations
COTS	Commercial off-the-shelf
СРІ	Critical Program Information
CRRA	Cyber Risk Remedation Analysis
CTSA	Cyber Threat Susceptibility Analysis
CVE™	Common Vulnerability Enumeration
CWE™	Common Weaknesses Enumeration
DHS	Department of Homeland Security
DoD	Department of Defense
км	Knowledge Management
LCC	Life Cycle Cost
MAUA	Multi-Attribute Utility Analysis
NIST	National Institute of Science and Technology
OSINT	Open Source Intelligence
PDR	Preliminary Design Review
RMF	Risk Management Framework
SCADA	Supervisory Control & Data Acquisition
SCG	Security Classification Guide
SCRM	Supply Chain Risk Management
SSE	Systems Security Engineering
TARA	Threat Assessment and Remediation Analysis
ттр	Tactics, Techniques, and Procedures
U/C ratio	Utility/Cost ratio
VG	Vector Group
XML	eXtensible Markup Language



# **For More Information**

#### Public release information and resources

http://www.mitre.org/sites/default/files/publications/pr-2359-threat-assessment-andremediation-analysis.pdf

http://www.mitre.org/publications/technical-papers/threat-assessment--remediationanalysis-tara/

http://www.mitre.org/publications/systems-engineering-guide/enterpriseengineering/systems-engineering-for-mission-assurance/cyber-threat-susceptibilityassessment

http://www.mitre.org/publications/systems-engineering-guide/enterpriseengineering/systems-engineering-for-mission-assurance/cyber-risk-remediation-analysis





MITRE's mission-driven teams are dedicated to solving problems for a safer world. Through our federally funded R&D centers and public-private partnerships, we work across government to tackle challenges to the safety, stability, and well-being of our nation.

Learn more www.mitre.org



