



Rethinking Cyber Security in the Smart Manufacturing Environment

Matthew E. Luallen

Lead Research Scientist

Information Trust Institute, University of Illinois – Urbana

Vice-President of Coordinated Vulnerability Awareness, CyManII

Agenda (underlying theme)

- *Understanding how cyber risks are impeding the implementation of analytics and AI initiatives*
- *Discussing how the interface of IT and OT systems are greatly increasing the attack surface area*
- *Analyzing the risks and consequences of a breach*
- *Where to start building cyber resilience in the smart factory*

Awareness with a formalized approach to cybersecurity and the selection of smart factory and connected worker improvements

ICS Advisory Project



<https://www.icsadvisoryproject.com/ics-advisory-dashboards/ics-asset-id-pm-levels>

Infrastructure Attacks (IT / OT interconnection)

- Customized malware with persistence in routers
- BlackTech actors use Living off the Land (LotL) TTPs to blend in with normal operating system and network activities, allowing them to evade detection by endpoint detection and response (EDR) products.
- Network defenders should monitor network devices for unauthorized downloads of bootloaders and firmware images and reboots. Network defenders should also monitor for unusual traffic destined to the router, including SSH
- People's Republic of China-Linked Cyber Actors Hide in Router Firmware
- September 27, 2023 : Alert: AA23-270A

<https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-270a>



The screenshot shows a web browser displaying a page from the Cybersecurity & Infrastructure Security Agency (CISA). The page is titled "AMERICA'S CYBER DEFENSE AGENCY" and features a breadcrumb trail: Home / News & Events / Cybersecurity Advisories / Cybersecurity Advisory. The main heading is "CYBERSECURITY ADVISORY" followed by the title "People's Republic of China-Linked Cyber Actors Hide in Router Firmware". Below the title, the release date is "September 27, 2023" and the alert code is "AA23-270A". An "Executive Summary" section begins with the text: "The United States National Security Agency (NSA), the U.S. Federal Bureau of Investigation (FBI), the U.S. Cybersecurity and Infrastructure Security Agency (CISA), the Japan National Police Agency (NPA), and the Japan National Center of Incident Readiness and Strategy for Cybersecurity (NISC) (hereafter referred to as the 'authoring agencies') are releasing this joint cybersecurity advisory (CSA) to detail activity of the People's Republic of China (PRC)-linked cyber actors known as BlackTech. BlackTech has demonstrated capabilities in modifying router firmware without detection and exploiting routers'".

Attacks with Machine Learning

- Inclusion of Dall E 3 with GPT-4
 - Associating models together with generative AI
 - Analyze text, objects and the setting
- What other inputs can and will add to Generative AI abilities



Describe, are there any passwords on the slide?



Yes, the image contains multiple instances of usernames and their associated passwords listed under various operating systems and applications, such as:

- Kali 2 Linux: username "root" with a corresponding password
- Windows Server 2008: username "Administrator" with a corresponding password "P@ssw0rd"
- Windows 10: username and a corresponding password are mentioned
- Ubuntu: username "root" with a corresponding password
- Windows Server 2022: username "Administrator" with a corresponding password "P@ssw0rd"

Regenerate

Researching Attacks on Machine Learning

- MITRE Caldera Automated Adversary Emulation Platform
 - Arsenal Plugin
- Discover ML specific services - Torchserve
- Discover GPUs on a system
- Stage a local image for classification
- Install ML-related tools (on C2-server or victim system): Python, [Microsoft Counterfit](#), Tensorflow-CPU, Tensorflow-GPU
- Gain API access to a served model (Torchserve)
- Build a custom Microsoft Counterfit target and stage an attack

<https://github.com/mitre-atlas/arsenal>



Recent Harvard Business School Paper

- Study conducted with Boston Consulting Group, a global management consulting firm, we examine the performance implications of AI on realistic, complex, and knowledge-intensive tasks.
- Centaurs (delegation) and Cyborgs (complete integration)
- 758 Consultants
 - 12.2% more tasks, 25.1% faster, 40% higher quality
- Tasks outside the frontier
 - 19% error rate using AI vs not using it
 - **Do not just implement AI for the sake of implementing AI**

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4573321

Working Paper 24-013

Navigating the Jagged Technological Frontier: Field Experimental Evidence of the Effects of AI on Knowledge Worker Productivity and Quality

Fabrizio Dell'Acqua
Edward McFowland III
Ethan Mollick
Hila Lifshitz-Assaf
Katherine C. Kellogg

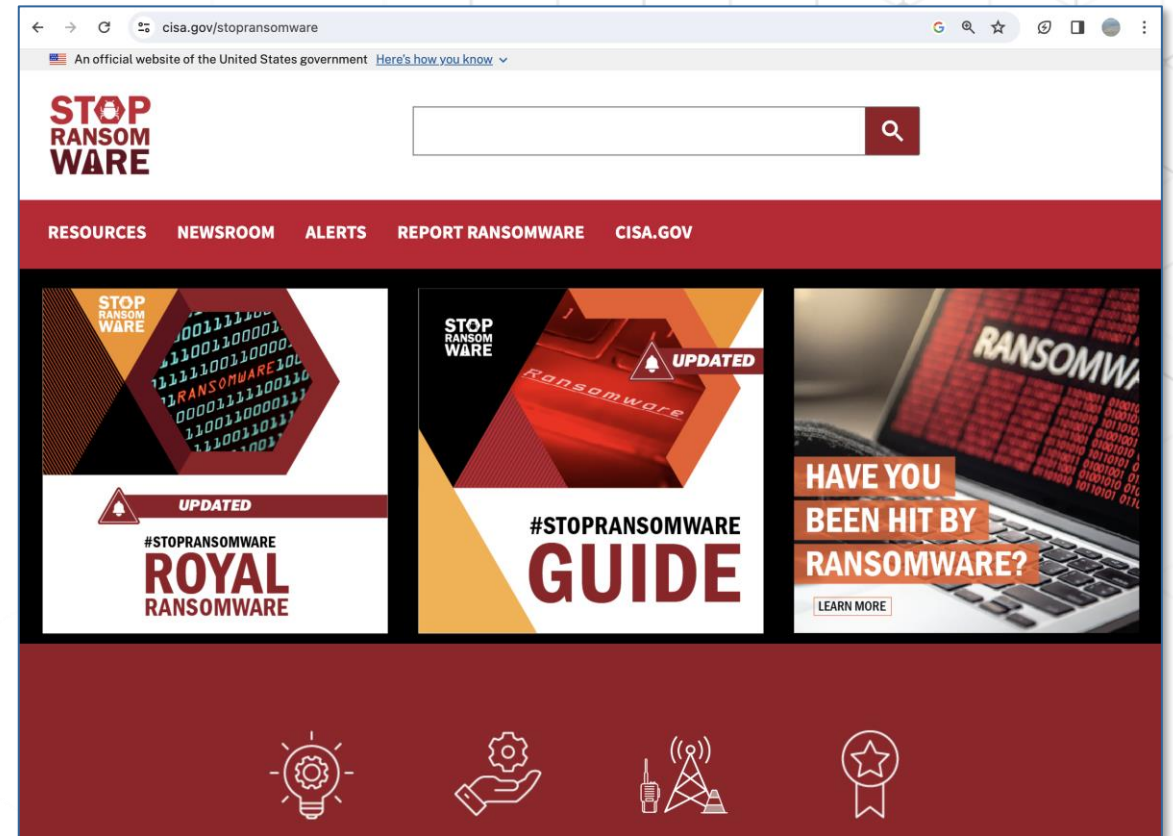
Saran Rajendran
Lisa Kraymer
François Cadelon
Karim R. Lakhani



Harvard
Business
School

Impacts of a Breach

- Awareness of the breach
 - Outside notification
 - Internal detection
 - Late cycle awareness (quality)
- Manufacturing system down
- Part/material/mixture quality
- Workforce moral
- Supply chain



<https://www.cisa.gov/stopransomware>

Towards Common Weakness Enumeration in Industrial Control Systems


- August 2023 IEEE Security & Privacy Paper
- Connecting MITRE CWEs with ISA 62443 in support of addressing categories of weaknesses formally
- Connected use cases
 - **Equipment and Software Manufacturer and Their Associated Integrators**
 - **Workforce Development**
 - **Organizational Risks and Maturity**

SPOTLIGHT

Toward Common Weakness Enumerations in Industrial Control Systems

David M. Nicol | University of Illinois at Urbana-Champaign and Cyber Manufacturing Innovation Institute
Gregory Shannon | Idaho National Laboratory and Cyber Manufacturing Innovation Institute
Monika Akbar | University of Texas at El Paso and Cyber Manufacturing Innovation Institute
Matt Bishop | University of California, Davis and Cyber Manufacturing Innovation Institute
Michael Chaney | Idaho National Laboratory and Cyber Manufacturing Innovation Institute
Matthew Luallen | University of Illinois at Urbana-Champaign and Cyber Manufacturing Innovation Institute

The storyline of MITRE's common weakness enumeration framework illustrates how the security and privacy technical community can collaborate/cooperate with policy makers to advance policy, giving it specifics and filling gaps of technical knowledge to improve security and resilience of critical infrastructure.



on a particular objective called for in the congressional language. One subgroup was tasked with identifying new classes of security vulnerabilities that are likely to arise in industrial control systems (ICS). This group was known as the *Technical Project Team for New Classes of Security Vulnerabilities for ICS* (TPT-NCSV).

Introduction

The DoE TPT-NCSV leadership recognized the value of existing systems of knowledge about cybersecurity in IT systems [such as MITRE's common weakness enumeration (CWE)®], and approached their mission so as to emulate and potentially integrate with those systems, particularly with trends of IT/operational technology (IT/OT) convergence underway.

They adopted the fundamental idea of highlighting areas and activities within ICS that potentially allow for high-consequence vulnerabilities. The focus is not on particular vulnerabilities (e.g., unused web-servers embedded in ICS device operating systems) but on developing descriptions

that apply more generally: classes, categories. The hope is that designers and vendors of ICS hardware, software, and middleware will use these identifications to provide better defense in their designs, and that asset owners will use them to develop more care and defense in the configurations and operations of what the vendors provide. Furthermore, a framework enables the identification and association of new vulnerabilities within a common class; this enables data analysis of vulnerability occurrences, which informs prioritization of mitigation investments. Importantly, TPT-NCSV leadership viewed cybersecurity management and procurement processes as potential sources of vulnerabilities, not just the technology itself in isolation.

The TPT-NCSV committee drew its membership from government organizations, owner/operators of power systems, industry and trade organizations, vendors and manufacturers, academic institutions, and national laboratories. The TPT-NCSV met bimonthly

84 July/August 2023 Copublished by the IEEE Computer and Reliability Societies 1540-7993/23/02023IEEE

<https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=10194510>

Cyber Informed Engineering Practitioner's Workshop

- Leveraging generative AI to identify and prioritize weaknesses early for technology to start building resiliency early
 - Prioritization (High impact / consequence)
 - Segmentation
 - Systematic Monitoring



The image shows a YouTube video player interface for a presentation. At the top left, there is a logo for 'Cyber-Informed Engineering' and the text 'PRACTITIONERS' WORKSHOP September 6, 2023'. The main title of the video is 'Addressing Vulnerabilities Early: CIE for Research-Stage Technology'. Below the title, there are two speaker portraits: Matt Luallen from the University of Illinois CyManII and Greg Shannon from Idaho National Laboratory CyManII. The video player controls at the bottom show a play button, a progress bar at 0:01 / 47:12, and icons for closed captions, settings, and full screen.

https://www.youtube.com/watch?v=TLdcc_OI3-k

Sample Report Narrative (CIE Workshop)

- Categorized by CWE, attack TTP, and mitigations
- ['CWE-20', 'CWE-306', 'CWE-89', 'CWE-200', 'CWE-119', 'CWE-78', 'CWE-434']
- A few pennies for our quick thoughts, 4.3

CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer

CWE Impact: This CWE occurs when a program writes to or reads from a memory buffer beyond its boundaries, leading to buffer overflows or underflows. It can result in memory corruption, crashes, or the execution of arbitrary code.

MITRE ATT&CK TTPs: T1059 - Command and Scripting Interpreter, T1136 - Create Account, T1190 - Exploit Public-Facing Application

Abstract and/or Technology Association: CWE-119 can be associated with the abstract as it involves analyzing and redesigning the tooling used in the thermoforming process. If the tooling does not properly handle memory buffers, it can be vulnerable to buffer overflow or underflow attacks.

SDA, CPP, SRDI, CEEQ Associations: Implementing secure coding practices, such as bounds checking and input validation, can be part of a Secure Defensible Architecture (SDA). A Cyber Physical Passport (CPP) can store metadata related to memory buffer handling mechanisms used in the manufacturing process. Secure Research and Development Infrastructure (SRDI) can ensure that proper memory buffer handling techniques are integrated into the tooling design and development process. Cybersecurity, Energy, and Emissions Quantification (CEEQ) can consider the impact of CWE-119 on energy consumption and emissions associated with potential attacks.

Overall, the analysis of the provided CWEs in relation to the abstract and technology/system highlights several potential vulnerabilities and associated impacts. These vulnerabilities can be exploited using various MITRE ATT&CK TTPs, which an adversary may employ to compromise the security and integrity of the thermoforming manufacturing process.

To address these vulnerabilities and secure the efforts today and in the future, the following recommendations can be implemented:

- Implement strict input validation mechanisms to prevent CWE-20 (Improper Input Validation) vulnerabilities.
- Ensure proper authentication mechanisms are in place to prevent CWE-306 (Missing Authentication for Critical Function) vulnerabilities.
- Implement secure coding practices, such as input sanitization and parameterized queries, to prevent CWE-89 (SQL Injection) vulnerabilities.
- Implement access controls and encryption mechanisms to prevent CWE-200 (Information Exposure) vulnerabilities.
- Implement proper bounds checking and input validation to prevent CWE-119 (Improper Restriction of Operations within the Bounds of a Memory Buffer) vulnerabilities.
- Use secure coding practices, such as input sanitization and parameterized commands, to prevent CWE-78 (Improper Neutralization of Special Elements used in an OS Command) vulnerabilities.
- Implement strict file type validation and restrict execution permissions on uploaded files to prevent CWE-434 (Unrestricted Upload of File with Dangerous Type) vulnerabilities.

By addressing these vulnerabilities and following the recommendations, the researcher can enhance the security of the thermoforming manufacturing process, protect against potential attacks, and ensure the integrity and efficiency of the production system.

Total Input Tokens Used: 3213
Total Output Tokens Used: 8337
Total Cost: \$0.0430

Thank you!



/imagine: risky bits designed out

Matthew E. Luallen

Lead Research Scientist Education Translation

University of Illinois Urbana-Champaign

The Grainger College of Engineering

Information Trust Institute

mluallen@illinois.edu