Specification of Source SLR and Sample
Fidelity of Statistical Reporting in 10 Years of Cyber Security User Studies[*]

Abstract

This specification of source Systematic Literature Review and incorporated sample represents the materials used for the study "Fidelity of Statistical Reporting in 10 Years of Cyber Security User Studies." Appendix A contains a summary of search procedure, inclusion and exclusion phases of the source SLR inputed for said study. Appendix B includes the entire sample with marked exclusions made.

A Underlying Systematic Literature Review

This meta-analytic study is based on a Systematic Literature Review (SLR), which was conducted in 2016/17 for the UK Research Institute in the Science of Cyber Security (RISCS). We adapt this description of the SLR's search from its technical report [1].

A.1 Search Strategy of the SLR Sample

The SLR included security and privacy papers published between 2006 and 2016 (inclusive).

The search was restricted to the following security and privacy venues:

- journals: IEEE Transactions on Dependable & Secure Computing (TDSC), ACM Transactions on Information and System Security (TISSEC),
- flagship security conferences: IEEE S&P, ACM CCS, ESORICS, and PETS or
- specialized conferences and workshops: LASER, SOUPS, USEC and WEIS.

The search was conducted on Google Scholar. Each query extracts articles mentioning "*user study*" and at least one of the words "*experiment*," "*evidence*" or "*evidence based*." The described query was executed for each of the 10 publication venues. In the advanced search option of Google Scholar, each of the following fields were set:

- with all words = *user study*
- at least one of the words = *experiment evidence "evidence based"*
- where my words occur = *anywhere in the article*
- return articles published in = [publication venue]
- return articles dated between = *2006–2016*

The search yielded 1157 publications.

A.2 SLR Inclusion/Exclusion Criteria

We adapt the inclusion/exclusion criteria of the 2017 SLR [1] for this pre-registration. The SLR focused on human factors studies including a human sample. The following *Inclusion Criteria* were ap-

[*]Open Science Framework: `https://osf.io/549qn/`

plied to its overall pool of 1157 publications:

- Studies including a user study with human participants.
- Studies concerned with evidence-based methods or eligible for hypothesis testing and statistical inference.
- Studies that lend themselves to quantitative evaluation, quoting statements of statistical significance, p-values or effect sizes.
- Studies with true experiments, quasi-experiments or observational analysis.

Of the papers included, the ones fulfilling the following *Exclusion Criteria* were excluded:

- Papers that were not subject to research peer-review, key note statements, posters and workshop proposals.
- Position papers or informal arguments.
- Papers not including a study with human participants,
- Theoretical papers.
- Studies with qualitative methodology.

This inclusion/exclusion process yielded a final sample of 146 publications.

B SLR Sample

Table 1: Sample of inputted SLR [1] and this study with marked exclusions (Ex.).

Tag	Tilte	Venue	Year	Ex.
AcqGro2006	Imagined Communities Awareness Information Sharing and Privacy on Facebook	PETS	2006	
AdAcBr2013	Sleights of Privacy Framing disclosures and the limits of transparency	SOUPS	2013	
AfBrGr2012	Detecting Hoaxes Frauds and Deception in Writing Style Online	S&P	2012	
AfCaSt2014	Doppelg”anger Finder Taking Stylometry to the Underground	S&P	2014	
AgShJa2013	Do not embarass Re-examining user concerns for online tracking and advertising	SOUPS	2013	
AhmIss2007	A New Biometric Technology Based on Mouse Dynamics	TDSC	2007	
AkhPor2013	Alice in warningland a large-scale field study of browser security warning effectiveness	USENIX	2013	
AlbMai2015	Evaluating the Effectiveness of Using Hints for Autobiographical Authentication A field Study	SOUPS	2015	
AlFaWr2015	The Impact of Cues and User Interaction on the Memorability of System Assigned Recognition-Based Graphical Passwords	SOUPS	2015	
AlPoRe2014	Your Reputation Precedes You History Reputation and the Chrome Malware Warning	SOUPS	2014	
AngOrt2015	WTH Experiences Reactions and Expectations Related to Online Privacy Panic Situations	SOUPS	2015	
AtBoHe2015	Leading Johnny to Water Designing for Usability and Trust	SOUPS	2015	
BaMaLi2014	The Privacy and Security Behaviors of Smartphone App Developers	USEC	2014	
BeGiKr2015	User Acceptance Factors for Anonymous Credentials	WEIS	2015	
BeLoSi2007	Establishing Darknet Connections An evaluation of Usability and Security	SOUPS	2007	
BelShe2016	Crowdsourcing for Context Regarding Privacy in Beacon Encounters via Contextual Integrity	PETS	2016	
BenRei2013	Should users be informed On risk-perception between Android and iPhone users	SOUPS	2013	
BeWaLi2010	The Impact of Social Navigation on Privacy Policy Configuration	SOUPS	2010	
BiCoIn2015	What the App is That Deception and Countermeasures in the Android User Interface	S&P	2015	
BonSch2014	Towards reliable storage of 56-bit secrets in human memory	USENIX	2014	

Continued on next page

Table 1 – *Sample. Continued from previous page*

Tag	Tilte	Venue	Year	Ex.
BoSaRe2012	Neuroscience Meets Cryptography Designing Crypto Primitives Secure Against Rubber Hose Attacks	USENIX	2012	
BrCrDo2013	Your Attention Please - Designing security-decision UIs to make genuine risks harder to ignore	SOUPS	2013	
BrCrKo2014	Harder to Ignore - Revisiting Pop-up Fatigue and Approaches to Prevent it	SOUPS	2014	
BrGrSt2011	Indirect content privacy surveys - measuring privacy without asking about it	SOUPS	2011	
BruVil2007	Improving Security Decisions with Polymorphic and Audited Dialogs	SOUPS	2007	
BrViDj2008	Evaluating the Usability of Usage Controls in Electronic Collaboration	SOUPS	2008	
BuBeFa2010	How good are Humans at Solving CAPTCHAs - A Large Scale Evaluation	S&P	2010	∅
BuBePa2011	The failure of Noise-Based Non-Continuous Audio Captchas	S&P	2011	
BuWoVo2014	Introducing Precautionary Behavior by Temporal Diversion of Voter Attention from Casting to Verifying their Vote	USEC	2014	
CaMiVa2016	Hidden Voice Commands	USENIX	2016	∅
CaoIve2006	Intentional Access Management - Making Access Control Usage for End-Users	SOUPS	2006	
ChBiOr2007	A second look at the usability of click-based graphical passwords	SOUPS	2007	
ChBoKa2014	On the Effectiveness of Obfuscation Techniques in Online Social Networks	PETS	2014	
ChChBa2015	You shouldnt collect my secrets - Thwarting sensitive keystroke leakage in mobile IME apps	USENIX	2015	
ChMuAs2015	On the impact of touch id on iphone passcodes	SOUPS	2015	
ChObSt2009	Sanitizations slippery slope- the design and study of a text revision assistant	SOUPS	2009	∅
ChPoSe2012	Measuring user confidence in smartphone security and privacy	SOUPS	2012	
ChStFo2012	Persuasive cued click-points - Design implementation and evaluation of a knowledge-based authentication mechanism	TDSC	2012	
CzDeYa2010	Parenting from the pocket - Value tensions and technical directions for secure and private parent-teen mobile safety	SOUPS	2010	
DaKrDa2014	Increasing security sensitivity with social proof - A large-scale experimental confirmation	CCS	2014	
DaPuRa2012	Impact of spam exposure on user engagement	USENIX	2012	
DewKul2006	Aligning usability and security - a usability study of Polaris	SOUPS	2006	

Continued on next page

Table 1 – *Sample. Continued from previous page*

Tag	Tilte	Venue	Year	Ex.
DuHeAs2010	A closer look at recognition-based graphical passwords on mobile devices	SOUPS	2010	
DuNiOl2008	Securing passfaces for description	SOUPS	2008	
EgJaPo2014	Are you ready to lock	CCS	2014	
FaFeSh2015	Anatomization and Protection of Mobile Apps Location Privacy Threats	USENIX	2015	
FaHaAc2013	On the ecological validity of a password study	SOUPS	2013	
FaHaMu2012	Helping Johnny 2.0 to encrypt his Facebook conversations	SOUPS	2012	
FoChOo2008	Improving text passwords through persuasion	SOUPS	2008	
GaCaCo2012	Risk communication design - video vs. text	PETS	2012	
GaCaMa2011	Designing risk communication for older adults	SOUPS	2011	
GaChLi2014	Effective risk communication for android apps	TDSC	2014	
GawFel2006	Password management strategies for online accounts	SOUPS	2006	
GiEgCr2006	Power Streip Prophylactics and Privacy Oh My	SOUPS	2006	
GrCoAl2016	Effect of cognitive depletion on password choice	LASER	2016	
GroBar2014	Social status and the demand for security and privacy	PETS	2014	
HaChDh2008	Use your illusion- secure authentication usable anywhere	SOUPS	2008	∅
HaChHa2009	New directions in multisensory authentication	SOUPS	2009	
HaCrKl2014	Targeted threat index - Characterizing and quantifying politically-motivated targeted malware	USENIX	2014	
HaDeSm2015	Where Have You Been - Using Location-Based Security Questions for Fallback Authentication	SOUPS	2015	
HaRiSt2012	Goldilocks and the two mobile devices - going beyond all-or-nothing access to a devices applications	SOUPS	2012	
HaScWr2014	Applying psychometrics to measure user comfort when constructing a strong password	SOUPS	2014	
HaZeFi2014	Its a hard lock life - A field study of smartphone un-locking behavior and risk perception	SOUPS	2014	
HuMoWa2012	Clickjacking - attacks and defenses	USENIX	2012	
HuOhKi2015	Surpass - System-initiated user-replaceable passwords	CCS	2015	
JaRaBe2014	To authorize or not authorize - helping users review access policies in organizations	SOUPS	2014	
JeSaJe2007	Tracking website data-collection and privacy practices with the iWatch web crawler	SOUPS	2007	
JoEgBe2012	Facebook and privacy - its complicated	SOUPS	2012	
JusAsp2009	Personal choice and challenge questions - a security and usability assessment	SOUPS	2009	
KaBrDa2014	Privacy Attitudes of Mechanical Turk Workers and the US Public	SOUPS	2014	

Continued on next page

Table 1 – *Sample. Continued from previous page*

Tag	Tilte	Venue	Year	Ex.
KaFlRo2010	Two heads are better than one - security and usability of device associations in group scenarios	SOUPS	2010	
KaMaSo2015	Sound-proof - Usable two-factor authentication based on ambient sound	USENIX	2015	
KaTyWa2009	Conditioned-Safe Ceremonies and a User Study of an Application to Web Authentication	SOUPS	2009	
KayTer2010	Textured agreements - re-envisioning electronic consent	SOUPS	2010	
KeBrCr2009	A nutrition label for privacy	SOUPS	2009	
KeCaLi2012	Self-identified experts lost on the interwebs - The importance of treating all results as learning experiences	LASER	2012	
KhHeVo2015	Usability and security perceptions of implicit authentication - Convenient secure sometimes annoying	SOUPS	2015	
KilMax2012	Free vs. transcribed text for keystroke-dynamics evaluations	LASER	2012	
KluZan2009	Balancing usability and security in a video CAPTCHA	SOUPS	2009	∅
KorBoh2014	Too Much Choice - End-User Privacy Decisions in the Context of Choice Proliferation	SOUPS	2014	
KoShCr2014	Telepathwords - Preventing weak passwords by reading users minds	SOUPS	2014	
KoSoTs2009	Serial hook-ups - a comparative usability study of secure device pairing methods	SOUPS	2009	
KrHuHo2016	Use the Force- Evaluating Force-Sensitive Authentication for Mobile Devices	SOUPS	2016	
KuCrAc2009	School of phish - a real-world evaluation of anti-phishing training	SOUPS	2009	∅
KuRoCr2006	Human selection of mnemonic phrase-based passwords	SOUPS	2006	
LeMoPe2016	Privacy Challenges in the Quantified Self Movement - An EU Perspective	PETS	2016	
LiAnSc2016	Follow my recommendations - A personalized privacy assistant for mobile app permissions	SOUPS	2016	
LiAsCa2008	Risk communication in security using mental models	USEC	2008	
LiBrYe2011	Demographic Profiling from MMOG Gameplay	PETS	2011	
LiLiSa2014	Modeling users' mobile app privacy preferences - Restoring usability in a sea of permission settings	SOUPS	2014	
LiXiPe2011	Smartening the crowds- computational techniques for improving human verification to fight phishing scams	SOUPS	2011	
LlPoAt2015	Face-off - Preventing Privacy Leakage From Photos in Social Networks	CCS	2015	

Continued on next page

Table 1 – *Sample. Continued from previous page*

Tag	Tilte	Venue	Year	Ex.
MaDeKe2011	Using data type based security alert dialogs to raise online security awareness	SOUPS	2011	
MaLeAd2012	The PViz comprehension tool for social network privacy settings	SOUPS	2012	
MalPre2013	Sign-up or give-up- Exploring user drop-out in web service registration	SOUPS	2013	
MoGaSa2014	Dynamic cognitive game captcha usability and detection of streaming-based farming	USEC	2014	
MohaBe2010	Do windows users follow the principle of least privilege - investigating user account control practices	SOUPS	2010	
MoLiVi2014	Understanding and specifying social access control lists	SOUPS	2014	
NoBlCa2014	Why Johnny Cant Blow the Whistle - Identifying and Reducing Usability Issues in Anonymity Systems	USEC	2014	
PanCut2010	Usably secure low-cost authentication for mobile banking	SOUPS	2010	
PaNoKa2012	Reasons rewards regrets - privacy considerations in location sharing as an interactive practice	SOUPS	2012	
PanPra2014	Crowdsourcing attacks on biometric systems	SOUPS	2014	∅
PeKoBu2014	Cloak and swagger - Understanding data sensitivity through the lens of user anonymity	S&P	2014	
PoHaEg2012	Android permissions - User attention comprehension and behavior	SOUPS	2012	
PoIlMa2014	Faces in the distorting mirror- Revisiting photo-based social authentication	CCS	2014	
PuGros2015	Towards a Model on the Factors Influencing Social App Users Valuation of Interdependent Privacy	PETS	2015	
RaBoJa2014	To befriend or not - a model of friend request acceptance on facebook	SOUPS	2014	
RaDeGr2016	Privacy Wedges- Area-Based Audience Selection for Social Network Posts	SOUPS	2016	
Rader2014	Awareness of Behavioral Tracking and Information Privacy Concern in Facebook and Google	SOUPS	2014	
RaHaBe2009	Revealing hidden context- improving mental models of personal firewall users	SOUPS	2009	
RajCam2016	Influence of Privacy Attitude and Privacy Cue Framing on Android App Choices	SOUPS	2016	
RaWaBr2012	Stories as informal lessons about security	SOUPS	2012	
ReKrMa2016	How I Learned to be Secure- a Census-Representative Survey of Security Advice Sources and Behavior	CCS2016		

Continued on next page

Table 1 – *Sample. Continued from previous page*

Tag	Tilte	Venue	Year	Ex.
RiBoMo2016	Measuring the influence of perceived cybercrime risk on online service avoidance	TDSC	2016	
RiQiSt2012	Progressive authentication- deciding when to authenticate on mobile phones	USENIX	2012	∅
RoCuJo2014	Behavioral Experiments Exploring Victims Response to Cyber-based Financial Fraud and Identity Theft Scenario Simulations	SOUPS	2014	
RuKiBu2013	Confused Johnny- when automatic encryption leads to confusion and mistakes	SOUPS	2013	
RuOnYo2016	User Attitudes Toward the Inspection of Encrypted Traffic	SOUPS	2016	
SchBon2015	Learning assigned secrets for unlocking mobile devices	SOUPS	2015	
SchRee2009	1 plus 1 equal you- measuring the comprehensibility of metaphors for configuring backup authentication	SOUPS	2009	
ScMcPa2011	Empowering end users to confine their own applications - The results of a usability study comparing SELinux AppArmor and FBAC-LSM	TISSEC	2011	
ScWaKo2013	Exploring the design space of graphical passwords on smartphones	SOUPS	2013	
ShBeRo2016	Behavioral Study of Users When Interacting with Active Honeytokens	TISSEC	2016	
ShKeKo2012	Correct horse battery staple- Exploring the usability of system-assigned passphrases	SOUPS	2012	
ShKoDu2016	Designing Password Policies for Strength and Usability	TISSEC	2016	
ShKoKe2010	Encountering stronger password requirements-user attitudes and behaviors	SOUPS	2010	
ShKrVi2015	Portrait of a Privacy Invasion	PETS	2015	∅
ShKuSe2014	Beware your hands reveal your secrets	CCS	2014	∅
ShMaKo2007	Anti-phishing phil- the design and evaluation of a game that teaches people not to fall for phish	SOUPS	2007	
SmeGoo2009	How users use access control	SOUPS	2009	∅
StHuBr2012	Are privacy concerns a turn-off- engagement and privacy in social networks	SOUPS	2012	
StoBid2013	Memory retrieval and graphical passwords	SOUPS	2013	
SuEgAl2009	Crying Wolf - An Empirical Study of SSL Warning Effectiveness	USENIX	2009	
TaOzHo2006	A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords	SOUPS	2006	
ThLiCh2016	What Questions Remain - An Examination of How Developers Understand an Interactive Static Analysis Tool	SOUPS	2016	∅
UrKeKo2012	How does your password measure up - the effect of strength meters on password creation	USENIX	2012	

Continued on next page

Table 1 – *Sample. Continued from previous page*

Tag	Tilte	Venue	Year	Ex.
VItak2015	Balancing privacy concerns and impression management strategies on Facebook	SOUPS	2015	
WaGeCh2016	On the Security and Usability of Segment-based Visual Cryptographic Authentication Protocols	CCS	2016	
WaRaBe2016	Understanding Password Choices - How Frequently Entered Passwords are Re-used Across Websites	SOUPS	2016	
WrPaBi2012	Do you see your password- applying recognition to textual passwords	SOUPS	2012	
WuMiLi2006	Web wallet- preventing phishing attacks by revealing user intentions	SOUPS	2006	
XuReCh2012	Security and usability challenges of moving-object CAPTCHAs- decoding codewords in motion	USENIX	2012	
YaLiCh2016	An Empirical Study of Mnemonic Sentence-based Password Generation Strategies	CCS	2016	
YeHeOp2014	An epidemiological study of malware encounters in a large enterprise	CCS	2014	
ZhPaWa2016	An Efficient User Verification System Using Angle-Based Mouse Movement Biometrics	TISSEC	2016	∅
ZhWaJi2014	Privacy Concerns in Online Recommender Systems- Influences of Control and User Data Input	SOUPS	2014	

References

[1] K. Coopamootoo and T. Groß. Systematic evaluation for evidence-based methods in cyber security. Technical Report TR-1528, Newcastle University, 2017.