



Controls Mapping

Michael Long



@michaellongii



@MITREattack

#ATTACKcon

Overview

- **Organizations need to implement information security controls**
 - NIST SP 800-53, PCI-DSS, CIS Controls
- **Control selection *should be* driven by threats and vulnerabilities**
 - ATT&CK can help!
- **We have challenges:**
 - Which controls do we select (and why)?
 - How do our controls map to ATT&CK techniques?
- **Many organizations create ATT&CK → Control mappings**
 - How can we as the ATT&CK team help centralize these?

ATT&CK-Controls Mapping

- **By mapping ATT&CK to common control frameworks we can:**
 - Identify controls that mitigate threats we care about
 - Identify capability gaps
 - Better understand our cybersecurity effectiveness

Legend:

Identify

Protect

Detect

Respond

Recover

	ATT&CK Tactics				
	Initial Access				
NSA Top 10 Mitigation Strategies	Identify	Protect	Detect	Respond	Recover
1. Update and Upgrade Software Immediately	Identify	Protect			
2. Defend Privileges and Accounts	Identify	Protect			
3. Enforce Signed Software Execution Policies	Identify	Protect			
4. Exercise a System Recovery Plan	Identify			Respond	Recover
5. Actively Manage Systems and Configurations	Identify	Protect			
6. Continuously Hunt for Network Intrusions			Detect	Respond	Recover
7. Leverage Modern Hardware Security Features	Identify	Protect			
8. Segregate Networks Using Application-Aware Defenses		Protect	Detect		
9. Integrate Threat Reputation Services		Protect	Detect		
10. Transition to Multi-Factor Authentication	Identify	Protect			

Prototype Mappings: ATT&CK-NIST 800-53

- Our prototype offers two views: Master & Control Family
- Master View displays the entire ATT&CK-NIST 800-53 mapping

		AC Access Control			
		AC-1 ACCESS CONTROL POLICY AND PROCEDURES		AC-2 ACCOUNT MANAGEMENT	
Initial Access	Drive-by Compromise	Protect	Detect		
	Exploit Public-Facing Application				
	External Remote Services				
	Hardware Additions				
	Replication Through Removable Media				
	Spearphishing Attachment				
	Spearphishing Link				
	Spearphishing via Service				
	Supply Chain Compromise				
	Trusted Relationship				

Prototype Mappings: ATT&CK-NIST 800-53

- Our prototype offers two views: Master & Control Family
- Master View displays the entire ATT&CK-NIST 800-53 mapping
 - 244 NIST 800-53 Controls

NIST 800-53 Controls					
		AC Access Control			
		AC-1 ACCESS CONTROL POLICY AND PROCEDURES		AC-2 ACCOUNT MANAGEMENT	
Initial Access	Drive-by Compromise	Protect	Detect		
	Exploit Public-Facing Application				
	External Remote Services				
	Hardware Additions				
	Replication Through Removable Media				
	Spearphishing Attachment				
	Spearphishing Link				
	Spearphishing via Service				
	Supply Chain Compromise				
	Trusted Relationship				

Prototype Mappings: ATT&CK-NIST 800-53

- Our prototype offers two views: Master & Control Family
- Master View displays the entire ATT&CK-NIST 800-53 mapping
 - 244 NIST 800-53 Controls
 - 266 ATT&CK Techniques

		NIST 800-53 Controls			
		AC Access Control			
		AC-1 ACCESS CONTROL POLICY AND PROCEDURES		AC-2 ACCOUNT MANAGEMENT	
ATT&CK Techniques	Initial Access	Protect	Detect		
		Drive-by Compromise			
		Exploit Public-Facing Application			
		External Remote Services			
		Hardware Additions			
		Replication Through Removable Media			
		Spearphishing Attachment			
		Spearphishing Link			
		Spearphishing via Service			
		Supply Chain Compromise			
		Trusted Relationship			

- **Control Family View lists ATT&CK mapping by Control Families**



Prototype Mappings: ATT&CK-NIST 800-53 (Continued)

- Control Family View lists ATT&CK mapping by Control Families

		AC-1 ACCESS CONTROL POLICY AND PROCEDURES	AC-2 ACCOUNT MANAGEMENT	AC-3 ACCESS ENFORCEMENT	AC-4 INFORMATION FLOW ENFORCEMENT	AC-5 SEPARATION OF DUTIES	AC-6 LEAST PRIVILEGE	AC-7 UNSUCCESSFUL LOGON ATTEMPTS	AC-8 SYSTEM USE NOTIFICATION	AC-9 PREVIOUS LOGON (ACCESS) NOTIFICATION
SS	Drive-by Compromise									
	Exploit Public-Facing Application									
	External Remote Services									
		AC-1 ACCESS CONTROL POLICY AND PROCEDURES	AC-2 ACCOUNT MANAGEMENT	AC-3 ACCESS ENFORCEMENT	AC-4 INFORMATION FLOW ENFORCEMENT	AC-5 SEPARATION OF DUTIES	AC-6 LEAST PRIVILEGE	AC-7 UNSUCCESSFUL LOGON ATTEMPTS	AC-8 SYSTEM USE NOTIFICATION	AC-9 PREVIOUS LOGON (ACCESS) NOTIFICATION
Execution	Local Job Scheduling									
	LSASS Driver									
	Mshsa									
	PowerShell									
	Regsvcs/Regasm									
	Regsvr32									
	Rundll32									
	Scheduled Task									
	Scripting									
	Service Execution									
	Signed Binary Proxy Execution									
	Signed Script Proxy Execution									
	Source									
	Space after Filename									
	Third-party Software									
	Trap									
	Trusted Developer Utilities									
	User Execution									
	Windows Management Instrumentation									
	Windows Remote Management									
	XSL Script Processing									

Mapping Challenges

- **Mapping criteria**
- **Changing control standards**
- **Scale**
- **Differing configurations and implementations**
- **Some organizations have created internal mappings but...**
 - Sharing externally can be difficult
 - Results in duplication of effort
 - Hinders collaboration and innovation

Our Future Goals

- **Provide a curated source of trusted mappings**
 - Support community contributions
- **Develop a flexible mapping data structure**
 - Responsive to change
 - Able to scale
- **Present mappings in a user-friendly application**
 - Similar to the ATT&CK Navigator

Going Forward

- **We need your input!**
 - Tell us what types of mappings you want and why
- **Do you want to share an awesome mapping?**
 - Let us know!
- **We can only win if we work together**
 - Let us know if you want to help

Michael Long

 @michaellongii

ATT&CKTM

attack@mitre.org

 @MITREattack

#ATTACKcon