CFAM JWG Technology Solutions Subgroup

April 11, 2016
TEAM

- Heather Moyer, Concurrent Technologies Corp (CTC)
- Vicki Barbur, CTC
- Craig Rieger, Idaho National Laboratory
- Frank Serna, Draper
- Devu Shila, United Technologies Research Center
- Tim Shinbara, Association for Manufacturing Technology
- Janet Twomey, Wichita State University
- Dawn Beyer, Lockheed Martin
- Donald Davidson, DoD CIO
- Gib Goodwin, BriteWerx
- Larry John, ANSER
- Michele Moss, DoD CIO CTR
- Kaye Ortiz, Defined Business Solutions
- Chris Peters, Lucrum Group
- Jimmy Poplin, Defined Business Solutions
- Stephanie Shankles, DoD CIO CTR
The Technology Solutions subgroup deliverable will be a Recommendations Report based on an analysis of cyber attack vectors within the manufacturing environment and a gap analysis of existing and emerging technical solutions to improve cybersecurity in manufacturing.

The report will answer the following questions posed in the CFAM terms of reference:

• What technical solutions can be identified, either available now or under development, to increase cybersecurity in the manufacturing environment?
• What new technology-based concepts should be explored?
Approach

- Develop Confidentiality, Availability, and Integrity use cases based on representative manufacturing scenarios
- For each use case, develop attack trees revealing remote, local, and physical attack vectors
- Identify cybersecurity technology requirements consistent with NIST SP800-53 security control families
- Research existing and emerging technology solutions leveraging existing research and materials where possible and engaging subject matter experts and end users
- Develop a technology matrix identifying near-term (including solutions for legacy systems), mid-term, and long-term solutions and gaps
- Based on the gap analysis, develop recommendations for additional research as well as suggestions for what the government can do to promote or accelerate the commercialization of solutions
**Integrity Use Case Example**

*Goal* — Attack the quality of the additive manufactured product

*Layers* — CAD model, .STL/.AMF file, Tool command file, Process Control Parameters, Controllers

*Attack vectors*

- Rogue designers inserting malicious logic into the CAD model, STL file or Tool command file
- 3rd party models or files embedded with unwanted logic
- Malicious 3rd party CAD/CAM software that inserts extraneous or deletes logic into the models/files
- Tampers models/files/control parameters via Malware infection (by exploiting insecure external communications and software vulnerabilities of CAD/CAM software or Operating systems)
- Modifying files or process control parameters by exploiting Insecure local area communications
- Update controller firmware by exploiting insecure physical interfaces such as USB
Subject Matter Experts

- AMT Technology Issues Committee
- National Cybersecurity Center of Excellence (NCCoE)
- Society of Manufacturing Engineers
- Industrial Control Systems-Cyber Emergency Response Team (ICS-CERT)
- National Cybersecurity and Communications Integration Center (NCCIC)
- Industrial Internet Consortium Security Working Group
- Repository of Industrial Security Incidents
- CISCO, Rockwell Automation, Siemens, etc.
- Boeing, Lockheed Martin, GE, Alcoa, etc.

via Tim Shinbara
via Don Woodbury
via Debbie Holton
via Bob Timpany
via Bob Timpany
via iiiconsortium.org
via risidata.com
Next Steps

- Finalize use cases (attack trees)
- Schedule SME interviews
- Ramp up identification of available technologies
- Research emerging technologies