WWW.IARIA.ORG

# PANEL
# SECURE/DEPEND

# Security and Dependability in Mobile Environments

**MODERATOR:**
**Kiran Makhijani, Huawei Technologies | America Research Center, US**

# Security and Dependability

- **Breaches are easy and happen often**

  **Take over car controls over wireless/cellular medium.**

  **Install malicious app to misuse personal data on phone.**

  **Using your identity/device for malicious activities.**

- **Security**

  **No security is 100 percent," said David Blumberg, managing partner of venture firm Blumberg Capital in San Francisco, and an investor in security start-ups. "It's a degree of difficulty, time and expense."**

- **Dependability ➔ availability and usability**

**Our lifestyle dependence on**

- **Smart car control features that are convenient and improve our experience (self-parking, antilock breaking systems, GPS).**
- **Phones for online shopping, navigation, social media**

**Security is overlooked or not understood.**

# Vehicles | Security, Dependability | what can go wrong?

- **Breaches**

https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

**Using cellular connection and uconnect cars controls were overridden.**

- **Security threats are unconventional**
  - **Not same as virus or malware that you can see on your PC.**
  - **Remote control car operations with malicious intent**
- **Dependability**
  - **Implied that auto-mode is superior than manual mode.**
  - **But then A Parked car gets hit by fails → a prius**

# Social Behavior in Mobile Era

- Extent of sharing

  Many individuals do not understand the risk of information sharing

  By checking in – you tell hackers where you are not.

- Dependability

  Text conversations stored on phone – personal data breach with lost/stolen phones.

# Panelists

**Moderator**

Kiran Makhijani, Huawei Technologies, CA , USA

**Panelists**

- Hans-Joachim Hof, Munich University of Applied Sciences, Germany
  [Are companies putting enough effort into efficient protection of security and privacy, Do we need strict liability regulation for software quality?, Is bad usability killing IT security, especially on mobile devices?"]
- Ludek Lukas, Tomas Bata University in Zlín, Czech Republic
  [The mobile environment and theory of security. Theory of security and its application in mobile environment.]
- Rolf Johansson, SP, Sweden
  [Security risks will be less Safety critical for road vehicles when they become autonomous and leaving the drivers out of the loop". (It is harder to cheat an autonomous car, than the system composed by a car and a driver)."]
- Geir Køien, University of Agder, Norway

  [Trust at Large: Who, What, When where and Why]
- Elena Troubitsyna, Abo Akademi University, Finland

  []

# Open discussion – Summary

- Lack of comprehensive security mechanisms
  - Know the impact of their choices about a software
  - End users need to be made aware, educated and trained
  - Implications of unsafe/insecure software - Burden of responsibility
- Unchartered territory of security and safety in autonomous systems (AS)
  - Unconventional ways in which such ASes may be hacked
  - Override controls of the machines (self-driving cars)
  - Burden of Responsibility - Man or Machine debate – who's held accountable if AS made seemingly incorrect decision.
  - Need both scientific and legal communities to work together framing.
  - It is no longer acceptable to release beta software that influence critical
  - There's not enough data, information to formulate laws around AS failures.
- Theoretical Model to access risks wrt safety and security of systems
  - Need to develop mathematical assessment models against which safety and security of the system maybe tested.

# Panel SECUREWARE/DEPEND

## Security and Dependability in Mobile Environments

rolf.johansson@sp.se

# Who I am - Dr. Rolf Johansson

- Ph.D in Computer Engineering from Chalmers University
- Ms.C in Engineering Physics from Lund University
- Accredited Safety Assessor for ISO26262 (automotive domain)
- Researcher at Sweden’s largest research institute since 2010
- Previous more than 20 years of industrial experience
  - 10 years in aerospace
  - 10 years in automotive

A safety (not security) guy!

But a safety guy also needs to consider security

# My statement:

**“Security risks will be less safety critical for road vehicles when they become autonomous and leaving the drivers out of the loop”.**

**(It is harder to cheat an autonomous car to become unsafe, than the system composed by a car and a driver).**

**Autonomous cars will imply**

more complex application features than today

continuous deployment of new features

security critical!

**Still:**

**Safety predicates may be possible to define statically**

if the vehicle is in control of its own driving

**But:**

**Safety predicates more complicated to define statically**

considering driver misunderstanding of non-static features

SP

your Science Partner

RI.
SE
INSTITUTES

# Legacy protocols in XXI century mobile networks: how to ensure security?

Elena Troubitsyna

Åbo Akademi University,

Turku Finland

# Legacy protocols in mobile networks

- Telecommunication networks consist of heterogeneous components executing specific operations
  - Components can be composed to implement complex aggregated services.
- The SS7 protocol suite introduced for telephony standardises interfaces of the services and operations
  - interoperability of services from different providers.
- SS7-MAP defines an application layer on which to build a variety of services
  - support the GSM network including billing, roaming, text messaging, etc.
- The SS7 protocol suite: only the trusted parties (government and large companies) would be operating telecom networks.
  - The protocol suit does not have any in-built authentication and security protection.

# Attacks on mobile networks

- Now it is a different ball game:  it became easy to get access to the network services
  - attracted not only a variety of small service providers but also attackers.

- The number of security attacks on the telecommunication networks is constantly increasing.
  - Attempts of call and SMS interceptions, unauthorised call re-directions or alternations of billing information, etc.

- Attackers can masquerade themselves as trusted network components, use the services provided by the standard network protocols
  - exploit network vulnerabilities with malicious intent

# Open problems

How to

- ensure end-to-end security?
- trade-off security and openness?
- predict performance overhead?
- systematically and automatically explore existing vulnerabilities?
- automate discovery of new attack scenarios?

Tomas Bata University in Zlín
Faculty of Applied Informatics

# The Mobile Environment and Theory of Security

**Ludek Lukas**

Tomas Bata University in Zlín

Czech Republic

# Introduction

**Mobile environment**

mobile communication and information technologies for:

- management,
- command and control,
- messaging,
- information sharing etc.

technology aspects: secure information and communication processes.

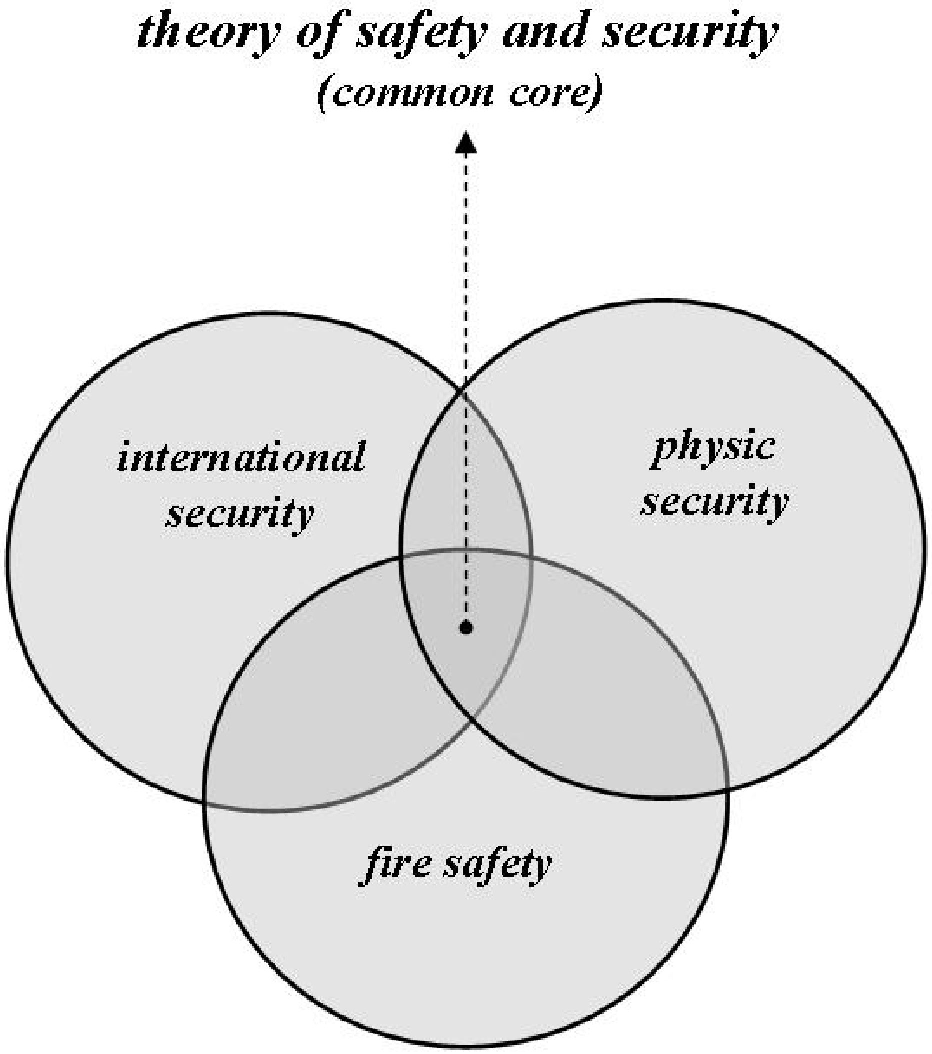
**Risk** = **Likelihood** x I**mpact (damage, harm..)**

what happens, if security fails ..

ALARA – 15 % of cost of damage

I think, we need theory of safety and security to understand why and how…

# Introduction



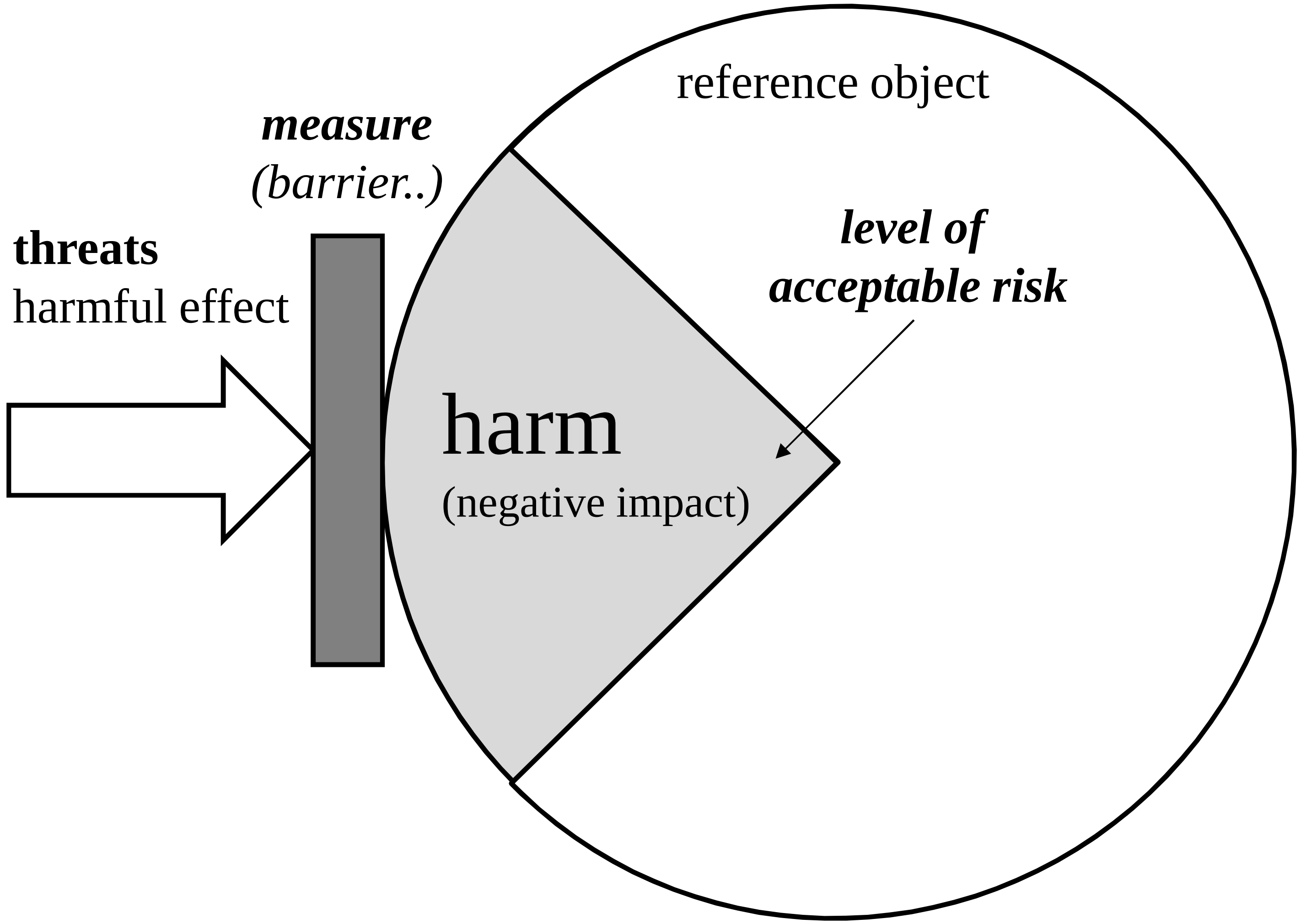
# Theory of Safety and Security

***Postulates of Theory of Safety and Security*:**

1. Safety / security does not exist itself, but it is always associated with the concrete reference object. The goal of safety or security is to prevent harms (negative impacts).
2. Safety / security is a status, where the risk arising from safety / security threats, is minimized to an acceptable level.
3. Acceptable level of risk is determined by the standard, decision or feeling.
4. Disruption of safety (safety **incident**) occurs due to ***negligence or accidentally***. Disruption of security (security **incident**) occurs ***intentionally.***
5. Safety / security is depended on external and internal factors.
6. Safety / security can be managed by the safety / security **measures.** Preventive measures reduce the frequency and repressive measures reduce the level of harm (negative impact).
7. Safety / security is ensured by the kinds of safety / security, which are discussed and accepted by the society.

# Theory of Safety and Security

***2. Safety / security is a status, where risk arising from safety / security threats, is minimized to an acceptable level.***

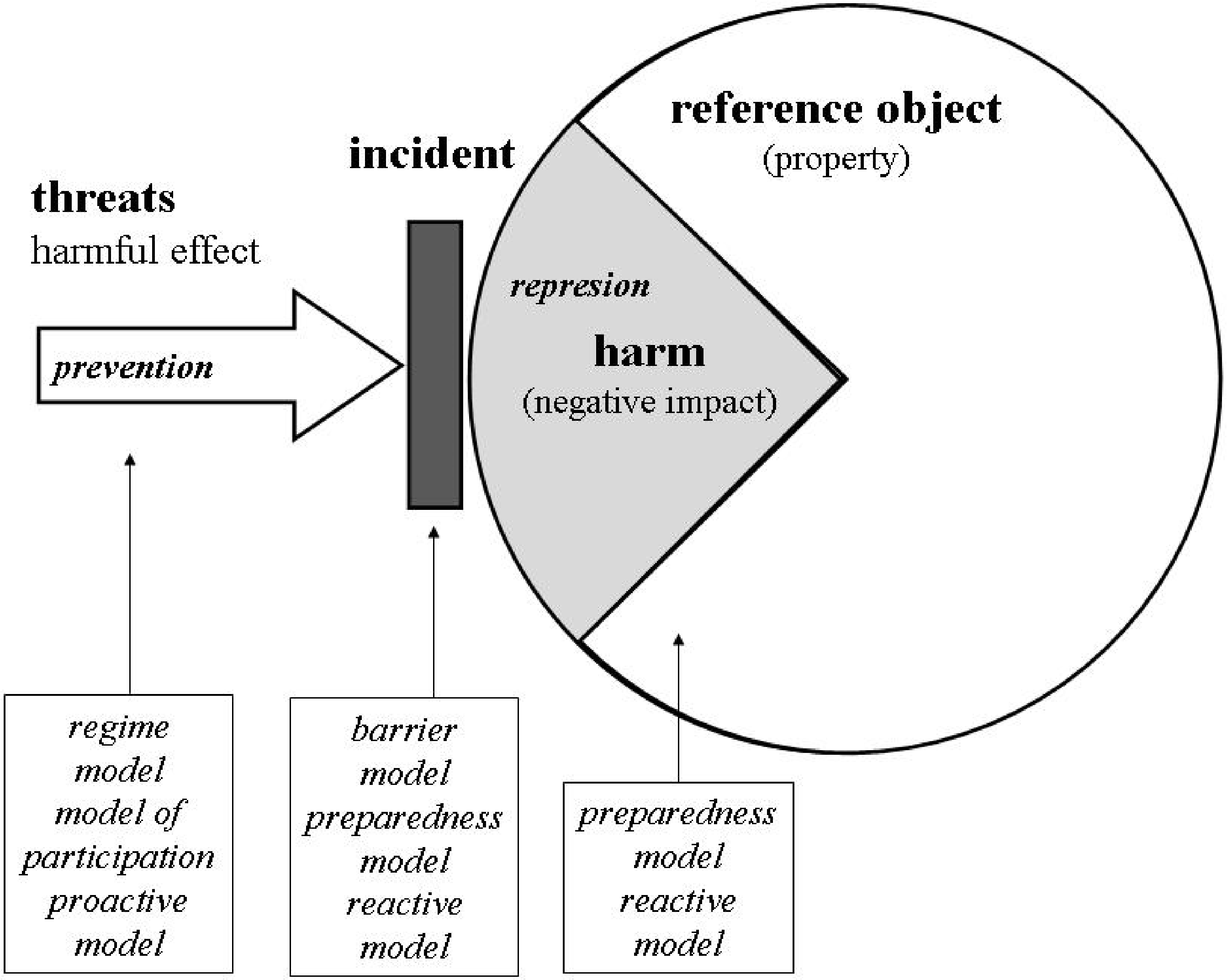


# Models of Safety and Security Ensuring

The safety and security models include (6th postulate):

- regime model,
- proactive model,
- barrier model,
- preparedness model,
- model of participation,
- reactive model.

# Models of Safety and Security Ensuring



**threats**
harmful effect

***prevention***

**incident**

**reference object**
(property)

***repression***

**harm**
(negative impact)

*regime model*
*model of participation*
*proactive model*

*barrier model*
*preparedness model*
*reactive model*

*preparedness model*
*reactive model*

# Conclusion

- mobile environment is service supporting persons, organizations and society,
- aim of security measures is to protect this environment,
- theory of safety and security allows to understand the safety and security problems in wider context,
- safety and security is here for people and society.

MuSe
Munich IT Security Research Group

# Panel „Security and Dependability in Mobile Environments“

Hans-Joachim Hof

hof@insi.science

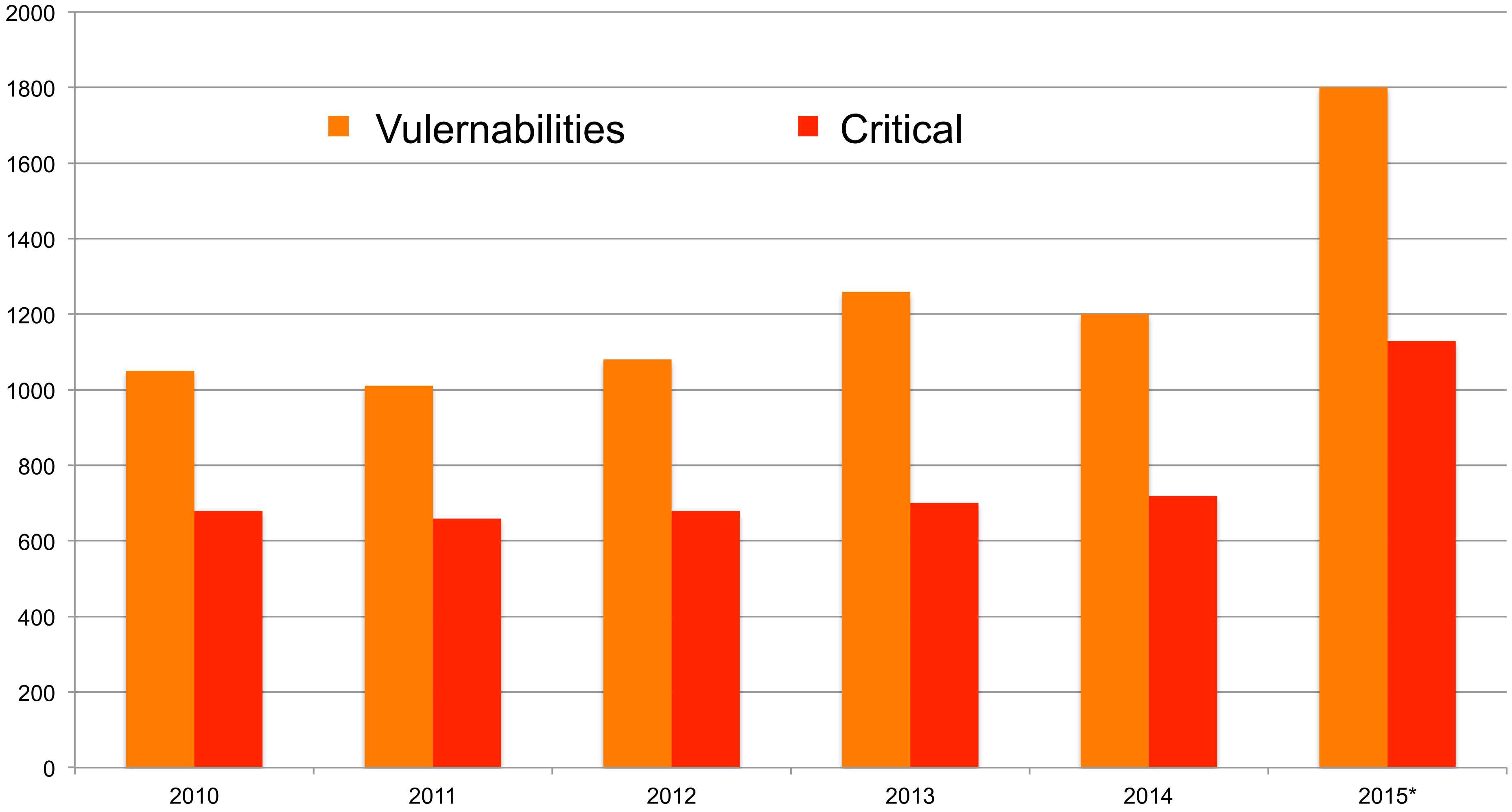
Munich IT Security Research Group

Munich University of Applied Sciences

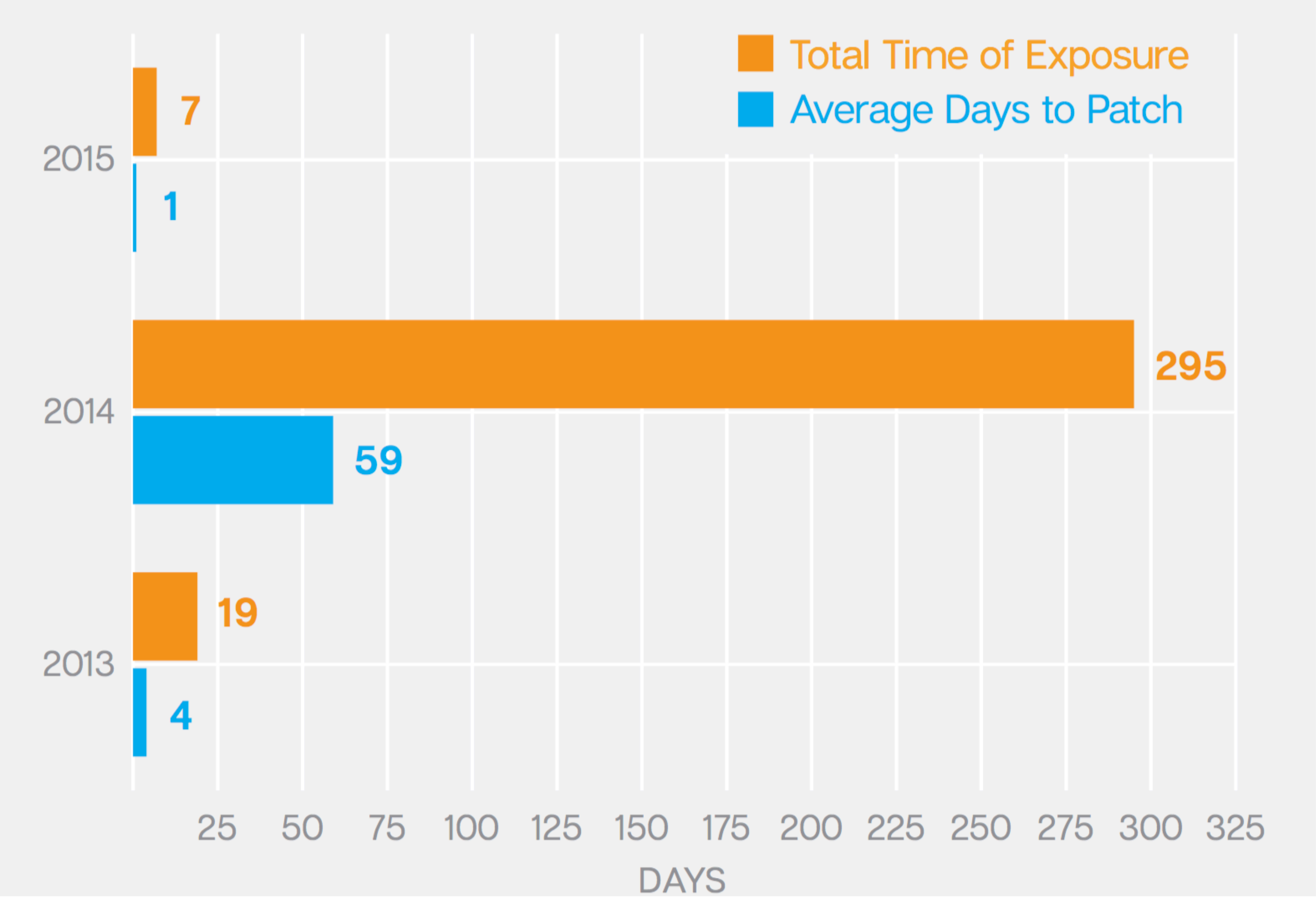
INSicherheit – Ingolstädter Forschungsgruppe angewandte
IT-Sicherheit, Technische Universität Ingolstadt

# Vulnerabilities

- Vulnerabilities for 13 popular standard software products  (BSI):



# Software Crisis: Handling of Vulnerabilities



Source: Symantec Internet Security Threats Report

# Software Crisis: Handling of Vulnerabilities

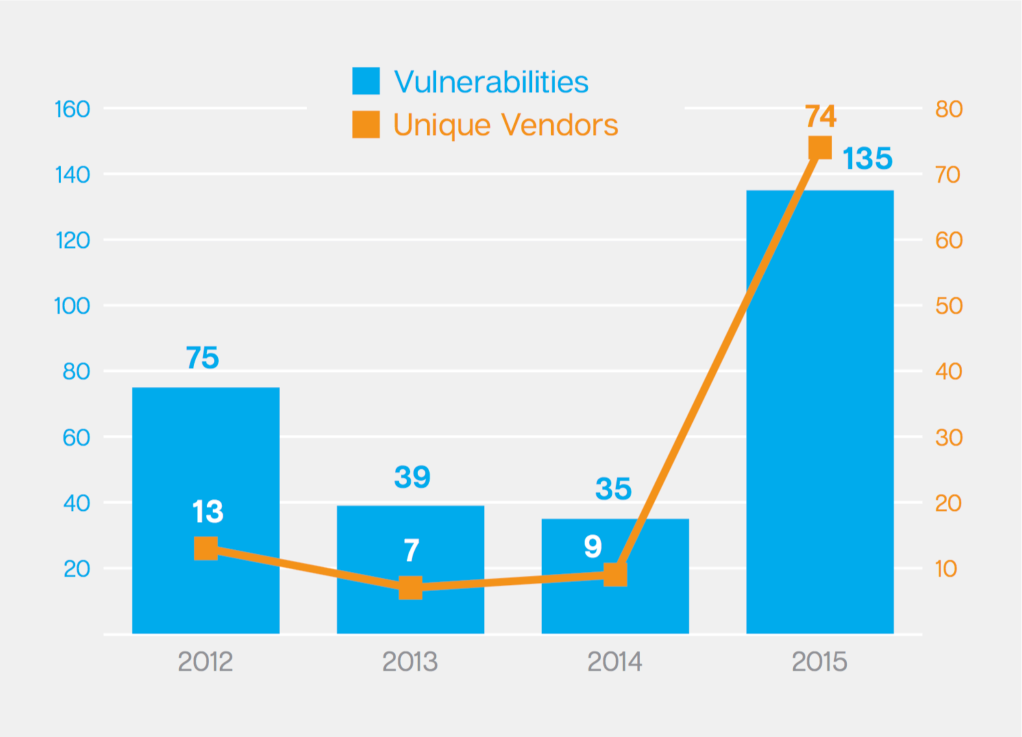
- Study of Heartbleed attack: Number of vulnerable hosts
  - Day 0 : 600.000
  - Day 0 + 30 : 300.000
  - Day 0 + 60 : 300.000 (!!!)
  - 43 % of admins tried to close vulnerability, only 14% succeeded

- Evaluation of web application vulnerabilities
  - 75% of websites had unpatched vulnerabilities
  - 15% of websites had critical unpatched vulnerabilities
  - Numbers do not change over years!!!

# Software Crisis: Can figures be transfered to new domains?

Munich IT Security Research Group

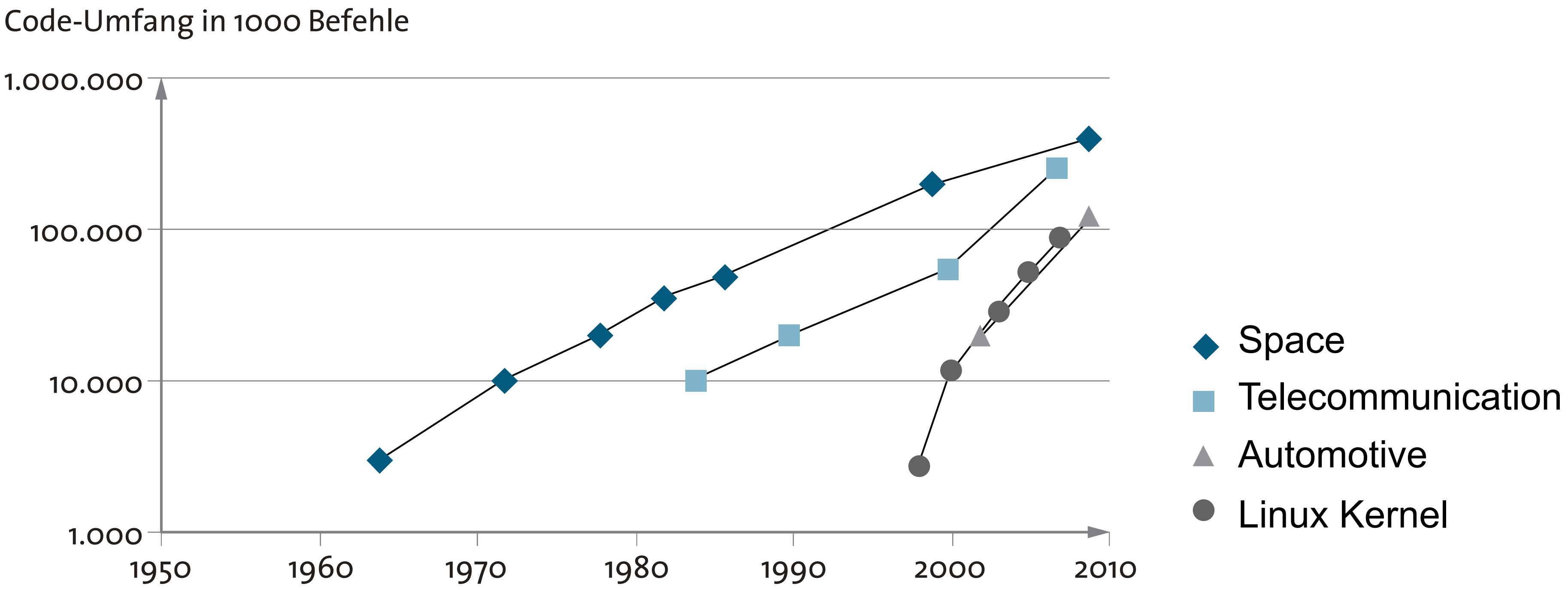
- McAffee: IoT devices often stay unpatched („installed and forgotten“)
- Vulnerablities of Industrial Control Systems (Symantec):



# Software Crisis: Can figures be transfered to new domains?

Munich IT Security Research Group

- Many domains with complexity higher than standard IT



Quelle: Bitkom „Eingebettete Systeme – ein strategisches Wachstumsfeld für Deutschland“

- There is hope: Other domains (e.g., automotive) achieve high quality of non-functional requirements (e.g., safety)

# Questions for Discussion

- Are companies putting enough effort into efficient protection of security and privacy?
- Do we need strict liability regulation for software quality?
- Is bad usability killing IT security, especially on mobile devices?

Security and Dependability in Mobile Environments

# Trust at Large

## *Why, Who, What, When and Where*

SecurWare 2016

Geir M. Køien
University of Agder, Institute of ICT,
Grimstad, Norway

# Trust - Problem in Context

## Context:

- **Mobile Environments**
  - «distance» between principal parties
    - Can’t really know who you are dealing with
    - Need to ascertain **I**dentity, **I**ntention and **A**bility

## Problem:

- **Security**
  - Assurance of conformance with expectations
  - What we want: «Protect my assets and me»
- **Dependability**
  - ASSUMPTION: I need the service!
    - Provide the service!
    - …and protect me / make me feel safe

# Why?

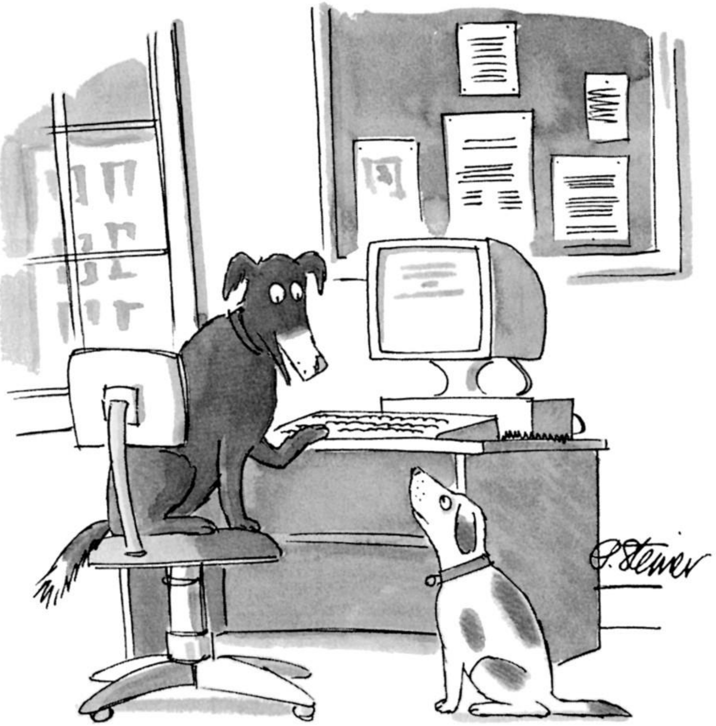
- **Why trust anybody?**
  - Don’t in general know who you're dealing with
  - Assurance is hard to get
  - Doesn’t have to be person either
- **Why trust at all?**
  - There are benefits too
- **Perceived or real:**
  - We need to be convinced that the risk is low enough
  - …and that the benefits are well worth the risk

# Who or What?

- **Who (or What)**
  - Who do you trust?
  - What do you trust?

## Brands?

SONY
adidas
PANTENE PRO-V
durex
HYUNDAI
SAMSUNG
LEGO
Kodak
TOYOTA
Reebok
Nintendo
Lufthansa
NIVEA



"On the Internet, nobody knows you're a dog."

Peter Steiner's cartoon (*The New Yorker),*

http://www.plsteiner.com/

# When and Where?

- **Spatio-Temporal Conditional Trust**
  - Prudent to ask **When**
  - Prudent to ask **Where**

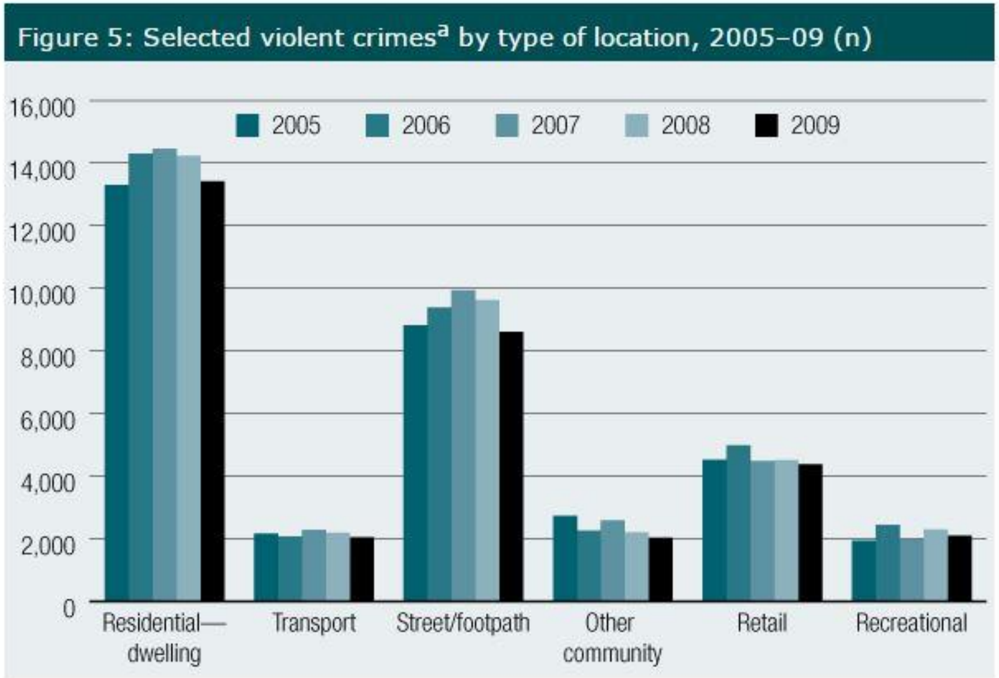
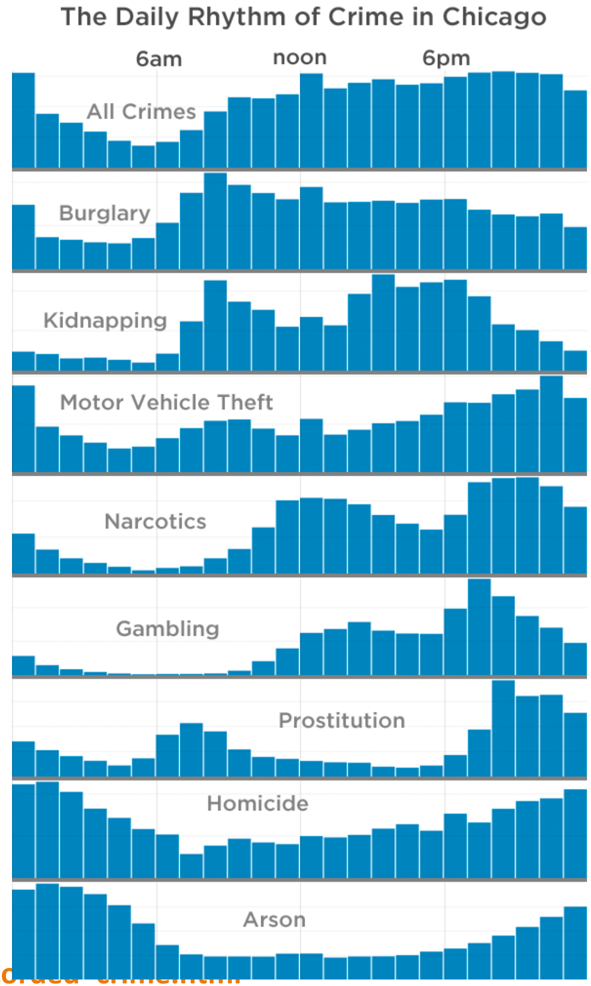


Figure 5: Selected violent crimes[a] by type of location, 2005–09 (n)



The Daily Rhythm of Crime in Chicago

http://www.aic.gov.au/publications/current%20series/facts/1-20/2010/1_recorded_crime.html

https://www.socrata.com/blog/crime-time-visualizing-crime-data-chicago/

# Assurance

- **Need to add benefits and remove obstacles**
  - Assured (authenticated) identities
  - Reputation and honesty (good intentions)
  - Trustworthiness (ability to behave in accordance with intentions)
- **Must have designs that facilitates assurance**
  - Too much quick’n’dirty today
- **Privacy must be part of it**
  - The users need some level of control over private data
    - Need transparency and manageability
  - Credible confidentiality protection is part of this
  - Balanced between “fair use” and “personal control”