IARPA ReSCIND
IBM Capabilities

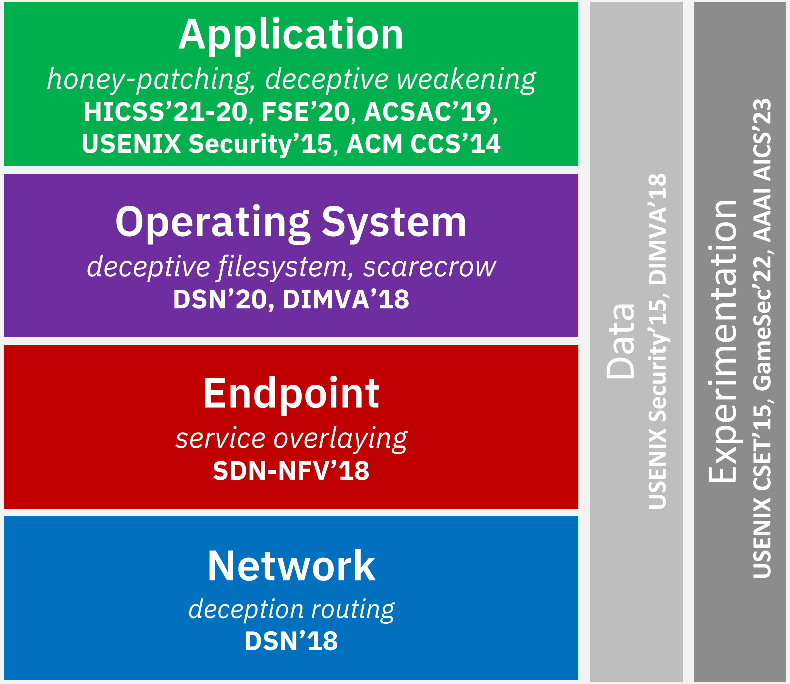
Fred Araujo, **Teryl** Taylor

Research

Cyberdeception Research at IBM

Embedded threat sensory and attacker engagement

Capabilities: language-based and systems security, compilers, program analysis, operating systems, access control, container/cloud technologies, machine learning, CTF, security gamification



Application

honey-patching, deceptive weakening

HICSS'21-20, FSE'20, ACSAC'19, USENIX Security'15, ACM CCS'14

Operating System

deceptive filesystem, scarecrow

DSN'20, DIMVA'18

Endpoint

service overlaying

SDN-NFV'18

Network

deception routing

DSN'18

Data

USENIX Security'15, DIMVA'18

Experimentation

USENIX CSET'15, GameSec'22, AAAI AICS'23

Technical approach

- Embed deceptions along production attack paths for increased threat visibility and high-fidelity attack signals
  - Application, middleware, operating systems, ...
  - Cf. conventional honeypots and honeynets
- Conceal high-value data and resources
- Explore attack biases to “crook source” attacker intelligence

Human-subject experimentation

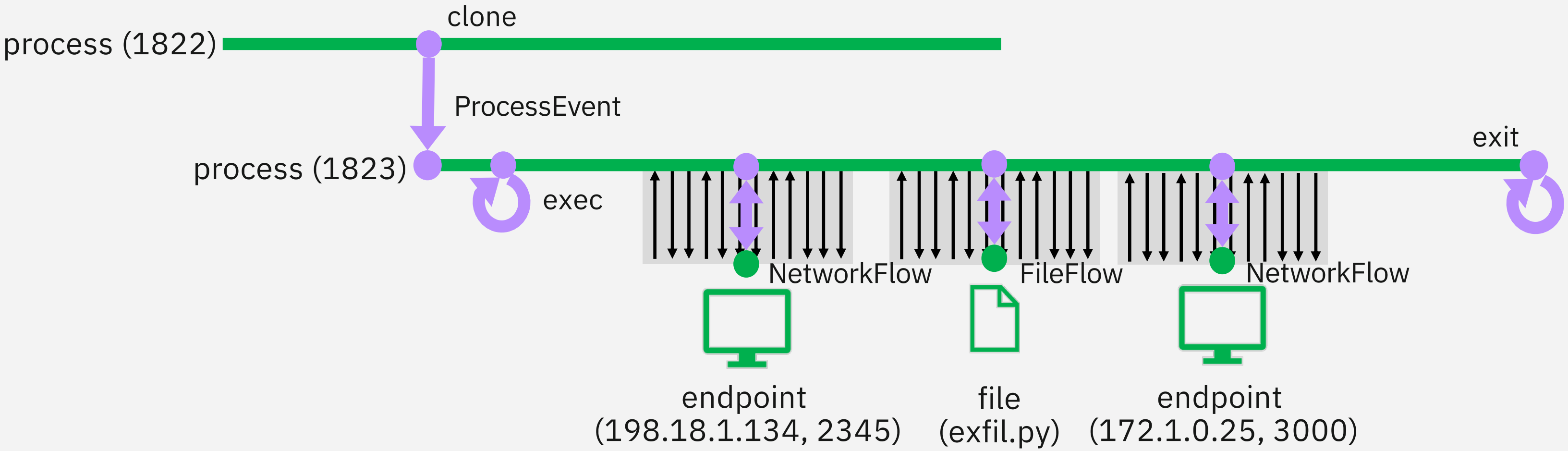
- Identify real-world adversarial threats
- Measure advantages of deploying deception strategies
  - Attack-defense CTFs
- Model human attacker behaviors
  - Role of game-theoretic decision models

Endpoint Observability Research at IBM

Relational observability

Capabilities: operating systems, eBPF, cloud-native computing, intrusion detection, rules engines, threat intelligence, graph analytics and representation learning, self-supervised learning

Semantically compressed system events for scalable **security monitoring** and **behavioral modeling**.

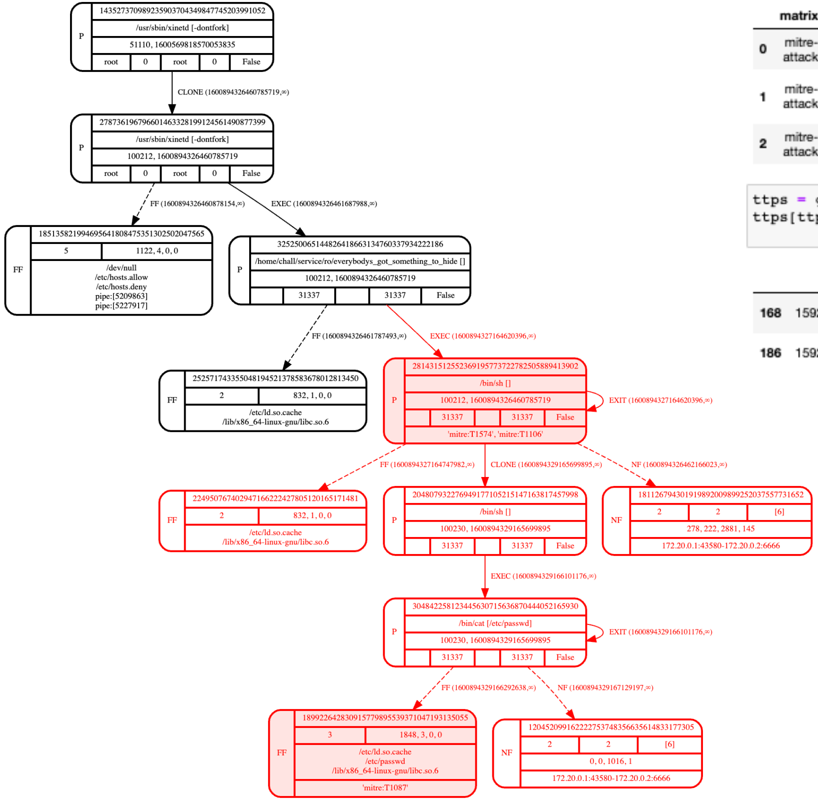


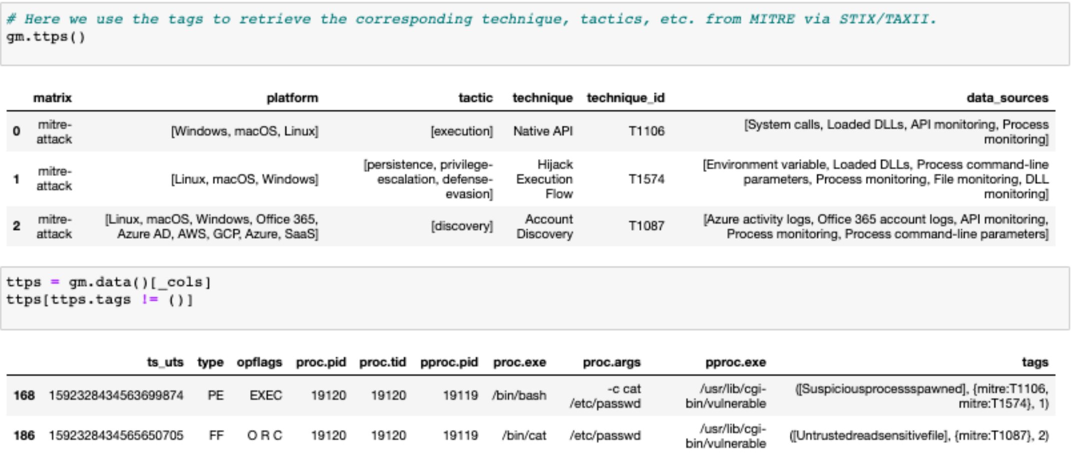
It’s open source!

sysflow.io | https://github.com/sysflow-telemetry

IEEE Big Data’20, FloCon’20-22, BlackHat Europe’21, AvengerCon’22

Provenance Tracking





```
# Here we use the tags to retrieve the corresponding technique, tactics, etc. from MITRE via STIX/TAXII.
gm.ttps()
```

	matrix	platform	tactic	technique	technique_id	data_sources
0	mitre-attack	[Windows, macOS, Linux]	[execution]	Native API	T1106	[System calls, Loaded DLLs, API monitoring, Process monitoring]
1	mitre-attack	[Linux, macOS, Windows]	[persistence, privilege-escalation, defense-evasion]	Hijack Execution Flow	T1574	[Environment variable, Loaded DLLs, Process command-line parameters, Process monitoring, File monitoring, DLL monitoring]
2	mitre-attack	[Linux, macOS, Windows, Office 365, Azure AD, AWS, GCP, Azure, SaaS]	[discovery]	Account Discovery	T1087	[Azure activity logs, Office 365 account logs, API monitoring, Process monitoring, Process command-line parameters]

```
ttps = gm.data()[_cols]
ttps[ttps.tags != ()]
```

	ts_uts	type	opflags	proc.pid	proc.tid	pproc.pid	proc.exe	proc.args	pproc.exe	tags
168	1592328434563699874	PE	EXEC	19120	19120	19119	/bin/bash	-c cat /etc/passwd	/usr/lib/cgi-bin/vulnerable	([Suspiciousprocessspawned], {mitre:T1106, mitre:T1574}, 1)
186	1592328434565650705	FF	O R C	19120	19120	19119	/bin/cat	/etc/passwd	/usr/lib/cgi-bin/vulnerable	([Untrustedreadsensitivefile], {mitre:T1087}, 2)

- Semantic system telemetry representation
  - Context, built-in provenance
  - Facilitates attacker modeling
- Automated MITRE TTP tagging
- Attack kill chain interpretation

Cyberpsychology-Informed Defenses

Model attacker limitations and cognitive biases

- Cyberdeception- and agility-based defense capabilities built into all layers of the IT stack
- Human-subject experimentation in controlled attack-defense scenarios

Understand, measure, and induce changes in cyber attack behavior

- Relational observability for cyber attack modeling and profiling
- Learning-based approaches based on observable security signals

Automate defensive cyber maneuvers based on observed cyber attack behavior

- Automated labeling and mapping of attacker TTPs to defensive cyber maneuvers
- Transparent injection of software, filesystem, and network deceptions into production networks

Thank you

—

Fred Araujo
frederico.araujo@ibm.com

Teryl Taylor
terylt@ibm.com

© Copyright IBM Corporation 2023. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represent only goals and objectives. IBM, the IBM logo, and ibm.com are trademarks of IBM Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available at Copyright and trademark information.