Conferência em Segurança Informática

17 de Março – 10 horas

Sala Auditório Professor Lima de Carvalho

Programa:

10h: Abertura (Por um elemento da direcção da ESCE)

10h30: Ivone Amorim (docente na Escola Superior de Tecnologia e Gestão do IPVC)

A Criptografia de Chave Pública

Até meados dos anos 70, a transmissão de mensagens cifradas era feita utilizando Criptografia Simétrica, ou seja, a mesma chave era utilizada para cifrar e decifrar as mensagens. Como resultado, dois quaisquer utilizadores de um dado sistema, que quisessem comunicar secretamente, teriam de ter previamente trocado a chave de forma segura. Em 1976, Diffie e Hellman revolucionaram, de alguma forma, o mundo da Criptografia, ao introduzirem o conceito de chave pública. Com este novo conceito não só passa a ser possível que duas entidades comuniquem secretamente , sem terem qualquer contacto prévio para acordarem uma chave, como passa a ser possível "garantir" que uma mensagem digital, que pode facilmente ser copiada, foi de facto enviada por aquele que se diz o seu emissor. Nesta apresentação pretende-se fazer uma breve introdução à Criptografia, descrever algumas cifras básicas, e explicar porque é que os Sistemas de Chave Pública foram um dos desenvolvimentos mais fantásticos da história da Criptografia.

11h: Coffee Break

11h30: Nelson Azevedo (Banco Português de Investimentos)

Segurança da Informação no Sector Bancário

O sector bancário é um dos sectores onde se mais evidencia o tema sobre a segurança da informação, sendo uma das suas mais principais tarefas salvaguardar a confidencialidade, integridade e disponibilidade da informação que é propriedade dos bancos ou que estejam sobre a sua responsabilidade. Para além de toda a conformidade legal e regulamentar que iremos apresentar, vamos também analisar casos em que ocorreram falhas na Segurança da Informação, e como estas se podem traduzir em impactos ao nível da imagem, da reputação e mesmo a nível financeiro dos bancos, podendo assim colocar em causa a própria continuidade do negócio.

12h-14h30: Pausa para almoço

14h30: Alexandre Pinto (docente no Instituto Superior da Maia)

Provas de Segurança

A criptografia tornou-se nos últimos anos uma ferramenta indispensável na segurança das comunicações, e serve de base a várias situações frequentes no dia-a-dia virtual, por exemplo no acesso a websites seguros, na criação de VPNs, na emissão de assinaturas digitais, no envio de email seguro ou na comunicação de dados confidenciais. Na base desta criptografia estão alguns esquemas, como o RSA, que se tornaram famosos muito para além da comunidade criptográfica. É comum pensar-se que o RSA é um método de cifra seguro, mas esta noção de segurança é difícil de compreender. O que é ser seguro? Seguro em relação a quê? E será o RSA um esquema seguro? Esta apresentação está focada sobre as noções tradicionais de segurança em criptografia, explicando o que são provas de segurança, diferentes tipos de provas e que garantias estas nos dão.

15h: Luís Antunes (docente na Faculdade de Ciências da Universidade do Porto)

Cartão do Cidadão: a sua identidade num mundo digital

Nesta palestra vamos explicar o funcionamento da assinatura digital e ilustrar a sua utilidade com alguns casos reais.

15h30: Ana Margarida Ferreira (Especialista de Informática da Faculdade de Medicina da Universidade do Porto)

Quebrar a segurança para melhorar a segurança

O standard RBAC (Role-Based Access Control) é comummente usado na área da saúde para definir os privilégios de acesso dos profissionais ao registo electrónico dos doentes. Apesar da sua fácil gestão, este modelo é rígido em situações de emergência ou imprevistas, porque tem apenas dois resultados possíveis: Permitir ou Negar o acesso. Esta investigação incluiu no modelo RBAC um terceiro resultado com a possibilidade de um utilizador escolher, a determinado momento, se pretende aceder informação que normalmente não tem acesso. Esta nova opção permite quebrar a política definida, ao mesmo tempo que regista todos os acessos para posterior verificação e justificação. O novo modelo BTG-RBAC permite acessos a informação em situações imprevistas (disponibilidade) mas também pode bloquear acessos a informação que não deveria estar disponível a um grupo de utilizadores (confidencialidade). O BTG-RBAC aumenta a flexibilidade e segurança da informação assim como a responsabilidade do utilizador.

16h: David Pereira (docente no Instituto Superior de Engenharia do Porto)

Introdução à verificação de software baseada em linguagens

Nesta palestra serão introduzidos os conceitos base da área de verificação de software baseada em linguagens. O objectivo principal será o de elucidar a audiência sobre as problemáticas associadas ao desenvolvimento de software para sistemas críticos (sistemas onde os erros de software podem levar a perdas irreparáveis tais como, por exemplo, a perda de vidas humanas) . Serão apresentados casos onde tais erros ocorreram e também qual a tecnologia disponível para atacar estes problemas de forma criar software o mais fiável possível.

16h30: Coffee Break

17h: Tiago Pedrosa (docente no Instituto Politécnico de Bragança)

Conhecendo o atacante

Os sistemas e redes informáticas estão sobre constante ameaça de ataques informáticos. Pretende-se identificar os vários perfis de ataques desde os mais inocentes de experimentação de ferramentas automáticas até aos ataques direccionados especializados. Serão descritas as fases e formas que os ataques normalmente tomam. Todas as máquinas são apetecíveis, seja pela informação que contém, por permitir aceder a outros recursos, ou para aumentar a capacidade bélica do atacante, permitindo ao mesmo tempo se anonimizar e se proteger de ser identificado como o originador de ataques. Cada máquina pode aumentar ou diminuir a segurança total da internet.

17h30: Henrique Santos (docente na Universidade do Minho)

Necessidade de segurança nos SI – Políticas de Segurança

18h: Sessão de encerramento