ETH zürich

sicherheitshalber.2019 | DFS Sicherheitstag, April 4th, 2019

DFS Deutsche Flugsicherung

Cyber Threats in Aviation

Any lessons from history?

Dr. Stefan Frei | frei@techzoom.net | Twitter @stefan_frei
www.techzoom.net

Lessons from numerous engagements as ethical hacker (penetration testing) for the largest and best defended organizations around the world

1. In each and every engagement, at the end we had the organization fully compromised.

2. More often than not, it was not necessary to dig deep in our bag of technical tricks to achieve the compromise.

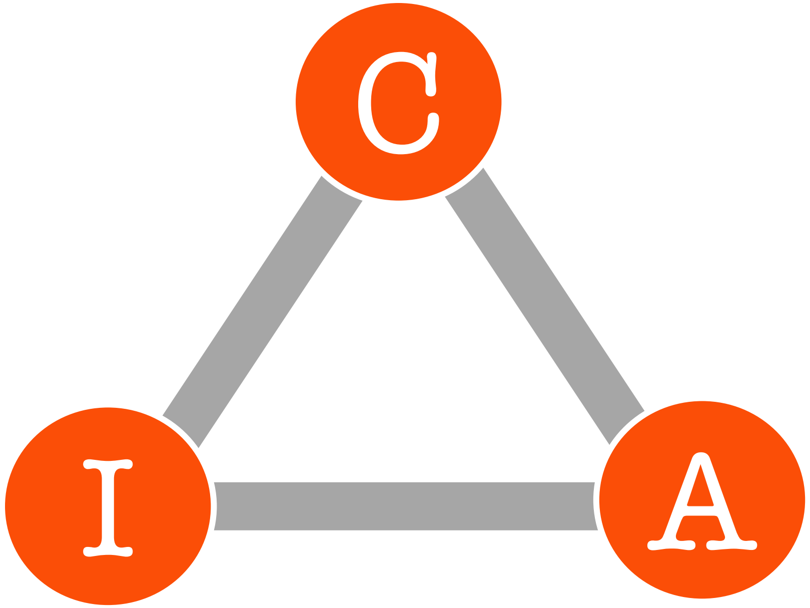
(1) is OK if you hire professionals.
(2) is worrisome, and understanding such failures drives the topics of this course.

Common Ground

INFORMATION SECURITY OBJECTIVES – CIA TRIAD

Confidentiality

Prevention of **unauthorized disclosure** of information.



Integrity

Prevention/detection of **unauthorized modification** or deletion of information.

Availability

Prevention of **unauthorized withholding** of information or service.

SAFETY VS. SECURITY

The English language differentiates SECURITY from SAFETY, for which there is only one expression SICHERHEIT in German.

SAFETY

- Safety is the protection **against random**, unwanted incidents - resulting from **coincidences** or driven by the environment
- **THE ENVIRONMENT DOES NOT ADAPT TO BYPASS SAFETY MEASURES.**

Natural Science
Controlled Experiments, Modelling

SECURITY

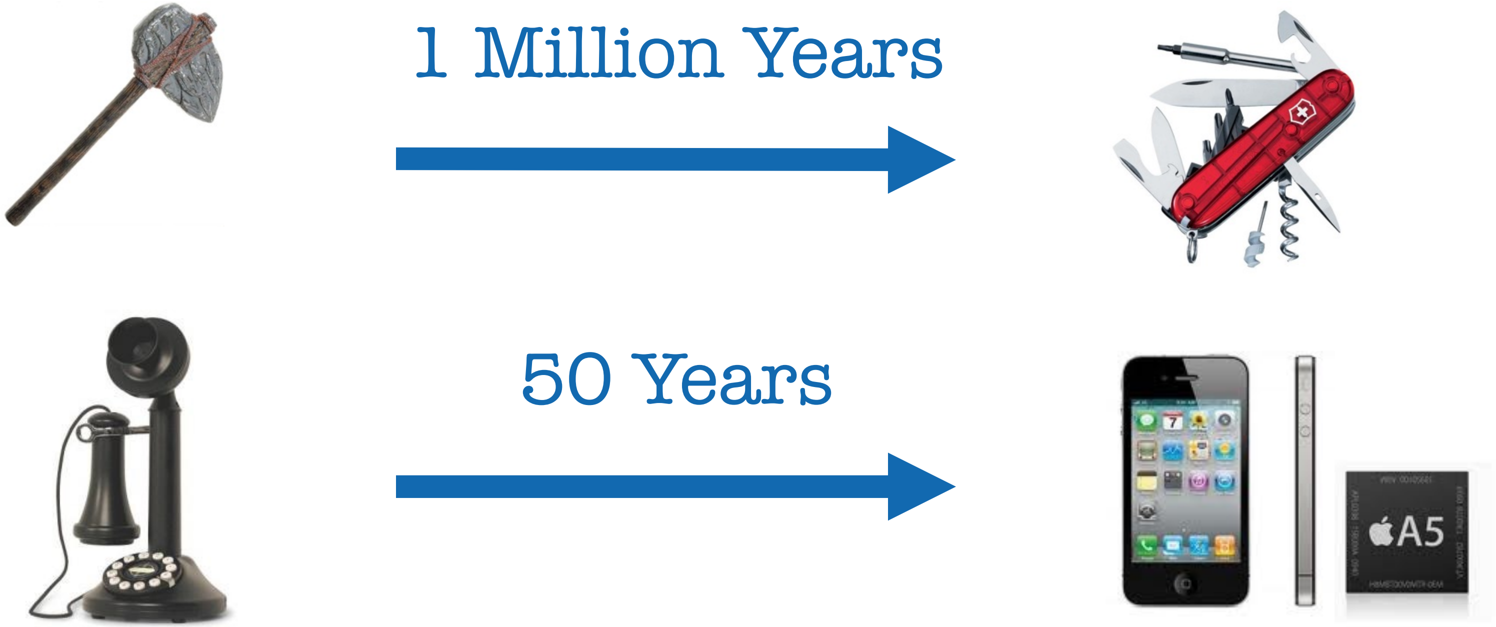
- Security is the protection **against intended incidents** – resulting from a **deliberate and planned act**
- Driven by targeted attacker.
- **DELIBERATE ACTS DRIVEN BY AN ADAPTIVE ATTACKER.**

Social Science
Ever Changing Environment

What makes the Cyber World different?

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, industry



CRIMINALS PROOFED REPEATEDLY TO BE VERY FAST ADOPTERS OF NEW TECHNOLOGIES.

THROUGHOUT HISTORY, NEW TECHNOLOGIES HAVE REVOLUTIONIZED CRIME AND WARFARE ALIKE

... so has Information & Communication Technology (ICT)

- Gunpowder
- Tanks
- Aircraft
- Satellites
- Computers
- Networks
- Internet of things
- ..

CRIMINALS ARE FAST ADOPTERS OF NEW TECHNOLOGIES

Example: Bonnot Gang (La Bande à Bonnot)

- A French criminal anarchist group, operated in France and Belgium from 1911 to 1912
- The gang **utilized cutting-edge technology not yet available to the French police:**

Automobiles and **Repeating Rifles**

$$V_{\text{Automobile}} >> V_{\text{Horse}} >> V_{\text{Bicycle}}$$

"They escaped in their stolen automobile as two policemen tried to catch them, one on horseback and the other on a bicycle."

HUMANS ARE NEW TO THE MECHANISMS AND ARTIFACTS OF CYBER RISK

We have no built-in concept to deal with abstract risks

No training needed to instantly get out of danger

INSTANT PERCEPTION OF RISKS

Security defects are invisible without proper testing

LIMITED OR NO PERCEPTION OF RISKS

- Difficult to get resources from CxO to counter abstract risks
- Illusion of control and accumulation of hidden risks

THERE IS DIFFERENCE A BETWEEN PERCEIVED AND ACTUAL RISK

we over-react to

INTENTIONAL ACTION

Anthrax

IMMEDIATE THREATS

Humans are hard-wired to do so instinctively

THINGS THAT OFFEND OUR MORALS

we under-react to

ACCIDENTS

Influenza, Falling down stairs

ABSTRACT EVENTS

Can't see it

CHANGES THAT OCCUR SLOWLY

Humans are new to predicting, global warming

Source: https://www.schneier.com/blog/archives/2006/11/perceived_risk_2.html

RISK PERCEPTION - EXPERIMENT

Consider the following two scenarios:

Game / Experiment	
Scenario 1	**Scenario 2**
I give you a dollar.	**We flip a fair coin:** ▪ Heads: I give you **$1,000** ▪ Tails: You give me **$998**
Expected Value: $1	**Expected Value: $1**
$E[\text{Scenario } 1] = 1 \cdot 1 = 1$	$E[\text{Scenario } 2] = 0.5 \cdot 1'000 - 0.5 \cdot 998 = 1$

The expected values are the same in both cases ($1), but the risks seem quite different.

THREATS THROUGH CONTINUED INNOVATION AND PRICE EROSION

Miniaturization and increased capabilities of tools while prices erode.

This development fundamentally changes how we acquire, share, operate, and use any kinds of goods:

- Todays transistors are **90,000x** more efficient and **60,000x** cheaper than 1971
- A car today would cost **CHF 0.25** and consume **0.2 ml fuel/100 km**

DRONES

3D PRINTER

ROBOTS

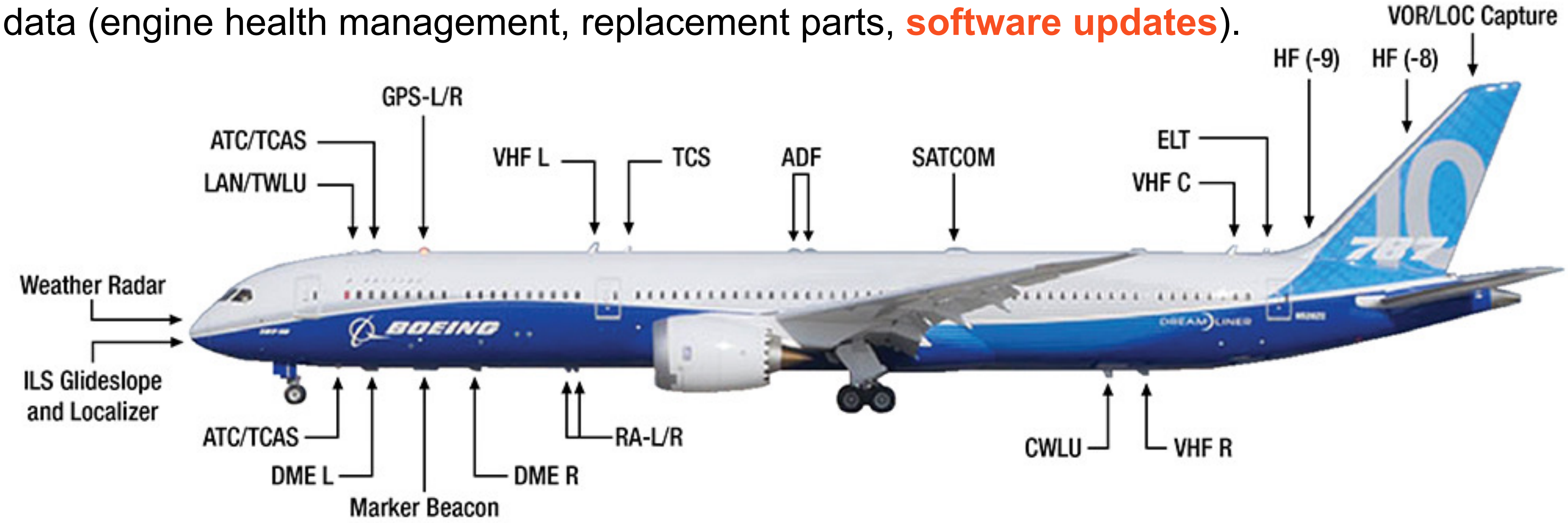
SOFTWARE DEFINED RADIOS

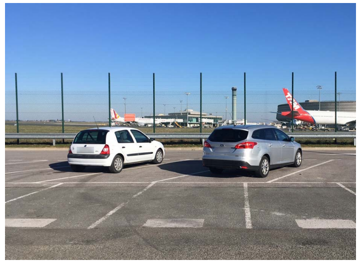
! **Any security assumption based on the limited *availability*, *capability*, or *high price* of (attack) tools become invalid and must be reconsidered.**

MODERN AIRPLANES – LEGACY COMMUNICATIONS

Hacking into wireless communication with software defined radios

Legacy flight critical **communication and navigation** systems are not protected.
Modern airplanes use **wireless (802.11 b/g) technology** while at the gate transferring maintenance and reliability data (engine health management, replacement parts, **software updates**).



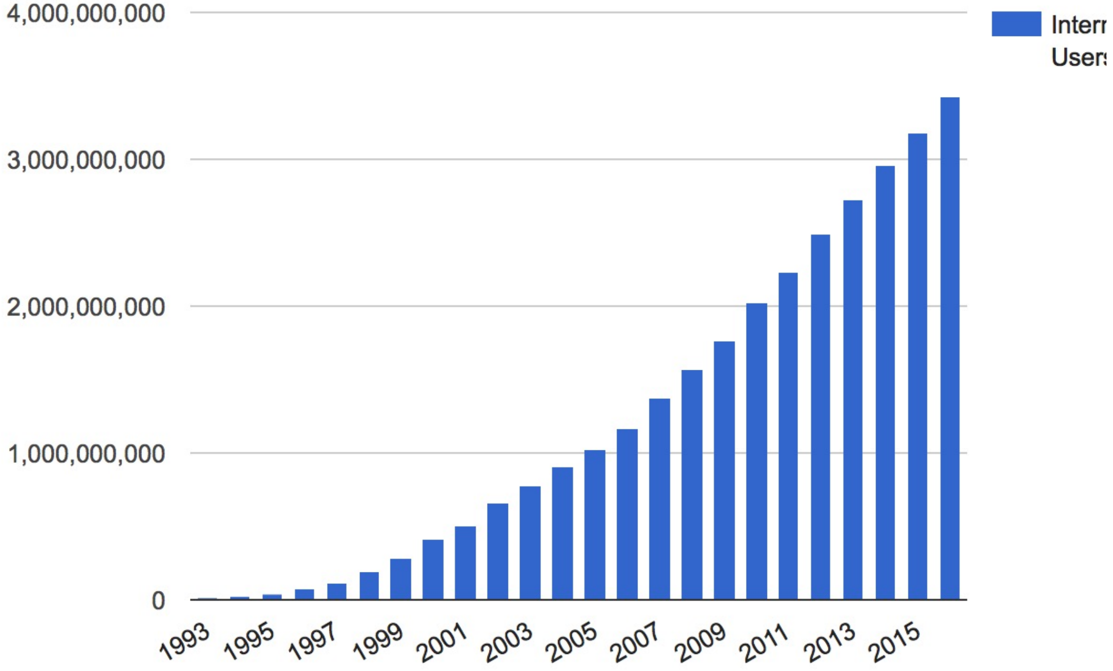


1. Intercept wireless communication between aircraft and airport terminal.
2. Team sits in parked car, connecting to target aircraft with software defined radio.
3. Accessed flight/cabin systems, modified code for specific flight plan.
4. **KNOCKING AT THE DOOR OF THE FMS**

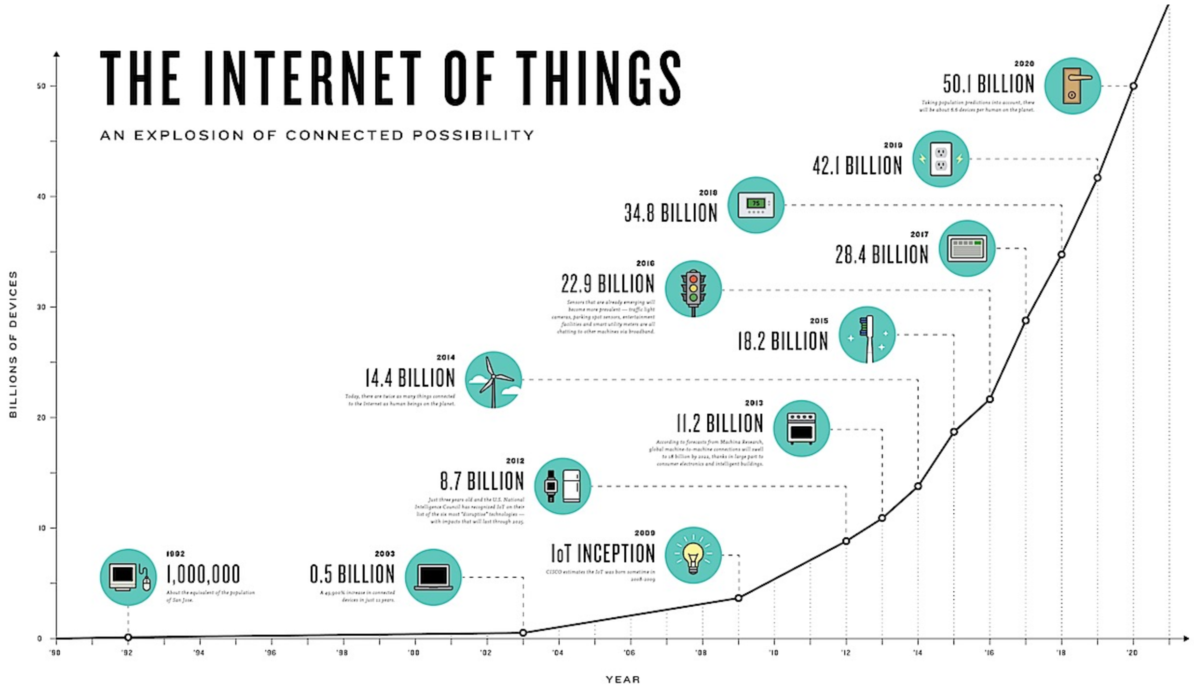
THE INTERNET OF THINGS AND PEOPLE

From an attackers perspective ..

>3 Billion People Today



> 50 Billion Devices by 2020

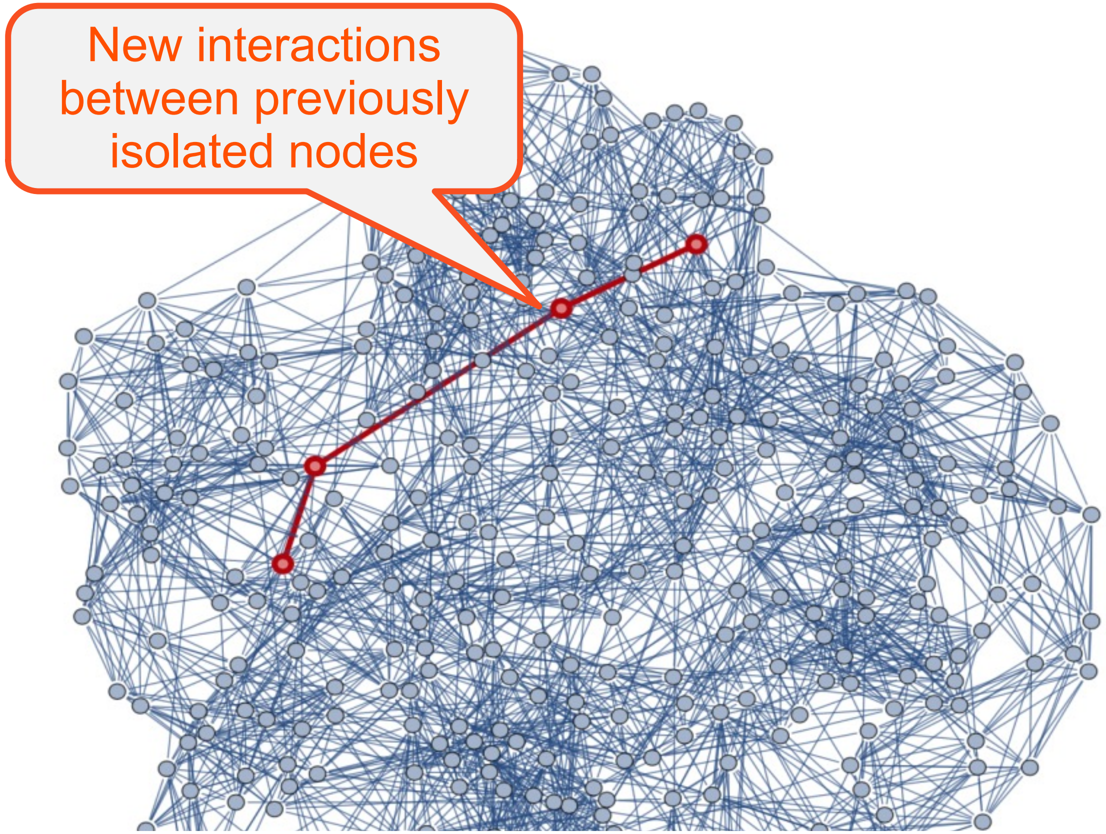


Numerous targets

.. even more targets

CONNECTING PEOPLE, SERVICES, .. & DEVICES

New ways of interaction also create fundamentally novel attack paths which are not predictable by definition


New interactions between previously isolated nodes

PROPERTIES OF COMPLEX ADAPTIVE SYSTEMS	
CONNECTIVITY	A decision in one part of the system will affect other related or distant parts.
SENSITIVE DEPENDENCE	Non-linearity, cascades.
EMERGENT ORDER	Emergent and unpredictable behavior, which cannot be predicted **even with full knowledge of all elements**

We have to adopt to permanent change, high dynamics, and decreased predictability

STRATEGIES TO HANDLE UNPREDICTABILITY

Different approaches between men and nature

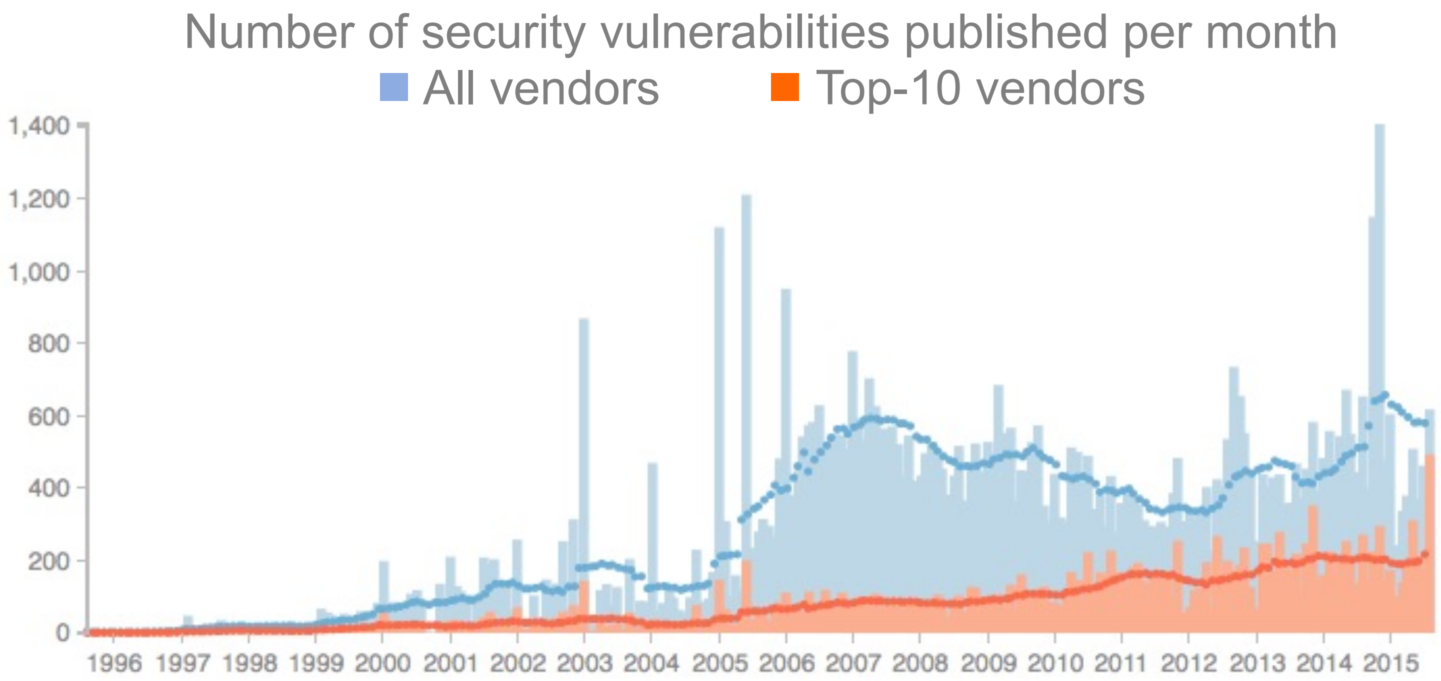
MEN	NATURE
Predict and model risks	**No attempt to predict risks**
> PREVENT SHOCKS <	**> ABSORB SHOCKS <**
▪ Relies on **accuracy of models** and **probabilities** ▪ Optimization: **Short term gain, efficiency**	▪ Relies on **redundancy, diversity** and **robustness** ▪ Absorption: **Long term survival, diversity**
> FRAGILE <	**> ANTI-FRAGILE <**

Management:

Balance degree of optimization: short term gains vs. long term survival

SOFTWARE EATS THE WORLD

In spite of increased investment, there will never be secure code, given the 'special' business model of software.



Microsoft IBM ORACLE redhat mozilla FOUNDATION Linux CISCO Google hp

Complex software with vulnerabilities drives everyday devices – we need to manage vulnerabilities.

FOLLOW THE MONEY

Economics often explains security defects better than technology.

>> NO PRODUCT LIABILITY FOR SOFTWARE <<

- A security patch is nothing but a **product recall at the expense of the customer**.
- Why do many **smart or IOT devices** offload critical functionality to the cloud?
- No **minimum security or quality standards** for software.

Threats

&

Attackers

TYPES OF ATTACKS

Targeted Attacks vs. Opportunistic Attacks, and Persistence

TARGETED ATTACK	▪ Actors have clearly defined objectives and targets that they pursue consistently. ▪ Usually with the backing of considerable resources (finances, expertise, human resources, tools & materials). ▪ Attackers of this kind are often relentless.
OPPORTUNISTIC ATTACK	▪ Actors take opportunities online, either by chance or because the target is not adequately protected.
PERSISTENT ATTACK	▪ The attack is capable of constantly increasing its penetration of systems and resources. ▪ Attackers pursue their goals over a longer period of time and via multiple parallel channels. ▪ Reinfection following failed or inadequate attempts.

THREAT ACTORS & ATTACKERS

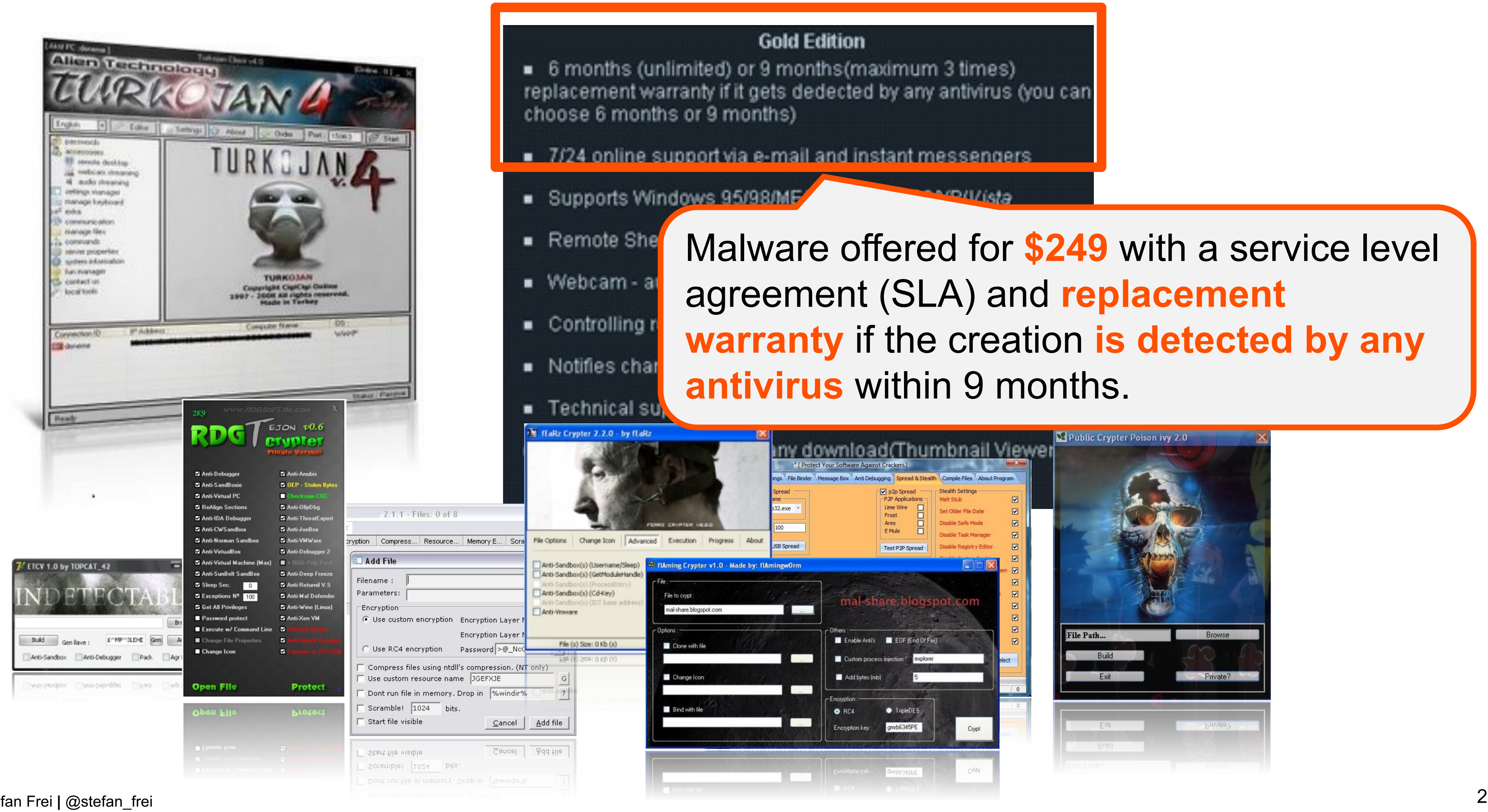
TARGETED ATTACK

OPPORTUNISTIC ATTACK

ATTACKER	OBJECTIVES	RESOURCES	PROCEEDING
Nation States, Agencies	• Information • Fighting Crime/Terrorism • Espionage • Sabotage	• Enormous 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 Uncertainty 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	• Existing gangs • Per case groups of specialists • Bribery
Hacktivists Groups	• Mass attention • Damage • Denounce vulnerabilities in systems/organizations	• Minimal financial resources • Large reach	• Highly motivated amateurs & specialists • Develops unpredictable momentum
Vandals Script Kiddies	• Fame • Reputation	• Minimal financial resources and know-how	• Available tools

PROFESSIONAL ATTACKERS & SERVICES

Automation, Easy To Use Tools, Service Level Agreements



Gold Edition

- 6 months (unlimited) or 9 months(maximum 3 times) replacement warranty if it gets dedected by any antivirus (you can choose 6 months or 9 months)
- 7/24 online support via e-mail and instant messengers
- Supports Windows 95/98/ME
- Remote She
- Webcam - a
- Controlling r
- Notifies char
- Technical su

any download(Thumbnail Viewer

Malware offered for **$249** with a service level agreement (SLA) and **replacement warranty** if the creation **is detected by any antivirus** within 9 months.

THE GERASIMOV DOCTRINE

Gerasimov took tactics developed by the Soviets, blended them with strategic military thinking about total war, and laid out a new theory of modern warfare:

He wrote

- “The very ‘rules of war’ have changed
- The role of nonmilitary means of achieving political and strategic goals has grown, and, in many cases, they have exceeded the power of force of weapons in their effectiveness

The doctrine looks more like hacking an enemy’s society than attacking it head-on.

Вале́рий Васи́льевич
Гера́симов

Source: https://www.politico.com/magazine/story/2017/09/05/gerasimov-doctrine-russia-foreign-policy-215538

ALMOST EVERYONE HAS ACCESS TO, AND CAN AFFORD THE LATEST IN CYBER WEAPON TECHNOLOGY

Main Battle Tank
≈ 5 Million

Fighter Aircraft
≈ 50 Million

Frigate
≈ 250 Million

Spy Satellite
≈ 500 Million

Market prices for exploits (= cyber weapons)

$1 Million for iPhone exploit

$700k for Android exploit

exploit price ≈ <market share> x <security of product>

The historic monopoly of states to access and operate the latest in weapon technology is now broken.

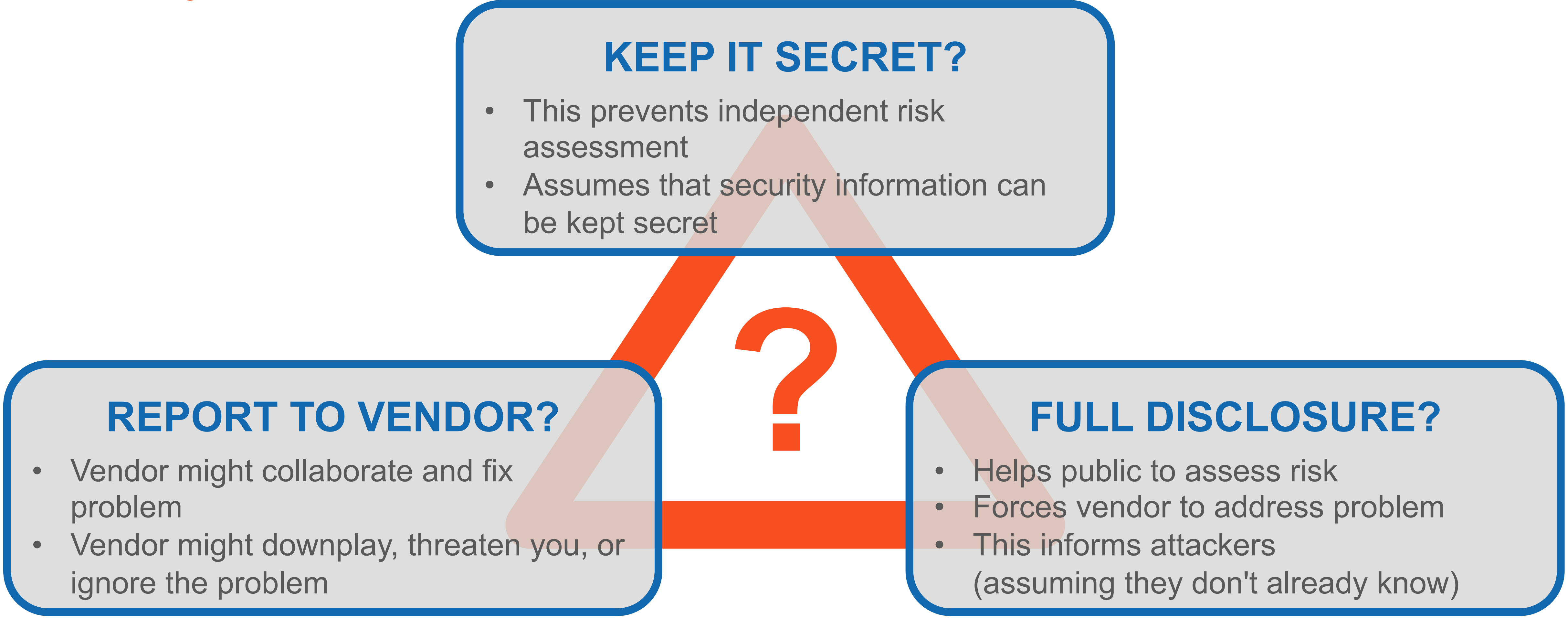
(Full)
Disclosure Debate

YOU DISCOVER A CRITICAL VULNERABILITY IN A POPULAR PROGRAM

What do you do next?

YOU DISCOVER A CRITICAL VULNERABILITY IN A POPULAR PROGRAM

What do you do next?



KEEP IT SECRET?

- This prevents independent risk assessment
- Assumes that security information can be kept secret

REPORT TO VENDOR?

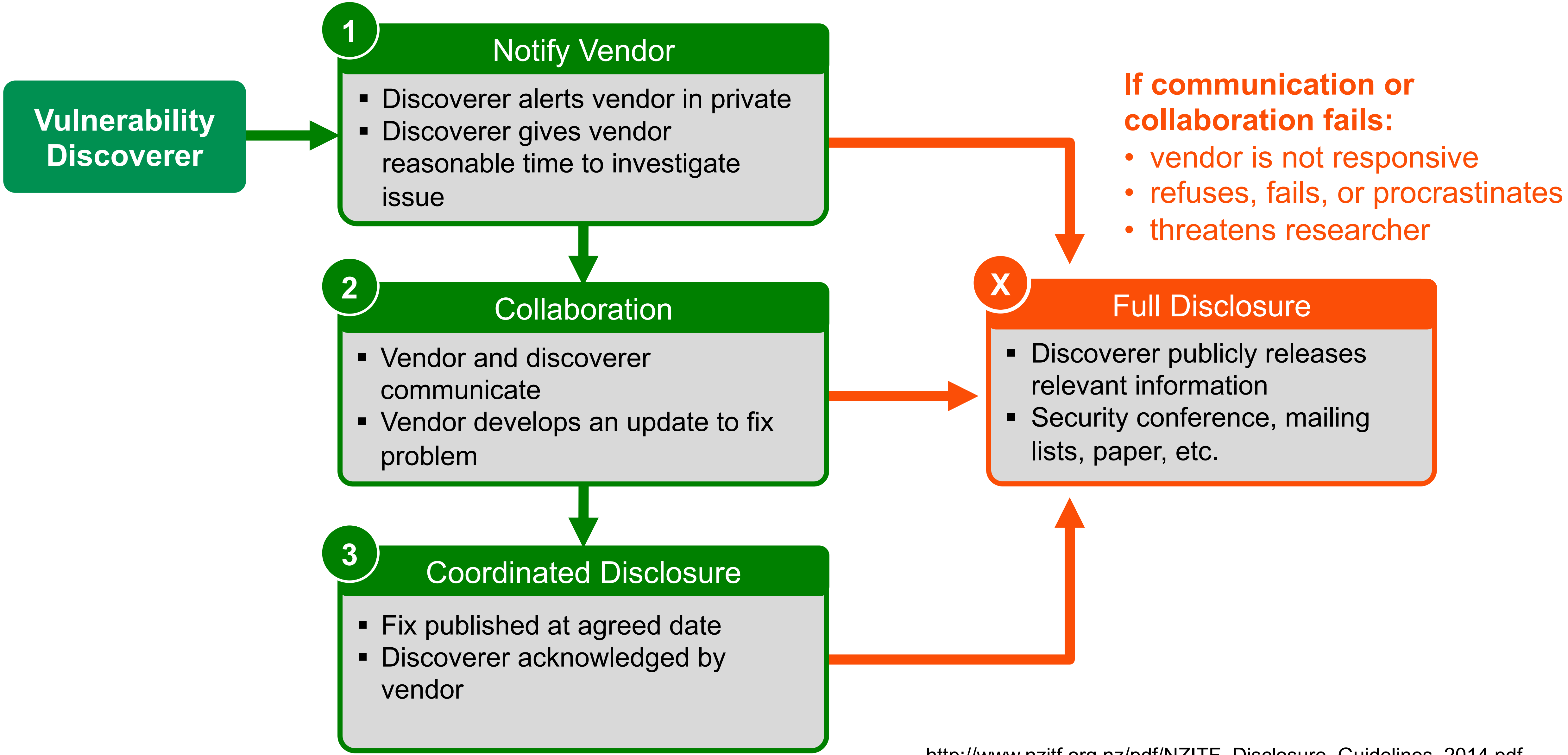
- Vendor might collaborate and fix problem
- Vendor might downplay, threaten you, or ignore the problem

FULL DISCLOSURE?

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

The desire of vendors to know about their vulnerabilities is not always matched by a willingness to act on the information.

COORDINATED DISCLOSURE PROCESS



Vulnerability Discoverer

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

If 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.

http://www.nzitf.org.nz/pdf/NZITF_Disclosure_Guidelines_2014.pdf

ISO29147 https://standards.iso.org/ittf/PubliclyAvailableStandards/c045170_ISO_IEC_29147_2014.zip

RISK MANAGEMENT CULTURE

Different approaches to risk management in organizations

- The purpose of risk management is **to improve the future, not to explain the past.**
- Risk management is about making decisions.

PATHOLOGIC	BUREAUCRATIC	GENERATIVE
Don’t want to know	May not find out	Actively seek
Messengers "shot"	Heard if they arrive	Messengers rewarded
Responsibility shirked	Compartmentalized	Responsibility shared
Failure punished	**Local repairs only**	**Failures beget reforms**
IDEAS DISCOURAGED	**IDEAS BEGET PROBLEMS**	**IDEAS WELCOMED**

Man-made Catastrophes and Risk Information Concealment https://www.springer.com/us/book/9783319242996

Digital Products

vs.

Physical Products

PERCEPTION OF RISK IN THE IOT WORLD

From the USERS perspective

Computer	Thermostat	Toaster	Smart Bear	Smart Meter	Smart-TV
dangerous	great	cool	cute	nice	cool

PERCEPTION OF RISK IN THE IOT WORLD

From the ATTACKERS perspective

Computer

antivirus, exploit mitigation patching

Thermostat

~~great~~

Toaster

~~cool~~

Smart Bear

~~cute~~

Smart Meter

~~nice~~

Smart-TV

~~cool~~

WE ARE PREPARED

WE ARE UNPREPARED

- For an attacker, all these devices are just **poorly protected networked computers**, running **complex software**, suffering the **same vulnerabilities**.
- **Easy targets**

KNOWN AND PROVEN SECURITY PRACTICE

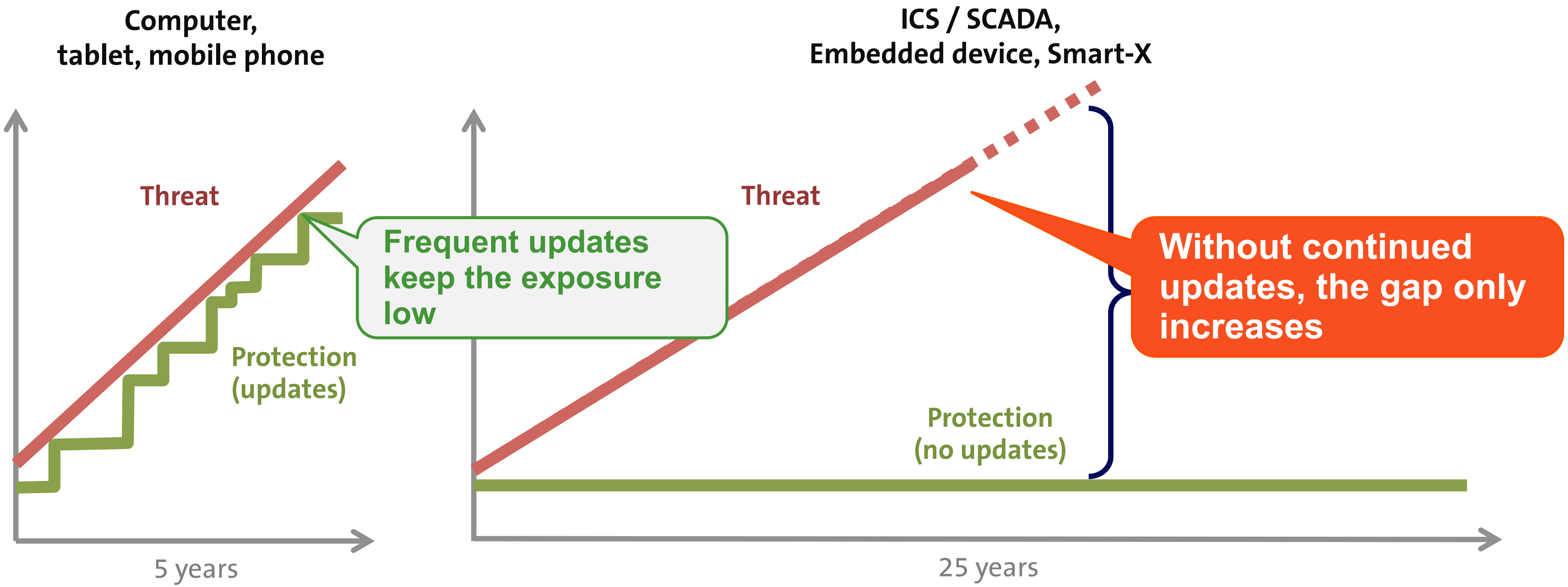
.. mostly ignored in the IOT world

PERSONAL COMPUTER	IOT DEVICE INDUSTRY CONTROL SYSTEMS (ICS)
▪ Networked and continuously hardened in battle ▪ Designed to withstand **external threats** ▪ **Secure defaults**	▪ Ran isolated for decades ▪ Designed for **high availability** and **safety,** not security ▪ **Insecure defaults**
▪ Exploit mitigation, antivirus ▪ **Frequent security updates**	▪ Old code, no protection ▪ **No security updates**

Most IOT and ICS systems are not fit for todays harsh threat environment: When deployed, or when being connected.

MANAGE AND PATCH VULNERABILITIES

Cyber devices require continued "security maintenance"



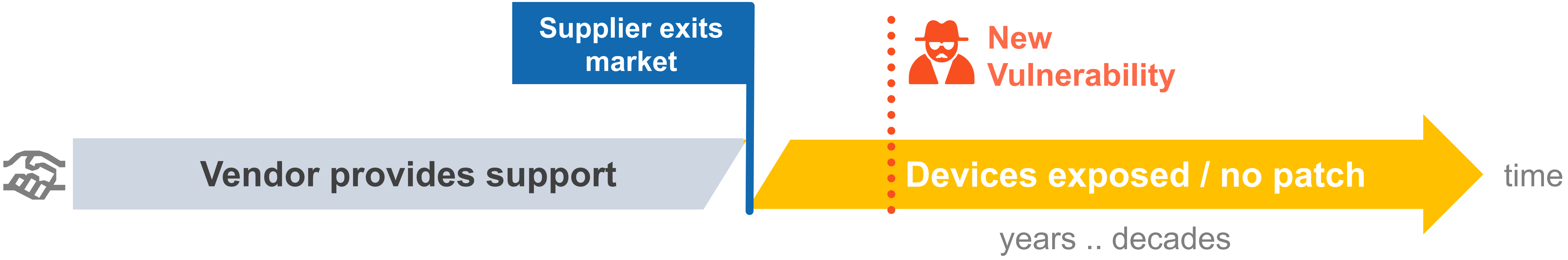
Frequent updates keep the exposure low

Without continued updates, the gap only increases

We rapidly create a huge future liability with devices lacking and automated and robust update functionality

TRADITIONAL PRODUCTS vs. DIGITAL PRODUCTS

Traditional products rarely change after delivery, whereas digital products constantly require security updates.



Supplier exits market

New Vulnerability

Vendor provides support

Devices exposed / no patch

time

years .. decades

Industry control systems (ICS) may have a **lifetime of decades ...**

THREAT

VENDOR GOES BANKRUPT WHILE DEVICES ARE STILL DEPLOYED

- Numerous devices left exposed with no security updates for years or decades
- Replacement is very difficult or too prohibitively expensive.

OPTIONS

PREPARE FOR THIS BEFORE PURCHASE

- **Code Escrow** - Copy of source code deposited with trusted third party.
  Open Source – Mandate to open source code

Lessons from History

OTHER CRITICAL GOODS

Historically, societies always developed binding norms to ensure the safety and security of critical goods – Enforced by harsh testing

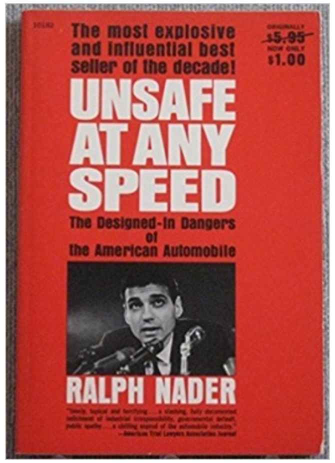
AUTOMOTIVE	▪ Extensive testing of vehicles before admission ▪ Periodic inspections	
AVIATION	▪ Extensive testing of aircraft before admission ▪ Extensive operations requirements ▪ Periodic inspections	
MEDICINE	▪ Extensive testing of new drugs before admission	
FOOD	▪ Extensive requirements for processing and delivery ▪ Periodic and surprise inspections	
CYBER	▪ **No norms or binding minimum requirements covering the security or the integrity of goods** ▪ **No product liability**	🚫

CALLS FOR SECURITY NORMS ARE TYPICALLY FIERCELY RESISTED BY THE INDUSTRY WITH ALWAYS THE SAME ARGUMENTS

INDUSTRY ARGUMENTS

- The product is safe - accidents are the fault of the user
- Security norms are unnecessary - they will ruin the industry
- Norms will stifle innovation

AUTOMOTIVE INDUSTRY
(industry still exists)

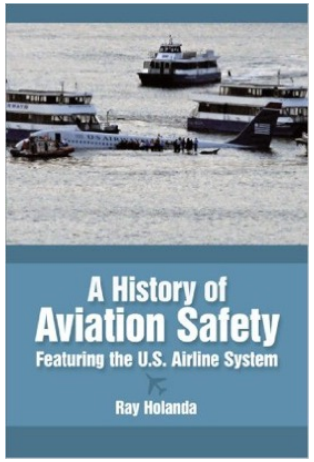

The most explosive and influential best seller of the decade!
$5.95
$1.00
UNSAFE AT ANY SPEED
The Designed-In Dangers of the American Automobile
RALPH NADER

Ralph Nader accusing car manufacturers of resistance to the introduction of safety features such as seat belts, and their general reluctance to spend money on improving safety.

Let to introduction of crash-test dummies and seat belts after disputes.

Source: https://en.wikipedia.org/wiki/Unsafe_at_Any_Speed

AVIATION INDUSTRY
(industry still exists)


A History of Aviation Safety
Featuring the U.S. Airline System
Ray Holanda

First 50 hour endurance tests for aircraft engines against the protests of the industry: Over half of the engines could not pass the initial test (1920-30)

Early philosophy:

Fly it, break it, fix it, blame the pilot

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

Too often, we wait for catastrophe to spur change.

Absence of evidence is not evidence of absence.

Thank You

NOT COVERED IN THIS TALK

Talk to me for more

- Economics of Cyber Security
- Supply Chain Security
- Protection vs. Detection
- Erosion of Privacy

- How to close FRA with a budget of $5'000 and two months preparation

- **Blockchain and Artificial Intelligence**
  (these solve all security problems according to the cyber industries' marketing ..)

CONCLUSION / RECOMMENDATIONS

Technology based security solutions have to complement other domains to achieve the desired security level.

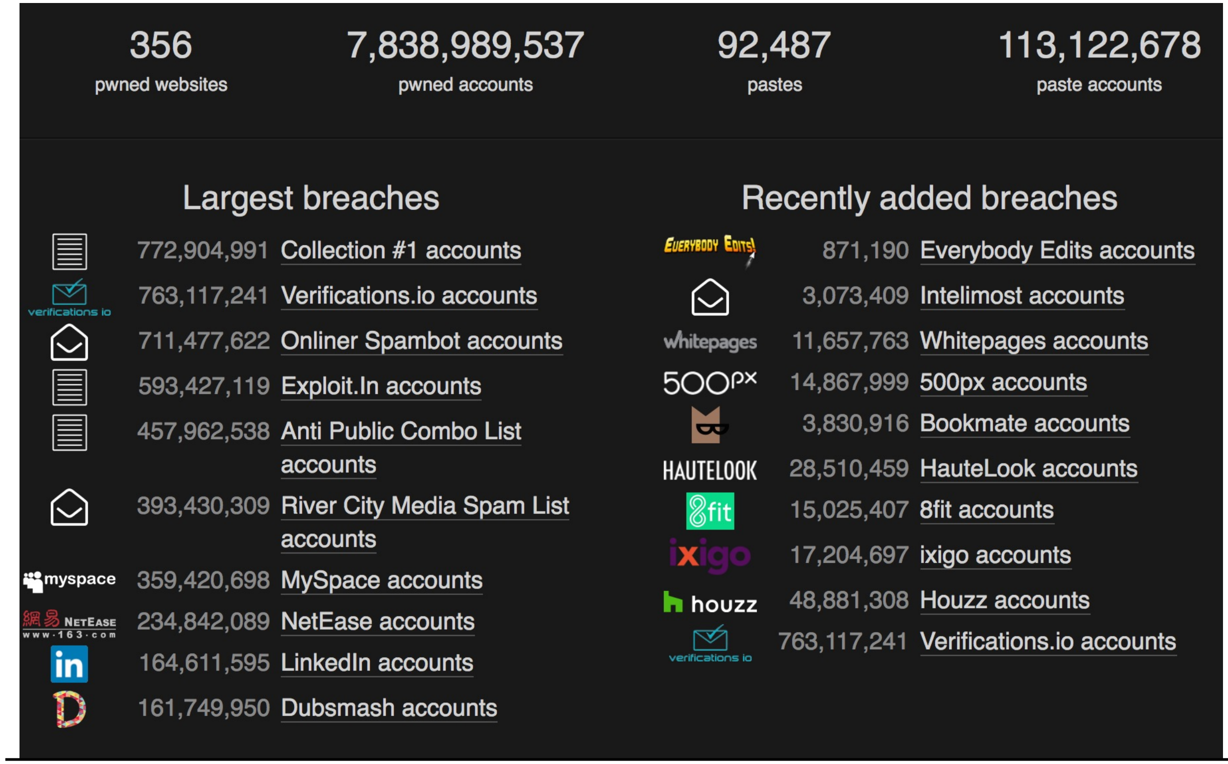
Challenges	What is needed
The security of individual components (e.g. technologies) **does not imply the security of the complete system** (connected vehicle ecosystem).	• Design systems with **redundancy and resiliency** (fail safe, fail secure, Secure SDLC). • Realistic testing plans for the **complete system (end-to-end).**
The continued innovation of attackers, threats, technologies, society, and use-cases creates **a dynamic and adaptive threat** landscape.	• Prepare for **continued adaptation** to new threats**, no matter what the driver or domain behind the attacker or threat**. • Comprehensive threat modelling and continued threat intelligence and **security monitoring**.
Software drives everything, and there is no such thing as secure software. Prepare for the continued **discovery and publication of vulnerabilities in software and hardware**.	• Active **management of vulnerabilities** (coordinated disclosure, bug bounty) • Robust and scalable process to deploy security updates timely and efficiently – **on any connected device**.
We depend on a **complex supply chain of hardware and software** components, which **can not be fully controlled**. Assume that some components are already compromised.	• Systematic **security and integrity testing** of all critical components (reverse engineering of software & hardware). • Comprehensive security appendix in contracts with suppliers

APPENDIX

Data Breaches

DATA BREACHES

Data breaches and leaked accounts increased



356	7,838,989,537	92,487	113,122,678
pwned websites	pwned accounts	pastes	paste accounts

Largest breaches

772,904,991	Collection #1 accounts
763,117,241	Verifications.io accounts
711,477,622	Onliner Spambot accounts
593,427,119	Exploit.In accounts
457,962,538	Anti Public Combo List accounts
393,430,309	River City Media Spam List accounts
359,420,698	MySpace accounts
234,842,089	NetEase accounts
164,611,595	LinkedIn accounts
161,749,950	Dubsmash accounts

Recently added breaches

871,190	Everybody Edits accounts
3,073,409	Intelimost accounts
11,657,763	Whitepages accounts
14,867,999	500px accounts
3,830,916	Bookmate accounts
28,510,459	HauteLook accounts
15,025,407	8fit accounts
17,204,697	ixigo accounts
48,881,308	Houzz accounts
763,117,241	Verifications.io accounts

Verified data breaches with accounts and passwords available at

https://haveibeenpwned.com/

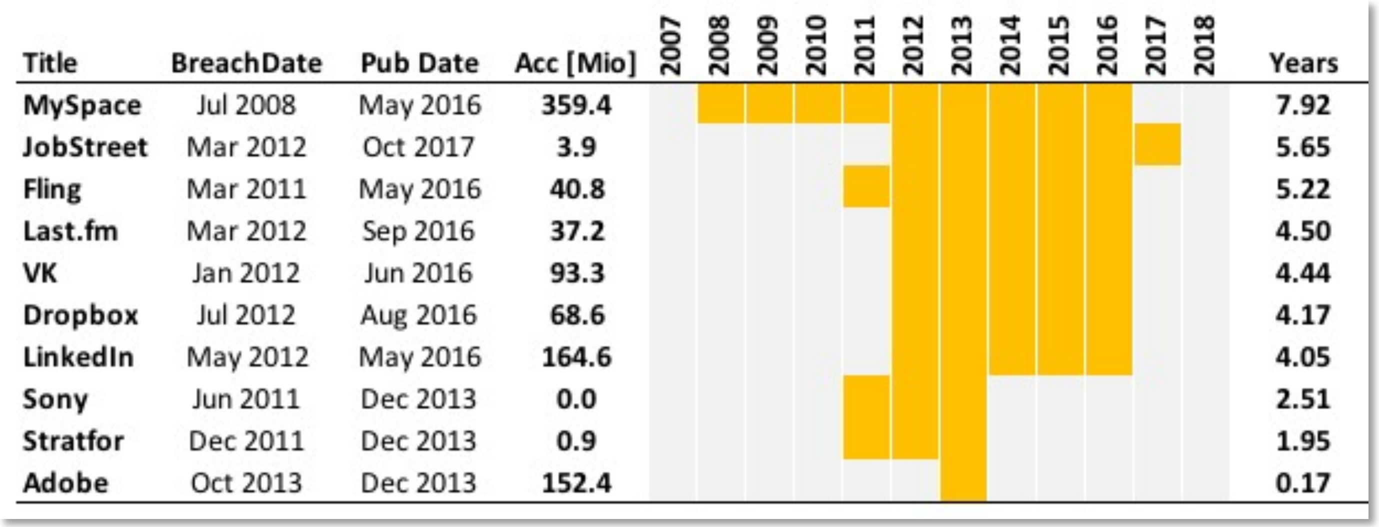
May 2017	May 2018	2019
240 verified breaches (total) **2,186** Million breached accounts	**283** verified breaches (total) **5,043** Million breached accounts	**356** verified breaches (total) **7,838** Million breached accounts
10 days between breaches days in 2017 **38.7** Million accounts/breach on average	**10** days between breaches in 2018 **20.2** Million accounts/breach on average	**18** days between breaches in 2019 **311** Million accounts/breach on average

WHAT ARE THE CONSEQUENCES OF DATA BREACHES?

We must assume that critical data of yet unpublished data breaches is silently used in the hands of criminals or nation states – also today.

Dropbox (68M), **LinkedIn** (164M), **Last.fm** (37.2M), and **VK** (93.3M) were all breached in **2012**, and the breaches became public in **2016**.

Until 2016 the **367.4 Million users** of these portals did not know that their account data was **available in the underground for years**.



Title	BreachDate	Pub Date	Acc [Mio]	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	Years
MySpace	Jul 2008	May 2016	359.4		■	■	■	■	■	■	■	■	■			7.92
JobStreet	Mar 2012	Oct 2017	3.9						■	■	■	■	■	■		5.65
Fling	Mar 2011	May 2016	40.8					■	■	■	■	■	■			5.22
Last.fm	Mar 2012	Sep 2016	37.2						■	■	■	■	■			4.50
VK	Jan 2012	Jun 2016	93.3						■	■	■	■	■			4.44
Dropbox	Jul 2012	Aug 2016	68.6						■	■	■	■	■			4.17
LinkedIn	May 2012	May 2016	164.6						■	■	■	■	■			4.05
Sony	Jun 2011	Dec 2013	0.0					■	■	■						2.51
Stratfor	Dec 2011	Dec 2013	0.9					■	■	■						1.95
Adobe	Oct 2013	Dec 2013	152.4							■						0.17

LAW OF SECURITY

- Absolutely secure systems do not exist.
- To halve your vulnerability, you have to double your expenditure.
- Cryptography is typically bypassed, not penetrated.

Adi Shamir, Turing Lecture 2004

SOFTWARE VULNERABILITIES AND EXPLOITS

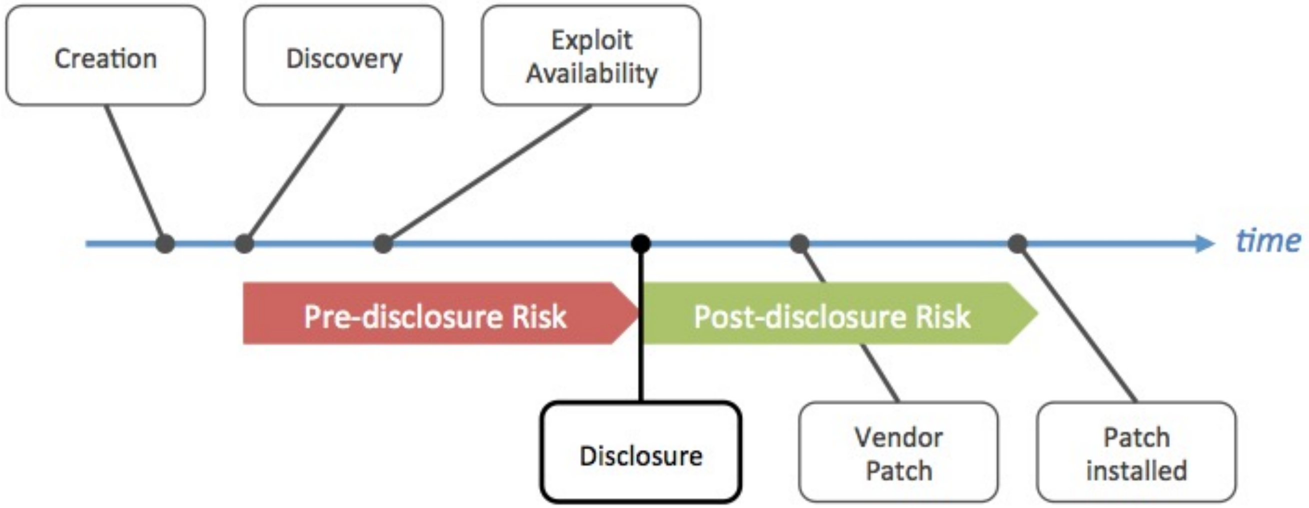
There is no unique definition of the term “vulnerability”. A vulnerability itself does no harm, but if exploited it typically results in unwanted consequences

VULNERABILITY A vulnerability is a weakness in software (or hardware) that enables an attacker to compromise the software or the data that it processes.

EXPLOIT An exploit is a piece of software, a set of data, or sequence of commands that takes advantage of a vulnerability in order to cause unintended or unanticipated behavior to occur in software or hardware.

VULNERABILITY LIFECYCLE PERIODS

What can users of vulnerable software know or do?



Period	Description	Control
Pre-disclosure risk	During the time from **discovery to disclosure**, only a privileged group is aware of the vulnerability. This group could be anyone from discoverer, hackers, to cyber-criminals. Users are vulnerable but cannot assess their risk as they are not aware of the vulnerability.	No Control
Post-disclosure risk	During the time from **disclosure to patch availability** the user of the software waits for the vendor to release a patch. However, the public can assess their individual risk and implement a workaround based on the information of the public disclosure.	Software Vendor
Post-patch phase	The time from **patch availability to patch installation**. The duration of this period is typically under direct control of the user of the affected software.	User

Source: http://www.techzoom.net/Papers/Modeling_The_Security_Ecosystem_(2009).pdf

OFFENCE CAN BE FAVORED OVER DEFENSE!

If you are the director of the NSA and have an exploit for the latest version of Windows - do you tell Microsoft?

You have an zero-day exploit
Do you tell the vendor to fix the product?

Tell the vendor	Don't tell the vendor
▪ Tell the vendor to fix the product ▪ Protect 300M Americans	▪ Don’t tell the vendor ▪ You are able to hack 400M European and 1,000M Chinese, ..., computers

- If the Chinese hack US systems, they keep quiet.
- If you hack their systems, you can brag about it to the President.

WannaCry: Exploit got stolen from NSA, NSA did not notify Microsoft when exploit was publicly offered for sale.

https://www.schneier.com/blog/archives/2017/05/who_are_the_sha.html