EGI Incident Response Task Force

Leif Nixon

Coordinator, Incident Response Task Force

September 14, 2010

What has happened thus far?

- Lots of boring stuff

What has happened thus far?

- Lots of boring stuff
- Incident handling procedure – seven pages of preamble (abstract, copyright, executive summary); two pages of actual content

What has happened thus far?

- Lots of boring stuff
- Incident handling procedure – seven pages of preamble (abstract, copyright, executive summary); two pages of actual content
- Mailing lists; how many should there be, what should they be called, who should be on them, which issues should go where

What has happened thus far?

- Lots of boring stuff
- Incident handling procedure – seven pages of preamble (abstract, copyright, executive summary); two pages of actual content
- Mailing lists; how many should there be, what should they be called, who should be on them, which issues should go where
- Some interesting stuff; 3–4 incidents (depending on how you count)

Statement #1

Type: Pompous

What we do is important.

Statement #1

Type: Pompous

What we do is important.

Fundamental research is important. Scientic computing is important.

Statement #1

Type: Pompous

What we do is important.

Fundamental research is important. Scientic computing is important.

But there are people out there trying to interrupt it.

Statement #1

Type: Pompous

What we do is important.

Fundamental research is important. Scientic computing is important.

But there are people out there trying to interrupt it.

We're here to stop that.

Statement #2

Type: Controversial

There ain’t no such thing as grid security.

Statement #2

Type: Controversial

There ain't no such thing as grid security.

From an operational standpoint, at least. A rooted system is a rooted system, no matter the entry vector.

Statement #2

Type: Controversial

There ain't no such thing as grid security.

From an operational standpoint, at least. A rooted system is a rooted system, no matter the entry vector.

We're not protecting the grid software – we're protecting the *infrastructure*.

Statement #2

Type: Controversial

There ain't no such thing as grid security.

From an operational standpoint, at least. A rooted system is a rooted system, no matter the entry vector.

We're not protecting the grid software – we're protecting the *infrastructure*.

For the infrastructure, a stolen ssh password can be as harmful as a stolen certificate – we can't limit ourselves to just the "pure" grid systems.

Statement #2

Type: Controversial

There ain't no such thing as grid security.

From an operational standpoint, at least. A rooted system is a rooted system, no matter the entry vector.

We're not protecting the grid software – we're protecting the *infrastructure*.

For the infrastructure, a stolen ssh password can be as harmful as a stolen certificate – we can't limit ourselves to just the "pure" grid systems.
We must apply a holistic view on security.

Statement #3

Type: Braggy

We're doing something new.

Statement #3

Type: Braggy

We’re doing something new.

For natural reasons, classic non-grid CSIRTs are hierarchically organized.

Statement #3

Type: Braggy

We're doing something new.

For natural reasons, classic non-grid CSIRTs are hierarchically organized.

We, on the other hand, are a lateral organization.

Statement #3

Type: Braggy

We're doing something new.

For natural reasons, classic non-grid CSIRTs are hierarchically organized.

We, on the other hand, are a lateral organization.

We have different perspectives and complement each other.

Statement #3

Type: Braggy

We're doing something new.

For natural reasons, classic non-grid CSIRTs are hierarchically organized.

We, on the other hand, are a lateral organization.

We have different perspectives and complement each other.

Good cooperation with classic CSIRTs is critical.

Looking forward

Things we want to get better at:

- Communication – streamlined, secure, efficient channels.

Looking forward

Things we want to get better at:

- Communication – streamlined, secure, efficient channels.
- Vulnerability assessment – identifying and classifying security holes

Looking forward

Things we want to get better at:

- Communication – streamlined, secure, efficient channels.
- Vulnerability assessment – identifying and classifying security holes
- Following up on unpatched sites – tools, policies, procedures