

Malcolm

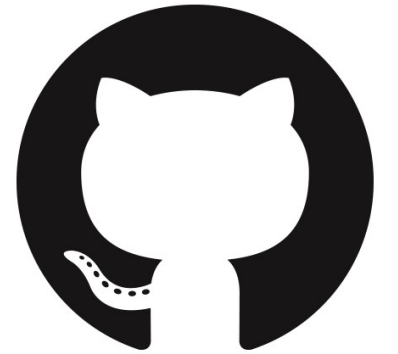


OT Protocol Support

Seth Grover, Malcolm developer • Cybersecurity R&D • Idaho National Lab

General Malcolm Information

- CISA Malcolm Documentation and Source Code
 - <https://github.com/cisagov/Malcolm>
 - Slides in `./Malcolm/docs/slides/`
- Malcolm Network Traffic Analysis Tool Suite YouTube channel
 - <https://www.youtube.com/c/MalcolmNetworkTrafficAnalysisToolSuite>
 - See “Network Traffic Analysis with Malcolm” and “Malcolm Exercises” tutorial videos
 - Videos detailing installation and configuration



Zeek OT Protocol Parser Sources



- ICSNPP - In-house development at INL for CISA
 - <https://github.com/cisagov/icsnpp>
- Amazon – Open-source plugins
 - <https://github.com/amzn?q=zeek>
 - Mostly replaced by ICSNPP at this point
- Zeek - Built-in support
 - Modbus and DNP3 (heavily augmented by ICSNPP)

OT Protocols in Malcolm

- Building Automation and Control (BACnet)
 - HVAC, lighting, access control, fire detection systems, etc.
- Bristol Standard Asynchronous Protocol (BSAP)
 - General use protocol, often used in water, power, chemical, oil and natural gas, communications, etc.
- Distributed Network Protocol 3 (DNP3)
 - Process automation systems mainly in power and water industries

OT Protocols in Malcolm (continued)

- EtherCAT
 - General use protocol, often seen in robotics, machine controls, power plants, wind turbines, manufacturing, etc.
- EtherNet/IP / Common Industrial Protocol (CIP)
 - General use protocol, widely used in many industries including manufacturing, pipeline, processing plants, water/wastewater treatment, etc.
- Modbus
 - General use protocol, de-facto standard for many industrial applications

OT Protocols in Malcolm (continued)

- MQ Telemetry Transport (MQTT)
 - Publish/subscribe messaging used in IoT, automotive, logistics, manufacturing, smart home, oil and gas, transportation, etc.
- Open Platform Communications Unified Architecture (OPC UA) Binary
 - Used in industrial automation for data exchange between sensors and cloud applications
- Process Field Net (PROFINET)
 - General use protocol seen in many industrial applications

OT Protocols in Malcolm (continued)

- S7comm / Connection Oriented Transport Protocol (COTP)
 - Proprietary protocol used by Siemens PLCs, widely used in power, pipeline, water/wastewater, and more
- Tabular Data Stream (TDS)
 - Protocol used by Microsoft SQL servers and many data historians

OT Protocols in Malcolm – Coming Soon

- Genisys (nearing release)
 - Somewhat obscure protocol used in the railway industry for control of signaling systems and interlockings
- S7comm Plus (nearing release)
 - Next generation of Siemens' proprietary protocol
- PROFINET/IO Context Manager (in development)
 - Manages communication between programmable controllers and IO-supervisors

"Best Guess" Fingerprinting for ICS Protocols

- Uses simple transport protocol, port and MAC address matching to identify potential ICS traffic for protocols without parser support
- Categorized in the ICS Best Guess dashboard
- Use as a pivot point to identify devices or investigate packet payloads in Arkime or Wireshark
- Higher potential for false positives

Data Tagging and Enrichment



- Logstash enriches Zeek log data
 - MAC addresses to hardware vendor/manufacturer
 - GeoIP and ASN lookups
 - Internal/external traffic based on IP ranges
 - Reverse DNS lookups
 - DNS query and hostname entropy analysis
 - Connection fingerprinting (JA3 for TLS, HASSH for SSH, Community ID for flows)
- `tags` field
 - Populated for both Arkime sessions and Zeek logs with tags provided on upload and words extracted from PCAP filenames
 - `internal_source`,
`internal_destination`,
`external_source`,
`external_destination`,
`cross_segment`



- Front end for Zeek logs
- Prebuilt visualizations for all Malcolm-supported protocols
 - General dashboards for high-level views and beginning investigation
 - Protocol-specific dashboards for IT and OT protocols
- Drill down from high-level trends to specific items of interest

Malcolm

Dashboard / Security Overview

Zeek Logs

General

[Overview](#)
[Security Overview](#)
[ICS/IoT Security Overview](#)
[Severity](#)
[Connections](#)
[Actions and Results](#)
[Files](#)
[Executables](#)
[Software](#)
[Notices](#)
[Weird](#)
[Signatures](#)
[Intel Feeds](#)
[Arkime](#)

Common Protocols

DCE/RPC ● DHCP ● DNS ● FTP / TFTP ●
HTTP ● IRC ● Kerberos ● LDAP ● MQTT
● MySQL ● NTLM ● NTP ● OSPF ●
QUIC ● RADIUS ● RDP ● RFB ● SIP ●
SMB ● SMTP ● SNMP ● SSH ● SSL /
X.509 Certificates ● STUN ● Syslog ●
TDS / TDS RPC / TDS SQL ● Telnet / rlogin
/ rsh ● Tunnels

ICS/IoT Protocols

Notices by Category

Notice Category	Count
SSL::Invalid_Server_Cert	50
ATTACK::Execution	27
ATTACK::Lateral_Movement	6
EternalSafety::EternalSynergy	5
ATTACK::Lateral_Movement_Multiple_Attempts	4
Signatures::Sensitive_Signature	4
ATTACK::Lateral_Movement_Extracted_File	2
EternalSafety::EternalChampion	2
EternalSafety::ViolationNtRename	2
EternalSafety::ViolationTx2Cmd	2
ATTACK::Discovery	1
EternalSafety::DoublePulsar	1
FTP::Bruteforcing	1
Ripple20::Treck_TCP_observed	1

Export: [Raw](#) [Formatted](#)

Outdated/Insecure Application Protocols

Application Protocol	Protocol Version	Count
ftp	-	1,063
smb	1	535
tftp	-	64
ntp	3	42
tls	TLSv10	38

Connections by Destination Country



Arkime

- Front end for **both** enriched Zeek logs and Arkime sessions
 - Malcolm's custom Arkime Zeek data source adds full support for Zeek logs to Arkime, including ICS protocols
- Filter by Zeek logs or Arkime sessions; or, view both together
- “Wireshark at scale”: full PCAP availability for
 - viewing packet payload
 - exporting filtered and joined PCAP sessions
 - running deep-packet searches (“packet grep”)
- Connections view
 - Visualize connections between network hosts

File Analysis

- Zeek can “carve” file transfers in common protocols
- Malcolm examines carved files and flags hits
 - ClamAV – open source antivirus engine
 - YARA – pattern matching swiss army knife
 - Capa – portable executable capabilities analyzer
 - VirusTotal – online database of file hashes
 - requires API token and internet connection
- Triggering files can be automatically saved for future investigation



Suricata IDS – Coming Soon



- Integration of Suricata into Malcolm is the focus of a capstone project for a team of undergraduate researchers at BYU
- Several Suricata rulesets for industrial control systems are publicly available and will be usable by Malcolm
- Project is nearing completion; expect Malcolm release early Q3 2022

Q&A

Malcolm



Thank you!

Visit [Malcolm on GitHub](#)
support!

Malcolm is Copyright © 2022 Battelle Energy Alliance, LLC, and is developed and released as open-source software through the cooperation of the Cybersecurity and Infrastructure Security Agency of the US Department of Homeland Security.