AVANT-PROPOS

A Social Science Perspective of Trust and Cyber Security

We depend on computers increasingly, often not appreciating how much we do so. For example, in the era before mobile phones, many people wore wristwatches. Anecdotal evidence suggests that younger people today are less likely to wear conventional wristwatches than their older peers: first the pager, then the mobile phone and now the smartwatch is the preferred device for telling time. The old-fashioned watch simply told time; the new technology may have motion sensors, a digital personal assistant, the ability to connect with nearby devices (such as headphones) *via* Bluetooth, and near field communication (NFC) technology to support payments using a credit or debit card. With apps, smart watches can play music, display messages, record audio, check in for flights or hotels, show maps and directions, and monitor health and fitness. Oh yes: they report the time, too.

These impressive and seemingly unlimited capabilities come with a downside, however. Whether using a smart watch, smartphone or other feature-rich electronic device, users are exposed to security and privacy risks not faced with simpler mechanical tools. The Bluetooth and NFC communications can pair with any wireless receiver that is close enough, so the smart device can be asked to exchange data with unknown or unexpected access points. The apps can potentially access any data or capabilities on the device, even those completely unrelated to the service the app is purportedly providing. For example, a music player could also record conversation, or an exercise coach could export the user's to-do list to another device. Recognizing that a user is on a trip, a calendar app could notify criminals that the user's house is likely to be empty and thus a burglary target. Most users have no idea what activities their devices are performing, let alone how to limit an activity. We trust these devices and their software not to exceed our expectations of functionality, but rarely are any limits specified. Rarer still are controls that the user can employ to govern the functionality in some way. More importantly, the appeal of new functionality leads users to ignore caution.

The Meaning of Trust

Here, trust is essential to the way we purchase and use technology. So let us consider carefully what we mean by "trust." We use the word in many ways. For instance, you trust a friend to use your house key. Or you trust the government to carry out administrative and judicial functions fairly. Or you trust a bridge to support your weight, or a web site to deliver accurate information. The *Merriam-Webster*

Dictionary defines trust in several ways, depending on the context of its use. The one most appropriate for technological use is this one: Trust is the *assured reliance on the character, ability, strength, or truth of someone or something.*

Assurance is fundamental to this definition: trust is not based on a whim or a belief; rather, it requires a foundation. You trust your friend with your house key because you have known the friend for some time and have seen evidence of the friend's honesty or character; the trust is based on the foundation of friendship and experience. A stranger has neither that standing relationship nor the evidence from experience, so you would probably not give the stranger your key. Even courts, when making a determination of guilt or innocence, accompany their rulings with a rationale; if people do not like the result, they can follow the chain of legal reasoning from which the judgments came, to convince themselves that the courts ruled fairly. Similarly, civil engineers must pass certification examinations, and governments establish safety standards for bridge design, so you can trust both the ability of the designer and strength of the design. In the same way, prior postings and citations confer credibility on the content of a web site. All these situations show that trust requires a solid footing.

Do the entities forming the trust matter? People trust other people, people trust animals (such as guide dogs for the blind), and people trust machines, data and software. Although the context is different, the basis for the trust is similar in all these cases: a giver of trust (known as the truster), a receiver of trust (known as the trustee), and the trust relationship.

We next want to know how the trust relationship is developed: why does a truster trust a trustee or how can a trustee obtain trust from a truster. Aristotle (*Rhetorica*, 1380) posed that trust comprises three determinants: good sense (knowledge and expertise), good moral character (virtue and goodness), and goodwill (benevolence), meaning that a truster is looking for these three properties in a potential trustee. Aristotle meant his principles to apply to a speaker trying to develop the trust of the audience, other humans. In other situations, specifically electronic interaction, trust depends on factors such as

– What is at risk: access to a room, a fixed sum of money, life savings, proprietary data, reputation.

– For what period of time: a single online session, a month, between fixed dates, indefinitely.

– For what uses or actions: to read, copy, modify or delete data; represent a position in court; perform medical tests; transfer funds electronically.

– On what evidence: testing, past experience, experience over a long period of time, credentials, product guarantees, recommendations – from friends, friends of friends, trusted third parties or anonymous reviewers, well-known brand name, under contract with a respected company that has an important reputation or significant assets at stake.

– Verified by what standard: by law or regulation, self-defined criteria, principles of a recognized body, individual (*ad hoc*) assessment, unsupported assertion.

– In what context: on a secure web site, via an encrypted connection, on a public computer or public network, face-to-face, under protective laws (for example, limiting the risk of fraudulent credit card use or mandating the privacy of medical data).

– With the truster in what state: relaxed, pressed for time, overextended on trust, transparent (where the motive, limitations or method of the other party is apparent).

– Under what instinct: feeling, intuition or emotion; comfort; personal connection; peer pressure; sense of foreboding; perception of security or privacy; physical appearance.

These characteristics illustrate that assessing and establishing trust depends on both objective and subjective criteria, and that there are many components that affect a trust relationship. As such, trust is a complicated issue to automate, because these criteria reflect the kinds of judgments humans make, rationally or irrationally. Castelfranco (2006) studied trust not from the perspective of the truster deciding to trust someone or something, but of the trustee. That work asserts that the trustee develops capital, roughly described as credibility, that can be built, managed and saved. Such trust represents power that a trustee can use strategically to achieve certain goals.

Measuring Trust

Online systems sometimes collect and publish trust factors that allow users to form their own assessments of trust. For example, eBay implements a reputation system in which seller and buyer rate each other, and future sellers and buyers can consider those cumulative ratings to decide whether to engage in a transaction. Online discussion boards and online dating sites use similar methods. The parties using them are building and "spending" their trust capital. To understand the impacts of such systems and whether they establish real trust, we need to analyze the individual components: who or what are the trusters, who or what are the trustees, how the relationship is established, how an initial level of trust is established, how the level of trust increases or decreases, and so on. Because these components usually involve people as truster, trustee or both, we need to look at the human factors that cause the trust to change over time. No formula or device determines how much an individual will trust a web site, for example; the human reaction is nuanced and not necessarily predictable. However, the study of human response, as done by psychologists and sociologists, reveals factors that may affect how a trust relationship evolves.

Several researchers have defined a calculus of trust, in an attempt to quantify and formalize the changes of a trust relationship. For example, Huang and Nicol (2010) defined a calculus of trust, using formal semantics and predicate logic to represent

aspects of the trust relationship. Within that framework the authors can model belief, confidence and risk, and derive certain conclusions regarding propagation of trust.

In a different use of the concept of calculus of trust, Dawes (2003) studied trust in government projects, ones in which the government was moving to private (non-government) parties providing services that previously had been done by government agencies; examples included both services under contract and public–private partnerships. Dawes identified three bases for trust: calculus-based, identity-based or institution-based. Calculus-based trust rests on information-based rational decisions about the trustee. Identity-based trust depends on familiarity and history among the participants. Institution-based trust relies on social structures and norms, such as laws and contracts, that define and limit acceptable behavior. Dawes recognizes that unquantifiable human judgment plays a role in decisions of trust.

One way a trust relationship grows involves persuasion, in which a trustee tries to persuade a truster to trust. Social science research into persuasion shows that consensus (following others) and authority (respect for people of greater knowledge, position or experience) are strong persuaders (Cialdini, 2001). Thus ratings systems ("this product gets a 4.7 out of 5.0 rating based on 23 reviews") use the powerful motivators of persuasion because the truster is conforming to the views of others who have more knowledge (having bought and used the product). But these same social science observations also give us the key to subverting ratings systems: Someone wanting to rise in a trust ranking could focus on building followers who praise the trustee's expertise. The fact that people corrupt online rating systems by getting friends to write glowing reviews could have been foreseen by a review of the psychology literature about trust. Critical readers ask who the 23 previous reviewers are and what bias they might have had, but gullible purchasers are persuaded to follow the lead of others.

Extending Trust

In human interaction, trust is not necessarily reciprocal: That person A trusts person B does not always imply that B trusts A or to a similar degree. However, sharing and experience can increase the level of trust between two individuals, especially over time. Trust among humans is also not necessarily transitive: if A trusts B and B trusts C, it does not always follow that A trusts C, although A's trust of B may increase A's willingness to trust C. (A friend's recommendation can influence your choice of a new doctor, for example.)

These properties can lead to difficulties in an electronic situation. Web sites frequently link to other sites and obtain content from several servers and sources. The site a user accesses has one URL displayed in the address bar, but individual pieces of content come from other locations, so users may not (or should not) trust all content on the page equally. However, most users are not discerning enough to distinguish among sources of different pieces of information on the page, especially when these pieces include graphics, activity trackers, and fetch-and-store operations

on databases. Thus, undeserved trust can affect users' security and privacy. And technology makes it more difficult for a user to decide whether someone or something deserves trust: Technologists have obscured the details (e.g. the origin of web page content) by which users would ordinarily judge the credibility of what they see.

An important way to learn these details is through knowledge sharing and transfer. Arduin *et al*. (2015) examined how people transfer knowledge and form shared, cooperative relationships. Their work, grounded in Nonaka's principles (1998), studies social structures (individuals, groups, organizations) and the transitions between tacit knowledge (personal, individual feelings and interpretations) and explicit knowledge (shared concepts). As individuals interact and share, they develop common understandings that then lead to group and organizational systems of explicit knowledge. Next, people in the organizations use the knowledge, leading to more individual experiences that grow tacit knowledge again. The cycle from individual to group to organization and back to individual, and from individual to shared knowledge, repeats as a spiral. Arduin and colleagues point out that humans are an essential part of an information system, because they, as users, process the information and convert it to knowledge to perform some task or achieve some result. Thus, web page users should be informed of the source of content on the page so they can properly assess the truth and usefulness of the content.

Trust and Technology

A particular aspect of trust involves people trusting technology. What factors affect the degree to which we trust technology? When is it appropriate to trust what technology is doing for (or to) us? Or, as with dangerous machinery such as radiotherapy machines or medical devices, when should we trust claims of safety or effectiveness? Again, we seek evidence, assurance and transparency. Since most technology is delivered to the user as an opaque object from unspecified background, providing this information can be difficult. Moreover, the instructions may describe what the device does but still may fail to meet its stated claims. But to enhance trust, such shortcomings, which tend to be apparent to testers and user, can be documented by the producer or user groups.

Security for computer programs also involves a more elusive requirement, "and nothing more": The code must not do other things the user does not need or want. If an app ostensibly provides driving directions, it should not also export email contacts to a public site. Code that collects and publishes data from home security cameras to enable remote monitoring should provide such video streams only to the user's smartphone (or other authorized devices); data should not also go to the manufacturer (unless with permission). However, it is more often the case that devices take actions while the user is generally unaware of what is really happening.

For example, if the ride-hailing company Über identifies customers as potential law enforcement personnel who might try to limit or block Über's operation in a city, its app sends the customer misleading information (Isaac, 2017). The social networking app Path paid a fine in 2013 for having illegally collected users' contacts without their permission (FTC, 2013). In these examples, the apps took actions unknown to and thus unapproved by their users. Program developers often request permission to access data unrelated to the purpose of the application; for example, a flashlight app may request access to the user's location. How can a user to develop trust in a product when the user cannot reliably know what the product is doing?

Smartphone users can choose from a huge array of apps, often free or of low price. But how do users decide which apps to install? Trust properties such as reputation of producer and potential risk of use can guide users in prudent selection. And social science work shows how to induce people to make these wise choices.

The Need for Psychosocial Underpinnings

Because human factors affect trust, research in psychology and sociology should augment technological advances to derive well-grounded results. The need for a combined approach is apparent when considering the efficacy of security devices. Technologists' traditional approach has been to constrain the user by encouraging "good" behavior while discouraging or preventing "bad" behavior. But this approach is flawed. For example, requiring complex passwords (including upper and lower case letters, numerals, and special characters) can frustrate users, causing them to revert to simpler forms that are easy to remember but also easy to guess, such as Pa$$w0rd. Or, faced with a system that prohibits reusing any of the five most recently used passwords, users have been known to go through six password changes at a time to get back to the favorite first password.

Similarly, Bélanger *et al.* at Virginia Tech (2011) studied the "resistance behavior" exhibited when people are faced with a mandatory password change. Many of the several hundred study respondents were slow to change passwords when advised to, because the users found that changing was an unwanted interruption of more important tasks. Adams and Sasse (1999) pointed out more than a decade earlier that users concentrate on performing their primary tasks, well known from psychologists' study of cognition; as a consequence, users view security as a disruptive secondary effort and withdraw from it mentally in order to maintain focus on their main emphasis.

Recent studies suggest that blending psychology theory with security can lead to effective results. For example, in U.K schools teaching online safety,

"Where the provision for e-safety was outstanding, the schools had managed rather than locked down systems. In the best practice seen, pupils were helped, from a very early age, to assess the risk of accessing sites and therefore gradually to acquire skills which would help them adopt safe practices even when they were not supervised." (Ofsted, 2010, p. 8).

In other words, explaining security risks and then trusting users to behave responsibly led to more secure outcomes. Bringing users into the system and empowering them as respected partners paid important dividends.

Caputo and Pfleeger (2012) have investigated many areas where taking a psychosocial approach to cyber security can lead to more secure behavior and outcomes. They point out that, "if humans using computer systems are given the tools and information they need, taught the meaning of responsible use, and then trusted to behave appropriately with respect to cyber security, desired outcomes may be obtained without security's being perceived as onerous or burdensome" (p. 598). In other words, "By both understanding the role of human behavior and leveraging behavioral science findings, the designers, developers and maintainers of information infrastructure can address real and perceived obstacles to productivity and provide more effective security" (Pfleeger and Caputo, 2012, p. 598).

Other researchers have applied social science methods to security and privacy. Acquisti *et al.* have developed a rich body of work on privacy based on behavioral economics: how and to what extent people value their privacy, and Anthony used sociological research approaches to explore privacy of medical data. Caputo used expertise in behavioral psychology to understand the nature of insider threats to computing systems and the effectiveness of spear-phishing attacks. Pfleeger and Sasse took a social psychology approach to the study of users' security behavior. In these and other bodies of work, researchers successfully joined cyber security fundamentals with social science perspectives to develop new approaches and better understanding.

Next Steps

Because computer security and privacy involve humans and their activities, technologists must learn from behavioral scientists to improve the design, development and use of technology. Similar methods can also be used to explore trust: between individual truster and trustee, in teams, among user communities, in networks, and throughout populations. We need to understand what motivates people to trust, how people gain and lose trust, what data and criteria affect the development of trust and how to present such data to users, and why people can be fooled into trusting that which they should not.

This special issue contains much-needed papers that explore the relationship between trust and computer security and privacy. But clearly more such work is required. By viewing security and privacy through the lens of trust we open up not only ways to incorporate human perspectives but also ways to identify choke points that need to be addressed both by technology and people.

Bibliography

Adams A. and Sasse M. A. (1999). Users are not the enemy. *Communications of the ACM*, 42, p. 40-46.

Arduin P.-E., Grundstein M., Sabroux, C. Rosenthal (2015). *Information and Knowledge System*. Wiley.

Bélanger F., Collignon S., Enget K., Negangard E. (2011). User resistance to mandatory security implementation. *Proceedings of the 2011 Dewald Roode Workshop on Information Systems Security Research, IFIP WG8.11/WG11.13*, paper 5, available at http://ifip.byu.edu/ifip2011.html.

Castelfranchi C., Falcone, R., Marzo F. (2006). Being Trusted in a Social Network: Trust as Relational Capital. *iTrust'06, Proceedings of the Fourth International Conference on Trust Management*, 16-19 May, Pisa, p. 19-32.

Cialdin R. B. (2001). *Influence: Science and practice* (4th Ed.), Boston: Allyn & Bacon.

Dawes S. (2003). The role of trust in new models of collaboration. University of Albany, NY: Center for Technology in Government.

FTC [U.S. Federal Trade Commission] (2013). *Path Social Networking App Settles FTC Charges it Deceived Consumers and Improperly Collected Personal Information from Users' Mobile Address Books*. Press release, 1 February.

Huang J. and Nicol D. (2010). A Formal-Semantics-Based Calculus of Trust. *Internet Computing* vol. 14, n° 5, p. 38-46.

Isaac M. (2017). How Über Deceives the Authorities Worldwide. *New York Times*, 3 March.

Nonaka I. and Konno N. (1998). The Concept of 'Ba': Building a Foundation for Knowledge Creation. *California Management Review*, vol. 40, n° 3, Spring, p. 40-54.

Ofsted [U.K. Office for Standards in Education, Children's Services and Skills] (2010). The safe use of new technologies (Report 090231). Manchester, UK: Ofsted.

Pfleeger S. L. and Caputo D. D. (2012). Leveraging behavioral science to mitigate cybersecurity risk. *Computers and Security*, 31, p. 597-611.

Sasse M. A. and Flechais I. (2005). Usable security: why do we need it? How do we get it? *Security and Usability*, L. F. Cranor and S. Garfinkel, (Eds.), Sebastopol, CA: O'Reilly Publishing, p. 13-30.

Charles P. PFLEEGER
Shari Lawrence PFLEEGER
Pfleeger Consulting Group, Washington, DC