ATN Security

Simon Blake-Wilson
BCI / FAA ACB-250
sblakewilson@bcisse.com

Agenda

- Wireless Security – Cautionary Tales
- ATN Security
- ATN Security – Open Issues
- Conclusions

Goals: To delve deeper into the issues raised in the ICAO letter, and to encourage AEEC to work on these issues.

Disclaimer: Questions about FAA policy will be deferred!

Wireless Security – Common Theme

With every wireless security solution:

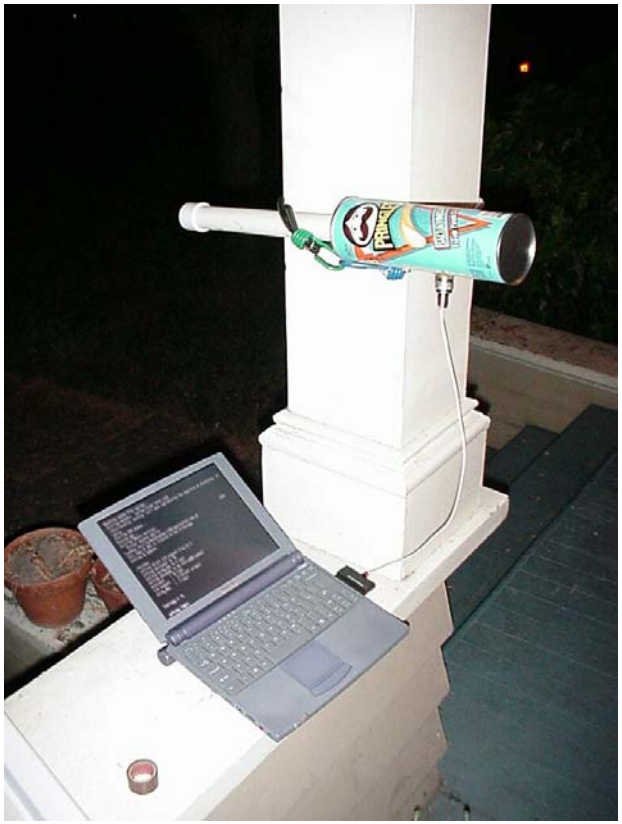
- "We don't need security"
- "Security is too expensive"
- "I've got a much cheaper (proprietary) solution that doesn't have bells and whistles, but is good enough"
- "We'll get the RF side working first, then we can come back and add security"

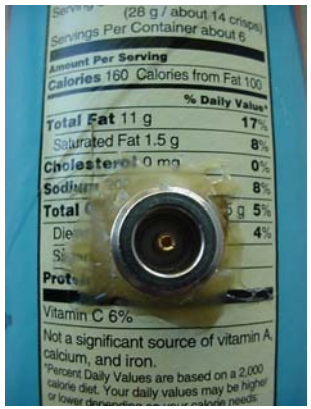
Wireless Security Examples - Cellular

Historically cellular networks have experienced large amounts of fraud. The device below is designed to monitor cellular traffic. It is owned by the UK Police and used to track suspects. In different hands, it could place fraudulent calls and the like.

Wireless Security Examples - WLAN

The WLAN WEP protocol is easy to crack. The result: “war driving”, “war chalking”, and some new “dual-use” goods.





Wireless Security – WLAN (cont)

WLAN security problems have already generated publicity concerning the use of WLAN is aeronautical environments.

Alaska Air Launches Wireless Check-in

Using free software on handhelds, travelers can check in, go directly to gate

Wireless LANs: Trouble in the Air

By Bob Brewin, Dan Verton and Jennifer DiSabatino
(Jan. 14, 2002) As the airline industry scrambles to meet a Jan. 18 deadline to screen every checked bag for explosives, security experts, analysts and government officials are raising serious concerns about the security of wireless technology that's integral to the effort.

Airport checks vulnerable to hackers, experts say

Carrie Kirby, Chronicle Staff Writer

Terrorist hackers could exploit wireless networks used to check baggage at major airports -- including San Jose's -- according to network security experts.

tion by airlines of industry-standard 802.11b, or Wi-Fi, wireless LANs
GHz band. These systems, which are widely viewed as inherently insecure,
ıpport such applications as bag matching and curbside and roving-agent

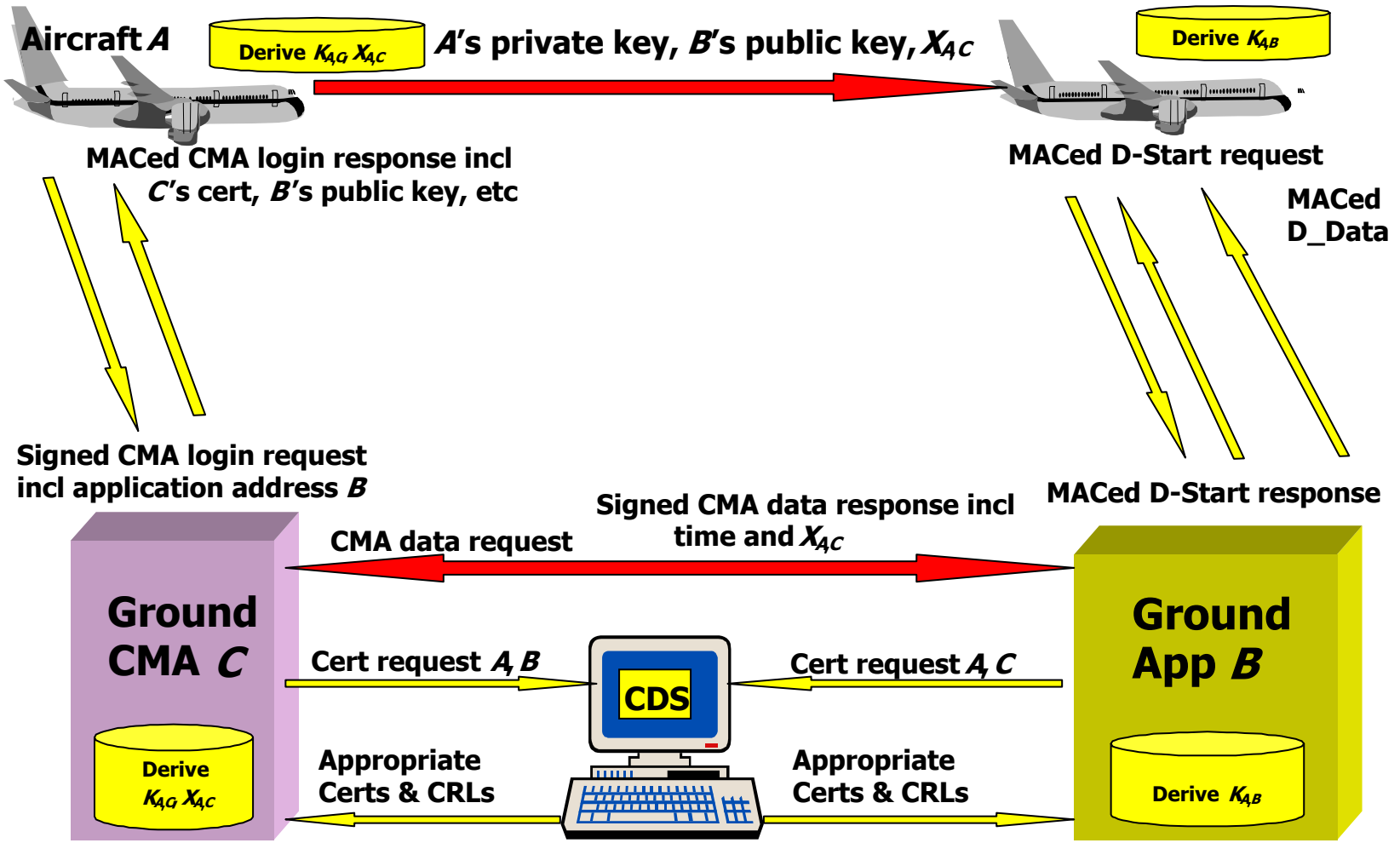
ır to be justified, based on two investigations that were conducted last week
ırity firms that analyzed airline wireless LAN systems at Denver International
e International Airport.

Wireless Security – Lessons Learned

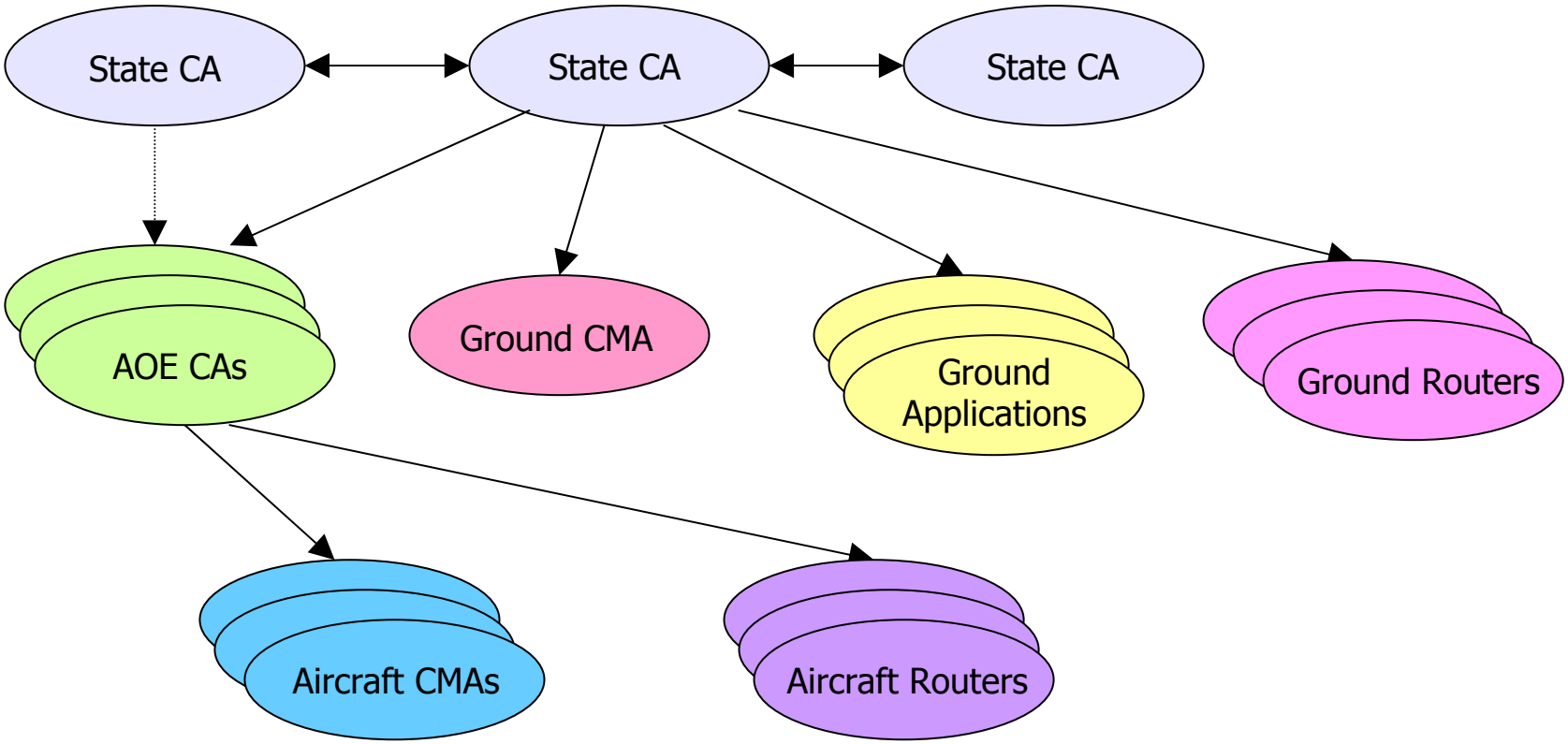
There are significant benefits when you:

- Value flexibility and resiliency as design goals
- Use open, publicly-scrutinized protocols
- Provide a design that scales down to today's needs rather than scales up to tomorrow's.
- Integrate security throughout your deployment plan

ATN Security - Overview



ATN Security - PKI



States and aircraft operating entities encouraged to share CAs.

ATN Security – Current Status

- Security added to ATN SARPS Edition 3 – published in 2002.
- Security implementation guidance recently completed.
- Some validation of security features performed:
  - FAA, NASA, and Germany implemented ATN Cryptographic Schemes.
  - Honeywell and OKI implemented Certificate Authority for PKI.
  - FAA implemented Ground-Ground IDRP Security.
  - French implemented Upper Layer Security.
  - French implemented Air-Ground IDRP signaling mechanisms.
- Current validation conclusion: core security operations available in COTS products
- Ongoing work to add encryption support

ATN Security – Design Overview

Some comments on the ATN Security design:

- Design focused on addressing issues identified in Eurocontrol risk analysis
- A number of other potential solutions were considered: hop-by-hop, Kerberos, symmetric with manual key management, etc
- Flexibility – new security services can be added without going back to the drawing board – e.g. encryption
- Flexibility – new algorithms can be added within the solution framework
- Flexibility – solution can be applied to environments other than ATN, and PKI re-used

ATN Security – Open Issues

ICAO and ATNP had a specific remit and a number of issues fell outside both the remit and expertise present:

- How private keys and certificates are loaded
- How CA public keys are loaded
- Making cross-certification painless
- Certificate Distribution Service
- Nailing down the PKI architecture
- Development of CP and CPS templates

ATN Security – Open Issues (cont.)

There are a number of options for how private keys and certificates are loaded:

- Load during manufacture
- Load during maintenance cycle
- Bulk certificate requests
- Onboard key generation vs centralized key generation
- Technical standards: PKCS, PKIX, and the alphabet soup
- Security of loading process

Standards in this area will facilitate interoperability between avionics and Certificate Authorities.

ATN Security – Open Issues (cont.)

Similarly there are a number of options for how CA public keys are loaded:

- Load during manufacture
- Load during maintenance cycle
- Emergency load process outside maintenance cycle
- Load format – self-signed cert vs identity and key
- Security of loading process

As before standards in this area will facilitate interoperability between avionics and Certificate Authorities.

ATN Security – Open Issues (cont.)

Cross-certification – “we can do it the easy way or the hard way”:

- Liability issues
- Cross certification request formats
- Standards for how information is expressed in CP and CPS
- Standards for CP and CPS baseline requirements

Easy, automated cross-certification is needed to make the ATN PKI work.

ATN Security – Open Issues (cont.)

Certificate distribution is often a challenge in PKI:

- Directory or not
- X.500, LDAP, Microsoft, etc
- Directories and certificate chaining
- Border directories
- Bilateral vs multilateral agreements

Agreements in this area will save so much time.

ATN Security – Open Issues (cont.)

SARPS left a number of options for the PKI architecture:

- CA sharing
- CA outsourcing
- CAs hosted by airlines
- RAs hosted by airlines
- Certification of airline CAs by multiple States

ATN Security – Open Issues (cont.)

At the heart of many of these issues – the CP and CPS:

- CP and CPS document the policies and procedures used by CA
- SARPS require use if IETF PKIX framework – enables easier comparison of provisions made by different CAs
- Makes sense to develop baseline CP and CPS provision for ATN and aeronautical to capture the issues raised and more:
  - Baseline certificate request process
  - Baseline directory support
  - Baseline certificate revocation standard
  - Baseline audit and archival stipulation
  - Etc

Conclusions

- ATN security solution is a strong design, ready today
- Re-use of the ATN security solution is other environments is possible and will enable cost-savings and migration path
- Like any security standard, ATN security solution must be worked early and integrated into deployment plans
- A number of issues have been left open and AEEC seems like a natural candidate to work the issues