Safety and Security
As Things Join the Internet

Presented by Mitch Trope - 15 February 2016
Legalese

• This material is Copyright © 2016 Garmin Ltd. or its subsidiaries
• All rights reserved
• Use within the context of EECS 700, Spring 2016, is permitted
• Copying and redistribution prohibited
MARKETS WE SERVE
AVIATION

Our industry-leading aviation technology has made the skies progressively easier to navigate. From portables to panel-mounts to integrated glass flight decks, and everything in between, Garmin innovation is modernizing the way people fly. Human factors testing ensures advanced Garmin avionics are a seamless extension of the pilot.

OEM, aftermarket and portable avionics for:

- Airplanes
- Helicopters
- Sport Aircraft

Category Highlights:
- Satellite weather, traffic, terrain and situational awareness
- Nav/Comm, transponders, indicators, instruments, and autopilot
- Complete ADS-B solutions
A Message From Our Co-Founder

• “The product is everything.” –Gary Burrell (the Gar in Garmin)

• In 1989, a “product” was just a physical device

• He’s still right, but the definition of “product” is now significantly different

• The whole ecosystem surrounding a device is included in “product”
The Market Demands Increased Connectivity

• Expectations are that everything can share data
  • ...with everything else
  • ...at any time

• Consumers get frustrated when systems don’t meet expectations

• “It should be easy”
Adding Connectivity Adds Risk

• Designs of older devices assumed they were isolated
  • No access control was necessary
  • Simple assumptions for availability, integrity, confidentiality

• Adding connectivity offers a persistent path for access

• The consequences of adding connectivity need to be assessed
  • Not all risks, threats are equal
  • Think about safety risk and business risk
General Attributes Of a System

• Availability – the system lets me do what I want, when I want
• Integrity – the system behaves correctly and provides expected outputs for given inputs
• Confidentiality – the system ensures data is only available to those authorized to use it
• Safety generally only concerned with Availability and Integrity
• Security concerned with all three
Safety Risk: Functional Hazard Assessment

• Failures cause failure conditions (condition with impact on vehicle) which can create hazards (potentially unsafe state)
• Various assessment methods define severity and likelihood of potential failure conditions
• Loss of function and misleading information may have different classification (misleading information is generally worse)
• Failures must be mitigated such that the risks are acceptable

# Safety Risk: Failure Classification

<table>
<thead>
<tr>
<th>Severity</th>
<th>No Safety Effect</th>
<th>Minor</th>
<th>Major</th>
<th>Hazardous</th>
<th>Catastrophic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operator Impact</td>
<td>No effect on safety</td>
<td>Slight increase in workload</td>
<td>Significant increase in workload</td>
<td>Excessive workload preventing task completion</td>
<td>Multiple fatalities or loss of system</td>
</tr>
<tr>
<td>Occupant Impact</td>
<td>N/A</td>
<td>Some physical discomfort</td>
<td>Physical distress including injuries</td>
<td>Serious or fatal injury to some occupants</td>
<td>Multiple fatalities or loss of system</td>
</tr>
<tr>
<td>Acceptable Likelihood</td>
<td>1</td>
<td>1 in 1,000</td>
<td>1 in 100,000</td>
<td>1 in 10,000,000</td>
<td>1 in 1,000,000,000</td>
</tr>
</tbody>
</table>

Source: FAA System Safety Handbook, Chapter 3
Business Risk: Legal and Contractual

- Legal obligations
  - Federal Trade Commission regulations
  - State consumer protection laws and regulations
  - Criminal and/or civil penalties for violations
- Contractual obligations
  - PCI (Payment Card Industry) requirements for credit card payments
  - Intellectual property protection – especially 3rd party IP
  - Accurate accounting and payment
  - Contracts govern penalties for violations
Business Risk: Visibility

- Damage to brand due to a security breach
- Brand becomes associated with “poor quality”
- Regaining customer trust can be a long process
- Breach on a “flagship” product is worse than a “fringe” product
  - Market leader in a category has the most exposure
  - Consider strategic importance of a product or service
Assessing Risks and Threats: Entry Points

- Connectivity – cellular, Wi-Fi for Internet accessibility...
- Other wireless radios – Bluetooth, ZigBee...
- Wired access – USB, Ethernet, CAN...
- Removable storage – SD Card, External SATA...
- Operating system – custom RTOS, Android, Linux, VxWorx...
- Physical access to device internals
Assessing Risks and Threats: Targets

- Physical consequences
  - "Cyber-physical systems" such as vehicles, control systems
- Connected systems – “trampoline” to something else
- Financial transactions
  - Downloadable pay-for content
  - Credit card data
- Stored credentials – Google, Facebook, Wi-Fi
- Personally identifiable information
  - Current or past location
  - Biometric data
**Information Flow**

- Understand how your system must exchange information with other systems
- Information flows between systems are trust boundaries
- Information flows between different layers of integrity or confidentiality are trust boundaries
- The edge of your system is the “security perimeter” you need to defend
- The sources and destinations of information are your “assets”
**Risk Acceptance**

- Determine if the risk posed by the threats against your assets is acceptable.

- How can the identified threats cause the device to:
  - Stop performing its intended function.
  - Perform some unintended function (possibly to the hardware limits).
  - Mislead the user or other connected system.

- Unacceptable risks must be mitigated to an acceptable level.
  - For safety risks, the thresholds are well defined.
  - For business risk, it’s highly dependent on the business environment.
Security Measures

• With the perimeter, assets and threats defined, security measures can be designed and implemented to address risks

• Consider publically available guidance where appropriate
  • NIST publications on crypto algorithms, key lengths

• Effective security measures mitigate the vulnerabilities against failures caused by the threats you’ve identified
Looking For Changes

- The security environment is not static
- Moore’s Law means “computationally infeasible” doesn’t last long
- New attacks are demonstrated on systems and algorithms
- Private key or certificate compromise
- Understand how long you need to maintain the security attributes of your system

CHANGE
WE CAN BELIEVE IN
Looking For Changes

• Monitor the environment for evidence of change
  • Public databases like CVE hold information on commonly used products and technologies
  • Customer or field quality issues
  • Design in necessary logging mechanisms and a way to retrieve the logs
• Specific notification mechanism for use by security researchers
Process Assurance

• Amount of necessary rigor governed by the risks posed by an error

• Process assurance
  • Ensure you get a good design by applying the proper amount of rigor to evaluating your design
  • Good process assurance mitigates design errors
    • Common mode failure
    • Design process may reveal the need for dissimilarity

• Validate and verify
Design Assurance

• Process governs taking requirements and ensuring implemented product meets the design requirements

• Product performs intended function

• Product does not contain unintended function

• Ensure the product performs in its intended operational environment
Incident Response

• Speed and scope of the response to a security incident depends on the severity of the incident
  • Determine if use of the product needs to be halted
  • Determine the technical remediation path
  • Manage communications with the public
• Consider incident response during product design – how will you update your device?
• Leadership – direct resources toward remediation as needed
• Engineering – perform remediation
• Communications – set and manage public expectations
Case Study: A Household Thermostat

- No heat in winter is a safety risk
  - Utilities not permitted to cut off gas or electric service during winter
- Old mechanical thermostats had well-understood failure modes
- Standalone solid state digital thermostats:
  - Provide scheduled control to save energy (and therefore money)
  - New failure mode: drained batteries lead to loss of heat
  - Mitigations: slow, constant current draw with low voltage user alert threshold
Case Study: A Household Thermostat

- Connected digital thermostat
  - More precise “occupied or not” environmental control
  - Remote monitoring and adjustment
  - Variable power usage
- New threats for new features
  - Unauthorized user could adjust temperature
  - Unauthorized user could determine if someone is home or not
- New threats may cause old failures
  - Have we created a way for an unauthorized user to draw down the battery?
Case Study: A Household Thermostat

- We’ve already established loss of heat is a safety issue
- We’ve already established loss of battery power can cause loss of heat
- Therefore, we must:
  - Mitigate the risk of design or implementation errors that can cause loss of battery power
  - Mitigate the risk that an attacker can cause loss of battery power
Case Study: A Household Thermostat

• What on our thermostat can consume a lot of power, quickly?
  • Design should ensure that we meet a power budget and monitor for possible issues

• What on our thermostat can be misused to consume a lot of power?
  • Could an attack force the CPU to run at its fastest setting?
  • Could an attack keep the display and/or backlight on full time?
  • Consider what impact specific countermeasures have on the rest of the system
“Life was simple before World War II. After that, we had systems.”

—RADM Grace Hopper
For Further Reading

• FAAAC 23.1309-1E, “System Safety Analysis and Assessment for Part 23 Airplanes”
• FAAAC 119-1, “Airworthiness and Operational Approval of Aircraft Network Security Program (ANSP)”
• FAA System Safety Handbook
• RTCA DO-356, “Airworthiness Security Methods and Considerations”
• SAE ARP 4754A, “Guidelines for Development of Civil Aircraft and Systems”
• SAE ARP 4761, “Guidelines And Methods For Conducting The Safety Assessment Process On Civil Airborne Systems And Equipment”
Do you want to help make “things” safer and more secure?

Anita Finn – Garmin recruiter for KU
Anita.Finn@garmin.com
Questions?

Thank you!