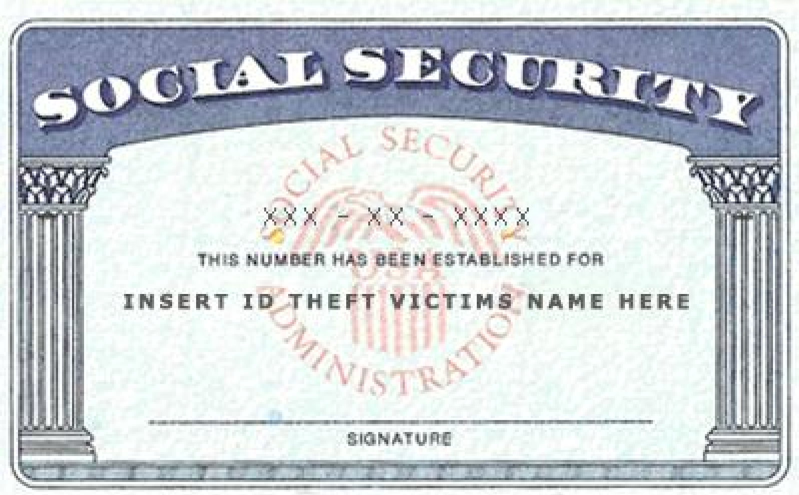
The Problem With Two-Factor Authentication

Garret Grajek — Temps de lectura: 13 minuts

DARKREADING

The Problem With Two-Factor Authentication

The failure of corporate security strategies to protect personal identity information from hackers resides more with system architecture than with authentication technology. Here's why.


SOCIAL SECURITY
SOCIAL SECURITY ADMINISTRATION
USA
XXX - XX - XXXX
THIS NUMBER HAS BEEN ESTABLISHED FOR
INSERT ID THEFT VICTIMS NAME HERE
SIGNATURE

For too long, enterprises have been looking for the perfect two-factor authentication. First, it was X.509, then hard tokens, then SMS, and now

Push and biometrics. And still, hackers keep winning. Just look at what happened with Target, Neiman Marcus, Living Social, Snapchat, and others.

The problem isn't the two-factor authentication technology. To be more specific, it's not just the two-factor authentication. It's the full integration, which includes the storage, accessing, validation, and assertion of identity throughout the authentication process.

But don't take my word for it. The forensics on most recent hacks reveal that hackers did not break the authentication mechanism itself. Rather, they broke the integration -- the identity passing and storage. That tells me websites (cloud or enterprise-based) that demand bulletproof security need to understand how authentication (single- or two-factor) is provisioned, conducted, validated from enterprise information, and asserted to the final resource -- and ultimately how the trust is reused at other resources.

How the authentication is provisioned

By this, I mean how the ID itself is granted to the user and how the credentials are provided to the users. The authentication process (single- or two-factor) should be quantified and scrutinized for weaknesses. One of the best ways to increase security in this procedure is to remove all human interaction (think: how to remove help desk interaction). You can validate users based on enterprise data or third-party social IDs and other data sources. You can then grant users reusable two-factor authentication credentials such as an X.509 certificate, an identity card, a mobile OATH token, or just the device itself.

Ideally, the registration process should be browser-based, which enables communication to match the client's native language automatically. Too often, however, each of these functionalities is siloed (e.g., coded after the two-factor product is purchased), and this is where the hacks occur. The hackers are breaching the architecture, not the authentication mechanism.

How and where the authentication takes place

Too often the validation algorithm is hosted or housed on servers or services that are beyond an enterprise's security control. These servers and services need to be scrutinized, because it is usually much easier for a hacker to breach the actual identity collection form (web or other form) than the actual authentication mechanism itself via cross-site scripting, SQL injection, or another attack vector against the form collector. Of course, this raises a raft of additional questions. Who wrote these collection forms? Are they housed on secure, enterprise servers? Have the forms been pen tested? Were they written by an outsourced contract service or hosted on insecure servers?

How the authentication is validated from enterprise PII

Most of the recent attacks have targeted enterprise-held personally identifiable information (PII), in which two-factor authentication methods prompted the company to sync up or migrate PII to other holders. As the Snapchat breach of 4.6 million users' phone numbers demonstrated, organizations need to secure their PII with the same security they use to keep passwords and other authentication information safe. Authentication information is, by its nature, PII, and allowing other services, especially authentication services, to use this data is simply asking for trouble.

How the authenticated identity is validated

Many authentication methods were created before resources like cloud and native mobile applications existed. As a result, common authentication mechanisms, such as tokens, were designed to use dated authentication protocols, like RADIUS, for resource-to-data-store validation. This type of authentication usually assumes that there is a proxy between the resource and the user, which is not always possible in the cloud and with mobile apps. In response, enterprises have implemented hackable integration methodologies that introduce vulnerabilities in the credential collection and identity-passing processes for these new resources.

Cloud resources should be secured with cryptographically signed assertions, like SAML or WS-Fed; similar mechanisms, including cryptographically validated web services, can be used for identity passing to native mobile apps. But these mechanisms are only as good as the services that encompass the identity passing. If the authentication system is separate from the identity-passing system, your enterprise needs to ensure that this transfer process is secure each and every time.

Don't ignore user fatigue
Ideally, all systems that users access (including network, cloud, enterprise, and mobile), should be set up to conduct some sort of identity validation. But if the enterprise forces a high-friction authentication such as SMS, token, or telephony, where the user has to re-enter credentials every session, it's pretty much guaranteed that the user will find a way to circumvent the best mechanisms and/or burden the help desk with repeated account lockouts or two-factor registration requests.

To alleviate this burden, SSO is the best solution. Look at consolidating enterprise resources into mechanisms that lend themselves to portal access where a single authentication (preferably, a strong one) allows access to multiple resources. Role-based is ideal, depending on what resources a particular user should see.

Organizations that demand bulletproof security must understand that true security is not in the authentication process alone. It's only when the entire system architecture -- from provisioning and validation through asserting identity -- is addressed from a security perspective that personal information will be truly safe from attack.

About the Author

Garret Grajek is a CISSP-certified security engineer with more than 20 years of experience in the information security and authentication space. As Chief Technical Officer and Chief Operating Officer for SecureAuth Corp., Garret is responsible for the company's identity enforcement product offerings. Prior to co-founding SecureAuth, he held leadership roles at some of the world's leading technology companies including Cisco and IBM, where he was responsible for consumer and network security products. He also served as western region lead field engineer for RSA Security and worked at Netegrity, where he led installations of SiteMinder, the security suite that controls all user access to the E*Trade Financial Services website. Garret began his career as an entrepreneur and founder of an independent programming company that specialized in operating systems and network utilities. He was a pioneer in the use of the Linux operating system in enterprise environments.

Keep up with the latest cybersecurity threats, newly discovered vulnerabilities, data breach information, and emerging trends. Delivered daily or weekly right to your email inbox.

You May Also Like

We Care About Your Privacy

We and our 848 partners store and/or access information on a device, such as unique IDs in cookies to process personal data. You may accept or manage your choices by clicking below, including your right to object where legitimate interest is used, or at any time in the privacy policy page. These choices will be signaled to our partners and will not affect browsing data.Privacy Policy

We and our partners process data to provide:

Use precise geolocation data. Actively scan device characteristics for identification. Store and/or access information on a device. Personalised advertising and content, advertising and content measurement, audience research and services development.

About Your Privacy

We process your data to deliver content or advertisements and measure the delivery of such content or advertisements to extract insights about our website. We share this information with our partners on the basis of consent and legitimate interest. You may exercise your right to consent or object to a legitimate interest, based on a specific purpose below or at a partner level in the link under each purpose. These choices will be signaled to our vendors participating in the Transparency and Consent Framework.
More information

Manage Consent Preferences

Performance Cookies

These cookies allow us to count visits and traffic sources so we can measure and improve the performance of our site. They help us to know which pages are the most and least popular and see how visitors move around the site. All information these cookies collect is aggregated and therefore anonymous. If you do not allow these cookies we will not know when you have visited our site, and will not be able to monitor its performance.

Functional Cookies

These cookies enable the website to provide enhanced functionality and personalisation. They may be set by us or by third party providers whose services we have added to our pages.   If you do not allow these cookies then some or all of these services may not function properly.

Strictly Necessary Cookies

These cookies are necessary for the website to function and cannot be switched off in our systems. They are usually only set in response to actions made by you which amount to a request for services, such as setting your privacy preferences, logging in or filling in forms.   You can set your browser to block or alert you about these cookies, but some parts of the site will not then work. These cookies do not store any personally identifiable information.

Targeting Cookies

These cookies may be set through our site by our advertising partners. They may be used by those companies to build a profile of your interests and show you relevant adverts on other sites.   They do not store directly personal information, but are based on uniquely identifying your browser and internet device. If you do not allow these cookies, you will experience less targeted advertising.

Store and/or access information on a device 683 partners can use this purpose

Store and/or access information on a device

Cookies, device or similar online identifiers (e.g. login-based identifiers, randomly assigned identifiers, network based identifiers) together with other information (e.g. browser type and information, language, screen size, supported technologies etc.) can be stored or read on your device to recognise it each time it connects to an app or to a website, for one or several of the purposes presented here.

Personalised advertising and content, advertising and content measurement, audience research and services development 812 partners can use this purpose

Personalised advertising and content, advertising and content measurement, audience research and services development

- **Use limited data to select advertising 621 partners can use this purpose**

  Advertising presented to you on this service can be based on limited data, such as the website or app you are using, your non-precise location, your device type or which content you are (or have been) interacting with (for example, to limit the number of times an ad is presented to you).

- **Create profiles for personalised advertising 500 partners can use this purpose**

  Information about your activity on this service (such as forms you submit, content you look at) can be stored and combined with other information about you (for example, information from your previous activity on this service and other websites or apps) or similar users. This is then used to build or improve a profile about you (that might include possible interests and personal aspects). Your profile can be used (also later) to present advertising that appears more relevant based on your possible interests by this and other entities.

- **Use profiles to select personalised advertising 497 partners can use this purpose**

Advertising presented to you on this service can be based on your advertising profiles, which can reflect your activity on this service or other websites or apps (like the forms you submit, content you look at), possible interests and personal aspects.

- **Create profiles to personalise content 221 partners can use this purpose**

  Information about your activity on this service (for instance, forms you submit, non-advertising content you look at) can be stored and combined with other information about you (such as your previous activity on this service or other websites or apps) or similar users. This is then used to build or improve a profile about you (which might for example include possible interests and personal aspects). Your profile can be used (also later) to present content that appears more relevant based on your possible interests, such as by adapting the order in which content is shown to you, so that it is even easier for you to find content that matches your interests.

- **Use profiles to select personalised content 194 partners can use this purpose**

  Content presented to you on this service can be based on your content personalisation profiles, which can reflect your activity on this or other services (for instance, the forms you submit, content you look at), possible interests and personal aspects. This can for example be used to adapt the order in which content is shown to you, so that it is even easier for you to find (non-advertising) content that matches your interests.

- **Measure advertising performance 723 partners can use this purpose**

  Information regarding which advertising is presented to you and how you interact with it can be used to determine how well an advert has worked for you or other users and whether the goals of the advertising were reached. For instance, whether you saw an ad, whether you clicked on it, whether it led you to buy a product or visit a website, etc. This is very helpful to understand the relevance of advertising campaigns.

- **Measure content performance 360 partners can use this purpose**

  Information regarding which content is presented to you and how you interact with it can be used to determine whether the (non-advertising) content e.g. reached its intended audience and matched your interests. For instance, whether you read an article, watch a video, listen to a podcast or look at a product description, how long you spent on this service and the web pages you visit etc. This is very helpful to understand the relevance of (non-advertising) content that is shown to you.

- **Understand audiences through statistics or combinations of data from different sources 457 partners can use this purpose**

  Reports can be generated based on the combination of data sets (like user profiles, statistics, market research, analytics data) regarding your interactions and those of other users with advertising or (non-advertising) content to identify common characteristics (for instance, to determine which target audiences are more receptive to an ad campaign or to certain contents).

- **Develop and improve services 546 partners can use this purpose**

  Information about your activity on this service, such as your interaction with ads or content, can be very helpful to improve products and services and to build new products and services based on user interactions, the type of audience, etc. This specific purpose does not include the development or improvement of user profiles and identifiers.

- **Use limited data to select content 128 partners can use this purpose**

  Content presented to you on this service can be based on limited data, such as the website or app you are using, your non-precise location, your device type, or which content you are (or have been) interacting with (for example, to limit the number of times a video or an article is presented to you).

Use precise geolocation data 263 partners can use this special feature

Use precise geolocation data

With your acceptance, your precise location (within a radius of less than 500 metres) may be used in support of the purposes explained in this notice.

Actively scan device characteristics for identification 127 partners can use this special feature

Actively scan device characteristics for identification

With your acceptance, certain characteristics specific to your device might be requested and used to distinguish it from other devices (such as the installed fonts or plugins, the resolution of your screen) in support of the purposes explained in this notice.

Ensure security, prevent and detect fraud, and fix errors 517 partners can use this special purpose

Your data can be used to monitor for and prevent unusual and possibly fraudulent activity (for example, regarding advertising, ad clicks by bots), and ensure systems and processes work properly and securely. It can also be used to correct any problems you, the publisher or the advertiser may encounter in the delivery of content and ads and in your interaction with them.

Deliver and present advertising and content 517 partners can use this special purpose

Certain information (like an IP address or device capabilities) is used to ensure the technical compatibility of the content or advertising, and to facilitate the transmission of the content or ad to your device.

Match and combine data from other data sources 363 partners can use this feature

Information about your activity on this service may be matched and combined with other information relating to you and originating from various sources (for instance your activity on a separate online service, your use of a loyalty card in-store, or your answers to a survey), in support of the purposes explained in this notice.

Link different devices 329 partners can use this feature

In support of the purposes explained in this notice, your device might be considered as likely linked to other devices that belong to you or your household (for instance because you are logged in to the same service on both your phone and your computer, or because you may use the same Internet connection on both devices).

Identify devices based on information transmitted automatically 496 partners can use this feature

Your device might be distinguished from other devices based on information it automatically sends when accessing the Internet (for instance, the IP

address of your Internet connection or the type of browser you are using) in support of the purposes exposed in this notice.

Cookie List

Your Privacy [`dialog closed`]