RSA大会：DNS或将免受中间人和缓存投毒攻击思科认证
PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/644/2021_2022_RSA_E5_A4_A7_E4_BC_9A_EF_c101_644492.htm 威瑞信（VeriSign）公司日前邀请互联网行业领导者加入由威瑞信新建立的，并由思科系统（Cisco Systems）、瞻博网络（Juniper Networks）等厂商共同参与的域名系统(DNS)安全扩展协议（DNSSEC）互通实验室，旨在改进具有互通解决方案的互联网通信安全。在3月初于旧金山举办的2010年RSA大会上，威瑞信高层将与硬件厂商、软件厂商、互联网服务提供商（ISP）和政府机构会面，阐述公司是如何帮助成功实施DNSSEC。同时,在RSA大会上，威瑞信执行主席James Bidzos将在3月4日下午三点发表主题演讲，重点阐述信任在确保互联网安全中所发挥的关键作用。 DNSSEC通过将数字签名应用到DNS数据，帮助防止DNS免受“ 中间人 ”和缓存投毒攻击。通过对DNS数据进行签名，DNSSEC会鉴别数据来源的真实性，并在数据通过互联网传送时核实其完整性。威瑞信正在与美国商务部和ICANN合作，并有条不紊而审慎地展开工作。威瑞信预计到2011年第一季度，DNSSEC将在.edu、.net和.com顶级域名中完成部署。 威瑞信公司高级副总裁兼首席技术官Ken Silva表示：“ DNSSEC为广大网民提供安全保护，但只有当它应用于端到端时才有效。如要消除目前仍存在于防火墙、负载均衡器及其它基础设施中的技术障碍，整个行业必须共同参与。思科、瞻博网络和其它行业领导者正在合理运用威瑞信DNSSEC互通实验室的测试环境所带来的优势，因此，解决方案提供商、ISP和政府机构的共同参与显得尤为重要。我

们非常荣幸能够与这些创新者合作，他们已经认识到，成功实现DNSSEC是在互联网上必须分担的一项责任。”威瑞信为DNSSEC试验室配备了专门的人员，他们可以为解决方案和服务提供商提供帮助，确定包含DNSSEC信息的DNS数据包是否会给互联网和企业基础设施各个组成要素带来问题，因为这些数据包要比标准DNS数据包大得多。例如，某些解决方案默认的DNS数据包尺寸和结构可能不再适用于DNSSEC。思科公司安全研究和运营总监Russell Smoak表示：“确保网络上共享数据的完整性，一直我们的追求目标。在过去25年中，作为网络领域的全球领导者，思科认识到保护DNS基础设施的好处。我们非常高兴地看到，威瑞信正采取积极措施，通过建立一个测试设施以使提供商了解DNSSEC对他们的解决方案和服务产生怎样的影响。互联网业界必须继续协同工作，帮助确保DNSSEC的成功部署。”瞻博网络公司首席安全架构师Nicko van Someren表示：“我们看到采用DNSSEC的需求量不断提高，也非常高兴威瑞信已采取措施确保负责任的解决方案提供商能够评估系统的互通能力。作为一家致力于改变网络体验和经济模式的公司，我们意识到尽快进行DNSSEC测试的重要性，而威瑞信DNSSEC互通实验室使其这一切变得轻松。”厂商可以将各自的解决方案带到位于美国弗吉尼亚州杜勒斯数据中心的威瑞信实验室，以确保DNSSEC请求和响应通过时的完整性。测试通过一系列设置DNSSEC和未设置DNSSEC的DNS查询和响应对系统进行评估。测试在位于杜勒斯设备的独立式环境中进行。威瑞信将不会进行性能测试和压力测试，也不会“证实”解决方案的DNSSEC互通能力。威瑞信正与业界领

导者和机构合作，以在2010年第二季度前为.edu域名提供安全解析服务，在2010年第四季度前为.net域名提供安全解析服务，在2011年第一季度前为.com提供安全解析服务。 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com