



Cyber-security Excellence Hub in Estonia and South Moravia

# The long road to autonomous security

Martin Drašar

drasar@ics.muni.cz

Funded by the European Union under Grant Agreement No. 101087529. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

#### **Driverless cars**

Driving

Hur South

0000000

0.

Ò

1

0

1

#### Art





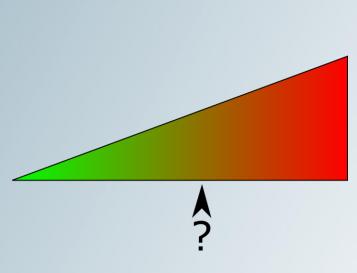


### **Chatbots that can pass Turing test**

	ow many times o the word "mayo		n" appear	0
8	The letter "n" a "mayonnaise".	appears 4 times		6
		Can you list eac r n appears in th		0
	positions in th 1. mayon <b>n</b> ai	e word 'mayonn ise	na - San Angelan an Ta	
	<ol> <li>2. mayonnai</li> <li>3. mayonnai</li> <li>4. mayonnai</li> </ol>	i <b>n</b> e		
A	口 Copy text C	P Retry	s S S	<u>۵</u>

#### So... how about security?







## What is the problem with security?

- Tesla: 250.000.000+ km of autonomous driving
- Stable diffusion: 160.000.000 images
- GPT-3: 45 TB of text data
- Security
  - Limited datasets
  - Dataset variability not even close to real world variability
  - Training environments not up to task

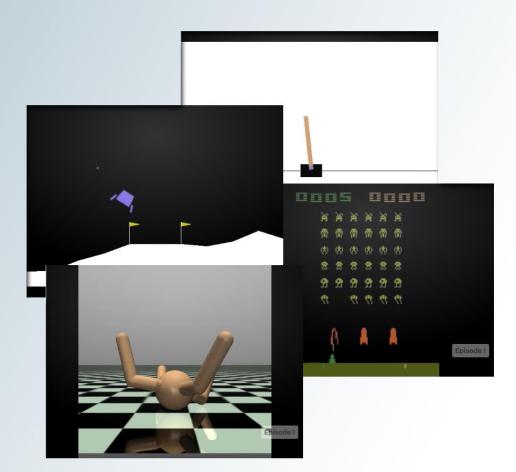


## Which training environment paradigm to choose?

- Simulation
- Emulation
- Virtualization
- Hybrid

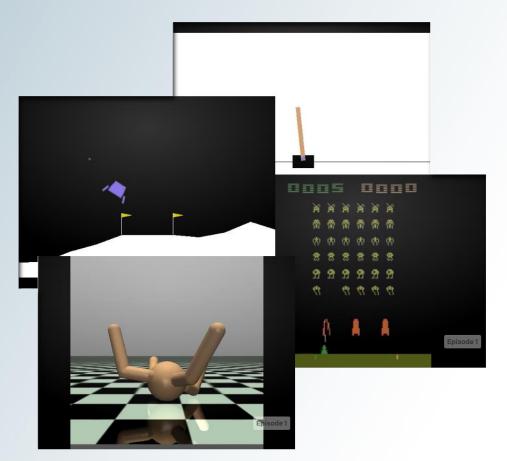
### **Quiz time!**

- What do you see?
- Why am I showing it?



#### **Simulation environments**

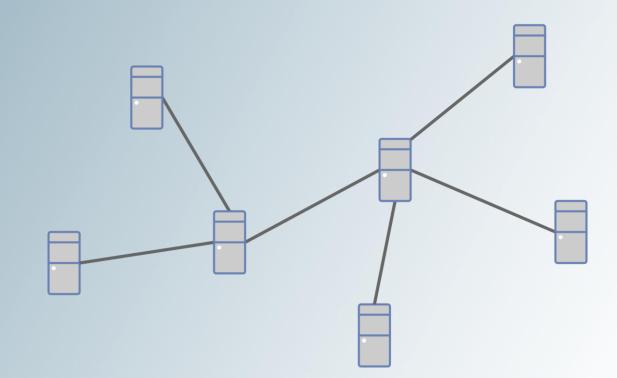
- Simple abstract problems
- Do not reflect domain complexity
- Static
- General simulation problems:
  - Data reliance
  - Specialization
  - High-level of abstraction
  - Simulation of new threats
  - Too defense-centric

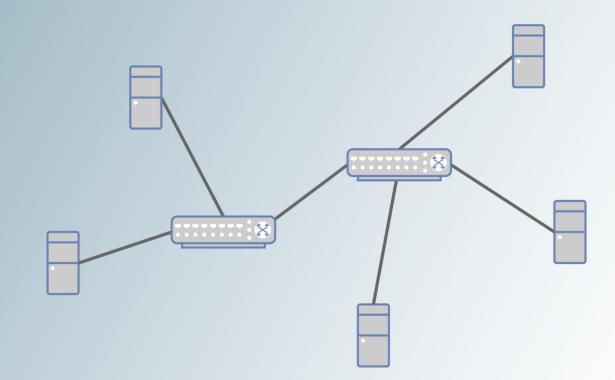


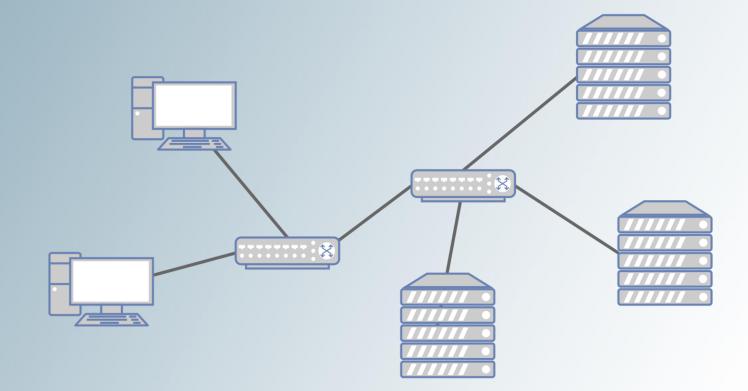


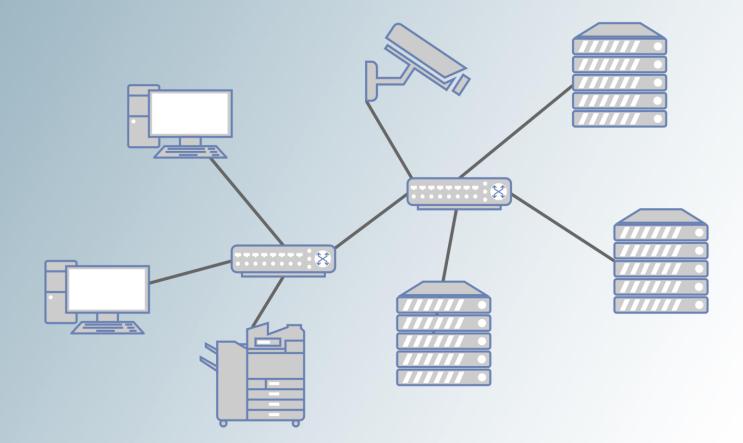
#### **Simulation creation – deep dive**

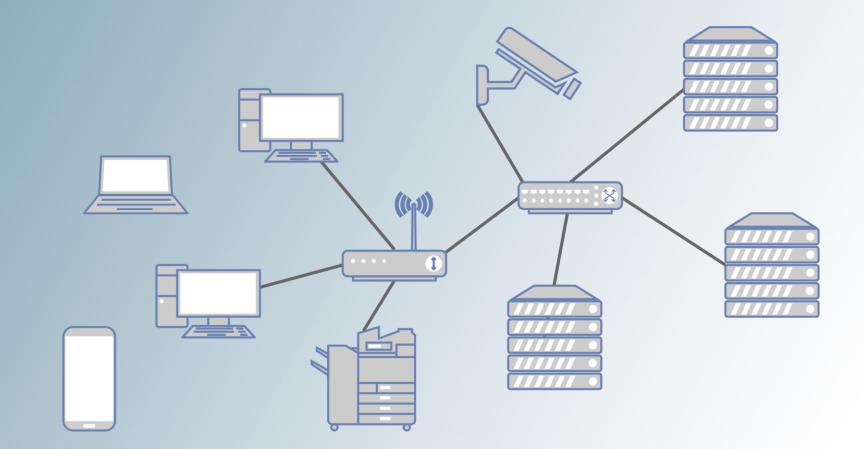
- Choose your modelling approach.
  - Discrete-event simulation, Markov processes, game theory, ...
- Choose your abstraction.

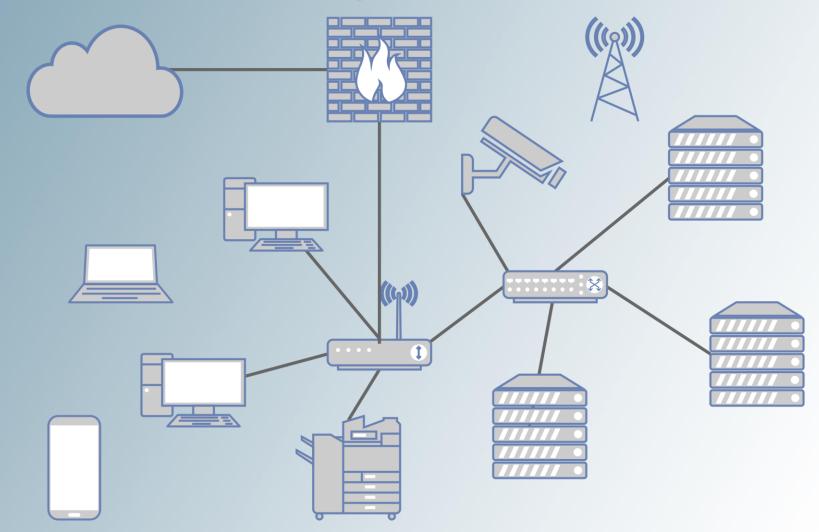












## **Host modelling**

- Type
- Purpose
- Operating system
- Services
- Files
- Memory
- Buses
- Extensions

## **Connections modelling**

- Medium (air/wire/optical/...)
- Properties (bandwidth, jitter, drops, ...)
- Protocols (abstract/concrete)

## **User modelling**

- Existence
- Identities
- Active or passive
- Traffic generation
- Activity cycles

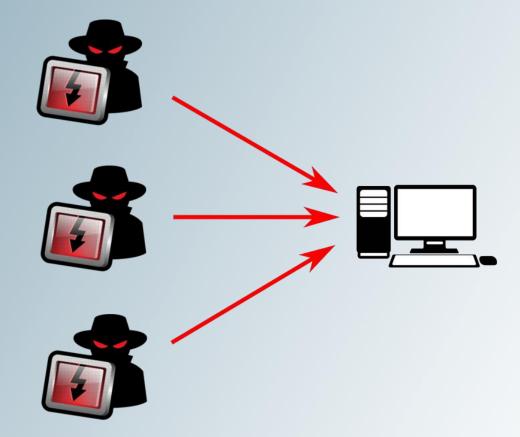
#### **Hundreds of considerations**

- Authentication and authorization, data handling, threats, vulnerabilities, exploits, failures, dynamics, ...
- Still only the passive side
- The active side must be decided as well ...

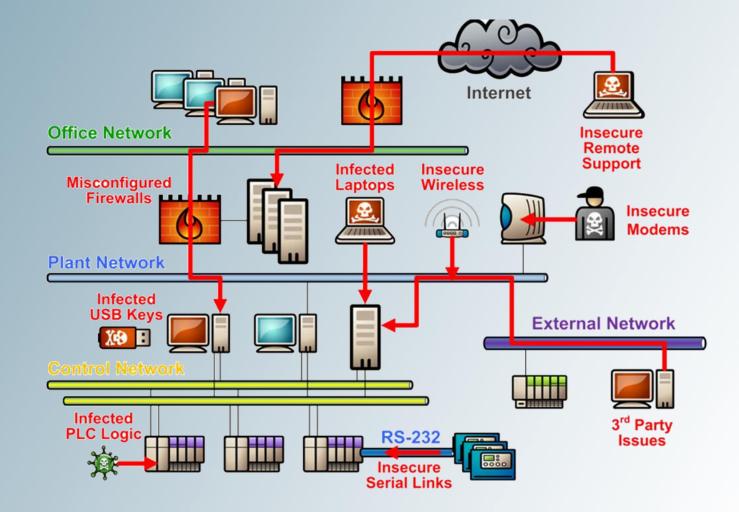
#### **Attack modelling**



#### **Attack modelling**



#### **Attack modelling**



#### **Actions and behavior**

- Actions and resulting behavior depend on the simulation model
- Action must be expressible within the model
- Abstract actions?
- Attack and defense taxonomies?
- Own approach?

Reconnaissance 10 techniques	Resource Development 7 techniques	t Initial Access 9 techniques	Execution 12 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 39 techniques	Credential Access 15 techniques	Discovery 27 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exchitration 9 techniques	Impact 13 technique
Active Scenning @	Acquire Infrastructure (p)	Drive-by Compromise	Command and Scripting	Account Manipulation (a)	Abuse Elevation Control	Abuse Elevation Control	Brute Force (a)	Account Discovery (a)	Exploitation of Remote	Archive Collected Date of	Application Layer	Automated Exfitration ro	Account Access Remo
Gather Victim Host Information (a)	Comptamise Accounts m	Exploit Public-Facing	Interpreter (2)	BITS Jobs	Mechanism (4)	Mechanism (4)	Dredentials from	Application Window Discovery	Services	Audio Capture	Protocol (4)	Deta Transfer Size Limits	Data Destruction
Gather Victim Identity	Compromise	Application	Container Administration Command	Boot or Logon Autostart	Access Tokes Manipulation (a	Access Token Manipulation (p)	Pessword Stores (g	Browser Bookmark Discovery	Internal Speerphishing	Automated Collection	Communication Through Removable Media	Exhibition Over	Data Encrypted for Imp
Information (3)	Infrastructure (2)	External Remote Services	Deploy Container	Execution (14)	Boot or Logion Autostart	BITS Jobs	Exploitation for Dredential Access	Cloud Infrastructure Discovery	Lateral Tool Transfer	Cipboard Data	Deta Encoding (p)	Alternative Protocol (3)	Data Manipulation
Gather Victim Network	Develop Capabilities (4)	Hardware Additions	Exploitation for Client	Boot or Logon Initialization Scripts (p)	Execution (14)	Build Image on Host	Forced Authentication	Cloud Service Dashboard	Remote Service Session Hijaching (2)	Data from Cloud Storage	Data Obfuscation (2)	Exfitration Over C2 Channel	Defacement co
Gather Victim Org Information (2)	Establish Accounts (2)	Phishing (2)	Execution	Browner Extensions	Bost or Logon Initialization Scripts of	Deobfuscate/Decode Files or Information	Forge Web Credentials (7)	Cloud Service Discovery	Remote Services on	Object.	Dynamic Resolution on	Exfituation Over Other	Disk Wps.m
Phishing for Information (2)	Obtain Capabilities (II	Replication Through Removable Media	Inter-Process Communication (s)	Compromise Client	Create or Modify System	Deploy Container	Input Capture (c)	Container and Resource Discovery	Replication Through	Data from Configuration Repository (2)	Encrypted Channel (2)	Network Medium (1)	Endpoint Denial of Se
	Stage Capabilities (5)		Nature API	Software Binary	Process ja				Removable Media			Extituation Over Physical	
Search Closed Sources (2)		Supply Chain Compromise (t)		Create Account (0)	Bornain Policy	Direct Volume Access	Manin-the-Middle 😄	Domein Trust Discovery	Software Deployment	Data from Information Repositories (0)	Failback Channels	Medium (1)	Firmwate Consption
Search Open Technical Databases (s)		Trusted Relationship	Scheduled Task/Job (7)	Create or Modify System	Mod fication (z)	Domain Policy Modification (2)	Modily Authentication Process (4)	File and Directory Discovery	Tools	Data from Local System	Ingress Tool Trensfer	Exfituation Over Web Service (2)	Inhibit System Recov
Search Open		Valid Accounts in	Shared Modules	Process (4	Escepe to Host	Execution Guardralia (7)	Natestrk Shiffing	Network Service Scanning	Taint Shared Content	Data from Network Shared	Multi-Stage Chennels	Scheduled Transfer	Network Denial of Se
Websites/Domains (3)		-	Software Deployment Tools	Event Triggered Execution cts	Event Triggered Execution cost	Exploitation for Defense Evasion	OS Credential Dumping (g)	Network Share Discovery	Use Atemate Authentication Material (4)	Drive	Non-Application Layer Protocol	Transfer Data to Cloud	Resource Hjacking
Search Victim-Dwned Websites			System Services (2)	External Remote Services	Exploitation for Privilege	File and Directory Permissions Modification	Basi Application Access	Network Sniffing		Date from Removable Media	Non-Standard Port	Account	Service Stop
			User Elecution (2)	Hinck Execution Flow and	Escalation	Hide Artifecta m	Tokan	Password Policy Discovery		Data Staged (2)	Protocol Tunneling		System Shutdown/R
			Windows Management	Implant Internal Image	Hijsck Execution Flow (11)	Hiack Execution Flow	Steal or Forge Kerberoe	Peripheral Device Discovery		Email Collection			
			menumentation	and the second sec	Process Injection (17)	a second s	Tickets (4	Permission Groups Discovery (2)		and the second se	Pravy (4)		
				Modify Authentication Process up	Scheduled Task/Job (7)	Impair Defenses (7)	Steal Web Session Cookie	Process Discovery		Input Capture (4)	Remote Access Software		
				Office Application	Valid Accounts (4)	Indicator Removal on Host (K)	Two-Factor Authentication Interception	Query Registry		Man in the Browser	Traffic Signaling (1)		
				Startup (s)		Indirect Command Execution	Unsecured Oredentials on	Remote System Discovery		Men in the Middle (2)	Neb Service (3)		
				Pre-QS Boot (8)		Masquarading (0)	1	Software Discovery m	8	Szreen Capture			
				Scheduled Task/Job (7)		Modify Authentication Process (4)		System Information Discovery		Video Cepture			
				Server Software Component of		Modify Cloud Compute Infrastructure (a)		System Location Discovery					
				Traffic Signaling (1)		Modify Registry		System Network Corrigutation					
				Valid Accounts (a)		Modify System Image (2)		Discovery (1)					
				Tano Postoana (g			-#	System Network Connections					
						Network Boundary Bridging (1)		Discovery					
						Obfuscated Files or Information (		System Owner/User Discovery					
						Pre-OS Boot (1)	-	System Service Discovery					
						Process Injection (11)	1	System Time Discovery					
						Rogue Domein Controller		Vintualization/Sandbox Evasion (2)					
						Rootket	-						
						Signed Binary Proxy Execution (11)							
						Signed Script Proxy Execution (1)							
						Subvert Trust Controls (0)							
						Template Injection							
						Traffic Signaling (1)							
						Trusted Developer Utilities Proxy	1						
						Execution (1)	M						
						Unused/Unsupported Cloud Regions							
						Use Alternate Authentication Material (4)							
						Valid Accounts (a)							
						Virtualization/Sandbox Evenion op	-						
						Weeken Encryption (2)	-11						
						XSL Script Processing							
						vor orabi magnesid							

DEFENSE

#### Attack ——

		Detect						Isolate		Deceive		Evict				
Application Hardening	Credential Hardening	Message Hardening	Platform Hardening	File Analysis	ldentifier Analysis	Message Analysis	Network Traffic Analysis	Platform Monitoring	Process Analysis	User Behavior Analysis	Execution Isolation	Network Isolation	Decoy Environment	Decoy Object	Credential Eviction	Process Eviction
Dead Code (1) Elimination	Certificate <sup>(2)</sup> Pinning	Message (2) Authentication	Disk Encryption	Dynamic Analysis	Homoglyph Detection	Sender () MTA Reputation	3 Administrative Network Activity	Firmware Verification	Database <sup>(1)</sup> Query String Analysis	Authentication Event Thresholding	() Hardware- based Process	Broadcast Domain Isolation	Honeynet	Decoy (*) File	Account Cocking	Process (2) Termination
Elimination Exception ①	Multi-factor Automation Multi-factor Automation One-Inne O Password Palacy	Authentiquion Message © Encryption Transfer Authentication		Analysis Emulated File Analysis File Content Rules File Hashing	Honegypti Beetolin URL Ö	MTA	Network	Verification Operating <sup>O</sup> Monitoring Interview Anatysis Lecourt Mentoring Memory Memory Tracking Soundary Tracking Soun	Query String	Event	based	Domain	Honeynet Inlegstad Inlegstad Standaone Honeynet	Decry © Resource Resource Persona Public Decry © Public Researce Resource R		<u>Termadon</u>

#### **CYST: One combination of all possible parameters**

- Discrete event simulator with message passing
- Hybrid stochastic simulation
- Hosts modelled as a collection of running processes
- One type of connection with extensible properties
- Users under construction
- Complex authentication/authorization framework
- Declarative vulnerabilities mapping to CVE and others
- Exploits tied to vulnerabilities, integration of Metasploit capabilities
- Pluggable behavioral models

### **CYST: Functional requirements**

- Simulation of multi-agent cybersecurity scenarios
- Integration with ML toolkits
- Integration and comparison of different behavioral models
- Fast prototyping of attack and defense strategies
- Integration of simulation and emulation (IDS or human in the loop)
- Deployment from simulation to emulation

#### CYST

- Get it, try it, break it!
- https://dl.acm.org/doi/abs/10.5555/3451906.3451908
- CODE: <a href="https://pypi.org/project/cyst-core/">https://pypi.org/project/cyst-core/</a>
- DOCS: <a href="https://muni.cz/go/cyst">https://muni.cz/go/cyst</a>

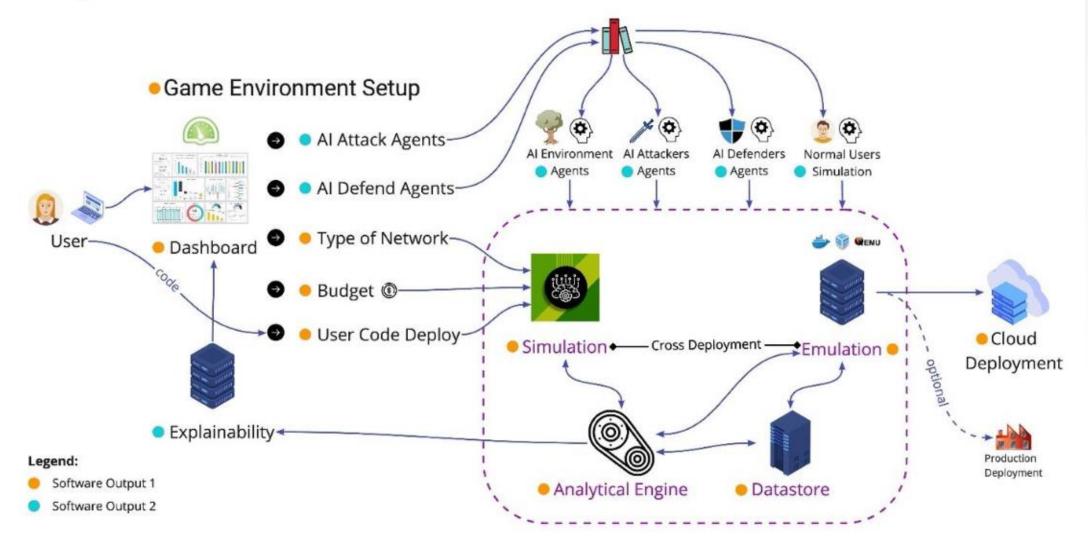
### **CYST – roadmap**

- Parametrized generation of realistic cybersecurity scenarios
- Transformation of simulation artifacts into datasets of network traces
  - https://github.com/Trace-Share
- Multiple behavioral models
- Visualization
- Support for stealthy actions
- Support for multi-agent collaboration and communication
- Parallel training of attackers and defenders
- Transfer from simulation to emulation to the real world
  - <u>https://beast-public.gitlab-pages.ics.muni.cz/cryton/cryton-documentation/</u>

#### That's too low level. Wake me up when it

- can be easily deployed in cloud,
- can create realistic simulated and emulated scenarios,
- allows me to train with or against autonomous agents,
- provides visual analytics,
- has one big green button to run everything.

#### Al-Dojo Software Architecture



#### **Autonomous security**

Either wait a few years

Or

Do it yourself...