we see
we judge
Case Studies of Cyber-threats to Critical Infrastructures

Tutorial on the Cybersecurity of Safety-Critical Systems
Prof. Chris Johnson,
School of Computing Science, University of Glasgow, Scotland.
http://www.dcs.gla.ac.uk/~johnson
PARANOIA?
First Briefing
Understanding the Threats
Detailed patterns of attack.

Second Briefing
What can be done?
Protection, forensics and recovery.

Third Briefing
More detailed case studies…
Securing space-based assets.
Future of Systems Engineering in ATM...

- **Rise of COTS:**
  - Commercial off the Shelf components...
- The Internet protocol (IP).
- Voice over IP (VOIP).
- Linux
- Satellite Based Augmentation Systems...
NextGen Advanced Automation System

Five segments:
- Peripheral adapter module replacement item;
- Initial sector suite system (replace workstations);
- Terminal Advanced Automation System;
- Tower Control Computer Complex;
- Area Control Computer Complex.

1994 Contract restructured:
- $2.6 billion spent, $1.5 billion “wasted”.

Peripheral adapter module replacement works
• NextGen and the FAA heavily criticized.

“Unable to provide adequate contractor oversight, realistic cost or time estimates”.

“Pathological reluctance to benefit from engineering and scientific experience outside of the FAA”
2011 ERAM Update

• $2.1 Billion upgrade by Dec 2010:
  – En Route Automation Modernization.

• Faults lead to ‘missing’ flight plans;
  – Other aircraft change identity in flight;
  – Again cannot transfer flight data to Atlanta etc.
  – Undermines ATCO confidence in system;
  – ‘fallback’ original 20 year old IBM system
  – IBM contract expired, uses Jovial – rarely used.

• Test deployment to Salt Lake City:
  – FAA spend $14 million, still not working.
  – Salt Lake City simple compared to Chicago...
• Catch-22 problem:
  – The new system is behind schedule;
  – We identify problems in the old system;
  – If we make changes to the old system;
  – Must change new system so it can be integrated;
  – Even before the new system is finished…

• Pressure to maintain schedules:
  – FAA management ignores technical problems;
  – Did not budget time to address problems;
  – Through Earned Value Management program.
Lack of Regulatory Competence

- 2012 Federal employees.
  - 28.4% trained in Science, Tech, Engineering or Math;
  - 41.3% have a medical background…

- Regulatory crisis in Europe:
  - Lack of proper career progression;
  - Competition with Google, Amazon etc;
  - Recession leads to public sector pay freeze.

- Leads to regulatory lag in key areas…
The Future: SESAR Deployment Manager
Case Study: Space-Based Augmentation System

GPS/GLONASS? Satellites

Master Station

Reference Stations

GEO

Integrity & Ranging corrections

Augmented Navigation

SBAS message


Copyright C.W. Johnson, 2012
### ICAO SARPS high-level integrity requirements on Signal In Space

<table>
<thead>
<tr>
<th>Typical Operation</th>
<th>Horizontal Alert Limit</th>
<th>Vertical Alert Limit</th>
<th>Integrity</th>
<th>Time to alert</th>
<th>Continuity</th>
<th>Availability</th>
</tr>
</thead>
<tbody>
<tr>
<td>En-route</td>
<td>2 NM</td>
<td>N/A</td>
<td>1x10^-7 /h</td>
<td>15 s</td>
<td>1x10^-4 /h to 1x10^-8 /h</td>
<td></td>
</tr>
<tr>
<td>En-route (terminal)</td>
<td>1 NM</td>
<td>N/A</td>
<td>1x10^-7 /h</td>
<td>15 s</td>
<td></td>
<td>0.999 to 0.99999</td>
</tr>
<tr>
<td>Initial approach, NPA departure</td>
<td>0.3 NM</td>
<td>N/A</td>
<td>1x10^-7 /h</td>
<td>10 s</td>
<td></td>
<td></td>
</tr>
<tr>
<td>APV-I</td>
<td>40.0 m</td>
<td>50 m</td>
<td>1-2x10^-7 /app (150s)</td>
<td>10 s</td>
<td></td>
<td></td>
</tr>
<tr>
<td>APV-II</td>
<td>40.0 m</td>
<td>20 m</td>
<td>1-2x10^-7 /app (150s)</td>
<td>6 s</td>
<td>1x10^-6 /h in any 15s</td>
<td></td>
</tr>
<tr>
<td>CAT I</td>
<td>40.0 m</td>
<td>15-10 m</td>
<td>1-2x10^-7 /app (150s)</td>
<td>6 s</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
There Can Still Be Problems...

EGNOS is divided into four functional segments:

1. The ground segment is composed of the following stations/centres which are mainly distributed in Europe and are interconnected between themselves through a land network:
   - 34 Ranging and Integrity Monitoring Stations (RIMS), 27 being deployed, receiving satellite signals and sending this information to the MCC centres.
   - 5 MCC (control and processing centres) receive the information from the RIMS stations and generate correction messages to improve satellite signal accuracy and inform users about the status of the satellites (integrity). The MCC acts as the EGNOS “brain.”
   - 12 SES (stations that access the geostationary satellites): they receive the correction messages from the MCCs for the upload of the data stream to the geostationary satellite and the generation of the GPS-like signal. This data is then transmitted to the users via the geostationary satellite.
• Different reliability engineering techniques.

• EGNOS identified ‘threats’ using:
  – Fault Trees, Failure Modes Effects Analysis.
  – Human factors, common-cause studies etc.

• Assumptions include:
  – ICAO accuracy, integrity, continuity, availability;
  – Integration of HW/SW/human factors;
  – No single operator error would sacrifice integrity.
Security Threats to GNSS (1)

- Dec. 1997, New Jersey approach:
  - Continental trans-Atlantic loses GPS signals;
  - Intentional jamming attack?
  - US military test, 200km “interference zone”;
  - GPS antenna, 5-watt signal, steps frequencies.

- 2009 UK Ministry of Defence (MOD):
  - jamming over area of UK coastline;
  - disrupts integrated bridge systems/autopilot;
  - multiple alarms erode situation awareness;
  - shore-based Vessel Traffic Services lost.
• Pullen and Gao 2012.

• Understanding the nature of the threat:
  1. Deliberate jamming (possible but unlikely?);
  2. Accidental jamming (typically malfunctions);
  3. Unintended jamming (personal protection).

• Type 3 most common in practice.

• But provides a template for type 1 attack.
• Triggered GBAS continuity alarms.

• Investigation found regular interference:
  – Every workday morning and afternoon.

• Eventually the police were waiting:
  – Pulled over driver and confiscated equipment.

• Paradoxically aircraft more resilient:
  – Above limited interference zones from roads…
Newark Antenna Arrays for GBAS
• GBAS algorithms detect signal discontinuity:
  – Eager to reject signals from RFI of devices…

• Receivers only separated by 100m:
  – Vehicle takes out successive receivers;
  – Delay in recovering from interference;
  – Integrity monitoring filters must be restarted;
  – Lose resilience of multiple antenna arrays.

• Interference extends above decision height?
Newark rejected, so now had to show:
- Continuity, integrity, availability for CAT-1;

Block 0 software detects/excludes RFI:
- Shut down if signal lost to more than one receiver;
- But led to alarms and service interruptions;
- Long recovery before pseudoranges accurate…

Block 1 software modification:
- Allows brief interruption, but only 2 receivers;
- Assume vehicle will move down the road…
- Reduce integrity to increase availability????
Newark Case Study (Denial of Service)

• Newark rejected, so now had to show:
  – Continuity, integrity, availability for CAT-1;

• Not just software, hardware changes...

• Receiver 2 had highest RFI vulnerability:
  – Had been raised to reduce multipath effects;
  – Signals from satellites bounced off buildings;
  – Increased RFI from cars, reduced obstacle shielding;
  – So lower the antenna array...

• Plans to separate pairs of antenna up to 1km...
Revised Siting Houston, TX
Multi-constellation, Mask Low Angle GPS
Safety Case Structure for SES Integration

Part A: Design, Development and Deployment
(Prepared by: EC, ESA etc).

Part B: Operations and Maintenance
(Prepared by: ESSP).

Application Safety Case 1: Eg SES integration for en-route approaches to non-precision approaches (Prepared by: ESSP).

Application Safety Case 2: Eg Localizer Performance with Vertical Guidance approaches. (Prepared by: Individual ANSPs)

EGNOS Infrastructure Safety Case

Copyright C.W. Johnson, 2012

G1: EGNOS SBAS is acceptably safe


G2: all identified hazards with accuracy, integrity, continuity and availability have been eliminated or mitigated to an acceptable level.

C2: Hazards and ‘feared events’ identified according to the EGNOS end-to-end validation programme

G3: SBAS operations conducted according to agreed SOPs.

C3: EGNOS Safety of Life Service Definition Document European Commission, DG Enterprise and Industry Ref : EGN-SDD SoL, V1.0 also RTCA/DO-229D

G4: Hazards to accuracy have been mitigated.

G5: Hazards to integrity have been mitigated.

G6: Hazards to availability have been mitigated.

G7: Hazards to, continuity have been mitigated.

G10: SBAS ops will be conducted following practices in European Cooperation for Space Standardization; Space Engineering – Verification; ECSS-E-10-02A; 17 November 1998.

G11: SBAS ops meet detailed requirements in Single European Sky Certification of ESSP

S1: Initial tests on limited geographical areas

S2: Real-time monitoring of Signal-in-Space data

S3: Simulator data eg EGNOS End to End Simulator (EETES)

S4: Fault tree for EGNOS components

S5: Evidence of Conformance from Audit eg French NSA for EC, July 2010.

S6: Process evidence from ESSP teams

SC1: Localized jamming of GPS or spoofing invisible to ground stations.

SC2: Concerns over insider threat to EGNOS ground stations.

G8: Probability of deterministic failure < 10(-5) per service hour

G9: Probability of random stochastic failure < 10(-5) per service hour

CE1: Excessive multipath at RIMS level jeopardizes continuity

G8: Probability of deterministic failure < 10(-5) per service hour

G9: Probability of random stochastic failure < 10(-5) per service hour

G10: SBAS ops will be conducted following practices in European Cooperation for Space Standardization; Space Engineering – Verification; ECSS-E-10-02A; 17 November 1998.

G11: SBAS ops meet detailed requirements in Single European Sky Certification of ESSP

S1: Initial tests on limited geographical areas

S2: Real-time monitoring of Signal-in-Space data

S3: Simulator data eg EGNOS End to End Simulator (EETES)

S4: Fault tree for EGNOS components

S5: Evidence of Conformance from Audit eg French NSA for EC, July 2010.

S6: Process evidence from ESSP teams

SC1: Localized jamming of GPS or spoofing invisible to ground stations.

SC2: Concerns over insider threat to EGNOS ground stations.
G1 Information System is acceptably Secure

S1 Argument over System Security by considering Threats and Vulnerabilities

G2 System Threats are sufficiently addressed

Sn1.1 Penetration Testing Result

Sn1.x Honey Pot Analysis Result...

C1 Security Standards ISO 17799 etc

C2 Security Policy defined for Organization

G3 System Vulnerabilities are sufficiently addressed

Sn2.1 Vulnerability Mitigation Record

Sn2.x Vulnerability Database...

G4 Unidentified Vulnerabilities are effectively controlled

S2 Argument over unidentified System Vulnerabilities

Sn3.1 Security Requirements Document

Sn3.2 Security Standards/Policy

Sn4.x Operational Management Solution

G6 Security Requirements comply with Security Policy/Standards

G7 Operational Management are effectively controlled

Sn5.x Functional Test Result...

Sn6.x Functional Test Result...

Sn7.x Security Configuration Record

G8 System Behaviors comply with Security Requirements

Sn8.x Incident Handling Scenario...

G9 Authentication Functionalities comply with Requirements

Sn9.x DLP Solution...

G10 Access Control Functionalities comply with Requirements

Sn10.x Functional Test Result...

G11 Software Security Configurations comply with Requirements

G12 System Incident Handling complies with Requirements

G13 Data Protection mechanism complies with Requirements

G14 Auditing Functionalities complies with Requirements

Sn7.x Incident Handling Scenario...

Sn8.x Incident Handling Scenario...

Sn9.x DLP Solution...

Sn10.x Functional Test Result...

S3 Argument over Security Functionalities
Many things are changing in ATM.

SESAR and NextGen –
  – Teething pains in development phase…
  – Enough good ATM engineers?
  – Can we keep old systems going?

How much do ops need to know?

Rise of COTS:
  – Commercial off the Shelf components…
Schedule

First Briefing
Understanding the Threats
Detailed patterns of attack.

Second Briefing
What can be done?
Protection, forensics and recovery.

Third Briefing
More detailed case studies…
Securing space-based assets.
Any Questions?