

Using Security Metrics to improve Cyber-Resilience

Tobias Eggendorfer, Katja Andresen



Presenter

- Tobias Eggendorfer
- Professor for IT-Security
@ TH Ingolstadt
- Prior:
 - Professor for IT-Security
in Ravensburg
 - Professor for IT-Forensics
in Hamburg



Presenter

- Katja Andresen
- Professor for Business Information Systems and IT-Security
@Berlin School of Economics and Law
- Prior:
 - Head of Division „Secure Society“,
Agency for Innovations in
Cybersecurity.



Overview

- The need for measurable IT security
- Cyber Resilience
- How security metrics affect Cyber Resilience

IT-Security - Current state

- IT-Security assessment is mostly based on
 - vendor claims and
 - belief
 - sometimes even on magic

IT-Security - Current state

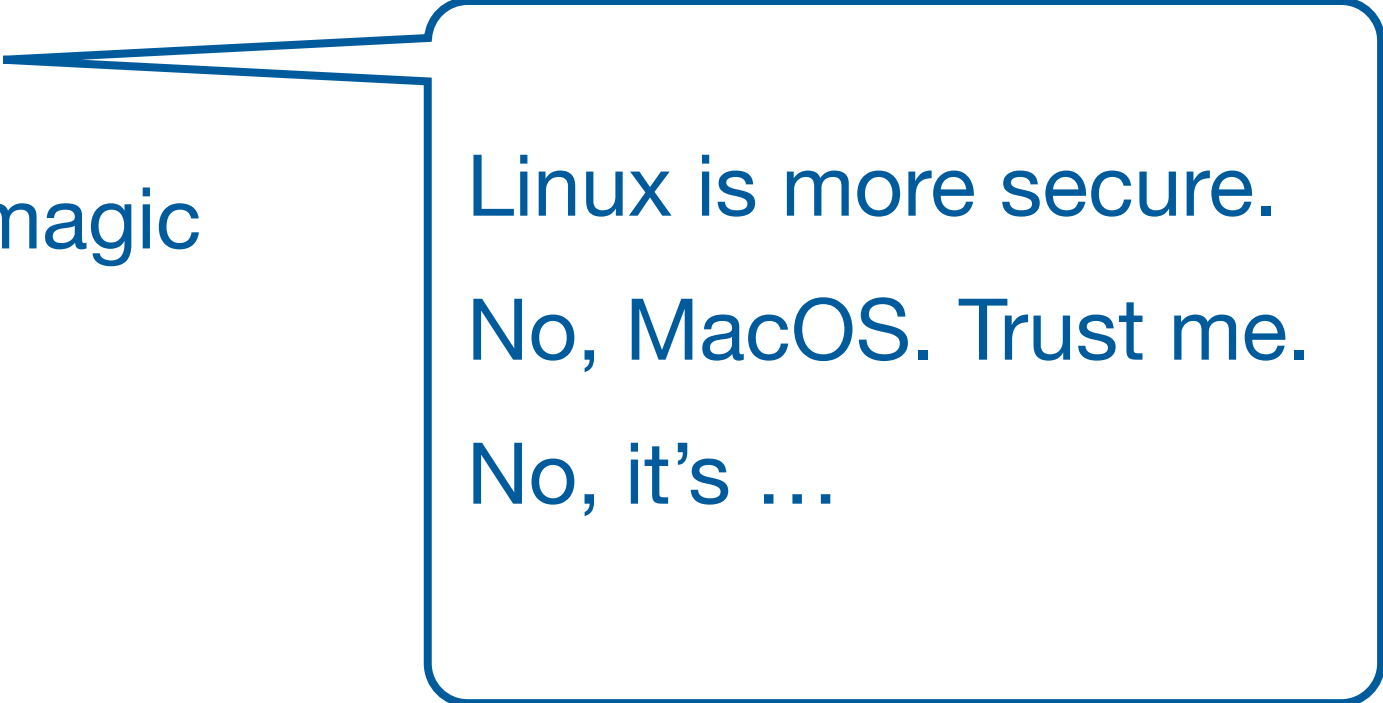
- IT-Security assessment is mostly based on
 - vendor claims and
 - belief
 - sometimes even on magic

Our software is secure.
See, our white-paper
says so too.

We are \$BIGCORP,
therefore it is secure.

IT-Security - Current state

- IT-Security assessment is mostly based on
 - vendor claims and
 - belief
 - sometimes even on magic



Linux is more secure.
No, MacOS. Trust me.
No, it's ...

IT-Security - Current state

- IT-Security assessment is mostly based on
 - vendor claims and
 - belief
 - sometimes even on magic

With this expensive IPS we cannot be hacked. Impossible.

IT-Security Standards

- Standards hardly ever define „security“, but manage processes around „security“

Security metrics

- With a measurable security value, security is comparable
- Much like EURO-NCAP or NutriScore



However: How to measure security?

- Need of a common understanding of security
- When, where and what to measure?
- How is a security score influenced?
- Is security comparable to quality?
- Could security scores be combined to a „system score“?

Understanding Security

- Is security the presence of encryption?
An assumption of some since GDPR etc.
- Is security the presence of a nice certificate?
How is this then achieved?
How do they know what to measure?
- Is security the absence of security flaws such as RCE?
How is absence proven?

Relation between Security and Quality

- Security \subseteq Quality
- Quality \subseteq Security
- Security = Quality



Relation between Security and Quality

- Security \subseteq Quality
- Quality \subseteq Security
- Security = Quality



Good quality:

Fulfills all requirements, i.e.,
has no bugs

Bugs cause security issues.
Ergo: No bugs, no issues.

Relation between Security and Quality

- Security \subseteq Quality
- Quality \subseteq Security
- Security = Quality



Security has additional requirements, such as confidentiality, integrity, authenticity, non-repudiation, availability, ...

Ergo: Security is more.

Relation between Security and Quality

- Security \subseteq Quality
- Quality \subseteq Security
- Security = Quality



At least, it is not the same.

Could quality metrics help?

- When it comes to code quality: Partly.
- But:
Are there (usable and useful) software quality metrics?

Not yet.

But: If there are no security metrics, we probably don't need them.

The need for security metrics

- Legal requirements
- Economical requirements
- Political needs
- Need for Cyber Resilience
- ...

Legal Requirements

- EU regulations such as NIS-2, Cyber Resilience Act, GDPR etc.
- Liability issues

Economical requirements

- Justify investments in specific products and technologies
- Need for business continuity and availability
- Dependence on IT and data
- Again: Liability and reputation

Political needs

- German government pays ~1 billion € per year to Microsoft
 - How could this be justified?
 - Is their technology of acceptable security?

US Government says no.

US Government says no

- Microsoft contradicts
- IT security specialists mostly claim: It's insecure
- Azure security specialists disagree.
- ...

With no objective metrics, this dispute cannot be resolved.

Need for Cyber Resilience

Cyber Resilience is the ability to react, respond, adapt or pro-actively anticipate incidents on cyber-connected infrastructures.

Anticipate incidents

- Without a metric for security, predicting security risks is like gambling.

Issue with Cyber Resilience

We have grown fairly accustomed to

- react
- respond and even
- adapt

to incidents.

But is this sufficient? Is it preventive enough?

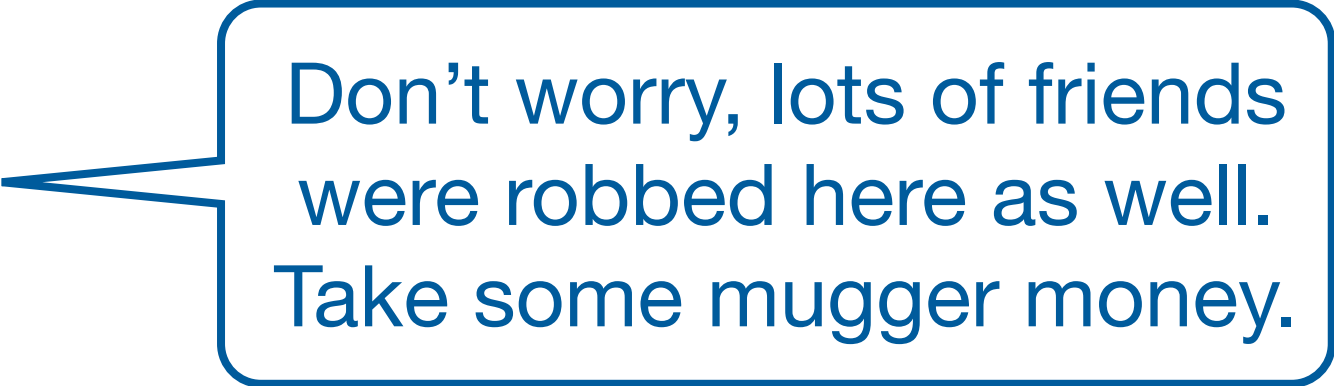
Issue with Cyber Resilience

We have grown fairly accustomed to

- react
- respond and even
- adapt

to incidents.

But is this sufficient? Is it preventive enough?



Don't worry, lots of friends were robbed here as well. Take some mugger money.

Issue with Cyber Resilience

We have grown fairly accustomed to

- react
- respond and even
- adapt

to incidents.

But is this sufficient? Is it preventing

Don't worry, lots of friends were robbed here as well. Take some mugger money.

Are backups an appropriate reaction to ransomware?

Cyber Resilience

- Is a challenge for a society and its political system.
- IT procurement decision affect cyber resilience.
- Procurement is affected by security expectations.
- Whether security expectations are met, cannot be measured yet.

Hence the need for security metrics.

Conclusion

Without the ability to measure IT security,
cyber resilience cannot be achieved.

Research in security metrics is urgently needed.

Remarks, comments, notes, ideas?

Tobias Eggendorfer

TH Ingolstadt

Faculty of Informatics

tobias.eggendorfer@thi.de

Katja Andresen

HWR Berlin

Faculty of Economics

katja.andresen@hwr-berlin.de