Testing Document Readers to the limit

The active display attack
Black-Box Testing of ABC Systems
EMP vulnerability report

Franz Daubner et al.

High-Performance Image Processing
Safety and Security Department
AIT Austrian Institute of Technology GmbH, Austria

franz.daubner@ait.ac.at
Active display attack

- Automated Border Control (ABC) systems
- Important aspect – identity document / document reader
- Unattended operation of the document reader necessary
- Opens up new attack scenarios
Active display attack
Active display attack

Light source → Display → p₂ → Anti-reflex coating

Lightsource → Camera
Active display attack

- It works!
- Off-the-shelf hardware can be used
- Will be an issue with wider deployment of ABC Gates
Document simulator

- Automated Border Control (ABC) systems
- Important aspect – identity document / document reader
- We need quality assessment of passport readers and software!
- Testing – very tedious
- Simulate documents for automatic testing
Exploit inherent “weakness” of state-of-the-art passport readers

Allows for
- Black-box testing of whole ABC gate
- Automated simulation of large quantities of passports
- Testing robustness against the active display attack

Simulator running on dedicated hardware
- 7“ full-HD display
- Small CPU board
- photo diode
- Wi-Fi access point
Usage scenarios
Simulator demo (Video)
Results

Original

Simulation
Conclusions

- The simulator can simulate all optical security features currently checked by state-of-the-art document readers (provided accurate calibration of the simulator)

- The simulator allows for simulating a broad range of documents as well as various effects determining apparent document quality on a range of document readers
Future work

- Reconsider requirements for passport readers
  - How big deviations from normal should be reliably detected by a reader?
  - How big errors are still acceptable and allowed to pass?

- Reconsider security features for optical document security
  - Automated verification of security documents becomes inevitably more and more important
  - Most security features are not designed with automated verification in mind
Investigation of the Vulnerability of Electronic Document Readers to High Power Electromagnetic signals

- What are electromagnetic threats?

- IEMI…Intentional Electromagnetic Interference
Motivation to use IEMI sources to attack ABC Systems

- Criminals want to blackmail providers of critical infrastructures and/or governmental institutions
- Attackers want to bypass security zones by disturbing border control systems
- Terrorists want to immobilize the critical infrastructure airport
- Curiosity, some individuals in the society want to create chaos and so they see distortion of electronic components at an airport as a challenge
Results

- Multiple disturbances, but no destruction of the electronic passport readers were observed in our tests
- Many disturbances made a manual reset of the devices necessary – need for skilled staff in order to re-establish routine procedures

- Highest sensitivity of both devices was found below 1 GHz

- In particular below 1 GHz disturbances can be induced by using small handheld IEMI sources – such systems can be easily hidden and do not require high qualified users
Results: Type of disturbances

- Interference: passport readers re-establish routine operation without external intervention

- Upset: external intervention is required in order to re-establish routine operation

<table>
<thead>
<tr>
<th>Errors</th>
<th>Effect during exposure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interference (no reset required)</td>
<td>• No picture, distorted picture&lt;br&gt;• No Machine Readable Zone (MRZ)&lt;br&gt;• RFID could not be read out</td>
</tr>
<tr>
<td>Upset (Reset necessary)</td>
<td>• USB disconnect&lt;br&gt;• Software error (crash)</td>
</tr>
</tbody>
</table>
Conclusion

- The campaign has shown that it is possible to disturb electronic passport readers with both pulsed and CW signals at various frequencies.

- Consequences of manipulated document readers on the ABC system?
  - loss of time, chaos on the airport, reduction of security at control point

- Measures to protect critical infrastructures against IEMI are required

- We have only looked at a part of the whole system!
Franz Daubner

High-Performance Image Processing
Safety and Security Department
AIT Austrian Institute of Technology GmbH, Austria

franz.daubner@ait.ac.at