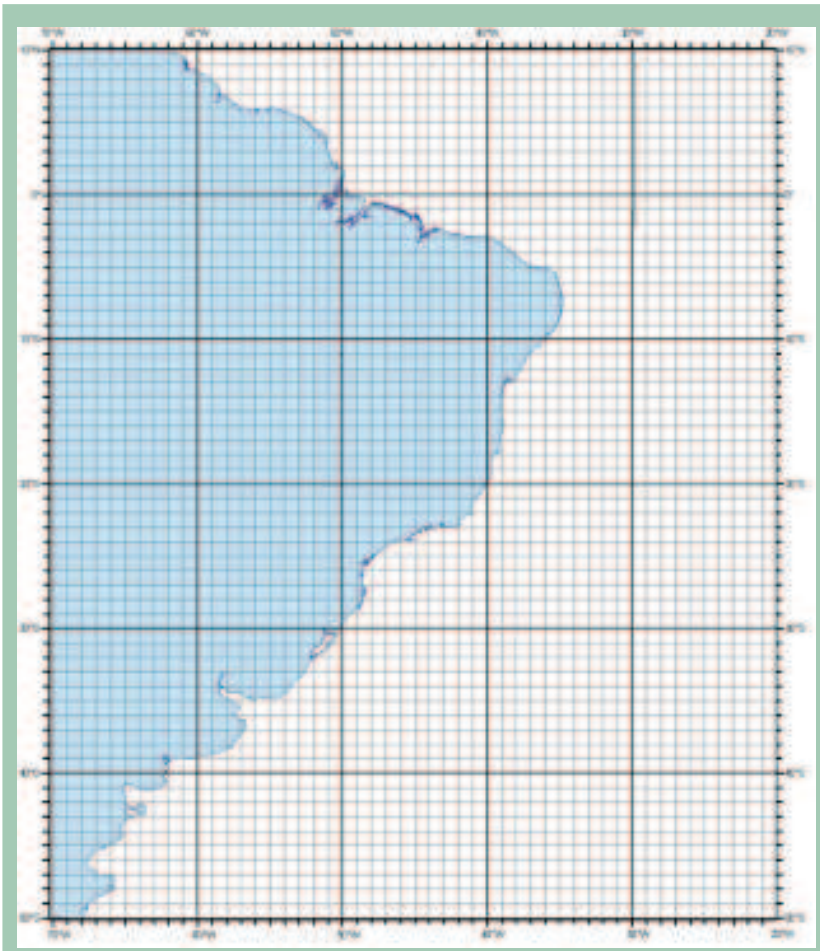
Segurança dos dados do Projeto SISPRES

Pablo Medeiros Jabor.
Assessor Técnico de Pesquisa da Divisão de Projetos de Propagação. Graduado em Oceanografia pela Universidade do Vale do Itajaí e pós-graduado (M.Sc.) em Geomática pela Universidade Estadual do Rio de Janeiro.

O projeto SISPRES, desenvolvido pelo IEAPM, utiliza um banco de dados com informações ambientais (BDAQ). Estes dados, que podem ser visualizados pelo Sistema Tático de Fatores Ambientais (STFA), também permitem que o módulo de previsão acústica (MODPRES) seja utilizado para o planejamento de operações navais. A BDAQ contém informações climatológicas de temperatura da água do mar, salinidade, temperatura na camada de mistura, profundidade de camada, temperatura do ar, umidade relativa ao nível do mar, pressão atmosférica ao nível do mar, precipitação, vento, batimetria e faciologia. A área de cobertura dos dados se estende de 10°N a 50°S e entre a linha de costa e 20°W.



Área de cobertura do banco de dados do Projeto SISPRES.

O processo de qualificação e tratamento dos dados que compõem a BDAQ requer a utilização de sistemas específicos desenvolvidos no IEAPM. Os dados de temperatura e salinidade, por exemplo, são submetidos a um processo que envolve as seguintes etapas: formatação, qualificação e tratamento. A etapa de formatação recebe os dados provenientes de diferentes instituições, coletados por diversos tipos ou modelos de equipamentos e os padroniza em um formato único. Na etapa de qualificação, os dados são submetidos a um sistema que aplica a cada ponto coletado testes sequenciais de qualidade e estabelece para cada um destes pontos uma marcação informativa quanto à qualidade do mesmo. Os dados que foram reprovados no sistema de qualificação passam para a etapa seguinte de tratamento. Nesta etapa, o analista pode aplicar aos dados

qualificados técnicas de correção específicas. Assim, é possível ter um conjunto de dados qualificados e tratados que possam ser submetidos ao tratamento estatístico para a obtenção de perfis médios mensais representativos para uma grade regular de 1°.

Na versão atual, entregue em outubro de 2009, a BDAQ contém cerca de quatro milhões de registros.

O projeto SISPRES é classificado como confidencial, portanto, seus algoritmos e parâmetros de cálculo de alcance sonar só podem ser utilizados por Organizações Militares que tenham credencial e necessidade de uso. Os desafios envolvidos incluem:

1 – manter o sistema acessível aos utilizadores, sem introduzir dificuldades de acesso;

2 – impedir que o sistema possa ser utilizado por terceiros (com cópias ilegais); e

3 – impedir acesso aos dados de outra forma que não por meio dos programas do sistema.

Para garantir a confidencialidade e manter a restrição do uso dos programas e dados que compõem o SISPRES, foram desenvolvidas e aplicadas duas soluções de segurança da informação: chave de hardware e criptografia.

Chave de Hardware

As chaves de hardware fornecem a proteção necessária de um dispositivo físico que precisa estar conectado no PC em que o programa esteja instalado. O SISPRES incorpora a chave de hardware e comunica-se com ela durante a sua utilização. Ao exigir a presença da "Chave" física instalada no PC, além de uma cópia do SISPRES, pretende-se garantir um maior nível de proteção contra a pirataria. A chave é disponível para a porta USB e se parece muito com uma *Pen Drive*.

A solução de proteção por chave de hardware apresenta um baixo custo de implementação, com a utilização do programa envelopador. O programa envelopador adiciona ao arquivo escolhido as chamadas de verificação da presença da chave.

Chave de Hardware do SISPRES

CRIPTOGRAFIA

A criptografia é o estudo dos princípios e técnicas pelas quais a informação pode ser transformada da sua forma original para outra ilegível, dentre os objetivos da criptografia destacamos: a confidencialidade e a integridade da informação. Este processo é feito por algoritmos que fazem o embaralhamento dos "bits" destes dados, a partir de uma determinada chave (sequência de caracteres usados na codificação e decodificação da informação).

O algoritmo de criptografia utilizado foi implementado pelo CASNAV (Centro de Análises de Sistemas Navais). Trata-se do algoritmo simétrico AES (Advanced Encryption Standard) disponibilizado livremente (com os termos ANSI), que utiliza uma chave simétrica de bloco de 128 "bits", com baixo requisito de memória e alta eficiência computacional. A tabela abaixo apresenta um exemplo dos dados cifrados e decifrados pelo AES.

Todos os dados da BDAQ foram previamente cifrados, os programas que compõem o SISPRES fazem uso do algoritmo de criptografia toda vez que acessam os dados da BDAQ para decifrá-los, desta forma, o usuário só terá como visualizar os dados utilizando o SISPRES, que, conforme mencionado anteriormente, só será executado se o PC estiver com a chave de *hardware* conectada.

Tabela 1 – Dados cifrados (A) e decifrados (B) pelo algoritmo de criptografia AES.

PROF	TEMP	SAL
0	32173.29	4057.938
10	31617.61	35787.57
18	14511.14	38756.93
20	30075.17	2026.164

A

PROF	TEMP	SAL
0	27.335	5.649
10	27.37	35.64
18	27.305	5.674
20	27.283	35.68

B