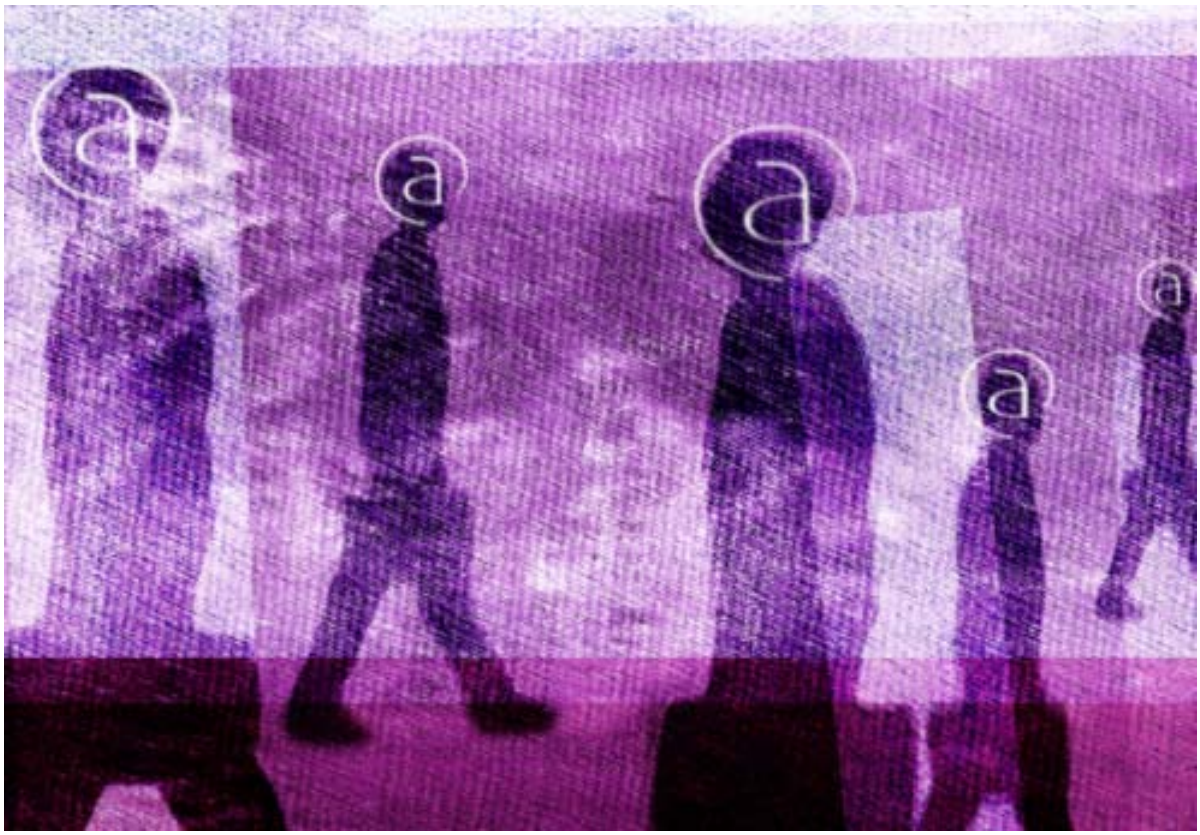
Center for Technology Innovation at BROOKINGS

January 11, 2011



Hannah Gal

Online Identity and Consumer Trust: Assessing Online Risk

Allan Friedman, Patrick Crowley, and Darrell West

Allan A. Friedman is research director of the Center for Technology Innovation at Brookings. He is also a fellow in Governance Studies.

Patrick Crowley is associate professor in the Department of Computer Science and Engineering at Washington University in St. Louis.

Darrell M. West is the founding director of the Center for Technology Innovation at Brookings. He is also vice president and director of Governance Studies and a senior fellow.

As the Internet continues to evolve into a more social and interactive space, new threats to online consumers emerge. Beyond the now commonplace malware, these threats target the relationship between online services and consumers by attacking the core of their relationship: identity. While consumers are increasingly aware of online dangers, they must be able to trust the idea of an interactive Internet to support the transformations possible through web services.

Trust is paramount. The Department of Commerce recently solicited input on online innovation, and respondents from a wide range of industries and ideological agendas continually returned to the idea that consumer trust is critical for the continued growth of e-commerce and online expression (IPTF, 2010).

This report highlights the importance of identity as a principle theme in the next five years of the growth of the Web. The identity mechanisms that allow users to exist as individuals on the web are under attack, exposing consumers to potential privacy invasion and real risks of identity fraud. We outline many of these risks, highlighting several emerging threats to online trust relationships, and explain the technical details in a policy context. By understanding the technology and the roles and incentives of each party, we can offer several policy recommendations to promote consumer trust without restricting innovation.

Identity Online

Identity on the web plays the critical role of differentiating between different entities. A full technical discussion of digital identity is beyond the scope of this report. The National Academy's 2002 study serves as an excellent theoretical introduction (Kent & Millet, 2002). Simply put, it serves to treat different people differently. Some interactive mechanism is needed to allow recognition of some individual properties so that web sites can deliver customized content, and databases can offer different sets of data to different users. Identity allows individuals to have a personal context in an online sphere that encompasses the whole globe. Over two thirds of the global top 100 web sites use some sort of digital identity system (Zhou and Evans, 2010).

There are several key concepts in any discussion of online identity. "Identity" has many different connotations in different fields, and even in information systems, there is some ambiguity. The National Academies 2002 report begins with the assumption that identity is relative to a context: "the identity of X relative to Y" (Kent and Millet, 2002) while NIST declares that a person has exactly one identity (MacGregor et al, 2006). This distinction aside, online identity mechanisms follow a basic model. An entity asserts that it is tied to a specific identity by presenting a set of *credentials.* The most common credentials are a username and password. The process of confirming and verifying the claimed identity is referred to as *authentication. Authorization* is a separate process, when the entity is given access to some part of the online system.

The classic means of authentication are the use of "Something you know, something you have, or something you are." While this can encompass cryptographically generated one-time passwords, sophisticated smart cards or biometrics, these technologies are expensive to deploy and even more expensive to effectively manage. Most web sites use the now-familiar password, something that is ostensibly known only to the user and the web service.

Passwords place the smallest initial burden on both parties to initially form a trusted relationship. They are, however, a serious weak link in the chain of trust. Users have been shown to be bad at devising passwords robust against guessing. They reuse them across domains, so that if one web server has been compromised, an attacker can take advantage of an entity's identity across multiple sites.

Passwords serve as a basis of trust, but trust requires an infrastructure for delegation and transfer. The most basic model of trust is simply the user trusting the website. This classic model reflects the human model of trust, but does not work for the complex online world, where much of the transaction is hidden (Camp, 2007). In between the user and the service provider lie a number of technical and organizational layers: the browser, the Internet service provider, and the standards and systems ensuring interoperability.

These layers have different models of trust, some stronger than others. The certificate management system used to trust digital certificates for the secure exchange of information via SSL/TLS uses a monolithic system of trust through association. There is a large set of Certificate Authorities from whom a web site can obtain a certificate used for these secure transactions. The web browser will automatically only engage in a secure connection with a web browser if the web site's certificate is approved by the one of the established set of Certificate Authorities. Recent work by Roosa and Schultze (2010) highlights the key flaw in this trust model: users have no way of differentiating between Certificate Authorities, and there is increasing evidence that some are not trustworthy at all.

An alternative model of trust is the tree-like model of delegated trust used in the Secure Domain Name System. Here, an authoritative root is automatically trusted. Each top level domain must reliably verify itself to the root, verifying its identity. Each layer down must authenticate with its parent in the tree. This parent has responsibility for that subdomain, and has the incentives to create a trustworthy environment. There is thus a chain of trust from a single trusted root down to the final entity.

The Expanding Role of Identity

As systems have developed, the importance of identity has expanded. Interactive web sites and user-generated content increase the importance of the individual on the Internet. Customization allows for a more personalized experience. Social media expands the zone of identity outside the boundaries of specific web sites to encompass all content on the web. Innovative collaborations

between firms require the sharing of identity information across technical and organizational boundaries.

Businesses have had to expand the role of identity systems and manage change across converging domains due to increasing organizational streamlining and technical consolidation. Consumers use identity mechanisms to access resources they see as under their own control, in the care of a third party provider. One's email on a website is still one's email. Users have had to manage growth across more and more distinct domains, each with their idiosyncrasies. Interestingly, the public sector faces both these challenges in the transition to e-government. Internally, stovepipes have had to be torn down, and systems coerced into interoperating. At the same time, the citizen-facing functionality has proliferated, and both managers and citizens have had to deal with greater complexity.

Risks from a Compromised Identity

An attack on an online identity can lead to real harms. While online services spend a great deal securing their systems, breaching the identity mechanisms can expose the whole value of the system. The financial sector is an attractive target, since compromise might allow an attacker to remove funds. Losing the keys to systems that safeguard sensitive information such as medical data can have substaintial consequences for many.

The risk in the identity mechanisms of the web is that credentials serve as keys to all the value held inside the systems. A social security number may be a unique identifier for all Americans, but it is also widely used as an authenticating secret, something that – it is assumed – only the individual knows and can therefore be used to verify the their identities as well. Moreover, risks spill across systems. When a popular social media website was attacked and the passwords of its users were compromised, experts warned that many users would use these passwords for other sites. Several other sites pre-emptively reset their own customers' passwords to mitigate the risk (Pegoraro, 2010). This concentration of value makes identity information an attractive target.

Attacks on Online Identity

Trust online can be eroded by a wide range of threats, targeting the user's privacy or property. These threats can come from one of many different components in the online ecosystem. Below we characterize four different attack vectors that explicitly target the relationship that consumers have with web services. Each exploits a different side of the consumer's online experience.

Online Surveillance

A recent academic survey reported that most Americans were uncomfortable with

the idea of being closely tracked on the web, particularly across different web sites. Less than one quarter of respondents said it would be "OK" for a website to use information about what they did on other web sites, even to offer them a discount (Turow et al, 2009). This reflects a key component of trust: a separation of contexts so that activities in domains that are perceived to be unrelated do not affect each other. Unfortunately, it is very possible to track users as they move across the web in a number of different ways. Cookies, small tokens that are stored in the web browser, can track users across different web sites. Under certain conditions, a cookie that is set by an advertisement on one website can be read by a second web site's ads, allowing the advertiser to know that the user visited both sites.

There are more sophisticated ways of tracking user behavior across the Internet. Because most individuals have slightly different configurations on their computers, when you consider the combination of OS and browser version along with the specific version of installed browser plugins, a user may be recognized by the unique fingerprint left in the way their computer interacts with the web server. Thus, a user who has tried to establish separate identities by, say, rejecting cookies, could still be identifiable. A recent study showed that 94 percent of browsers with common features, such as Flash and Java, are uniquely identifiable in a very large sample, with a very high likelihood of being trackable over time (Eckersley, 2010). Browser fingerprints are a form of identifier that can be correlated with other identifiers and user behavior without the user's knowledge. This enables a very robust form of tracking online, even if the user has specifically taken action to avoid being tracked by disabling cookies or using a browser's private mode.

One's browser history is also open to a form of surveillance. In an attack known as "history sniffing" a website can learn whether the user has visited an arbitrary list of online resources. The attack works due to a browser specification that displays links to visited URLs differently. A website can query the browser to learn whether a link will be displayed as visited, ostensibly to allow more control over how to render the web page. However, an unscrupulous website can send a series of invisible queries to the user's browser to learn a great deal about that user's past web browsing habits if they happened to ask about the right links. A recent study demonstrated that it was possible to detect as many as 30,000 links per second (Janc and Olejnik, 2010). The researchers also found that this attack works even if the user is using security-enhancing plugins. A UCSD research team discovered 46 of the top 50,000 web sites engaging in this behavior (Jang et al, 2010). One of them was a pornographic website that has since been sued (Shankland, 2010).

Local Network Threats

When communicating via a wireline, it is intuitive to most that the data traffic is leaving the computer through a data cord to an interface that connects with the Internet Service Provider. Users have an established relationship with the service

provider, and a reasonable understanding of the physical integrity of the cables, if not the information systems. It is quite difficult for a typical cyber criminal to intercept data on a broadband or telephone-modem cable that he had not physically tapped. The same cannot be said of wireless network communications. Malicious actors can learn a great deal from unencrypted Wi-Fi links in their vicinity.

First, if the wireless connection is not itself encrypted using a modern standard (i.e. WPA2), then any nearby attacker can listen to all unencrypted traffic traveling between the computer and the wireless router. The data are being broadcast to the surrounding area by both the computer and the router in the same way that noise from a conversation is vulnerable to eavesdroppers. Thus, information that is not encrypted at the end points of the transaction can be intercepted. Tools to capture this traffic and reassemble the data packets into web pages are widely available, and usable to any moderately sophisticated computer user.

Fortunately, standard practice on the Internet dictates that identity information should be exchanged between the user to the web server via a set of encrypted transactions. Almost every website will do this, so there is little risk of a password or other authenticator being intercepted. End-to-end encryption using SSL/TSL keeps the password safe between the browser and the web server. Many sensitive web sites, such as most financial services sites, also encrypt the entire session. All communication between the user and the web service is encrypted, so a wireless eavesdropper would not be able to obtain critical information.

However, encrypting entire sessions is computationally more expensive that not doing so, and may sites avoid it to keep from slowing the user's experience. As an alternative, many web sites encrypt the authentication step, and return a token called a "session cookie". This cookie is hard to forge, so the user can continue to resend the cookie to the web server to maintain the session without having to resend the password. This cookie becomes the identifier of the session as well as the authenticator of the user.

The chief threat here is that if the session cookie is not transmitted securely, then an eavesdropper might be able to intercept it. On a Wi-Fi network, where eavesdropping is easy, the cookie is easily recoverable by a third party. This third party can then present the session cookie to the web server and claim to be the original, authenticated user. Since the attacker has the session cookie, it is now inside the trusted perimeter, functionally indistinguishable from the original user. This attack, known as "session hijacking" allows an attacker to easily log in as the authorized user, since it has adopted, for the time being, the user's full identity.

The danger of this is obvious. While in an unencrypted Wi-Fi network, the attacker would already be able to observe the user's online behavior, now a malicious actor can gain complete control of the user's account, access any data and perpetrate any actions available to the original user. It is one threat to have ones email read or behavior on a social networking site observed; quite another to have a malicious actor actually take over the email or social networking account.

Moreover, since the attacker is passively eavesdropping, there is nothing the victim can do to detect a successful attack.

The risks of this attack have become more immediate. While this attack has been known for quite some time (Dittrich, 1999), people have progressively developed tools to make it easier. Some new tools, including Hamster, developed by Robert Graham, still required some technical knowledge. In October of 2010, Eric Butler and Ian Gallagher introduced Firesheep, a very simple browser extension that any average computer user could use. It installs quickly, and is instantly usable, allowing the casual user to obtain critical identity credentials for everything from newspapers to widely used web-based email accounts. By January of 2011, the tool had been downloaded over a million times.

Browser-based Web attacks

As the Web has matured, and web technologies grown more sophisticated, the browsers have taken on a more central role in delivering applications and interfaces to users. Web applications run on web servers, but some aspects of the code runs inside the user's browser. Browsers must be capable of interpreting and executing scripts sent from web pages. A new class of security vulnerabilities has emerged that allows injection of unauthorized code into the browser side of a web application. These cross-site scripting attacks exploit the automatic trust relationship assumed when a browser visits a web page. They are further complicated because the target web service may be different from the venue of the attack (the vulnerable web site). Attack venues are often popular web sites with community-driven features such as social network sites, blogs, message boards and chat rooms.

Unlike some online threats, this family of attacks does not directly target the web server. The attacker uploads some content to the venue. This uploading may be ostensibly legitimate (social media) or through an exploited vulnerability on the venue web server. This content contains some exploit code (usually written in the web languages of HTML and JavaScript). The code is downloaded as part of the web page when the victim visits the venue site. Alternatively, the user can be tricked into clicking a link that will reflect some malicious executable code back to the browser. While interpreting the legitimate code on the venue site to display for the user, the browser will execute the malicious code. The attacker can then access user information, such as the session cookie of any target website the user has logged into, such as an email account (see above). Some attacks can even force the user to execute arbitrary code from her browser.

These attacks have a few unique features. They do not exploit any vulnerability in the web browser or operating system, nor do they exploit a vulnerability in the software on the target website's web server. Rather, it takes advantage of the browser's trust in the website to automatically process the code sent to it from a web server. If the content on a venue website is only that of approved legitimate

users, then the trust model holds. However, the Web 2.0 world encourages everyone to share content through blog, public forums and other interactive sites. If this content can be uploaded by an attacker, it will not target the web server, but rather other browsers that load the shared content. If the content is not carefully filtered, it can contain malicious code masquerading as benign code. Since the content comes from a site that is ostensibly trusted by the browser (since it is loading the rest of the page), the browser will interpret the malicious code, perhaps sending cookie information to a third party, or sending a request to the attacker for instructions.

Here, the trusted web application, with whom the user already has some relationship, is a passive medium unknowingly serving malicious code. Web applications can fight back by trying to sanitize content, but attackers continually try to find new holes. The applications also have to ensure that the authorized users can still engage with the site and post desirable content. Attacks can be combined with other social engineering attacks. For instance, if a user can be tricked into clicking a cleverly formatted link for a poorly-protected website, the URL can contain hidden code that will cause some malicious action on the (legitimate) domain. For example, the cookie for legitimate payment website could be accessible to a malicious website, something that should not occur under standard operation of web sites.

Browser-based web attacks are difficult for users to detect. Moreover, because each potential web application behaves a little differently, vulnerabilities may be unique to specific web sites. This makes the process of finding and closing vulnerabilities expensive, more akin to traditional client software vulnerabilities.

Social Engineering

Social engineering attacks directly target users, inducing them to voluntarily turn over identity information or voluntarily take some action to assist the attacker. In the context of online identity, the most common form is "phishing", where the where an attacker manipulates a user to disclose their online identity information to a website in control of the attacker. Users are lured in through the now ubiquitous mass-emails purporting to be from financial sites, online stores, and major online services.

Phishing is noteworthy from a trust perspective. First, as a visible threat to consumers, its very presence can undermine trust in the online economy. Second, when a channel like email is overwhelmed by fraudulent emails from online services, it makes it much harder for legitimate services to use that channel. Consumers will be less likely to trust them—even trained to do so.

Finally, phishing illustrates the important two-way nature authentication. Certainly, any service provider must authenticate the user to make sure the user has the appropriate privileges in the system. But the user must also authenticate the service provider. Social engineering attacks are often devoted to tricking the

user into trusting an imposter. Identity systems require reliable mechanisms for mutual trust.

Solutions: Policy and Technology

The threats to online identity discussed above don't have perfect, easy to implement solutions. One reason is that all require coordination between technical tools and policy implementations, at the public or private level. Identity problems involve at least two parties, and many of the solutions require multiple parties to change their behavior or adopt a new technology. If the risks of the status quo are not sufficiently split between the stakeholders, then external incentives will be necessary to induce adoption. The need to integrate technical solutions into a policy context requires and understanding of the complexities of both sides.

Take online surveillance and tracking, for example. Purely technical solutions are impractical: it is too easy to track even the most careful of individuals, and modern security tools that try to obfuscate user identities are not terribly practical. Yet a policy outright banning all user tracking would cripple a growing industry in behavioral advertising that may not bother many Internet users, particularly if free services are available in return. A recent FTC proposal encourages browser-based mechanisms for opting out of tracking, as well as an enhanced policy tools to deter future privacy violations.

Even this relatively modest proposal requires the buy-in of a wide range of actors. Web sites, web analytics firms and large advertisers must change their systems to accommodate this. Browser developers must integrate the changes, test them and then convince users to upgrade their browsing software. Users must learn about the tools and decide whether and how to use them. The government must develop enforcement mechanisms, as well as explore options to detect non-compliance.

Both the technical and policy components are critical. By enabling a clear personal preference, rather than just trying to block specific tracking mechanisms, we avoid an arms race between advertisers and annoyed consumers (Soghoian, 2009). By using a browser-based solution, we allow for a more extensible, adaptable and customizable model while at the same time not creating a database of unique identities, similar to the FTC's Do Not Call list. On the policy side, making it a personal, opt-in choice preserves the current regime to user control, while requesting greater administrative and enforcement abilities for the FTC to create incentives for voluntary compliance.

The other threats discussed above are even more complex. For local network attacks, the stakeholders expand to include Internet service providers, and various businesses that operate Wi-Fi hotspots. Web sites can help mitigate the threat by implementing full encryption for web sessions, not just the initial authentication. This certainly makes sense for web sites with personal data, such as webmail and

social networking sites. This can be costly to implement, however, and can make the web experience slower. Google only enabled network-level encryption by default for its webmail service by default in January of 2010 (it had been optional but not well publicized since 2008) and Microsoft enabled it as an option in October of 2010. The vast majority of other heavily used social media web sites to not have this option.

While using network-layer security to encrypt web traffic with HTTPS can be tricky, recent improvements to the SSL/TLS mechanism have sharply reduced the computational and memory overhead for web servers (Langley, Modadugu and Chang, 2010). This software, to which Google contributed greatly, is open source and available, but still requires some substantial costs for large-scale implementation. Yet it must be implemented at each site—there is no centralized technical solution.

Coordination takes time, particularly if the solution is not only on the server side. An enhancement to HTTP that can prevent a cross-site scripting attack from stealing cookies was introduced by Microsoft in 2002 (Zhou and Evans, 2010). Known as an HTTP-only cookie, it does not encrypt the information, but does preclude many of the attacks seen on the Internet. HTTP-only cookies are set by the web server, but also require the user's browser to be capable of recognizing and handling the request. While it was introduced into Microsoft's Internet Explorer in 2002, the popular web browser Firefox did not begin to allow some users to use HTTP-only cookies through an extension until 2006, and did not automatically support it until 2007. Popular web server programming kits such as Ruby on Rails did not support it until 2008. A recent survey found that this simple security option is still not deployed by a majority of the most popular web sites (Zhou and Evans, 2010).

While technical tools will mitigate some threats, they both require widespread independent action and time for adoption and do not completely solve the problem. Even if solutions were implemented, other threat vectors would remain. This phenomenon is endemic in computer security as the attackers adapt to defenses and find new threat vectors. This does not mean that these defenses are not useful: many believe that the goal of computer security should be to raise the cost to the attacker, rather than only pursue 100% effective solutions (Boehme and Moore, 2009). Phishing attacks remain a threat, but have become harder to execute as companies actively try to take down the web sites. User education and browser-based tools have had some effect. One study has shown that banks who actively pursue web-based phishing attempts have greater success than international law enforcement has had removing child pornography (Moore and Clayton, 2008).

The Future of Identity Protection

We identify three particular areas that will need to be addressed by researchers

and policy makers. Each area requires coordination between private actors, and an understanding of the technical details, incentives and social risks to all parties.

Identity Infrastructure

One approach is to standardize many components of the identity ecosystem across the Internet. In July of 2010, the White House released a draft National Strategy For Trusted Identities in Cyberspace outlining key goals (NSTIC). This strategy affirms the goals of many private sector players already working to improve identity by seeking to allow digital identity information to be legitimately shared securely across networks and applications. The Strategy, formally announced in January 2011, aims to stimulate industry efforts to create a broad range of voluntary secure-ID products and services from multiple public and private suppliers. Instead of individuals having distinct relationships with each online identity, the Strategy builds on existing proposals to encourage a more organic and market-oriented approach.

There are three basic parties: users, identity providers and relying parties. Identity providers will enroll users and establish their digital identity information. The strategy envisions an open market of identity providers who can verify user identity as strongly or as weakly as they choose. When a user seeks to assert her identity or attributes to an online service—the relying party—will interact with the identity provider to verify the relevant information.

This model is very open, extensible and flexible. It is decentralized and market-driven: web services can demand particular identity verifications, and users can choose how much information to share with whom. Several systems that are already beginning to be deployed in this model enable "single sign on" that make it easier for users to move across services seamlessly (e.g. OpenID). By encouraging standards and shifting the process of identity verification to specialized parties, this approach can make identity online more trustworthy. Independently developed identity frameworks in this model use secure transmission of identity information. They can also enable a very robust form of privacy, as users can restrict the information shared to the limits of need-to-know. In an online purchase, for example, the merchant only needs to know the purchase information, the payer, the payment information and the shipper, the shipping information. (Hansen, Schwartz and Cooper, 2008).

Of course, serious challenges remain for the widespread and effective deployment of such a system. A single sign on system that allowed access to many services would be an attractive target for phishing and malware attacks. Who would bear responsibility for a vulnerability that allowed a successful exploit? Too little liability to the identity providers, and users and relying parties may not trust them; too much would deter market entrants. The actual structure of the market is also vague. The dynamics of economies of scale and first mover advantage do not predict an equilibrium of many diverse competing services. As the market evolves,

consumer protection policies may become necessary.

Red Flags Model

As part of the Fair and Accurate Credit Transaction Act of 2003, the FTC released the Red Flag rules, which went into effect December 31, 2010. Under these regulations, businesses which qualify as a "creditor" must monitor for "indicators of possible identity theft" or red flags. Compliance involves identifying relevant indicators specific to the firm, setting up procedures to detect them, and having a process for response and mitigation. The rule applies to both financial institutions and "creditor" organizations that regularly defer payment and bill consumers after the fact, such as telecommunications companies and healthcare providers. The rules make scant explicit mention of online identity. Any firm that is compliant with the Federal Financial Institutions Examinations Council's 2005 guidelines, "Authentication in an Internet Banking Environment" will already be compliant. However, the approach of identifying firm-specific risks will mitigate many threats if done correctly.

Compliance must have a strong online component. The FFIEC requires audit features that can assist in the detection of compromised passwords, but offers little specific guidance on how to do this, or how likely such detection should be (FFIEC, 2007).[1] Examining user behavior to detect specific activity must be a critical line of defense. Detection tools should be regularly updated to fit with trends in attacks on identity systems. Services that use identity systems to carefully monitor their customers for better service provision (such as determining what new promotions to offer) should leverage this technology to continually watch for anomalous behavior. The more sophisticated the identity infrastructure, the more sophisticated the behavioral modeling can be.

Red Flag rules only apply to financial institutions and creditors, and do not currently apply to the largest set of online services discussed above: the free ones. Yet three of the top five targets for phishing attacks in 2010 (eBay, Facebook, and Google) are not financial services web sites (Gudkova, 2010), and are thus are not necessarily covered by extant rules. Many other online services, including webmail sites, web hosting sites and social network sites are frequent targets. Clearly they are attractive targets for malicious actors seeking identity information, even if those identities are not actually the paying customers of those firms. Access to credentials of these sites can expose highly sensitive information and serve as the jumping off point to serious and highly customized fraud attempts. For email and social networking sites, attacks can be particularly insidious, since a sophisticated adversary can intercept messages to the user inside the system, making user vigilance much harder.

[1] Federal Financial Institutions Examination Council (FFIEC) "Authentication in an Internet Banking Environment" Guidance Statement. 2005

Application of the Red Flag model to online services raises several concerns. While the large potential targets should be strongly encouraged to adhere to the highest protection models, one might not expect this of smaller firms. One advantage of the market structure is that sites providing free services are often supported by advertisements, and have built an infrastructure to carefully monitor and track the behavior of users for personalized marketing. These tracking mechanisms are exactly what is needed to detect the irregular activity of malicious actors. Suddenly sending thousands of emails is an obvious signal. the source, timing, and usage pattern of credentials, to determine whether any vary sufficiently from the norm to raise suspicion.

Such regulation, if implemented properly, would not impose too high a burden on web services firms known to be targets of identity-based attacks. Yet rulemaking may not be necessary if a sufficiently large population can demonstrate that they are already making a strong effort to identify potential vectors of attack and are actively monitoring them. In a voluntary compliance model, consumer protection agencies can gauge protection efforts, and leverage their powers as conveners to promulgate best practices. Consumer advocacy groups should name and shame firms lagging behind the market leaders.

The Human Factor

Ultimately, the trust decision in online identity mechanisms resides in the consumer. The consumer must be able to actually use the protection mechanisms. Security engineers sometimes forget that users use a system for their own reasons, and security mechanisms are often things that stand in their way. If they are too onerous or complex, users will circumvent protections, or find alternatives. Systems must be easy to use. This is more than just the degree of technical competence required: the information should be usable as well. Rather than wade through privacy policies that have been shown to be incomprehensible (McDonald et al, 2009), why not focus on what people actually care about? Mozilla convened a workshop of privacy experts to identify key distinct aspects of online privacy that actually matter, and came up with a set of simple privacy icons representing an aspect of identity privacy (Raskin, 2010). Examples include whether data will be sold, whether it will be kept for longer than one month and whether data will be only used for its intended purpose. These definitions are standardized, so that all sites displaying the icon will comply to the same privacy standard on that issue.

On the other hand, one must be wary of presenting too much information. Information overload is a problem in the data saturated environment of the web. Developers should limit the number of decisions a user must make (Dhamija and Dusseault, 2008). Cognitive load is something that users will seek to avoid—their mental efforts will be devoted to the task at hand, not to navigating the transaction. Note that this does not always correlate with the classic model of informed consent in the Fair Information Practice model.

A final usability issue is the question of how to recover from a compromised identity mechanism. When an attack is finally successful, or a web service cannot authenticate a user, perhaps because of a lost password, how should an individual go about reasserting her identity? Using the traditional "secrets" such as mother's maiden name or social security numbers has been proven to be unsecure, since both can frequently be derived from public records (Acquisti and Gross, 2009). The increasingly common practice of "secret questions" such as pet names and childhood facts has also been shown to be vulnerable to guessing, particularly from acquaintances. (Schechter, Brush, and Egelman, 2009). The same study also demonstrated poor reliability—many people simply can't remember the answers they gave earlier. Another alternative is to rely on another communication channel that is relatively less likely to be compromised. A code could be sent to one's mobile phone via SMS, for example. Phones can be stolen or cloned, but this now raises the effort involved for a successful attack. In-person attestations with physical ID are another option, as a form of biometric security, but maintaining such physical presence can be quite expensive if not associated with an existing institution (the German post office serves this function, for example). A Microsoft researcher recently proposed one particularly clever approach: rely on social contacts to attest that the friend has indeed lost his password (Schechter, Egelman and Reeder, 2009). The more people depend on identity mechanisms, the more secure and reliable the recovery mechanisms must be.

Absent a trustworthy environment, the trend to increasingly participate in public life online may diminish. There are great potential gains to be made in everything from online political processes to eHealth initiatives. New applications will require more information to flow between more parties. These information flows must be secure, and they must respect users' expectations of privacy and integrity.

Conclusion

Risks to online identity have been with us almost as long as the first online identity systems. Yet the web has grown and evolved dramatically and people continue to use it. Why should we worry? Even as web services become a more important part of our lives, the attacks increase and evolve apace. The identity layer is a fragile and brittle component of all online applications, and we do not know how robust it is. Not only are identity credentials an attractive target, the identity layer itself is under attack. Many of these threats require a coordinated defense between actors who may not be directly at risk, and the victim is frequently unaware of an attack.

At the same time, it is also important to preserve an open Internet where consumers are willing to experiment with new and innovative online experiences. Balancing trust and openness will require careful collaboration between the technology and policy communities.

References

Acquisti, Alessandro and Ralph Gross. "Predicting Social Security Numbers from Public Data," Proceedings of the National Academy of Science, 106(27), 10975-10980, 2009.

Boehme, Rainer and Tyler Moore The Iterated Weakest Link - A Model of Adaptive Security InvestmentThe Eighth Workshop on the Economics of Information Security (WEIS 2009), University College London, UK 24-25 June 2009

Camp, Jean. "Net Trust: Signaling Malicious Web Sites", *I/S A Journal of Law and Policy in the Information Society*, 2007, Vol. 3, No 2: 211-235.

Dittrich, David. Session Hijacking Demonstration and Notes. 1998. http://staff.washington.edu/dittrich/talks/qsm-sec/hijack.html

Dhamija, Rachna and Lisa Dusseault. "The Seven Flaws of Identity Management: Usability and Security Challenges." IEEE Security and Privacy, 6:2. 2008.

Eckersley, Peter. "How Unique is Your Browser?" Privacy Enhancing Technologies Symposium, 2010.

Gudkova, Darya "Spam in the Second Quarter of 2010" Securelist Analysis, 2010 http://www.securelist.com/en/analysis/204792129/Spam_in_the_Second_Quarter_of_2010

Hansen, Marit, Ari Schwartz, and Alissa Cooper, "Privacy and Identity Management," IEEE Security and Privacy, 6:2. 2008.

Internet Policy Task Force. "Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework" Department of Commerce Green Paper, 2010.

Jang, Dongseok, Ranjit Jhala, Sorin Lerner, and Hovav Shacham. "
An empirical study of privacy-violating information flows in JavaScript web applications." Proceedings of the 17th ACM conference on Computer and Communications Security, 2010.

Kent, Stephen T. and Lynette I. Millett, eds. IDs -- Not That Easy: Questions About Nationwide Identity Systems. National Academies Press, 2002.

Langley, Adam, Nagendra Modadugu, and Wan-The Chang. "Overclocking SSL." O'Reilly Velocity Conference, 2010. Notes at http://www.imperialviolet.org/2010/06/25/overclocking-ssl.html

MacGregor, Willian, William Dutcher and Jamil Khan. "An Ontology of Identity Credentials. NIST Special Publication 800-103. 2006

McDonald, Aleecia, Robert W. Reeder, PatrickG. Kelley, and Lorrie F. Cranor. "A comparative study of online privacy policies and formats." Privacy Enhancing Techonologies Symposium 2009.

Moore, Tyler, and Richard Clayton, The Impact of Incentives on Notice and Take-down, WEIS 2008 - Seventh Workshop on Economics of Information Security, Hanover NH, 25-28 June 2008.

Pegaro, Rob. "Gawker Breach Fallout" The Washington Post Faster Forward Blog. December 15, 2010 http://voices.washingtonpost.com/fasterforward/2010/12/gawker_breach_fallout_linkedin.html

Raskin, Aza. "Privacy Icons: Alpha Release" 2010 http://www.azarask.in/blog/post/privacy-icons/

Roosa, Steven and Stephen Schultze. "The "Certificate Authority" Trust Model for SSL: A Defective Foundation for Encrypted Web Traffic and a Legal Quagmire" Intellectual Property and Technology Law Journal. 22:11 2010

Schechter, Stuart. A. J. Bernheim Brush, and Serge Egelman, It's no secret: Measuring the security and reliability of authentication via 'secret' questions, in Proceedings of the 2009 IEEE Symposium on Security and Privacy, IEEE Computer Society, Berkeley, CA, USA, 17 May 2009

Schechter, Stuart, Serge Egelman, and Robert W. Reeder, It's Not What You Know, But Who You Know: A social approach to last-resort authentication, in CHI '09: Proceeding of the twenty-seventh annual SIGCHI conference on Human factors in computing systems, ACM, New York, NY, USA, 9 April 2009

Shankland, Stephen. "Youporn sued for sniffing browser history" CNET Deep Tech News. Dec 6, 2010. http://news.cnet.com/8301-30685_3-20024696-264.html

Soghian, Christopher. "The benefits of using opt-outs". Slight Paranoia Blog, March 21, 2009.

Turow, Joseph, Jennifer King, Chris Hoofnagle, Amy Bleakley, and Michael Hennessey. "Americans Reject Tailored Advertising and the Three Activities That Enable It." September 29, 2009. Available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1478214

Zhou, Yuchen, and David Evans. "Why Aren't HTTP-only Cookies More Widely Deployed?" Web 2.0 Security and Privacy 2010.

Governance Studies
The Brookings Institution
1775 Massachusetts Ave., NW
Washington, DC 20036
Tel: 202.797.6090
Fax: 202.797.6144
www.brookings.edu/governance.aspx

Editor
Christine Jacobs

Production & Layout
John S Seo

E-mail your comments to gscomments@brookings.edu