Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Cyber Threats in Aviation

ANY LESSONS FROM OTHER INDUSTRIES EXPERIENCE WITH CYBER?

Dr. Stefan Frei

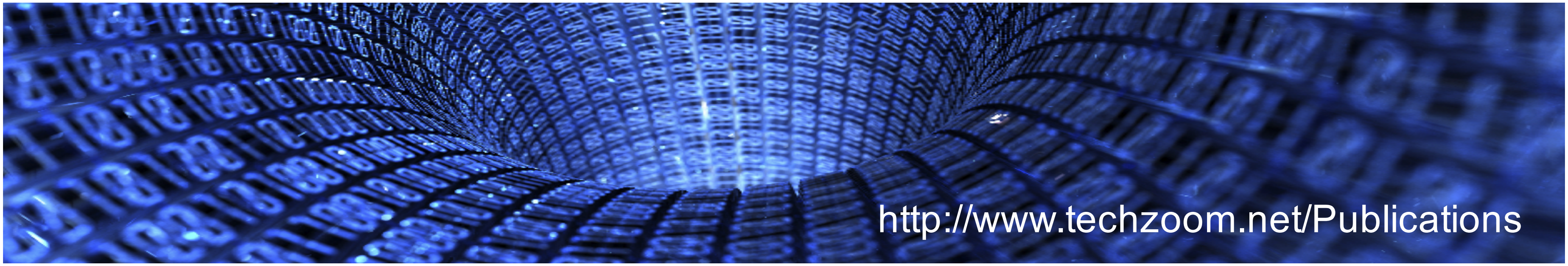
Security Architect at Swisscom, Lecturer at ETH Zurich

frei@techzoom.net   Twitter @stefan_frei

With special thanks to

Gallus Bammert, Aviation Expert, FI

Christ Roberts, CTO One World Labs



http://www.techzoom.net/Publications

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 adopt to permanent change and high dynamics

1 Million Years

50 Years

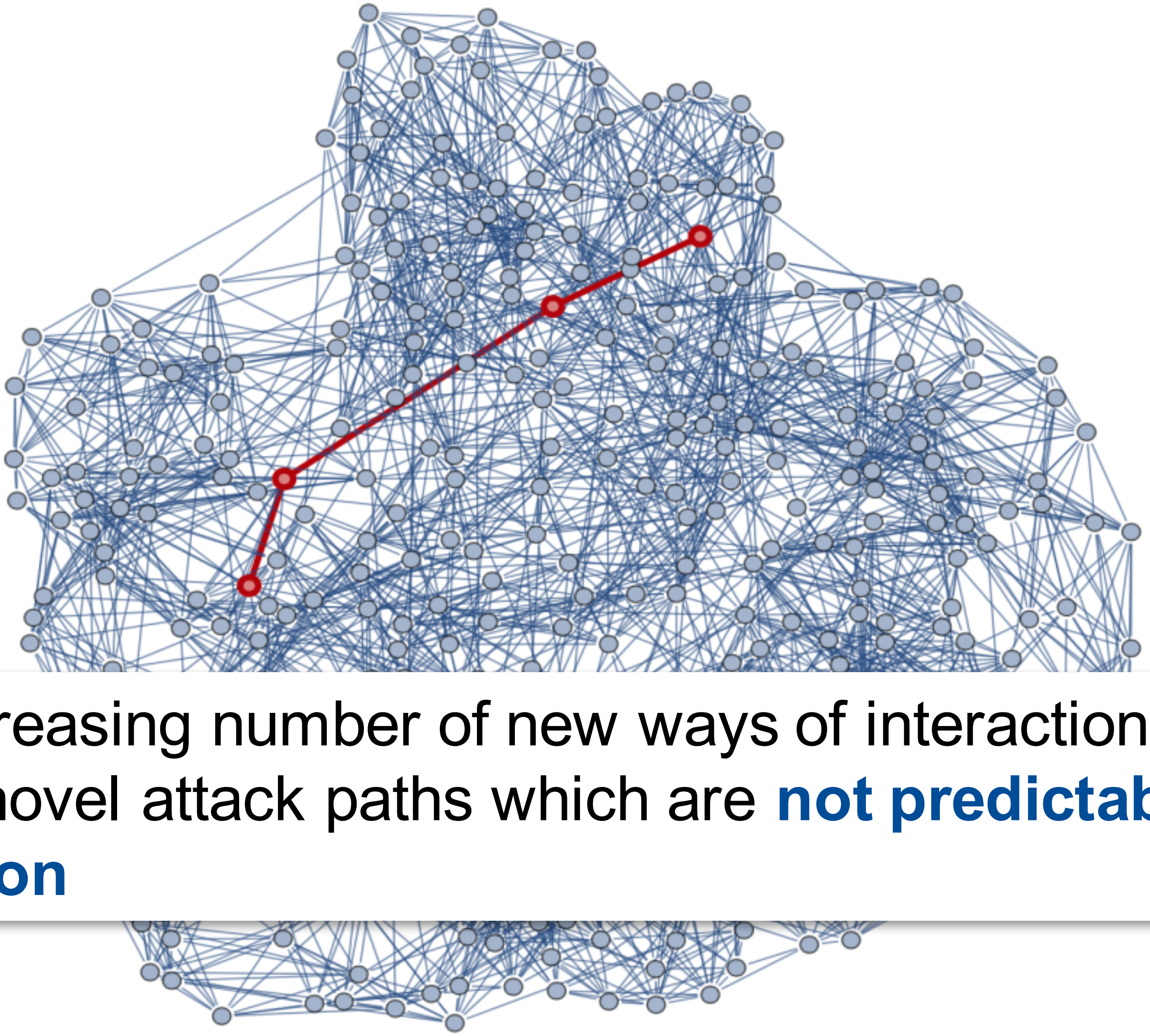
Actors & Attackers

	Attacker	Objectives	Resources	Proceeding
Targeted	Nation States, Agencies	• Information • Fightting Crime/Terrorismus • Espionage • Sabotage	• Enourmous financial resources • Focus on result, not cost	• Build & buy know-how • Persistent & well hidden attacks • Subversion of supply chain
	Terrorists	• Damage • Attention • Manipulation of politics • Fear Uncertantity and Doubt (FUD)	• Considerable financial resources • Potentially large network of supporters	• Buy know-how on black market • Physical attacks
	(Organized) Crime	• Financial	• Business • Make money on long term • Profit/loss driven	• Exsisting gangs • Per case groups of specialists • Bribery
Opportunistic	Hacktivists, Groups	• Mass attention • Damage • Denounce vulnerabilities in systems/organizations	• Minimal financial resources • Large reach	• Highly motivated amateurs & specilalists • Develops unpredictable momentum
	Vandals, Skript Kiddies	• Fame • Reputation	• Minimal financial resouces and know-kow	• Available tools

What makes the cyber world special?

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

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

Source: http://web.mit.edu/esd.83/www/notebook/Complex%20Adaptive%20Systems.pdf

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 ***robustnes***
- Absorbtion:
  long term survival, diversity

> anti-fragile

Source: Antifragile: Things That Gain from Disorder, by Nassim Nicholas Taleb

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 controll systems (ask Fiat/Chrysler)

complexity

- complexity and interaction between systems is growing continously
- 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

Source: The Economist, The End of Moore's Law

Innovation & Price Erosion

Nonexistent or previously unavailable technologies become common goods

Software Defined Radio

USD 500,000

15 Years

USD 500

Revalidate security assumptions based on the

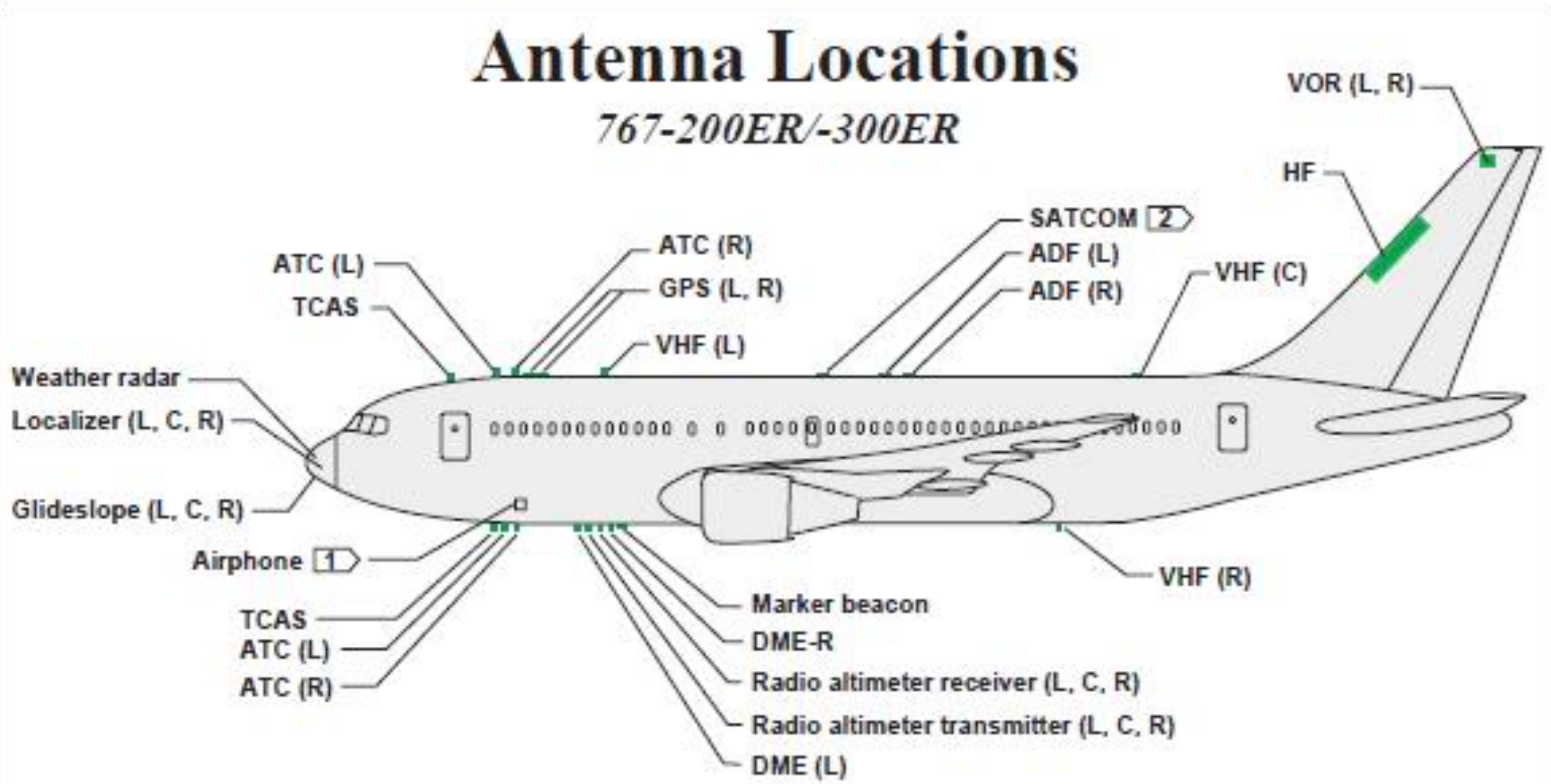
> (A) limited availability, (B) unaffordability, or
> (B) limited performance

of a technology

Examples of new Attack Vectors

- Software Defined Radios (SDR)
  - All radio communication and protocols without hard crypto protection are highly exposed
- Drones
  - Drones easily bypass perimeters to sniff or insert eavesdropping devices
- Robots
  - Robots can access areas not accessible by humans. Remotely controlled to manipulate, monitor, or take other actions

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

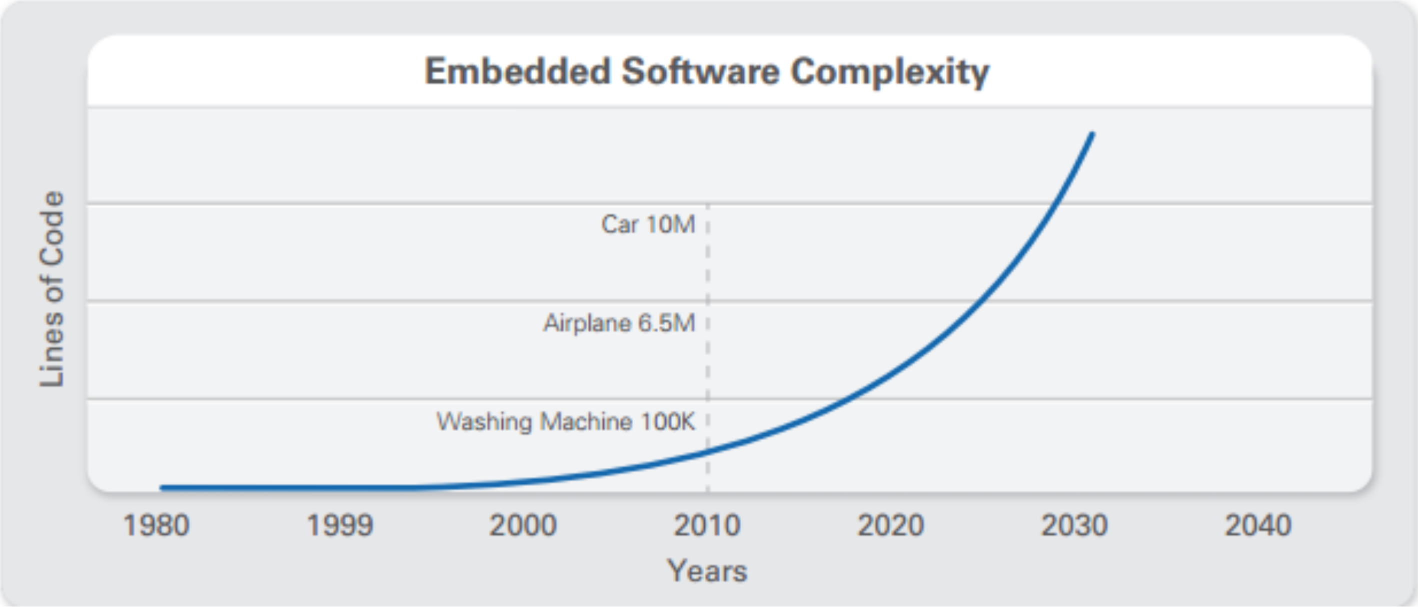
- Software complexity is increasing
- There is no secure software

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



Source: NASA Report http://www.nasa.gov/pdf/418878main_FSWC_Final_Report.pdf

Aviation Systems Are Not Prepared

Internet Computer

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

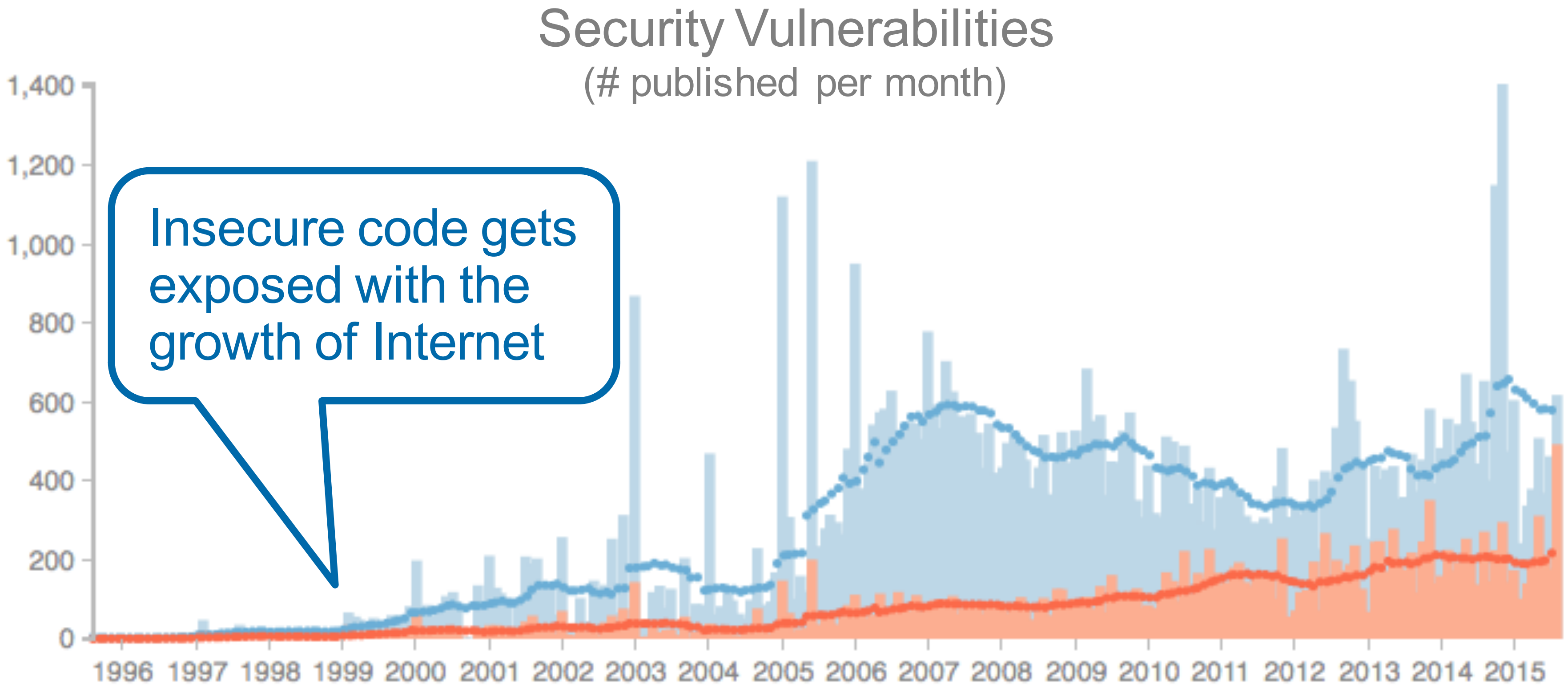
Aviation Computer

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

- Today's aviation systems where 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



Security Vulnerabilities
(# published per month)

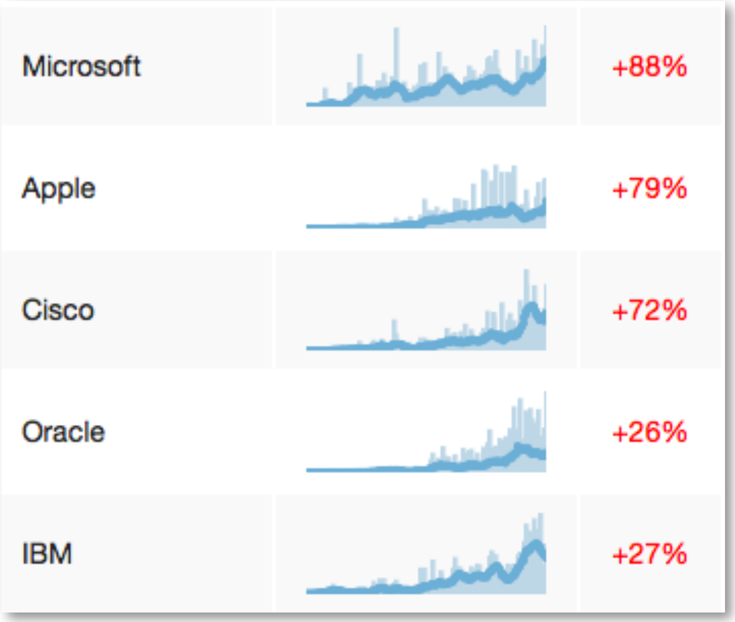
Insecure code gets exposed with the growth of Internet

(red: top-10 software vendors)

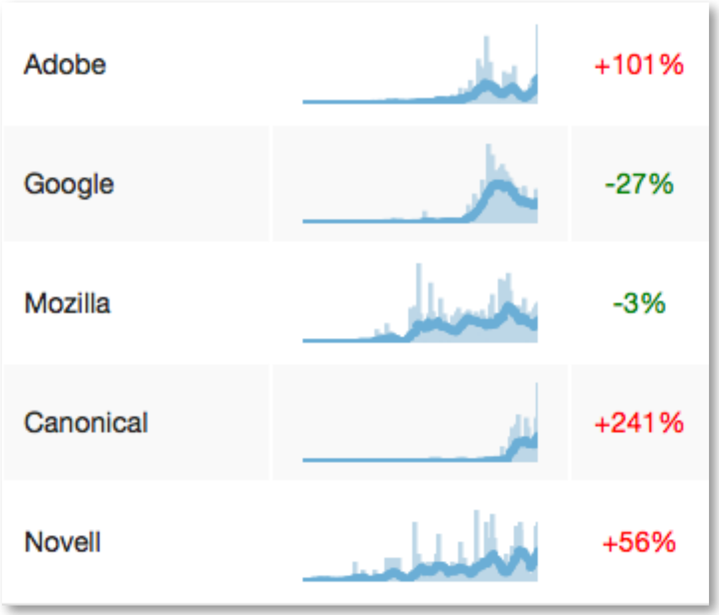
Source: http://techzoom.net/BugBounty/SecureSoftware

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*



Microsoft		+88%
Apple		+79%
Cisco		+72%
Oracle		+26%
IBM		+27%



Adobe		+101%
Google		-27%
Mozilla		-3%
Canonical		+241%
Novell		+56%

Trend 5 yrs vs. last year

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

Source: http://techzoom.net/BugBounty/SecureSoftware

Cyber Security Testing ≠ Compliance Testing

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

Internal Testing	External Testing
• Constrained, biased • Uninspired, lack of diversity • Experts in compliance and availability testing	• Independent, unconstrained • Unbiased, creative, diversity • Experts in breaking systems

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

You Discovered a Vunlerability – What Do You Do?

Keep it secret?

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

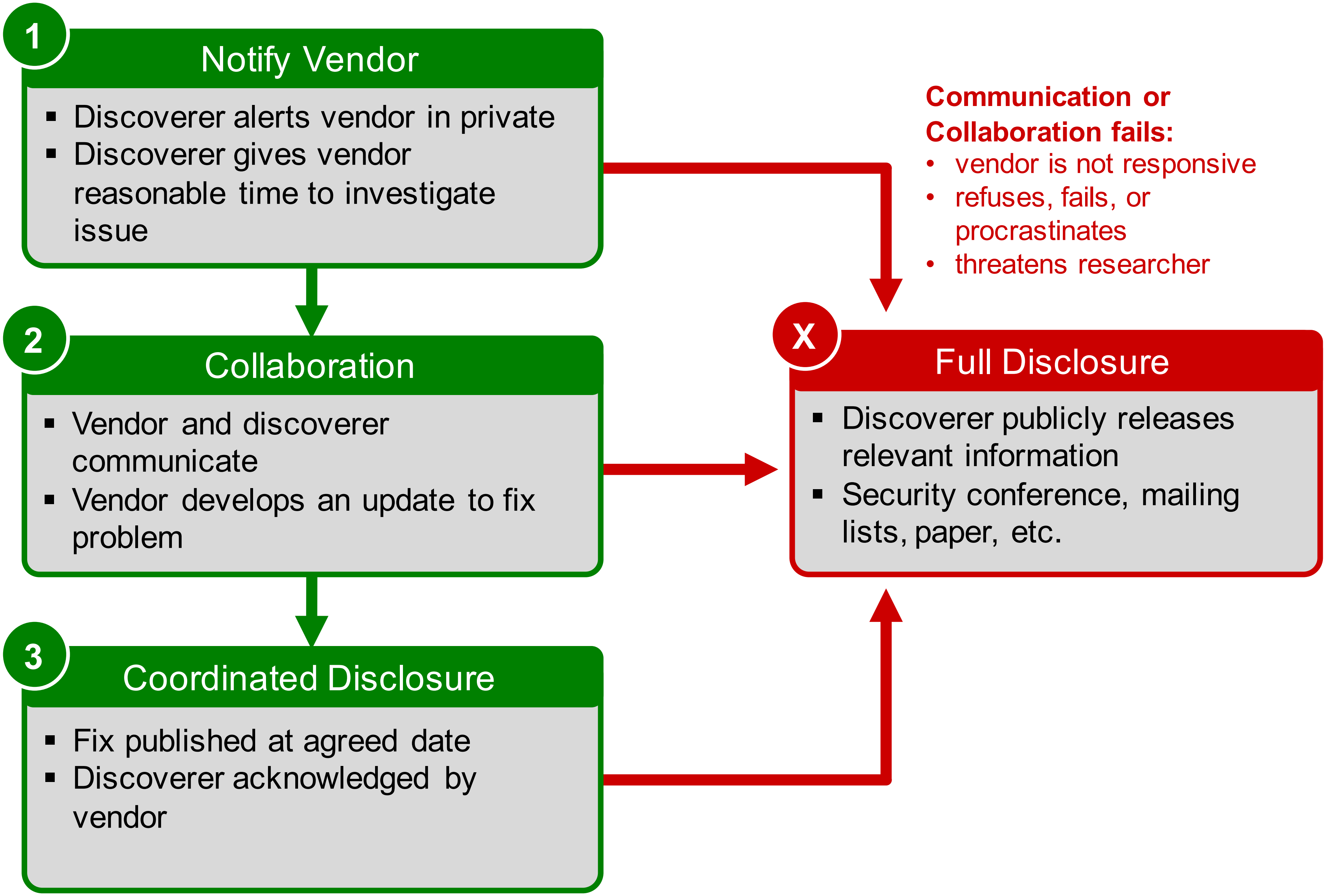
Report to Vendor?

- 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)

Coordinated Disclosure Process



1 Notify Vendor

- Discoverer alerts vendor in private
- Discoverer gives vendor reasonable time to investigate issue

2 Collaboration

- Vendor and discoverer communicate
- Vendor develops an update to fix problem

3 Coordinated Disclosure

- Fix published at agreed date
- Discoverer acknowledged by vendor

Communication or Collaboration fails:

- vendor is not responsive
- refuses, fails, or procrastinates
- threatens researcher

X Full Disclosure

- Discoverer publicly releases relevant information
- Security conference, mailing lists, paper, etc.

Lessons Learned: Coordinated Disclosure

Coordinated disclosure is a relatively simple method and process for finders and organizations 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

Source: Coordinated Disclosure Guidelines - http://www.nzitf.org.nz/pdf/NZITF_Disclosure_Guidelines_2014.pdf

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

Aviation Industry (has not yet arrived in the 21st 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

Security through obscurity does not work

- Have your airplanes tested by independent cyber experts
- Identify vulnerabilities early - and have them fixed

Threat Scenario

- What if a billionaire provides his Airbus/Boeing VIP aircraft to terrorists to identify vulnerabilities?

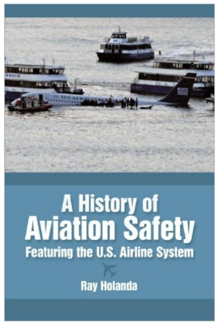
Who is first to identify a critical vulnerability?

A History of Aviation Safety - A Comparison

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

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 mandantory. 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 GWPS 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.

Source: http://www.amazon.com/History-Aviation-Safety-Featuring-Airline/dp/144900797X

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
- Support independent cyber testing of complete airplanes (e.g. during maintenance)
- Disallow new connectivity before the systems pass realistic tests
- Adopt a coordinated disclosure process
- Embrace the security community and adopt the many free lessons they provide

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

Recommendations - Tasks

Training

- Training of crew and related personnel to handle an adaptive and creative attacker
  - Not random faults – but targeted interference with operations
- Include cyber experts to create scenarios

Sample Scenario

- Attacker records ATC radio instructions over time
- Targeted and adaptive replay of specific & conflicting TWR/ATC messages to create conflicts at busy airport during bad weather
- Do the same 30 min later at the alternate destinations

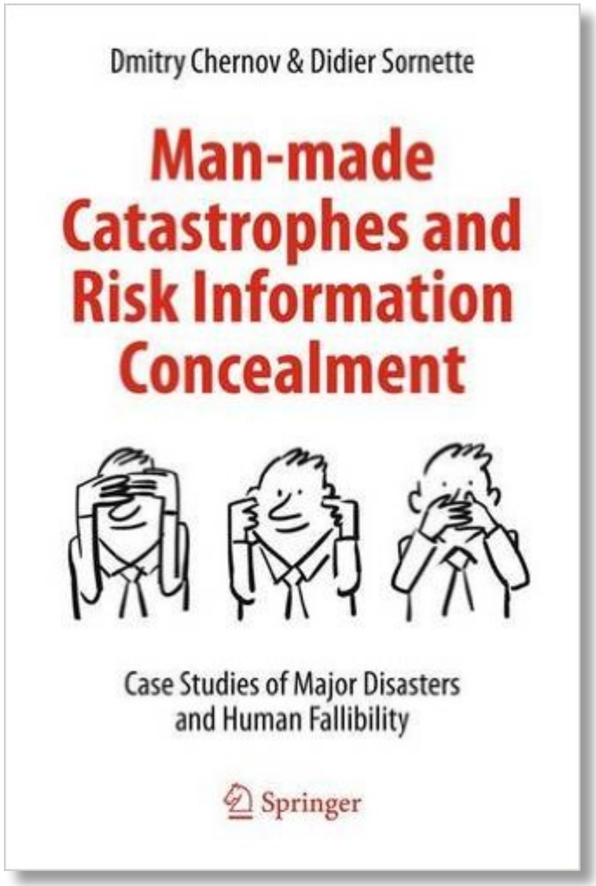
Conclusion

- Decision and policy making processes in aviation are outpaced by the dynamics of the cyber domain (we are now in the 21st 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

Recommended Books

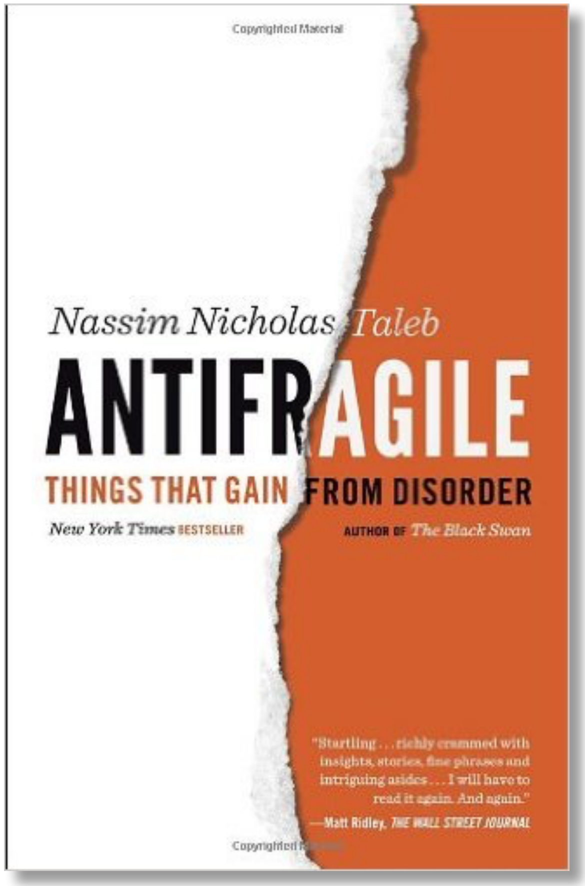


Dmitry Chernov & Didier Sornette

Man-made Catastrophes and Risk Information Concealment

Case Studies of Major Disasters and Human Fallibility

Springer



Nassim Nicholas Taleb

ANTIFRAGILE

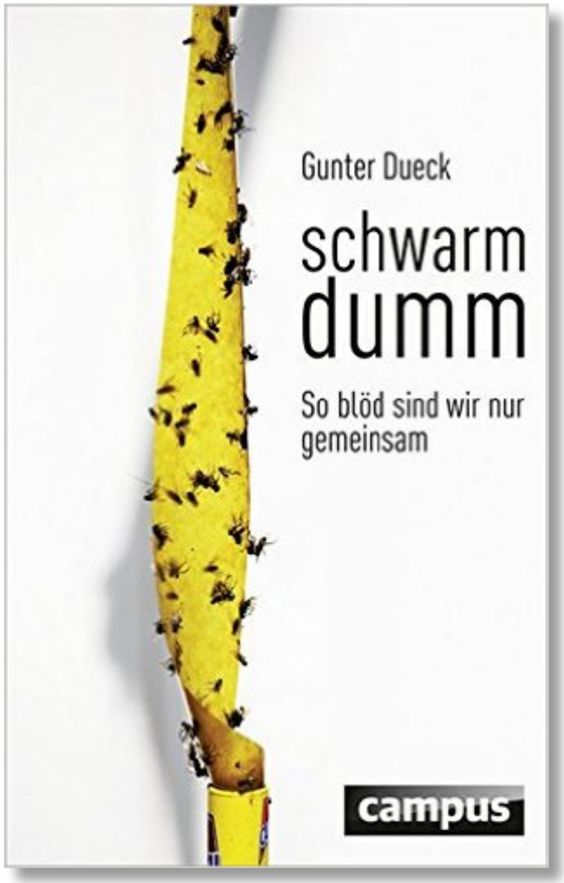
THINGS THAT GAIN FROM DISORDER

New York Times BESTSELLER

AUTHOR OF *The Black Swan*

"Startling . . . richly crammed with insights, stories, fine phrases and intriguing asides . . . I will have to read it again. And again."

—Matt Ridley, *THE WALL STREET JOURNAL*



Gunter Dueck

schwarm dumm

So blöd sind wir nur gemeinsam

campus

Further Resources

Further Reading

- Cyber Security: Die aktuelle Bedrohungslage - Stefan Frei
  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

Security Conferences

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

Come a little closer
Funeral services Borgemann & Sohn
Jonasstraße 7, 10551 Berlin Tiergarten, phone (030) 390 10 15, www.billiger-bestatten.de

Questions?

frei@techzoom.net