PennState
Applied Research
Laboratory

Automated Attack Framework for Test & Evaluation (AAFT)

2017 International Test and Evaluation Association Cyber Security Workshop

March 29, 2017

Mr. Andrew Shaffer

The Applied Research Laboratory
The Pennsylvania State University

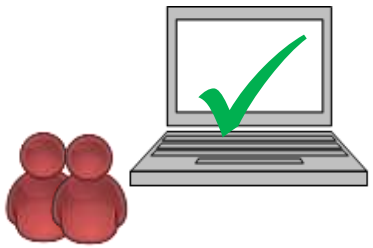
PennState Applied Research Laboratory

Outline

- Test & Evaluation Needs
- AAFT Overview
- Development Approach
- Attack Scripts and Autonomous Attack Engine
- Autonomous Attack Example
- System Tools and Capabilities
- Potential Use Cases
- Summary
- Future Work

PennState Applied Research Laboratory

Test & Evaluation Needs



System Accredited Following Red Team Testing

New System Delayed By Limited Red Team Availability

Deployed System Compromised Before Red Team Testing Completed

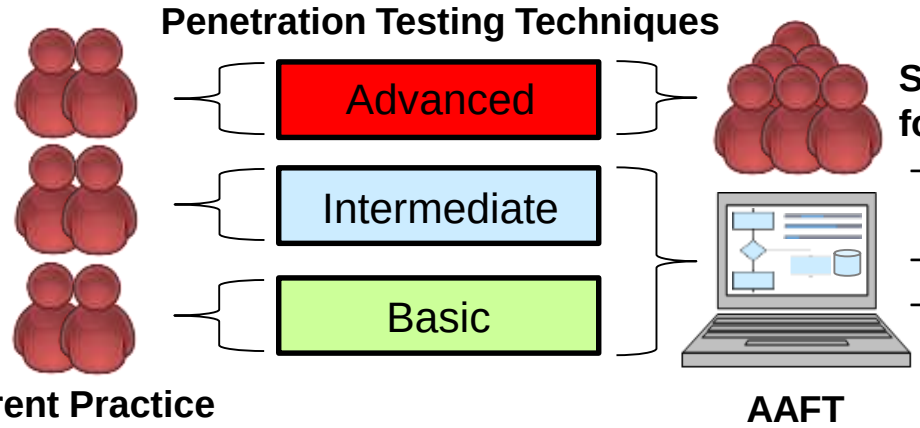
- **DoD 8500.01 requires Red Team cyber penetration testing**
  - Continuous and comprehensive monitoring are recommended
- **Lack of Red Team availability for all required system testing**
  - Limited availability delays system accreditation and increases risk
  - Tools to improve Red Team utilization and efficiency are needed
- **Blue Team validation and training require additional support**
  - Automated Red Team tools are needed to free up testing personnel
- **Red Team training is time-consuming and highly specialized**
  - Knowledge of one attack tool does not necessarily translate to others
  - Tools supporting high-level directives are needed

Automated tools are needed to improve Red Team utilization & efficiency

PennState Applied Research Laboratory

AAFT Overview

Few available skilled Red Team testers must:
- Emulate all threats
- Train Blue Teams
- Validate vulnerabilities

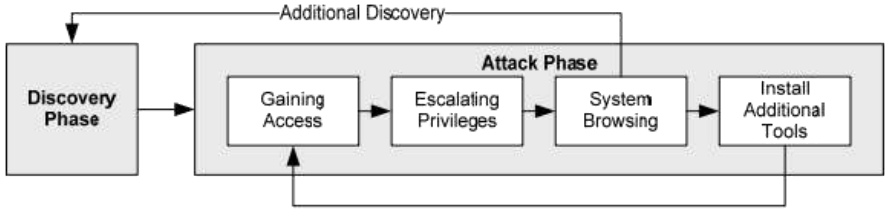


Skilled Red Team testers can focus on advanced threats:
- AAFT emulates basic/intermediate threats
- AAFT trains Blue Teams
- AAFT validates vulnerabilities

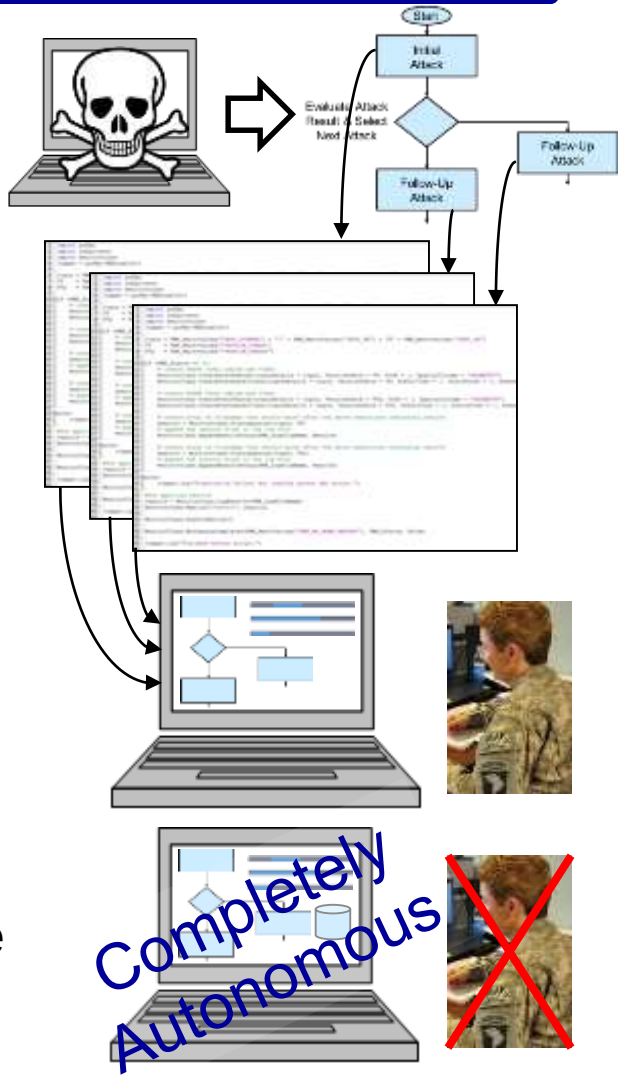
- **Provides automated basic and intermediate-level penetration testing**
  - Enables DoD 8500.01 comprehensive continuous monitoring
- **Supports easy-to-use framework to facilitate integration of new attacks**
  - Provides high-level attack directives to improve Red Team effectiveness
  - Supports easy integration with new open-source and custom tools
  - Framework comparable to Metasploit with support for multiple attack tools
- **Allows skilled Red Teams to focus on advanced threat emulation**
  - Takes over less challenging penetration testing tasks
  - Takes over Blue Team training and rapid vulnerability verification

AAFT provides an integrated framework to automate cyber attacks

Development Approach



http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf

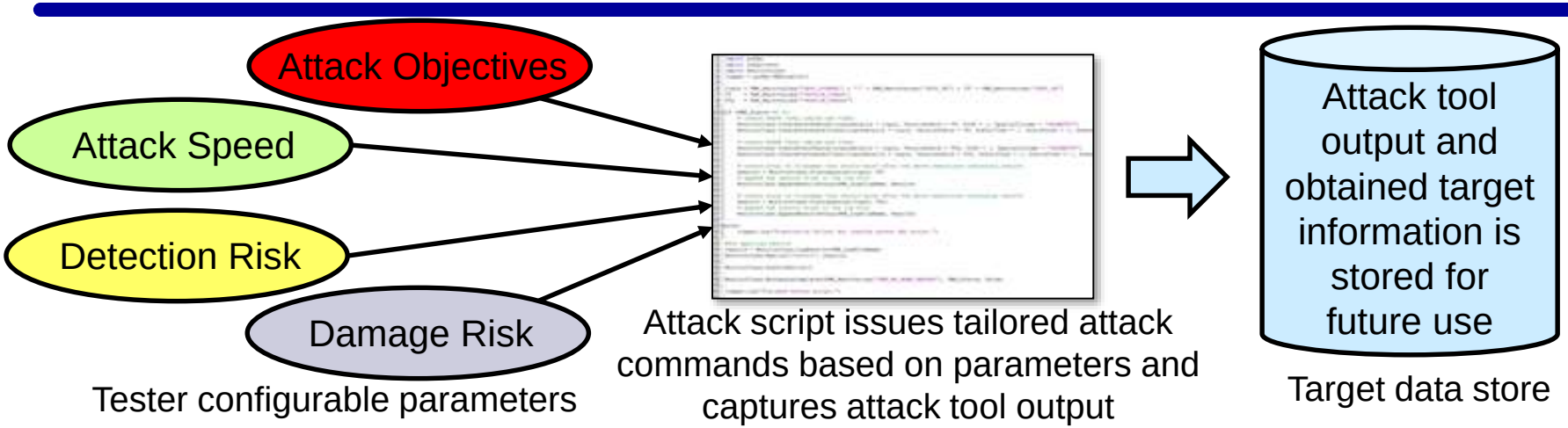


- **Model real-world attacks using flowchart**
  - Based on NIST procedures, tutorials, and real-world Red Team exercises
- **Create single-tool attack scripts using high-level directives**
  - Support open-source and custom attack tools
  - Allow attack objective and parameter specification
- **Develop user-directed attack GUI**
  - Support using scripts or manual commands
- **Develop novel Autonomous Attack Engine**
  - Implement flowchart as reconfigurable data structure
  - Create flowchart navigation engine and target data store

Incremental development ensures ongoing capability improvement

PennState Applied Research Laboratory

Attack Scripts

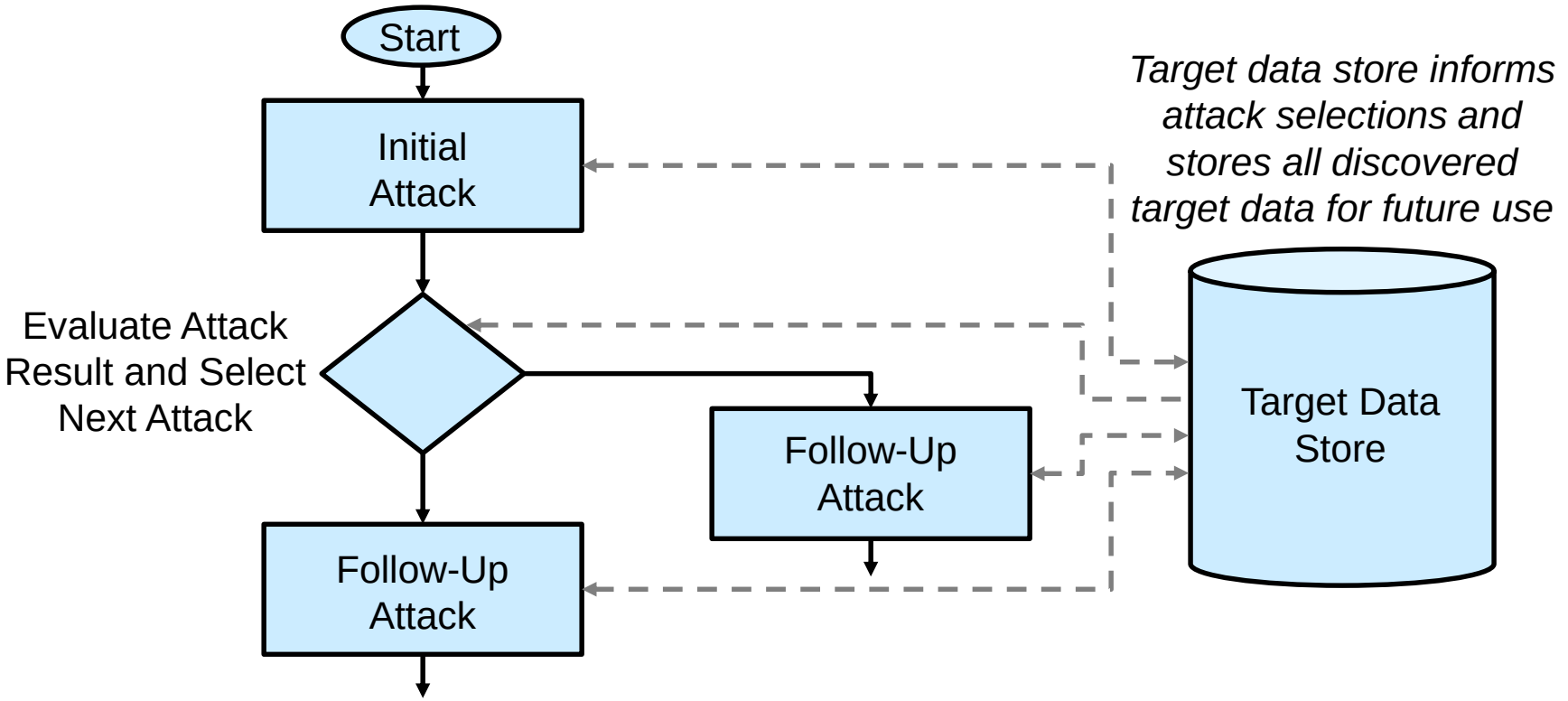


- **Each attack script enables high-level attack directives for a single attack tool**
  - Specify attack objectives: compromise confidentiality, integrity, and/or availability (root access = all three)
  - Specify minimum and maximum allowable attack speeds
  - Specify allowable detection risk and target damage risk
- **Attack scripts translate objectives & parameters into tool commands**
  - Script queries available target information to refine attack command selection
- **Script captures attack tool output following attack execution**
  - Also records any collateral target information obtained during attack

Attack scripts enable high-level directives for individual tools

PennState Applied Research Laboratory

Autonomous Attack Engine



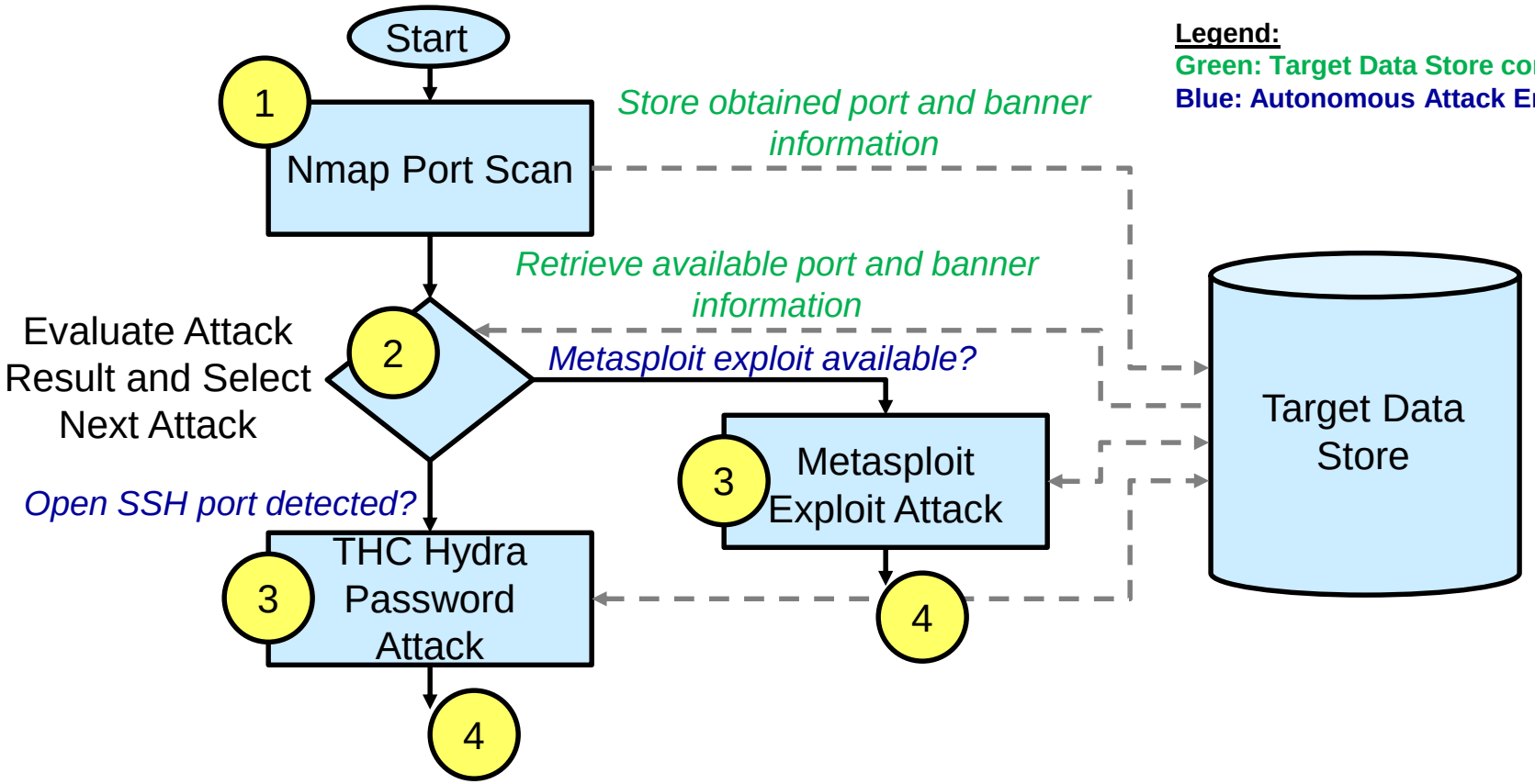
Autonomous Attack Engine navigates through AAFT attack flowchart

- Selects tools to use based on objectives, parameters, and target information
- Manages parameters used by attack scripts
- Maintains target data store to inform attack selections and attack scripts

Autonomous Attack Engine provides high-level direction for AAFT attack

PennState Applied Research Laboratory

Autonomous Attack Example



Autonomous Attack Engine directs port scan and initial attack:

1. Uses Nmap to detect open ports and collect banner information
2. Uses results of Nmap scan to select next attack
3. Performs selected attack based on objectives and speed/risk parameters
4. Proceeds through remainder of attack flowchart until objectives achieved

PennState Applied Research Laboratory

System Tools

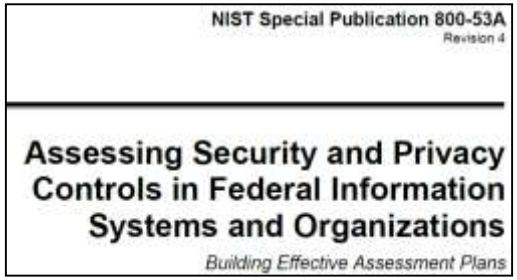
- **Initial AAFT development is focused on commonly used open-source penetration testing tools**
  - Nmap (network mapper)
  - Metasploit (integrated attack framework)
  - THC Hydra (online login cracker)
  - John the Ripper (offline password cracker)

- **Future development will add support for more sophisticated tools and attacks**
  - Both open-source and custom tools will be supported
  - Tools are integrated using Python scripts

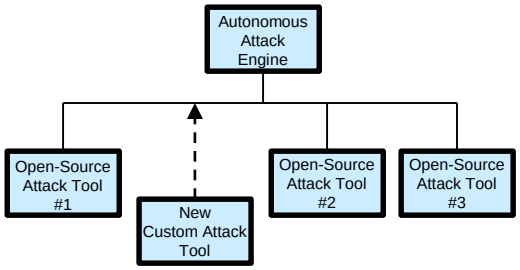
- **Target data and attack flowchart stored in MySQL database**

AAFT framework being developed for open-source and custom tools

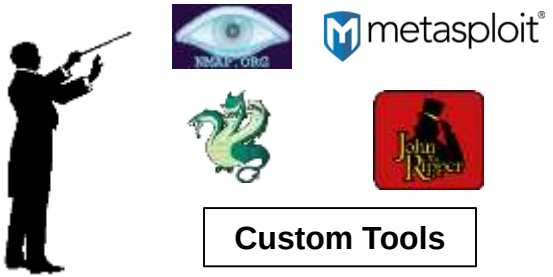
System Capabilities



Automation enables continuous comprehensive monitoring



Framework design enables easy new tool integration



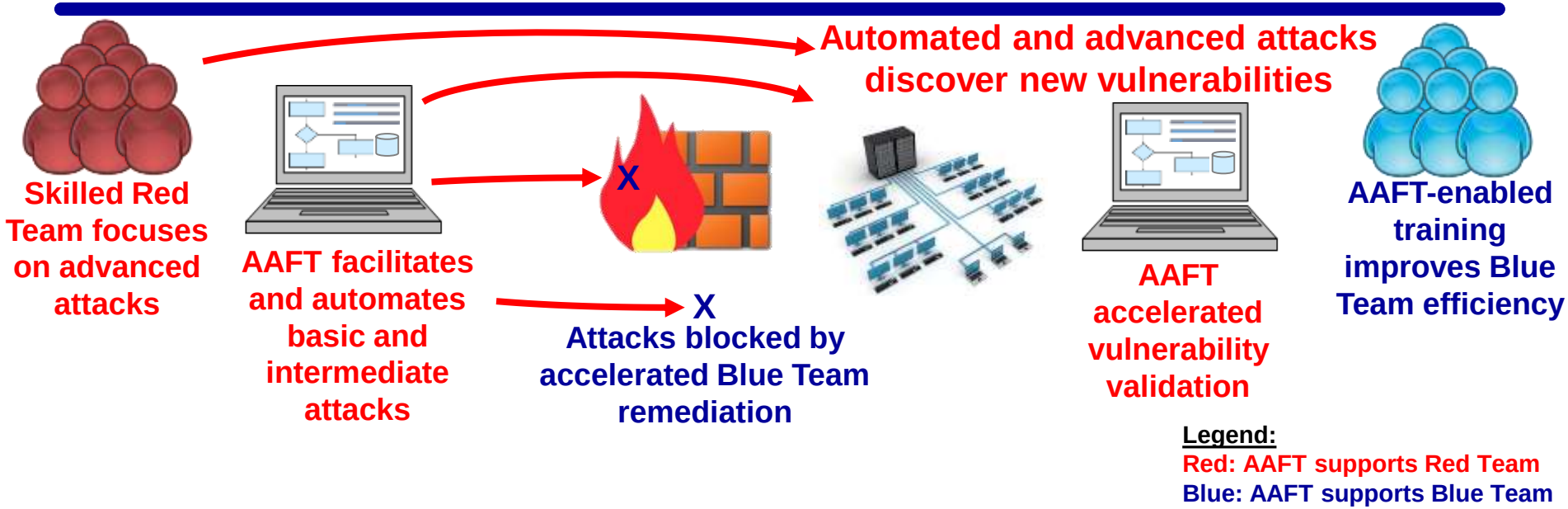
High-level directives expand Red Team capabilities

- **Automation supports DoD 8500.01 continuous monitoring**
  - Increases testing rigor and reduces reauthorization costs
- **Framework enables easy integration with current and future tools**
  - Leverages developments in open-source attack tools
  - Supports customized/proprietary attack tools
- **Automation and attack directives expand Red Team capabilities**
  - Allow skilled testing personnel to focus on more challenging tasks
  - Increase capabilities of entry-level cyber testing personnel
  - Improve Blue Team vulnerability validation and training

AAFT automation, integration framework, and high-level attack directives improve cyber test and evaluation capabilities

PennState Applied Research Laboratory

Potential Use Cases

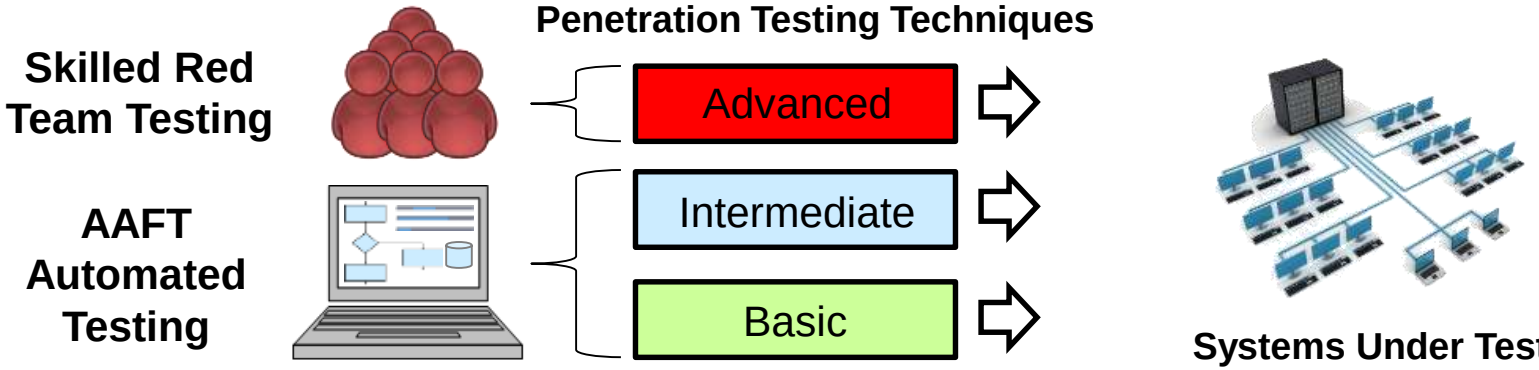


- **Allow skilled Red Team testers to focus on advanced attacks rather than emulating all levels of threat attacks**
- **Perform basic and intermediate-level Red Team attacks using an innovative autonomous framework and attack directives**
- **Accelerate vulnerability validation and remediation**
- **Support Blue Team training**

AAFT supports both Red Team and Blue Team cybersecurity efforts

PennState Applied Research Laboratory

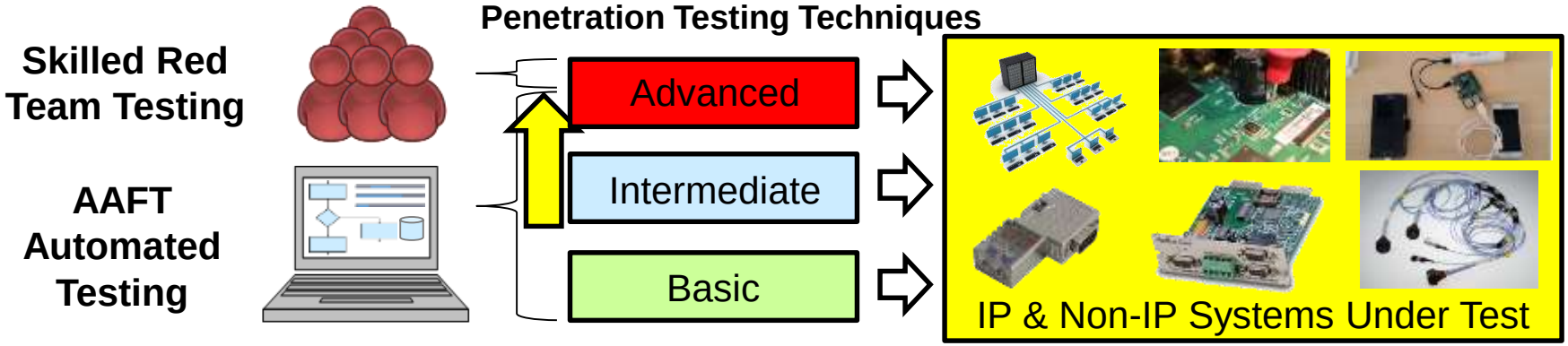
Summary



- **Attack scripts and Autonomous Attack Engine are new technologies that advance cybersecurity test and evaluation**
  - Applying autonomy research to cybersecurity improves state-of-the-art in Red Team and Blue Team testing
- **AAFT addresses critical cybersecurity Test and Evaluation needs**
  - Enables better utilization and efficiency of available Red Team testers
  - Increases scope of cybersecurity testing that can be performed
- **System design and development is ongoing**
  - Configured initial cyber test lab for prototype testing
  - Began cyber tutorials and started attack flowchart development
  - System implementation continuing

AAFT advances state-of-the-art in Red Team and Blue Team testing

Future Work



- **Incrementally increase tool and attack sophistication**
  - Add support for concurrent, persistent, and social engineering attacks
- **Add support for community development of new attack scripts and Autonomous Attack Engine flowchart paths**
  - Facilitate knowledge and code sharing across government, industry & academia
  - Increase AAFT system development speed
- **Automate and accelerate non-IP testing**
  - Non-802.11 wireless, acoustic, serial, USB, MIL-STD-1553, ARINC-429, PROFIBUS, Modbus, etc… also require penetration testing
  - Standardized protocol decoding and attacks can significantly accelerate testing

Legend:
Yellow: Future Work Focus

Seeking opportunities for system maturation and future transition

Points of Contact

Andrew Shaffer
Penn State Applied Research Laboratory
814-863-0312
aps148@arl.psu.edu

Bruce Einfalt
Penn State Applied Research Laboratory
814-863-4142
bte2@arl.psu.edu

PennState Applied Research Laboratory

Questions