CV and Research Statement

Markus Jakobsson

1 My Background

- **Focus.** *Identification of security problems, trends and solution along four axes* – computational, structural, physical *and* social*; quantitative and qualitative fraud analysis; development of disruptive security technologies.*
- **Education.** *PhD* (Computer Science/Cryptography, University of California at San Diego, 1997); *MSc* (Computer Engineering, Lund Institute of Technology, Sweden, 1994).
- **Research labs.** *San Diego Supercomputer Center* (Researcher, 1996-1997); *Bell Labs* (Member of Technical Staff, 1997-2001); *RSA Labs* (Principal Research Scientist, 2001-2004); *Xerox PARC* (Principal Scientist, 2008-2010); *PayPal* (Principal Scientist, 2011-2013); *Qualcomm* (Senior Director, 2013-2015); *Agari* (Chief Scientist, 2016-2018) ; *Amber Solutions* (Chief of Security and Data Analytics, 2018-)
- **Academia.** *New York University* (Adjunct Associate Professor, 2002-2004); *Indiana University* (Associate Professor & Associate Director, 2004-2008; Adjunct Associate Professor, 2008-2010).
- **Entrepreneurial activity.** *RavenWhite* (Authentication solutions; Founder, 2005); *Extricatus* (Security consulting; Founder, 2007); *FatSkunk* (Malware detection; Founder, 2009); *LifeLock* (Id theft protection; Member of fraud advisory board, 2009-2010); *CellFony* (Mobile security; Member of advisory board, 2009-2010).
- **Anti-fraud consulting.** *KommuneData* [Danish govt. entity] (1996); *J.P. Morgan Chase* (2006-2007); *PayPal* (2007-2010); *Boku* (2009-2010); *Western Union* (2009-2010).
- **Intellectual Property.** *Inventor of 100+ patents; expert witness in several patent litigation cases* (McDermott, Will & Emery; Bereskin & Parr; WilmerHale).
- **Publications**. Two books – *Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft* (Wiley, 2006); *Crimeware: Understanding New Attacks and Defenses* (Symantec Press, 2008); *100+ peer-reviewed publications* (list available separately).

2 My Beliefs

What is security? Computer security allows the enforcement of rules, standards and desirable behaviors. It hinges on an understanding of how systems can fail, followed by a design – whether on the protocol level or algorithm level – that forces a potential adversary to align his behavior with the desired behavior. Systems that achieve this are *secure*.

However, it is not meaningful to speak about security without first understanding the goals and limitations of the adversary: security is a *relative* concept. A system can be secure against one form of abuse without being secure against another. This makes it crucial to understand the constraints of potential adversaries. These constraints may be *computational* (requiring an understanding of lower bounds of computational efforts), *structural* (related to an understanding of protocols and business models), *physical* (e.g., be relative to how an adversary can manipulate devices), and *social* (such as in the context of phishing, where consumer psychology is defining the abilities of the adversary.) The client devices and the security measures running on these can be characterized in a similar manner. Computer security requires an understanding of all the dimensions of a problem, and the devices or resources we wish to protect.

Computer security: invisible and dynamic. No matter where we look, abuse is conceivable. The failure to defend against it can affect the privacy of individuals, the intellectual property investments of organizations, and the integrity of governments. Everybody is affected. But not everybody should have to worry: Security should be automatic, natural, and built in.

Since abuse is not static, but is a reaction to opportunities, security must be proactive. This makes it vital to understand trends – in computational ability, device deployment, application usage, and social and human constraints. To the extent that it is possible, these features must be measured, their results extrapolated.

3 My Work

How I select what to work on. My work is cross-disciplinary, and driven by market forces – *before* they express themselves. I spend time identifying potential trends and testing hypotheses before I embark on an effort. Let me give two examples to explain what I mean.

- **Social aspects of security.** In year 2001, years before media used the term "phishing", I was put in charge of identifying trends that could affect the revenue of my employer (RSA Security). I anticipated that the growth of online commerce would result in an increase in online fraud, and identified it as a *socio-technical* computer security problem. (This belief was considered bordercase ludicrous at the time.) My work on phishing grew out of a conviction that this would become a significant issue. The needs to understand the human aspect of the problem led me to study psychology

and to develop experimental approaches that can measure vulnerability to fraud (standard surveys will *not*). This fueled my work on ethical experimentation, and required an understanding of the goals of Internal Review Boards.

Having identified what makes people vulnerable, I could establish technical goals. For example, I had determined that the most common way for consumers to identify phishing attempts was by identifying the *presence* of *incorrect* information (as opposed to the *absence* of *correct* information). This begged the question whether a fraudster could construct an email message that will say "Dear Wells Fargo client" only to actual Wells Fargo clients, and "Dear PayPal user" to actual PayPal users? (My students and I established that the answer is *yes*; see `browser-recon.info` for a demo.) Similarly, I knew that password reset was – and still is – one of the weak links. This prompted me to develop alternative ways for backup authentication that did not rely on long-term memory; which avoided common attacks; and which were usable. (For a demo of one way to address this problem, see `www.visual-blue-moon-authentication.com`.)

One of the attached papers (not yet published) describes how the security of this password reset scheme can be quantified.

- **Physical aspects of security.** Similarly, my understanding of the power limitations of handheld devices has driven my work on alternative anti-virus paradigms for mobile computing. I am convinced that the status quo is doomed: One cannot constantly run a computationally intensive process on a device with limited power. (This is not a practical problem yet, as the power consumption depends on the number of malware threats in a manner that varies between logarithmic and linear, and there is hardly any mobile malware in circulation. In 2-3 years, as smartphones are estimated to surpass Windows machines in commonality, it will be a real and pressing problem, though.) This insight fueled my work on software-based attestation, where I have developed the first provably secure technology – no heuristics needed – for which the execution time to screen a device is a matter if milliseconds. This based on the simple fact that in order for a malware agent to be *active*, it needs to take up *some* space in RAM. If all RAM overwritten by a pseudorandom string, the malware agent needs to relocate some of this data; later, if we compute a keyed checksum of the entire RAM, then this relocated data needs to be accessed. This causes a delay, which then becomes indicative of the existence of an active malware agent.

  One of the attached papers (not yet published) describes this approach in detail.

  My work on mobile malware also motivated me to understand how carriers can use anomaly detection to identify and classify epidemics. Virus or trojan? Propagated by Bluetooth or SMS? It is possible to tell without ever analyzing the malware code, but just by looking at how it moves

through the network. The detection is fast, central, and does not drain the batteries of the client devices.

Management style. I have managed groups of researchers in a number of different roles – most recently as Principal Scientist at Xerox PARC, and as a Founder/CTO of FatSkunk, previously as a faculty member managing PhD students and junior colleagues. I believe in delegation and personal responsibility, and begin management relationships by determining the degree of independence (and desired independence) of each team members. I do not micro-manage, but I do provide suggestions for improvements.

Vision of future needs. It is not meaningful to try to defend against a threat that one does not understand. The first step must be to understand and quantify the problem, and to recognize what constrains the possible solutions. This must be done in terms of the *computational*, *structural*, *physical* and *social* dimensions.

There is a substantial need for work that secures the infrastructure, whether from technical or social threats. This will involve malware detection and recovery; robustness against denial of service and denigration attacks; establishment of identity (whether device or user); maintenance of trust (on both a technical and human level); user communication (including avoidance of social engineering, how to communicate important information to unmotivated users, and how to build security mechanisms that are usable in the face of adversarial campaigns). There is also need to recover from failures on various levels; and to use anomaly detection for early-warning systems. It is important to understand that user behavior will change dramatically in situations of attack, and this may in itself destabilize systems. To address these issues, a broad understanding of vulnerabilities, technologies, and trends is necessary.

4 Three Sample Publications

I have published two books and 100+ peer-reviewed articles. An extended version of this document with three sample publications at `markus-jakobsson.info`.

- *"Using Amazon Mechanical Turk to Improve Internet Security: The Case of Visual Password Reset"* demonstrates my understanding for novel experimental designs to deliver and evaluate security in socio-technical contexts.
- *"Practical and Provably Secure Software-Based Attestation"* shows my ability to challenge traditional paradigms and produce disruptive technologies.
- *"Almost Optimal Hash Sequence Traversal"* demonstrates my mathematical abilities and eye to computational efficiency.