ASREN
Arab States Research and Education Network

الجمهورية التونسية
وزارة التعليم العالي والبحث العلمي

مركز الحساب الخوارزمي
Centre de Calcul El-Khawarizmi
www.cck.rnu.tn

Networks & Security: Active Defense and Cyber Deception

Slim Rekhis

Higher School of communications of Tunis (SUP’COM)

slim.rekhis@supcom.tn

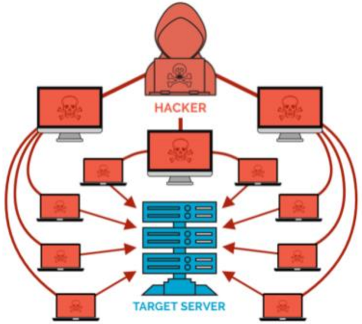
Open Science – The Way Forward: 19-20 July 2022

Outline

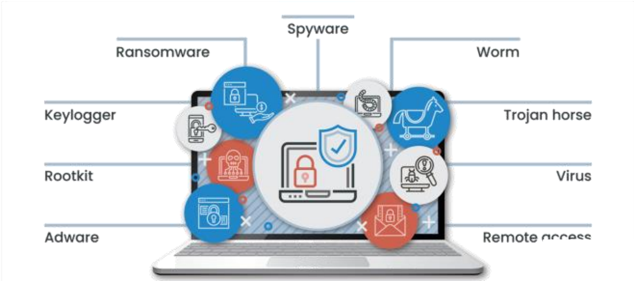
- Attacks evolution and characteristics
- Active defense and cyber defense
- Honeypots and Honeytokens
- Moving target Defense
- Deception in depth for active defense

Threats to Networks

IoT attacks



DDoS



Malware

Man In the Middle

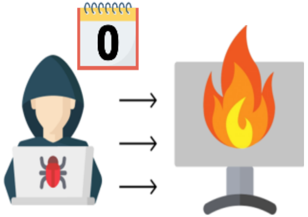
phishing

SQL injection

Ransomware

Insider threats

Zero-Day exploits



Cyber Security Statistics* in 2022

Sine the start of the COVID-19 pandemic, there has been a **300% increase** in the number of cybercrimes

In 2021, the ransomware industry is worth **$14 BILLION.**[5]

As of January 2021, Google registered over 2 million phishing websites. Compared to January 2020, this was a 27% increase.[4]

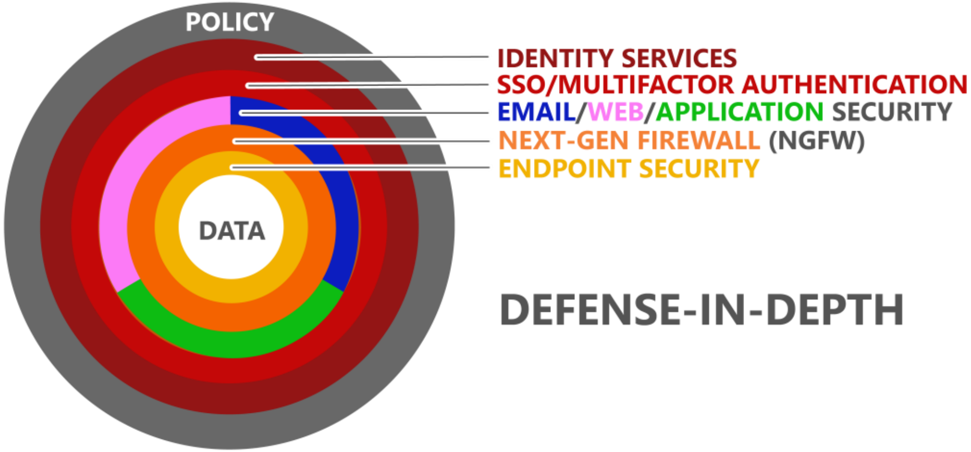
* www.judge.com

Complexity and sophistication of attacks

- Automated, remotely executed and rapidly self propagating in the infrastructure
- Disruptive (encrypting data, physically damaging assets)
- Artificial intelligence empowered (smart, converge as quickly as possible)
- Large-scale and coordinated
- Capable of shifting to the cloud and increasingly targeting critical infrastructures
- Highly sophisticated and impact supply chain
- Polymorphic and metamorphic
- Offered as a managed service to anyone who wills to pay (e.g., Ransomware-As-A-Service)

Limitation of conventional network security measures

- Convention defense measures
  - Firewalls
  - Identity and access management
  - Anti-virus and anti-malware software
  - Email, Web and Application security
  - Behavioral analytics
  - Data loss prevention systems
  - Mobile device security
  - Security Information and Event Management
  - Security Orchestration Automation and Response
  - …

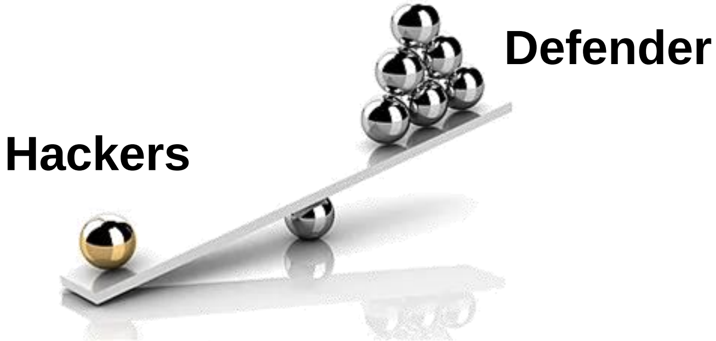


DEFENSE-IN-DEPTH

- Are proven weak against infiltration
- Can generate an overwhelming number of false positive alerts
- Have difficulty to prevent Advanced Persistent Threat (APT) that exploit zero-day vulnerabilities

Security asymmetry

- Continuous battle between hackers and cyber defenders
- Offense has the upper hand
  - Cyber defenders: must make sure everything is properly maintained and prevent intrusions at every single point
  - Hackers: Just take advantage of one vulnerability to breach the defense

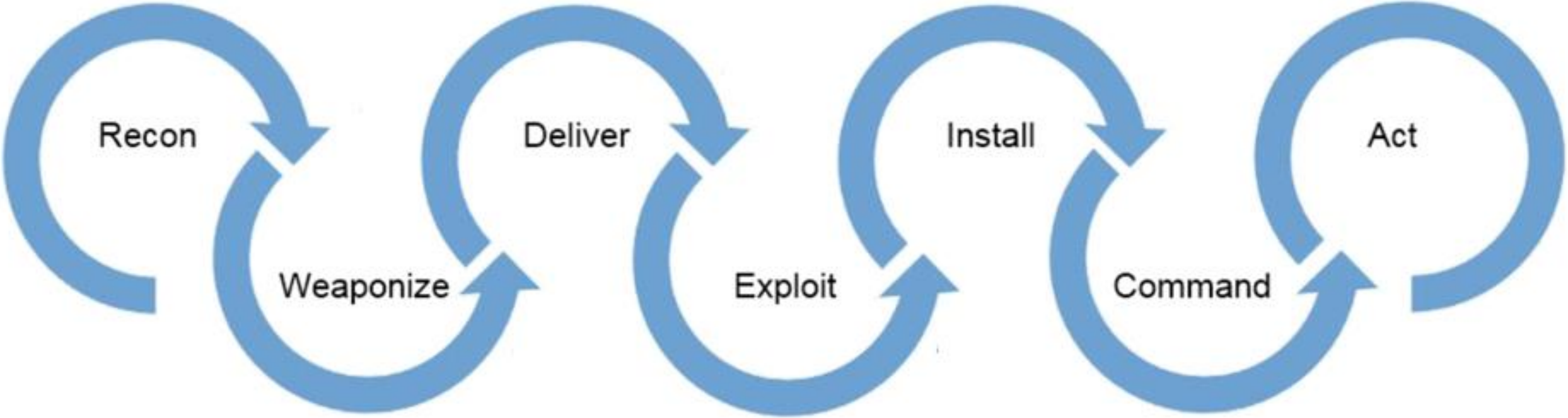


Defensive deception comes to rebalance this asymmetric disadvantage for cyber defenders

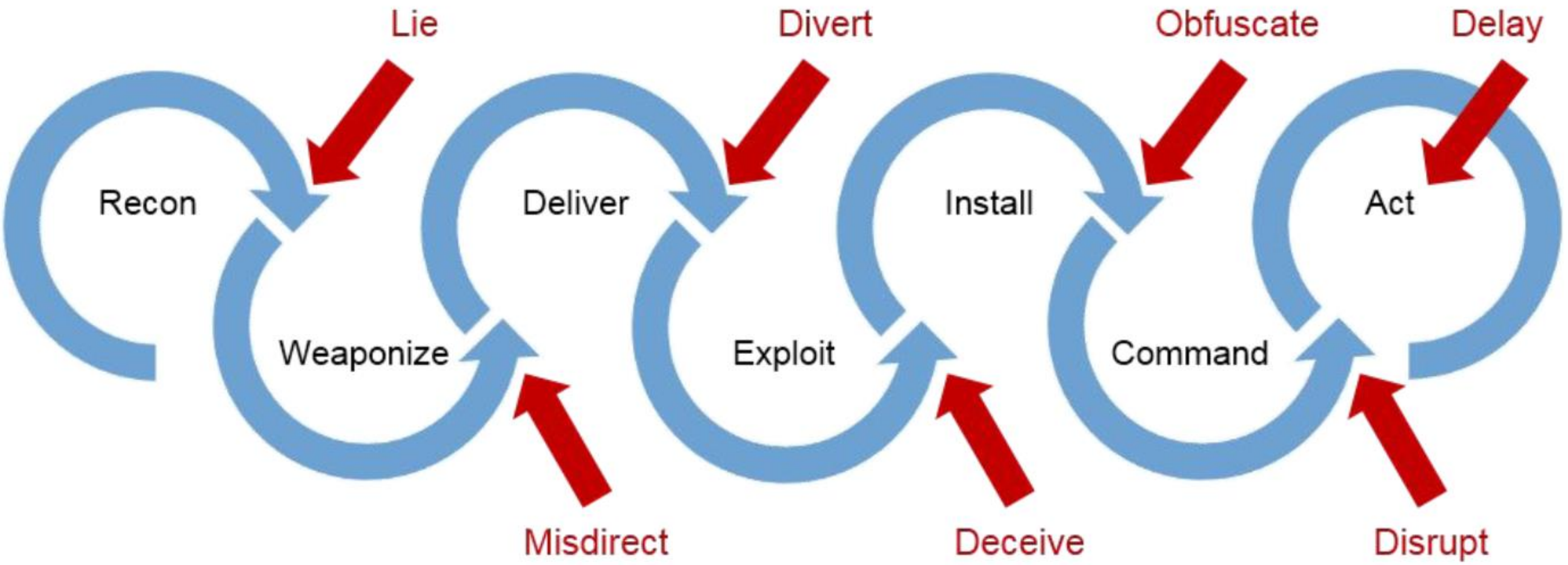
Active defense and cyber deception

- Active Defense
  - Use of limited offensive action and counterattacks to deny a contested area or position to the enemy
  - Proactive, anticipatory, and reactionary actions against attackers
- Cyber deception
  - Deceive attackers to provide a better defense
  - Confuse mislead, and deceive attackers by obfuscating the attack surface and hiding critical assets from attackers and confusing or misleading them
  - Slow down attacks, increase the costs of the adversary, and gather new threat intelligence for preventing similar attacks

Cyber kill Chain Model



Cyber kill Chain Model: Deception applied



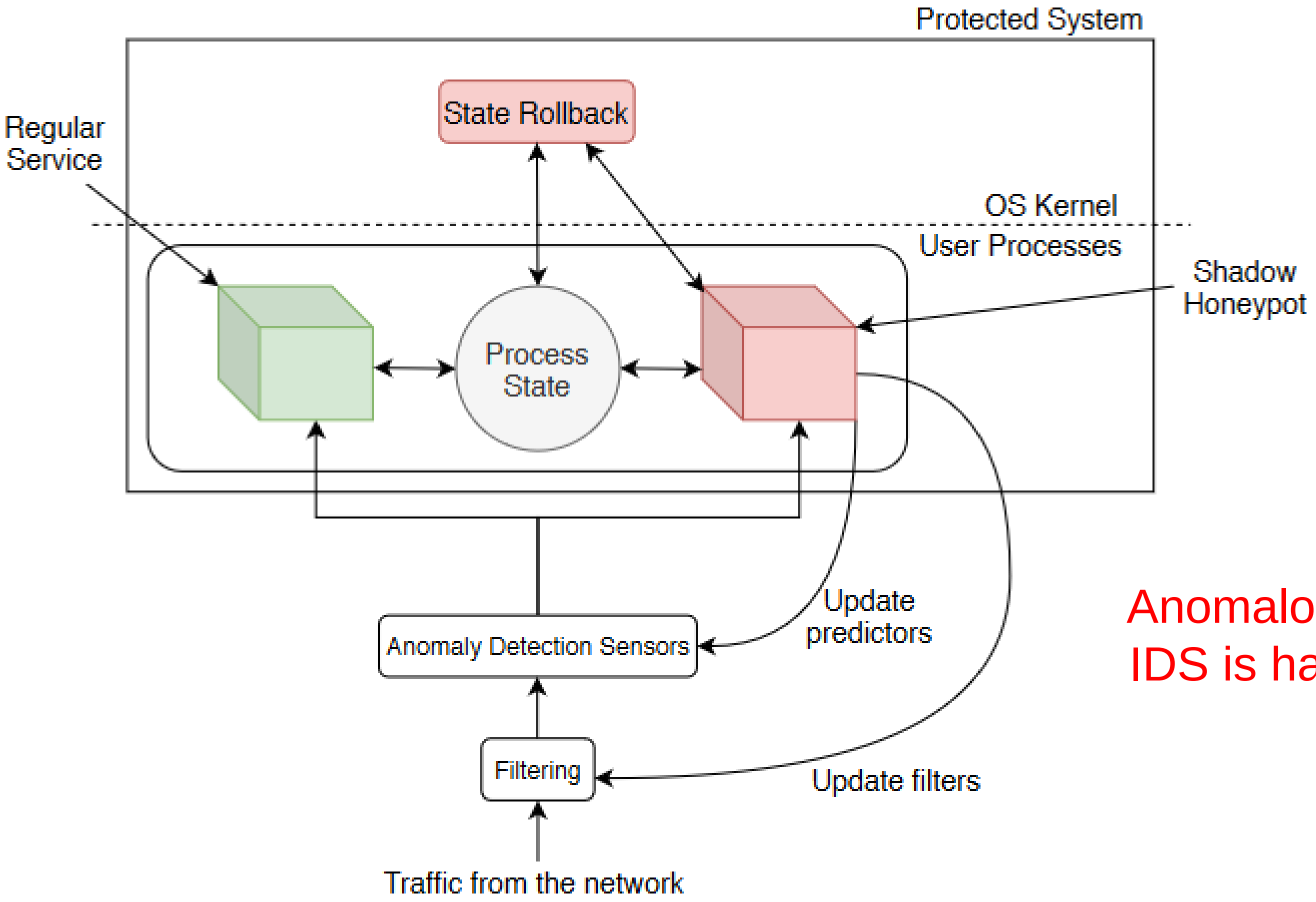
Deception using Honeypots

- Security resources whose value lies in being probed, attacked, or compromised
- Objective: intelligence gathering and risk mitigation
- Can be low interaction or high interaction; Real systems or virtual machines (VMs).

Common deployment

- Sacrificial Lamb
  - An isolated system that has no entry point to production systems
- Hacker Zoo
  - A subnet of honeypots isolated from production systems
- Minefield:
  - Several honeypots placed in forefront to serve as first attack targets
- Proximity Decoys
  - Honeypots deployed near production systems
- Redirection Shield
  - External honeypots that appear on production systems through port redirection

Example of shadow Honeypot architecture

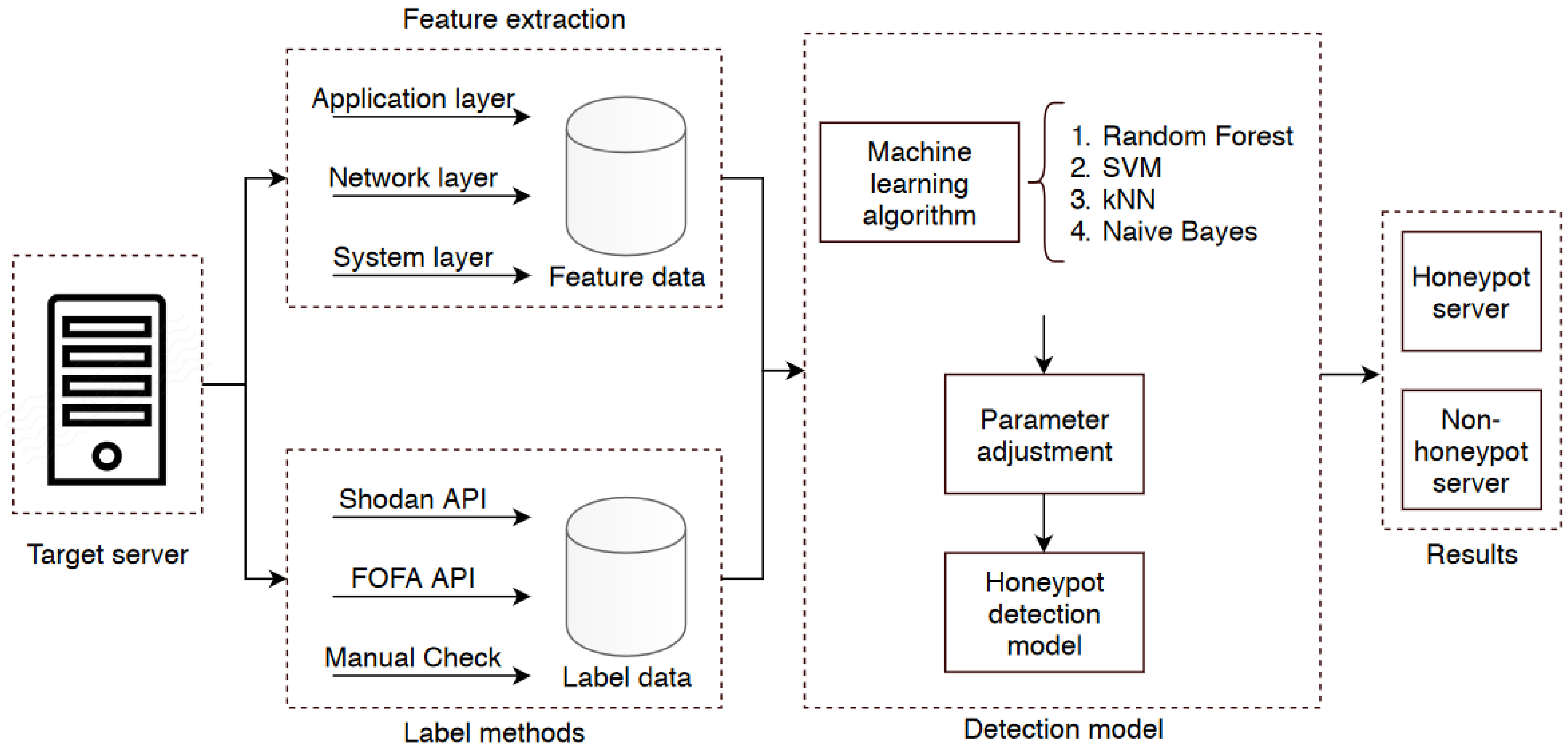


Anomalous traffic identified by IDS is handled by the shadow honeypot

Evading and detecting honeypots

- Attackers want to identify to Honeypots to circumvent them or keep the malicious payload dormant
- How to fingerprint them?
  - Check timing or behavior discrepancies in responding to bad packets
  - Examine responses to specially crafted packets
  - Check whether the compromised machine can successfully send out unmodified malicious traffic

Machine learning based Honeypot detection



Honeytokens

- Can be in the form of any digital entity and placed anywhere
- Simple to deploy and cost effective
- Trigger alerts whenever accessed or used
- The uncertainty of whether and where honeytokens are placed will slow down attackers and may even turn them away (i.e., the deterrent effect).
- Use of machine, deep and reinforcement learning models to optimize their deployment/redeployment

Honeytoken examples

- Bogus profiles on social networks to deceive attackers that generate phishing campaigns
- Decoy hyperlinks in webpages (invisible to humans but interpretable by programs)
- Deceptive response to OS fingerprints
- “booby trap” codes in protected software that sends deceptive responses to attacks
- Honeypatches on vulnerabilities so exploitation attempts are redirected to honeypots
- Decoy traffic with enticing information (credential, identities, ..)
- Extend role-based access control (RBAC) with decoy permissions
- Multiple fake passwords along with real password for each account
- Decoy database entries (e.g., TABLE CREDIT_CARDS or VIEW EMPLOYEES_SALARY)
- Decoy user/system files
- Watermarks in file content (to be detected when the file is loaded in memory or sent over the network anywhere)

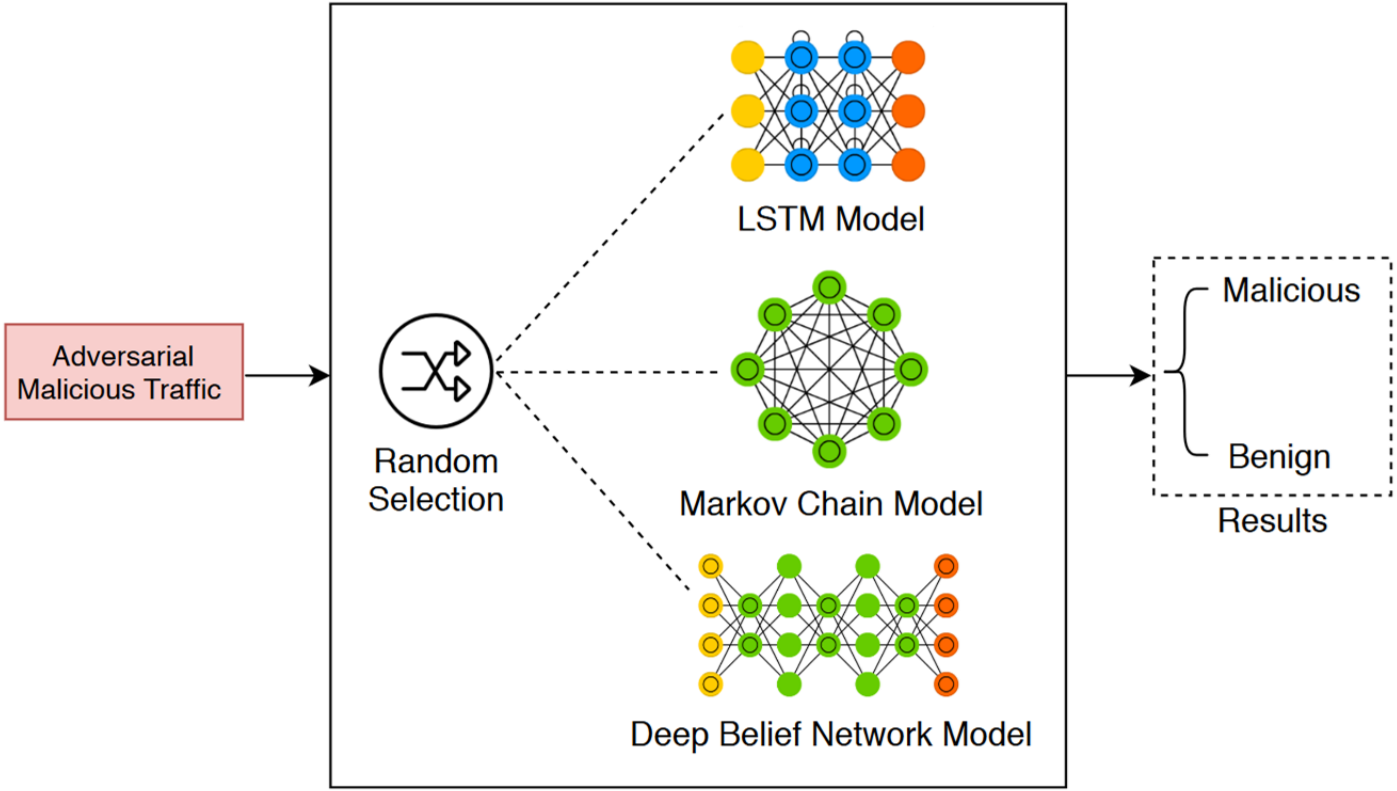
Moving Target defense

- Create a constantly evolving attack surface for the protected network to retain a resilient security posture
- Randomize network components to reduce the likelihood and lifetime of a successful attack, and limit the damage
- Force the attacker to spend more effort and time to study the system, locate and re-locate its vulnerabilities

Moving Target defense

- IP obfuscation by network address space randomization to prevent tracing hosts in the network by attackers
  - Short IP address leases by a modified DHCP server
  - OpenFlow Random IP Host Mutation
- OS obfuscation to defend against OS fingerprinting
  - SDN based method that randomizes TCP sequence numbers and payload patterns in TCP, UDP, and ICMP protocols
  - Dynamically and continuously changing IDS placement over time
  - Randomized classifier models to mitigate adversarial attacks that try to evade a know classification model (e.g., LSTM)

Randomized classifier

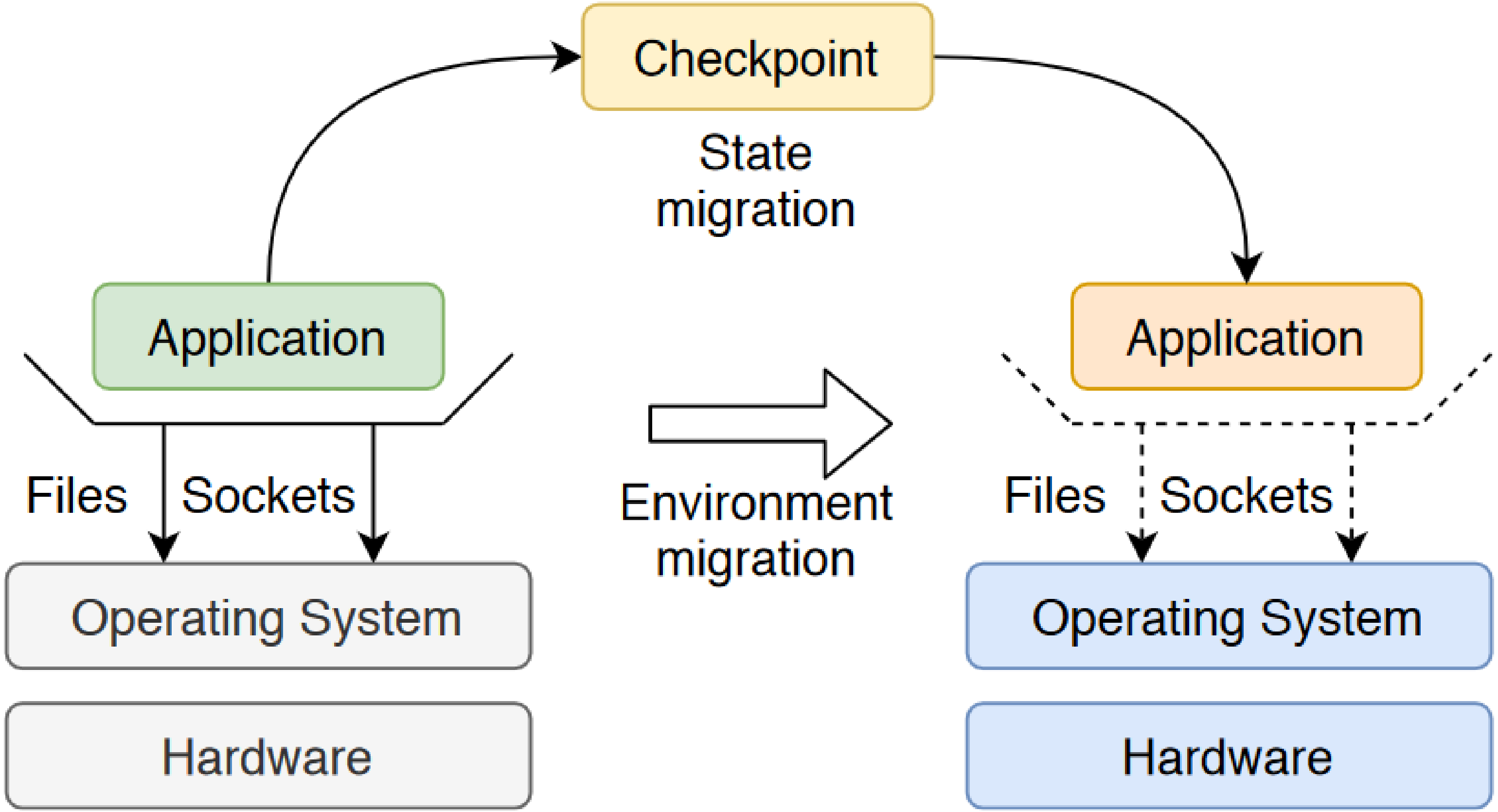


Randomized classifier models to mitigate adversarial attacks that try to evade a know classification model (e.g., LSTM)

Moving Target defense

- System Dynamic in memory address space to defend memory corruption and code injection vulnerabilities
  - Randomizing memory addresses of a loaded software
  - Randomizing software instructions sets when loaded into the memory
  - Rotating an application on a set of VM equipped with different OS that share the same database
- Software Dynamics to prevent exploiting application vulnerabilities
  - Divide a complex program into smaller tasks composed of executable variants that are functionally equivalent but with different quality attributes (e.g., performance, robustness). Executable variants are then shuffled when loading the program to change attack surface
  - Use SDN features to exchange each portion of datagrams on different routes between distributed software components in the network
  - Partition a secret key into randoms shares based on threshold cryptography, store them in different VMs, and regenerate them periodically to prevent key extraction from a VM in the cloud using cross-VM side-channel attacks.

MTD: Application migration on different VMs



Deception in depth for active defense

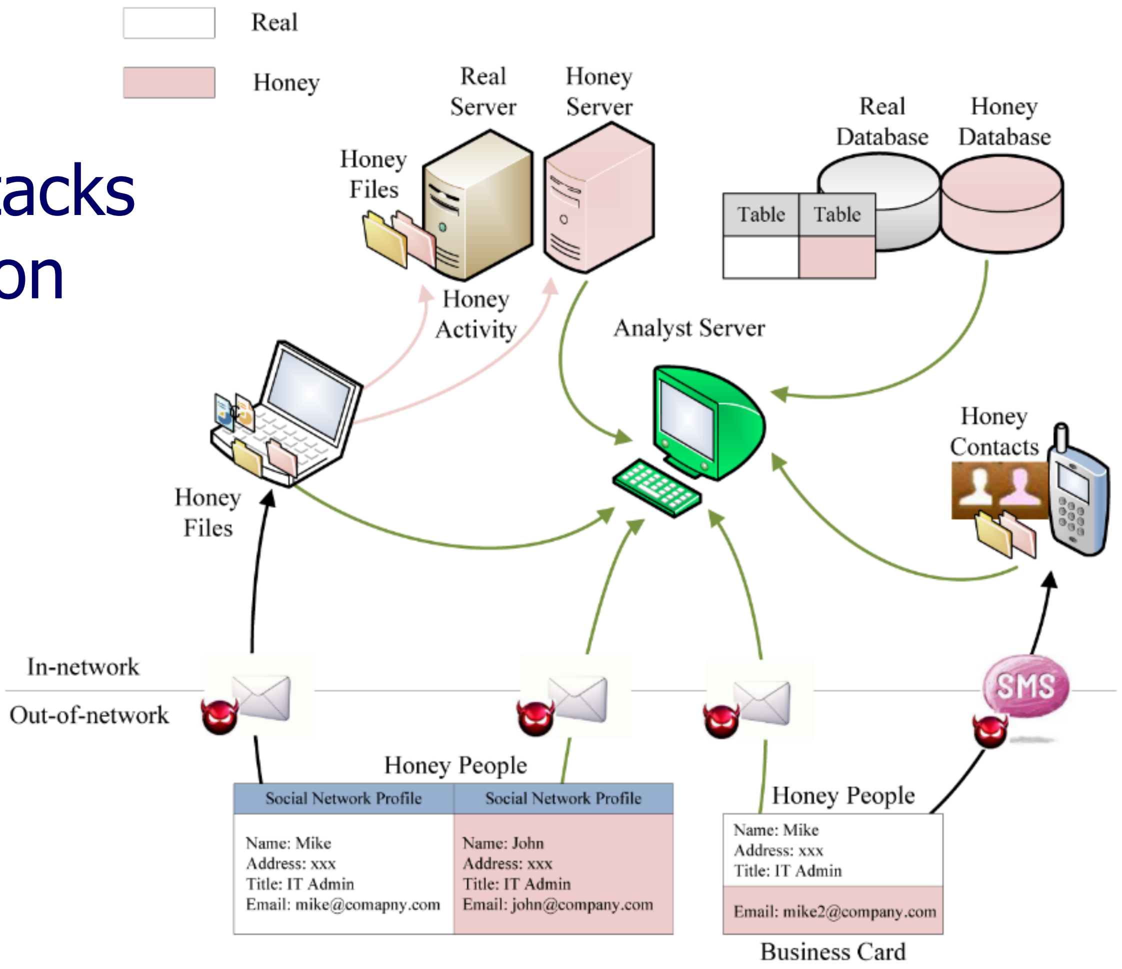
- When a deception technique is used alone, attackers can always find a way to circumvent it
- When multiple deception techniques that complement with each other are used together, a more resilient cyber defense posture can be established

➔ Deception in Depth

  - ➔ Cover several or even all layers (network, system, software, data) in the deception stack.
  - Achieve comprehensive defense against the onslaught of advanced adversaries and attack techniques

Detecting targeted attacks by multi-layer deception

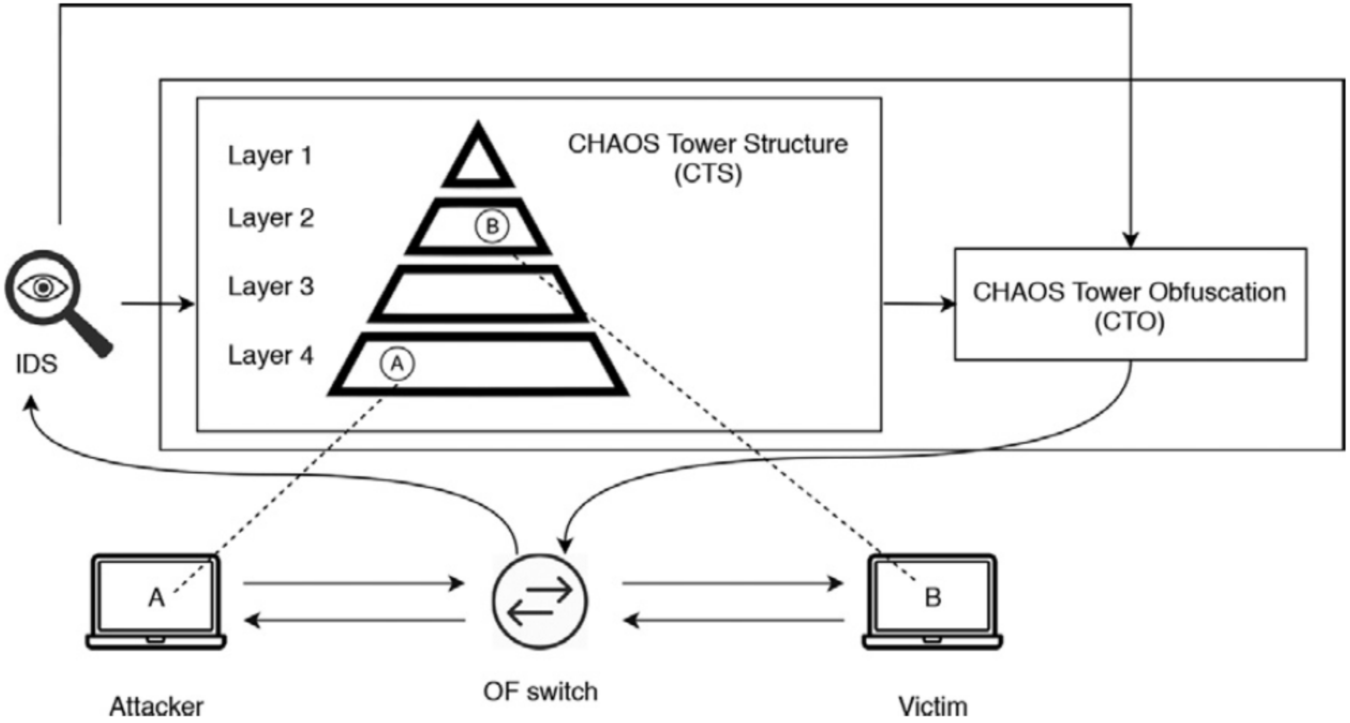
Alerts from deception entities are sent to the analyst server, where correlation and analysis are performed to confirm or re move the alerts



Social Network Profile	Social Network Profile
Name: Mike Address: xxx Title: IT Admin Email: mike@comapny.com	Name: John Address: xxx Title: IT Admin Email: john@company.com

Name: Mike
Address: xxx
Title: IT Admin
Email: mike2@company.com

SDN Based Moving Target Defense



- Machines in the network is divided into several layers according to their security levels
- Suspicious communications (determined by the CTS module or identified by IDS) will be forwarded to a CHAOS tower obfuscation (CTO) module
- Three types deception mechanisms (e.g., decoy servers, fake response to port scan, random host mutation) are implemented according to predefined strategies

Outlook and concluding remarks

- Compared to conventional prevention mechanisms which can only impede the adversary’s current actions, deception techniques may have long-term impact on the adversary.
- Thanks to virtualization and SDN technology, which simplifies and automates the tedious process, deception techniques become scalable in real-life networks.
- Deception techniques must be carefully maintained to stay effective over a long period
- The current trend is to provide *deception as a service* through automatically orchestrated deception deployment with minimal human involvement
- Artificial intelligence and game theory are being used to provide intelligent and strategic selection and deployment of deception mechanism, and a dynamic update of the hopping frequencies of MTD techniques
- The recent testbed and experimentation platforms will be an ideal environment for finding the optimal composition of different deception building blocks.

Thanks for your attention!

Questions