GENERAL DYNAMICS
Mission Systems

Cybersecurity – Endpoint Protection

Sean McGaughey, Chief Engineer

General Dynamics Mission Systems

So What? Who Cares?

- What topic is being addressed?
  - The cybersecurity of security equipment
- What problem has been solved?
  - How to address the cybersecurity of security equipment without treating it like IT equipment and using the same checklists that one would use for a laptop
- How has the problem been solved?
  - By treating the Operational Technology (OT) equipment on your network differently than you treat your IT equipment, focusing on the availability and integrity of the systems vice the confidentiality. The solution relies on applying principles of cross-domain security that have been validated in extremely high security environments for decades
  - Essentially, a “Guard” device is employed to transition between IT and OT networks, carefully examining the data passing both ways and applying policy to enable or disable that data flowing
  - The very predictable data flows from security equipment are ideal for employment of a whitelist device like this, insuring protection from not only known threat signatures but future unknown threat signatures
  - This guard enables the security device (the OT equipment) to be “off” the IT network of the system and not have to chase every patch Tuesday update and all the other cyber hygiene requirements of your IT network; this increases availability and reduces costs
- Why should TSA, DHS and the audience care about your solution?
  - Highly secure against known and unknown threats
  - Higher availability than solutions applied on the OT devices directly
  - Reduced cost when compared to frequent OT device updates
  - Applicable to both legacy and new systems

OT vs IT

- OT systems are focused on the monitoring and control of the physical world
- IT systems focus on access to, storing, and sharing of information
- Differing security considerations:

- Security equipment is OT, but it has to provide data to and be controlled by IT systems, so a gap has to be bridged.
  - This looks a lot like the problem of connecting different security domains.

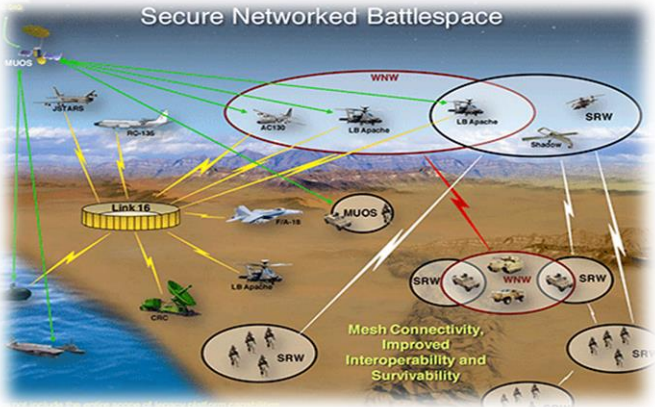
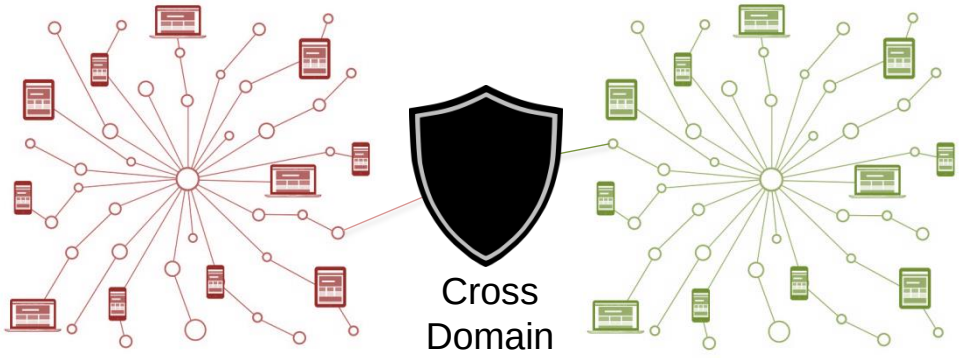


Image Source: http://www.doncio.navy.mil/CHIPS/ArticleDetails.aspx?ID=4344

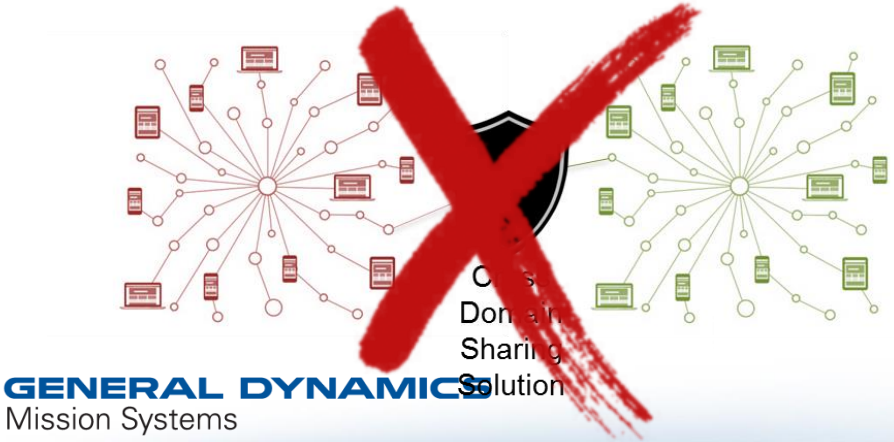


Cross Domain Sharing Solution

GENERAL DYNAMICS
Mission Systems

What does the guard do?

- Complies with IT security requirements as a system endpoint
  - It isn't performing physical security protection functions, it is built as IT equipment
  - Acts as the endpoint on the IT network instead of the security equipment
- Inspects all traffic running to/from the security equipment
  - This is data that is well structured and complies with an interface specification, which will form your "policy" for data that is permitted to pass
  - Whitelisting will protect against even unanticipated threats, because you are explicitly choosing what is allowed to pass rather than trying to keep finding bad signatures
- This is not a firewall or other network appliance, focused on network traffic, but a guard, focused on the data and commands passing to and from the security device
- Where the analogy begins to break down



GENERAL DYNAMICS
Mission Systems

Image Source: http://twistedsifter.com/2012/04/confluences-around-the-world/

The Solution

- Low cost, high reliability hardware tailored to your environment with guard software




- Configured and managed centrally on IT network
- Full connectivity of OT devices without the risks – highly secure against known and unknown threats
- Higher availability than solutions applied on the OT devices directly
- Lower cost than frequent OT device updates
- Easily applied to both legacy and new systems

GENERAL DYNAMICS
Mission Systems