ADVERSARY EMULATION

GENERATING MITRE ATT&CK TECHNIQUE SEQUENCES

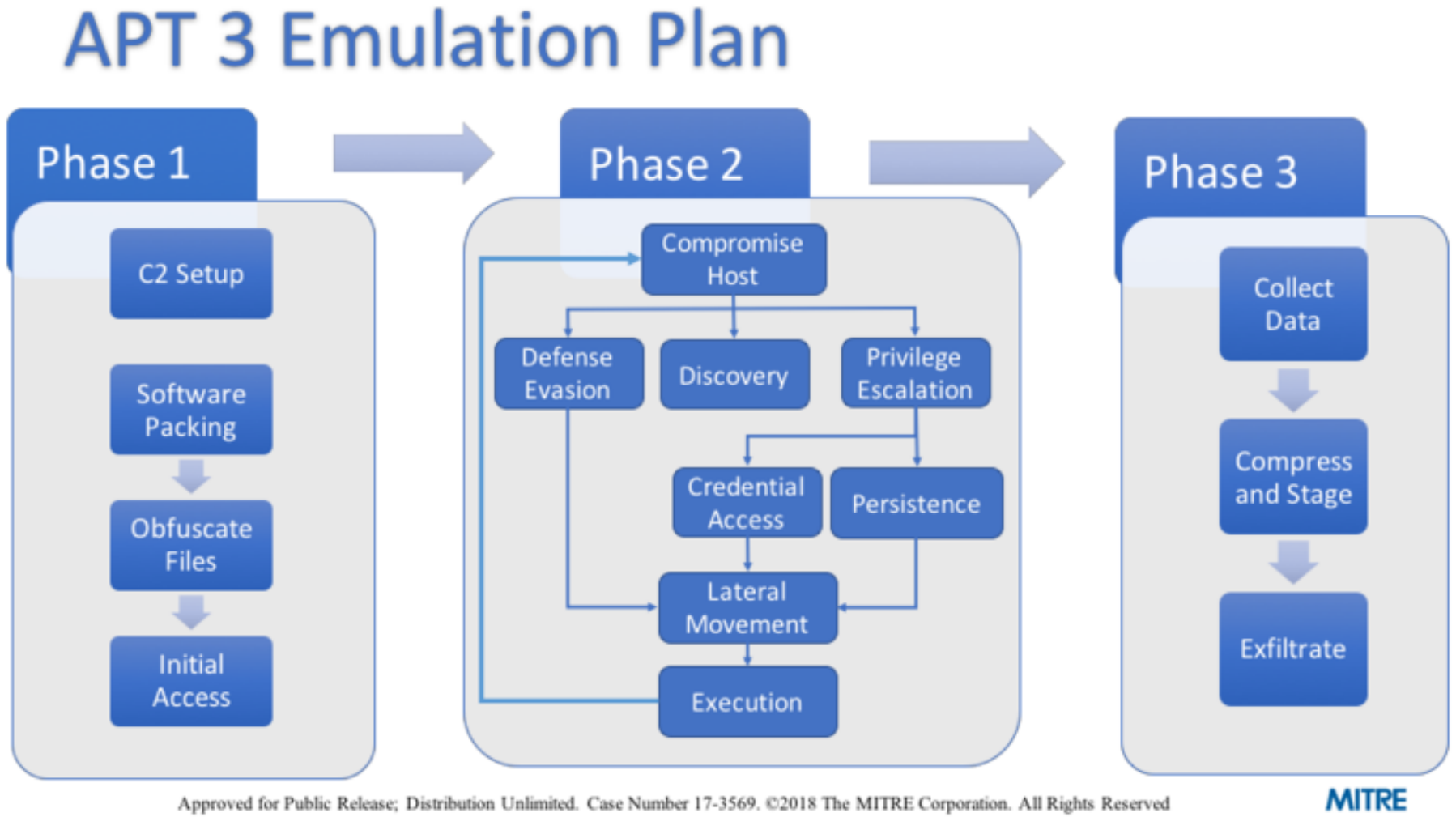
PRESENTED BY MARTIN EIAN

mnemonic

Adversary Emulation

Test your defenses based on real-world adversary behaviors

Adversary Emulation Plan: APT3



https://attack.mitre.org/resources/adversary-emulation-plans/

Adversary Emulation Plans

- Intelligence Summary
  - An overview of the adversary and references to cited Intelligence
- Operational Flow
  - Chains techniques together into a logical flow of the major steps that commonly occur across the selected adversary's operations
- Emulation Plan
  - The TTP-by-TTP, command-by-command walkthrough to implement the adversary's operational tradecraft as described in the Intelligence Summary and the Operational Flow

https://medium.com/mitre-engenuity/introducing-the-all-new-adversary-emulation-plan-library-234b1d543f6b

MITRE ATT&CK

“MITRE ATT&CK is a curated knowledge base and model for cyber adversary behavior, reflecting the various phases of an adversary’s attack lifecycle and the platforms they are known to target.”

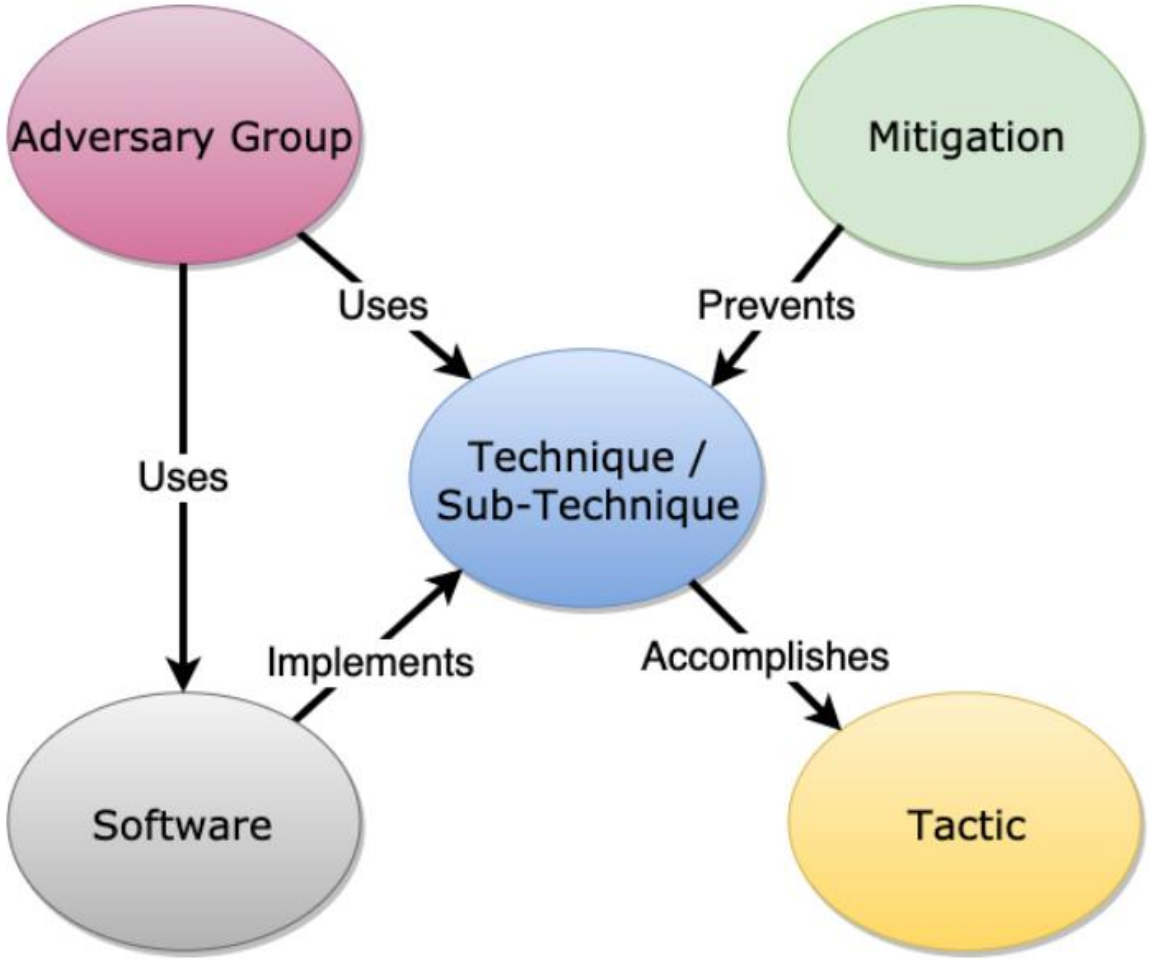
https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf

MITRE ATT&CK Core Components

- Tactics
  - short-term, tactical adversary goals during an attack
- Techniques
  - the means by which adversaries achieve tactical goals
- Sub-techniques
  - more specific means by which adversaries achieve tactical goals at a lower level than techniques
- Adversary usage of techniques, their procedures, and other metadata

https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf

MITRE ATT&CK Object Relationships



https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf

Problem Statement

Generate the Operational Flow of an Adversary Group, campaign or incident

Previous Work

- MITRE CALDERA
  - https://github.com/mitre/caldera
- “Finding Dependencies Between Adversary Techniques”
  - FIRST Conference 2019
  - Andy Applebaum, MITRE
  - https://www.first.org/resources/papers/conf2019/1100-Applebaum.pdf

Promise Theory

- Autonomous agents
- Promises
  - Statement of intent
  - “I can provide this”
- Benefits
  - Scalable
  - Distributed

https://link.springer.com/content/pdf/10.1007/11568285_9.pdf

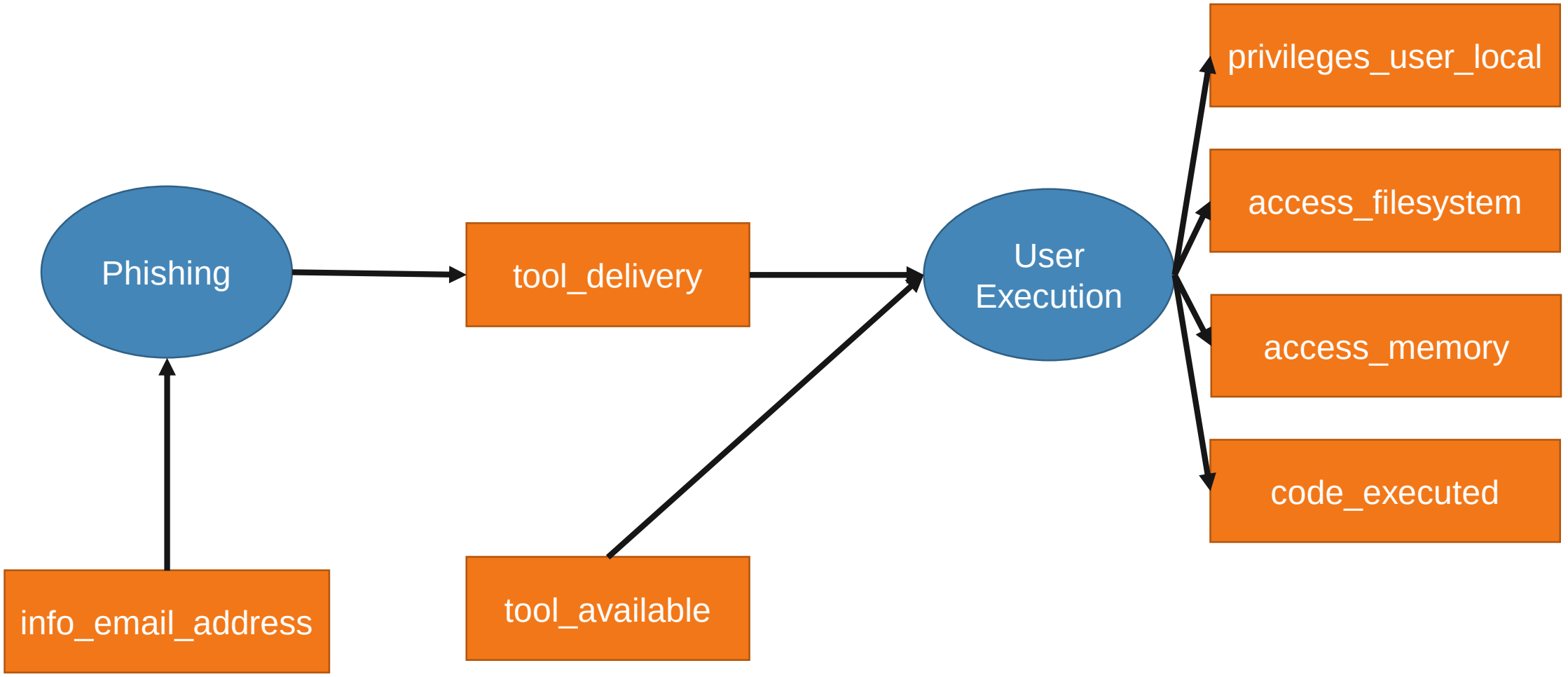
General Model

- (Sub-)Technique
  - Autonomous agent
- Requires (preconditions)
  - Set of promises needed to execute the technique
- Provides (postconditions)
  - Set of promises provided after execution of the technique

Example: Remote Services


```
"T1021": {
        "name": "Remote Services",
        "provides": [
            "moved_laterally"
        ],
        "relevant_for": [
            "client",
            "content_management_server",
            "file_server",
            "login_server",
            "web_server"
        ],
        "requires": [
            "access_network",
            "credentials_users",
            "info_network_hosts",
            "info_network_services"
        ],
        "tactic": [
            "Lateral Movement"
        ]
    },
```

Example: Phishing and User Execution



Approach

- Develop vocabulary of promises
  - STIX and MAEC not suitable
- Review all (sub-)techniques
  - Define “requires” and “provides”
- Develop tool
  - Generate attack stages
  - https://github.com/mnemonic-no/aep

Tool Overview

- Inputs:
  - List of (sub-)techniques
    - ATT&CK Navigator Layer
    - Simple JSON
  - Definitions of “requires” and “provides”
  - End condition (objective)
- Initialization:
  - Create empty queue
- Execution: For each attack stage
  - Execute (sub-)techniques where all “requires” are present in queue
  - Add “provides” to queue
- Output:
  - Attack stages with corresponding (sub-)techniques
  - Verdict

TOOL DEMO

mnemonic

ATT&CK Issues

- Defense Evasion and Persistence
- “How it’s done”-techniques
  - Exploit Public-Facing Application
- “What you get”-techniques
  - Valid Accounts

Side Effects

- Identify missing (sub-)techniques in ATT&CK
  - Submit to MITRE

Caveats

- Adversary Groups vs incidents/campaigns
- Attack on specific infrastructure
- Vocabulary coverage
- Mapping bias
- Completeness

Future Work

- Standard vocabulary of promises
- ATT&CK integration
- SOCCRATES platform integration
- Structured procedure definitions

SOCCRATES

- Stakeholder group
- Web site
  - https://soccrates.eu