On the Importance of Human Timing for Quantitative Cyber Risks Management

Swiss Cyber Storm 4, Luzern

June 13, 2013

Thomas Maillart

Swiss National Science Foundation Fellow

School of Information

UC Berkeley, California, USA

Human Timing

Software Updates & Human Timing

Duration before users perform software updates

- Pareto distribution : “80/20 rule”

Explanation

- prioritization of daily life tasks
- optimization of time consumption as a non storable resource

Main Result

⇒ **incentives drive human timing**

joint work with

Human Timing & Cyber Risks

- software deployment and updates by users
- lack of time for proper security monitoring
- delays in patch development and release by software editors
- learning curve & expertise acquisition

⇒ time has become the main scarce resource...

... and cyber criminals exploit it !

⇒ but since we understand human timing we can make predictions.

Information Security vs. Forecasts

Two approaches to cope with cyber risks :

(a) keep a sufficient technological advance

(b) predict the next move by cyber criminals

experience shows that (a)

cannot be systematically achieved

:-(

Information Security vs. Forecasts

Two approaches to cope with cyber risks :

(a) keep a sufficient technological advance

(b) predict the next move by cyber criminals

but if we can perform (b) accurately,

(a) gets simpler

:-)

Information Security vs. Forecasts

Two approaches to cope with cyber risks :

(a) keep a sufficient technological advance

(b) predict the next move by cyber criminals

unfortunately,

(b) is stochastic

:-(

Information Security vs. Forecasts

Two approaches to cope with cyber risks :

(a) keep a sufficient technological advance

(b) predict the next move by cyber criminals

unfortunately,

there are plenty of scenarios to test

:-(

Information Security vs. Forecasts

Two approaches to cope with cyber risks :

(a) keep a sufficient technological advance

(b) predict the next move by cyber criminals

but with good quantitative risk models,

we can handle stochasticity,

scale up,

and make good forecasts

:-)

Applications

1. Cyber Risks “Weather” Forecasting

a. Analyze vulnerability dynamics per software and/or vendor

b. Calibrate the “human timing” model with records of Internet attacks

c. Make a prediction

d. Measure error and recalibrate [go to (b)]

e. Deliver a quantitative measure of cyber risks per software and/or vendor

Fields of application

- general awareness
- policy making
- cyber (re)insurance

Main features

- predict intensity of attacks at the Internet scale
- deliver a quantitative cyber risk measure,
given a portfolio of software (e.g. used by a company)

2. Network Closed Circuit TV (netCCTV)

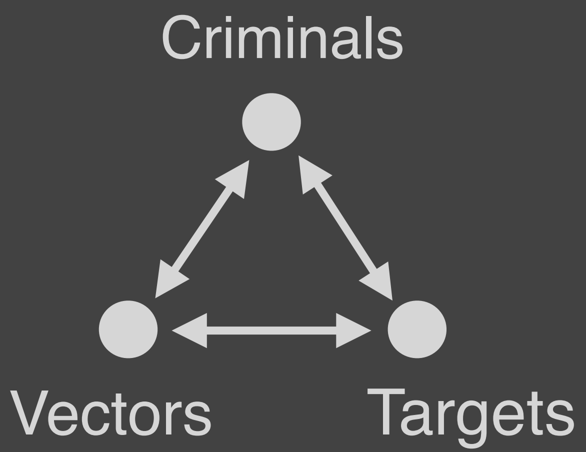
Field of application

- information systems
- user / binary / network connections behavioral analysis
- massive log data analytics

Main features

- predict the activation of binaries by users
- forecast future states of the information system (at various coarse-grained levels)
- anomaly detection
- quantitative risk metrics at the information system level

3. Prediction of Cyber Criminal Next Move(s)



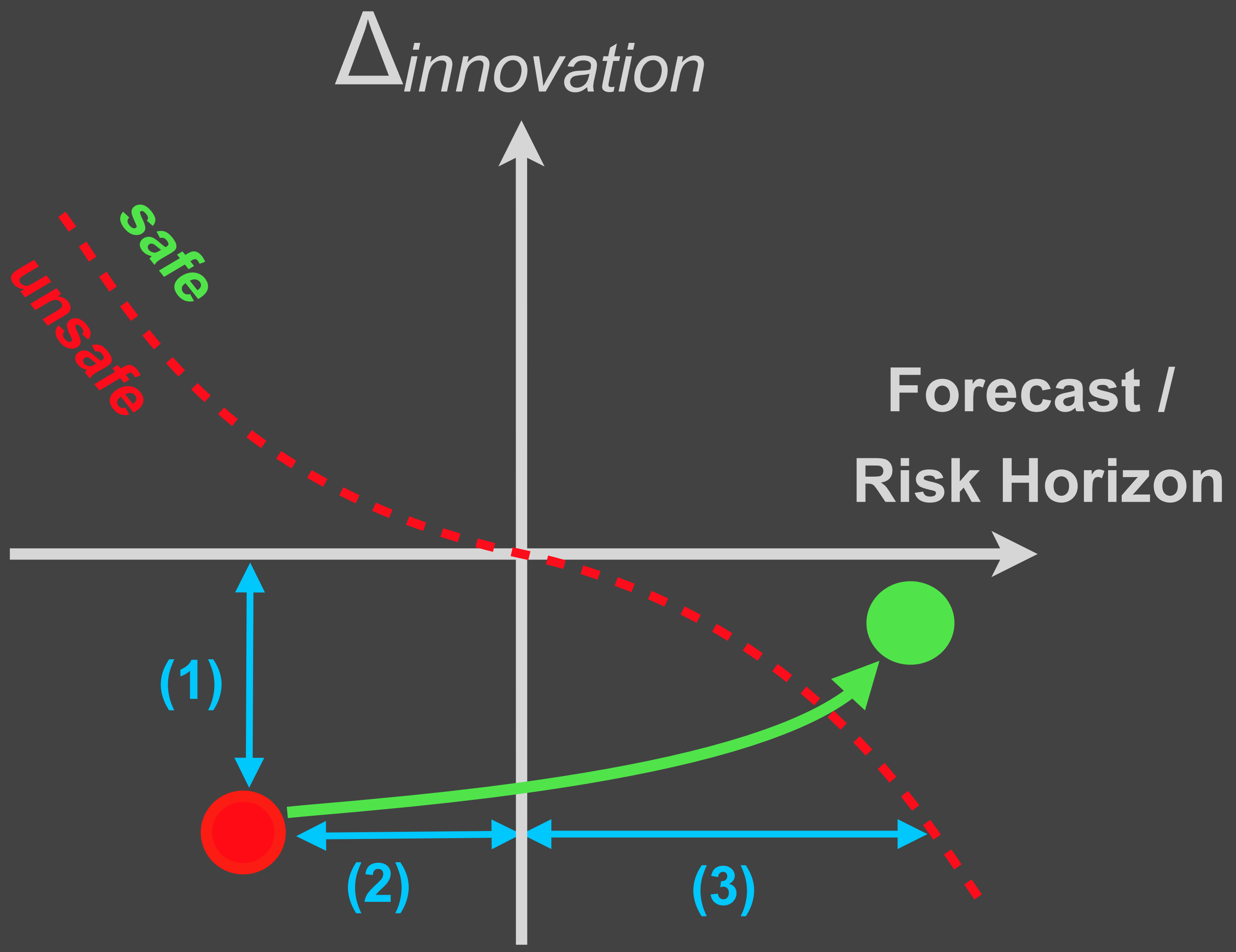
Field of application

- cyber defense at regional levels
- expertise and incentive based behavioral analysis

Main features

- identification of fields of expertise based on cyber criminal activity
- matching with opportunities offered by vulnerabilities
- measure of potential learning opportunities
- (statistical) prediction of possible next moves
- aggregate quantitative measure of risks based on incentives and expertise

Cyber Risks Phase Diagram



(1) innovation gap
(2) monitoring gap
(3) forecasting gap

● where we are currently

● a point we have
a chance to reach

→ improvement trajectory

- - - - - (theoretical) safety line

Thank You !