ATM Security Research in SESAR

ART Workshop
ENAC, Toulouse
23/03/2016

John Hird, DATM/RDS/PM/ATM Security
Manager, SESAR Project16.06.02 - ATM Security Coordination & Support
Topics

• The Scope of ATM Security
• The Evolving Risk Environment
• Myth Busting
• How is SESAR Addressing Security?
• Security Reference Material – Components
• Security Database Application
• Supporting the Projects
• SESAR 2020
THE SCOPE OF ATM SECURITY
Failing to adequately address security - impacts SESAR KPAs and other goals
We call **SAFETY** everything related to accidental events able to affect material and people (*failures, …*).

**SECURITY** concerns the prevention of deliberate malicious acts aimed at impacting the ATM system as a whole (*theft, hacking, jamming, spoofing, DoS*…).

Whatever can happen accidentally can be caused deliberately…

… the potential impact may be the same
ATM Security within Aviation Security

Airport Security
• Safeguarding of the airport

Aircraft Security
• Safeguarding of the aircraft

Airspace Security
• Safeguarding of the airspace

ATM Security
• Safeguarding of the ATM System
• Collaborative support to national / Pan European aviation security incident management
ATM System Assets
– What Are We Trying to Protect?

Service Provision

**Physical:** e.g. Communications, Navigation, Surveillance (CNS), ATM centres, ...

**Staff:** Operational, Engineering, IT …

**Information:** Operational, Historical

**Organisational:** Financial, Reputation
Threats past …

… and present!
THE EVOLVING RISK ENVIRONMENT
The Transition to the New System

Today's ATM System

ASAS 4D

New Operational Concepts

Evolution

Transition

More COTS Products

CWP FDP RDP

Open Standards

TCP/IP XML HTML

More Interconnected Systems

SWIM AG GG

AIM CIA provenance

More Data Sharing

Tomorrow's ATM System
Risk Evolution in the Changing Security Environment

**Risk** = Impact x Likelihood

**Likelihood** (probability) of attack on ATM

Drivers - increased hacking; criminality; State sponsorship

**Impact** (severity) of attack on ATM

Drivers – system interdependency; data sharing

**Transition**

LIKELIHOOD
How likely is the event

RISK
Combined likelihood and impact

IMPACT
How bad can the event be?
Key Driver – Minimise Impacts on the Following

- **Personnel**: Stress, minor injury, ..., fatality
- **Capacity**: Reduction, loss
- **Performance**: Reduction, loss
- **Economic**: Financial loss
- **Branding**: Reputation
- **Regulatory**: Breach of requirement
- **Environment**: Impact on environment
ATM Security Evolution

Pre-9/11:
Distress Traffic & Hijack Support

Single European Sky
→ ANSP
→ Security Management

Doc 8954 “KPA”
Annex 17
Amendment 12
→ ATSP
→ Cyber
Doc9985

Doc 30
Chapter 13
→ ANSP

ATM / ANS “critical” infrastructure

ATM Master Plan
SESAR
MYTH BUSTING
ATM is not a Target?

Absence of evidence ≠ Absence of threat
Many compromises not discovered for years

Why Attack ATM or other Critical Infrastructures?

• To deny, degrade, disrupt, or destroy information systems and gain publicity

Potential players:

• Hackers/hacktivists – seeking challenge, notoriety, supporting ideological/political beliefs
• Terrorists – seeking a visible impact on a significant infrastructure
• Nation states – strategic target if state relationships deteriorate; possibility of military conflict

The target of the attack is not the system → it’s the public’s confidence in the integrity of networks and systems

Information sharing on ATM security incidents?
No legal requirement - Difficult to establish – Sensitive (commercially, reputationally)
ATM has never been attacked

Imagine:

- Theft of copper, batteries and other equipment ✓
- Injection of data, spoofing of systems ✓
- Unauthorised access to operational centers ✓
- Leaving ‘suspect’ packages to cause operational disruption ✓
- Electronic hacking into data systems ✓
- Deliberate use of substandard products in operational systems ✓
- IT systems containing unauthorised programmes (and viruses) ✓
- System overload (Denial of service attacks) ✓
- GPS jamming ✓

**Luckily**, so far:
- “Known” financial impact not substantial
- No businesses severely impacted
- No injuries or loss of life
2006:
- Web-based viral attack infected ATC systems
- Part of ATC system in Alaska had to be shut down

2008:
- Hackers briefly controlled FAA critical network servers

2009:
- Hackers breached public-facing website
- Gained unauthorized access to personal information on 48,000 current and former employees

Audit revealed: 3800+ vulnerabilities in 70 Web apps (760 high-risk)

"In our opinion, unless effective action is taken quickly, it is likely to be a matter of when, not if, ATC systems encounter attacks that do serious harm to ATC operations"
Other Aviation

ATC Pilot-Controller Voice Communications (UK) : Communications disrupted; false instructions to pilots; fake distress calls (lack of authentication, compromise of integrity)

1998 - 3 incidents reported; 2010 - 18 incidents reported; 2011 - 20 incidents reported

Airline Network Hacked - 2011 : Pure Hacking (Penetration testing consultancy) -

- While penetration testing gained access to an airlines critical systems using a simple hack (Asia Pacific AVSEC Conference, Canberra, 2011)

GPS : Jamming - Newark airport, August 2013 – Sporadic outages of GBAS (Ground Based Augmentation System) caused by truck driver’s GPS jammer

“GPS Jammers and Spoofers Threaten Infrastructure” - http://arstechnica.com/business/2012/02/uk-research-measures-growing-gps-jamming-threat/


17th December 2015 : 19-year-old Teen Steals 150,000 dollars by Hacking Into Airline’s Website - http://thehackernews.com/2015/12/airline-tickets-hacked.html

30th November 2015 : Guess who doesn’t do cyber-resilience testing? Yep, air traffic control - http://www.theregister.co.uk/2015/11/30/cyber_resilience_analysis/
Potential Threats

- Corruption of data
- Unauthorized use of equipment
- Electromagnetic radiation/pulses
- Radiation disturbance
- Destruction of equipment or media
- Social Engineering
- Unauthorized Action
- Compromise of Information
- Loss of Essential Service
- Tampering with HW/SW
- Eavesdropping
- Theft of media, documents, equipment
- Communications
- Power
- Physical Damage
- Loss of Essential Service
- Tomorrow’s ATM System
HOW IS SESAR ADDRESSING SECURITY?
How should you spend your money to gain a proportionate reduction in risk?

Suddenly, a heated exchange took place between the king and the moat contractor.
The 16.06.02 Approach to Security

We need:
A structured, rational approach to
- Identify risks
- Prioritize them
- Decide how to address (Treat, Transfer, Terminate, Tolerate)
- Act to reduce risk to an acceptable level

The approach:
- Ensure that security is designed-in
- Address from beginning of the development lifecycle
- Use a holistic approach

Goal:
- Design in Security

Retrofitting can be:
- Expensive
- Time-consuming
- Not feasible
Safeguarding the ATM System: *Incident Preparedness and Operational Continuity Management (IPOCM)*

- Preventing an incident by protecting the system from an attack
- Recovering to normal operations as safely/quickly as possible

\[ \text{KPA} \]

100%

With Controls

Post-event control to speed-up recovery

Without Controls

Pre-event control to reduce Likelihood or impact

- IPOCM is realised by performing a *Security Risk Assessment* to identify *what* needs to be protected and *how* to protect it
Security Risk Assessment

Confidentiality
Integrity
Availability

ASSETS

Vulnerabilities

CONTROLS

THREATS
The Security Risk Assessment Methodology

Identify:

- Assets
- Impacts on CIA
- Risks
- Controls
### Risk Matrix

<table>
<thead>
<tr>
<th>Likelihood</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Low</td>
<td>High</td>
<td>High</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>4</td>
<td>Low</td>
<td>Medium</td>
<td>High</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>3</td>
<td>Low</td>
<td>Low</td>
<td>Medium</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>2</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Medium</td>
<td>High</td>
</tr>
<tr>
<td>1</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Medium</td>
<td>Medium</td>
</tr>
</tbody>
</table>
If you think technology can solve your security problems, then you don’t understand the problems and you don’t understand the technology. Bruce Schneier
### Risk Reduction – more than IT

**Controls to Reduce Impact:**
- Network isolation
- Staff training
- Governance structure
- Redundancy, backups

**Controls to Reduce Likelihood:**
- Network isolation
- Physical protection
- Security staff

#### Likelihood Impact Matrix

<table>
<thead>
<tr>
<th>Likelihood</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Low</td>
<td>High</td>
<td>High</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>4</td>
<td>Low</td>
<td>Medium</td>
<td>High</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>3</td>
<td>Low</td>
<td>Low</td>
<td>Medium</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>2</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Medium</td>
<td>High</td>
</tr>
<tr>
<td>1</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Medium</td>
<td>Medium</td>
</tr>
</tbody>
</table>
SECURITY REFERENCE MATERIAL - COMPONENTS
ATM Security Reference Material

### ATM SECURITY POLICY

**GOAL**
Security shall be addressed, in the context of the SESAR programme in accordance with the regulatory framework. The following areas shall be covered: the self-protection and resilience of the ATM System; and the collaborative support to national aviation security agencies and authorities.

**SECURITY MANAGEMENT APPROACH**

A systematic approach is applied to ATM Security Management which achieves the following:

1. **Ensures** the self-protection and resilience of the ATM system and enables collaborative support of the ATM system to authorities concerned with security incidents;

2. **Establishes** ATM security as an integral part of SESAR design and development;

3. **Promotes and adopts** industry standards and best practices for security and security management;

4. **Supports** the validation that SESAR deliverables are acceptably secure.

<table>
<thead>
<tr>
<th>Security Management Approach</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Ensures the self-protection and resilience of the ATM system and enables collaborative support of the ATM system to authorities concerned with security incidents;</td>
<td>Ensuring the application of the ATM Security Policy</td>
</tr>
<tr>
<td>2. Establishes ATM security as an integral part of SESAR design and development;</td>
<td>ATM Security assessment and assurance activities are carried out on identified aspects of the SESAR design and development based on the Security Risk Assessment Method</td>
</tr>
<tr>
<td>3. Promotes and adopts industry standards and best practices for security and security management;</td>
<td>Harmonised interpretation and implementation of the regulatory framework and standardisation activities</td>
</tr>
<tr>
<td>4. Supports the validation that SESAR deliverables are acceptably secure.</td>
<td>SESAR ATM Security Cases which support the deployment of the SESAR products</td>
</tr>
</tbody>
</table>

---

**Including:**

Security Policy; Security Risk Assessment Methodology; Supporting Implementation Guidelines; Worked examples; Risk Treatment; Minimum Set of Security Controls (MSSC); …
SECURITY DATABASE APPLICATION (CTRL_S)
## Security assessment menu

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>00</td>
<td>Enter: Project / Solution details</td>
</tr>
<tr>
<td>01</td>
<td>Input: Primary Asset details (PA)</td>
</tr>
<tr>
<td>02</td>
<td>Input: Supporting Asset details (SA)</td>
</tr>
<tr>
<td>03</td>
<td>Link: Supporting to Primary Assets</td>
</tr>
<tr>
<td>04</td>
<td>Link: Generic Vulnerabilities to SA</td>
</tr>
<tr>
<td>05</td>
<td>Link: Threats to Supporting Assets</td>
</tr>
<tr>
<td>06</td>
<td>Evaluate: Risk</td>
</tr>
<tr>
<td>07</td>
<td>Assign: Controls (CTRL)</td>
</tr>
<tr>
<td>08</td>
<td>Report: Assessment Detail</td>
</tr>
<tr>
<td>09</td>
<td>Export: Finished assessment to the Central Repository</td>
</tr>
<tr>
<td>10</td>
<td>Review: Cross OFA / End to End scenario - PAs</td>
</tr>
</tbody>
</table>

[QUIT]
CTRL_S – Export screen

Security Assessment Summary Report Export

- Export PA to Template Format PDF
- Export PA short overview Excel
- Export PA overall impact Excel
- Export SA short overview Excel
- Export textual short overview RTF
- Export TH scenario overview Excel
- Export TH mitigated scenario overview Excel
- Export all data to single Excel

Close
SUPPORTING THE PROJECTS
• Awareness Material –
  • Explains the need for security

• Reference Material
  • What to do and how

• Coaching & Training
  Providing support in:
  • Applying the Reference Material
  • Performing Security Risk Assessments
Completed Risk Assessments

- Completed assessments being input into CTRL_S

<table>
<thead>
<tr>
<th>OFA Code</th>
<th>OFA Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>ENB02.01.01</td>
<td>SWIM</td>
</tr>
<tr>
<td>OFA01.01.01</td>
<td>LVPs using GBAS</td>
</tr>
<tr>
<td>OFA01.02.01</td>
<td>Airport safety nets</td>
</tr>
<tr>
<td>OFA01.03.01</td>
<td>Enhanced Runway Throughput</td>
</tr>
<tr>
<td>OFA03.01.04</td>
<td>Business and Mission Trajectory</td>
</tr>
<tr>
<td>OFA03.03.01</td>
<td>Ground Based Separation Provision in En Route</td>
</tr>
<tr>
<td>OFA04.01.02</td>
<td>Enhanced Arrival &amp; Departure Management in TMA and En Route</td>
</tr>
<tr>
<td>OFA04.02.01</td>
<td>Integrated Surface Management</td>
</tr>
<tr>
<td>OFA05.03.04</td>
<td>Enhanced ATFCM processes</td>
</tr>
<tr>
<td>OFA06.02.01</td>
<td>CWP En Route and TMA</td>
</tr>
<tr>
<td>OFA06.03.01</td>
<td>Remote Tower</td>
</tr>
<tr>
<td>OFA03.01.01</td>
<td>Trajectory Management Framework</td>
</tr>
<tr>
<td>OFA04.01.05</td>
<td>i4D and CTA</td>
</tr>
</tbody>
</table>
SESAR 2020
SESAR 2020 and ATM Security

• SESAR ATM Security Reference Material will be applied in SESAR 2020

• Re-packaging ongoing:
  • Simplified and bundled in function of the user
    • Each user can identify for each type of activity what is to be done
  • Built from existing materials + 2020 amendments
  • Compliant with 2020 principles (PMP) and put under change management
SESAR 2020 Supporting Documents

SESAR 2020

- SESAR 2020 Programme Management Plan
- Project Handbook (Enabling or Solution)
  - For Project Managers & Experts
- Transversal Activity Handbook
  - For Program Life Cycle
- Detailed methodologies & guidance
  - For domain experts using SESAR1 derived content such as checklists, user guides, templates, etc....

SESAR 1

SecRM Level 1

SecRM Level 2 +
ATM Security Research - Observations

In ATM

- ATM Security still relatively immature
- ATM moving into unfamiliar domain with high exposure to risk
  - more COTS products, connectivity, data sharing, ...
- Security viewed as a cost overhead rather than
  - an enabler for other KPAs (safety, capacity, cost effectiveness, ..)
  - the cost of doing business
- It is difficult to quantify a Return On Investment (ROI) for security
- In ATM there exists a general reluctance to engage with security
  - historically a trusting environment

In SESAR

- 16.06.02 helping many OFAs/projects to integrate security in their work:
  - Performing risk assessments, developing security cases
  - Enabling collaborative support

SESAR 2020

- Will apply the SESAR ATM Security Reference Material
- Currently preparing for commencement in late-2016
Selling umbrellas in the sunshine?
FAA: No, You Can't Take Down A Plane With An Android App

ASHLEY FEINBERG 13 APRIL 2013 11:45 AM

Remember how the internet got itself all riled up a few days ago when it found out that it would only take one rogue Android user to hack and take over an entire plane? Yeah, about that — it’s not true.

When Hugo Teso gave his demonstration at the Hack In The Box security conference, he used a PC-based ACARS (Aircraft Communications Addressing and Reporting System) to show how you could falsify data and adjust the heading, altitude, and speed of an entire aeroplane. The thing is, the vulnerabilities he exploited exist only in the PC-based training version of the software. The FAA has dismissed the claims in a statement released earlier.
Questions?

Thank you!