Mission Assurance for the Enterprise

Barbara Braun The Aerospace Corporation

November 2023

© The Aerospace Corporation, 2023

Approved for Public Release. OTR202400097

Existing Cybersecurity Matrices

1

Instruction Mode sub-balance Reconnaissance Reconnerse Initial Access Execution Persistence Privilege Defense Evasion Credenieue To techniques Bechnique Initial Access Execution Persistence Privilege Defense Evasion Credenieue Acquire Internation (a) Acquire Acquire Comparated Acquire Comparated Acquire <	٨	AITRE ATT8	«CK°				Ma	atric	ces - Tactic	s -	Techniques -	Da	ata Sources
Reconnaissance 10 techniques Resource bechniques Initial Access Execution 14 techniques Persistence 19 techniques Privilege 13 techniques Defense Fusion 42 techniques									layout: sid	e▼	show sub-techni	ques	s hide sub-
D Bechniques 3 Bechniques 14 Bechniques <th></th> <th>Reconnaissance</th> <th>Resource Development</th> <th>Initial Access</th> <th>Execution</th> <th></th> <th>Persistence</th> <th></th> <th>Privilege Escalation</th> <th></th> <th>Defense Evasion</th> <th></th> <th>Credential Access</th>		Reconnaissance	Resource Development	Initial Access	Execution		Persistence		Privilege Escalation		Defense Evasion		Credential Access
Gather Victim Host Information (2) Acquire Infastucture (6) Compromise Exploit Public- Application (formation (2)) Control (mapplication (2)) Control		Active Scanning (3)	Acquire Access	Drive-by	Cloud		Account		Abuse Elevation		Abuse Elevation Control		17 techniques
Image: Second region Image: Second region <td< td=""><td></td><td>Gather Victim Host</td><td>Acquire</td><td>Compromise Exploit Public-</td><td>Administration Command</td><td></td><td>Manipulation (5)</td><td>"</td><td>Control Mechanism ₍₄₎</td><td>"</td><td>Mechanism (4)</td><td></td><td>SPA</td></td<>		Gather Victim Host	Acquire	Compromise Exploit Public-	Administration Command		Manipulation (5)	"	Control Mechanism ₍₄₎	"	Mechanism (4)		SPA
Interpretent (g) Account (g) Develop Compromise (Gradming (g)) Develop (Gradming (g))		Gather Victim Identity	Compromise	Facing Application	Command and Scripting		Boot or Logon		Access Token Manipulation ₍₅₎	u į	Manipulation (5)		SPACE ATTACK F
Information (6) Infrastructure (7) Hardware Administration Bod or Logon Bod or Logon Debugger Evasion Gather Victim Org Establish Replication Files (2) Bod or Logon Debugger Evasion Debugger Evasion Pishing for Establish Replication Troogh Bod or Logon Debugger Evasion Debugger Evasion Search Closed Obtain Capabilities (6) Supply Chain Native API Create Command Deploy Container Direct Volume Access Search Open Technical Stage Trusted Scheduled Scheduled Establish Esceution (10) Esceution (10) Modification (2) If Gather S Search Open Technical Stage Trusted Scheduled Scheduled Esceution (10) Esceution (10) Esceution (10) Esceution (10) Gather S Search Open Technical Valid Accounts (2) Trusted Scheduled Files or Modify Esceution (10) Esce		Gather Victim Network	Compromise	External Remote Services	Container		Execution (14)		Boot or Logon Autostart		Build Image on Host		
Information (a) Image: capabilities (a)		Gather Victim Org	Develop	Hardware Additions	Administration Command		Boot or Logon Initialization Scripts ₍₅₎		Execution (14) Boot or Logon		Debugger Evasion		-
Information (a) Accounts (a) Replication Client Execution Compromise Compromise Client Execution Direct Volume Access Domain Policy Domain P		Phishing for	Capabilities (4) Establish	Phishing (3)	Deploy Container Exploitation for		Browser Extensions		Initialization Scripts ₍₅₎	1	Deobfuscate/Decode Files or Information		, n
Sources (2) I Capabilities (6) I Media Communication (2) I Informat Search Open Technical Databases (6) Stage Supply Chain Communication (2) I Native API Create or Modify System Escape to Host Execution Guardials (1) I Gather S Search Open Websites/Domains (3) I Trusted Relationship Serverless Execution Shared Modules Event Triggered Exploitation for Defense Evaluation for Defense <td></td> <td>Information (3)</td> <td>Accounts (3)</td> <td>Replication Through Removable</td> <td>Client Execution</td> <td></td> <td>Compromise</td> <td></td> <td>Create or Modify System Process (a)</td> <td>n</td> <td>Deploy Container</td> <td></td> <td>Gather Sp</td>		Information (3)	Accounts (3)	Replication Through Removable	Client Execution		Compromise		Create or Modify System Process (a)	n	Deploy Container		Gather Sp
Stage Stage Istage Stage Istage Modification (2) Modification (2) Modification (2) Modification (2) Modification (2) Modification (2) Gather S Search Open Websites/Domains (3) Instant Modules Scheduled Instant Modules Scheduled Instant Modification (2) Execution Go Defense Execution Go Defense Execution (16) Execution (16) Execution (16) Execution (16) Instant Modification (2) Instant Modification (2) Instant Modification (2) Instant Modification (2) Gather S Search Victim-Owned Valid Accounts (4) Instant Modules Software Event Triggered Event Triated Event Tria		Sources (2)	Capabilities (6)	Media	Communication (3)	"	Binary		Domain Policy		Domain Policy		Informati
Search Open Websites/Domains (3) I Task/Job (5) I Create or Modify Serverless Execution I Exploitation for Defense Evasion Exploitation for Defense Evasion Exploitation for Defense Evasion I Gather L Serverless Execution Websites Software Deployment Tools Software Deployment Tools Event Triggered Execution (16) I File and Directory Permissions I Eavesdre Gather L Windows Management Instrumentation Windows Impair Internal Image Impair Internal Image I I Impair Internal Image I <td></td> <td>Databases (5)</td> <td>Capabilities (6)</td> <td>Compromise (3)</td> <td>Scheduled</td> <td></td> <td>Account (3)</td> <td>"</td> <td>Escape to Host</td> <td></td> <td>Execution Guardrails (1)</td> <td></td> <td>Gather Sp</td>		Databases (5)	Capabilities (6)	Compromise (3)	Scheduled		Account (3)	"	Escape to Host		Execution Guardrails (1)		Gather Sp
Search Victim-Owned Websites Valid Accounts (a) I <td< td=""><td></td><td>Search Open Websites/Domains (3)</td><td></td><td>Trusted Relationship</td><td>Task/Job (5)</td><td>"</td><td>Create or Modify System Process (a)</td><td>n</td><td>Event Triggered</td><td></td><td>Exploitation for Defense</td><td></td><td>Commun</td></td<>		Search Open Websites/Domains (3)		Trusted Relationship	Task/Job (5)	"	Create or Modify System Process (a)	n	Event Triggered		Exploitation for Defense		Commun
Software Deployment Tools System Services (2) User Execution (3) Windows Management Instrumentation Startup (6) Coffice Application Startup (6) Scheduled Task/Job (5) Tre-OS Boot (5) Scheduled Task/Job (5) Tre-OS Boot (5)		Search Victim-Owned Websites		Valid Accounts (4)	Shared Modules		Event Triggered		Exploitation for		File and Directory	1	Gather La
System Services (2) I User Execution (3) I Windows Implant Internal Instrumentation Modify Modify Authentication Process (8) I Office Application I Scheduled I Pre-OS Boot (5) I Scheduled I Task/Job (5) I Modify Catholication I Modify Catholication <td></td> <td></td> <td></td> <td></td> <td>Software Deployment Tools</td> <td></td> <td>External Remote</td> <td></td> <td>Privilege Escalation</td> <td></td> <td>Modification (2)</td> <td></td> <td>Eavesdro</td>					Software Deployment Tools		External Remote		Privilege Escalation		Modification (2)		Eavesdro
User Execution (3) I Flow (12) Process (11) Indicator Removal (3) I Windows Management Instrumentation Modify Authentication Trask/Job (5) Indicator Removal (3) I Indicator Removal (3) I Office Application Startup (6) Office Application Startup (6) I Modify Authentication Process (8) I Modify Authentication Process (8) I Modify Cloud Compute Infrastructure (4) I					System Services (2)	ш	Services Hijack Execution		Hijack Execution Flow (12)		Hide Artifacts (10) Hijack Execution	"	Gather FS Informati
Windows Implant Internal Management Instrumentation Modify Authentication Process (g) Implant Internal Office Application Strutup (g) Implant Jetenses (10) Implant Jetenses					User Execution (3)	н	Flow (12)	"	Process Injection (12)	u	Flow (12)		Monitor f
Modify Process (8) Valid Accounts (4) Indirect Command Execution Indit Indirect Command Execution					Management Instrumentation		Image		Scheduled Task/Job ₍₅₎		Impair Defenses (10) Indicator Removal (9)		Gather St
Office Application Startup (6) II Masquerading (8) II Pre-OS Boot (5) II Modify Authentication Process (8) II Scheduled Task/Job (5) II Modify Cloud Compute Infrastructure (a) II							Modify Authentication Process (e)		Valid Accounts (4)		Indirect Command Execution		Informati
Startup (6) Modify Authentication Pre-OS Boot (5) Modify Authentication Process (8) II Scheduled Task/Job (5) Modify Cloud Compute Infrastructure (4) II							Office Application			[Masquerading ₍₈₎	11	Gather M
Scheduled Task/Job (5) n Modify Cloud Compute Infrastructure (4) n							Pre-OS Boot (5)				Modify Authentication Process (8)		
							Scheduled Task/Job ₍₅₎	"			Modify Cloud Compute Infrastructure ₍₄₎		

techniques			
			silow
Reconnaissance	Resource Development	Initial Access	Execution
9 techniques	5 techniques	12 techniques	18 techniques
Gather Spacecraft Design	Acquire Infrastructure (4)	II Compromise Supply Chain (3)	II Replay ₍₂₎
Gather Spacecraft Descriptors (3)	Compromise Infrastructure (3)	II Compromise Software Defined Radio ₍₀₎	Position, Navigation, and Timing (PNT) Geofencing ₍₀₎
Gather Spacecraft Communications Information (4)	Obtain Cyber Capabilities (2) Obtain Non-Cyber	ا Crosslink via Compromised , Neighbor ന	Modify Authentication Process ₍
Gather Launch Information	Capabilities (4)	Secondary/Backup	Compromise Boot Memory (0)
Eavesdropping (4)	Stage Capabilities ₍₂₎	Communication Channel (2)	Exploit Hardware/Firmware Corruption (2)
Gather FSW Development		Rendezvous & Proximity Operations ₍₃₎	Disable/Bypass Encryption (0)
		Compromise Hosted Payload ₍₀₎	Trigger Single Event Upset ₍₀₎
Indicators (0)		Compromise Ground System (2)	II Time Synchronized Execution (2)
Gather Supply Chain		Rogue External Entity ₍₃₎	II Exploit Code Flaws ₍₃₎
		Trusted Relationship ₍₃₎	Malicious Code (4)
Gather Mission Information (0)		Exploit Reduced Protections During Safe-Mode ₍₀₎	Exploit Reduced Protections Dur Safe-Mode ₍₀₎
		Auxiliary Device Compromise (0)	Modify On-Board Values (13)
		Assembly, Test, and Launch	Flooding ₍₂₎
		operation compromise (0)	Jamming ₍₃₎

Side-Channel Attack ₍₀₎ Kinetic Physical Attack ₍₂₎

Spoofing (5)

Non-Kinetic Physical Attack (3)

Mission Assurance Baseline Matrix

Mission Assurance Baseline v2.10



The System Engineering "V"



Image Credit: Herman Bruyninckx, used under Creative Commons Share-Alike 3.0

Consider the Internet...

... if it were a space acquisition program

- Possible Key Performance Parameters:
 - The system shall support at least three billion unique users on a daily basis
 - The system shall support at least one billion unique content sites
 - The system shall support exchange of at least 200 million rich text messages every minute
 - The system shall allow users to access sites and content via any device that conforms to a few simple communication protocols
 - Users shall be able to use a protocol-conforming device to send 1MB of data via the system to any protocol-conforming device anywhere on earth in less than one second
 - The system shall allow for near-instantaneous search of all hosted content
 - The system shall support secure exchange of sensitive data
 - The system shall achieve 99.9 percent functional availability

From Dr. Erin Ryan, "Designing for Principles"

- If these had been the KPPs, we could reasonably expect that this program would either:
 - Not have delivered on even a small fraction of the performance requirements
 - Have been cancelled
 - Be the most expensive program in the history of civilization



How Do We Design an Enterprise?

- Balance performance requirements with non-functional requirements such as:
 - Independence (Each system function or functional requirement should be satisfied by an independent design parameter)
 - Integrability (Characterized by compatibility and interoperability)
 - Decentralization (Characterized by a decentralized distribution of control, information, resources, attributes, and properties within the system architecture)
 - Flexibility
 - Adaptability
 - Modifiability
 - Simplicity
 - Modularity
 - Scalability
 - Redundancy



List from Dr. Erin Ryan, "Designing for Principles" and Armin Schulz and Ernst Fricke, "Design for Changeability"

How Do We <u>Assure</u> an Enterprise?

What might and	9. Enterprise Segment	
Enterprise Mission Assurance Baseline look like?	Scalability	 Ensure load testing is planned and applied Ensure scalability testing is planned and applied Evaluate if additional units can be manufactured quickly Evaluate vertical and horizontal scaling options
What other things should we measure?	Modifiability	 Ensure software changes can be accomplished easily Ensure sufficient hardware margin is available for upgrades Ensure standard ISAM registration decals are applied
	Modularity	 Evaluate conformance to interoperability standards Evaluate swapability of components Ensure mass model availability Ensure availability of a digital model

List from Dr. Erin Ryan, "Designing for Principles" and Armin Schulz and Ernst Fricke, "Design for Changeability"

Parting Thoughts

- Leadership in Energy and Environmental Design (LEED)
 - Developed and administered by the U.S. Green Building Council
 - Similar models exist (e.g., "meaningful use" funding for healthcare)
- Allows for an incremental approach to the adoption of enterprise and interoperability requirements

(LEED v4 for BD+C: New Construction and Major Renovation Project Checklist					Space System Enterprise Certification Project Checklist					
	Y ·	?	N	Credit Integrative Process		1		Y	?	N	Credit	Integrative Process		1
	0	0	0	Location and Transportation 1		16		0	0 0 Location and Transportation		tion and Transportation		31	
				Credit	LEED for Neighborhood Development Location	16					Credit	Compatible with enterprise ground requirements		10
				Credit	Sensitive Land Protection	1					Credit	Uses CCSDS compatible downlink		1
				Credit	High Priority Site	2					Credit	Digital twin available		2
				Credit	Surrounding Density and Diverse Uses	5					Credit	Complies with SSC MOSA Standard v.1.1		5
		-		Credit	Access to Quality Transit	5					Credit	Incorporates standard hosted payload interface		5
		-		Credit	Bicycle Facilities	1					Credit	Incorporates digital engineering practices		1
				Credit	Reduced Parking Footprint	1					Credit	Compatible with NSSL Standard Service		1
				Credit	Green Vehicles	1					Credit	Incorporates standard crosslink		16

https://support.usgbc.org/hc/en-us/articles/4404406912403-What-is-LEED-certification

Parting Thoughts

- What About "Inverted V" Acquisitions?
- The "Inverted V" uses existing solutions to address needs at all levels
 - Allows for "flow up" of solutions into systems into architecture to improve the enterprise
- Off-the-shelf solutions
 - Obtain readily available, or easily modifiable, products or services
- Gaps are flowed back into either the regular or inverted "V"

