Articles for Oral Presentation

Assignment 1 (0 marks)
COMPSCI 725, S2 2017

Clark Thomborson
University of Auckland
Version 1.00 of 24 July 2017

Instructions:

1) You should submit a rank-ordered list of three articles you're willing to present orally in this course.
   a) List your highest preference first.
   b) Your articles must be chosen from the ones referenced in this handout.
   c) Identify each article on your list by the **surname** of its **first** author and the year of publication e.g. "Walker 2012, Baki 2017, Yampolskiy 2016". Hint: use the bracketed label on the article's bibliographic details.
   d) I strongly encourage you to pick articles that build on knowledge you gained in your undergraduate studies, e.g. in operating systems, UI design, software design, hardware architecture, networking, cryptography. (Every student in this class should have some knowledge of some of these topics, as they are taught at an advanced undergraduate level in a reputable university.)
   e) Submit on https://canvas.auckland.ac.nz/courses/22109/assignments/67736
   f) **Deadline** for submission: midnight Friday 4 August.
      i) You will get 0 marks on your oral presentation, if you fail to submit a preference list before the deadline.
      ii) If you change your mind after submitting your list, you may resubmit by email to me on cthombor@cs.auckland.ac.nz at any time prior to the due-date for this assignment.
      iii) I'll handle all first-submissions before I reassign anyone.

What happens next:

2) I will assign up to three students to an article, using a **first-come-first-served** (FCFS) allocation strategy.
   a) I'll make assignments approximately daily, at some unpredictable time each day. I'll update the oral report schedule for S2 2017 to show the new assignments.
   b) If you submit early, you're more likely to get your first choice, and you're more likely to be required to present your oral report early in the semester.
   c) I will maintain an average of about 2.5 students per article.
3) At the beginning of the third week of classes, I will finalise the list of articles to be presented orally. I will also propose dates for all student oral presentation on the oral report schedule for S2 2017.
   a) I will try to arrange the schedule so that all oral presentations on the same article are presented during the same week of lectures – ideally during the same lecture period.
   b) If I assign you to an oral-presentation day on which you are unable to attend lectures, please let me know as soon as possible so that I can adjust the draft schedule.

4) All students are expected to read each article ***before*** the first day on which it will be presented orally.
    a) All students are expected to contribute (at least occasionally) to the discussion-period after each presentation.
5) I will finalise the oral report schedule for S2 2017 at the end of the third week.
    a) You will get 0 marks on your oral presentation, if you fail to present on your scheduled day for any avoidable reason.
    b) Please review the "Handling absence or illness" section of the lecture page.
    c) The marking schedule for your oral presentation is in the first set of lecture slides.

List of articles

There will be six themes for this year's offering of COMPSCI 725 as listed below: ethical security, human factors in security, security science(?), software (in)security, hardware (in)security, and privacy.

Any article that is presented orally in class by a COMPSCI 725 student is on the required-reading list for this offering of the course. The other articles listed below will *not* be on the required reading list. Therefore your choice of article will help to decide the relative importance of the six themes in this offering of COMPSCI 725.

A. Ethical Security

1. [Walker 2012] Mary Walker and Cynthia Townley, "Contract cheating: a new challenge for academic honesty?" *Journal of Academic Ethics* 10:1, 2012, pp. 27-44. [Download]

    Abstract: 'Contract cheating' has recently emerged as a form of academic dishonesty. It involves students contracting out their coursework to writers in order to submit the purchased assignments as their own work, usually via the internet. This form of cheating involves epistemic and ethical problems that are continuous with older forms of cheating, but which it also casts in a new form. It is a concern to educators because it is very difficult to detect, because it is arguably more fraudulent than some other forms of plagiarism, and because it appears to be connected to a range of systemic problems within modern higher education. This paper provides an overview of the information and literature thus far available on the topic, including its definition, the problems it involves, its causal factors, and the ways in which educators might respond. We argue that while contract cheating is a concern, some of the suggested responses are themselves problematic, and that best practice responses to the issue should avoid moral panic and remain focussed on supporting honest students and good academic practice.

2. [Wu 2017]. Xiaolin Wu and Xi Zhang, "Automated Inference on Criminality using Face Images", arXiv:1611.04135v3 [cs.CV], CoRR, 26 May 2017, 14 pp. [Download]

    Abstract: We study, for the first time, automated inference on criminality based solely on still face images, which is free of any biases of subjective judgments of human observers. Via supervised machine learning, we build four classifiers (logistic regression, KNN, SVM, CNN) using facial images of 1856 real persons controlled for race, gender, age and facial expressions, nearly half of whom were convicted criminals, for discriminating between criminals and non-criminals. All four classifiers perform consistently well and empirically establish the validity of automated face-induced inference on criminality, despite the historical controversy surrounding this line of enquiry. Also, some discriminating structural features for predicting criminality have been found by machine learning. Above all, the most important discovery of this research is that criminal and non-criminal face images populate two quite distinctive manifolds. The variation among criminal faces is significantly greater than that of the non-criminal faces. The two manifolds consisting of criminal and non-criminal faces appear to be concentric, with the non-criminal manifold lying in the kernel with a smaller span, exhibiting a law of "normality" for faces of non-criminals. In other words, the faces of general law-biding public have a greater degree of resemblance compared with the faces of criminals, or criminals have a higher degree of dissimilarity in facial appearance than non-criminals.

Preface [added in v3]: In November 2016 we submitted to arXiv our paper "Automated Inference on Criminality Using Face Images". It generated a great deal of discussions in the Internet and some media outlets. Our work is only intended for pure academic discussions; how it has become a media consumption is a total surprise to us. Although in agreement with our critics on the need and importance of policing AI research for the general good of the society, we are deeply baffled by the ways some of them mispresented our work, in particular the motive and objective of our research.

3. [Yampolskiy 2016]. Roman V. Yampolskiy and M. S. Spellchecker, "Artificial Intelligence Safety and Cybersecurity: a Timeline of AI Failures", *arXiv:1610.07997v1 [cs.AI]*, CoRR, 25 Oct 2016, 12 pp. [Download]

   Abstract: In this work, we present and analyze reported failures of artificially intelligent systems and extrapolate our analysis to future AIs. We suggest that both the frequency and the seriousness of future AI failures will steadily increase. AI Safety can be improved based on ideas developed by cybersecurity experts. For narrow AIs safety failures are at the same, moderate, level of criticality as in cybersecurity, however for general AI, failures have a fundamentally different impact. A single failure of a superintelligent system may cause a catastrophic event without a chance for recovery. The goal of cybersecurity is to reduce the number of successful attacks on the system; the goal of AI Safety is to make sure zero attacks succeed in bypassing the safety mechanisms. Unfortunately, such a level of performance is unachievable. Every security system will eventually fail; there is no such thing as a 100% secure system.

B. Human Factors in Security

4. [Baki 2017]. Shahryar Baki, Rakesh Verma, Arjun Mukherjee, and Omprakash Gnawali, "Scaling and Effectiveness of Email Masquerade Attacks: Exploiting Natural Language Generation", *Proc. 2017 ACM on Asia Conference on Computer and Communications Security*, ACM, 2017, pp. 469-482. [Download]

   Abstract: We focus on email-based attacks, a rich field with well-publicized consequences. We show how current Natural Language Generation (NLG) technology allows an attacker to generate masquerade attacks on scale, and study their effectiveness with a within-subjects study. We also gather insights on what parts of an email do users focus on and how users identify attacks in this realm, by planting signals and also by asking them for their reasoning. We find that: (i) 17% of participants could not identify any of the signals that were inserted in emails, and (ii) Participants were unable to perform better than random guessing on these attacks. The insights gathered and the tools and techniques employed could help defenders in: (i) implementing new, customized anti-phishing solutions for Internet users including training next-generation email filters that go beyond vanilla spam filters and capable of addressing masquerade, (ii) more effectively training and upgrading the skills of email users, and (iii) understanding the dynamics of this novel attack and its ability of tricking humans.

5. [Liang 2016]. Nan (Peter) Liang, David P. Biros, and Andy Luse, "An Empirical Validation of Malicious Insider Characteristics", *Journal of Management Information Systems 33*:2, Springer, 2016, pp. 361-392. [Download]

   Abstract: Malicious insiders continue to pose a great threat to organizations. With their knowledge and access to organizational resources, malicious insiders could launch attacks more easily that result in more damaging impacts compared to outsiders. However, empirical research about malicious insiders is rare due to the unavailability of data. With few exceptions, many studies focus on a small number of cases. In order to identify common characteristics of a large number of malicious insiders, this study employs text mining to analyze 133 real-world cases of offenders from military units, intelligence agencies, and business organizations with data available to the public. Contributions of this study reside in two aspects: first, we use public data from documented malicious insider cases, implying a potentially valuable data source for future studies in this domain; second, we validate malicious insider characteristics identified in previous research, thereby establishing a foundation for more comprehensive research in the future.

6. [McReynolds 2017]. Emily McReynolds, Sarah Hubbard, Timothy Lau, Aditya Saraf, Maya Cakmak, and Franziska Roesner, "Toys That Listen: A Study of Parents, Children, and Internet-Connected Toys", in *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (CHI '17)*, 2017, pp. 5197-5207. [Download]

   Abstract: Hello Barbie, CogniToys Dino, and Amazon Echo are part of a new wave of connected toys and gadgets for the home that listen. Unlike the smartphone, these devices are always on, blending into the background until needed. We conducted interviews with parent-child pairs in which they interacted with Hello Barbie and CogniToys Dino, shedding light on children's expectations of the toys' "intelligence" and parents' privacy concerns and expectations for parental controls. We find that children were often unaware that others might be able to hear what was said to the toy, and that some parents draw connections between the toys and similar tools not intended as toys (e.g., Siri, Alexa) with which their children already interact. Our findings illuminate people's mental models and experiences with these emerging technologies and will help inform the future designs of interactive, connected toys and gadgets. We conclude with recommendations for designers and policy makers.

7. [Mehrnezhad 2017]. Maryam Mehrnezhad, Ehsan Toreini, Siamak F. Shahandashti, and Feng Hao, “Stealing PINs via mobile sensors: Actual risk versus user perception”, *International Journal of Information Security*, 2017, pp. 1-23. [Download]

   Abstract: In this paper, we present the actual risks of stealing user PINs by using mobile sensors versus the perceived risks by users. First, we propose PINlogger.js which is a JavaScript-based side channel attack revealing user PINs on an Android mobile phone. In this attack, once the user visits a website controlled by an attacker, the JavaScript code embedded in the web page starts listening to the motion and orientation sensor streams without needing any permission from the user. By analysing these streams, it infers the user's PIN using an artificial neural network. Based on a test set of fifty 4-digit PINs, PINlogger.js is able to correctly identify PINs in the first attempt with a success rate of 74% which increases to 86 and 94% in the second and third attempts, respectively. The high success rates of stealing user PINs on mobile devices via JavaScript indicate a serious threat to user security. With the technical understanding of the information leakage caused by mobile phone sensors, we then study users’ perception of the risks associated with these sensors. We design user studies to measure the general familiarity with different sensors and their functionality, and to investigate how concerned users are about their PIN being discovered by an app that has access to all these sensors. Our studies show that there is significant disparity between the actual and perceived levels of threat with regard to the compromise of the user PIN. We confirm our results by interviewing our participants using two different approaches, within-subject and between-subject, and compare the results. We discuss how this observation, along with other factors, renders many academic and industry solutions ineffective in preventing such side channel attacks.

8. [Twyman 2015]. Nathan W. Twyman, Jeffrey Gainer Proudfoot, Ryan M. Schuetzler, Aaron C. Elkins, and Douglas C. Derrick, “Robustness of Multiple Indicators in Automated Screening Systems for Deception Detection”, *Journal of Management Information Systems 32*: 4, pp. 215-245, 2015. [Download]

   Abstract: This study investigates the effectiveness of an automatic system for detection of deception by individuals with the use of multiple indicators of such potential deception. Deception detection research in the information systems discipline has postulated increased accuracy through a new class of screening systems that automatically conduct interviews and track multiple indicators of deception simultaneously. Understanding the robustness of this new class of systems and the limitations of its theoretical improved performance is important for refinement of the conceptual design. The design science proof-of-concept study presented here implemented and evaluated the robustness of these systems for automated screening for deception detection. A large experiment was used to evaluate the effectiveness of a constructed multiple-indicator system, both under normal conditions and with the presence of common types of countermeasures (mental and physical). The results shed light on the relative strength and robustness of various types of deception indicators within this new context. The findings further suggest the possibility of increased accuracy through the measurement of multiple indicators if classification algorithms can compensate for human attempts to counter effectiveness.

C. Security Science(?)

9. [Herley 2017]. C. Herley and P. C. v. Oorschot, “SoK: Science, Security and the Elusive Goal of Security as a Scientific Pursuit”, in *2017 IEEE Symposium on Security and Privacy (SP)*, May 2017, pp. 99-120. [Download]

   Abstract: The past ten years has seen increasing calls to make security research more “scientific”. On the surface, most agree that this is desirable, given universal recognition of “science” as a positive force. However, we find that there is little clarity on what “scientific” means in the context of computer security research, or consensus on what a “Science of Security” should look like. We selectively review work in the history and philosophy of science and more recent work under the label “Science of Security”. We explore what has been done under the theme of relating science and security, put this in context with historical science, and offer observations and insights we hope may motivate further exploration and guidance. Among our findings are that practices on which the rest of science has reached consensus appear little used or recognized in security, and a pattern of methodological errors continues unaddressed.

D. Software (In)security

10. [Brown 2017]. F. Brown and S. Narayan, R. S. Wahby, D. Engler, R. Jhala, and D. Stefan, “Finding and Preventing Bugs in JavaScript Bindings”, *2017 IEEE Symposium on Security and Privacy (SP)*, May 2017, pp. 559-578. [Download]

    Abstract: JavaScript, like many high-level languages, relies on runtime in low-level C and C++. For example, the Node.js runtime system gives JavaScript code access to the underlying filesystem, networking, and I/O by implementing utility functions in C++. Since C++’s type system, memory model, and execution model differ significantly from JavaScript’s, JavaScript code must call these runtime functions via intermediate binding layer code that translates type, state, and failure between the two languages. Unfortunately, binding code is both hard to avoid and hard to get right.

    This paper describes several types of exploitable errors that binding code creates, and develops both a suite of easily-to-build static checkers to detect such errors and a backwards-compatible, low-overhead API to prevent them. We show that binding flaws are a serious security problem by using our checkers to craft 81 proof-of-concept exploits for security flaws in the binding layers of the Node.js and Chrome, runtime systems that support hundreds of millions of users. As one practical measure of binding bug severity, we were awarded $6,000 in bounties for just two Chrome bug reports.

11. [Gelernter 2017]. N. Gelernter, S. Kalma, B. Magnezi, and H. Porcilan, “The Password Reset MitM Attack”, *2017 IEEE Symposium on Security and Privacy (SP)*, 2017, pp. 251-267. [Download]

    Abstract: We present the password reset MitM (PRMitM) attack and show how it can be used to take over user accounts. The PRMitM attack exploits the similarity of the registration and password reset processes to launch a man in the middle (MitM) attack at the application level. The attacker initiates a password reset process with a website and forwards every challenge to the victim who either wishes to register in the attacking site or to access a particular resource on it. The attack has several variants, including exploitation of a password reset process that relies on the victim's mobile phone, using either SMS or phone call. We evaluated the PRMitM attacks on Google and Facebook users in several experiments, and found that their password reset process is vulnerable to the PRMitM attack. Other websites and some popular mobile applications are vulnerable as well. Although solutions seem trivial in some cases, our experiments show that the straightforward solutions are not as effective as expected. We designed and evaluated two secure password reset processes and evaluated them on users of Google and Facebook. Our results indicate a significant improvement in the security. Since millions of accounts are currently vulnerable to the PRMitM attack, we also present a list of recommendations for implementing and auditing the password reset process.

12. [Holzinger 2016] Philipp Holzinger, Stefan Triller, Alexandre Bartel, and Eric Bodden, "An In-Depth Study of More Than Ten Years of Java Exploitation", Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, ACM, 2016, pp. 779-790. [Download]

    Abstract: When created, the Java platform was among the first run-times designed with security in mind. Yet, numerous Java versions were shown to contain far-reaching vulnerabilities, permitting denial-of-service attacks or even worse allowing intruders to bypass the runtime's sandbox mechanisms, opening the host system up to many kinds of further attacks.

    This paper presents a systematic in-depth study of 87 publicly available Java exploits found in the wild. By collecting, minimizing and categorizing those exploits, we identify their commonalities and root causes, with the goal of determining the weak spots in the Java security architecture and possible countermeasures.

    Our findings reveal that the exploits heavily rely on a set of nine weaknesses, including unauthorized use of restricted classes and confused deputies in combination with caller-sensitive methods. We further show that all attack vectors implemented by the exploits belong to one of three categories: single-step attacks, restricted-class attacks, and information hiding attacks.

    The analysis allows us to propose ideas for improving the security architecture to spawn further research in this area.

13. [Jia 2016] Yaoqi Jia, Zheng Leong Chua, Hong Hu, Shuo Chen, Prateek Saxena, and Zhenkai Liang, "The 'Web/Local Boundary' Is Fuzzy: A Security Study of Chrome's Process-based Sandboxing", *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, ACM, 2016, pp. 791-804. [Download]

    Abstract: Process-based isolation, suggested by several research prototypes, is a cornerstone of modern browser security architectures. Google Chrome is the first commercial browser that adopts this architecture. Unlike several research prototypes, Chrome's process-based design does not isolate different web origins, but primarily promises to protect "the local system" from "the web". However, as billions of users now use web-based cloud services (e.g., Dropbox and Google Drive), which are integrated into the local system, the premise that browsers can effectively isolate the web from the local system has become questionable. In this paper, we argue that, if the process-based isolation disregards the same-origin policy as one of its goals, then its promise of maintaining the “web/local system (local)” separation is doubtful. Specifically, we show that existing memory vulnerabilities in Chrome’s renderer can be used as a stepping-stone to drop executables/scripts in the local file system, install unwanted applications and misuse system sensors. These attacks are purely data-oriented and do not alter any control flow or import foreign code. Thus, such attacks bypass binary-level protection mechanisms, including ASLR and in-memory partitioning. Finally, we discuss various full defenses and present a possible way to mitigate the attacks presented.

E. Hardware (In)security

14. [Guri 2016]. M. Guri, Y. Solewicz, A. Daidakulov, and Y. Elovici, “SPEAKE(a)R: Turn Speakers to Microphones for Fun and Profit”, *arXiv:1611.07350v1 [cs.CR]*, CoRR, 22 November 2016, pp. [Download]

    Abstract: It is possible to manipulate the headphones (or earphones) connected to a computer, silently turning them into a pair of eavesdropping microphones - with software alone. The same is also true for some types of loudspeakers. This paper focuses on this threat in a cyber-security context. We present SPEAKE(a)R, a software that can covertly turn the headphones connected to a PC into a microphone. We present technical background and explain why most of PCs and laptops are susceptible to this type of attack. We examine an attack scenario in which malware can use a computer as an eavesdropping device, even when a microphone is not present, muted, taped, or turned off. We measure the signal quality and the effective distance, and survey the defensive countermeasures.

15. [Roy 2017] A. Roy, N. Memon, and A. Ross, “MasterPrint: Exploring the Vulnerability of Partial Fingerprint-based Authentication Systems”, *IEEE Transactions on Information Forensics and Security 99*: PP, 2017, 13 pp. [Download].

    Abstract: This paper investigates the security of partial fingerprint-based authentication systems, especially when multiple fingerprints of a user are enrolled. A number of consumer electronic devices, such as smartphones, are beginning to incorporate fingerprint sensors for user authentication. The sensors embedded in these devices are generally small and the resulting images are, therefore, limited in size. To compensate for the limited size, these devices often acquire multiple partial impressions of a single finger during enrollment to ensure that at least one of them will successfully match with the image obtained from the user during authentication. Further, in some cases, the user is allowed to enroll multiple fingers, and the impressions pertaining to multiple partial fingers are associated with the same identity (i.e., one user). A user is said to be successfully authenticated if the partial fingerprint obtained during authentication matches any one of the stored templates. This paper investigates the possibility of generating a “MasterPrint”, a synthetic or real partial fingerprint that serendipitously matches one or more of the stored templates for a significant number of users. Our preliminary results on an optical fingerprint dataset and a capacitive fingerprint dataset indicate that it is indeed possible to locate or generate partial fingerprints that can be used to impersonate a large number of users. In this regard, we expose a potential vulnerability of partial fingerprint-based authentication systems, especially when multiple impressions are enrolled per finger.

16. [Katzenbeisser 2012]. Stefan Katzenbeisser, Ünal Kocabaş, Vladimir Rožić, Ahmad-Reza Sadeghi, Ingrid Verbauwhede, and Christian Wachsmann, "PUFs: Myth, Fact or Busted? A Security Evaluation of Physically Unclonable Functions (PUFs) Cast in Silicon", in *Cryptographic Hardware and Embedded Systems (CHES 2012),* LNCS 7428, Springer, 2012, pp. 283-301. [Download]

    Abstract: Physically Unclonable Functions (PUFs) are an emerging technology and have been proposed as central building blocks in a variety of cryptographic protocols and security architectures. However, the security features of PUFs are still under investigation: Evaluation results in the literature are difficult to compare due to varying test conditions, different analysis methods and the fact that representative data sets are publicly unavailable.

    In this paper, we present the first large-scale security analysis of ASIC implementations of the five most popular intrinsic electronic PUF types, including arbiter, ring oscillator, SRAM, flip-flop and latch PUFs. Our analysis is based on PUF data obtained at different operating conditions from 96 ASICs housing multiple PUF instances, which have been manufactured in TSMC 65 nm CMOS technology. In this context, we present an evaluation methodology and quantify the robustness and unpredictability properties of PUFs. Since all PUFs have been implemented in the same ASIC and analyzed with the same evaluation methodology, our results allow for the first time a fair comparison of their properties.

17. [Quarta 2017]. D. Quarta, M. Pogliani, M. Polino, F. Maggi, A. M. Zanchettin, and S. Zanero, An Experimental Security Analysis of an Industrial Robot Controller, *2017 IEEE Symposium on Security and Privacy (SP),* May 2017, pp. 268-286. [Download]

    Abstract: Industrial robots, automated manufacturing, and efficient logistics processes are at the heart of the upcoming fourth industrial revolution. While there are seminal studies on the vulnerabilities of cyber-physical systems in the industry, as of today there has been no systematic analysis of the security of industrial robot controllers. We examine the standard architecture of an industrial robot and analyze a concrete deployment from a systems security standpoint. Then, we propose an attacker model and confront it with the minimal set of requirements that industrial robots should honor: precision in sensing the environment, correctness in execution of control logic, and safety for human operators. Following an experimental and practical approach, we then show how our modeled attacker can subvert such requirements through the exploitation of software vulnerabilities, leading to severe consequences that are unique to the robotics domain. We conclude by discussing safety standards and security challenges in industrial robotics.

F. Privacy

18. Shane Ahern, Simon King, Mor Naaman, and Rahul Nair, "Over-exposed?: Privacy Patterns and *Considerations* in Online and Mobile Photo Sharing", Proceedings of

the SIGCHI Conference on Human Factors in Computing Systems, ACM, 2007, pp. 357-366. [Download]

Abstract: As sharing personal media online becomes easier and widely spread, new privacy concerns emerge – especially when the persistent nature of the media and associated context reveals details about the physical and social context in which the media items were created. In a first-of-its-kind study, we use context-aware camera-phone devices to examine privacy decisions in mobile and online photo sharing. Through data analysis on a corpus of privacy decisions and associated context data from a real-world system, we identify relationships between location of photo capture and photo privacy settings. Our data analysis leads to further questions which we investigate through a set of interviews with 15 users. The interviews reveal common themes in privacy considerations: *security*, *social disclosure*, *identity* and *convenience*. Finally, we highlight several implications and opportunities for design of media sharing applications, including using past privacy patterns to prevent oversights and errors.

19. Yinzhi Cao, Song Li, and Erik Wijmans, "(Cross-)Browser Fingerprinting via OS and Hardware Level Features", *Proc. of Network & Distributed System Security Symposium (NDSS)*, Internet Society, 2017, 15 pp. [Download]

    Abstract: In this paper, we propose a browser fingerprinting technique that can track users not only within a single browser but also across different browsers on the same machine. Specifically, our approach utilizes many novel OS and hardware level features, such as those from graphics cards, CPU, and installed writing scripts. We extract these features by asking browsers to perform tasks that rely on corresponding OS and hardware functionalities.

    Our evaluation shows that our approach can successfully identify 99.24% of users as opposed to 90.84% for state of the art on single-browser fingerprinting against the same dataset. Further, our approach can achieve higher uniqueness rate than the only cross-browser approach in the literature with similar stability.

20. [Doty 2013] Nick Doty and Mohit Gupta, "Privacy Design Patterns and Anti-Patterns: Patterns Misapplied and Unintended Consequences", *A Turn for the Worse: Trustbusters for User Interfaces Workshop (affiliated with SOUPS 2013)*, CyLab Usable Privacy and *Security* Laboratory, Carnegie-Mellon University, 2013. [Download]

    Abstract: One critique of Privacy-by-Design has focused on its lack of concrete guidance for implementation. We have proposed privacy design patterns (drawing from architectural design patterns and object-oriented programming design patterns) as documentation that can be more directly applicable and have established a site to coordinate collaborative development of such patterns. We argue that patterns which define a problem and a solution within a certain context can also help us understand and classify many anti-patterns as patterns misapplied.

    Rather than providing examples of poor or perverse user interface, we examine several design anti-pattern examples, describing: applying a pattern to a different problem; for a different audience; and, with unintended consequences, advantageous and not. With those models, we provide possible directions for how the community should document patterns and anti-patterns to improve future designs.

21. [Mulligan 2016] Deirdre K. Mulligan, Colin Koopman, and Nick Doty, “Privacy is an essentially contested concept: a multi-dimensional analytic for mapping privacy”, *Philosophical* Transactions *of the Royal Society of London A: Mathematical, Physical and Engineering Sciences 374*: 2083, The Royal Society, 2016, 17 pp. [Download]

    Abstract: The meaning of privacy has been much disputed throughout its history in response to wave after wave of new technological capabilities and social configurations. The current round of disputes over privacy fuelled by data science has been a cause of despair for many commentators and a death knell for privacy itself for others. We argue that privacy’s disputes are neither an accidental feature of the concept nor a lamentable condition of its applicability. Privacy is essentially contested. Because it is, privacy is transformable according to changing technological and social conditions. To make productive use of privacy’s essential contestability, we argue for a new approach to privacy research and practical design, focused on the development of conceptual analytics that facilitate dissecting privacy’s multiple uses across multiple contexts.

    This article is part of the themed issue ‘The ethical impact of data science’.

22. [Starov 2017]. Oleksii Starov and Nick Nikiforakis, “XHOUND: Quantifying the Fingerprintability of Browser Extensions, *2017 IEEE Symposium on Security and Privacy (SP)*, IEEE, May 2017, pp. 941-956. [Download]

    Abstract: In recent years, researchers have shown that unwanted web tracking is on the rise, as advertisers are trying to capitalize on users’ online activity, using increasingly intrusive and sophisticated techniques. Among these, browser fingerprinting has received the most attention since it allows trackers to uniquely identify users despite the clearing of cookies and the use of a browser's private mode.

    In this paper, we investigate and quantify the fingerprintability of browser extensions, such as, AdBlock and Ghostery. We show that an extension's organic activity in a page's DOM can be used to infer its presence, and develop XHOUND, the first fully automated system for fingerprinting browser extensions. By applying XHOUND to the 10,000 most popular Google Chrome extensions, we find that a significant fraction of popular browser extensions are fingerprintable and could thus be used to supplement existing fingerprinting methods. Moreover, by surveying the installed extensions of 854 users, we discover that many users tend to install different sets of fingerprintable browser extensions and could thus be uniquely, or near-uniquely identifiable by extension-based fingerprinting. We use XHOUND’s results to build a proof-of-concept extension-fingerprinting script and show that trackers can fingerprint tens of extensions in just a few seconds. Finally, we describe why the fingerprinting of extensions is more intrusive than the fingerprinting of other browser and system properties, and sketch two different approaches towards defending against extension-based fingerprinting.