v

Current SCADA security implementations typically utilize rule-based filtering, stateful packet inspection, and threshold-based filtering. According to Embedded.com, SCADA firewalls can “control who the device talks to (IP and MAC address filtering) and what traffic is allowed (port and protocol filtering) by filtering network traffic”[19]. These mechanisms create a “virtual closed network” by restricting communications to only what is required, but they don’t specifically implement time-window constraints.

Timing-Based Security Research

Recent academic research has explored timing characteristics of SCADA traffic, but primarily for anomaly detection rather than access control. One doctoral thesis states, “We focus on modeling the timing attributes of SCADA traffic for two reasons: (1) the timing regularity fits the automation nature of SCADA systems, and (2) the timing information is less prone to intentional manipulation by an attacker”[18]. This research models inter-arrival times to detect anomalies but doesn’t describe implementing time windows for segmentation control.

Assessment of Time-Based Segmentation Novelty

Timing Concepts in Current Research

While timing is already a component in SCADA security research, it’s primarily used in a different context. Current timing approaches focus on “modeling the timing attributes of SCADA traffic” for detecting anomalies and “finding sequential patterns of spontaneous event inter-arrival times”[18]. These methods analyze timing patterns to identify attacks rather than using time to control access between network zones.

Distinctive Aspects of the Proposed Approach

The proposed time-based segmentation would create temporal boundaries for access control, which differs significantly from existing approaches. Current segmentation strategies primarily focus on persistent rules rather than time-variable permissions. The concept of “simulating real-time operating constraints in critical infrastructure” through time windows represents a different security paradigm than what appears in the examined literature.

Conclusion

Based on the available search results, the specific concept of time-based segmentation for SCADA systems-allowing communication between zones only during pre-approved time windows and locking down all ports outside these windows-appears to be novel. None of the examined sources directly describe this approach to SCADA network security.

While timing characteristics are used in anomaly detection and various segmentation strategies exist for SCADA networks, the temporal access control mechanism described in your query represents a potentially innovative approach to SCADA security. The concept merges temporal constraints with traditional segmentation in a way that doesn’t appear to be currently implemented according to the available literature.

It should be noted that this assessment is based on the search results provided, which represent a sample of available literature. A more comprehensive literature review would be recommended before proceeding with research to ensure the approach is truly novel.

Citations:

[1] (https://www.diva-portal.org/smash/get/diva2:1287404/FULLTEXT02)

[2] (https://arxiv.org/pdf/2210.10352.pdf)

[3] (https://uppaal.org/texts/mmstt-icssa19.pdf)

[4] (https://hoop.dev/blog/time-based-access-network-segmentation-a-simple-guide-for-tech-managers/)

[5] (https://techdocs.broadcom.com/us/en/vmware-security-load-balancing/vdefend/vdefend-firewall/4-2/security-administration-guide/security/time-based-firewall-policy.html)

[6] (https://www.cisco.com/c/en/us/td/docs/Technology/industrial-automation-security-design-guide/m-segment-the-network-into-smaller-trust-zones.html)

[7] (https://docs.fortinet.com/document/fortivoice-enterprise/7.2.0/fortivoice-cookbook/520123/creating-schedules)

[8] (https://media.txone.com/prod/uploads/2023/09/Securing-Digital-Manufacturing-The-Essence-of-ISA-IEC-62443-Implementation-TXOne-WP-202309.pdf)

[9] (https://www.cisco.com/c/en/us/support/docs/quality-of-service-qos/qos-configuration-monitoring/11035-time-qos.html)

[10] (https://docs.paloaltonetworks.com/best-practices/security-policy-best-practices/security-policy-best-practices/deploy-security-policy-best-practices/security-policy-rule-best-practices)

[11] (https://www.directdefense.com/tales-from-the-road-if-your-scada-network-isnt-segmented-its-not-secure/)

[12] (https://docs.aveva.com/bundle/plant-scada/page/1121797.html)

[13] (https://www.directdefense.com/tales-from-the-road-when-it-comes-to-your-scada-network-segment/)

[14] (https://levelblue.com/blogs/security-essentials/10-strategies-to-fortify-scada-system-security)

[15] (https://www.energy.gov/oe/articles/good-practice-guide-firewall-deployment-scada-and-process-control-networks)

[16] (https://internationalpubls.com/index.php/cana/article/download/2644/1580/4723)

[17] (https://community.checkpoint.com/t5/IoT-Protect/SCADA-security-using-firewall-policies-pdf/td-p/39065)

[18] (https://www.diva-portal.org/smash/get/diva2:1424481/FULLTEXT01.pdf)

[19] (https://www.embedded.com/protecting-scada-devices-from-threats-and-hackers/)

[20] (https://pecb.com/article/what-is-scada-and-how-does-it-work)

[21] (https://iris.unipa.it/retrieve/handle/10447/15550/26632/Chapter7.pdf)

[22] (https://community.se.com/t5/Geo-SCADA-Knowledge-Base/Time-Synchronisation/ba-p/278751)

[23] (https://hoop.dev/blog/how-to-leverage-network-segmentation-for-time-based-access-control/)

[24] (https://gca.isa.org/blog/9-scada-system-vulnerabilities-and-how-to-secure-them)

[25] (https://is.mpg.de/ics/publications/human-action-segmentation-dynamic-clustering)

[26] (https://www.infosecinstitute.com/resources/scada-ics-security/ics-scada-access-controls/)

[27] (https://blog.heycoach.in/network-segmentation-tools/)

[28] (https://www.ssh.com/academy/operational-technology/scada-security-essentials-need-to-know-guide)

[29] (https://www.ri.cmu.edu/pub_files/2009/6/espriggs_cvpr_w09.pdf)

[30] (https://www.mhi.co.jp/technology/review/pdf/e492/e492007.pdf)

[31] (https://www.cisco.com/c/en_in/products/security/what-is-network-segmentation.html)

[32] (https://scadahacker.com/library/Documents/Standards/NIST - 800-41 - Guidelines on Firewalls and Firewall Policies.pdf)

[33] (https://www.tufin.com/blog/embracing-industrial-network-segmentation-strategic-approach-cybersecurity)

[34] (https://www.youtube.com/watch?v=xiBqg87kKRU)

[35] (https://www.wallix.com/blogpost/how-pam-enables-iec-62443-implementation/)

[36] (https://levelblue.com/blogs/security-essentials/10-strategies-to-fortify-scada-system-security)

[37] (https://gca.isa.org/blog/industrial-control-system-ics-security-and-segmentation)

[38] (https://www.nozominetworks.com/blog/advance-it-ics-cybersecurity-with-nozomi-networks-and-fortinet)

[39] (https://www.cisco.com/c/en/us/products/collateral/security/isaiec-62443-3-3-wp.html)

[40] (https://www.sciencedirect.com/science/article/abs/pii/S0167404818308071)

[41] (https://verveindustrial.com/resources/whitepaper/network-segmentation-in-ot-environments/)

[42] (https://www.fortinet.com/content/dam/fortinet/assets/white-papers/wp-advanced-threat-protection-industrial-control-systems-ot.pdf)

[43] (https://www.fortinet.com/content/dam/fortinet/assets/analyst-reports/report-sans-cybersecurity-iec-62443.pdf)

[44] (https://www.usenix.org/system/files/raid2019-lin-chih-yuan.pdf)

[45] (https://bufferzonesecurity.com/stop-worrying-and-start-isolating-protecting-industrial-control-system-ics/)

[46] (https://proactive.co.in/blog-details/streamlining-network-segmentation-with-cisco-ise-beyond-basic-vlans)

[47] (https://www.sciencedirect.com/science/article/pii/S0893608023002915)

[48] (https://www.armis.com/blog/chapter-7-network-segmentation-a-cybersecurity-best-practice-to-protect-industrial-assets/)

[49] (https://www.zscaler.com/resources/security-terms-glossary/what-is-purdue-model-ics-security)

[50] (https://www.cisco.com/c/en_in/products/security/network-visibility-segmentation/index.html)

[51] (https://www.dragos.com/blog/improving-ics-ot-security-perimeters-with-network-segmentation/)

[52] (https://nilesecure.com/network-design/network-isolation)

[53] (https://www.cisco.com/c/en/us/support/docs/smb/switches/Cisco-Business-Switching/kmgmt-2859-configure-time-

based-port-management-CBS-220.html)

[54] (https://www.nozominetworks.com/blog/nozomi-networks-integrates-with-palo-alto-networks-next-generation-firewall)

[55] (https://cache.industry.siemens.com/dl/files/913/109475913/att_951755/v1/GS_SCALANCE-S615_76.pdf)

[56] (https://industrialcyber.co/cisa/cisa-flags-hardware-vulnerabilities-in-ics-and-medical-devices-affects-br-schneider-electric-rockwell-bd-systems/)

[57] (https://www.rockwellautomation.com/en-in/company/news/blogs/restrict-and-contain-security-threats-with-network-segmentation.html)

[58] (http://cstor.com/wp-content/uploads/2016/10/Palo-Alto-Networks_SCADA-and-Industrial-Control-Systems_Solution-Brief.pdf)

[59] (https://support.industry.siemens.com/forum/WW/en/posts/time-setup-on-scalance-x-400/37276)

[60] (https://www.runzero.com/blog/schneider-electric/)

[61] (https://www.rockwellautomation.com/en-in/company/news/blogs/what-is-ics-security.html)

[62] (https://www.reddit.com/r/paloaltonetworks/comments/138vbbg/first_time_palo_deployment_any_favorite_initial/)

[63] (https://cache.industry.siemens.com/dl/files/963/109485963/att_878545/v1/ps7tsy_b_en-US.pdf)

[64] (https://www.se.com/in/en/faqs/FA405708/)

[65] (https://www.rockwellautomation.com/en-us/company/news/the-journal/accelerate-ot-industrial-network-segmentation.html)

[66] (https://onlinelibrary.wiley.com/doi/10.1002/qre.3626)

[67] (https://www.mdpi.com/1996-1073/17/11/2514)

[68] (https://attack.mitre.org/mitigations/M0930/)

[69] (https://inldigitallibrary.inl.gov/sites/sti/sti/Sort_64100.pdf)

[70] (https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/policy/security-policy/create-a-security-policy-rule)

[71] (https://www.westconcomstor.com/content/dam/wcgcom/Global/CorpSite/pdfs/Palo-Alto-Networks-Security-reference-blueprint-for-industrial-control-systems-white-paper-EN.pdf)

[72] (https://www.dragos.com/blog/industry-news/securing-industrial-control-systems-ics-against-cyber-threats-with-dragos-palo-alto-networks-integration/)

[73] (https://www.tenable.com/sites/default/files/integrations/SO-OT-Palo-Alto-Networks.pdf)

[74] (https://www.siemens-pro.ru/docs/scalance/GS_SCALANCE-S615_76.pdf)

[75] (https://thecyberexpress.com/ics-vulnerabilities-reported-this-week/)

[76] (https://literature.rockwellautomation.com/idc/groups/literature/documents/at/enet-at004_-en-e.pdf)

vv