SAFE-BioPharma®

SAFE-BioPharma Association

Navigating the Identity Landscape

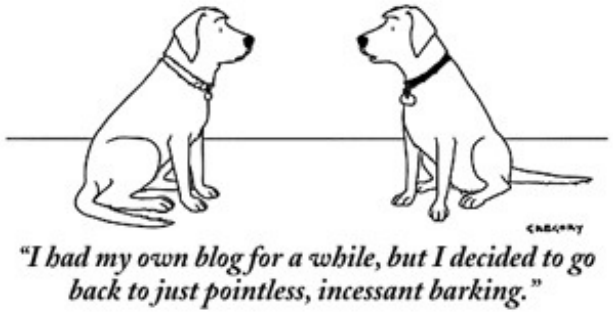
Rich Furr

Head, Global Regulatory Affairs and Chief Compliance Officer, SAFE-BioPharma Association

Overview

- An overview of US and EU government and industry-driven identity management initiatives to develop a trusted internet identity community.
  - types and levels of identity credentials and tokens,
  - government and industry organizations involved in establishing identity trust infrastructures,
  - applicable standards,
  - governance models, and
  - approaches to cloud based identity management

What is the big issue with the Cloud?



So who is the “dog”?

- The treasurer for John Edwards' 2008 presidential bid says the campaign has been electronically signing his name to federal spending reports without his knowledge and he wants it to stop.
- Campaign finance experts, including a former chairman of the Federal Election Commission, said there is nothing in the law that addresses whether Edwards' staff can use the treasurer's electronic signature affirm the accuracy of documents he has never seen
- the electronic signature has the same legal weight as a hand-written one, and using someone else's name on the form is the same as signing another person's signature
- It is not acceptable procedure to electronically sign the treasurer's name to an FEC report without the treasurer reviewing it and agreeing to have their name applied to it, because the treasurer is personally liable for any mistakes or false statements that are made in the report

SAFE-BioPharma®

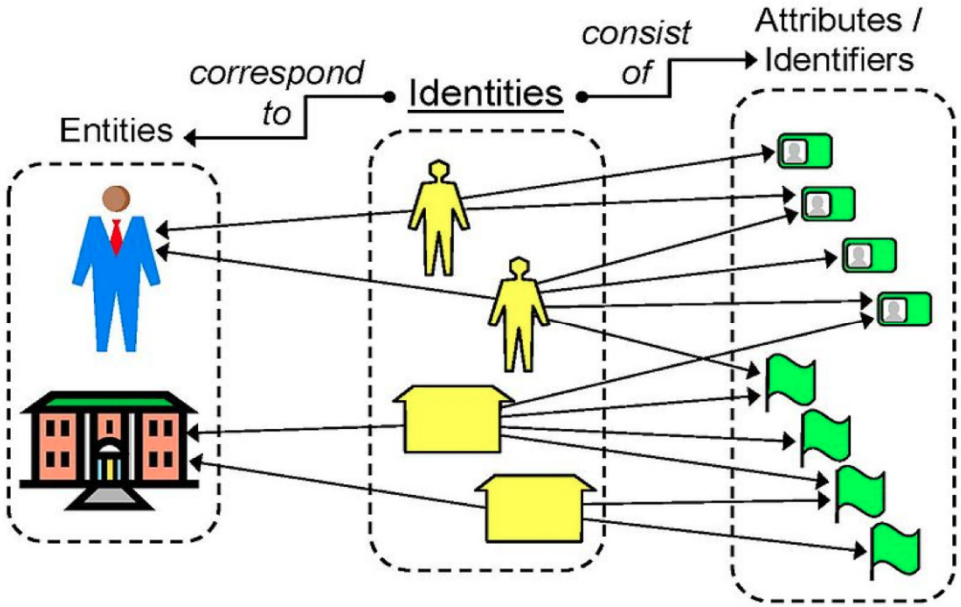
The Problem Today

Table 8. Top 15 Threat Action Types by number of breaches and number of records

	Category	Threat Action Type	Short Name	Breaches	Records
1	Malware	Send data to external site/entity	SNDATA	297	1,729,719
2	Malware	Backdoor (allows remote access / control)	MALBAK	294	2,065,001
3	Hacking	Exploitation of backdoor or command and control channel	HAKBAK	279	1,751,530
4	Hacking	Exploitation of default or guessable credentials	DFCRED	257	1,169,300
5	Malware	Keylogger/Form-grabber/Spyware (capture data from user activity)	KEYLOG	250	1,538,680
6	Physical	Tampering	TAMPER	216	371,470
7	Hacking	Brute force and dictionary attacks	BRUTE	200	1,316,588
8	Malware	Disable or interfere with security controls	DISABL	189	736,884
9	Hacking	Footprinting and Fingerprinting	FTPRNT	185	720,129
10	Malware	System/network utilities (PsTools, Netcat)	UTILITY	121	1,098,643
11	Misuse	Embezzlement, skimming, and related fraud	EMBZZL	100	37,229
12	Malware	RAM scraper (captures data from volatile memory)	RAMSCR	95	606,354
13	Hacking	Use of stolen login credentials	STLCRED	79	817,159
14	Misuse	Abuse of system access/privileges	ABUSE	65	22,364
15	Social	Solicitation/Bribery	BRIBE	59	23,361

Definitions

- **Identity –** A set of attributes that uniquely describe a person within a given context.



Picture: Copyright Audun Josang

Definitions

- **Credential** - An object or data structure that authoritatively binds an identity (and optionally, additional attributes) to a token possessed and controlled by a Subscriber.
- **Token** - registered with the CSP and is used to prove the bearer's identity. The token contains a secret the Claimant can use to prove that he or she is the Subscriber named in a particular credential
  - Something you know
  - Something you have
  - Something you are

Definitions

- **Identity Assurance -** In the case where the entity is a person, is the level at which the credential being presented can be trusted to be a proxy for the individual to whom it was issued and not someone else.
- **Federated Identity Management** amounts to having a common set of policies, practices and protocols in place to manage the identity and trust into IT users and devices across organizations.
- **Authentication** - The process of establishing confidence in the identity of users or information systems.

Levels of Assurance

- Assurance is defined as 1) the degree of confidence in the *vetting process* used to establish the identity of the individual to whom the credential was issued, and 2) the degree of confidence that the individual who uses the credential is the individual to whom the credential was issued.
- Four levels of assurance
  - LOA 1 – little or no confidence in the asserted identity
  - LOA 2 – some confidence in the asserted identity
  - LOA 3 – high confidence in the asserted identity
  - LOA 4 – very high confidence in the asserted identity

Type and levels of tokens

- Tokens may be single-factor or multi-factor
  - Single-factor Token – A token that uses one of the three factors to achieve authentication.
  - Multi-factor Token – A token that uses two or more factors to achieve authentication.
- Token types include:
  - Memorized Secret Token
  - Pre-registered Knowledge Token
  - Look-up Secret Token
  - Out of Band Token
  - Single-factor (SF) One-Time Password (OTP) Device
  - Single-factor (SF) Cryptographic Device
  - Multi-factor (MF) Software Cryptographic Token

Who are the players?

- **US Government**
  - US Federal Bridge Certification Authority for PKI
  - Federal Identity, Credentialing and Access Management for non-PKI
  - National Strategy for Trusted Identities in Cyberspace
- **EU**
  - ETSI SI TC – working with the EC to revise 1999 e-Signature Directive and include identity management
    - Feb 9th – first ever joint ETSI-US meeting in Reston, VA to coordinate with US IDM community
  - STORK - aims at implementing an EU wide interoperable system for recognition of eID and authentication that will enable businesses, citizens and government employees to use their national electronic identities in any Member State

Who are the players?

- **International Standards Development Organizations**
  - ISO – ISO Std 29115,
  - OASIS – trust elevation, cloud identity,
  - ETSI – as mentioned
  - ANSI - Identity Theft Prevention and Identity Management Standards Panel (IDSP)
- **US Trust Framework Providers (FICAM Certified)**
  - SAFE-BioPharma - LOA 2-3
  - Kantara – LOA 1-4
  - OIX – LOA 1
  - InCommon – LOA 1 & 2

Applicable Standards & Guidance

- **Draft ISO 29115 –** Entity Authentication Assurance Framework
- **NIST SP 8-00-63** - Electronic Authentication Guideline
- **OMB Circular 04-04 -** E-Authentication Guidance for Federal Agencies
- **EU Directive 1999/93/EC** – Community Framework on Electronic Signatures
- **Federal CIO Council** - Use of Electronic Signatures in Federal Agency Transactions

Trust Frameworks

- Framework - A combination of software mechanisms, contracts, and rules for defining, governing and enforcing the sharing and protection of information according to a common and independently verifiable standard of performance. Whenever possible, such governance mechanisms and contracts should be self-executing and self-correcting.
- Identity Trust Framework – the above applied to the management of identity information

SAFE-BioPharma®

SAFE-BioPharma Association

Governance

- **Bilateral agreements** – peer to peer trust based on agreement
  - Rapidly becomes unmanageable as number of partners grows
- **Trust Framework Provider** – provides the rules, processes and specifications against which IdP/CSPs are certified
  - May or may not include formal contracts for stakeholders (IdP/CSP, relying parties, subscribers)
    - SAFE-BioPharma is contract based and provides liability, dispute resolution and other stakeholder protections as part of the framework
    - Kantara – provides the rules, processes and specifications but is not contract based in terms of IdP/CSP or relying parties
  - May be open or closed
    - Closed – generally restricted to operate a small number specific vertical markets
    - Open – broader reach based on individual subscribers

SAFE-BioPharma Credentials

- **Four types**
  - PKI certificates are cross certified with the US Federal Bridge CA
  - non-PKI certified by FICAM
  - Basic Assurance – LOA 2 software certificate
  - Medium Assurance
    - Software
    - Hardware – USB token, EU qualified
    - ZFR – roaming certificate hosted on cloud based hardware security module; includes FICAM certified non-PKI LOA 3, 2-factor authentication credential

SAFE-BioPharma Identity Verification

- **Cloud-based service to perform LOA 2 & 3 proofing**
- **Multiple processes all approved by the US FBCA**
  - Face to face – notary and trusted agent
  - Antecedent – on-line and enterprise
- **Tightly binds assured identity to the credential**

Questions?

Contact information:

Rich Furr

rfurr@safe-biopharma.org

980-236-7576

704-575-1680