
Photo by Jean-Daniel Beley

مركز دراسات الجرائم المعلوماتية

الهُوِيَّة الرَّقمِيَّة: إِدارتها وسرقتها!

د. وليد بن أحمد الرزوضان

waleed@waleed-security.com
waleed-security.com
@warodhan

تعريف بالمُحاضِر

- حاصل على الدكتوراه من جامعة لندن (هولوي الملكية) في عام 2011م، في تخصص أمن المعلومات.
- حاصل على الماجستير من جامعة لندن (هولوي الملكية) مع مرتبة الشرف الأولى في عام 2005م، في تخصص أمن المعلومات.
- حاصل على البكالوريوس من كلية علوم الحاسب و المعلومات في جامعة الملك سعود في عام 2002م، في تخصص علوم الحاسب.
- محكم للعديد من المجلات العلمية العريقة (كمجلة The Computer Journal من جامعة Oxford البريطانية، ومجلة Security and Communication Networks, Wiley الأمريكية) والمؤتمرات العالمية (كمؤتمرات NordSec وEuroPKI) والكتب (ككتاب Fundamentals of Digital Forensics).
- له مؤلفان في مجال أمن المعلومات وإدارة الهوية الرقمية وهما: **Identity Management Systems: Academic Overview** عن دار النشر الألمانية VDM - Verlag Dr. Müller GmbH. و **Digital Identity and Access Management: Technologies and Framework** عن دار النشر الأمريكية IGI Global. بالإضافة إلى عشرات الأبحاث الأكاديمية المنشورة في أوعية عالمية.

وهو حالياً:

- أستاذ مساعد في قسم علوم الحاسب في كلية علوم الحاسب و المعلومات في جامعة الامام محمد بن سعود الإسلامية.
- وكيل عمادة تقنية المعلومات في جامعة الامام محمد بن سعود الإسلامية.
- رئيس مجلس البحث العلمي في كلية علوم الحاسب والمعلومات في جامعة الامام محمد بن سعود الإسلامية.
- رئيس وحدة البحوث في كلية علوم الحاسب و المعلومات في جامعة الامام محمد بن سعود الإسلامية.
- عضو مجلس الخبراء في مركز دراسات جرائم المعلوماتية في جامعة الإمام محمد بن سعود الإسلامية.
- رئيس مجموعة أمن المعلومات في جمعية الحاسبات السعودية.
- مستشار غير متفرغ لعدد من الجهات.

عن ماذا سنتحدث؟

الهُوية

- مفهوم الهوية.
- مفهوم الهوية الرقمية.

إدارة الهُوية الرقمية

- مفهوم إدارة الهوية الرقمية.
- إدارة الهوية الرقمية على الويب.
- نماذج تطبيقية.
- أنظمة إدارة الهوية الرقمية.

سرقة الهُوية الرقمية

- تعريف ولمحة تاريخية.
- أساليب السرقة.
- الوضع الحالي.
- وسائل الحماية.

الهُوِيَّة

مفهوم الهوية – 1

- ما معنى هُوِيَّة؟

- "حَقِيقَة الشَّيْء أَو الشَّخْص الَّتِي تميزه عَن غَيره." - المعجم الوسيط.

- *"the characteristics determining who or what a person or thing is."* - Oxford Dictionary.

- ISO/IEC 24760: It is the representation of an ***entity*** in a given context, where an entity is something that has a distinct existence and can be uniquely identified (e.g. a person or an organisation). This representation takes the form of a defined collection of entity attributes or distinctive characteristics.
(These attributes and characteristics are also collectively referred to as personally identifiable information (PII)).

- ITU-T X.1250: It is the representation of an entity (or group of entities) in the form of one or more information elements which allow the entity(s) to be uniquely recognised within a context to the extent that is necessary (for the Relevant applications).

مفهوم الهوية – 2

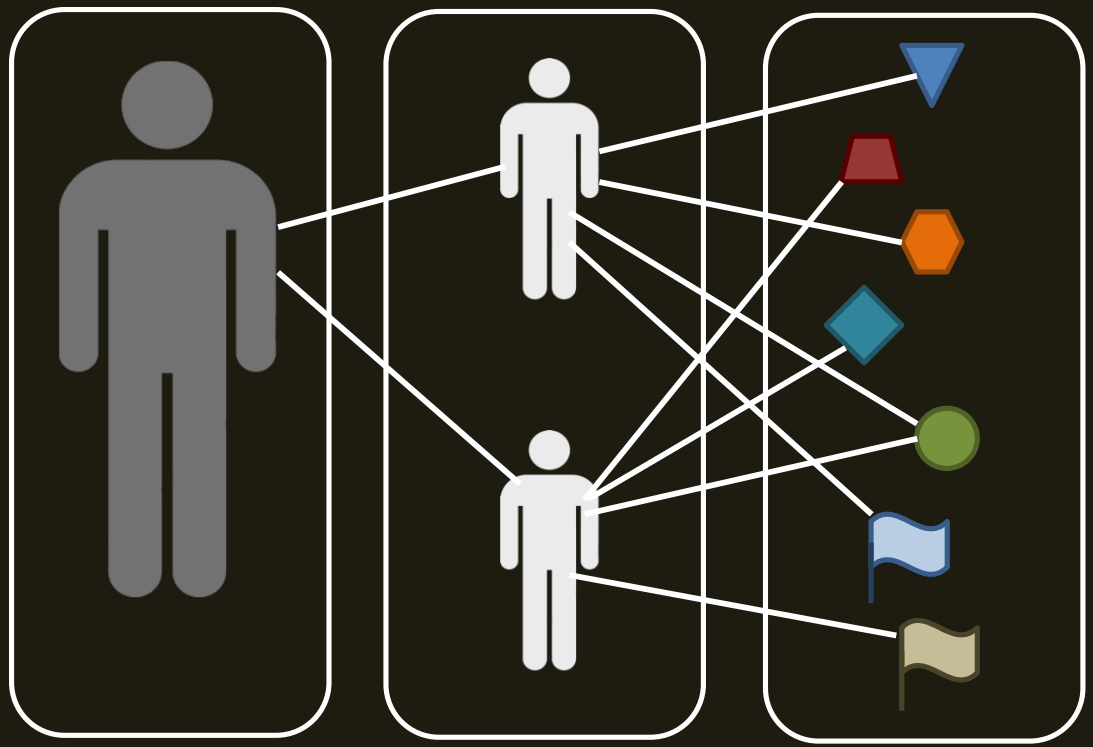
- **الهوية الشاملة** whole identity تحوي جميع الخصائص والصفات والمعلومات المتعلقة بكيان ما (شخص، مؤسسة، الخ.)، بينما تحوي **الهوية الجزئية** partial identity مجموعة محدودة من هذه الخصائص أو الصفات أو المعلومات.
- لكل كيان هوية شاملة واحدة فقط، لكن يمكن أن يكون له مجموعة كبيرة من الهويات الجزئية المختلفة.
- المُعرِّف والتَعرُّف.

- An identifier is a unique label for an object, that can be used to refer to an entity in a specific context (e.g. a national ID number, a student number, or a username that refers to a user's digital account).
  We can consider an identifier as a special attribute of an entity that must be unique within its context of use.

- Identification can be defined as a “process to determine that presented identity information associated with a particular entity is sufficient for the entity to be recognised in a particular domain”. – ISO/IEC 24760

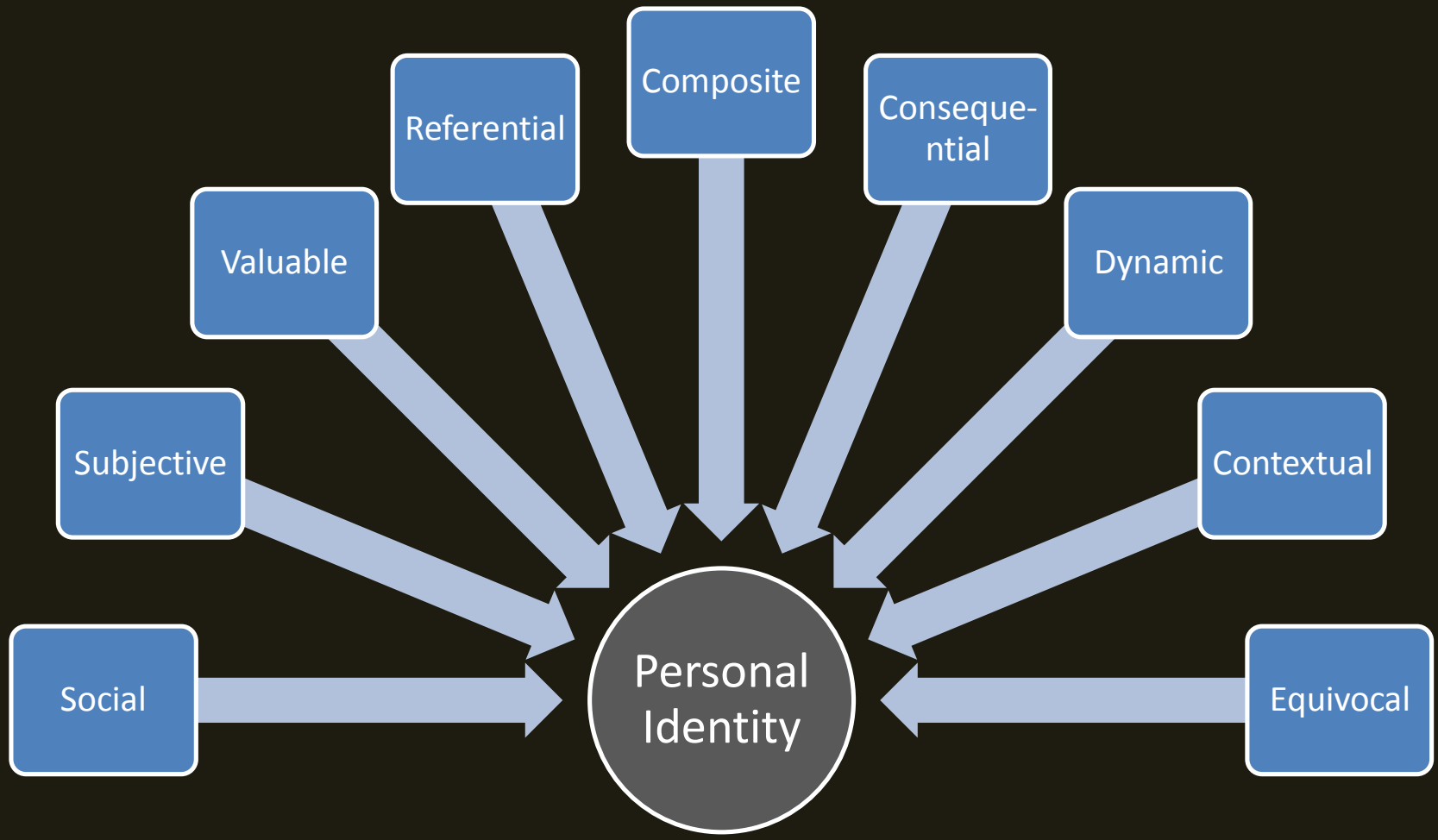
مفهوم الهوية – 3

العلاقة بين الكيانات والهويّات والمعرِّفات



مفهوم الهوية – 4

الخصائص التي يجب أن تتوفر في الهوية الشخصية (أي المتعلقة بأشخاص) حسب معايير الـ OECD:

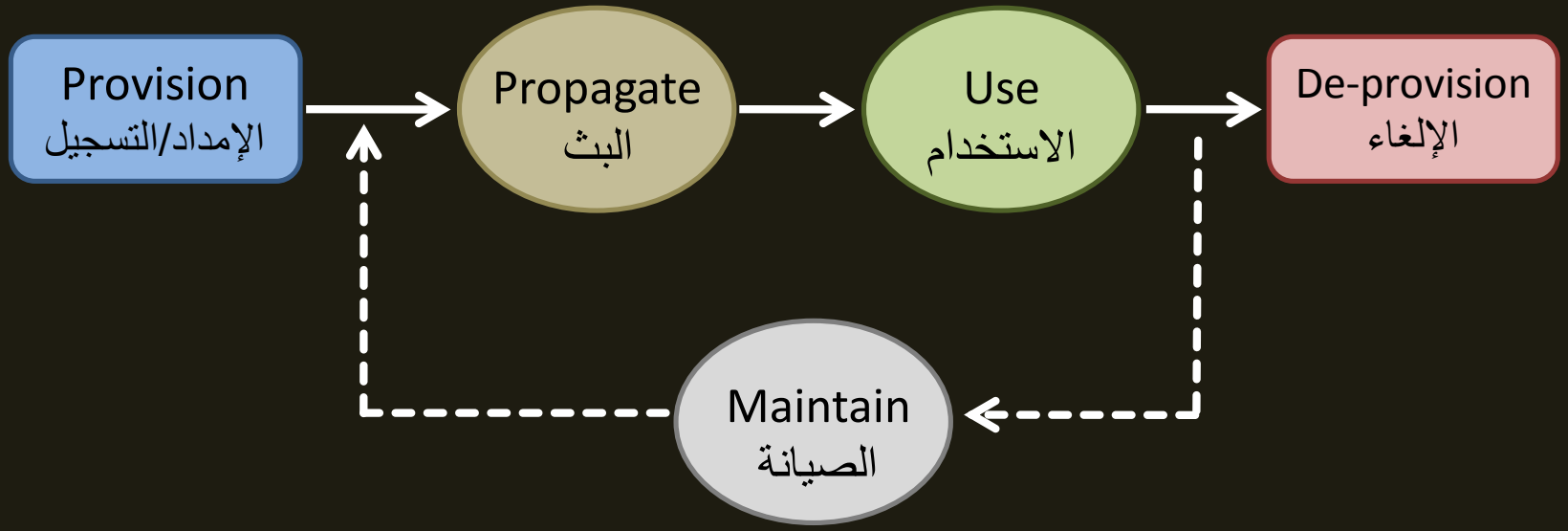


مفهوم الهوية الرقمية

- عندما تتم 'محاكاة ' الهوية داخل نظام رقمي (أو حاسوبي) فإنها تسمى **هوية رقمية**.

ابتداءً من الشريحة القادمة عند ذكر كلمة 'هوية' فإن المقصود هو دائما 'هوية رقمية'

- دورة حياة الهوية الرقمية:

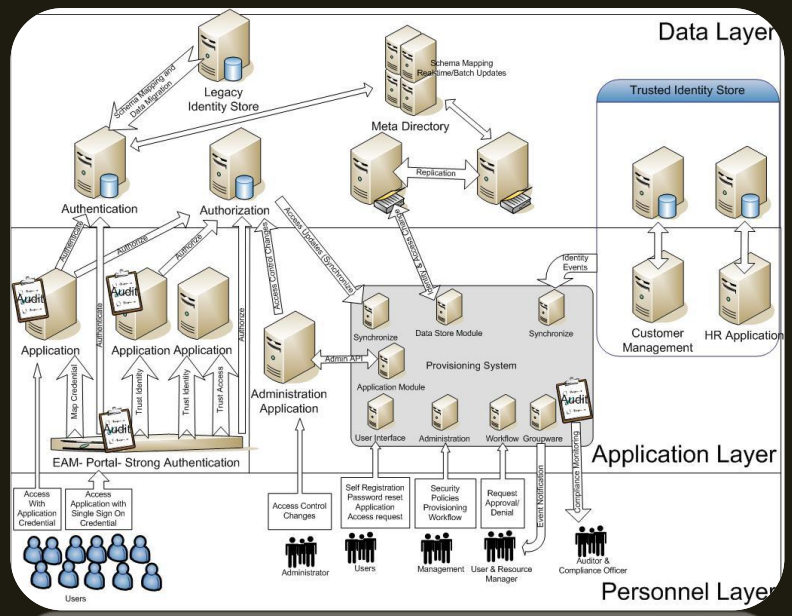


إدارة الهوية الرقمية

إِدَارَةُ الهُوِيَّة الرَّقَمِيَّة

1 – مفهوم إدارة الهوية الرقمية

- **إدارة الهوية الرقمية** تعني تنظيم مجموعة العمليات والسياسات والتقنيات التي تساعد سُلطَة الهوية والكيانات الفردية على استخدام كافة المعلومات المتعلقة بالهوية الرقمية.
- إدارة الهوية الرقمية تشمل إدارةَ كلٍ من:
  - دورة حياة الهوية الرقمية.
  - المعلومات المتعلقة بالهوية الرقمية.
  - التحقق من هوية الكيانات.



2 – مفهوم إدارة الهوية الرقمية

• ISO/IEC 24760: ***identity management*** is a set of processes, policies and technologies that help authoritative sources* as well as individual entities to manage and use identity Information. Identity management processes include *management of*: the *identity lifecycle*, *identity information*, and *entity authentication* as a preparatory step for authorisation.

* An ***authoritative source*** (or identity authority) of identity information is a place from which a relying party can obtain reliable information about the attributes of a given entity.

• ITU-T Y.2720: ***identity management*** is a set of functions and capabilities (e.g. administration, management and maintenance, discovery, communication exchanges, correlation and binding, policy enforcement, authentication and assertions) used for:

- *assurance of identity information* (e.g. identifiers, credentials, attributes);
- *assurance of the identity of an entity* (e.g. users/subscribers, groups, user devices, organisations, network and service providers, network elements and objects, and virtual objects); and
- *enabling business and security applications*.

3 – مفهوم إدارة الهوية الرقمية

- Identity management is an essential part of many security services, since it provides assurance of user legitimacy. As a result, identity management is an integral part of any ***access management system***.
  - IDM Vs. IDAM.
- Since identity management requires storing, processing, and transforming of identity information, it raises many privacy concerns. Moreover, requirements for privacy and identity management may conflict.
  - Requirements of OECD, Data Protection Act, HIPPA, etc.

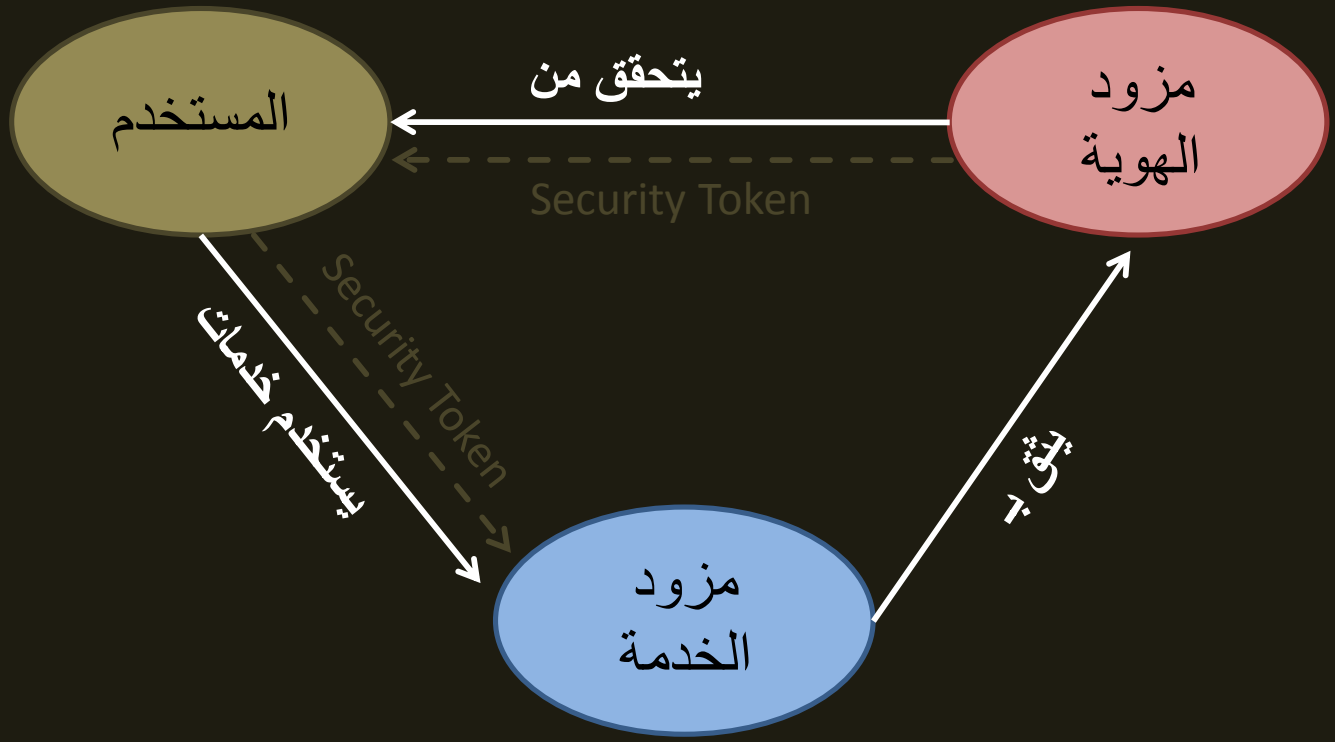
إدارة الهوية الرقمية على الويب – 1

- في عالم اليوم أصبح من الضروري أن يملك كل منا عدة هويات رقمية. إدارة هذه الهويات وحماية وسائل التحقق منها (ككلمات المرور مثلاً) أضحت عملية صعبة ومتعبة للمستخدم.
- إدارة الهوية الرقمية على الويب مبنية على استخدام بروتوكولات الويب العالمي WWW وخدمات الويب *-WS كوسيلة تواصل بين الأطراف الأساسية في نظام إدارة الهوية الرقمية.
- هذا النظام يخدم بشكل أساسي مستخدمي الإنترنت.

- Three main parties can be identified within the web-based identity management model:
  1. **The Identity Provider or Identity Issuer (IdP) [مزود الهوية]** issues an identity to the user, and is trusted by the other parties for the purposes of identity management.
  2. **The Service Provider (SP) [مقدم الخدمة]** (or Relying Party (RP) in Microsoft terminology), needs to identify the user before providing services to him/her.
  3. **The User [المستخدم]** needs to use the SP services. Typically, the user employs a user agent (e.g. a web browser) as the means by which she/he interacts with the IdPs and SPs.

إدارة الهوية الرقمية على الويب – 2

- النموذج النظري لإدارة الهوية الرقمية على الويب



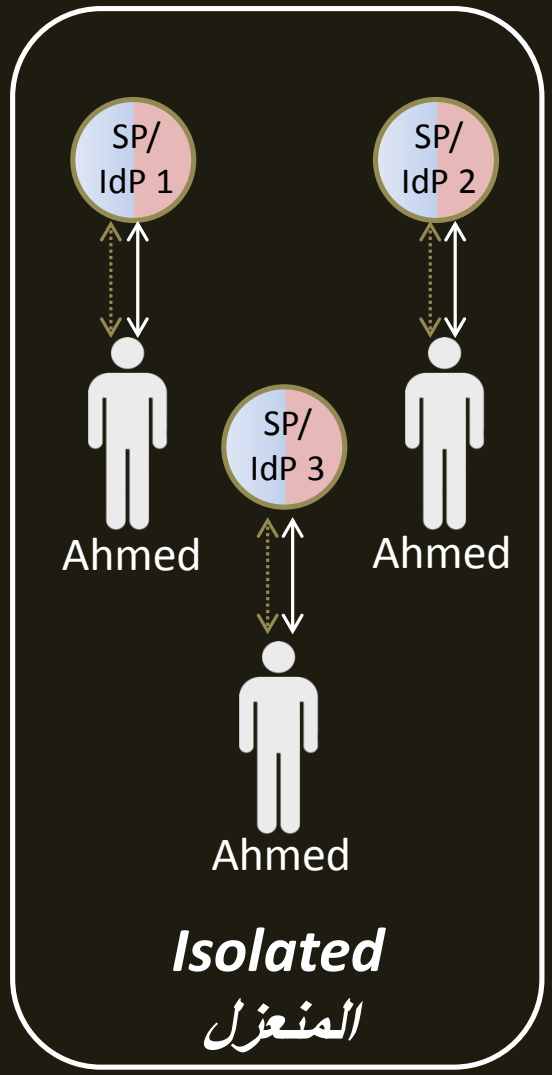
- User(W3C, P3P, APPEL)/SP/IdP security policies – security token/assertion – DoIS – PoF – etc...

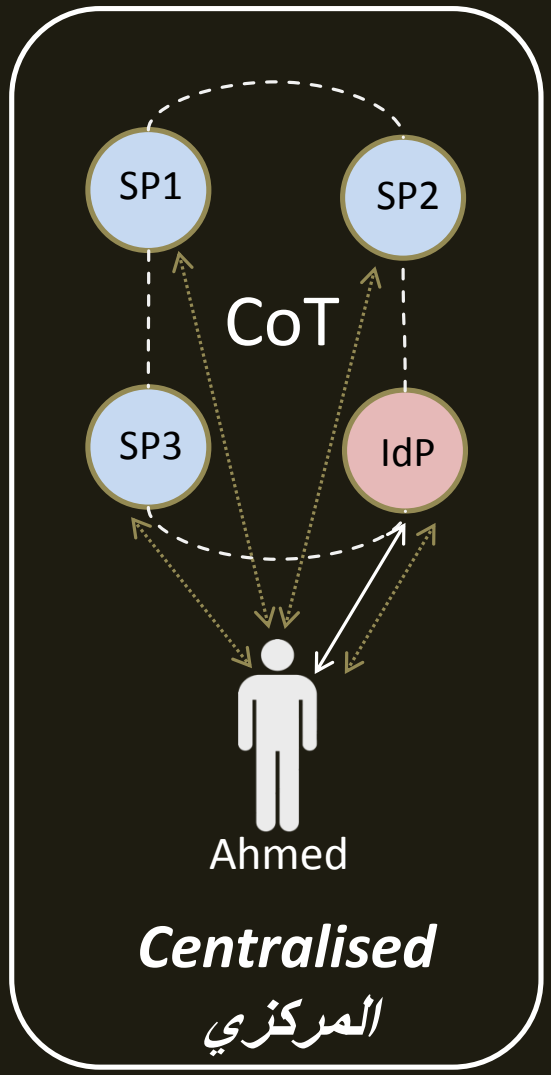
إدارة الهوية الرقمية على الويب – 3

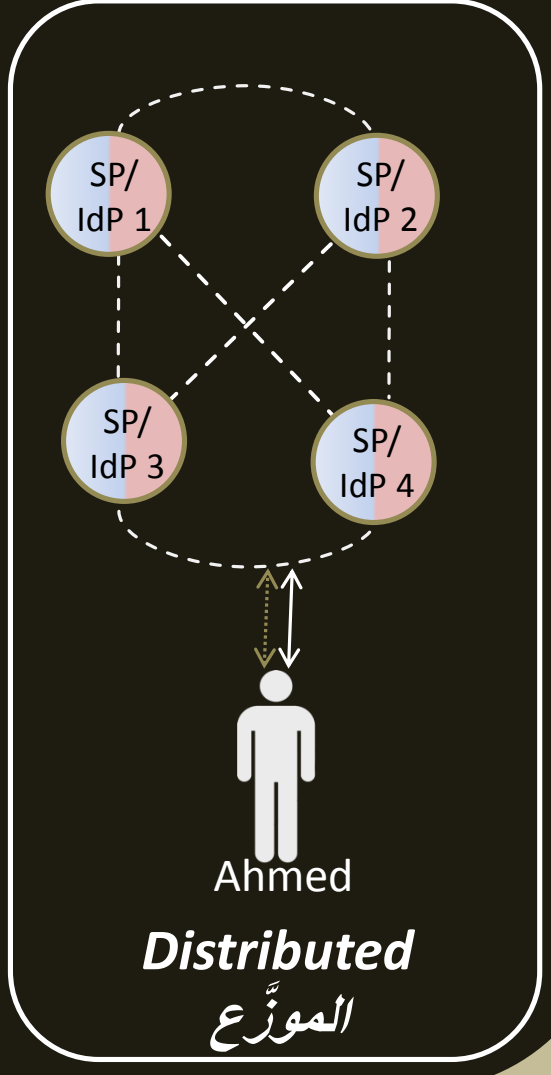
- ***Web-based IDM frameworks*** can be classified into the following three main classes, depending on the nature of the IdP/IdP and IdP/SP relationships.

1. **Isolated framework [المنعزل]**. In such a framework there is no co-operation between parties to support user authentication. The SP trusts only itself, and also plays the role of the IdP.
2. **Centralised framework [المركزي]**. A framework of this type has a single IdP that provides identity services to other participating SPs within a closed domain or 'circle of trust' (CoT).
3. **Distributed framework [الموزَّع]**. In such a framework each party within a given group trusts some or all of the parties within this group. This means that every party within a group is either an IdP that is trusted by some or all members of this group, or an SP that trusts some or all of the IdPs within the group.

إدارة الهوية الرقمية على الويب – 4







نماذج تطبيقية – 1

- These models are defined in terms of the techniques used for user ***authentication*** and ***identification***.

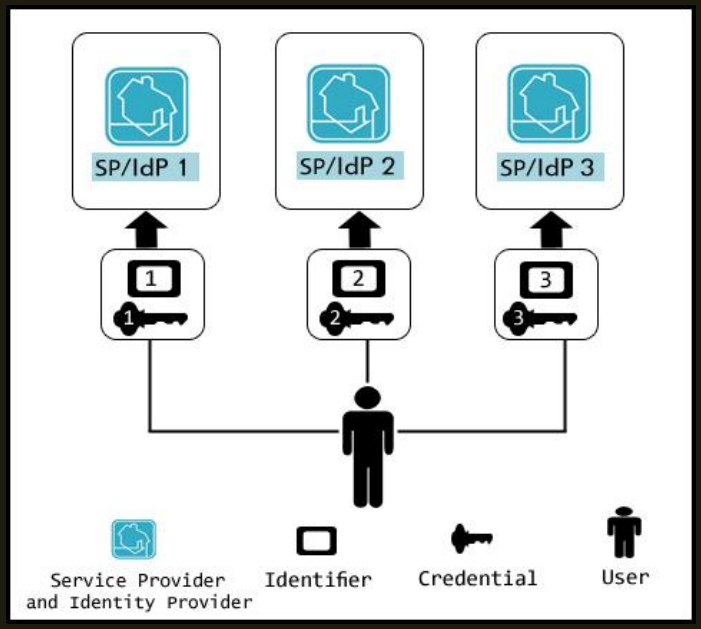
1. Isolated IDM. 2. Information Card-based IDM. 3. Federated IDM.

نماذج تطبيقية – 2

1. Isolated IDM.

An isolated identity management scheme is one in which there is no cooperation between parties for the purposes of user authentication. Historically, most Internet service providers operated isolated identity management systems. As a result, users were, and often still are, required to maintain a distinct identifier for each service provider.

Not fair?!



2. Information Card-Based IDM.

An Information Card-based identity management (ICIM) scheme (also known as a claim-based identity management scheme) is one which has the following properties:

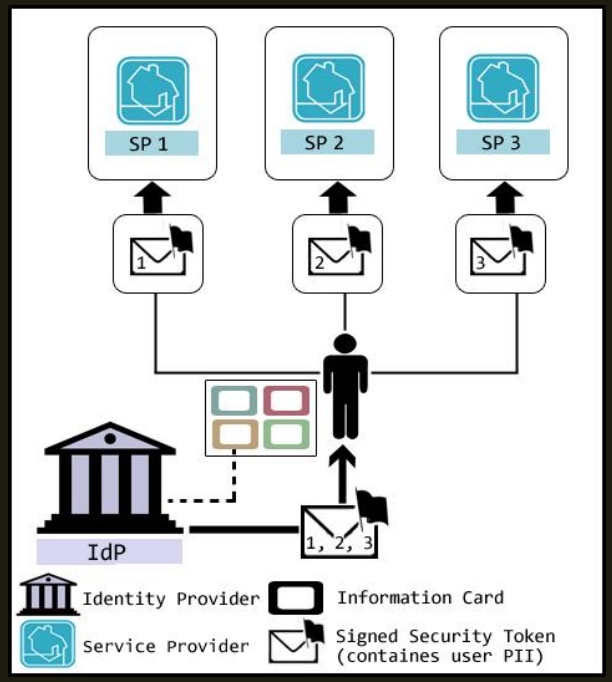
- for each IdP with which the user has a relationship, there is a defined set of claims, i.e. pieces of PII for which the IdP is prepared to generate an assertion;
- when using the system, the user is presented with a choice of IdPs using a 'card-based' user interface;
- at least one proof-of-rightful-possession method is supported;
- users are capable of asserting their own claims; and
- IdP discovery is performed on the user machine.

نماذج تطبيقية – 4

2. Information Card-Based IDM.

ICIM schemes have been designed to make identity management easier for Internet users; such schemes enable users to employ their IdP-asserted PII to identify themselves to SPs, instead of using service provider specific identifiers (e.g. usernames) and access credentials (e.g. passwords).

CardSpace, DigitalMe, Higgins, etc.



3. Federated IDM.

A Federated identity management (FIM) scheme is one which has the following properties:

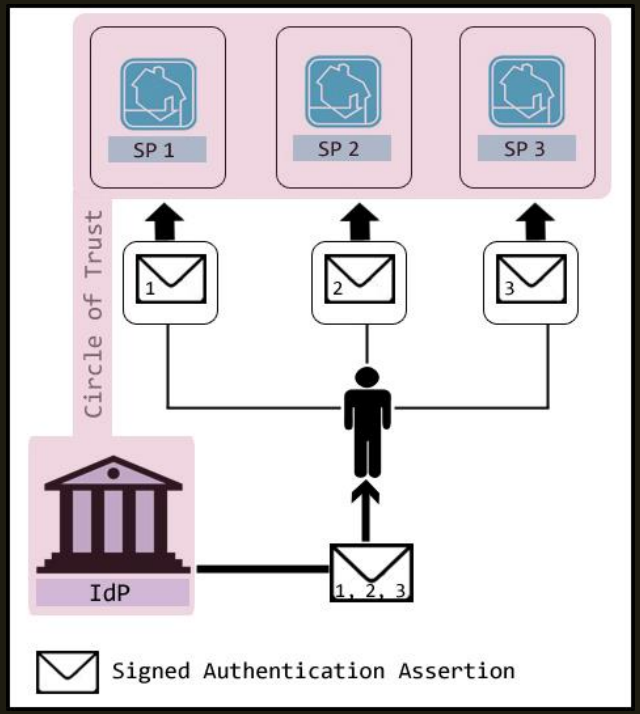
- identity federation process is supported, in which the user SP-issued identity is linked with the user IdP-issued identity;
- the use of public global identifiers is not supported;
- SSO is supported;
- the scheme is built on an open, standardised, communication framework (e.g. the SAML SSO profiles); and
- at least one proof-of-rightful-possession method is supported.

نماذج تطبيقية – 6

3. Federated IDM.

In a Federated identity management system, the user might have one or more ‘local’ identities issued by SPs, in addition to a single identity issued by the IdP within a specific domain called a circle of trust (CoT).

Liberty Alliance, Shibboleth, Ufed, etc.
OpenID?



نماذج تطبيقية – 7

- ICIM Vs. FIM.

Comparison Point	ICIM	FIM
Discovery of IdP	Performed on the user machine	Typically performed on the SP server
Pseudonyms	Used	Used
Identity federation	Not supported	Supported
Software enabling component on the user machine	Required	Typically not required
Self-issued assertions	Supported	Not supported
Single Sign-On	Not supported	Typically supported
Built on SAML SSO profiles	No	Yes
The IdP must be informed of all the accessed SPs	No	Yes
Proof-of-rightful-possession methods	Symmetric, Asymmetric, and Bearer	Holder-of-Key (Symmetric and Asymmetric), Sender-Vouches, and Bearer

أنظمة إدارة الهوية الرقمية

- الوقت؟
- للمزيد حول أنظمة الهوية الرقمية:

- **Waleed A. Alrodhan, *Digital Identity and Access Management: Technologies and Framework*. Chapters: Identity Management, Identity Management Systems;** IGI Global. State University of New York, Buffalo, NY, USA. 2011.
- **Waleed A. Alrodhan, Privacy and Practicality of Identity Management Systems:Academic Overview**; VDM Verlag Dr. Müller GmbH, Germany. ISBN 978-3639380255, 2011.

- And other stuff..

سَرِقَةُ الهُوِيَّةِ الرَّقَمِيَّة

تعريف ولمحة تاريخية – 1

- في حياتنا العامة، قد نضطر للخضوع لعمليات تحقق من قبل سُلُطات معينة أو مزودي الخدمات بغرض إثبات هوياتنا (باستخدام بطاقة الأحوال مثلاً).
- في العالم الرقمي، تحدث عمليات تحقق مماثلة لكن بوسائل أخرى (كلمة مرور، بطاقة ذكية، رمز التحقق الشخصي، الخ).
- سرقة الهوية تعني انتحال هوية كيان آخر (شخص آخر مثلاً) بأن يدعي السارق بأنه هو صاحب هذه الهوية، غالباً بهدف الوصول إلى معلومات أو خدمات معينة أو الحصول على مكاسب ومميزات خاصة بصاحب الهوية الشرعي. في حال تمت ممارسة أي عمل غير قانوني بهوية مُنتحلة، فإن صاحب الهوية الشرعي سيتحمل تبعات ذلك لاحقاً.
- عدد ضحايا جرائم سرقة الهوية في الولايات المتحدة الأمريكية في العام 2013م هو 11,571,900 شخص، وإجمالي الضرر يقدر بـ 21 مليار دولار (وزارة العدل الأمريكية).

تعريف ولمحة تاريخية – 2

- سرقة الهوية الرقمية تتأتى غالباً بثلاثة طرق:
  1. بالحصول على وسائل التحقق security credential من الهوية الرقمية (ككلمة المرور أو الهاتف الجوال مثلاً).
  2. بمعرفة كافة الخصائص والصفات والمعلومات الخاصة بالهوية المسروقة المسجلة في النظام الرقمي (مثلاً: رقم الهاتف أو الرقم الجامعي أو عنوان البريد، الخ).
  3. انتحال الهوية خارج النظام الرقمي للتسجيل في النظام الرقمي قبل صاحب الهوية الشرعي.
- الطريقة الأولى هي الأكثر شيوعاً، ويمكن تحقيقها من خلال وسائل تطفل كثيرة (مثلاً: الاصطياد phishing، الاستزراع pharming، الهندسة الاجتماعية social engineering، الخ.)
- سارق الهوية الرقمية سيعتبر تلقائيا من النظام الرقمي (الحاسوبي) حاملاً لكل الصفات والخصائص المسجلة للهوية الرقمية المسروقة.

تعريف ولمحة تاريخية – 3

- تم استخدام مصطلح سرقة الهوية لأول مرة في العام 1964م، على الرغم من أنه لا يمكن فعليا 'سرقة' هوية ما! (لذا هناك من يفضل مصطلحات أخرى مثل *انتحال الهوية*)
- على الرغم من أن قوانين كثير من دول العالم تجرم سرقة (أو انتحال) الهوية منذ سنوات طويلة وتنص على عقوبات رادعة لمرتكبي ذلك، مثلاً:
  - أستراليا: السجن 5 سنوات (Criminal Code Act 1995).
  - كندا: السجن لمدة أقصاها 5 سنوات (Criminal Code of Canada).
  - فرنسا: السجن لمدة أقصاها 5 سنوات وغرامة مالية ضخمة.
  - هونج كونج: السجن 14 عاماً (Theft Ordinance).
  - الولايات المتحدة الأمريكية: عقوبات مختلفة تتراوح ما بين 5 و 15 و 20 و 30 عاماً. يعتمد على القانون المطبق وسياق الجريمة.

فإن هذه الدول واجهت صعوبات تشريعية قبل أعوام في مواجهة جرائم سرقة الهوية الرقمية (بعضها إلى اليوم: محكمة نيويورك فبراير 2014: 165.45[2] و 155.30[4]).

- **المادة الرابعة من نظام مكافحة جرائم المعلوماتية السعودي:**

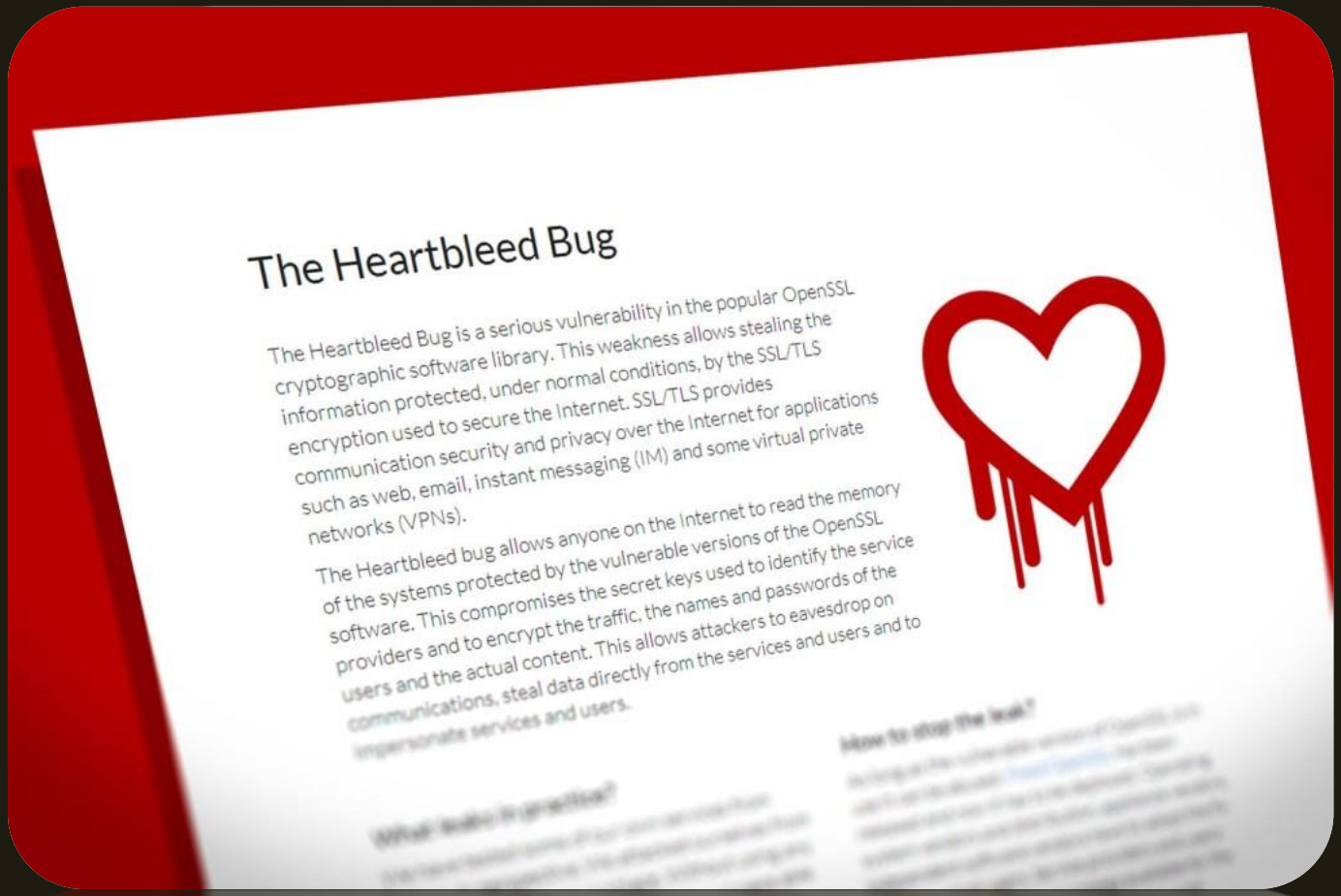
يعاقب بالسجن مدة لا تزيد على ثلاث سنوات وبغرامة لا تزيد على مليوني ريال، أو بإحدى هاتين العقوبتين؛ كل شخص يرتكب أياً من الجرائم المعلوماتية الآتية:

1. **الاستيلاء لنفسه أو لغيره على مال منقول أو على سند، أو توقيع هذا السند، وذلك عن طريق الاحتيال أو اتخاذ اسم كاذب، أو انتحال صفة غير صحيحة.**
2. **الوصول -دون مسوغ نظامي صحيح- إلى بيانات بنكية، أو ائتمانية، أو بيانات متعلقة بملكية أوراق مالية للحصول على بيانات، أو معلومات، أو أموال...**

أساليب السرقة

- الاصطياد و الاستزراع.
- الهندسة الاجتماعية.
- اختراق النظام.
- التجسس.
- أخرى.

الوضع الحالي



وسائل الحماية

- لا تضغط على أي رابط في رسالة إلكترونية.
- تأكد دائماً من عنوان الموقع في شريط العنوان في المتصفح.
- لا تدخل كلمة المرور في موقع غير مشفر (رمز القفل).
- لا تفشِ أسرارك الخاصة بوسائل التحقق لأي شخص!
- تعلم! (ما معنى شهادة رقمية وكيف يمكن التحقق من صحتها، مثلاً)
- لا تكن صيداً سهلاً: اختر كلمات مرور صعبة التخمين، ضع رمزاً سرياً لهاتفك وجهازك المحمول، استخدم مضاد للفايروسات، تخلص من الأوراق التي تحوي معلومات مهمة بطريقة حذرة، لا ترسل بياناتك الشخصية لأرملة المليارديير الإفريقي... الخ!
- IPv6 – DNSSec?

أسئلة؟

مركز
دراسات الجرائم المعلوماتية

شكراً جزيلاً