

# Assessing ICT Security Risks in Socio-Technical Systems

Edited by

Tyler W. Moore<sup>1</sup>, Christian W. Probst<sup>2</sup>, Kai Rannenberg<sup>3</sup>, and Michel van Eeten<sup>4</sup>

**1** University of Tulsa, US, [tyler-moore@utulsa.edu](mailto:tyler-moore@utulsa.edu)

**2** Technical University of Denmark – Lyngby, DK, [cwpr@dtu.dk](mailto:cwpr@dtu.dk)

**3** Goethe-Universität Frankfurt am Main, DE, [kai.rannenberg@m-chair.de](mailto:kai.rannenberg@m-chair.de)

**4** TU Delft, NL, [m.j.g.vaneeten@tudelft.nl](mailto:m.j.g.vaneeten@tudelft.nl)

---

## Abstract

This report documents the program and the outcomes of Dagstuhl Seminar 16461 “Assessing ICT Security Risks in Socio-Technical Systems”. As we progress from classic mechanical or electrical production systems, over ICT systems, to socio-technical systems, risk assessment becomes increasingly complex and difficult. Risk assessment for traditional engineering systems assumes the systems to be deterministic. In non-deterministic systems, standard procedure is to fix those factors that are not deterministic. These techniques do not scale to ICT systems where many risks are hard to trace due to the immaterial nature of information. Beyond ICT systems, socio-technical systems also contain human actors as integral parts of the system. In such socio-technical systems there may occur unforeseen interactions between the system, the environment, and the human actors, especially insiders. Assessing ICT security risks for socio-technical systems and their economic environment requires methods and tools that integrate relevant socio-technical security metrics. In this seminar we investigated systematic methods and tools to estimate those ICT security risks in socio-technical systems and their economic environment. In particular, we searched for novel security risk assessment methods that integrate different types of socio-technical security metrics.

**Seminar** November 13–18, 2016 – <http://www.dagstuhl.de/16461>

**1998 ACM Subject Classification** J.4 Social and Behavioral Sciences, K.6.5 Security and Protection

**Keywords and phrases** economics of risk assessment, human factor, return on security investment, security risk management, socio-technical security

**Digital Object Identifier** 10.4230/DagRep.6.11.63

**Edited in cooperation with** Christian Sillaber

## 1 Summary

*Tyler W. Moore*

*Christian W. Probst*

*Kai Rannenberg*

*Michel van Eeten*

**License** © Creative Commons BY 3.0 Unported license

© Tyler W. Moore, Christian W. Probst, Kai Rannenberg, and Michel van Eeten

The Dagstuhl Seminar 16461 “Assessing ICT Security Risks in Socio-Technical Systems” is part of a series of seminars that explore aspects of risk and security in socio-technical systems. After initial work on insider threats, the focus has turned towards understanding of relevant metrics and their application in novel security risk assessment methods.



Except where otherwise noted, content of this report is licensed under a Creative Commons BY 3.0 Unported license

Assessing ICT Security Risks in Socio-Technical Systems, *Dagstuhl Reports*, Vol. 6, Issue 11, pp. 63–89

Editors: Tyler W. Moore, Christian W. Probst, Kai Rannenberg, and Michel van Eeten



DAGSTUHL  
REPORTS

Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

## Classical Risk Assessment

Assessing risk in classic mechanical or electrical production systems is difficult but possible, as experience shows. Historical knowledge provides us with approximation of likelihood of failures of machines and components. We can combine these likelihoods in modular ways, mapping the impact of the loss of a system component to the processes that component contributes to.

This approach works for traditional engineering systems, since the dependencies between components are expected to be known, and their behaviour is assumed to be deterministic. To reach a comparable level of predictability for risk assessment in areas that are less governed by machines, for example economics, standard procedure is to fix those factors that are not deterministic. The behaviour of buyers and sellers on a market, for example, is assumed to be gain-oriented and rational; dealing with irrational actors is less explored and hard to model.

## Risk in ICT Systems and the Immaterial Nature of Information

The techniques that work well for assessing risk in classic mechanical or electrical production systems do not scale to ICT systems. A primary reason is that there is no clear connection between the usage of a system and the risk of failure. Many risks that we need to consider in ICT are hard to trace due to the immaterial nature of information [2]. Examples of such risks are unauthorized or illegitimate information flows. Information flows are more difficult to trace than material flows, as the flow is usually caused by a copying operation; the information is not missing at the source, which in the material world is an indicator of an illegitimate flow, *e.g.*, when goods are stolen. Moreover, the damage is barely related to the measurable amount of information [5, 9]. Several megabytes of, *e.g.*, white noise can be relatively harmless, while a single health data record or financial record of limited size can be a major problem, *e.g.*, in terms of loss of trust, reputation, or damage compensation payments.

Another reason why classic approaches have struggled to assess risk is that the threat from strategic adversaries is harder to model than random failures. Whereas events triggered by nature occur randomly, attackers can readily identify and target the weakest links present in systems, and adapt to evade defenses.

A final reason why assessing security risks is hard is that there is often an incentive to hide failures from public view, due to fears of reputational damage. This makes collecting data to empirically estimate loss probabilities very difficult.

## Risk in Socio-technical Systems

Beyond ICT systems, socio-technical systems also contain human actors as integral parts of the system. In such socio-technical systems there may occur unforeseen interactions between the system, the environment, and the human actors, especially insiders [8].

Assessing the risk of the ICT system for human actors is difficult [4]; the assessment must take into account the effect of the ICT system on the environment, and it must quantify the likelihood for this risk to materialize. Assessing the risk of the human actor for the ICT system is difficult, too. As mentioned above, economics models human actors by assuming them to be gain-oriented and rational; dealing with irrational actors is less explored and hard to model. However, one of the biggest risks from human actors for an ICT system is irrational behaviour, or an unknown gain function.

### **Economics of Risk Assessment**

The economic aspect both of the risk identified and the process of assessing risk often prohibits either risk mitigation or the assessment itself. Protection against irrational threats requires appropriate preventive measure, be it too restrictive policies or too intense surveillance. Neither the cost nor the effects of these measures are easily predictable [1].

Even worse, the cost for risk assessment itself can also be prohibitive. For example, trying to identify the actual risk for irrational behaviour or its impact on the system can be impossible or at least imply a too high price [4].

### **Security Metrics**

As we concluded after the previous Dagstuhl Seminar 14491, well-defined data sources and clear instructions for use of the metrics are key assets “to understand security in today’s complex socio-technical systems, and to provide decision support to those who can influence security”.

Security metrics obviously cannot be applied on their own, but must be embedded in a well-defined framework of sources for metrics and computations on them [7]. Important topics include understanding the aspects surrounding metrics, such as sources, computations on metrics, relations to economics, and the analyses based on metrics.

### **Assessing ICT Security Risks in Socio-Technical Systems**

Making risk in socio-technical systems assessable requires an understanding of how to address issues in these systems in a systematic way [3, 6]. In this seminar, we built upon the work in the predecessor seminars on insider threats and security metrics, and explores the embedding of human behaviour and security metrics into methods to support risk assessment.

### **Main findings**

We established five working groups in the seminar, that discussed several times during the week and reported back in plenum. The results are presented in Section 4, and briefly summarized here.

#### **Which data do we need to collect?**

In a working group on “Collecting Data for the Security Investment Model”, we considered the relationship between efforts to secure an organisation, the actual security level achieved through these efforts, and their effect on moderating attacks and the induced losses. We identified relevant, measurable indicators for the components in the model that relate metrics about components to the expected risk. Model outcomes could be used to guide security investments.

#### **Which security risks should we consider?**

To identify relevant risk assessment methods, we discussed the kind of risk relevant to measure in two working groups. On the one hand we explored “New Frontiers of Socio-Technical Security”, where we considered disrupting new technologies and how they influence and change our perception of risk, or its limitations. The main example were orphaned devices in IoT systems, which often cannot be switched off, but pose a threat to the overall system

if they remain unmaintained. A similar problem space was explored in the working group on “Software Liability Regimes”, which considered liability or lack thereof of producers to identify and fix problems.

### **Which attacker and user traits do we need to consider?**

To understand relevant aspects of human actors involved in socio-technical systems, we established two more working groups. The group on “Unpacking the motivations of attackers” discussed how to understand attacker motivations in highly integrated socio-technical systems, where purpose and means play a fundamental role in the way and at which level(s) the cyberspace can be disrupted.

## **Conclusions**

Assessing risk in socio-technical systems is and remains difficult, but can be supported by techniques and understanding of limitations and properties inherent to the system and the risk assessment methods applied. This seminar has explored how to identify these limitations and properties by exploring the different layers of socio-technical systems, their interactions, and their defining attributes.

A total of 36 researchers participated in the seminar across from different communities, which together span the range relevant to developing novel security risk assessment methods and to ensure the continuation from the previous seminars’ results: cyber security, information security, data-driven security, security architecture, security economics, human factors, (security) risk management, crime science, formal methods, and social science.

## **References**

- 1 Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M. J. G., Levi, M., Moore, T., and Savage, S. (2012). Measuring the Cost of Cybercrime. Paper presented at the Workshop of Economics and Information Security (WEIS 2012), Berlin.
- 2 Blakley, B., McDermott, E., Morgan, J. P., and Geer, D. (2001). Information security is information risk management. In: NSPW’01 Proceedings of the 2001 workshop on New security paradigms (pp. 97–104). New York, NY: ACM.
- 3 Gollmann, D. (2012). From Insider Threats to Business Processes that are Secure-by-Design. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, 3 (1/2), 4–12.
- 4 Hunker, J. and Probst, C. W. (2009). The Risk of Risk Analysis, And its relation to the Economics of Insider Threats. In: WEIS’09 Proceedings of the 2009 workshop on Economics of Information Security.
- 5 Johnson, M. E, Goetz, E., and Pfleeger, S. L. (2009). Security through Information Risk Management, *IEEE Security and Privacy*, 7(3):45–52.
- 6 Littlewood, B., Brocklehurst, S., Fenton, N., Mellor, P., Page, S., Wright, D., Dobson, J., McDermid, J., and Gollmann, D. (1993). Towards Operational Measures of Computer Security. *Journal of Computer Security*, 2(2–3):211–229.
- 7 Pieters, W., Van der Ven, S. H. G., and Probst, C. W. (2012). A move in the security measurement stalemate: Elo-style ratings to quantify vulnerability. In Proceedings of the 2012 New Security Paradigms Workshop (NSPW’12) (pp. 1–14). New York, NY: ACM. doi: 10.1145/2413296.2413298.
- 8 Probst, C. W., Hunker, J., Bishop, M. and Gollmann, D. (2009). Countering Insider Threats. *ENISA Quarterly Review*, 5(2).

- 9 Tschersich, M., Kahl, C., Heim, S., Crane, S., Böttcher, K., Krontiris, I., Rannenberg, K. (2011). Towards Privacy-enhanced Mobile Communities – Architecture, Concepts and User Trials. In: Journal of Systems and Software, Volume 84, Issue 11, pp. 1947–1960, November 2011,

## 2 Table of Contents

### Summary

*Tyler W. Moore, Christian W. Probst, Kai Rannenberg, and Michel van Eeten . . .* 63

### Overview of Talks


Complex socio-technical systems	
<i>Ross Anderson . . . . .</i>	70
Dealing with High-Consequence Low-Probability Events	
<i>Johannes M. Bauer . . . . .</i>	70
Usable Recovery	
<i>Zinaida Benenson . . . . .</i>	70
A security measurement model	
<i>Rainer Böhme . . . . .</i>	71
Human-Centered Security Requires Risk Communication	
<i>L. Jean Camp . . . . .</i>	71
Systems Modelling and Behavioural Economics	
<i>Tristan Caulfield . . . . .</i>	72
The Security Behavior Observatory	
<i>Nicolas Christin . . . . .</i>	72
Improving Risk Decisions on Mobile Devices	
<i>Serge Egelman . . . . .</i>	72
Value-sensitive design of Internet-based services (the commensurability challenge)	
<i>Hannes Hartenstein . . . . .</i>	73
Modeling and Analysis of Security for Human Centric Systems	
<i>Florian Kammüller . . . . .</i>	73
Socio-Technical Q&A	
<i>Stewart Kowalski . . . . .</i>	74
Attack Surface of Socio-Technical Systems	
<i>Kwok-Yan Lam . . . . .</i>	74
Cyber Risk Information Sharing	
<i>Stefan Laube . . . . .</i>	76
Heavy-tailed cyber security incidents: Which organization design to manage extreme events?	
<i>Thomas Maillart . . . . .</i>	76
How do you know that it works? The curses of empirical security analysis	
<i>Fabio Massacci . . . . .</i>	77
Enhancing Researches in the ICT Security Field	
<i>Kanta Matsuura . . . . .</i>	78
Security Challenges in Small Organisations	
<i>Simon Parkin . . . . .</i>	79
Agent-based modelling for cybersecurity	
<i>Wolter Pieters . . . . .</i>	79

Metrics for security-related behaviours and organisational economics and performance	
<i>Martina Angela Sasse</i> . . . . .	80
Socio-Technical-Artifact Driven Security and Risk Analysis	
<i>Christian Sillaber</i> . . . . .	81
Assessing ICT security risks in socio-technical systems: Policy implications	
<i>Edgar A. Whitley</i> . . . . .	82
Human Factors in Information Security	
<i>Sven Übelacker</i> . . . . .	82
<b>Working groups</b>	
Collecting Data for the Security Investment Model	
<i>Tristan Caulfield, Rainer Böhme, Kanta Matsuura, Tyler W. Moore, Martina Angela Sasse, Michel van Eeten, and Maarten van Wieren</i> . . . . .	83
New frontiers of socio-technical security	
<i>Carlos H. Ganan, Zinaida Benenson, Hannes Hartenstein, Stewart Kowalski, Kwok-Yan Lam, Christian W. Probst, Edgar A. Whitley, and Jeff Yan</i> . . . . .	84
Unpacking the motivations of attackers	
<i>Thomas Maillart, Ross Anderson, Johannes M. Bauer, Barbara Kordy, Gabriele Lenzini, and Sebastian Pape</i> . . . . .	85
Software Liability Regimes	
<i>Christian Sillaber, Nicolas Christin, Richard Clayton, Stefan Laube, Fabio Massacci, Tyler W. Moore, Kai Rannenberg, and Michel van Eeten</i> . . . . .	86
User-centred Security Models	
<i>Sven Übelacker, Vincent Koenig, and Simon Parkin</i> . . . . .	87
<b>Participants</b> . . . . .	89

### 3 Overview of Talks

#### 3.1 Complex socio-technical systems

*Ross Anderson (University of Cambridge, GB)*

License  Creative Commons BY 3.0 Unported license  
© Ross Anderson

When analysing the risks of complex socio-technical systems we have a lot of historical examples to use as a guide, from the Roman army through the Chinese civil service to the banking system as it emerged in the 19th century. What changes when you add software is that action is no longer local and personal; so the traditional ways of scaling action (ideologies, hierarchies, markets) are no longer all there is. Another factor that changes is the time constant. An important and neglected aspect is safety regulation. Traditionally, safety-critical equipment from cars through medical devices to electrotechnical equipment has been regulated by pre-market inspection, which has a time constant roughly equal to the product lifecycle, typically ten years. Once everything is online and hackable, your car will need monthly software updates just like your laptop and your phone. The current institutional arrangements are unable to cope, and major change is necessary. Richard Clayton, Eireann Leverett and I have done a big project on this for the European Commission; an academic paper should be out next year. The political vision is that just as Europe has become the world's privacy regulator (as Washington doesn't care and nobody else is big enough to matter), so also Europe should aim to be the world's safety regulator too.

#### 3.2 Dealing with High-Consequence Low-Probability Events

*Johannes M. Bauer (Michigan State University – East Lansing, US)*

License  Creative Commons BY 3.0 Unported license  
© Johannes M. Bauer

With increased connectivity and the multiplication of devices the ICT system increasingly resembles a complex adaptive system. In such systems, small changes may have large repercussions for overall system performance. Security incidents that have a low probability but potentially catastrophic consequences cannot easily be captured by statistical analyses and traditional forms of cost-benefit analysis. The alternative of preventing such events has potentially serious downsides, such as reducing the rate of innovation and possibly prohibitive costs. An alternative is to aim at designing resilient organizations, communities, nations, and global systems.

#### 3.3 Usable Recovery

*Zinaida Benenson (Universität Erlangen-Nürnberg, DE)*

License  Creative Commons BY 3.0 Unported license  
© Zinaida Benenson

Joint work of Zinaida Benenson, Daniela Oliveira

We propose usable recovery as a new paradigm to solve the “user involvement” dilemma in security. The security community expects that users should perform perimeter security tasks that will protect their devices from compromise. These tasks include installing antivirus,



choosing and managing strong passwords, making informed decisions when encountering security warnings, paying attention to deception cues in emails and on websites, updating all installed software, etc. The dilemma is that the effort required for those tasks does not match the security benefit that users would get by performing them: The cumulative effort required from non-expert users has become overwhelming and they may still not be able to protect their devices and data because of lack of time or skills, and the never-ending evolvement of the attack landscape. Our paradigm argues that because of this mismatch, home computer users should not be expected to perform these security tasks and, instead, be equipped with usable, nearly transparent (minimum and reasonable effort) recovery mechanisms. Thus, when a security incident is detected, the users can bring their machine to a functional state with most of their functionality, settings and data preserved. We systematically discuss the pros and cons of usable recovery and map the way forward to achieving low-effort usable security by means of usable recovery.

### 3.4 A security measurement model

*Rainer Böhme (Universität Innsbruck, AT)*

License  Creative Commons BY 3.0 Unported license  
© Rainer Böhme

I reported on the main insight of Dagstuhl Seminar 14491, “Socio-Technical Security Metrics”, a security measurement model. We tried to map out the simplest core, putting all limiting assumptions on the board. Using the notation of structural equations modelling, the core of the model describes how an attacker’s efforts cause a loss, a relation that is influenced by how a defender’s efforts result in security. Randomness comes in in several forms, chiefly through measurement error and (by assumption) attacker behaviour.

### 3.5 Human-Centered Security Requires Risk Communication

*L. Jean Camp (Indiana University – Bloomington, US)*

License  Creative Commons BY 3.0 Unported license  
© L. Jean Camp

Safe, reliable, and secure computing requires risk-aware human behaviors. Specifically individuals must be empowered to distinguish not only between high risk and low risk choices when interacting with computers but also be able to act on that knowledge. They need to be able to identify risk and have those risks identified in a manner that informs their behavior. The capacity of humans as security managers depends on the creation of technology that is built upon a well-founded understanding of the behavior of human users and the half-century of research on risk communication. Thus systems must not only be “trustworthy” but also must systematically communicate the risks associated with behaviors enabled by even well-designed systems. Currently, computers that are trusted are not trustworthy, but in truth there is rarely 0% or 100% certainty of harm. My work seeks to align the semantically similar but fundamentally discordant concepts of risky and trustworthy by combining computer science with risk communication. Network analysts and computer scientists can identify possible harm, but only users can determine the behavior and risk appropriate for the task at hand. Beyond usable security we seek to design to enable users to make informed decisions.

### 3.6 Systems Modelling and Behavioural Economics

*Tristan Caulfield (University College London, GB)*

License  Creative Commons BY 3.0 Unported license  
© Tristan Caulfield

Security managers in companies must design security policies that meet their organization's security requirements. The many interactions between security policy, security controls and technology, business processes, and human behaviour make it difficult to evaluate the consequences of different choices. Systems models can create a representation of the system which can then be used to explore the effects of different policy choices. These models include human decision-making and recently we have been interested in seeing if models of decision-making from behavioural economics are applicable to security decisions and, if so, how they can be integrated into the modelling framework. We use a simple example of challenging behaviour and implement a model where decisions are based on social learning/herding.

### 3.7 The Security Behavior Observatory

*Nicolas Christin (Carnegie Mellon University – Pittsburgh, US)*

License  Creative Commons BY 3.0 Unported license  
© Nicolas Christin

I introduced the Security Behavior Observatory (SBO). The SBO is a dedicated panel of participants who opt in to instrumentation of their home computers. This allows us to take a hybrid approach to computer security user experimentation: the control and depth of laboratory experiments performed in the user's natural environment over a prolonged period of time. The SBO allows us to perform longitudinal studies of how attacks proliferate, how users notice and respond to attacks, and the effectiveness of various security mitigations. This infrastructure allows us to combine tracking, experimental, and survey data that will result in a unique understanding of real-world user behavior that will benefit researchers in a variety of computer science disciplines. We have a working prototype of the SBO, with approximately 400 participants enrolled to date. I also reported on a couple of experiments we have been running and solicited feedback on them.

### 3.8 Improving Risk Decisions on Mobile Devices

*Serge Egelman (ICSI – Berkeley, US)*

License  Creative Commons BY 3.0 Unported license  
© Serge Egelman


In the beginning, Android smartphones showed users all the permissions third-party apps needed at install-time. My group performed several qualitative and quantitative studies and showed this was bad because benign requests (e.g., Internet access, requested by 90% of applications) habituated users to more dangerous requests. Things changed: both iOS and Android now prompt at runtime, the first time an app requests any of a much narrower set of "dangerous" permissions. This runtime prompting allows the user to consider context: what they were doing at the time the first request occurs. Of course, this ignores the context of

subsequent requests. As a result, we have built a classifier to manage when users are shown permission requests, thereby reducing errors by a factor of five.

We have also been exploring users' decisions to screen lock their devices. We observed bounded rationality: many users provide seemingly rational decisions for not employing security, though often underestimate the sensitivity of their data. Similarly, even users using screen locks believe it takes too long – an average of 2s or 60s/day. Thus, any new mobile authentication scheme that takes more than two seconds is a non-starter.

### 3.9 Value-sensitive design of Internet-based services (the commensurability challenge)

*Hannes Hartenstein (KIT – Karlsruher Institut für Technologie, DE)*

License  Creative Commons BY 3.0 Unported license  
© Hannes Hartenstein

The main thesis of this pitch is that value-sensitive design is about the assessment of the risk that certain values are not fulfilled – not simply on costs, but on values – and, thus, can be used to assess ICT risks of socio-technical systems. There is a lot of activity in recent years in the area of ‘responsible innovation’ and ‘value-sensitive design’ (VSD). Van den Poel gives a definition and a linking of the notions of values, norm and technical requirements/designs. For our ‘use case’, access control, we compare VSD with OM-AM of Ravi Sandhu. The challenge is to ‘meet in the middle’, at the level of a norm. We (a recent paper by my group) approach this challenge and show that the approach clarifies the line between objectivity and subjectivity. Decision making under value conflicts and tradeoffs are pretty similar from a philosopher’s point of view and a computer scientist. The key challenges are clarification of terms, reaching consensus on value impacts and scoring approaches (‘value commensurability’). Our first steps to check whether VSD could be applied in the field of access control focusses on “who has the power/resources?” and on “self-direction” and, thus, what is known as the ‘administrative model’ or the identity and access governance. Our first findings show that categories can be determined and scoring looks possible. To conclude, value-sensitive design helps in linking technical design decision with the values they affect – and the risk assessment can link to those values as well, as long as the ‘commensurability challenge’ is something we can manage.

### 3.10 Modeling and Analysis of Security for Human Centric Systems

*Florian Kammüller (Middlesex University – London, GB)*

License  Creative Commons BY 3.0 Unported license  
© Florian Kammüller

We propose the application of formal methods to model infrastructure, actors, and policies in order to analyse security policies. In our work, we started from invalidating global policies by a complete exploration of the state space using Modelchecking. However, to counter the state explosion problem we now moved on to Higher Order Logic using the interactive theorem prover Isabelle. The expressive power allows modeling the process of social explanation inspired by Max Weber into an Isabelle Insider Threat framework. Recent applications are to airplane safety and security, insider threats for the IoT and for auction

protocols. The CHIST-ERA project SUCCESS plans to use the framework in combination with attack trees, and the Behaviour Interaction Priority (BIP) component architecture model to develop security and privacy enhanced IoT solutions. A pilot from the health care sector, cost-effective IoT-based bio-marker monitoring for early Alzheimer's diagnosis, will investigate the feasibility of the approach. Critical needs as an input for this process ICT Risk assessment methods to understand what security and privacy questions we need to answer to the stakeholders including patients, nurses and doctors.

### 3.11 Socio-Technical Q&A

*Stewart Kowalski (Norwegian University of Science & Technology – Gjøvik, NO)*

License © Creative Commons BY 3.0 Unported license  
© Stewart Kowalski

To be or not to be secure  
enough.  
That Is the question  
of our abilities  
and of our courage  
to ask  
the challenging  
socio-technical questions.  
So  
that we can  
Thinking, feeling, know  
and act  
to  
**Deter** our enemies  
**Protect** our friends  
**Respond** to attacks and crisis's.  
And  
If necessary  
**recover** through questioning  
not  
blaming  
all stakeholders.

### 3.12 Attack Surface of Socio-Technical Systems

*Kwok-Yan Lam (Nanyang TU – Singapore, SG)*

License © Creative Commons BY 3.0 Unported license  
© Kwok-Yan Lam

Researchers in technical disciplines are familiar with concepts such as risks, attack surface, attack vectors, exposure, threats and vulnerabilities. In this talk, we first look at the key security pillars behind the attack surface of a distributed system. Security protection behind the attack surface is typically enforced by a combination of physical security, technical

mechanisms, and organizational policies in order to achieve the security objectives in an efficient and effective manner. The risk and security controls employed by a system will depend on the nature of the system such as Government (civilian vs national security), Enterprise (Critical Information Infrastructure vs non-CII) or Consumer application systems (e.g. free Internet/cloud application services).

Security has always been taking into consideration people's aspects, though have been mostly piecemeal, ad hoc, implicit and over-simplified. For example, in the study of practical security, we choose key length and password length that is manageable by people, cover time of crypto algorithm before sensitivity of data does not matter anymore, classification of data according to their impact on real world.

In real world situations, security requirements/objectives always start from people e.g. defining business objectives of a system by the business owner. When studying the cybersecurity of socio-technical systems, it is useful to identify the steps and processes where people are involved in the security consideration of the system development lifecycle. The people/social factors are typically one of the major source of vulnerabilities, and vary from system to system. In reality, it is not uncommon that the same person may view security differently when involved in different type of systems. Conversely, different people involved in the same system may have different views on security. It is therefore important to identify the various stakeholders of a system, and study the security concerns of these stakeholders. In a typical real world scenario, we usually can identify the following stakeholders:

- System owners: their security concerns are mainly related to reputation and compliance with laws and regulations.
- System sponsors: their main security concerns include operational resilience (robustness and availability) and efficiency.
- System designer/developers: their security interests are typically the traditional information security issues.
- System administrators/operators: their main security interests include implementation audit and control procedures, enforcement of the corresponding policies, and sometimes involve in the compliance of physical security,
- End users: their security interests are mainly stemmed from their concerns for their accountability and liability.

Security risks lead to uncertainty to the liabilities of the people. Socio-technical systems take into consideration the social/people factors in the risk assessment of information systems. Ultimately, people are most concerned about liabilities though technical people tend to look at the security issues as risks. For example, in an Internet banking system, most users are mainly concerned about their liabilities should fraudulent transactions be detected. System owners and business sponsors of a system tend to consider liabilities while system designers/developers tend to look at risks. It'll be useful to establish a framework and model to understand the relationship between risk and liability.

The Information Systems community developed the Enterprise Architecture as a tool for establishing a framework and methodology for enabling/facilitating communications among all stakeholders so as to make sure the business/people requirements are taken into consideration in the entire system development lifecycle. It'll be useful for the security research community to explore the use of the EA as a basis for developing risk assessment models for socio-technical systems.


Another area that is important to look into is the massive deployment of IoT devices in new generation smart city/nation systems. The attack surface and risk model is more complicated. As a kind of socio-technical system, IoT-based applications are very different

from existing socio-technical systems because a lot of IoT devices are operated in open environment, hence a lot of physical security and organization processes are not enforceable. It deserves much attention of the cybersecurity research community in that it needs new approach to address cybersecurity of IoT-based application systems. Key socio-technical problems include:

- Identify the applicable laws and regulations for IoT applications.
- Study the social aspects of such systems such as the role of people in the security considerations of the development lifecycle of such systems.
- Investigate security requirements for IoT-based socio-technical systems.
- Develop models for analyzing security requirements and risks of such systems.
- Develop architectural frameworks for devising security protection and control measures for such systems.

### 3.13 Cyber Risk Information Sharing

*Stefan Laube (Universität Münster, DE)*

License  Creative Commons BY 3.0 Unported license  
© Stefan Laube

Cyber risk management in modern days reduces to a race for information between defenders and attackers. This is why cyber risk information sharing is recognized by scholars and politicians alike as a measure for defenders to gain an edge over attackers. However, rational defenders' sharing incentives are guided by selfish reasons, moderated by the effects of cyber risk information sharing. In my talk, I introduce how to rigorously survey these effects. Specifically, I consider information sharing as an act of communication, that can be analyzed by Lasswell's model of communication: "Who says what to whom in which channel with what effect?".

### 3.14 Heavy-tailed cyber security incidents: Which organization design to manage extreme events?

*Thomas Maillart (University of Geneva, CH)*

License  Creative Commons BY 3.0 Unported license  
© Thomas Maillart

There is broad evidence that cyber risks have extreme "heavy-tail" components, with quantitative evidence for personal data breaches, browser update delays, and cyber security incidents. With co-authors, analyzing the statistical properties of sixty thousand security events collected over six years at a large organization, we found that the distribution of costs induced by security incidents is in general highly skewed, following a power law tail distribution. However, this distribution of incident severity becomes less skewed over time, suggesting that the organization under scrutiny has managed to reduce the impact of large events. We illustrate this result with a case study focused on the empirical effects of full disk encryption on the severity of incidents involving lost or stolen devices. However, quantifying extreme risks at the aggregate level may not necessary provide insights at the fine-grained level. In this talk, I have therefore introduced a simple fine-grained cascading model, inspired from the St. Petersburg Paradox, which calibrates to all sorts of heavy-tailed distributions

(e.g., power-law, stretched exponential). This model may be used to statistically map real attack processes, involving overcoming layers of defenses, with incremental lower probability and higher potential damage.

### 3.15 How do you know that it works? The curses of empirical security analysis

*Fabio Massacci (University of Trento, IT)*

**License** © Creative Commons BY 3.0 Unported license  
© Fabio Massacci

**Joint work of** Luca Allodi, Stanislav Dashevskyi, Martina de Gramatica, Katsyarina Labunets, Fabio Massacci, Federica Paci, Viet Hung Nguyen, Julian Williams

**Main reference** M. de Gramatica, F. Massacci, W. Shim, U. Turhan, J. Williams, “Agency Problems and Airport Security: Quantitative and Qualitative Evidence on the Impact of Security Training”, preprint, 2016.

**URL** <http://materials.dagstuhl.de/files/16/16461/16461.FabioMassacci.Slides.pdf>

In this talk I discuss the difficulties behind empirical security analysis by illustrating some particular pitfalls through bad papers.

1. Partial data: some dataset might not contain the same type of information for different entities in the very same DB field and as a result we might infer completely wrong information (typical example is using NVD for comparing ProS vs FOSS). Some example bad papers are
  - Muhammad Shahzad et al., “A Large Scale Exploratory Analysis of Software Vulnerability Life Cycles,” Proc. of ICSE’13.
  - R. Sen, G. R. Heim, “Managing Enterprise Risks of Technological Systems: An Exploratory Empirical Analysis of Vulnerability Characteristics as Drivers of Exploit Publication,” Decision Sciences, 2016.
2. Too big to fail: several statistical tests were invented to deal with small samples. Statistical significance ( $p < 0.05$ ) comes therefore for free with large audit trails. If we confuse it with practical significance we obtain a wrong conclusion as the paper below:
  - K. Seung Hyun and K. Bung Cho, “Differential Effects of Prior Experience on the Malware Resolution Process,” MIS Quarterly 2014.
3. Who said it works: this is an ubiquitous problem in CS. We test our own system. While this is acceptable (at the beginning of one’s research) to know whether a technology really works we need to put it into the hands of its final users.
4. How do you know? We often decide which are the important metrics based on industry suggestions. This can be structured with proper qualitative studies.

#### References

- 1 L. Allodi, M. Corradin, F. Massacci. Then and Now: On The Maturity of the Cybercrime Markets. The lesson black-hat marketeers learned. IEEE Transactions on Emerging Topics in Computing. 4(1):35–46, 2016.
- 2 L. Allodi, V. Kotov, F. Massacci. MalwareLab: Experimenting with Cybercrime Attack Tools. In: Proc. of Usenix Security CSET 2013, Washington D.C., USA.
- 3 V. Kotov and F. Massacci. Anatomy of Exploit Kits: Preliminary Analysis of Exploit Kits as Software Artefacts. Proc. of ESSoS 2013, pp. 181–196.
- 4 F. Massacci, F. Paci, L. M. S. Tran, A. Tedeschi: Assessing a requirements evolution approach: Empirical studies in the air traffic management domain. Journal of Systems and Software 95:70–88 (2014).

- 5 L. Allodi, F. Massacci. The Work-Averse Attacker Model. In the Proceedings of the 23rd European Conference on Information Systems (2015).
- 6 V.H. Nguyen, S. Dashevskiy, and F. Massacci. An Automatic Method for Assessing the Versions Affected by a Vulnerability, Empirical Software Engineering Journal. (2015). Short version in V.H.Nguyen and F.Massacci. The (Un)Reliability of Vulnerable Version Data of NVD: an Empirical Experiment on Chrome Vulnerabilities. In: Proceeding of the 8th ACM Symposium on Information, Computer and Communications Security (ASIACCS)'13, May 7-10, 2013.
- 7 L. Allodi, F. Massacci. Comparing vulnerability severity and exploits using case-control studies. In ACM Transactions on Information and System Security (TISSEC). Short version in L. Allodi, F. Massacci. How CVSS is DOSSing your patching policy (and wasting your money). Presentation at BlackHat USA 2013, Las Vegas, USA.
- 8 F. Massacci, V. H. Nguyen. An Empirical Methodology to Evaluate Vulnerability Discovery Models. In IEEE Transactions on Software Engineering (TSE), 40(12):1147–1162, 2014.
- 9 Woohyun Shim, Luca Allodi, Fabio Massacci. Crime Pays If You Are Just an Average Hacker. Proceedings of IEEE/ASE 2012 Cyber Security Conference. Complementary publication in ASE Journal 2012, Vol. 2.
- 10 Massacci F., and Paci F. How to Select a Security Requirements Method? A comparative study with students and practitioners. In Proceedings of the 17th Nordic Conference in Secure IT Systems (NordSec), 2012.
- 11 K. Labunets, F. Massacci, F. Paci, S. Marczak, F. Moreira de Oliveira. Model Comprehension for Security Risk Assessment: An Empirical Comparison of Tabular vs. Graphical Representations To appear in Empirical Software Engineering.
- 12 K. Labunets, F. Massacci and F. Paci. On the Equivalence Between Graphical and Tabular Representations for Security Risk Assessment. To appear in Proceedings of REFSQ'17.
- 13 K. Labunets, F. Paci, F. Massacci. Which Security Catalogue Is Better for Novices? In Proc. of EmpiRE Workshop at IEEE RE'15.
- 14 M. de Gramatica, K. Labunets, F. Massacci, F. Paci, A. Tedeschi. The Role of Catalogues of Threats and Security Controls in Security Risk Assessment: An Empirical Study with ATM Professionals In the Proceedings of REFSQ 2015.
- 15 K. Labunets, F. Paci, F. Massacci, and R. Ruprai. An Experiment on Comparing Textual vs. Visual Industrial Methods for Security Risk Assessment. In Proc. of EmpiRE Workshop at IEEE RE'14.
- 16 Labunets, K., Massacci, F., Paci, F., and Tran, L.M.S. An experimental comparison of two risk-based security methods. In Proceedings of the 7th ACM International Symposium on Empirical Software Engineering and Measurement (ESEM), 163–172, 2013.

### 3.16 Enhancing Researches in the ICT Security Field

*Kanta Matsuura (University of Tokyo, JP)*

License  Creative Commons BY 3.0 Unported license  
© Kanta Matsuura

Let us explore approaches for enhancing researches in this field.

Establishing nice theories – Yes, they would have great impacts. They can help empirical studies, new problem formulation, and so on. Young researchers can be inspired.

Providing datasets – Yes, many of us wish to have good data for research purposes. Considering the scientific requirement such as reproducibility of the results, common datasets would be helpful. However, there is an intrinsic limitation: as long as the data is observed



before the defense method under research is published, the attack included in the dataset assumes that the attacker does not know the defense method.

Having competitions – Yes, the use of a common data on-site at a competition event associated with a conference can have educational effects as well.

Finally, testbeds – Yes, this may solve the problems inherent to the dataset approach to some extent. However, this approach can be very expensive (and hence quite hard to do in reality) if you try to do everything by yourself. In my poster and short pitch talk, I introduce a new venture of testbed: *bsafe.network*. *Bsafe* is a test network for the research of blockchain technologies and their applications. Although there are a lot of challenges, we consider the use of the lessons from the Internet. Details are described at <http://bsafe.network>, particularly in the white paper there. A wide variety of researches may be designed in the network, ranging from distributed ledger protocols to socio-technical applications.

### 3.17 Security Challenges in Small Organisations

*Simon Parkin (University College London, GB)*

**License** © Creative Commons BY 3.0 Unported license  
© Simon Parkin

**Joint work of** Simon Parkin, Andrew Fielder, Alex Ashby

**Main reference** S. Parkin, A. Fielder, A. Ashby, “Pragmatic Security: Modelling IT Security Management Responsibilities for SME Archetypes”, in Proc. of the 8th ACM CCS International Workshop on Managing Insider Security Threats (MIST’16), pp. 69–80, ACM, 2016.

**URL** <http://dx.doi.org/10.1145/2995959.2995967>

Here I provide a brief overview of a programme of user-centred security research involving micro- and small-sized organisations. Formal security training and in-house expertise may be limited or non-existent in these smaller organisations. Security vendors and providers of IT services and leased premises can play a role in the security posture of these organisations. The work involves collaboration with outsourced IT providers (and their clients) and other groups of organisations, such as charity associations. Small organisations can be diverse in their use of IT and daily interactions, where we are developing a range of SME archetypes as representative examples. I also discuss the Available Responsibility Budget (ARB) of small organisations, as a representation of organisation members’ collective capacity to manage a range of security controls, as well as high-level findings of initial interviews with representatives of small organisations.

### 3.18 Agent-based modelling for cybersecurity

*Wolter Pieters (TU Delft, NL)*

**License** © Creative Commons BY 3.0 Unported license  
© Wolter Pieters

Based on the expertise in our faculty, we are interested in developing further applications of agent-based models to study aspects of the security ecosystem, in particular in the critical infrastructure domain. In agent-based modelling, effects at system level (such as number of attacks) are studied based on modelling and simulating the behaviour of individual agents involved (such as attackers, defenders). This enables defenders to make better decisions, taking the expected responses of the other actors into account.


We have a successful proof-of-concept representing the vulnerability ecosystem, including behavioural models of attackers, discoverers, software vendors and software users, providing suggestions for the best patching strategies for vendors and users. We are also developing methods for investigating how these different actors make choices. We are interested in getting in touch with problem owners in the critical infrastructure domain who face security decision problems in multi-actor situations. By extending our models to new case studies, we can support security decisions as well as advance our research.

### References

- 1 Breukers, Y. P. (2016). The Vulnerability Ecosystem: Exploring vulnerability discovery and the resulting cyberattacks through agent-based modelling. Master's thesis, TU Delft.
- 2 Meeuwisse, K. V. M. (2016). The usability-security trade-off: Exploring employees' perceptions and preferences for technical security measures using choice modelling. Master's thesis, TU Delft.
- 3 Slangen, R. (2016). Understanding Cyber-risk by Investigating the Behaviour of Defender and Threat Agent Organisations: Why a Complex Adaptive Systems Perspective Contributes to Further Understanding Cyber-risk. Master's thesis, TU Delft.
- 4 van Wieren, M., Doerr, C., Jacobs, V., and Pieters, W. (2016). Understanding Bifurcation of Slow Versus Fast Cyber-Attackers. In: International Workshop on Data Privacy Management (pp. 19–33). Springer International Publishing.

## 3.19 Metrics for security-related behaviours and organisational economics and performance

*Martina Angela Sasse (University College London, GB)*

License  Creative Commons BY 3.0 Unported license  
© Martina Angela Sasse

In this talk, I reflected on metrics we have used over the past 20 years when studying security-related behaviours and organisational economics and performance. In the first study in 1996, realised it the importance of understanding the mental and physical workload [1] that security policies create for users, and the impact it has on their performance on the primary task. Users have an acute sense of the amount of time that is diverted from their primary productive activity, and when they have reached that compliance budget, they will look for ways of diverting it [2]. We subsequently proposed that security managers must measure the effort employees spend on security, and work with business decision-makers to balance that effort with the risk mitigation achieved [3]. In later studies, we found that not only the time spent on the security task counts, but that disruption of the primary task means up to 40% of that effort has to be re-done [4]. Users' behaviour is also driven by their degree of risk understanding, and users' emotional stance towards the organisation [5]. More recent studies have shown that the degree of communication and collaboration between security specialists and other members of the organisation is a good indicator for how effective security is [6], and finally the degree of trust the organisation places in their staff [7].

### References

- 1 Adams, A., Sasse, M. A. (1999). Users are not the enemy. *Communications of the ACM*, 42 (12):40–46.

- 2 Beutement, A., Sasse, M. A., Wonham, M. (2008). The compliance budget: managing security behaviour in organisations. Proceedings of New Security Paradigms Workshop.
- 3 Parkin, S., van Moorsel, A., Inglesant, P., Sasse, M. A. (2010). A stealth approach to usable security: helping IT security managers to identify workable security solutions. Proceedings of New Security Paradigms Workshop.
- 4 Steves, M., Chisnell, D., Sasse, A., Krol, K., Theofanos, M., Wald, H. (2014). Report: Authentication Diary Study. National Institute of Standards and Technology. <http://dx.doi.org/10.6028/NIST.IR.7983>
- 5 Beris, O., Beutement, A., Sasse, M. A. (2015). Employee Rule Breakers, Excuse Makers and Security Champions:: Mapping the Risk Perceptions and Emotions That Drive Security Behaviors. Procs NSPW.
- 6 Kirlappos, I., Parkin, S., Sasse, M. A. (2015). “Shadow security” as a tool for the learning organization. ACM SIGCAS Computers and Society, 45 (1):29–37.
- 7 Kirlappos, I., Sasse, M. A. (2015). Fixing Security Together: Leveraging trust relationships to improve security in organizations. Proceedings USEC.

### 3.20 Socio-Technical-Artefact Driven Security and Risk Analysis

*Christian Sillaber (Universität Innsbruck, AT)*

License © Creative Commons BY 3.0 Unported license  
© Christian Sillaber

Joint work of Ruth Breu

We propose a structured quality assessment process to utilize models of a system and related artefacts created by stakeholders (system, business process, activity diagrams, etc.) to improve the identification of potential security risks. While research considers users as the most important resource in security and risk management processes, little attention is given to various artefacts created by them during the creation and operationalization of complex systems. The proposed methodology can unveil inherent misunderstandings and miscommunications between the stakeholders, by comparing the produced models against each other, that could have introduced security issues during the development of the system. We conducted several field studies to evaluate the viability of the approach using a variety of different modelling languages and frameworks.

#### References

- 1 Sillaber, C., and Breu, R. (2015). Identifying Blind Spots in IS Security Risk Management Processes Using Qualitative Model Analysis. In T. Tryfonas & I. Askoxylakis (Eds.), *Human Aspects of Information Security, Privacy, and Trust* (Vol. 19, pp. 252–259).
- 2 Sillaber, C., and Breu, R. (2015). Using Stakeholder Knowledge for Data Quality Assessment in IS Security Risk Management Processes. In Proceedings of the 2015 ACM SIGMIS Conference on Computers and People Research (pp. 153–159).
- 3 Sillaber, C., and Breu, R. (2015). Using Business Process Model Awareness to improve Stakeholder Participation in Information Systems Security Risk Management Processes. In *Wirtschaftsinformatik 2015 Proceedings*.

### 3.21 Assessing ICT security risks in socio-technical systems: Policy implications

*Edgar A. Whitley (London School of Economics, GB)*

**License** © Creative Commons BY 3.0 Unported license  
© Edgar A. Whitley

**Joint work of** Latour, B. (2004). *Politics of nature: how to bring the sciences into democracy*, Harvard University Press Cambridge, Mass.; London.

**Main reference** E. A. Whitley, I. R. Hosein, “Doing the politics of technological decision making: Due process and the debate about identity cards in the UK”, *European Journal of Information Systems*, 17(6):668–677, Springer, 2008.

**URL** <http://dx.doi.org/10.1057/ejis.2008.53>

**Main reference** B. Latour, “Politics of Nature: How to Bring the Sciences into Democracy”, Harvard University Press, 2004.

**URL** <http://www.hup.harvard.edu/catalog.php?isbn=9780674013476&content=reviews>

My presentation had two components. It focussed on the socio-technical aspect of the workshop title more than the assessment of risk. It began by considering the expressions of socio-technical as presented in the “about me” posters produced by workshop participants. This was supplemented by oral descriptions of “socio-technical” in my working group. This indicated that the notion of socio-technical is very broadly understood and has many inconsistent interpretations. This can be significant because the different ways in which we conceptualise technology and its relationship to the social can have very different effects in terms of research design and real world policy implications.

Academically, the concept of socio-technical has a long, and specific, history, from its earliest uses in relation to the work of the Tavistock institute. More recently, there has been increased theorisation of how the social and technological might relate to each other, going beyond a simplistic “everything that is not the technological”.

One particular way of considering the relationship between the social and the technological (or facts versus values) is presented by Bruno Latour, particularly his book on the politics of nature. I reviewed this model and highlighted the ways in which it could help clarify the different roles of technologists: working through perplexities (i.e. areas where there is no agreement on what is “true” (e.g. the best ways to assess ICT security risk”) and institution (i.e. areas where there is agreement on what is true (or what is no longer suitable / acceptable as a practice in the field)).

### 3.22 Human Factors in Information Security

*Sven Übelacker (TU Hamburg-Harburg, DE)*

**License** © Creative Commons BY 3.0 Unported license  
© Sven Übelacker

The working title of my PhD thesis covers the ample intertwined area of human interaction with information and communication systems regarding security. I focus on the targeted side of socio-technical attacks: what kind of enablers exist; why are some people (more) susceptible to social engineering attacks (than others). By doing so, I am facing two main challenges:

First of all, evidence of social engineering attacks needs to be discovered, analysed and understand. However, successful real-life attacks are rarely documented reliably and in detail. How can we draw generalisable conclusions for the real world? Experiments can hopefully shed a bit of light on a specific sample size in a small time frame, but can be as realistic

as they can be intrusive, ethically questionable or counterproductive for a security culture in the long run. If we look at documented cases, how reliable can we determine the source is reporting honestly? We are living in click-bait times of online “news”; hear-saying and interviews – of victims or (former) criminals – on real events can not be re-evaluated by fellow researchers and can only be qualitative. Law enforcement agencies publish their statistics, but most of the time their databases with more detailed information remain confidential and re-calculating or re-categorising their data is almost impossible. Consulting companies publish their reports and surveys with no public access to the data and may have their own interests like to acquire new customers. Expert opinion and guesstimates on possible attack scenarios can help to understand the knowledge of novel attack vectors, but how realistic and feasible are they without proper real events or experimentalisation? Finding reliable, useful and detailed evidence for holistic analyses should still be a valuable prerequisite before designing detection and mitigation strategies of attacks targeting humans. I am confident a good combination of various approaches and sources can lead to a better understanding, i.e., conducting experiments based on real events, re-conducting questionnaires and experiments internationally, or mapping incidents to expert opinion.

Secondly and complementing the anterior paragraph, it is crucial to understand the susceptibility of targeted persons. Many disciplines present ideas about human behaviour, biases, habits, irrationality, heuristic systems, usability, persuasion, personality, gullibility, risk perception/assessment, impulsiveness, stressors or cultural background to name a few. Insights can be very helpful for adapting the work environment and its culture, improving security mechanisms with respect to usability, organisational policies, interventions and trainings. Interdisciplinary research and a combination of the mentioned factors may leverage results.

## 4 Working groups

### 4.1 Collecting Data for the Security Investment Model

*Tristan Caulfield (University College London, GB), Rainer Böhme (Universität Innsbruck, AT), Kanta Matsuura (University of Tokyo, JP), Tyler W. Moore (University of Tulsa, US), Martina Angela Sasse (University College London, GB), Michel van Eeten (TU Delft, NL), and Maarten van Wieren (Deloitte – Amsterdam, NL)*

**License** © Creative Commons BY 3.0 Unported license  
© Tristan Caulfield, Rainer Böhme, Kanta Matsuura, Tyler W. Moore, Martina Angela Sasse, Michel van Eeten, and Maarten van Wieren

We considered a security investment model, proposed by Rainer Böhme, to estimate from data the relationships between efforts to secure an organization, the level of security actually achieved, and how well this level of security moderates efforts to attack the organization and the losses experienced. This model can be applied to many different types of organizations or systems to understand how investments in different security efforts affect security and prevent incidents and losses. While we briefly discussed examples such as hosting providers and bitcoin exchanges, we mainly explored how it could be applied to typical organizations, such as small-to-medium enterprises (SMEs).

We compiled a list of different indicators that could be measured for each component of the model. For indicators of effort towards security, the list includes organizational efforts, such as how much budget or staff-hours are allocated to security, as well as formal controls,

such as the existence of policy documents and continuity plans, and informal controls, such as whether employees share passwords, use of encryption, and security awareness training. For the level of security, the indicators must be independent of the attacker; it would be incorrect, for example, to use the number of machines infected with malware as an indicator here. Indicators for security include patch level and patch speed, results of brute force password cracking, penetration testing results, indicators of network and system hygiene, such as open mail relays and unused but running VM instances or servers, as well as human measures, including the Behavioural Security Grid to gauge employees' attitudes and behaviours towards security.

For attacker effort, possible measurable indicators could include network attack indicators, such as IDS events, ports scans, and malware encounters, as well as social engineering attempts, and types and frequencies of different attacks. The value for attacker effort could also be held constant across different organizations, if this information is too difficult to gather. Losses represent the impact and consequential effects of attacks. Indicators discussed include the number of incidents of ransomware and phishing, incidents of data theft, PCI incidents, DDoS attacks that interrupt business, theft of information or equipment, and incidents of different types of fraud. It is also possible to use various types of monetary loss as indicators, such as fines, investigation or recovery costs, lost revenue, and productivity losses resulting from an incident.

With data from a large number of companies, this model can be used to explore the effects of investments in different security efforts on organizations' security. This can then be used to help guide security investment by, for example, determining if a particular security control has an impact on the incidents or losses for organizations of a given size, or by finding the optimal investment in different security efforts for a given budget. Finally, we discussed what steps could be taken to collect this data, with a focus on working with IT service providers to gather data about and distribute surveys to their SME clients.

## 4.2 New frontiers of socio-technical security

*Carlos H. Ganan (TU Delft, NL), Zinaida Benenson (Universität Erlangen-Nürnberg, DE), Hannes Hartenstein (KIT – Karlsruher Institut für Technologie, DE), Stewart Kowalski (Norwegian University of Science & Technology – Gjøvik, NO), Kwok-Yan Lam (Nanyang TU – Singapore, SG), Christian W. Probst (Technical University of Denmark – Lyngby, DK), Edgar A. Whitley (London School of Economics, GB), and Jeff Yan (Lancaster University, GB)*

**License** © Creative Commons BY 3.0 Unported license  
 © Carlos H. Ganan, Zinaida Benenson, Hannes Hartenstein, Stewart Kowalski, Kwok-Yan Lam, Christian W. Probst, Edgar A. Whitley, and Jeff Yan

Socio-technical security paradigms continue emerging and new frontiers have to be identified to address these paradigms. New approaches and methods are required to investigate these frontiers where the human factor becomes a critical component of these socio-technical systems (STS). Analyzing these systems using multi-actor theories shed light to these systems and provides an essential tool to investigate new frontiers. The Internet of Things constitutes an example of these complex STS where new frontiers have to be defined. One of the main security challenges of such systems is that a lot of existing security architecture/models are not applicable to such scenarios. Another challenge is that a lot of IoT devices are developed and released to the market, a lot of organizations are making big promises for the

pervasive use of IoT devices in smart city/nation applications, but there is very little prior experience/knowledge for designing and analyzing the security of such systems. New solutions have to be envisioned to take over the security of IoT devices which become “orphaned” either because they are abandoned by their manufacturer or because the manufacturer goes out of business. Software escrow and graceful degradation are potential mechanisms that will help to mitigate the impact of orphaned IoT devices. The implementation and coexistence of these mechanisms with IoT devices already in the market arises new challenges that need to be addressed from a socio-technical perspective.

### 4.3 Unpacking the motivations of attackers

*Thomas Maillart (University of Geneva, CH), Ross Anderson (University of Cambridge, GB), Johannes M. Bauer (Michigan State University – East Lansing, US), Barbara Kordy (IRISA – Rennes, FR), Gabriele Lenzini (University of Luxembourg, LU), and Sebastian Pape (Goethe-Universität Frankfurt am Main, DE)*

License © Creative Commons BY 3.0 Unported license

© Thomas Maillart, Ross Anderson, Johannes M. Bauer, Barbara Kordy, Gabriele Lenzini, and Sebastian Pape

The Internet was once thought to remain a conflict free space. Following technical innovation and its progressive integration in the social fabric, attacks and conflicts have appeared early on. They have since then steadily developed in sophistication, diversity and span. Analyzing the strategic motivations and modus operandi of both landmark and outstanding cyber-attacks and cyber-conflicts, we have found that they are aimed at disrupting the socio-technical system through the social sub-system (e.g., social engineering, deception, blackmail, mass media manipulation) through the technical sub-system (e.g., exploiting a vulnerability, manipulating social media), or through a combination of both.

Disruption may occur at various levels and time-horizons, which can be partitioned as proposed by John Groenewegen:

- level 0: resource allocation (i.e., continuous time operations),
- level 1: governance (1 to 10 years),
- level 2: institutional environment (10 to 100 years),
- level 3: embeddedness (100 to 1000 years).

Cyber attacks are aimed at gaining technical, social, economic, political or cultural power. On the contrary, they may be aimed at ensuring the status quo. We provide a few examples to give flesh:

- Crypto War 1 was the NSA trying to defend its level 2 institutional business model against disruptive changes at levels 0 and 1. The debate over DRM was the exact same, more or less; Hollywood and the music industry wanted to defend their business model against disruptive change and set out to bully the tech industry to redesign the world. The tech industry pretended to do so but ate their lunch.
- Crime Policing: The failure of policing as crime goes online may reflect a failure of the police to create the needed international institutions for fast cheap MLAT, but on the surface is much like crypto wars or DRM. As for the cybercriminals there’s now a new institution, namely the international network of cybercrime operators and their suppliers, who appear to collude with some governments.

- Early hacktivism (such as the cypherpunks) was an attempt to use action at level 0 (writing software) to change ultimately all higher levels, by creating an ungovernable space in which people could transact with digital cash over anonymous remailers regardless of the wishes of established governments. It was perhaps more an attack on level 2, trying to establish Californian social norms worldwide at level 3 – or at least trying to make available to all a space in which these norms were the rule.
- Cyberbullying is mostly operational; it can be worse than real-world bullying as it doesn't stop when you get home, but better in that the teacher has a trail of who did it (provided she can get US-based providers to cooperate, which is level 1 intrusion).

Unpacking the motivations of attackers in the cyberspace requires to recognize the increasing integration of the socio-technical system. In this integrated system, the (strategic) purpose and (tactical) means play a fundamental role in the way and at which level(s) the cyberspace can be disrupted (resp. the status quo preserved). As a result, cyber attacks may have implications at corresponding time horizons, ranging from the disruption of immediate operations to the disruption of governance, institutions, and even long-established cultural norms. Our approach shall provide a sense of importance of (intent of) attacks in the cyber space-time, and hence help set more insightful and efficient agenda in order to prevent or mitigate attacks, or on the contrary, to promote such attempts to disruption if perceived as a potentially positive outcome.

#### 4.4 Software Liability Regimes

*Christian Sillaber (Universität Innsbruck, AT), Nicolas Christin (Carnegie Mellon University – Pittsburgh, US), Richard Clayton (University of Cambridge, GB), Stefan Laube (Universität Münster, DE), Fabio Massacci (University of Trento, IT), Tyler W. Moore (University of Tulsa, US), Kai Rannenberg (Goethe-Universität Frankfurt am Main, DE), and Michel van Eeten (TU Delft, NL)*

**License** © Creative Commons BY 3.0 Unported license  
 © Christian Sillaber, Nicolas Christin, Richard Clayton, Stefan Laube, Fabio Massacci, Tyler W. Moore, Kai Rannenberg, and Michel van Eeten

New software based services are currently not covered through product liability regimes as software that is sold through licenses is not considered a product. This introduced a market where the parties that are in a position to fix problems (i.e. software developers and service providers) are not assigned any liability for resulting damages. This increases social costs and does not incentivise companies to invest in quality and security improvements for their software and services.

To address this imbalance, we call for the introduction of a software liability regime to cover negligent software development practice. To establish whether a software developer has been negligent or not, standards are required (to prove a violation).

A first logical step would be the introduction of mandatory certifications and standards for commercial software. However, standards are quickly out-of-date and the software industry has no incentives to buy in. Therefore, software security standards may be enforced by law. These should focus on the processes to be followed during implementations, as it is easier to certify development processes and the usage of state-of-the-art components that software properties. A baseline for such a standards should define testing processes (e.g. buffer overflow testing). The certifying body should not only audit that the software development processes



follow best-practice but also perform (randomized) sampling of the actual functioning of used software tests.

To steer public discussion into an appropriate direction, it would make sense to differentiate between commodities (e.g. household appliances) that are sold to and used by uneducated users and professional appliances. Software running on such devices should either be fully managed or certified by a licensed professional to be “safe for uneducated users” without them needing to do anything. If the manufacturer of commoditized software chooses an upgrade strategy over the Internet, then any upgrade should be safe for the uneducated user. Upgrades developed for such devices should be subject to the same rules as spare parts for physical products. Professional appliances should be explicitly labelled as such and there should be a process to determine whether a user has indeed the required professional competence (e.g. licence, expertise) to handle and configure a professional device.

In summary, policy makers should get active and introduce appropriate legislation.

The following questions have been raised during the working group discussions and will be investigated further:

- How can we test for negligence as an indicator for liability?
- What does strict liability and negligence mean?
- How can we attribute the faulty code? Forensics? Proofs?
- How is a customer able to provide enough probable cause?
- Is it necessary to start a discussion on mandatory certification of commercial software?
- What about software that becomes vulnerable over time (e.g. RC4/MD5)? How long are re-sellers/developers required to provide security updates?
- Which accountability functionalities for software should be required by law?
- What should the lawmaker do about software whose functionality is not 100% understandable? E.g. AI gone wrong.
- How can poor development be proven by experts? E.g. openssl, easy ex-post, but difficult ex-ante.
- How to handle installation v.s. maintenance?
- What is the safety and security level that can be expected from a device?
- What about free software developers? Would a too strict liability regime stifle innovation?
- How should a universal computer be treated differently from a (closed) consumer device?
- How to handle negligence of a consumer device was jailbroken?
- How should maintenance be handled? Any device should be updatable by a layman/uneducated user?
- What is the relationship between insurance and certification?

## 4.5 User-centred Security Models

*Sven Übelacker (TU Hamburg-Harburg, DE), Vincent Koenig (University of Luxembourg, LU), and Simon Parkin (University College London, GB)*

**License** © Creative Commons BY 3.0 Unported license  
© Sven Übelacker, Vincent Koenig, and Simon Parkin

The working group began with discussions about how cognitive biases leave users behind in some security tasks, and that we will suffer to achieve an acceptable level of security. This then led to identification of factors – contextual, psychological, social – which influence security-relevant choices. A range of approaches were discussed by the working group:

- Identifying stakeholders and mapping them to decisions about security infrastructure. Are all stakeholders represented adequately in security-related decisions?
- When designing processes, security is not an add-on. 100% security may not be achievable, and security is a process. Is it feasible and desirable to bound security responsibilities, e.g., by being responsible for others? Can we define a minimum level of security effort for users?
- How much security is “good enough”? We have no universal definition of “good” security behaviour, and we postulate to stay away from normative approaches where the user is forced to comply. This also points to the issue of ethics in security that is “good enough”. The group discussed this and also compared the problematic to that of the “Collingridge dilemma”.
- Whether there is any security advice which will remain stable over time, for instance when teaching children about security. This affects the lifetime of models.

Overall, many researchers are already investigating these areas, and yet barriers remain which may be better understood through development of user-centred models.

## Participants

- Ross Anderson  
University of Cambridge, GB
- Johannes M. Bauer  
Michigan State University –  
East Lansing, US
- Zinaida Benenson  
Universität Erlangen-  
Nürnberg, DE
- Rainer Böhme  
Universität Innsbruck, AT
- L. Jean Camp  
Indiana University –  
Bloomington, US
- Tristan Caulfield  
University College London, GB
- Nicolas Christin  
Carnegie Mellon University –  
Pittsburgh, US
- Richard Clayton  
University of Cambridge, GB
- Serge Egelman  
ICSI – Berkeley, US
- Carlos H. Ganan  
TU Delft, NL
- Dieter Gollmann  
TU Hamburg-Harburg, DE
- Hannes Hartenstein  
KIT – Karlsruher Institut für  
Technologie, DE
- Florian Kammüller  
Middlesex University –  
London, GB
- Vincent Koenig  
University of Luxembourg, LU
- Barbara Kordy  
IRISA – Rennes, FR
- Stewart Kowalski  
Norwegian Univ. of Science &  
Technology – Gjøvik, NO
- Kwok-Yan Lam  
Nanyang TU – Singapore, SG
- Stefan Laube  
Universität Münster, DE
- Gabriele Lenzini  
University of Luxembourg, LU
- Thomas Maillart  
University of Geneva, CH
- Fabio Massacci  
University of Trento, IT
- Kanta Matsuura  
University of Tokyo, JP
- Tyler W. Moore  
University of Tulsa, US
- Sebastian Pape  
Goethe-Universität  
Frankfurt am Main, DE
- Simon Parkin  
University College London, GB
- Wolter Pieters  
TU Delft, NL
- Christian W. Probst  
Technical University of Denmark  
– Lyngby, DK
- Kai Rannenberg  
Goethe-Universität  
Frankfurt am Main, DE
- Martina Angela Sasse  
University College London, GB
- Christian Sillaber  
Universität Innsbruck, AT
- Sven Übelacker  
TU Hamburg-Harburg, DE
- Michel van Eeten  
TU Delft, NL
- Maarten van Wieren  
Deloitte – Amsterdam, NL
- Melanie Volkamer  
Karlstad University, SE
- Edgar A. Whitley  
London School of Economics, GB
- Jeff Yan  
Lancaster University, GB

