http://www.EICAR.org

Building Trust and Confidence One Step at a Time - eTEN/CASES

CASES

Cyberworld Awareness and Security Enhancement Structure

http://security.weburb.net/frame/EWISdoc/CASES.html

Professor Urs E. Gattiker, Ph.D.

- **Member of the Board --• EICAR**
- **Scientific Director - EICAR**
- **Aalborg University**

CASES

What is CASES and e-TEN? Objectives

Cyberworld

Awareness and Security

Enhancement Structure

Today's Plan

- **Cases intends to provide the following deliverables:**
  - **- Verification** of warnings and alerts (e.g., malicious code, attacks)
  - **- Technical** analysis
  - - Education/**best practices** material for target groups/markets
  - - Providing threat/statistical assessment using **operational indicators**
- **National nodes link within a country**
- **No new structure or organisational form**
  - **– build on what we have but leverage it better**
- **Managed by EU Member States => *e*TEN**

CASES Who Will Manage - Structure Buck Stops Here

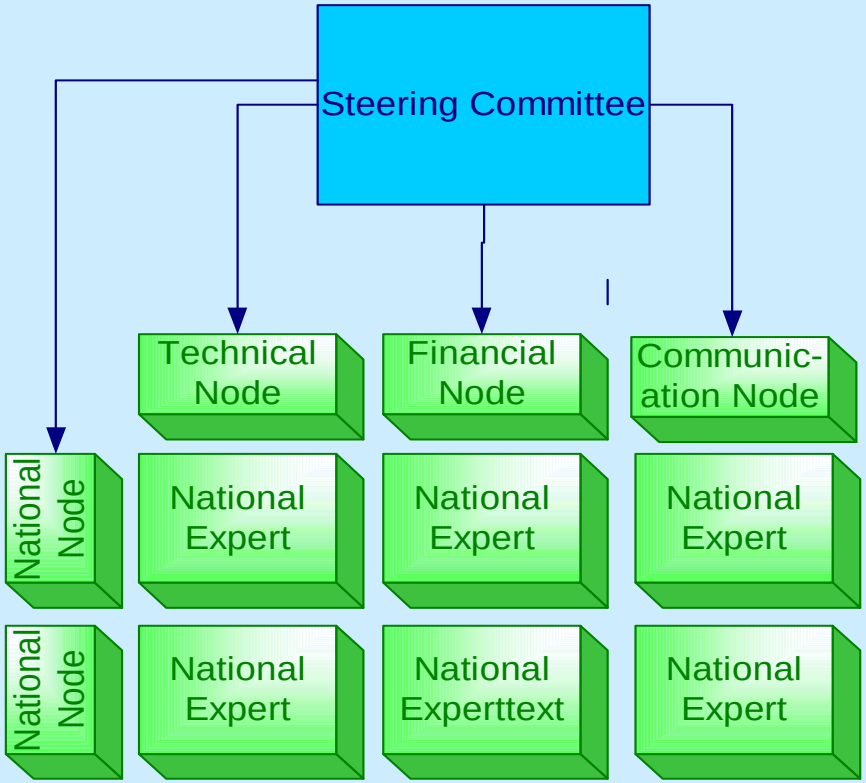
Cyberworld

Awareness and Security

Enhancement Structure

- **National Nodes**
  - 2-3 experts, one technical
- **Technical Node**
  - 6-10 experts
  - virtual?
- **Communication Node**
  - .5 people
- **Financial Node**
  - .5 people

Matrix Structure for CASES



Note. Steering Committee has functional authority over CASES. Technical, Financial and Communication Nodes are advisory, line authority comes from National Node

Planned Activities - *eTEN*

Cyberworld

Awareness and Security

Enhancement Structure

Tomorrow - 2003 - Market Evaluation

Verify - What for?

Is Communicating not Good Enough?

NOT !!

CASES

Cyberworld

Awareness and Security

Enhancement Structure

If CERTS already do the Technical Work and Verification Tasks-?

- about malicious code, vulnerabilities, and software bugs – being able and doing is different --

WHY :

1) do nations than want to participate in EWIS and CASES approaches?

2) are CERTs not working closely with AV industry?

3) are CERTs not looking into

  - "unified naming convention",
  - central database on malicious code

- are CERTs unable to produce?
  - **standardized statistics about who reported what and**
  - **the type of vulnerabilities/threats we have, thereby allowing benchmarking?**

CASES

Cyberworld

Awareness and Security

Enhancement Structure

If CERTS already do the Technical Work and Verification Tasks-?

If nations are claiming they have this capability already, it is their choice to integrate it into CASES.

CASES is more than CERT,

but CERTs play a central role within CASES.

CASES

Cyberworld

Awareness and Security

Enhancement Structure

Achievements and Milestones 2004

- **Begin with full roll-out -awareness**
- **Co-ordinate with FP6 research efforts to integrate new tools**

- **Expand technical excellence and combine with standard work**
- **Benchmark and compare progress toward *e*Europe trust, confidence and “security culture” targets**

*e*Health, IPv6, G3 - Pervasive Computing - Field Test Needed

- **accelerate use of IPv6 in health settings**
- **field test**
  - **IPv6, G3, hospital, ambulances, households**
    - security
    - privacy
- **doctors or medics gets info about patient (e.g., allergies, heart condition) via mobile**
    - sending images from accident site back to emergency ward
    - data exchange with patient at home
- **CASES - supporting field test - social/security**
    - hacker attacks
    - viruses

Conclusion

- IPv6, G3, *e*health field test in **collaboration** with CASES should provide information about:
  - feasibility (technology, medical personnel and patients),
  - social issues, and
  - security threats (technical and social!)

eEurope 2005 Action Plan:

able to benchmark & compare countries' progress on security and trust toward a culture of security using:

- **IPv6**
- **G3, and**
- **pervasive computing**

IPv6 Task Force - Mandate?

Cyberworld

Awareness and Security

Enhancement Structure

- **World of computing is hierarchical**
  - servers are the bourgeoisie, enjoying power & status at the center of the networked world
  - clients (e.g., PCs, PDAs, & mobile phones) sit at the edge of the network, the disenfranchised proletariat

- **IPv6 - everybody in the network has equal status**
  - every device is a “peer” and
  - each peer is free to request or provide services to any other
  - your milk will know how old it is (radio frequency identification)

Commissioner Erkki Liikanen: What is our Mandate?

It Should Include:

- Wealth - power - influence -Are there only winners?
  - Automotive,
  - e-commerce,

could this maybe mean:

  - outstrip people's ability to adapt,
  - digital divide,
  - privacy out the window?

CASES

Cyberworld

Awareness and Security

Enhancement Structure

Conclusion

What Do CASES and IPv6 have in Common?

- **Relying on good judgment means:**
  - **a good decision implemented immediately is better,**
  - **than a perfect decision implemented late.**

Hence, Mandate Should Include:

CASES', IPv6 Field Studies AND

IPv6 Vision - What IF

eEurope 2005 and IPv6: Building Trust and Confidence

Professor Urs E. Gattiker, Ph.D.

- **Get the Facts:**

- **http://security.weburb.net/frame/EWISdoc/CASES.html (CASES docs)**
  - **http://www.ten-telecom.org (*e*TEN - CASES)**
- **http://security.WebUrb.net/frame/EWISdoc/eHealthIPv6.html (IPv6 & *e*health)**
  - **http//security.weburb.net/frame/newsletters/other/information_security.html**

CASES – Data – Verification – Benchmarking – Trends → Communication

To: Information Security This Week subscribers <securitynews-news@/"
EUDORA="AUTOURL"www.weburb.dk>
Subject: Information Security This Week 2002/36
From: Newsletter service <newsletter@weburb.net>
Reply-To: newsletter@weburb.net

To subscribe: security-subscribe@News.WebUrb.dk
To unsubscribe: security-unsubscribe@News.WebUrb.dk
Newslwetter-Archive:
<http://security.weburb.net/frame/newsletters/other/information_security.html>

****
INFORMATION SECURITY THIS WEEK ISSN:1600-1869
Fridays: IT Infrastructure Protection News - Providing Analyses and Sources
News from http://Security.WebUrb.net
in collaboration with http://www.EICAR.org
September 6, 2002 Vol.3 No.33
Urs E. Gattiker(Editor)
****
~~~~~~~~~~~~~~~~~~~~~~~~~~~

02 Sep 2002 - **Is Spam Really as Big a Problem as these Figures Suggest?**

Recently some data have been circulating claiming that during July, spam in the USA made up **36% of** email traffic, 36%!? The news item claims that spam could make up the up the majority of message traffic on the Internet by the end of 2002. Apparently this figure is up from 8% in July 2001. So we tried to follow this trail of information and tracked it to cNet that run this story last week.

<http://freebies.weburb.net/newsservice/link/2785/http://news.com.com/2100-1001-955842.html>

Than we searched the Websites of both sources cited in the story, namely

- Brightmail - nothing on website to back up Enrique Salem, CEO of anti-spam service provider Brightmail
- Postini - had a story on the Website (dated Aug. 13)

<http://freebies.weburb.net/newsservice/link/2785/http://www.postini.com/products/dha_wp.pdf>

But even in this story there is little to be learned about the following facts:

- sample characteristics (e.g., location of clients, what type of clients, number of e-mails, etc.)
- descriptive satistics (e.g., mean, standard deviation)

If any of our readers have such information from another study, their own data or whatever, please let us know we would gladly put something in Information Security this Week.

We feel that such **claims without data backup give the security profession a bad name**, you be the judge. Maybe these firms are too busy trying to get business but does this mean a **cNet journalist has to fall for it?**

See also related stories about EU efforts regarding spam.
RELATED STORIES:
The Directive on Privacy and Electronic Communication - Deadline October 31, 2003
- http://security.weburb.net/show/news/2765

The Directive on Privacy and Electronic Communication - Deadline October 31
- http://security.weburb.net/show/news/2754
~~~~~~~~~~~~~~~~~~~~~~~~~~~

CASES – Data – Verification – Benchmarking – Trends → Communication

Hoax.....Verification is the Key to CASES' Success!

Subject: Information Security This Week 2002/35

30 Aug 2002 - Vnunet - in the Doghouse - Did DDOS Attacks Double?

This Tuesday Vnut published an online article about the number of high-profile distributed denial of service attacks. The story stated that in the first seven months of 2002, **DDOS were being reported as having reached more than twice as a high level as all of last year.**

In the article a Neil Barrett was cited trying to explain why the numbers had increased so much. A follow up with his firm revealed that the consultancy Information Risk Management just felt that the **large increase was due to more high-profile companies reporting incidents**.

Neither a request about data sources to Vnunet nor Neil Barrett produced a response by this Friday 1AM GMAT. Claims are easy to make but do they really help? Maybe you should refrain from choosing this firm?...

<http://freebies.weburb.net/newsservice/link/2768/http://www.irmplc.com/>

Nonetheless, searching on Google brought a surprising amount of other information sites having linked to the article that borders on a hoax or lacks being based on facts.

Is There A Link B/W Autism and Hacking?

Another story in Vnunet this week claimed that sophisticated **hackers may be suffering from Asperger's syndrome, a neurobiological disorder that resembles mild autism**. This was attributed to researchers at **Cambridge University**. We followed up and nobody in the autism group at Cambridge apparently had any idea about this 'research.'

But somebody else did namely Tony Attwood who answered us:
'The article which you refer to was based on a telephone conversation with a journalist and based on my extensive clinical experience of Asperger's Syndrome rather than a research study on this specific topic.'

We asked: "...what you are saying is that you have **no scientific proof for your statement its just a hunch, correct**?'

To which he answered: 'Yes, **a hunch** based on the cognitive and personality profile of adults with Asperger's disorder.'

<http://freebies.weburb.net/newsservice/link/2768/http://www.atwood.com>

Vnunet goofed twice with this story:

- taking a researchers hunch selling it as scientific fact, and
- being **sloppy by attributing it to a university** which had nothing to do with it (trying to beef up credibility maybe?)

How can we trust news when they are researched so sloppely? And what about Attwood.com, can we trust his research when he makes such outrageous claims? NO, there is no study that shows a link between autism and hacking, simply false!

But this raises another question, should we continue reading Vnunet? You be the judge :-))

September 12, 2002

From: Professor Dr. Urs E. Gattiker, EICAR and Aalborg University, Denmark
Dr. Inger Marie Giversen (MD), The National Board of Health, Denmark

RE: **Electronic Medical Records, e-Health & Information Networks: Security Issues with Internet Protocol version 6 (IPv6) – eEurope 2005 –e-TEN program**
http://europa.eu.int/information_society/eeurope/action_plan/index_en.htm

The implementaton of electronic medical information systems (**EMISs**), electronic medical records (**EMRs**) and medical databases (**MDBs**) in health care calls for the solution of a wide range of problems, among which security issues constitute but a few (Urs E. Gattiker and Inger Marie Giversen: The Digitized Health Service. A Theoretical Framework for Public Administration. In E. Vigoda: **Public Administration. An Interdisciplinary Critical Analysis**. Marcel Dekker, 2002). Addressing security matters, however, is a precondition for the acceptance of the systems in the medical profession, among legislators and above all in the general public. The introduction of EMRs in Denmark as in the rest of the European Union (EU) is scheduled for the year 2005 according to the eEurope – Action Plan. Addressing the security issues is thus both an important and a very urgent matter to assure citizens' trust and confidentiality in governments' e-health efforts including providing access to patient files online.

At the same time, the new Internet Protocol version 6 (IPv6) and wireless technology (e.g., UMTS/G3) will make it feasible to enable devices with IP addresses at many locations. Accordingly, the physician at an accident site may transfer data to the emergency ward at a nearby hospital using UMTS/G3 mobile technology with IPv6 (device to device communication). E-health will bring many new benefits to health professionals and patients alike but only, if wireless technology and IPv6 applications are done in such a way to assure the best possible level of confidentiality, integrity, availability and accountability (**CIAA**) regarding medical information and databases.

An effective plug and play implementation at homes, hospitals and in telecommunication networks, while maintaining satisfactory security levels for the patients and health information networks, must be realized. However, various steps are needed and must be implemented for taking full advantage of the end-to-end security and communication benefits IPv6 offers compared to Network Address Translation (NAT) while taking advantage of UMTS opportunities.

At this stage we have yet to address these matters and to iron out the security issues including infrastructure design and implementation challenges. We also need to carefully think about the **social and political impacts of such change.**We feel a pilot project about the possible roll-out with UMTS and IPv6 would offer the best possibilities to see how things might work out before large-scale systems will be implemented. The **pilot project** possibly initiated by Member States using the EC's **e-TEN** (http://www.ten-telecom.org) should address

- how **IPv6 implementation** with **UMTS technology** will enable to access e-health information (e.g., medical staff at accident site, transferring data and video via mobile);
- patients at home communicating with hospital staff or **general physician**, checking **personal health records** on-line, entering data and transferring data;
- social impacts including **digital divide** issues

The above encompasses issues of adding and changing data, while making sure that the CIAA of medical databases is maintained in an environment where **pervasive computing is ubiquitous**. Moreover, how this may change health care delivery (e.g., more home-care versus other) should be considered including social issues.

EICAR Office Denmark
Islands Brygge 24A, 4., 1.
2300 Copenhagen S.
Denmark

Tel: +45 3295 5090 or +45 222 111 40
Fax: +44 (0)70 92376036 (dial 2, send)
http://www.EICAR.org or http://Conference.EICAR.org
http://Research.WebUrb.dk/?Urs

Appendix

The security issues can be divided into four categories:

Confidentiality, integrity, availability and accountability (**CIAA**).

Confidentiality means that information entered into an EMR is not disclosed to unauthorized parties. Confidentiality is the basis of trust between doctor and patient. If confidentiality cannot be ensured, the patient may choose to withhold information from the doctor with the inevitable risk of endangering the correct diagnosis and treatment. Needless to say, the multiplication and easy spread of information from computer to computer gravely endangers the confidentiality. The decision to implement Internet protocol version 6 (Ipv6) enhances the danger further, since Ipv6 makes it possible to connect apparatus and machinery wirelessly to EMIS and thus facilitates the hacking into EMIS.

Integrity of information means the information has not been altered or modified in an unauthorized manner. The security issue is to prevent unauthorized staff or others to alter information. Also, addition, deletion and changes of information made by authorized staff must be tracked and kept in record.

Accountability for information means that medical personnel must provide identification for accessing the EMRs and for entering and using information in the EMRs.

Availability of information means that the information is accessible and useable as required to perform the necessary tasks relating to diagnosis, treatment, nursing, physical rehabilitation (EMRs) and research (EMRs and MDBs).

Revision History

2002, August 3: Initial draft

2002, August 20, Updated – editing and incorporating of input from various experts [http://Security.WebUrb.net/frame/EWIS.html]

2002, September 12 : Initial release