Supporting European Aviation

EUROCONTROL

(New) PENS and the EATM CERT

Cybersecurity Considerations

Nathalie Moedersheim
PENS Management Unit Lead
CRV OG11 - 01 February 2023

CONSORTIUM COORDINATOR sesar DEPLOYMENT MANAGER
FOUNDING MEMBER sesar JOINT UNDERTAKING
NETWORK MANAGER

Presentation Outline

The presentation generically introduces:

- Security management practices from the PENS Community perspective
- The activities of the EATM CERT (The European Air Traffic Management Computer Emergency Response Team) with a focus on penetration testing (ethical testing)

For more information on the EATM CERT:

Patrick Mana
EATM CERT Manager
Patrick.Mana@eurocontrol.int
European Air Traffic Management Computer Emergency Response Team (EATM-CERT) | EUROCONTROL

PENS - A Closed User Group Network

- IP transport solution is end-to-end managed by the Service Provider
- Built upon
  - A highly resilient MPLS core
  - Access nodes (sites or Service Delivery Points)
- Virtualisation provides logical separation between groups/types of ATM flows (voice, data, surveillance…..)
- Stringent security requirements apply to the network service provider (including their underlying supply chain)
- Only explicitly authorised traffic is allowed on the network – it is otherwise forbidden

Contract Robustness in the Cyber Field

- At the end of 2018, EUROCONTROL/NM conducted a Cybersecurity Assessment with objectives to:
  - Develop an ATM Cybersecurity Maturity Model for industry
  - Review cybersecurity of key suppliers to NM (including the PENS and NewPENS providers)
  - Facilitate improved risk and threat assessment processes
  - Dissemination/increase awareness of latest offensive techniques
- The assessment highlighted that the **<u>NewPENS Contract/Service incorporates all industry good practices on security requirements</u>**
- The supply chain *(aka the 'soft underbelly')* is increasingly being targeted by criminals and state actors
  - Wide ranges of suppliers/products/services makes it hard to assure
  - Common assurance practices are vital

National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF)

+

ISO27001: Information Security Management Systems

"Leadership, governance and management are crucial"

PENS – Community Approach to User Security

Protect your organisation

- **Each NewPENS User is requested to implement appropriate security measures** to protect their systems in line with their security policy
- **The NewPENS Service Provider ensures only authorised traffic is carried-over the network**
- Network physical components are monitored for intrusion attempts and information is automatically relayed to the PENS's supplier Security Operation Centre (SOC). Information is thereafter disseminated to the community (as appropriate) through the PENS Service Management Framework
- The PENS Service Catalogue allows for an extensive range of security peripheral to be deployed at the network edge (intrusion/detection systems, encryption…..)

PENS Community approach to CyberSecurity

- Collaboration is established and further developed between **PENS and the EATM-CERT**
  - Information sharing with BT on cybersecurity feeds collected from National Cybersecurity Centres, aviation stakeholders, Cyber Threat Intelligence vendors and EATM-CERT findings
  - Conduct security assessment (e.g. penetration testing) on BT services and infrastructure supporting PENS
  - Conduct security assessment of end points (PENS sites) to derive generic lessons learned to improve Users security and reciprocal trust
- PENS User Security is continuously being considered and developed

The European Air Traffic Management Computer Emergency Response Team (EATM CERT)

- The EATM CERT is Established in EUROCONTROL
- The mission of the EATM CERT is to support ATM stakeholders (ANSPs, Airport Operators and Airspace Users of the EUROCONTROL Member States) in protecting themselves against cyber threats that would impact the confidentiality, integrity and availability of their operational IP assets and data
- The EATM CET provides the following services:
  - proactive cyber-security services, within EUROCONTROL, and, **on a voluntary basis**, progressively to EUROCONTROL stakeholders;
  - collection, generation and distribution of ATM-relevant cyber intelligence within EUROCONTROL and, on a voluntary basis, to EUROCONTROL stakeholders;
  - coordination of pan-European ATM response to ATM relevant cyber-security alerts and incidents, on a voluntary basis (including support to EACCC);
  - procurement of cyber services of common interest for the aviation community;
  - support to national CERTs in fulfilling their role as per NIS Directive for ATM-related Operators of Essential Services (OES).

Penetration Testing Methodology

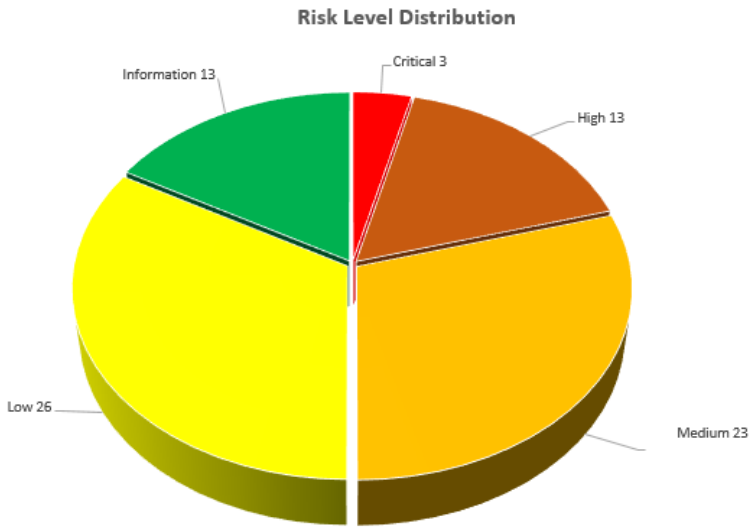
- Penetration testing methodology is organised around 7 phases:

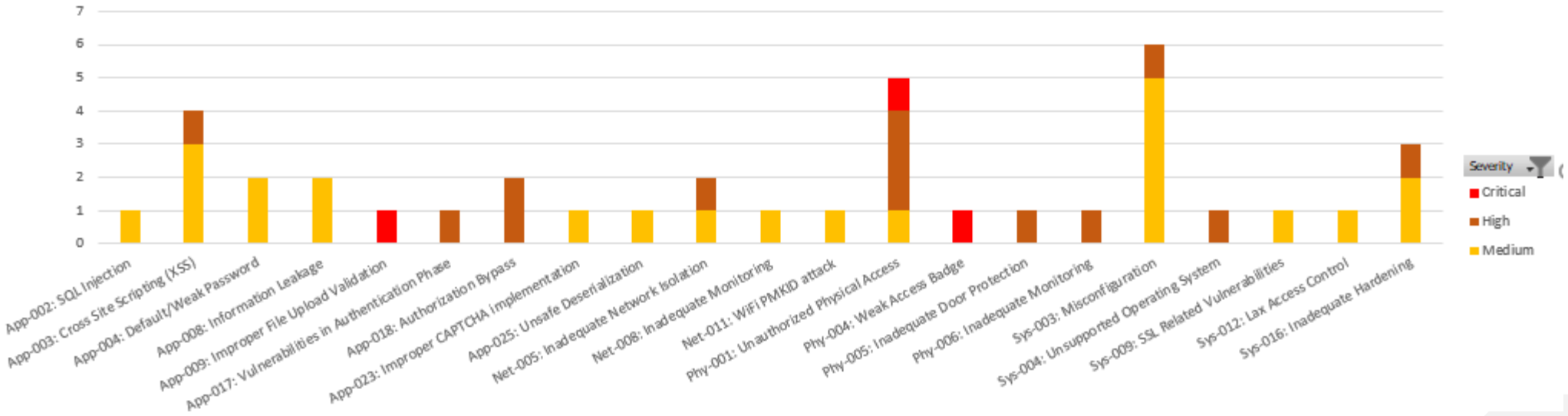
1) Information Gathering Phase;
2) Enumeration Phase;
3) Penetration Phase;
4) Post-exploitation Phase;
5) Maintaining Access Phase;
6) Cleaning Phase;
7) Reporting Phase.

Penetration testing on aviation systems

- Tests conducted so far (total ~60 since 2018):
  - on EUROCONTROL systems, services, products (NM, MUAC, CRCO, ARTAS, …)
  - on aviation stakeholders systems (ANSPs, airport operators)
- Able to conduct max 8 to 12 pentests on stakeholders systems
  - Free of charge (for stakeholders of EUROCONTROL Member States)
  - **Collaborative**
    - ✓ 3 steps:
      - Scoping document: collaborative definition of scope, objectives, scenarios, schedule
      - One-week on-site tests. No risk of operational impact. Joint activity.
      - Final report subject to review-approval
    - ✓ 2 categories of findings:
      - Local: only for stakeholder
      - Generic: de-identified and shared with aviation community on a need to know basis

Pentests – Example of findings



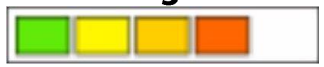


Risk levels definition

Risk Level					
Impact\Likelihood	Very unlikely	Unlikely	Moderate	Likely	Very likely
Trivial	Low	Low	Low	Medium	Medium
Minor	Low	Low	Medium	Medium	**High**
Moderate	Low	Medium	**High**	**High**	**High**
Major	Medium	**High**	**High**	**Critical**	**Critical**
Serious	**High**	**High**	**Critical**	**Critical**	**Critical**

Likelihood	Explanation
Very Unlikely	The vulnerability in this likelihood is very unlikely to be exploited since many authentication and authorization mechanisms exist, i.e. attackers have to pass many defence-in-depth mechanisms. Local access with single or multi factor authentication is an example of this kind of defence-in-depth mechanisms. The threat actors may be insiders, advanced attackers and threat groups who bypass physical security protections and access to network by stealing some credentials.
Unlikely	The vulnerability in this likelihood is unlikely to be exploited since a few authentication and authorization mechanisms exist, i.e. attackers have to pass a few protection mechanisms. Local access without single or multi factor authentication is an example of this kind of protection mechanisms. The threat actors may be insiders and/or attackers and threat groups who bypass physical security protections and directly access the network or easily bypass network access protections.
Moderate	The vulnerability in this likelihood is moderate to be exploited since many authentication and authorization mechanisms exist, but the vulnerability may be exploited from the Internet and not only from Internal. Attackers have to pass many defence-in-depth mechanisms like multi factor authentication, Internet access with strong authentication like certificates and/or multi factor authentication. IP access restrictions are also an example of this kind of the defence-in-depth mechanisms. The threat actors may be targeted advanced attackers and threat groups.
Likely	The vulnerability in this likelihood is likely to be exploited since a few authentication and authorization mechanisms exist, but the vulnerability may be exploited from the Internet and not only from Internal. Attackers have to pass a few defence-in-depth mechanisms like weak authentication, Internet access with user/password authentication or IP access restrictions can be example of this kind of protections. The threat actors may be novice attackers, untargeted threat groups in addition to advanced attackers and targeted groups.
Very likely	The vulnerability in this likelihood is very likely to be exploited since it can be easily exploited from the Internet and not only from Internal. Attackers can directly attack to the systems without bypassing the defence-in-depth mechanisms. The threat actors may be scripts kiddies in addition to novice, advanced attackers and threat groups.

Impact	Explanation
Insignificant	**Operations**: Insignificant impact when operational/safety services can be provided as usual. **Finance**: Impact can be managed within business unit/branch/section budget. **Service Delivery**: It causes negligible effects on the ability to provide a business service. **Reputation**: The reputation can be effected by the isolated complaints of individual stakeholders.
Minor	**Operations**: Minor impact when some operational/safety services are degraded. **Finance**: Impact requires delegated approval for response. **Service Delivery**: It impairs the ability to provide a business service. **Reputation**: The reputation can be affected by the complaints of a key stakeholder on organization/company services and activities.
Moderate	**Operations**: Moderate impact when some operational/safety services cannot be provided anymore. **Finance**: Impact requires upper management approval for response. **Service Delivery**: It severely compromises the ability to provide a business service. **Reputation**: The reputation can be affected on organization/company services and activities by a key stakeholder.
Major	**Operations**: Major impact when a majority of operational/safety services cannot be provided anymore for a significant time. **Finance**: Impact requires the board approval for response. **Service Delivery**: It causes the short-term inability to provide a critical business service. **Reputation**: The reputation can be affected on capability to provide functions/services by the majority of the stakeholders.
Serious	**Operations**: Serious impact when all operational/safety services cannot be provided anymore for a sustained time-frame. **Finance**: Impact requires government support. **Service Delivery**: It causes sustained inability to provide a service. **Reputation**: The reputation cannot be repaired with stakeholders and the organization/company may not continue in its current form.

Risk Level	Example
Critical 	*Vulnerabilities in this category cause a serious impact on the operational ATM environment from the Internet.* *Ex. Shut down air traffic control systems from a web portal.*
High 	*Vulnerabilities in this category can cause a partial impact on the operational ATM environment.* *Ex. Degradation of ATC systems by inserting fake flight plan information from a web portal requiring strong authentication.*
Medium 	*Vulnerabilities in this category can cause a serious impact to ATM supporting systems from the Internet or a partial impact on ATM systems from the local ATM environment.* *Ex. Shut down monitoring systems of ATC environment from a web portal.*
Low 	*Vulnerabilities in this category have limited impact to ATM supporting systems or non-ATM related systems.* *Ex. Vulnerabilities to corporate email infrastructure from local network.*
Information 	*Gaining limited information about configuration is classifie d as level 1 informational -level vulnerabilities. The vulnerability in this category gives some basic information to the attacker about the system.* *Ex. Information leaked by web server headers about software version.*