Acquisition Research Program:
Creating Synergy for Informed Change

Architecture-Based Security for UxVs

V. Berzins

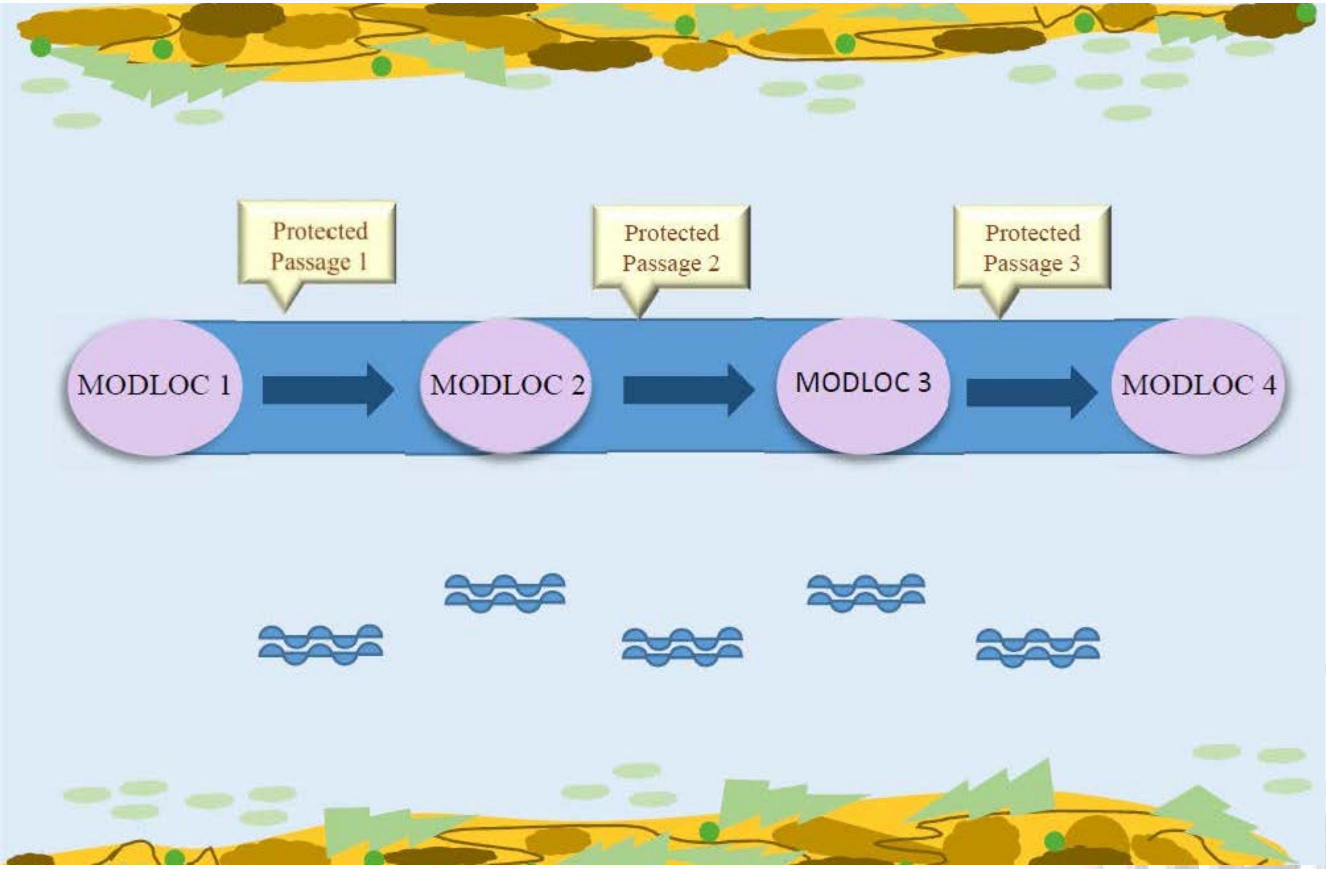
The views presented is this paper are those of the author
and do not necessarily represent the views of DoD or its Components.

UxV Security Challenges

- Security is key for Unmanned Vehicles (UxVs)
  – Worst case: adversary could take control and use them and the information they contain against us
- UxV security has unique concerns
  – Physical security cannot be guaranteed
  – Weak deterrence: retaliation for captured UxV unlikely
  – UxVs may not have defensive weapons
- UxVs are cyber-physical systems
  – Integrated software, physical parts, & communications
  – Need special certification methods
  – Claim: also need special acquisition methods

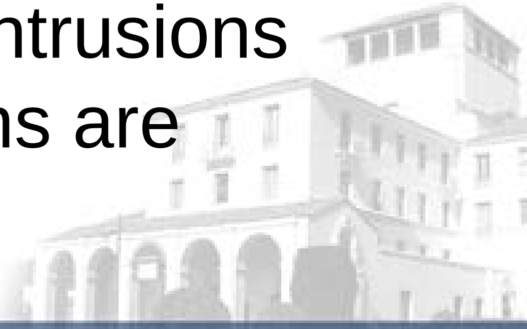
Case Study: USVs for ASW

- USVs as submarine detection pickets



Mitigations for Physical Intrusions

- Limit the sensitive information contained in UxVs to the bare minimum needed.
- Encrypt all sensitive information held in non-volatile memory.
- Protect the encryption keys with multiple redundant methods for defense in depth.
- Use multiple methods for sensing intrusions and erase sensitive data if intrusions are detected.



Acquisition Implications

- Mitigations apply to all kinds of UxVs
- Make them reusable requirements parts
  - Incorporate by reference into all contracts for unmanned military systems.
- Professional adversaries will eventually find ways to compromise barriers
  - Expect an arms race in developing counter-measures, counter-counter-measures, etc.
  - Make them replaceable parts in architecture/TRF

Conclusions

- Security of UxVs is a dynamic process strongly affected by changing circumstances

- UxV requirements and architectures should be organized around standardized, modular parts
- Each part should have multiple variants matching likely future circumstances.

- Want rapid reconfiguration by component swapping, matching capabilities to current situations using a plug-and-fight concept

Recommendations

- Develop a Technical Reference Framework (TRF) for UxVs that defines fragments of system and software architecture for mitigating security threats.
  - Needed to support interchangeable components that adapt capabilities in a plug-and-fight mode
- Establish a Navy/Joint organization for developing and managing improvements to the TRF recommended above
  - Provide it with the resources needed to support an ongoing effort to keep TRF mitigations effective.

Recommendations

- UxVs are supposed to be expendable
- Don’t put sensitive information on them

https://www.heartland.org/news-opinion/news/the-real-reasons-africa-has-another-locust-plague

Thank you