# RISK AND RESILIENCE BOOTCAMP

TEKsystems Global Services

# WORKFORCE DEVELOPMENT

# ADVERSARIAL RISK ANALYSIS

This module introduces adversarial risk analysis

# ADVERSARIAL RISK ANALYSIS

- Modern risk environments
  - Such as cybersecurity, fraud prevention, counter-intelligence, regulatory strategy, and operational resilience require more than static risk models
  - Traditional risk assessments often assume passive threats
  - In reality, many risks involve intelligent adversaries who actively adapt, probe, and innovate which constantly changes the risk landscape
- Adversarial Risk Analysis (ARA)
  - Provides a dynamic approach that models attackers' motivations, capabilities, and likely behaviors alongside defensive strategies

# ROBUST SYSTEMS

- A system is robust when it has
  - "The ability to cope with errors during execution and to handle erroneous input"
- Three types of robustness
  - *Safe*: when the system can detect, respond to or prevent accidental harm
  - *Secure*: when the system can detect, respond to or prevent intentional harm
  - *Survivable*: when the system is both safe and secure

# SOFTWARE ENGINEERING

- Focuses on eliminating defects
  - To remove any faults that prevent the software from working as specified
  - To ensure the software handles the normal and reasonable situations and inputs correctly, including invalid inputs
- Does not focus on intentional attacks
  - Attacks usually involve attempting to put the system into an abnormal situation or unusual state
  - Attacks also usually involve bizarre, unreasonable and highly unusual inputs
  - Not the type of inputs that would be thought of when looking at normal operations
  - Also, the inputs may occur with a volume and velocity that would stress the system
  - The imposed stress would cause the system to go into an unstable state

# SECURITY ENGINEERING

- A security flaw is
  - A defect in or a feature of the software that can be exploited by an attacker
  - A defect that is fixed for normal operations (i.e. safe) may still be a security flaw
  - Not all defects are security flaws
  - Only defects that can be exploited are security flaws
- A vulnerability is
  - A set of circumstances that allow an attacker to exploit  a security flaw

# SECURITY ENGINEERING

- A mitigation is the removal of a vulnerability either
  - By fixing the underlying security flaw; or
  - Developing a workaround that prevents attackers from accessing the security flaw
- Not all security flaws can be fixed
  - The cost of fixing the flaw may be prohibitive
  - The flaw may be complex or involve multiple components which means it may be a systemic problem, not a defect

# SECURITY: PREVENTIVE PLANNING

- Design with the objective that the system will eventually be accessible from the public internet
  - Even if there are no immediate plans to do so
- Use a common authentication and authorization pattern, preferably based on existing security components
  - Avoid creating a unique solution for each system
- Least privilege
  - Access and authorization should be assigned to system clients based on the minimal amount of access they need to carry out the functions required

# SECURITY: PREVENTIVE PLANNING

- Maximize entropy (randomness) of security credentials
  - Use API Keys rather than usernames and passwords for API
  - Balance performance with security with reference to key lifetimes and encryption/decryption overheads
  - Standard secure coding practices should be integrated
- Security testing capability is incorporated into the development cycle
  - Continuous, repeatable and automated tests to find security vulnerabilities in APIs and other applications during development and testing

# SECURITY: USE CVE

- CVE = Common Vulnerabilities and Exposures.
  - An international, community-driven effort that identifies and catalogs publicly known cybersecurity vulnerabilities
  - Each vulnerability is assigned a unique CVE ID (e.g., CVE-2024-12345).
  - Managed by the CVE Program,
  - Overseen by MITRE Corporation
  - Sponsored by the U.S. Department of Homeland Security (DHS CISA).
- Goals of CVE
  - Provide a single, standardized identifier for vulnerabilities
  - Eliminate confusion caused by multiple vendors using different names for the same issue
  - Enable security tools, databases, and services to reference vulnerabilities consistently
  - Serve as the foundation for related resources like the NVD (National Vulnerability Database)

# SECURITY: USE CVE

- How CVE IDs are assigned
  - A researcher or vendor finds a vulnerability
  - They request a CVE ID from a CVE Numbering Authority (CNA) (e.g., Microsoft, Red Hat, Apache, or MITRE)
  - Once confirmed, the vulnerability is published with its CVE ID
- Example CVE Record
  - CVE-2023-4863
  - *Description*: A heap buffer overflow in the WebP image library (libwebp)
  - *Impact*: Remote code execution when processing malicious images
  - *References*: Links to Google advisory and patches
  - *Status*: Published

# SECURITY: USE CVE

- How risk assessments should use CVE
  - *Monitor*: Stay aware of new vulnerabilities in the software in use
  - *Use* CVE feeds or vendor advisories
  - *Assess Risk*: Cross-check with NVD for CVSS severity ratings
  - *Patch*: Apply vendor updates or mitigations as soon as possible
  - *Document*: Track CVEs relevant to your systems for compliance reports
  - *Integrate*: Use automated tools (e.g., pip-audit for Python, OWASP Dependency-Check for Java/Maven) that map library vulnerabilities to CVE IDs

# RED TEAM VS. BLUE TEAM

- A Red Team emulates real-world adversaries
  - Their goal is to
    - Identify vulnerabilities
    - Exploit weaknesses
    - Bypass controls
    - Validate the organization’s defensive readiness
    - Think creatively and asymmetrically

# RED TEAM VS. BLUE TEAM

- A Red Team emulates real-world adversaries
  - Simulate the strategies of motivated threat actors such as:
    - Cybercriminals
    - Insider threats
    - State-sponsored attackers
    - Competitors
    - Fraudsters
  - Red Team mindset
    - “What would I do to break this system? How can I cause maximum impact at lowest cost?”

# RED TEAM VS. BLUE TEAM

- Blue Team (Defender Perspective)
  - The Blue Team represents the defenders responsible for:
    - Protecting assets
    - Detecting threats
    - Responding to incidents
    - Strengthening resilience
    - Analyzing attack paths and closing gaps
  - They maintain controls, monitor systems, and ensure compliance with risk and security frameworks
  - Blue Team mindset
    - "How do we detect and prevent attacks? What controls fail under pressure? How do we reduce impact when controls break?"

# RED–BLUE INTEGRATION

- Advanced risk analysis uses Red Team and Blue Team insights in combination
  - Red Team identifies realistic threat behaviors
  - Blue Team validates control effectiveness
  - Results feed directly into risk assessments, scenario analysis, control optimization, and investment decisions
- This interplay creates a continuous improvement cycle
  - Known as Purple Teaming
  - A collaboration model where both sides learn and adapt

# ADVERSARIAL RISK ANALYSIS

- Adversarial Risk Analysis (ARA)
  - Mathematical and strategic framework designed to address situations where risks arise from strategic interactions between intelligent opponents
  - Unlike traditional risk assessment, which treats threats as random events, ARA
    - Models attackers as decision-makers
    - Estimates the utility and preferences of adversaries
    - Predicts attacker actions given defensive controls
    - Helps defenders choose optimal strategies
  - ARA is widely used in
    - Cybersecurity modeling
    - Anti-fraud systems
    - Military and intelligence operations
    - Regulatory enforcement
    - Competitive market strategy

# KEY CONCEPTS

- Attacker utility and goal modeling
  - Attackers differ in
    - Motivation (financial gain, disruption, espionage)
    - Risk tolerance
    - Resource availability
    - Skill level
    - Time horizon
  - ARA attempts to quantify
    - Expected benefit to the attacker
    - Expected cost (effort, detection, penalties)
    - Probability of success
  - Enables defenders to anticipate which attack paths are most appealing to an adversary

# KEY CONCEPTS

- Defender Modeling
  - Defenders assess
    - Control effectiveness
    - Detection and response capabilities
    - Costs of mitigation
    - Probability of stopping different attack strategies
  - ARA integrates attacker and defender models to produce strategic recommendations, not just static risk scores

# KEY CONCEPTS

- Game theory integration
  - ARA incorporates elements of game theory, where:
    - Attackers and defenders are players
    - Each takes actions to maximize their outcomes
  - Both adjust strategies based on expectations of each other
  - However, ARA improves on traditional game theory by adding uncertainty modeling into attacker decision-making.

# KEY CONCEPTS

- Probabilistic forecasting
  - ARA uses
    - Bayesian models
    - Monte Carlo simulation
    - Influence diagrams
    - Decision tree analysis
  - These techniques help defenders estimate
    - The likelihood of different attack strategies
    - The expected loss given various defensive investments
    - Optimal allocation of limited security resources

# RED TEAM / BLUE TEAM AND ARA

- Red Teams supply real-world attacker tactics
  - Attack paths
  - Exploit likelihood
  - Lateral movement patterns
  - Social engineering scenarios
  - Control bypass strategies
- Blue Teams validate defensive assumptions
  - Actual control effectiveness
  - Detection performance
  - Control interaction failures
  - True incident response times

# RED TEAM / BLUE TEAM AND ARA

- ARA converts these insights into actionable risk intelligence
  - Which attacker strategies are most likely?
  - How would adversaries adapt after a control upgrade?
  - Where should limited defensive budgets be spent?
  - What attack paths provide attackers their highest utility?

# EXAMPLES

- Cybersecurity
  - Red Team simulates phishing attack
  - Blue Team analyzes email filters and incident response
  - ARA predicts attacker's next likely exploit path
  - Organization strengthens MFA enforcement to reduce attacker utility
- Fraud prevention
  - Red Team models fraudster behavior in a payments system
  - Blue Team tests detection rules
  - ARA evaluates which fraud strategies yield the highest payout relative to detection risk

# TIGER TEAMS

- Refers to a small, highly skilled, cross-functional group of experts tasked with aggressively probing a system for weaknesses
  - Originated in the U.S. military and aerospace industries and has since become common in adversarial risk exploration
- A tiger team is:
  - *Elite*: Typically composed of top specialists in cybersecurity, system architecture, penetration testing, networking, and sometimes social engineering
  - *Goal-driven*: They attempt to break into or compromise a system in the same way a real attacker would
  - *Independent*: Operate separately from the defenders team to avoid bias – the defenders may be unaware it is a test so that they respond realistically
  - *Persistent and creative:* Use both conventional and unconventional methods to uncover vulnerabilities

# TIGER TEAMS

- A tiger team may:
  - Perform penetration testing on networks, systems, or applications
  - Conduct red-team exercises (adversarial simulations)
  - Test incident response and defensive capabilities
  - Attempt social engineering attacks
  - Identify design flaws, misconfigurations, or implementation issues
  - Evaluate overall organizational security posture
- They essentially act as ethical adversaries whose mission is to expose weaknesses before real attackers do

# TIGER TEAMS

| Tiger Team | Red Team |
| --- | --- |
| Broader scope: may analyze design, architecture, physical security, or business processes | Focuses on adversarial attack simulation |
| Common in engineering and aerospace for problem-solving | Common specifically in cybersecurity |
| One-time or special-mission teams | Frequently ongoing, repeated exercises |

# ADVANTAGES OF ARA

- Realistic modeling of intelligent threats
  - Traditional models assume randomness while ARA assumes strategy
- Enables dynamic risk assessment
  - Adversaries change tactics; ARA accounts for adaptive behavior
- More accurate prioritization of controls
  - Budget is allocated where it most changes attacker decisions
- Supports proactive rather than reactive security
  - Defenders can anticipate next-step attacker moves
- Bridges the gap between qualitative and quantitative methods
  - ARA leverages SME insights and probabilistic modeling

# PITFALLS AND CHALLENGES OF ARA

- Requires deeper expertise
  - ARA demands knowledge of game theory, attacker modeling, and Bayesian analysis.
- Sensitive to modeling assumptions
  - Small errors in attacker utility estimation can alter predictions
- Red Teaming must be mature
  - Poor-quality Red Team exercises produce misleading insights
- Resource-intensive
  - Complex modeling takes time and computational effort
- Can create overly complex output for executives
  - Requires translation into business-relevant language (risk scenarios, expected losses)

# INTEGRATING ARA INTO RISK MANAGEMENT

- Effective integration involves:
  - Building threat profiles
    - Attacker types, motivations, resources, preferred methods
  - Conducting structured Red Team assessments
    - Not just penetration tests; full attack-chain simulations
  - Aligning Blue Team detection, monitoring, and IR metrics
    - Ensure control performance data is available for modeling

# INTEGRATING ARA INTO RISK MANAGEMENT

- Effective integration involves
  - Developing probabilistic attacker models
    - Using Bayesian stats, loss-event data, and scenario analysis.
  - Linking ARA outputs to risk registers and governance
  - Translate attacker likelihood and defender effectiveness into
    - Inherent/residual risk
    - Control priorities
    - Investment justification
  - Conducting iterative cycles
    - ARA improves over time as attacker and defender actions evolve.

# Q&A AND OPEN DISCUSSION