Cybersecurity in military systems

Tarmo Aia, TalTech & EDF

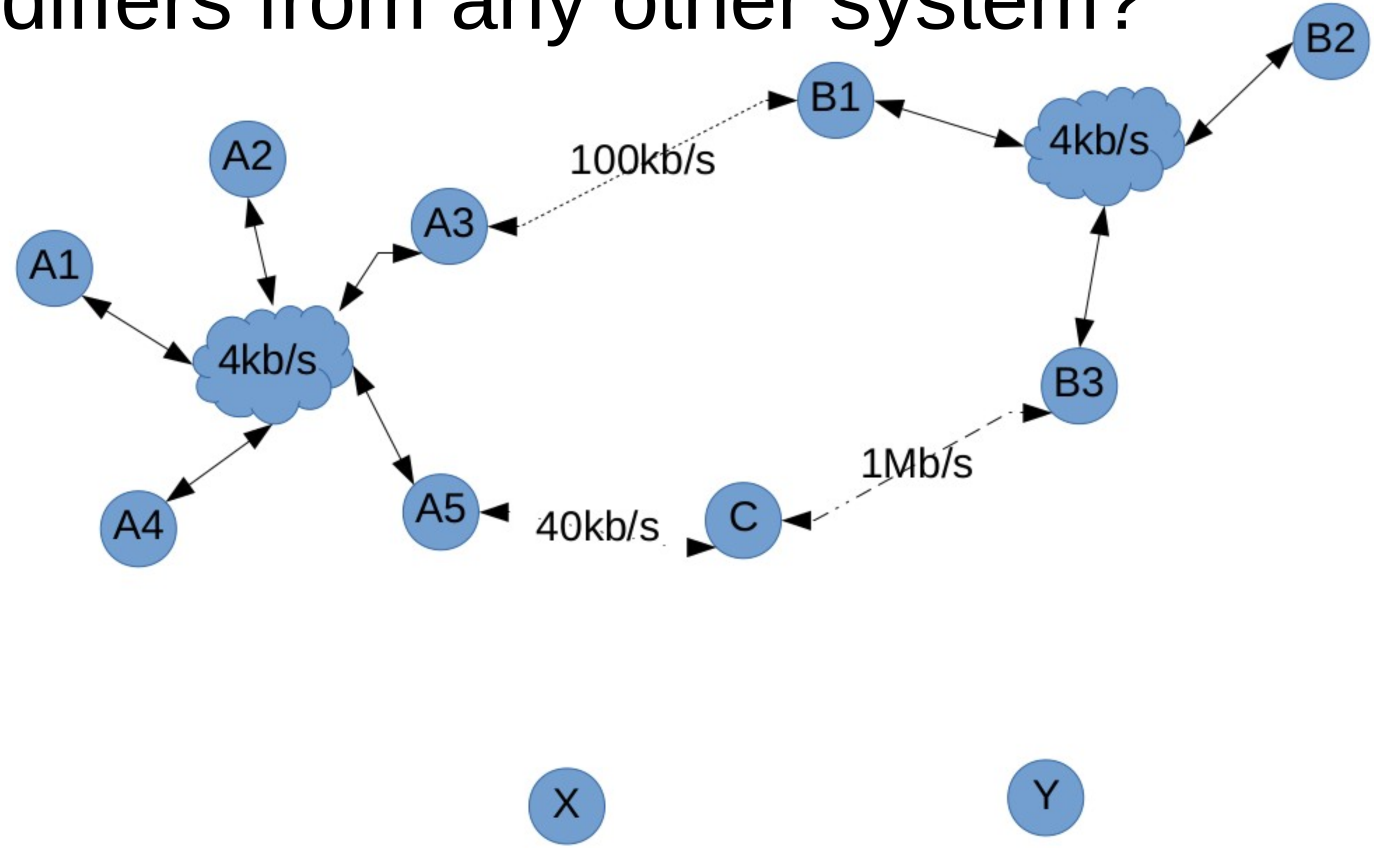
2018

Cybersecurity in military systems

- Introduction
- GAO 19-128
- What was told
- What was really told
- Some real life examples and problems
- Questions

Intro

- What is military (comm) system and how it differs from any other system?



Introduction

- Comms vs bombs problem
- Cyber and comms
- False illusion of “our internal network is secure”

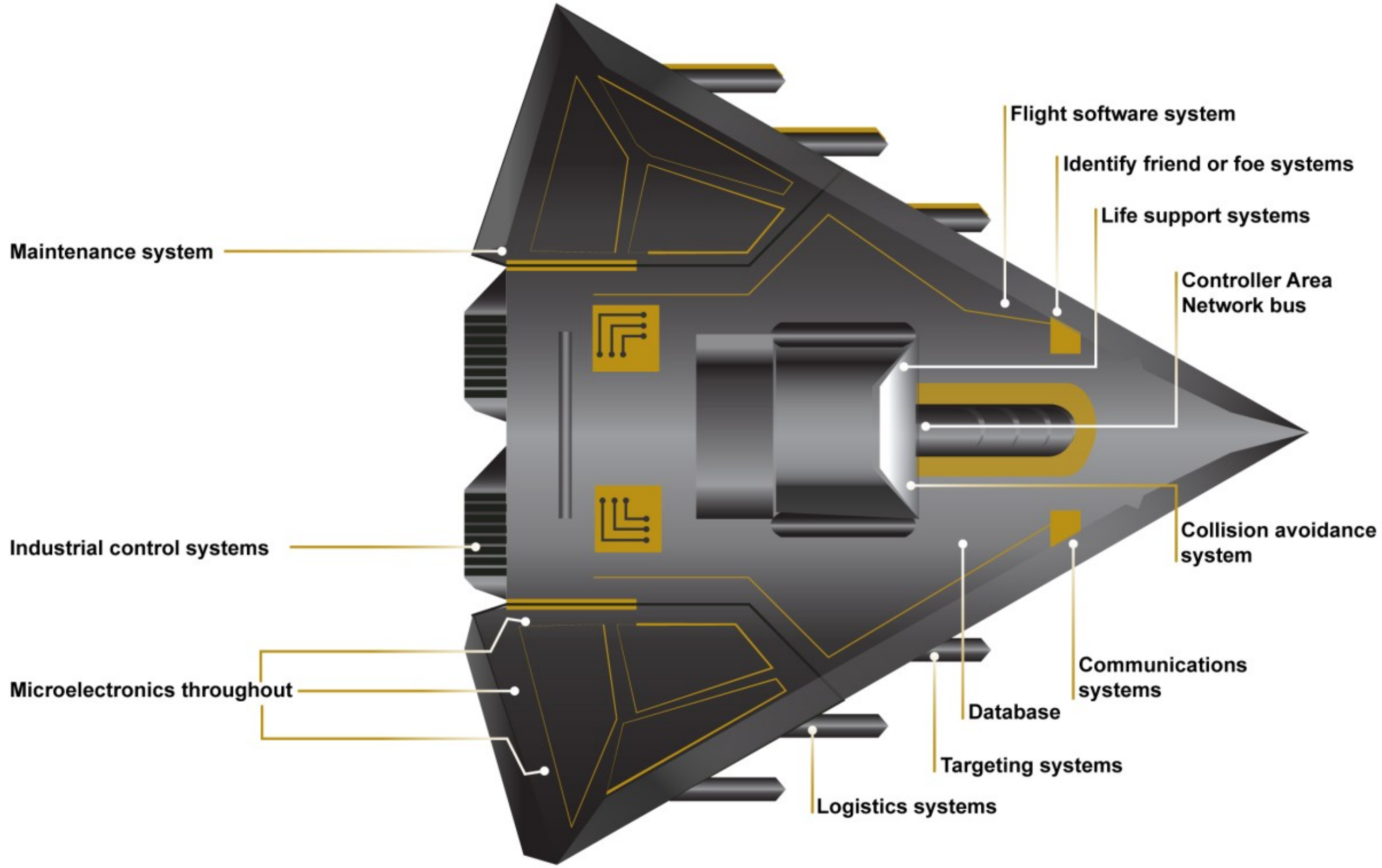
GAO 19-128

- U.S. Goverment Accountability Office
- https://www.gao.gov/products/GAO-19-128

GAO 19-128

- DOD Just Beginning to Grapple with Scale of Vulnerabilities
- Translation: DOD does has not implemented any systematic security in (weapons) systems
- First talk about cybersecurity began in 2014 (regulations)
- Report covers only weapons system under development

GAO report


Flight software system
Identify friend or foe systems
Life support systems
Maintenance system
Controller Area Network bus
Industrial control systems
Collision avoidance system
Microelectronics throughout
Communications systems
Database
Targeting systems
Logistics systems

Source: GAO analysis of Department of Defense information. | GAO-19-128

GAO report

- Almost all major weapon systems had critical, exploitable vulnerabilities (2012-2017)
- Many performed tests were very limited and probably found only couple (fastest) exploits
- In many cases, previously found issues was uncorrected

GAO report

- Information classification problem – most of vulnerabilities information has TOP SECRET classification
- Information are not shared cross different platforms – design flaws not corrected
- Testing was performed usually only used limited time and basic tools

GAO report

- In some cases security measures are implemented but not correctly (plain text passwords etc)
- Security measures detected intrusion in some scenarios but it was not noticed by operators

GAO report - translated

- DOD lacks trained personnel who can operate security devices
- Most of cybersecurity has invested/deployed to protected “normal” IT infrastructure
- High security classification of vulnerabalities makes them impossible to correct mistakes in real life
- Tested were only “in development” weapons system, meaning older systems are even more vulnerable

Examples and problems

- Release cycle
- SLA and delivery of patches – on or off site, factory?
- Technical debt
- Closed or restricted source codes
- Procurement: times, resources, additional funding and maintenance
- Security through obscurity

Examples and problems

- Vendor restricted alghoritms – no warranty that standard is implemented correctly
- Vendor firmware locks
- Unimaginable number of old (unsecure) technologies/protocols – telnet, SNMPv1, tftp or their vendor variations
- Old encryption standards
- Hardcoded passwords
- Goverments regulations (e.g. ITAR)

Examples and problems

- Encryption not used where it could be used easily: HTTP, SIP/RTP
- Remote control – e.g CAN bus
- https://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-acceleration-hacks/
- Operation systems – WindowsXP still used in many active systems
- No real (standard) way to authenticate devices

Comms vs bombs

- Due to restrictions (cyber)security is not often part of the system initial requirements and design – i.e. is not integral part of the system

Cybersecurity in military systems

- Questions?