Innovative or “Fully Secure”? – Pick one.

Karsten Nohl <nohl@srlabs.de>

Security Research Labs

whoami

Karsten Nohl

Founder of SRLabs (2010-)

- Conducting hacking research in Berlin. We found systematic weaknesses in a range of technologies: GSM, SIM cards, SS7, DECT phones, payment protocols, …
- Developed SRLabs into leading boutique consultancy for managing hacking risks

CISO at Reliance Jio (2014-2017)

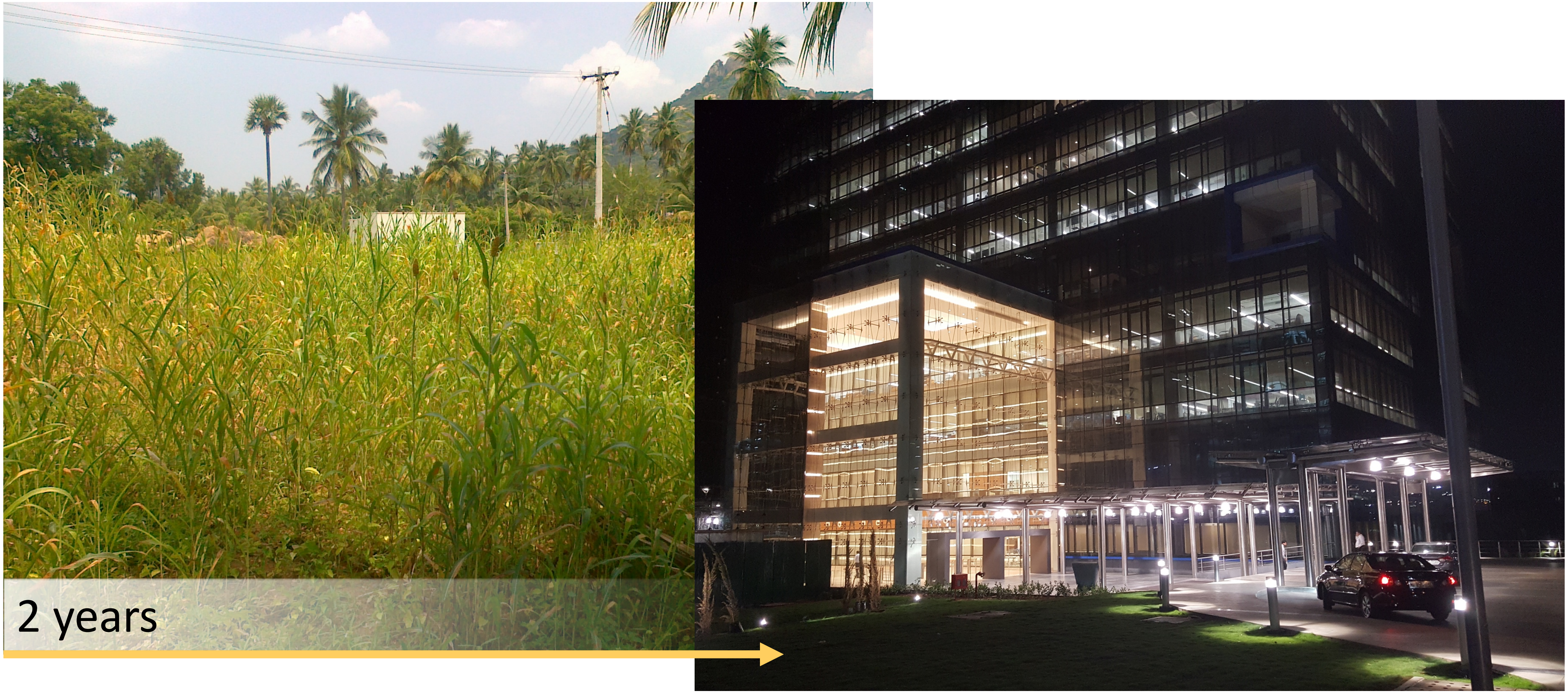
- Largest and fastest growing start-up in history, offering telco and digital services
- Acquired 100 million telco customers in India in its first 6 months
- Leading a team of 140 security experts

CISO at Axiata (2017)

- Telco group with 300 million subscribers across eight countries in Asia
- Building a central team to establish and coordinate hacking defense across the group

Who will fully digitize faster?

A true green field start-up



Jio

“We are not creating a brand. We are starting a

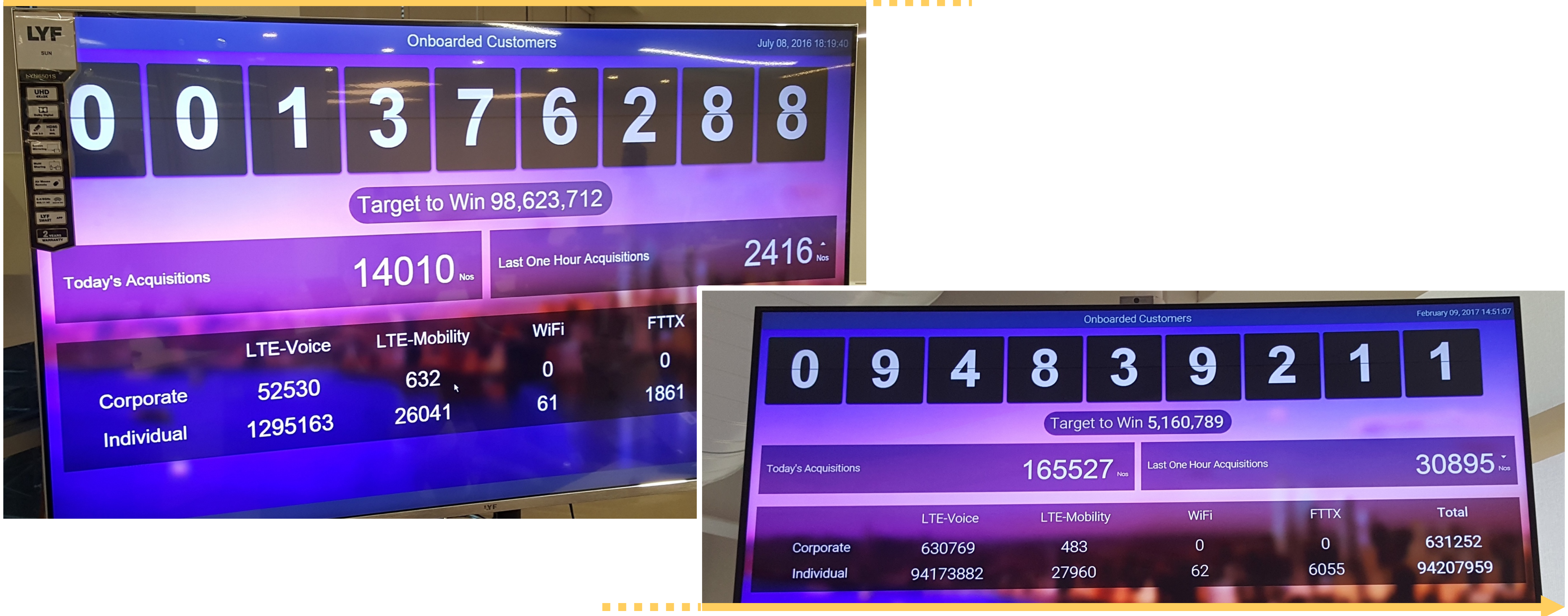
movement...

A movement that’s not about Reliance, but what we want to do for people. A movement for millions of Indians.”

Mukesh Ambani

Technology at mega scale – Launching Jio

Internal testing with 1 million employees + family



Onboarded Customers

July 08, 2016 18:19:40

0 0 1 3 7 6 2 8 8

Target to Win 98,623,712

Today's Acquisitions 14010 Nos

Last One Hour Acquisitions 2416 Nos

	LTE-Voice	LTE-Mobility	WiFi	FTTX
Corporate	52530	632	0	0
Individual	1295163	26041	61	1861

Onboarded Customers

February 09, 2017 14:51:07

0 9 4 8 3 9 2 1 1

Target to Win 5,160,789

Today's Acquisitions 165527 Nos

Last One Hour Acquisitions 30895 Nos

	LTE-Voice	LTE-Mobility	WiFi	FTTX	Total
Corporate	630769	483	0	0	631252
Individual	94173882	27960	62	6055	94207959

5 months after launch: 100 million SIM customers

Great products require some freedom during development

How do you enforce standards in the world's largest startup?

Don't even try!

- + Minimal set of mandatory interface technologies: SSO, Charging
- + 100% agile development in autonomous teams
- + Extensive testing, both automated and with hundreds of students

- Technology teams can create what and how they want without toll gates, heavy architecture requirements, or release planning
- Quality and consistency is enforced through rigorous testing before launch
- Security is managed through Readiness Dashboards

How much security should we be aiming for?

My goal is to convince you that:

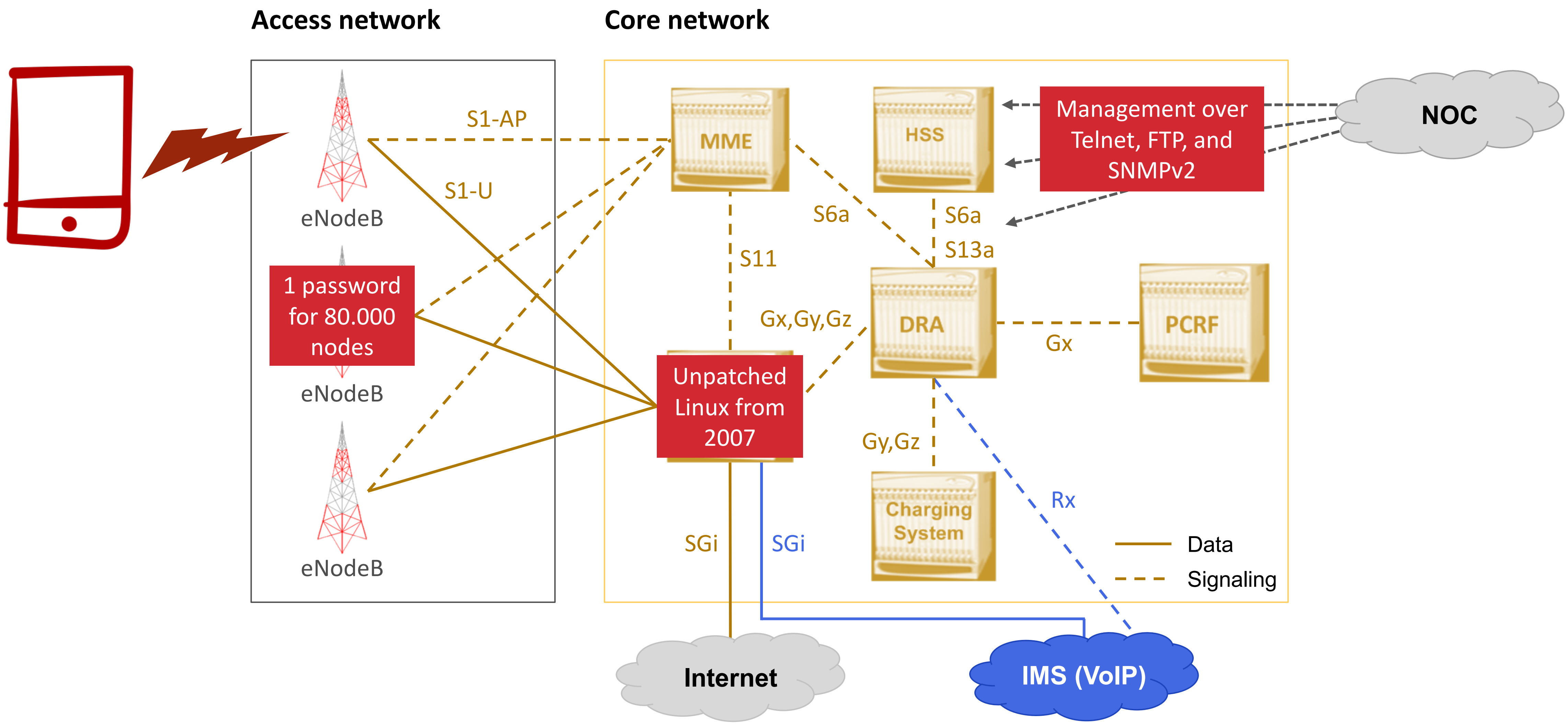
1	A high security level is near impossible to achieve
2	Trying to achieve high security kills innovation and companies in the long run

So we can then talk about:

A	How to set realistic security goals
B	How to best measure and manage security
C	How to embed security in a innovation-friendly way

Security vs. Legacy – The practical limits of security

4G/LTE is a revolution of all mobile network components, but not of their security :-/



1 password for 80.000 nodes

Unpatched Linux from 2007

Management over Telnet, FTP, and SNMPv2

Security Research Labs

Legacy challenges extend onto endpoints

Employee security

Goal: Authenticate with strong biometrics to Windows and Enterprise services

Status: Fail.
A one-year-research project could not identify a biometric vendor/solution to work in a large ActiveDirectory

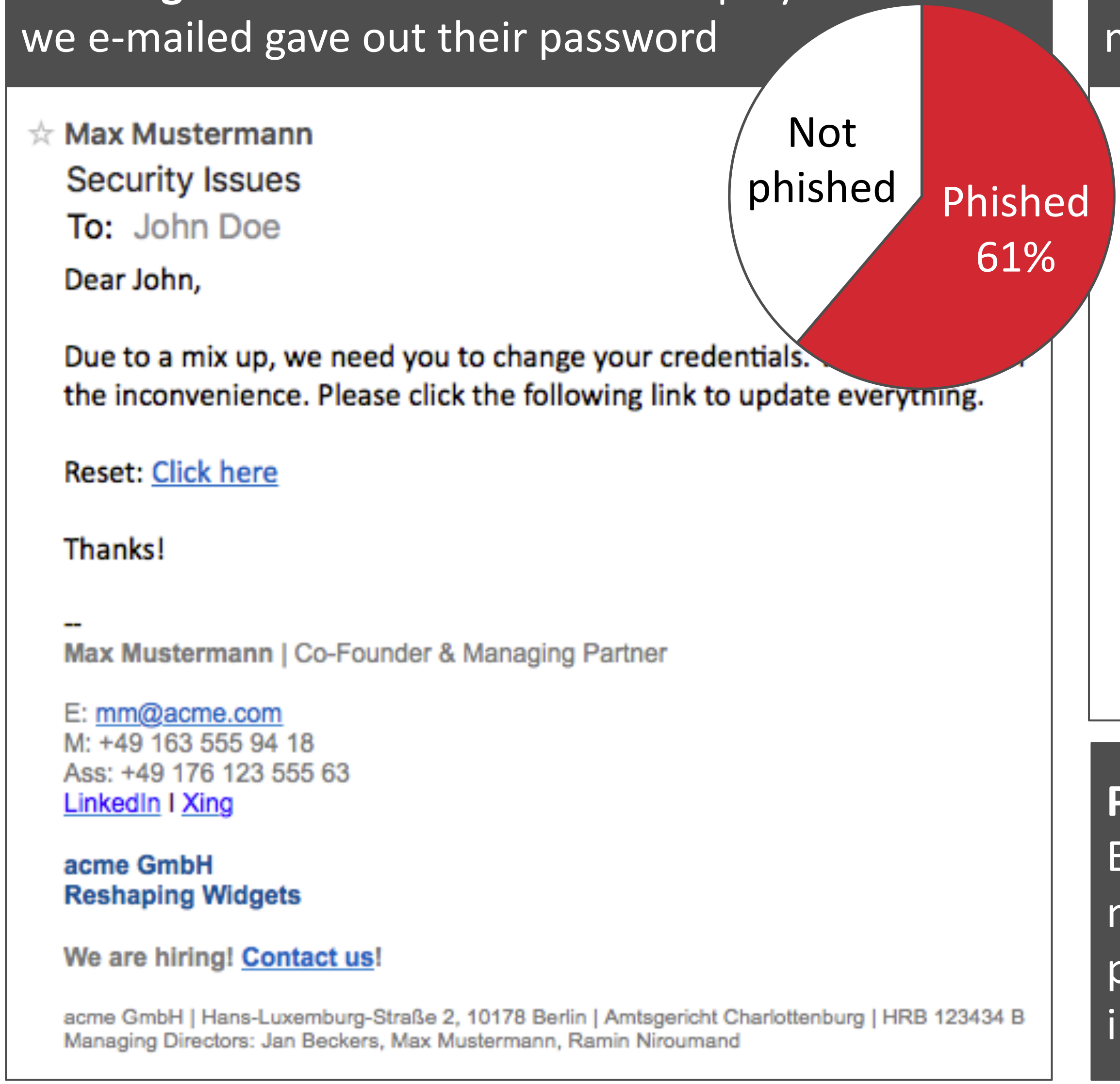
Customer security

Goal: Provide an up-to-date Android to mobile customers

Status: Fail.
Could not find any vendor other than Google themselves who installs all security patches

Majority of employees initially fell for phishing and vishing attacks

Phishing – More than half of the employees we e-mailed gave out their password



☆ Max Mustermann

Security Issues

To: John Doe

Dear John,

Due to a mix up, we need you to change your credentials. … the inconvenience. Please click the following link to update everything.

Reset: Click here

Thanks!

--

Max Mustermann | Co-Founder & Managing Partner

E: mm@acme.com
M: +49 163 555 94 18
Ass: +49 176 123 555 63
LinkedIn I Xing

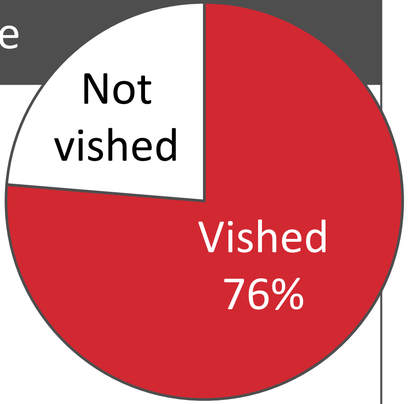
acme GmbH
Reshaping Widgets

We are hiring! Contact us!

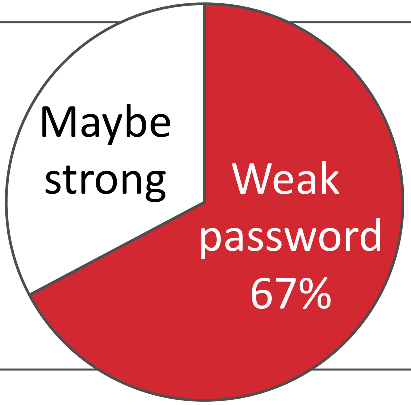
acme GmbH | Hans-Luxemburg-Straße 2, 10178 Berlin | Amtsgericht Charlottenburg | HRB 123434 B
Managing Directors: Jan Beckers, Max Mustermann, Ramin Niroumand

Vishing – Of the employees that we called, the vast majority gave us their passwords over the phone

Hi! Sujeet from Helpdesk here. I need to update our user database. Could I have your login name and password?
Sure Sujeet…It's win@1234
Details



Password quality – Equally concerning, many of these passwords were insecure



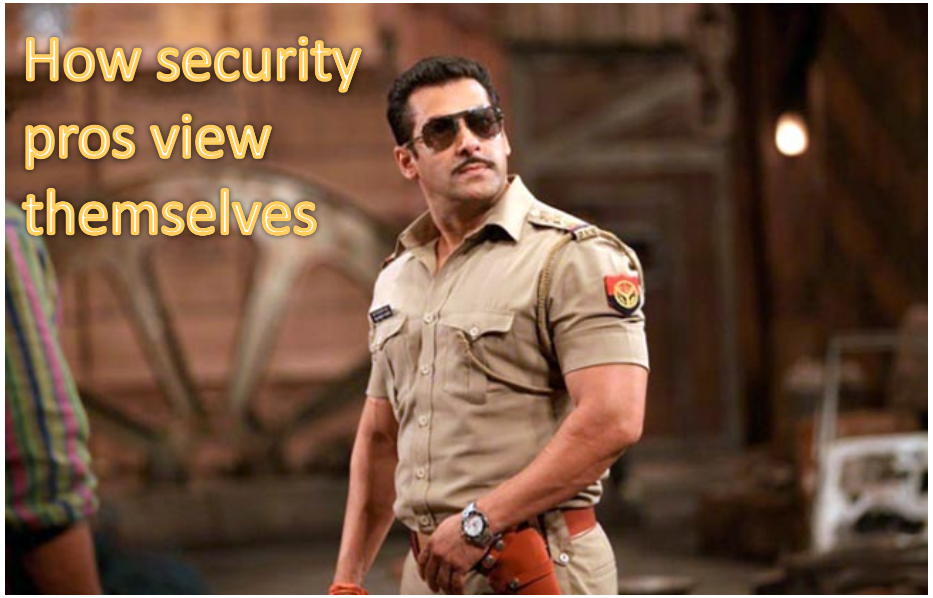
”Security by design” is a mere dream

Even a 100% greenfield start-up is tied to insecure legacy

Servers	▪ Often insecure operating system and middleware
Endpoints	▪ Windows and Android
IT ops	▪ Insecure access and management standards
Employees	▪ Gullible human beings ☹

Security vs. Innovation –
Why trying to reach high security levels often backfires

How should we fight legacy security issues?



vs.

Are you insane!? This bottle might be a deadly bomb capable of killing hundreds of people! So I'll throw it in this wastebasket right next to me ...

Attention for hacking news hinders effective security management

1 Security researchers* take extreme positions

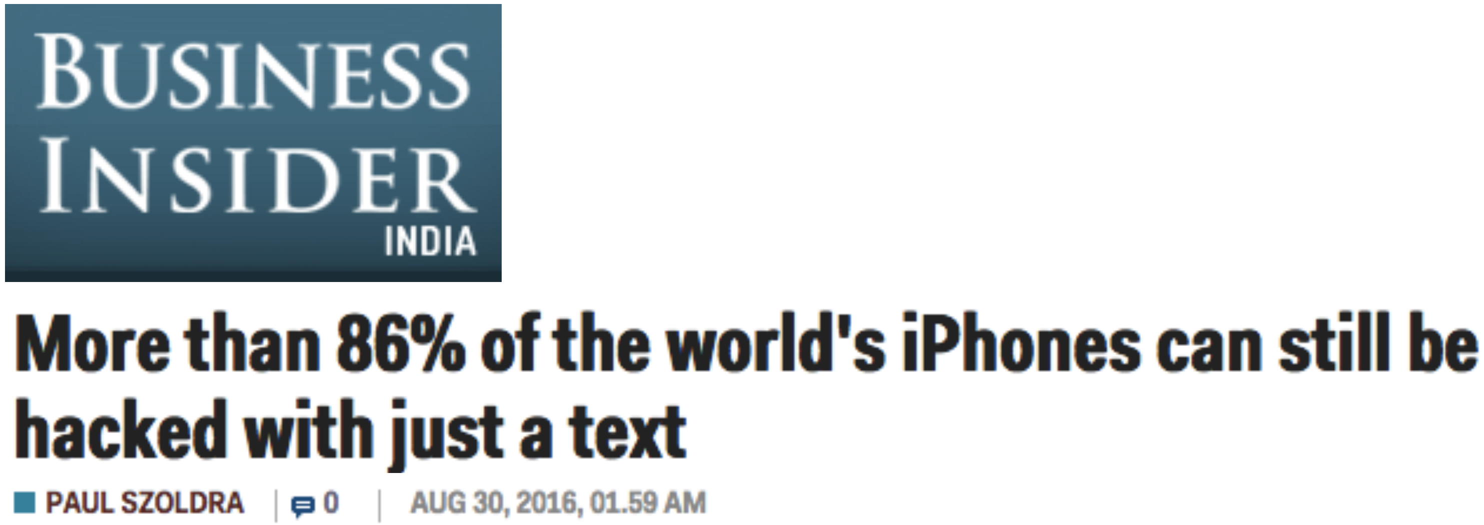
2 Many companies only react to extreme positions

3 The security community is fighting vulnerabilities, not risks

* As reported in the media

iOS is insecure, right?

Pegasus malware

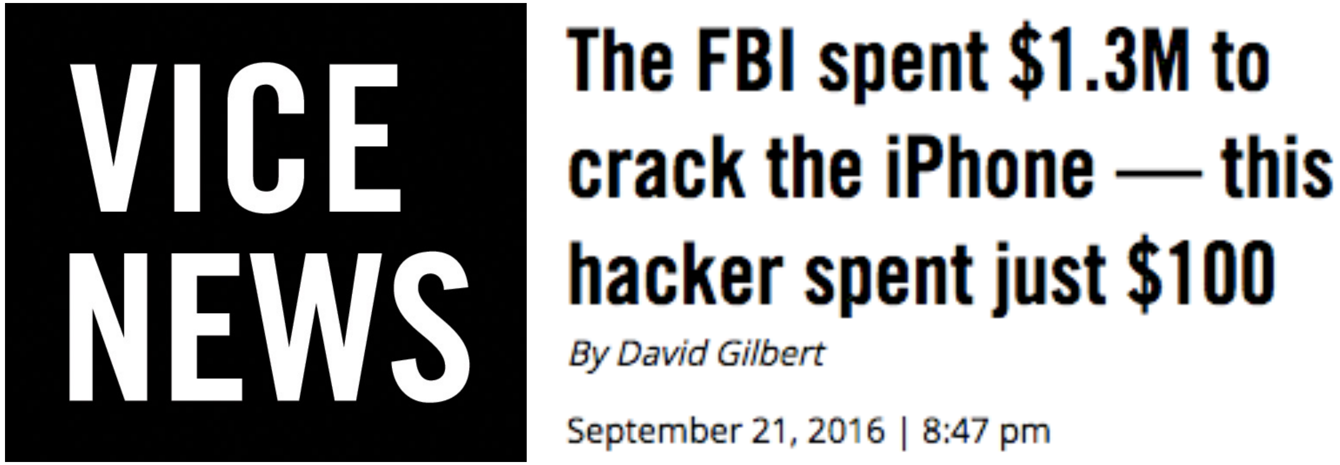


BUSINESS INSIDER INDIA

More than 86% of the world's iPhones can still be hacked with just a text

PAUL SZOLDRA | 0 | AUG 30, 2016, 01.59 AM

FBI-style hardware hacking



VICE NEWS

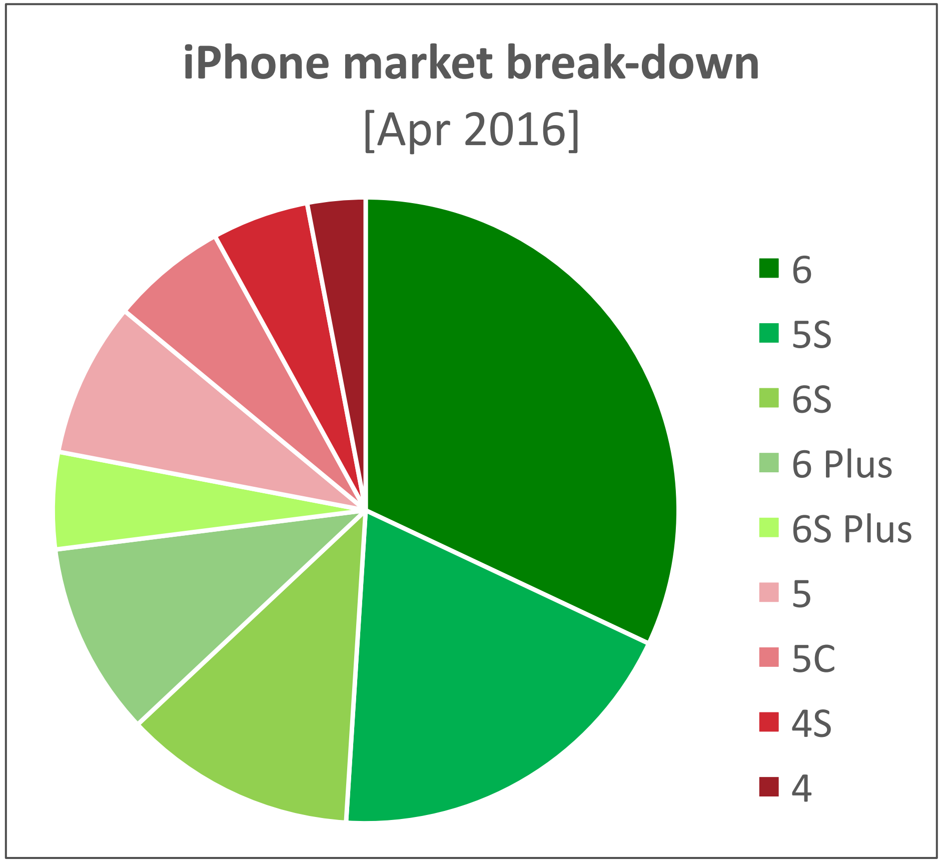
The FBI spent $1.3M to crack the iPhone — this hacker spent just $100

By David Gilbert

September 21, 2016 | 8:47 pm

Your iPhone getting hacked is rather unlikely

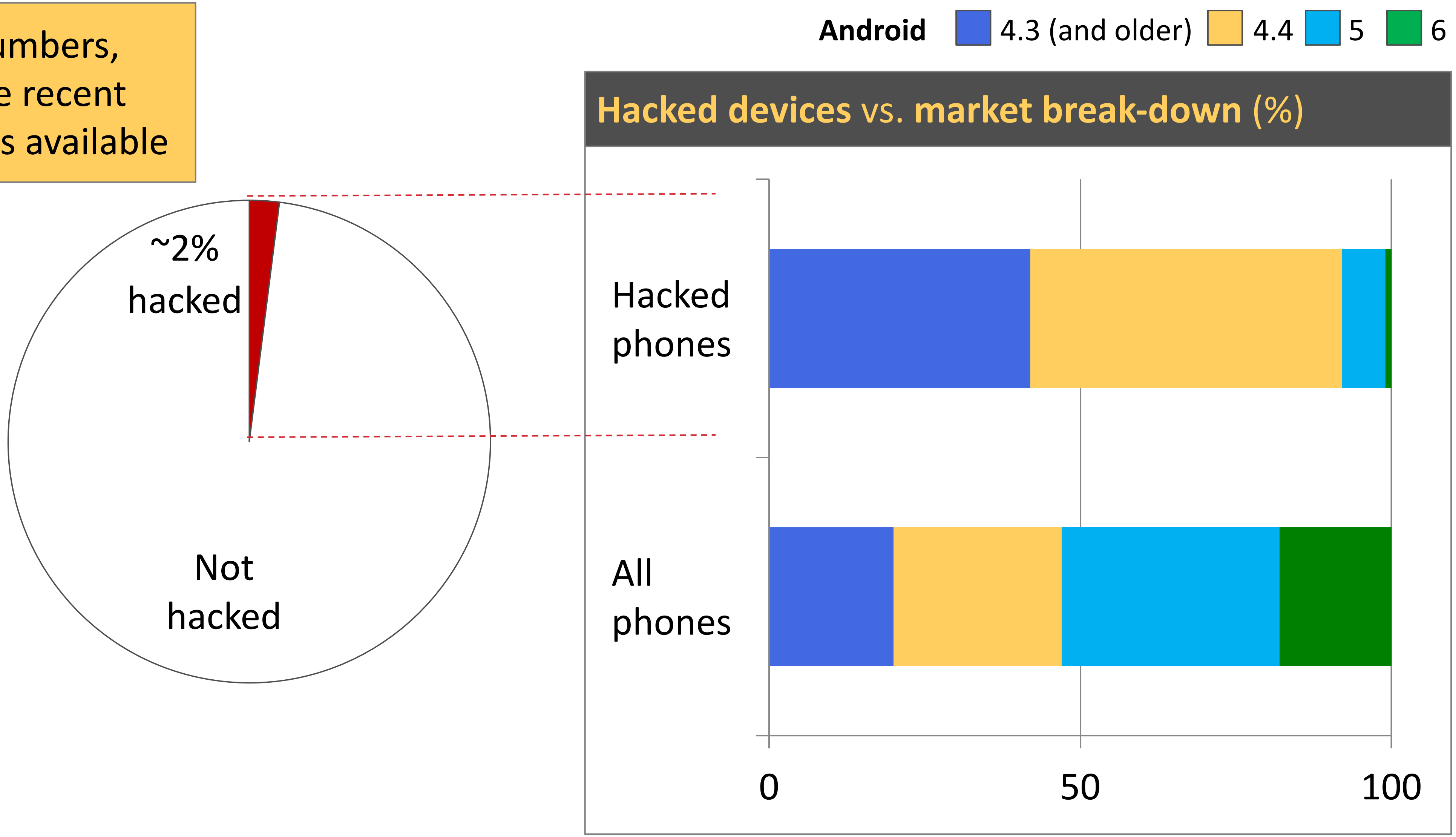
BUSINESS INSIDER INDIA	Pegasus malware	- 1 billion iOS devices possibly vulnerable + Only one (!) attempted infection + Apple patched the vulnerability within 10 days
VICE NEWS	FBI-style hardware hacking	- Hack is now publicly available at low cost + Only possible with hardware access + Only works against the oldest 22% of iPhones (5c and older, March 2016)



Source for graph: http://info.localytics.com/blog/how-will-apples-newest-iphone-impact-mobile-engagement

Few Android phones get hacked; those that do are outdated

2016 numbers,
no more recent
statistics available

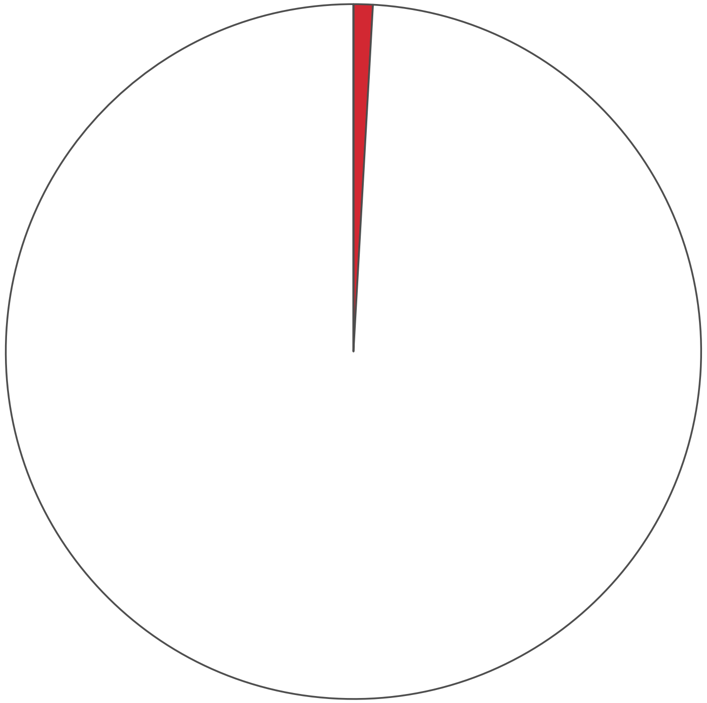


Source: developer.android.com/about/dashboards/index.html ,
https://blog.checkpoint.com/wp-content/uploads/2016/07/HummingBad-Research-report_FINAL-62916.pdf

Should mobile really be a chief security concern?

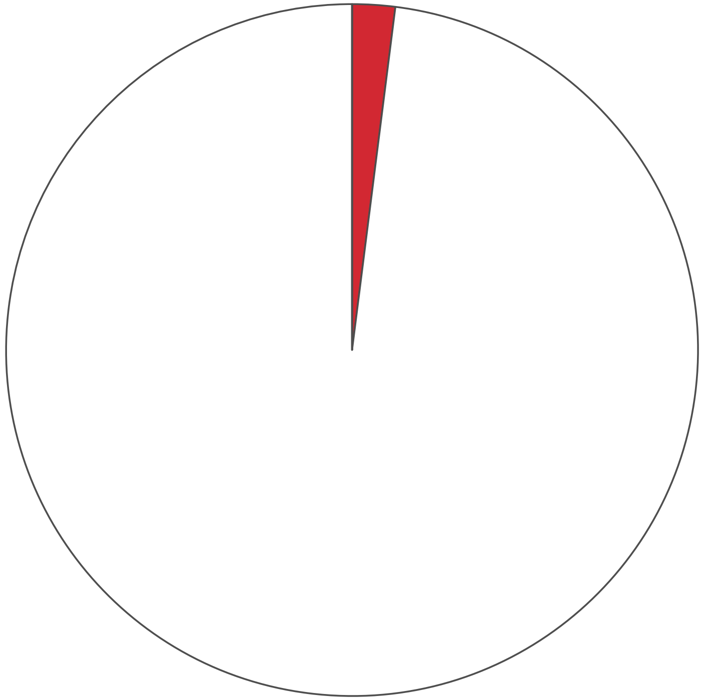
iOS infection rate

<0.1%



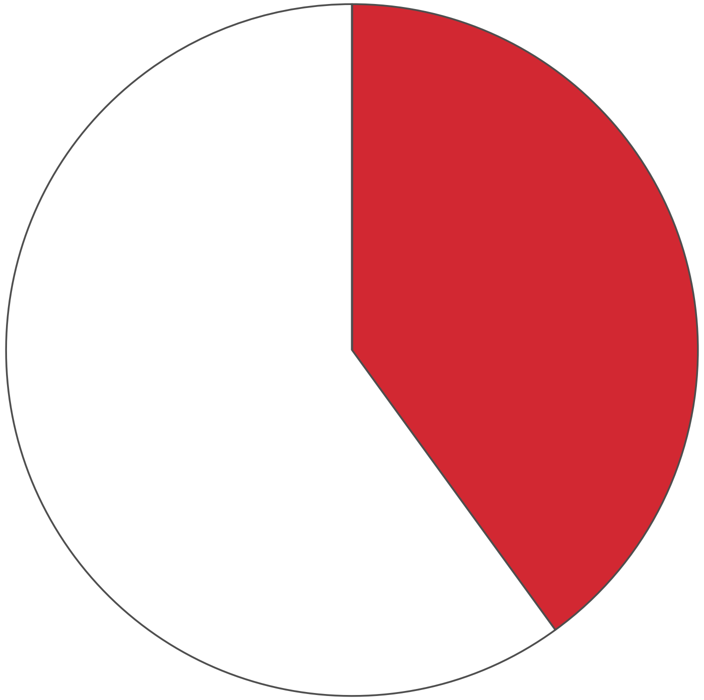
Android infection rate

~2%
(<0.2% for current devices)



Windows infection

20-40%



Security Research Labs

http://www.pandasecurity.com/mediacenter/src/uploads/2016/05/Pandalabs-2016-T1-EN-LR.pdf

Attention for hacking news hinders effective security management

1. Security researchers take extreme positions
2. Many companies only react to extreme positions
3. The security community is fighting vulnerabilities, not risks

Companies InfoSec priorities are not aligned with actual incidents

ILLUSTRATIVE

Typical corporate InfoSec priorities

1. Buy **iOS** security software
2. Ban or lock down **Android** devices

…

10. Do something uncreative about **Windows** security, like upgrading antivirus software

vs.

Actual hacking incidents

1. **Windows**
2. **Windows**
3. Social engineering
4. **Windows**

…

100. **Android**

Attention for hacking news hinders effective security management

1 Security researchers take extreme positions

2 Many companies only react to extreme positions

3 The security community is fighting vulnerabilities, not risks

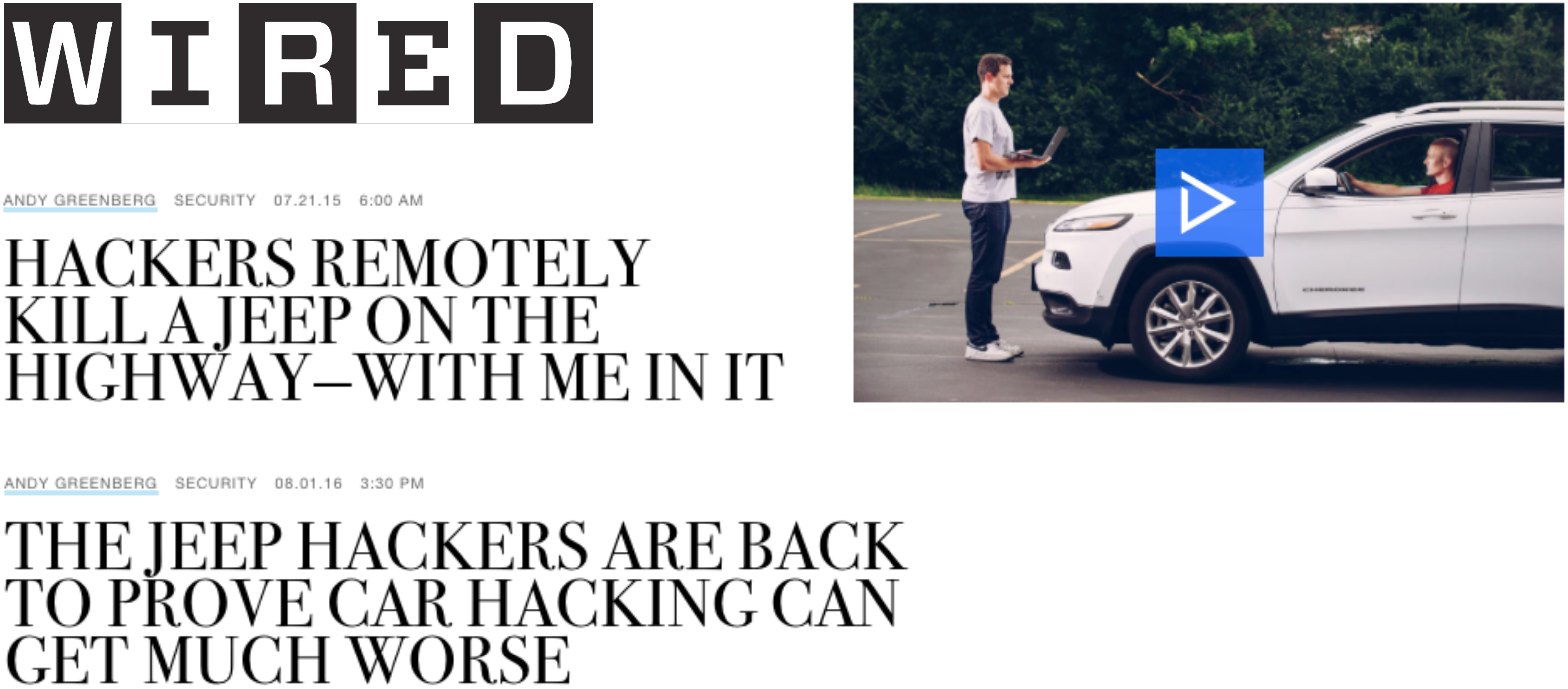
Your time is best spent protecting from most likely threats

ILLUSTRATIVE

○ Low ◐ Medium ● High

	Vulnerability / Hacking ease	×	Hacker incentive	×	Damage	=	Risk	
BadUSB	◐ Infect computers from USB firmwares		○ Local attack propagation		(Varies by system)		◐	Don’t bother protecting your Internet-exposed computers from BadUSB before you solved the malware challenge
Targeted malware	● Infect Windows through e-mail attachments or malicious websites		● Remote infection		(Varies by system)		●	

Next big hacking frontier: Cars?



WIRED

ANDY GREENBERG SECURITY 07.21.15 6:00 AM

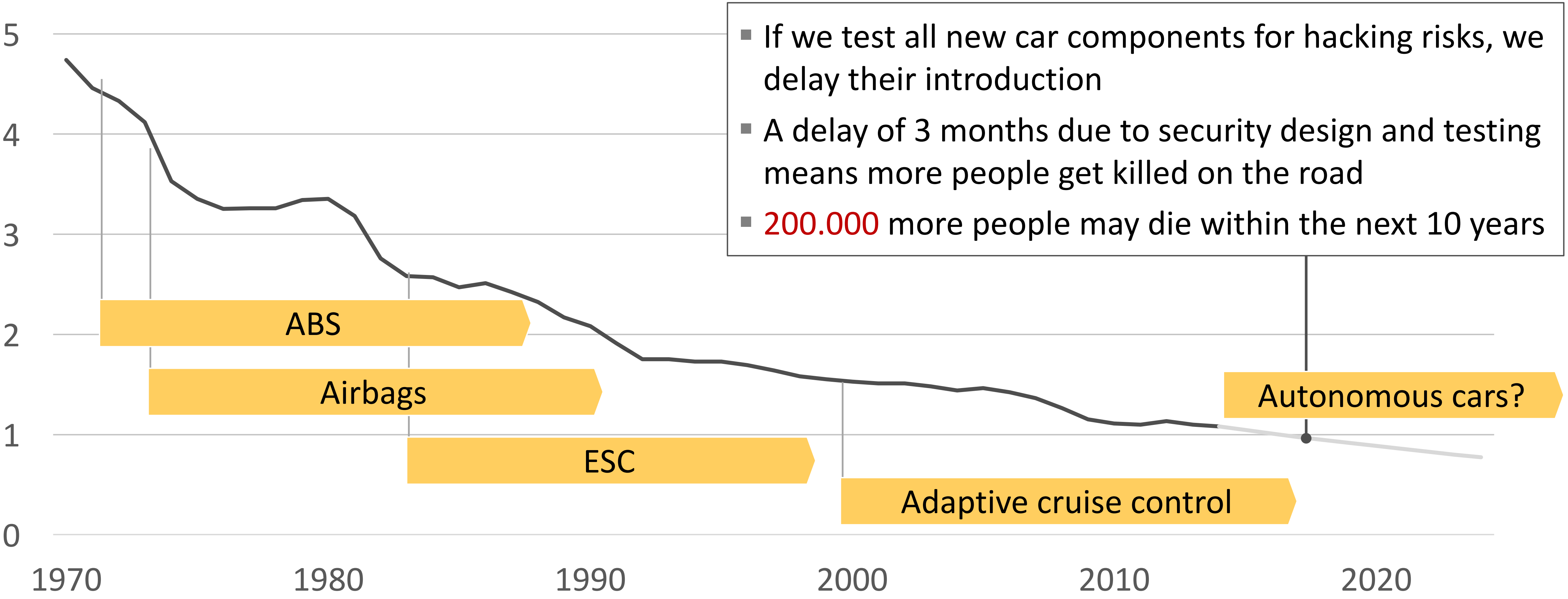
HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT

ANDY GREENBERG SECURITY 08.01.16 3:30 PM

THE JEEP HACKERS ARE BACK TO PROVE CAR HACKING CAN GET MUCH WORSE

Security caution can delay safety, and ultimately kill people

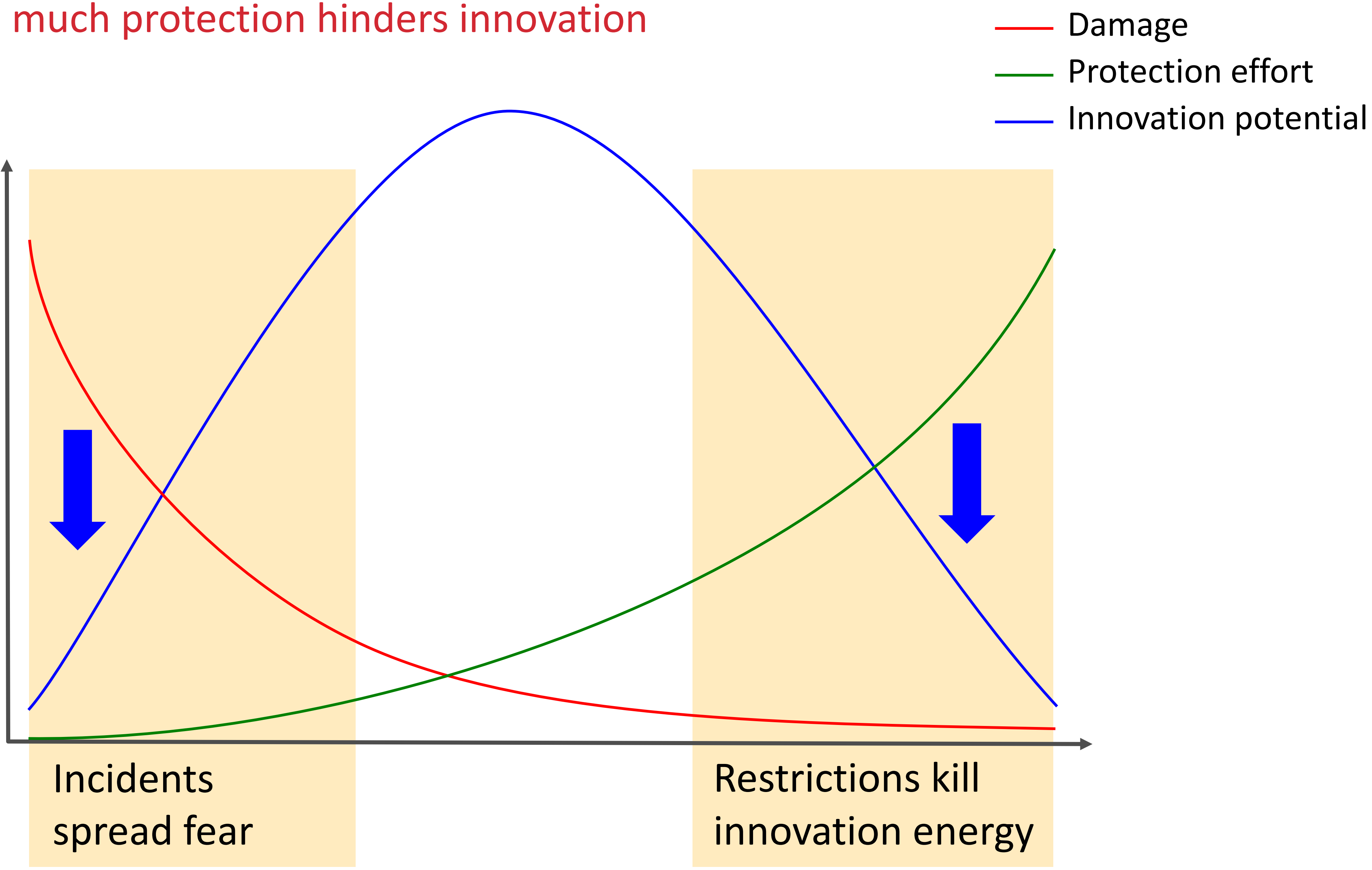
Car fatalities per 100 million miles [US]



- If we test all new car components for hacking risks, we delay their introduction
- A delay of 3 months due to security design and testing means more people get killed on the road
- 200.000 more people may die within the next 10 years

SOURCE: https://en.m.wikipedia.org/wiki/List_of_motor_vehicle_deaths_in_U.S._by_year

Too little and too much protection hinders innovation



Incidents spread fear

Restrictions kill innovation energy

Who will fully digitize faster?

Digital government ID ✓

Password-less authentication

Unified IP communication Jio

Contact-less payment

Take aways

- **Legacy is the biggest hurdle to digitization, and to security**

- **Even 100% greenfield deployments depend heavily on legacy IT**

- **Security often comes with externalities: More security is not always better**

Questions?

Karsten Nohl <nohl@srlabs.de>