Security Standardisation, ENISA perspective

Giles Hogben, ENISA
Overview

- ENISA - introduction
- Interesting new developments in Social Networking/IDM
- Web 2.0 – Security challenges
- Resilience of telecommunications networks – the challenge of getting standards implemented – ENISA experiences.
Key Facts

eEurope 2005 Action Plan → set up in 2004 by EU Regulation

Operational since September 2005 in Heraklion, Greece

~50 Staff

~34.8 M€ for 5 years
ENISA’s Role

... maintain internal expertise, at the disposal for EU and Member State competent bodies (respond to Requests and Calls for Assistance)
ENISA Standardisation Role

- Security Standardisation Roadmap, (with ITU) [http://enisasec.notlong.com](http://enisasec.notlong.com)
- eID directory [http://enisaIDDir.notlong.com](http://enisaIDDir.notlong.com)
- Contributions from Risk-assessment studies
  - Member of W3C, OASIS
  - Liaison- co-operation with
    - ITU (FG-IDM, Security Standards Portal),
    - ETSI
    - CEN/CENELEC (European Citizen Card)
ENISA Activities for 2008 and beyond

Current focus on:

- Identifying Emerging Risks
- Improving Resilience in European e-Communication Networks
- Co-operation between Member States
- Building information confidence with Micro Enterprises
Emerging Risk Activity

Identifying Emerging Risks for creating trust and confidence – topic areas

- Social networking
- Reputation systems
- Mobile eID
- Web 2.0
- Virtual Worlds and Gaming
- Virtualisation security
- eID interoperability (e.g. privacy features of eID cards)
Social Networking
Social Networking is now an Identity Management System

• Storage of Personal Data
• Tools for managing personal data and how it’s viewed
• Access control to personal data based on credentials.
• Tools for finding out who has accessed personal data.
Identity Management System

• **Storage of personal data**
  • Tools for managing personal data and how it’s viewed
  • Access control to personal data based on credentials.
  • Tools for finding out who has accessed personal data.
Social Networking is an Identity Management System.

LOTS of Juicy Personal data:

Recognise these from somewhere?

(a) Racial or ethnic origin
(b) Political opinions
(c) Religious beliefs
(e) Physical or mental health or condition
(f) Sex life

(EU Directive 95/46 – definition of sensitive personal data)
Identity Management System

• Storage of Personal Data
• **Tools for managing personal data and how it’s viewed**
• Access control to personal data based on credentials.
• Tools for finding out who has accessed personal data.
Tools for Organising my personal data
Identity Management System

- Storage of Personal Data
- Tools for managing personal data and how it’s viewed

**Access control to personal data based on credentials.**
- Tools for finding out who has accessed personal data.
Social Networking Provides Access Control
Tools for managing access based on credentials

Privacy

Profile
Control who can see your profile and personal information.

Search
Control who can search for you, and how you can be contacted.

News Feed and Mini-Feed
Control what stories about you get published to your profile and to your friends’ News Feeds.

Applications
Control what information is available to applications you use on Facebook.

Block People
If you block someone, they will not be able to search for you, see your profile, or contact you on Facebook. Any ties you currently have with a person you block will be broken (friendship connections, relationships, etc.).
Lock-in – the Hotel California effect.

“Social Networking is like the Hotel California. You can check out, but you can never leave”

Nipon Das to the New York Times
Leaving the Hotel California?

- No export facility
- Caches
- Internet archives
- “Disactivation” of the account
- Delete comments from other people’s walls?
• Economic success is inversely proportional to strength of privacy settings.
Attacking the root cause

• Break data monopolies to improve privacy and security:
  – Standardised portable networks (leaving the Hotel California and going to another one)
  – PLUS Portable, standardised access-control and security (with a secure briefcase).
Nice idea but where's the business model?
Important new developments in social applications

- The big players embrace data portability and portable authentication...
- Social Networking takes another step in the direction of IAM.
Grow traffic when friends connect on your site

Google Friend Connect lets you grow traffic by easily adding social features to your website. With just a few snippets of code, you can connect deeply with your site.

Attract more visitors. Visitors bring along friends from social networks, encouraging others to interact on your site.

Enrich your site with social features. Choose engaging social features from gadgets provided by Google and the OpenSocial developer community.

No programming whatsoever. Just copy and paste snippets of code. Google Friend Connect does the rest.

Please note: this is a preview release. Google Friend Connect is being made available to a limited number of site owners as it approaches full release. If you are interested in participating, please fill out this short form. You will be notified if you are approved as a partner.

Copyright © 2008 Google, Inc.
Based on open FIM compatible specs
Google Friend Connect

- Sign-in with an existing account (Google, Yahoo, OpenID...)
- Invite and show activity to existing friends from social networks (Facebook, Google Talk...)
- Browse member profiles across social networks
Announcing Facebook Connect

12:32pm Friday, May 9
Published by Dave Morin

At Facebook, we're committed to enabling people to communicate and stay connected wherever they go.

In August 2006, we introduced the first version of the Facebook API, enabling users to share their information with the third party websites and applications they choose. Hundreds of companies have leveraged these APIs, allowing users to dynamically connect their identity information from Facebook, such as basic profile, friends, photos information and more, to third party websites, as well as desktop and mobile applications.

In May 2007, we launched Facebook Platform, which allowed third party developers to build rich social applications within Facebook. More than 350,000 developers and entrepreneurs from 225 countries have signed up, and started developing applications, and have seen significant adoption by Facebook users worldwide.

Today we are announcing Facebook Connect. Facebook Connect is the next iteration of Facebook Platform that allows users to "connect" their Facebook identity, friends and privacy to any site. This will now enable third party websites to implement and offer even more features of Facebook Platform off of Facebook – similar to features available to third party applications today on Facebook.

Here are just a few of the coming features of Facebook Connect:

**Trusted Authentication**
Users will be able to connect...
Here are just a few of the coming features of Facebook Connect:

**Trusted Authentication**
Users will be able to connect their Facebook account with any partner website using a trusted authentication method. Whether at login, or anywhere else a developer would like to add social context, the user will be able to authenticate and connect their account in a trusted environment. They control the permissions granted.

**Real Identity**
Facebook users represent themselves with their real names and real identities. With Facebook Connect, users can bring their real identity information with them wherever they go on the Web, including: basic profile information, profile picture, name, friends, photos, events, groups, and more.

**Friends Access**
Users count on Facebook to stay connected to their friends and family. With Facebook Connect, users can take their friends with them wherever they go on the Web. Developers will be able to add this social interaction.
MySpace Embraces Data Portability

By HEATHER HAVENSTEIN, Computerworld, IDG
Published: May 8, 2008

MySpace Thursday unveiled its response to one of the most contentious issues surrounding social networking - information portability with a new project that allows its users to share content from their profiles with any Web site.

The new MySpace Data Availability project is its first in a series of initiatives by the company to support data portability, allowing users to take the content they create in one network and easily add it to other sites, MySpace said. Until now, social networking sites like MySpace have favored the "walled garden" approach, where they essentially lock their users into their own site.

MySpace said that it has signed agreements with Yahoo, eBay, Photobucket and Twitter to participate in the project. Over the next several weeks, MySpace users will be able to add their MySpace data to those sites with the click of a button, noted Chris DeWolfe, CEO and co-founder of MySpace.

"We are pioneering a new way for the global community to integrate their social community experiences Web wide," DeWolfe said. "Today MySpace no longer operates as a closed system using proprietary protocols to communicate. We are embracing the open Internet and allowing users to share their content with other sites and services through the MySpace Data Availability project."

"We're excited to team up with MySpace and participate in the MySpace Data Availability project," stated YouTube president Susan Wojcicki. "The open Internet has always been a core philosophy at YouTube, and we believe this project is a significant step forward in making the Web a more open and connected experience for all."

More news from IDG
• CIO - Business Technology Leadership
• Computerworld - News & Top Stories on Software, Hardware, Windows & VOIP
• InfoWorld - Get Technology Right
• Network World - Software, Hardware, Electronics & Gadgets
• The Industry Standard

More Articles in Technology »

Travel Deals e-mail newsletter
Sign up for travel deals and discounts on airfare, hotel, transportation and more!

See Sample | Privacy Policy

Content from this site web site is blocked.
ad.doubleclick.net

Please contact ENISA IT Support if you need assistance. Thank you.
Or does it?
Web 2.0

★ The Browser has become an Operating System in its own right.

★ It shares many characteristics with a virtual machine.

★ Browser is probably used more than any other feature of underlying OS.
Web 2.0 Security Challenges

May 2007 / May 2008 Scansafe State of the Web Comparative

- The volume of threats confronting web surfers has increased 220%
- Risk of exposure to exploits and compromised web sites increased 407%
- In May 2008, 68% of Web-based malware exposure was via compromised web sites
Web 2.0 Patterns - Syndication

- Information may be syndicated (e.g. using RSS) and altered many times from its original source, making provenance, control and pedigree of information difficult to trace.

Diagram:
- Source 1
- Source 2
- Source 3
- Browser
Web 2.0 patterns - Collaborative Content

Information which appears as a single source or article is edited by multiple (possibly unnamed and untraceable) users.
Web 2.0 Patterns - Embedded Widgets and XMLHttp

★ One page contains content and even executable code from multiple sources communicating with multiple servers.

[Diagram showing interactions between Server 1, Server 2, Widget 1, Origin Domain 1, Widget 2, Origin Domain 2, communicating with Server 1, Server 2.]
Sticky Access Control Policies – data exported and exchanged between different services must maintain access control rules.
Web 2.0 Patterns - Authorisation for services

★ Authorisation and access delegated to services
Web 2.0 – other interesting features for security

- Information and executable code sources are likely to be from private individuals.

- Developers with security training are very few!

- Trust in information is established through user-votes and reputation systems rather than brand names or PKI.
Web 2.0 Challenges for Access Control Standards

- “Same-origin” policy doesn’t work so well in Web 2.0.
  - Multiple “widgets” in a single browser context need to communicate across domains =>
  - Developers forced to circumvent access restrictions
  - Multiple loopholes - opens users up to attacks (CSRF) but no other basis available for protecting resources.
Web 2.0 Authorisation Challenges

★ E.g. Delegate Access to Email/Bank account
  ★ For limited period
  ★ To limited fields
  ★ Specify who authorisation can be passed to
  ★ I can trace it if it something goes wrong
Web 2.0 and Information Pedigree

- The difficulty of tracing “information pedigree”
  - Pump and dump stocks
  - Astro-turfing (adverjournalism)
  - Political fraud
  - Fraudulent factual information
Resilience

The ability of a system to provide & maintain an **acceptable level of service** in face of faults (**unintentional, intentional, or naturally caused**) affecting normal operation.
ENISA Resilience Work – Background Info

★ Objectives
- Analyze current and emerging technologies used by network and service providers to enhance the resilience of their operations

★ Scope
- IP backbone technologies

★ Target Group
- Regulators and Policy Makers
- Operators
- Vendors
Selected Technologies – to improve resilience

- **IPv6**
  - OSI Layer 3 technology replacing IPv4
  - Action Plan for the deployment of Internet Protocol version 6 (IPv6) in Europe

- **MPLS**
  - OSI Layer 2.5 technology
  - Used by operators in IP backbones, replacing Frame Relay and ATM

- **DNSSec**
  - A technology improving the security of Domain Resolution Service
Standards uptake

★ What policy measures can foster uptake (E.g. IPV6, DNSSec, MPLS, ECC)?

★ **Economic incentives** – who wants to go first – e.g. funding of pilots.

★ **Government takes liability** – e.g. For identity infrastructure, DNS security.

★ **Lead by example** – implement in government systems.

★ **Release from reporting obligations.**
Uptake – standards need to make choices

★ A standard which has every possible feature but is too complex to implement or understand will not fly.

http://www.flickr.com/photos/nathansnyder/4971360862/
Uptake – half-compatible standards

★ Many half-compatible standards

★ E.g. In Mobile eID area, NFC/ISO 14443A/ISO 14443B not compatible
Take Home Messages

★ Social networking applications are becoming big players in the Identity Management Space
  ★ Importance of portable formats
  ★ Access and Authorisation is a key piece of the puzzle
★ The browser is the new OS
  ★ Fixing access control and authorisation is URGENT!
★ Standards uptake (e.g. For network resilience) needs economic and policy incentives to foster take-up.