Identity protection and privacy: Ensuring online safety through secure access

No matter how you look at the trends, it's clear that data has become an essential part of everyday life. Whether it's the rapid expansion of public and private networks, the increased use of cloud computing, the mass deployment of smart objects, the rise of social media, or the adoption of electronic ID credentials — we gather, store, access, share, and rely on more digital information than ever before.

Our growing use of data serves to underscore the importance of security. As we increase our dependence on data, we also increase our need to ensure its privacy and protect it from being accessed by the wrong people. Effective security, at every point where data is entered, stored, or transmitted, helps ensure that citizens stay safe, essential services continue uninterrupted, governments operate effectively, and economies remain stable.

Cyber criminals are active in all online venues, and today's networks are at risk of attack at every level, from the local to the national and international. The reality is that there are vulnerabilities everywhere, throughout the civilian and military infrastructures.

According to US Defense Secretary Ashton Carter, *"We're not anywhere near where we should be as a country… Not only is our civilian infrastructure susceptible to cyberattack, but we have to be concerned about our military infrastructure."*

The importance of authentication

Online security can mean different things to different people, but the tasks of keeping data private and ensuring cyber safety essentially come down to one thing: access. Whenever there's a failure in security, due to a data breach, a denial-of-service attack, identity theft, the spread of malware, or some other act of sabotage, the failure can almost always be tied to unauthorized access. At some point, someone (or something) found a way to be where they shouldn't have been, and did damage.

This means that maintaining security is, at its core, about preventing anyone or anything from gaining unauthorized access. Before being allowed to submit data, modify information, save settings, or execute tasks, whoever is trying to gain access – be it a person, a device, or a piece of software – must first verify that they are, indeed, who they say they are. This process, known as authentication, is the starting point for all online security. When done right, authentication protects every interaction, and makes it safer for people, devices, and applications to access and share data.

Authentication is needed everywhere

No matter what the online scenario, authentication plays an essential role in keeping the process secure for everyone involved. For people using computers,

cars, smartphones, wearables, smartcards, or electronic IDs to access services and exchange information, effective authentication ensures security for making purchases, logging onto a corporate network, riding public transport, updating health records, driving a car, using government services, or simply sending an email or sharing a photo.

For the rapidly growing number of network-connected devices, known as the Internet of Things or the IoT, effective security prevents criminals from accessing data. This protects against the kinds of sabotage that can cripple the public infrastructure — which increasingly relies on smart grids and other network-controlled operations – and makes the IoT a safe place for private users, from the homeowner programming a remotely-controlled thermostat to the global corporation managing thousands of connected devices.

While it makes sense, in theory, to require all IoT devices to meet baseline security requirements, the reality is that adding security costs money, and there is little, if any, short-term return on the investment for the manufacturer. To prompt IoT manufacturers to make the investment, we could take a lesson from the automotive industry, where drivers are required to carry liability insurance that pays for damage they might do to others on the road. In similar fashion, IoT manufacturers could be required to add a minimum set of security features, so as to minimize the risk of online sabotage and, in a way, invest in the safety of others.

At another level in the network, in the purely cyber realm, where operating systems and software code can interact on their own, effective authentication prevents intrusions, thefts, and attempts to introduce viruses or malware.

Throughout the online world, it's as simple as this: without authentication, there can be no security.

Staying one step ahead

The main challenge with authentication, though, is that authentication algorithms can become outmoded. Cyber security has been likened to an arms race, with previously secure systems becoming vulnerable as hackers and other criminals begin to erode the protection mechanisms. Data that was safe yesterday may not be safe today or tomorrow.

Keeping one step ahead involves two things: optimizing the algorithms themselves, to make them stronger, and creating better ways to protect the authentication process. In particular, the cryptographic keys used to safeguard authentication data must never be allowed on the network. Any time keys are transmitted over a network, they run the risk of being discovered, and that means the information they protect can also be discovered. To ensure privacy, and prevent cryptographic keys from being discovered, the authentication environment needs to isolate keys from the network. The best way to do this is to store the keys locally, in hardware, using a tamper-resistant circuit called a secure element. With the addition of hardware-based secure elements, the authentication process

gains an extra level of protection simply not possible with a software-only approach.

Adding support for online connectivity increases the complexity of any system, and complexity usually leads to errors, especially in terms of software. Even the most carefully reviewed source code can have a bug every few hundred lines, so it's important that any added functionality, such as online connectivity, be as simple to implement as possible. Secure elements help with this, since they essentially create a fence around the device. The fence streamlines traffic, reduces the amount of communication going in and out, and enables a smarter system that is, at the same time, less complex to manage, easier to design, and faster to debug.

NXP is security

Authentication is an area of special expertise for NXP Semiconductors. NXP has made authentication a top priority for more than 20 years, and has continually reached new levels of performance by making authentication algorithms more resilient, and by increasing the robustness of secure elements. We are a recognized leader in authentication, known for our ability to deliver trusted security in many of the world's most high-profile applications.

Leadership

NXP's strength in secure solutions is closely tied to eGovernment, electronic ID, and payment. With a presence in 80 percent of the world's electronic passport projects, our technology is trusted by more national governments to increase security while reducing wait times at international borders. Our products enable government employees around the world to access their IT systems securely, and make it easy for citizens to safely access government services and provide electronic signatures for various transactions. We are helping to expand the use of electronic documents throughout government, and our repeated successes with large-scale implementations for electronic IDs, public transport, connected cars, and multi-application cards (which combine payment, transport, identification, and other services on a single card), make us a trusted partner to municipalities, transit authorities, and banking and payment organizations worldwide.

Experience

We have advised nearly 100 governments on a variety of security solutions, providing guidance on everything from access and transportation to electronic IDs, health cards, and other types of social services. Our long-standing relationship with Germany, one of the most advanced countries in terms of cyber security, has produced a number of industry firsts: our technology helped Germany launch the first multi-functional credit card with smartcard technology (1996), made possible the first ePassport program to use asymmetric cryptography and support biometric data (2007), and is the foundation for the country's national ID cards (2010), which have been credited with setting new standards for document security, privacy protection, and citizen convenience.

Expertise

Our secure elements, and the production processes used to produce them, are certified according to the internationally recognized ISO/IEC 15408 standard, the Common Criteria for Information

Technology Security Evaluation. We routinely pass the required audits for this standard, and have earned EAL6+ certification, which represents the highest practical level of evaluation assurance.

As a supplier of end-to-end solutions, ranging from integrated circuits (ICs) to infrastructure components and secure applications, we bring a comprehensive set of skills to each security challenge. We add to our in-house know-how by leveraging relationships, with a broad spectrum of security leaders, to deliver tailored solutions that address the particular needs of each application.

Innovation

We are the inventor of MIFARE, the world's leading contactless technology for transport, and the co-inventor of Near Field Communication (NFC), the wireless proximity technology bringing new levels of simplicity and security to interactions of all kinds. Our secure elements, which build on our groundbreaking work in microcontroller design, lead the industry in shipments. We are also a high-level contributor to standards bodies, including the FIDO Alliance, whose work promises to usher in a new era of online security, making the need to remember complex passwords a thing of the past.

Research

We keep our eye on the future, with extensive in-house resources dedicated to developing security, and have well-established projects, at several universities, that are expected to yield dozens of new security features. Our focus is on securing identities in a convenient way, and have several initiatives underway, including the increased use of biometrics and new methods for reducing power consumption, that will both enhance and simplify security.

To learn more about NXP Semiconductors and our industry-leading security solutions, please visit **www.nxp.com.**

www.nxp.com

Date of release: April 2105
Published in the USA