

# Cyber Threats in Aviation

ANY LESSONS FROM OTHER INDUSTRIES EXPERIENCE WITH CYBER?

*Dr. Stefan Frei*

*Security Architect at Swisscom, Lecturer at ETH Zurich*

*frei@techzoom.net Twitter @stefan\_frei*

With special thanks to

*Gallus Bammert, Aviation Expert, FI*

*Christ Roberts, CTO One World Labs*

# Abstract

- With the rise of the internet and the increasing dependence of our society and economy on communication technologies, cyber security has become critical issue for all types of businesses. In just two decades, various industries were confronted with fundamentally new types of threats, threat actors and dynamics.
- This talk first addresses the peculiarities of the cyber security field and what the software industry had to painfully learn in the past decades in order to adapt to these new threats. To understand the cyber landscape and how it affects aviation we classify threat actors and explain global developments that critically impact the security (such as interdisciplinary, complexity, miniaturization, diversity of the crowd, price erosion, dynamics of the security community, ...). Based on the realization that cyber security is a complex adaptive system (CAS), rather than a simple technological issue, we highlight fundamental properties of a CAS that help us understand future threats, design effective security, and to identify ineffective security approaches.
- In part two the talk examines how the aviation industry and authorities handled safety and security issues in the past 100 years – and challenges the applicability of these processes to address current and future cyber threats. We show how previously secure and isolated aviation systems become critically exposed and identify security assumptions that are prone to fail in the present cyber landscape.
- The talk concludes with key lessens learned by other industries and how these can be applied to the aviation sector. Recommendations on the organizational, system design, and technical level are given in the hope to create awareness and avoid preventable issues with cyber security in aviation. For many of the challenges solutions already exist – let's get them implement before they get exploited.

# Cyber Security

- Cyber security has become critical issue for all types of industries
- But in many aspects, cyber security differs fundamentally from past challenges



# Recent Cyber Security Incidents in Aviation

- Chris Roberts – 2015  
*Manipulation of EICAS messages from passenger seat*  
<http://bit.ly/EICASHack> (Reuters)
- Ruben Santamarta – 2014  
*Backdoors and remote control of SatCom Military & Civil Aviation radios*  
<http://bit.ly/SatComHack> (Paper)
- Hugo Teso – 2013  
*Remote manipulation of FMS through ACARS*  
<http://bit.ly/FMSHack> (Forbes)

# Technology & Innovation

In just two decades, new technologies and the Internet transformed society and businesses alike

We had little time to learn or adopt – as individuals, society or industry

We have to adapt to permanent change and high dynamics



1 Million Years



50 Years



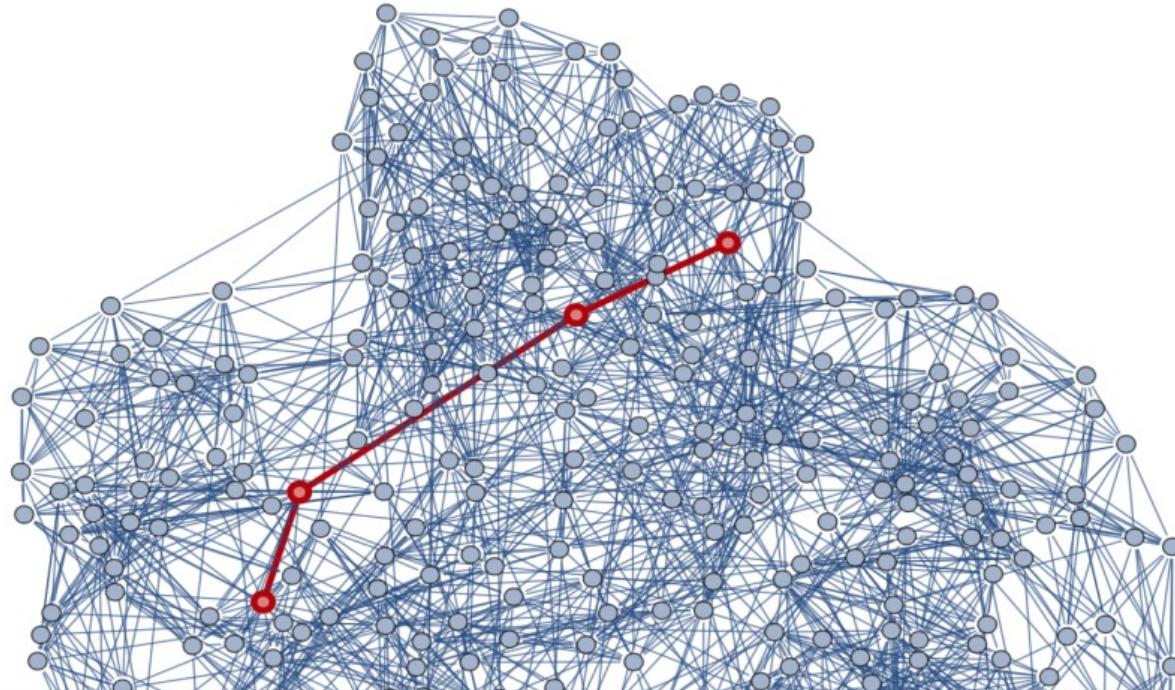
# Actors & Attackers

Attacker	Objectives	Resources	Proceeding
Nation States, Agencies	<ul style="list-style-type: none"><li>Information</li><li>Fighting Crime/Terrorism</li><li>Espionage</li><li>Sabotage</li></ul>	<ul style="list-style-type: none"><li>Enourmous financial resources</li><li>Focus on result, not cost</li></ul>	<ul style="list-style-type: none"><li>Build &amp; buy know-how</li><li>Persistent &amp; well hidden attacks</li><li>Subversion of supply chain</li></ul>
Terrorists	<ul style="list-style-type: none"><li>Damage</li><li>Attention</li><li>Manipulation of politics</li><li>Fear Uncertainty and Doubt (FUD)</li></ul>	<ul style="list-style-type: none"><li>Considerable financial resources</li><li>Potentially large network of supporters</li></ul>	<ul style="list-style-type: none"><li>Buy know-how on black market</li><li>Physical attacks</li></ul>
(Organized) Crime	<ul style="list-style-type: none"><li>Financial</li></ul>	<ul style="list-style-type: none"><li>Business</li><li>Make money on long term</li><li>Profit/loss driven</li></ul>	<ul style="list-style-type: none"><li>Existing gangs</li><li>Per case groups of specialists</li><li>Bribery</li></ul>
Hacktivists, Groups	<ul style="list-style-type: none"><li>Mass attention</li><li>Damage</li><li>Denounce vulnerabilities in systems/organizations</li></ul>	<ul style="list-style-type: none"><li>Minimal financial resources</li><li>Large reach</li></ul>	<ul style="list-style-type: none"><li>Highly motivated amateurs &amp; specialists</li><li>Develops unpredictable momentum</li></ul>
Vandals, Skript Kiddies	<ul style="list-style-type: none"><li>Fame</li><li>Reputation</li></ul>	<ul style="list-style-type: none"><li>Minimal financial resouces and know-kow</li></ul>	<ul style="list-style-type: none"><li>Available tools</li></ul>

# What makes the cyber world special?

- Communication between people, machines and devices
- Increase of computing performance
- Price erosion
- Software eats the world

# Network of People, Devices, and Services



The increasing number of new ways of interaction also create novel attack paths which are **not predictable by definition**



# Complex Adaptive System (CAS)

- **Connectivity**

A decision on one part will affect all other related parts

- **Co-Evolution**

Elements can change based on their interaction between one another and the environment

- **Sensitive Dependence**

Sensitivity to initial conditions (non-linearity, cascades)

- **Emergent Order**

Potential for emergent and unpredictable behaviour

# Strategies to Handle Unpredictability

## Men

- Predict and model risks

Prevent Shocks

- Relies on **accuracy** of models and **probabilities**
- Optimization:  
short term gain, efficiency

> **fragile**

## Nature, Evolution

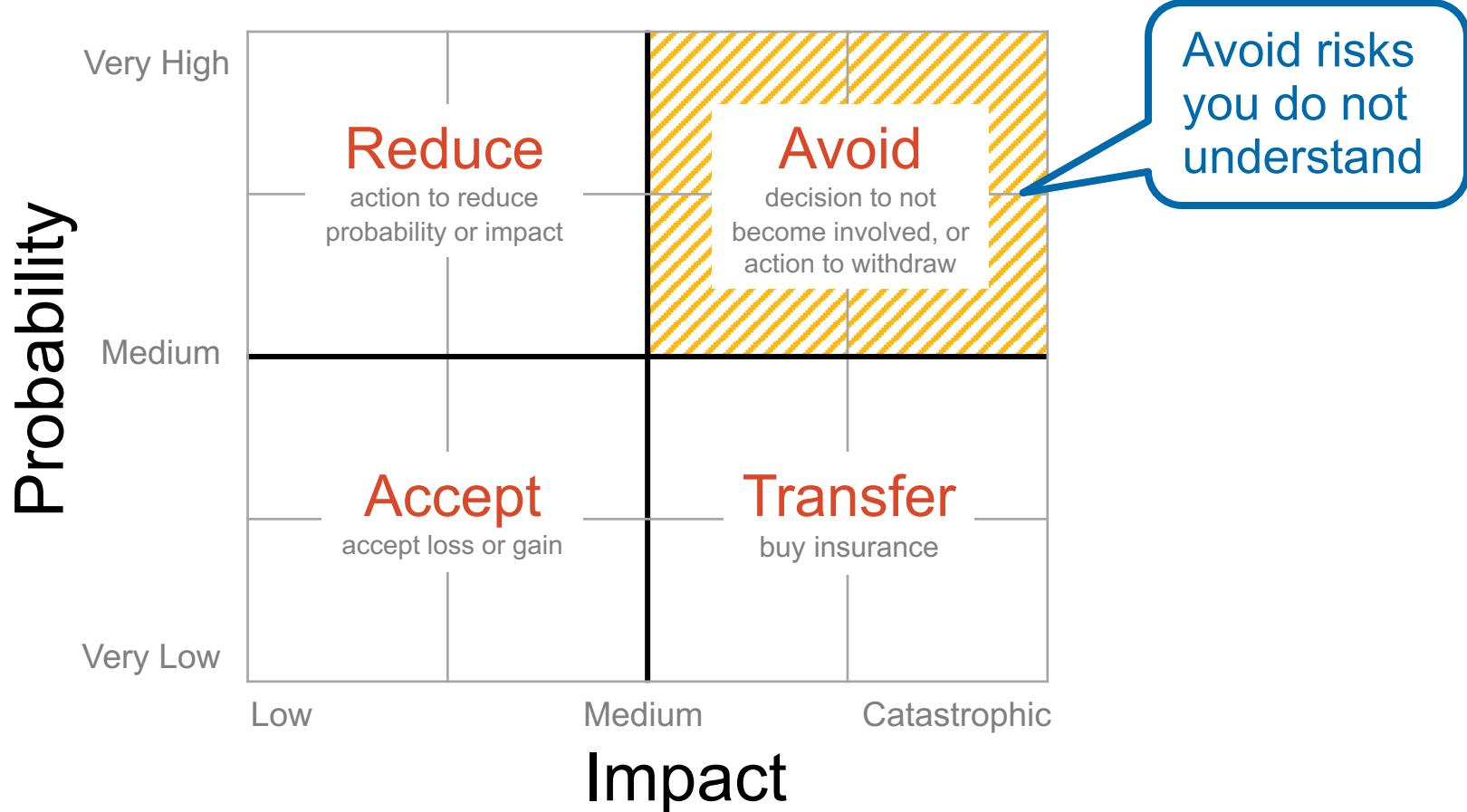
- No attempt to predict risks

Absorb Shocks

- Relies on **redundancy** and **robustness**
- Absorbtion:  
long term survival, diversity

> **anti-fragile**

# Dealing with Risks



"It is better to take risks you understand than to try to understand risks you are taking."

Nassim N. Taleb, Author of *The Black Swan*

# Unnecessary Risk Taking

- Do not connect a critical system to the outside unless you know exactly what the consequences are
  
- Is connecting the inflight entertainment bus to the flight control bus worth the risk?
- Can you even assess this risk?
- Are these systems truly separated?
- You are about to give passengers and the Internet access to control systems (ask Fiat/Chrysler)

# complexity

- complexity and interaction between systems is growing continuously
- complexity is the worst enemy of security

# Innovation & Price Erosion

- Continued miniaturisation and price erosion
- Todays transisors are **90,000x** more efficient and **60,000x** cheaper than 1971
- A car today would cost **USD 0.25** and consume **0.2 ml/100 km** of fuel

# Innovation & Price Erosion

Inexistent or previously unavailable technologies become common goods

Software Define Radio



USD 500'000.-



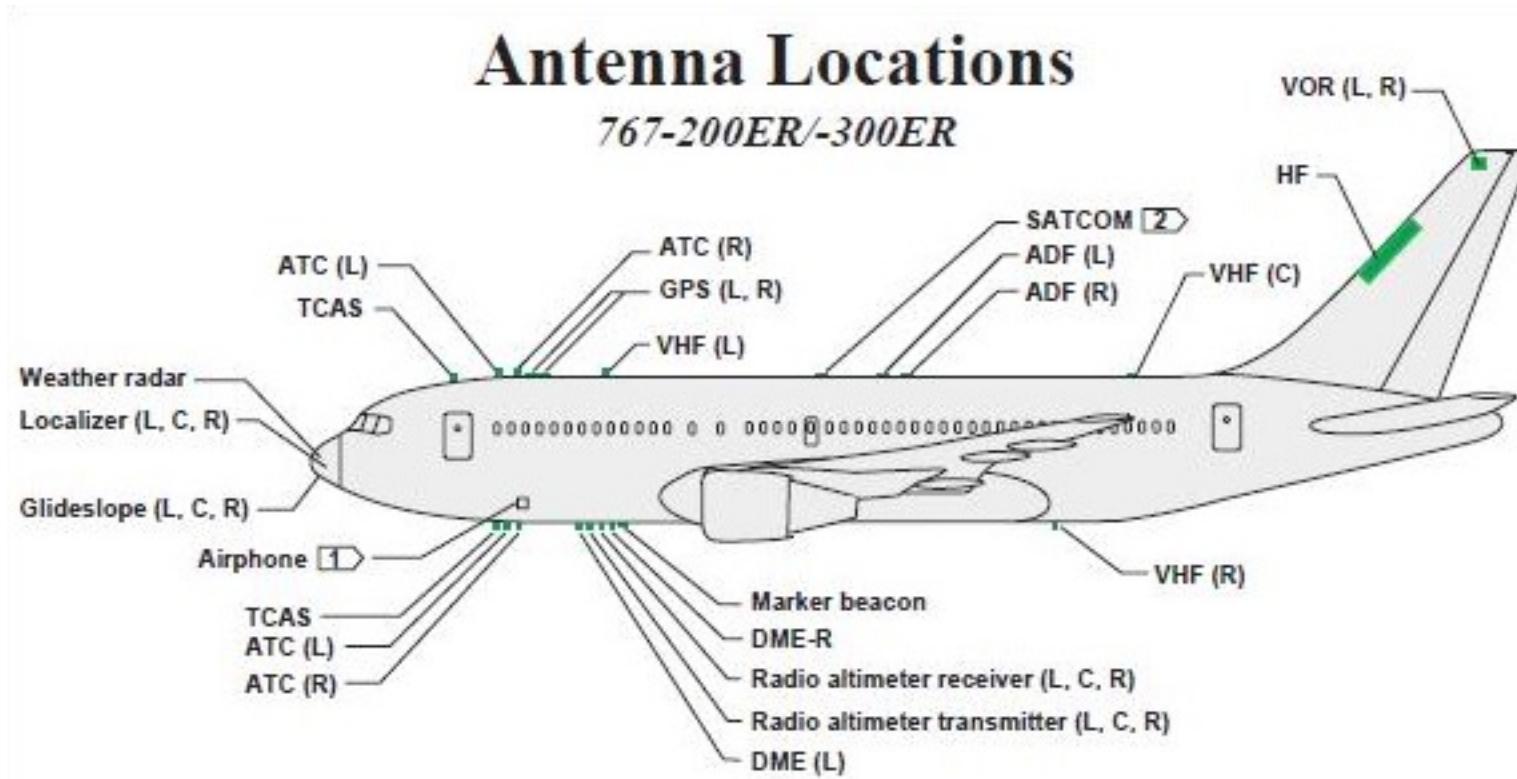
15 Years



USD 500.-

Revalidate security assumptions based on the  
(A) limited availability, (B) unaffordability, or  
(B) limited performance  
of a technology

# Playground for Software Defined Radios (SDR)



- Consider all radio communications and protocols as critically exposed

# today

attackers can afford functionality and tools that were beyond their reach a decade ago

# Software Complexity and Aviation

## Facts

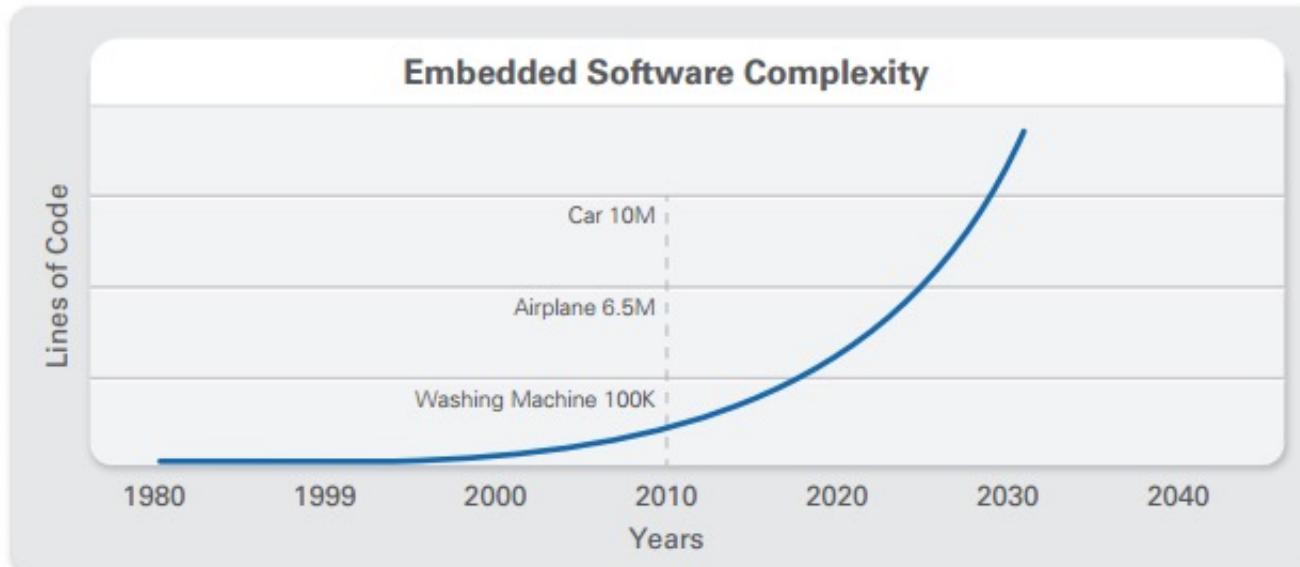
- Software complexity is increasing
- There is no secure software

## Thus, we need to

- handle **vulnerabilities**
- deploy **software updates** efficiently
- systematically test **the security** of critical systems

# Software Complexity is Increasing in all Industries

- Flight software lines of code (LOC) increases **10x** in ten years
- Functionality provided by software to pilots has grown from **8% to 80%** from 1960 to 2000
- Airbus A380 estimated to have **180 Million LOC**  
Windows OS **50 Million LOC**



# Aviation Systems Are Not Prepared



## Internet Computer

- Networked and continuously hardened in battle
- Designed to withstand **external threats**
- Exploit mitigation, antivirus, frequent security updates



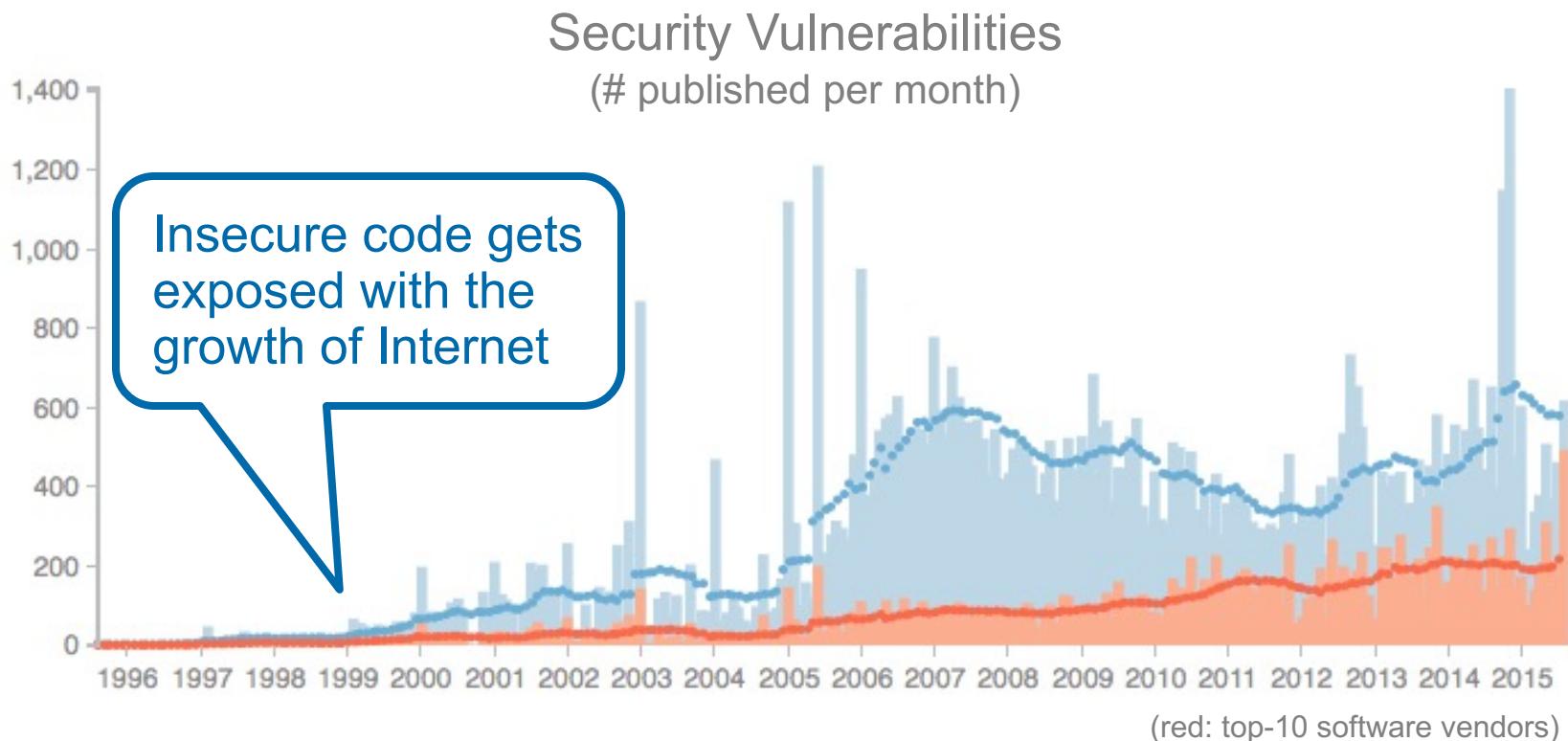
## Aviation Computer

- For decades systems ran isolated
- Designed for **high availability, not security**
- Old code, no protection, no/few security updates

- Today's aviation systems were designed in a time when the cyber threat landscape was tame

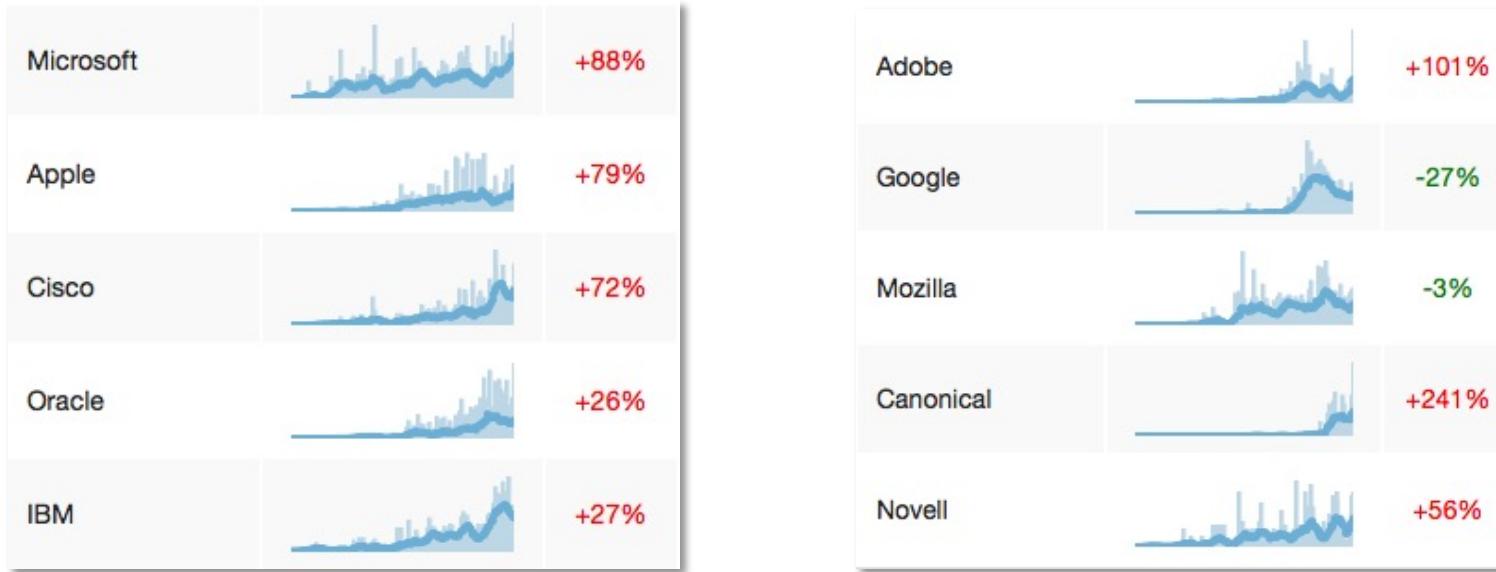
# There Is No Secure Software

In spite of increased investment, the software industry at large is still unable to produce secure code



# Software Complexity & Security

Only two of the top-10 software vendors reduced vulnerabilities over 5 year period - *they employ the best computer scientists and engineers*



- We need to handle and fix software vulnerabilities - and deploy updates effectively

# Cyber Security Testing ≠ Compliance Testing

- We need to systematically test aviation systems against cyber threats
- Compliance **does not imply** security

Internal Testing	External Testing
<ul style="list-style-type: none"><li>• Constrained, biased</li><li>• Uninspired, lack of diversity</li><li>• Experts in compliance and availability testing</li></ul>	<ul style="list-style-type: none"><li>• Independent, unconstrained</li><li>• Unbiased, creative, diversity</li><li>• Experts in breaking systems</li></ul>

- Aviation industry needs their systems tested by external experts (including complete aircraft, not only isolated components)

# You Discovered a Vulnerability – What Do You Do?

## Keep it secret?

- *Prevents independent risk assessment*
- *Assumes that security information can be kept secret*

## Report to Vendor?

- Vendor might collaborate and fix problem
- *Vendor might downplay, threaten you, or ignore the problem*



## Full Disclosure?

- Helps public to assess risk
- Forces vendor to address problem
- *Informs attackers (assuming they don't already know)*

# Lessons Learned: Coordinated Disclosure

- Coordinated disclosure is a relatively simple method and process for finders and organisations to work together to identify, understand, and fix security vulnerabilities

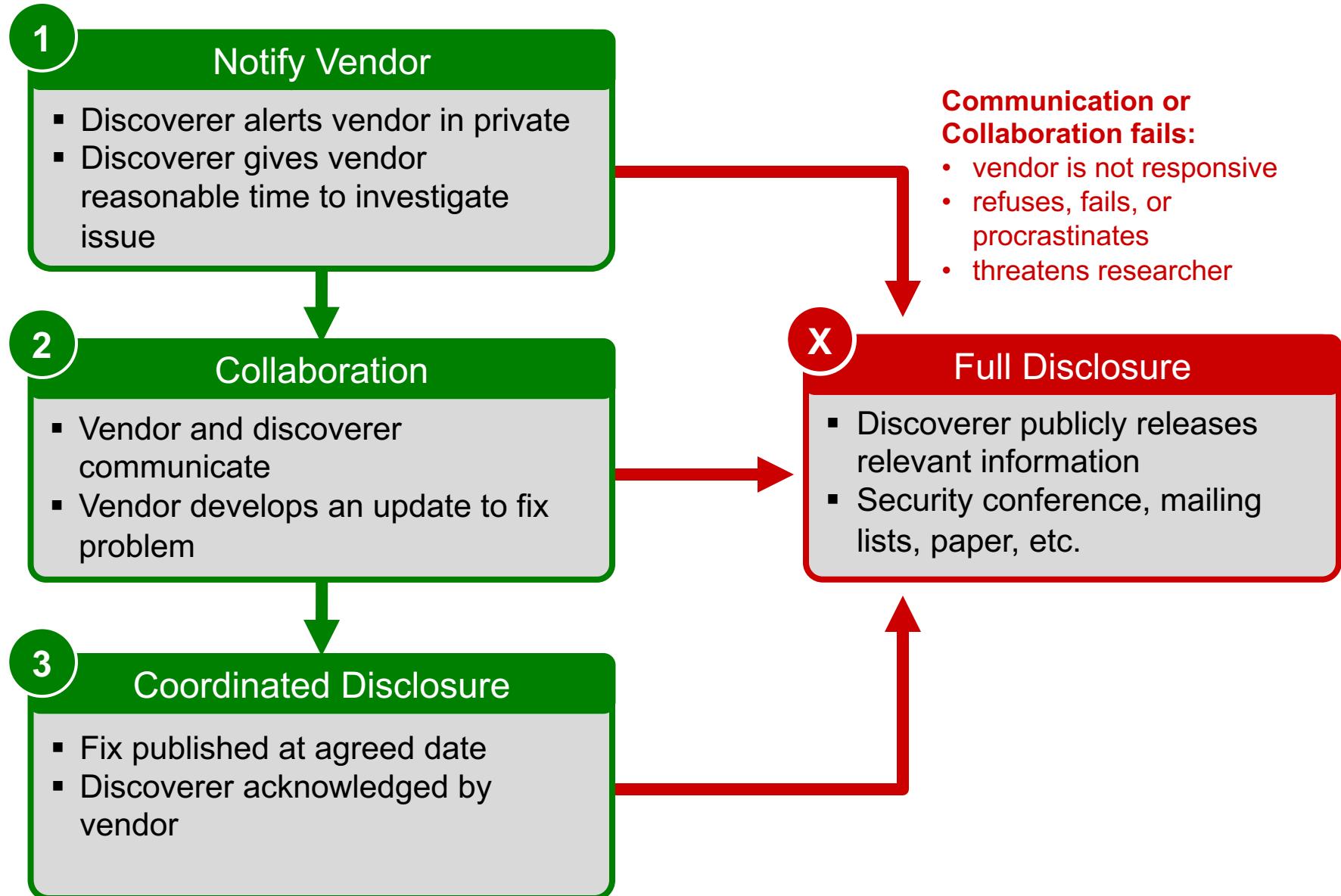
## Discoverer

- Document vulnerability
- Notify organization in a secure manner
- Provide additional info on request (within reason)
- Work with organization on an agreed publication method

## Organization

- Have a coordinated disclosure policy
- Acknowledge receipt of report, thank the discoverer
- Inform on next steps and timeframes
- Fix vulnerability, update the discoverer
- Work with discoverer to agree how and when to publish

# Coordinated Disclosure Process



# Coordinated Disclosure at Work

- Good
  - Tesla and Fiat/Chrysler privately informed. Both had a fix ready upon publication of research at BlackHat Conference. Chrysler recalled 1.4 Million cars.  
<http://bit.ly/ChryslerHack2015>  
<http://bit.ly/TeslaHack2015> (greatly handled by Tesla!)
- Very Bad
  - Volkswagen sued researchers and universities in order to prevent publication of critical issues in the keyless car access system (also used by Audi, Fiat, Honda, Kia and Volvo)  
<http://bit.ly/VWHack2015>

# Blame the Messenger

Volkswagen acknowledged the technological flaw in its cars. But the company stressed that the hack takes "considerable, complex effort" that's unlikely to be used except by tech-savvy, organized crime syndicates.

It didn't comment on its attempt to silence researchers, though.

Source: <http://bit.ly/VWHack2015>

## Note to self:

- Cyber attacks are typically highly automated and made available in easy to use tools after the hard initial research is complete
- Organized crime is (by definition) well organized and capable
- Why supressing a publication if it is unlikely to be used?

# Aviation Industry (has not yet arrived in the 21<sup>st</sup> century)

## Recent experience of a researcher reporting vulnerabilities to manufacturers:

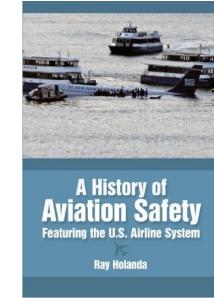
- Reporting a vulnerability does not result in addressing or fixing it by the vendor
- The avionics suppliers blame each other, and Boeing/Airbus blame them, and the airplane operators blame the manufacturers
- Poor isolation of critical systems and cabin systems on airplanes
- Poor security of AFDX network switches

# A History of Aviation Safety - A Comparison

Powered Flight – 1920-30	Cyber - 2015
	<h3>Perception</h3> <p>In the early days it was not fully appreciated that <b>thunderstorms</b> could generate forces that could <b>exceed the structural strength</b> of airplanes.</p>
	<p>It is currently not well understood or accepted that critical aircraft functions can <b>fail or be abused by cyber attacks</b>.</p>
	<h3>Testing</h3> <p>The first time engines had to pass a 50 hours endurance test caused the <b>rejection of 50%</b> of the engines.</p>
	<p>Unless tested rigorously, <b>serious quality issues</b> in cyber systems <b>go undetected</b>. <b>False sense</b> of security w/o testing.</p>

# A History of Aviation Safety

"A common theme appears throughout the history of aviation safety in the U.S. airline system: a technical solution was already available to solve a safety problem before that solution was implemented into the system."



- 1958      CVR and FDR made mandatory. Pilots lobbied against it and airlines opposed them because of the cost.
- 1969      After another midair collision the FAA went ahead to incorporate the Terminal Control Area (TCA) system, requiring transponders for all planes at the large airports.
- 1976      All major commercial airlines required to have Ground Proximity Warning System (GPWS). After that date no more CFITs on GPWS equipped aircraft, while CFIT continued to be a major cause for commuter airlines.
- 1981      United adopted a Crew Resource Management (CRM) program. Hull loss rate decreased from 1:1 Million to 1:5 Million operations.

# Conclusion Recommendations

## Recommendations - Tasks

- Isolated systems become critically exposed when linked to external systems
  - Carefully choose what and when to allow external connectivity (it is your choice, evaluate consequences thoroughly)
  - Ensure the system is ready for the harsh new environment
  - Ensure an effective security update process is in place
  - Ensure you can handle and correct vulnerabilities swiftly
- Don't complain that security updates break certification.  
By connecting isolated systems you chose to enter the new environment.

# Recommendations - Tasks

- Independent security testing of critical systems
  - Have critical computing and communication systems tested by external experts
  - Disallow new connectivity before the systems pass realistic tests
  - Adopt and live a coordinated disclosure process
  - Embrace the security community and adopt the many free lessons they provide (go to CCC, DefCon, BlackHat and similar conferences, listen open minded)
  - *Remember that in 1926 more than 50% of the engines failed when first subjected to a realistic test*

## Recommendations - Tasks

- Critical Communications (e.g. Radio, Networks)
  - Critical communications must be secured (authentication, confidentiality, integrity, availability)
  - Consider all unprotected radio communication as potentially compromised
  - Test the isolation between critical and non critical systems

# Conclusion

- Decision and policy making processes in aviation are outpaced by the dynamics of the cyber domain (we are now in the 21<sup>st</sup> century)
- There are valuable lessons from other industries
- Cyber security issues are a safety issue

“Ignoring reality is not an effective way to get healthier, or smarter, or safer, even though it might temporarily make you feel better”

Bruce Schneier

# Resources

## Books

- Schwarmdumm: So blöd sind wir nur gemeinsam  
*by Gunter Dueck*  
<http://www.amazon.de/Schwarmdumm-blöd-sind-wir-gemeinsam/dp/3593502178>
- Antifragile: Things that gain from disorder  
*by Nassim N. Taleb*  
<http://www.amazon.com/Antifragile-Things-That-Disorder-Incerto/dp/0812979680>

## Security Conferences

- CCC - <https://www.ccc.de>
- DefCon - <https://www.defcon.org>
- BlackHat - <https://www.blackhat.com>

# Resources

## Further Reading

- Cyber Security: Die aktuelle Bedrohungslage  
by Stefan Frei, Swisscom  
<http://techzoom.net/Publications/Papers/bedrohungslage2015>

## Coordinated Disclosure Process

- CERT Vulnerability Disclosure  
<http://www.cert.org/vulnerability-analysis/vul-disclosure.cfm>
- New Zealand Internet Task Force - Coordinated Disclosure Guidelines  
[http://www.nzitf.org.nz/pdf/NZITF\\_Disclosure\\_Guidelines\\_2014.pdf](http://www.nzitf.org.nz/pdf/NZITF_Disclosure_Guidelines_2014.pdf)

# Questions?

Come a little closer



Funeral services Bergmann & Sohn  
Johannstraße 7, 10551 Berlin-Tiergarten, phone: 030/36 18 18, [www.bergmann-sohn.de](http://www.bergmann-sohn.de)

[frei@techzoom.net](mailto:frei@techzoom.net)