Control do Acceso

Identificación, Autenticación, Autorización e Auditoría

Conceptos Básicos

- A **Identificación** consiste na comprobación da identidade do usuario (por exemplo, cun nome de usuario)
- A **Autenticación** consiste en verificar de modo fidedigno a identificación realizada (por exemplo, cun contrasinal)
- A **Autorización** consiste en determinar qué pode facer e qué non pode facer un usuario nos sistemas (por exemplo, cos permisos sobre os ficheiros)
- A **Auditoría** consiste en rexistrar todos os accesos correctos e todos os accesos erróneos xunto con toda a información asociada. As auditorías deben tamén rexistrar todas as accións do usuario proporcionando *non repudio* sobre as súas accións.

O conxunto de datos identificativos e de autenticación reciben o nome de ***credenciais do usuario***

Identificación

Os identificadores de usuario deberían cumprir coas seguintes características:

- Ser **único**. Non poden existir dous usuarios co mesmo identificador.
- **Non** ser **descriptivo**. Non se debe poder deducir o nivel de autorización do usuario a partir da súa identificación. Por exemplo non é boa idea utilizar *mariaDBA* ou *belenAdmin* como identificadores.
- Debe ser **emitido de xeito seguro** de modo que o usuario deba cambiar a súa contrasinal no primeiro acceso.

Factores de Autenticación

Un *factor de autenticación* é un elemento que se pode utilizar como proba da identidade do usuario. O factor de autenticación máis común son as contrasinais.

En xeral podemos distinguir 3 tipos de factores:

- Algo que se coñece (como un contrasinal)
- Algo que se ten (como unha chave ou un teléfono móbil concreto)
- Algo que se é (como unha pegada dactilar)

Sin embargo, non é seguro xa que tanto o contrasinal/PIN como as respostas ás cuestións poden ser obtidas por algún atacante de xeitos mais ou menos simples.

Factor de Coñecemento: Contrasinais

As contrasinais son o factor de autenticación máis estendido, se debe ter especial coidado no seu deseño xa que son susceptibles de varios tipos de ataque:

- Interceptación
- Acceso o ficheiro de contrasinais
- Forza Bruta por Dicionario
- Enxeñería social
- Forza Bruta mediante Rainbow Tables (e un diccionario de hashes ao que é vulnerable o ficheiro *SAM (Security Account Manager)* de contrasinais de Windows)

Os ataques de forza bruta son particularmente efectivos si as contrasinais son demasiado simples. E importante establecer unha ***política de contrasinais*** que estableza:

- A Lonxitude e complexidade das chaves
- A caducidade máxima e mínima
- O xeito de almacenalas
- O procedemento en que se asignan as contrasinais aos usuarios
- O proceso de recuperación en caso de non recordar unha contrasinal
- O número máximo de intentos de acceso fallidos que se permiten

https://howsecureismypassword.net/

Factor de Posesión

A posesión de algo pode ser tamén un factor utilizado na autenticación. Por exemplo, unha *tarxeta de acceso corporativa*, un *token RSA*, un *token OTP-SMS* ou un *certificado*.

Estes factores de autenticación son máis fiables, especialmente os token RSA / OTP (One Time Password), pero tamén son máis caros de implementar.

Os token RSA crean un código mediante o ID de usuario o ID do token e a data e hora. O servidor emprega o mesmo algoritmo para xerar o código. Si o código coincide, a autenticación ten éxito.

Factor Biométrico

Este factor ***se basea nas características físicas ou de comportamento*** da persoa que se desexa autenticar, como por exemplo a pegada dactilar, o recoñecemento facial ou o escáner de retina.

Este factor de autenticación é o máis fiable, xa que non é posible difundilo, compartilo ou ser roubado. Sin embargo, e o máis caro de implementar e en caso de ser vulnerado non se pode sustituír. Os datos biométricos son especialmente sensibles, e están regulados pola ley de protección de datos (GDPR).

Se dividen en dous grupos:

- ***Sistemas fisiolóxicos***, que se basan nas características físicas únicas dos individuos
- ***Sistemas comportamentais***, que se basan no xeito único en que os usuarios realizan certas actividades, como o análise de voz, de escritura, xeito de teclear, a firma física, o movemento dos músculos da cara....

Os sensores biométricos transforman a información do escáner en información binaria que se cifra e se almacena nunha base de datos de autenticación de xeito que no futuro poda ser comparada cos datos obtidos. E complicado obter información fiable no 100% dos casos xa que a lectura pode estar influída por moitos factores, por exemplo a retina ten cambios nos embarazos das mulleres.

O método biométrico máis fiable e o escáner de retina.

A precisión dos sistemas biométricos se mide en función de dous parámetros, o FRR (False Rejection Rate) e FAR (False Acceptance Rate) cos que se calcula o CER (Crossover Error Rate) que é o punto no que o FRR coincide co CER. ***Os sistemas máis precisos son os que o seu valor CER é o máis próximo a 0***.

Autenticación Multifactor

Hoxe en día se tende a utilizar simultaneamente varios factores de autenticación, sendo requisito legal para algúns servizos como os servizos de medios de pago.

https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32015L2366&from=EN

Este procedemento se lle chama ***autenticación multifactor*** ou reforzada. Deste xeito podemos falar de autenticación de factor dobre, triplo, cuádruplo….. etc.

Google Authenticator xera contrasinais aleatorias de un minuto de duración para varios servizos (Amazon, Google Suite, LinkedIn…). No momento de acceso se solicitará usuario, contrasinal e o código que proporciona Google Authenticator.

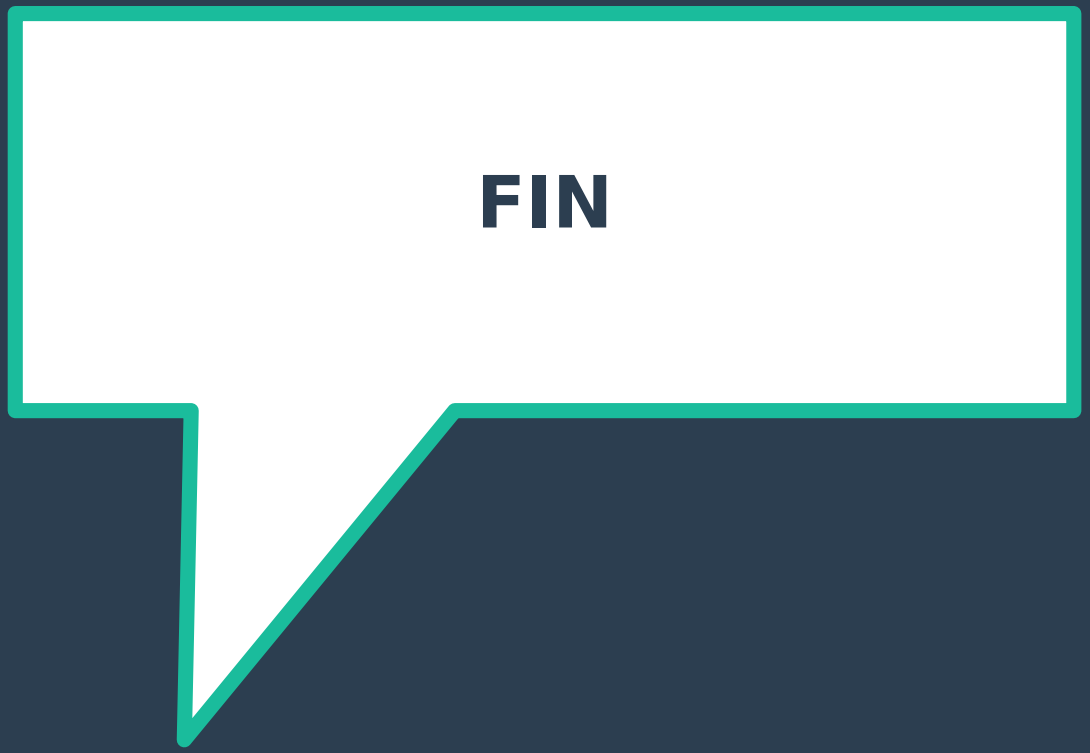
Auditoría e non repudio

A auditoría permite recoller os eventos e accións que leva a cabo un usuario durante o uso dos sistemas de información. **Se recomenda recoller:**

- Intentos de acceso
- ID do usuario
- Data e Hora
- Información do dispositivo que realiza o acceso (IP como mínimo)
- Eventos de acceso (concedido / denegado)

Os obxectivos son:

- Responsabilizar ao usuario das actividades realizadas
- Identificar incidencias en tempo real
- Axuda para a solución de incidencias de seguridade e de funcionamento
- Soporte en tarefas forenses


FIN