Reports (REPORT)

<?xml version="1.0" encoding="utf-8"?>

<TEI xmlns="http://www.tei-c.org/ns/1.0" xmlns:hal="http://hal.archives-ouvertes.fr">

    <text>

       <body>

           <listBibl>

               <biblFull>

                   <titleStmt>

                       <title xml:lang="en">Consequences of compromised zone keys in DNSSEC </title><!-- %%mandatory field -->

                       <author role="aut"><!-- %%mandatory field -->

                           <persName>

                               <forename type="first">Gilles</forename>

                               <surname>Guette</surname>

                           </persName>

                           <affiliation ref="#struct-100681"></affiliation>

                       </author>

                   </titleStmt>

                   <editionStmt>

                       <edition>

                           <ref type="file" target="rapportfulltxt.pdf" subtype="author" n="1"/>

                       </edition>

                   </editionStmt>

                   <notesStmt>

                       <note type="report" n="6"/><!-- %%mandatory field -->

                   </notesStmt>

                   <sourceDesc>

                       <biblStruct>

                           <analytic>

                               <title xml:lang="en">Consequences of compromised zone keys in DNSSEC </title>

                               <author role="aut">

                                   <persName>

                                       <forename type="first">Gilles</forename>

                                       <surname>Guette</surname>

                                   </persName>

                                   <affiliation ref="#struct-100681"></affiliation>

                               </author>

                           </analytic>

                           <monogr>

                               <idno type="reportnumber">PI1787</idno>

                               <imprint>

                                   <date type="datePub">2006</date><!-- %%mandatory field -->

                               </imprint>

                               <authority type="institution">Ecole Nationale Supérieure des Télécommunications de Bretagne</authority><!-- %%mandatory field -->

                           </monogr>

                       </biblStruct>

                   </sourceDesc>

                   <profileDesc>

                       <langUsage>

                           <language ident="en"></language><!-- %%mandatory field -->

                       </langUsage>

                       <textClass>

                           <keywords scheme="author">

                               <term xml:lang="en">key compromission</term>

                               <term xml:lang="en">network security</term>

                           </keywords>

                           <classCode scheme="halDomain" n="info.info-na"></classCode><!-- %%mandatory field -->

                           <classCode scheme="halDomain" n="info.info-oh"></classCode>

                           <classCode scheme="halTypology" n="REPORT"></classCode><!-- %%mandatory field -->

                       </textClass>

                       <abstract xml:lang="en">The Domain Name System is a distributed tree-based database. The DNS protocol is largely used to translate a human readable machine name into an IP address. The DNS security extensions (DNSSEC) has been designed to protect the DNS protocol. DNSSEC uses public key cryptography and digital signatures. A secure DNS zone owns at least a key pair (public/private) to provide two security services: data integrity and authentication. To trust some DNS data, a DNS client has to verify the signature of this data with the right zone key. This verification is based on the establishment of a chain of trust between secure zones. To build this chain of trust, a DNSSEC client needs a secure entry point: a zone key configured as trusted in the client. And then, the client must find a secure path from a secure entry point to the queried DNS resource. Zone keys are critical in DNSSEC and are used in every steps of a name resolution. In this report, we present a study on consequences of a compromised key in DNSSEC. We describe compromised key attacks and we present current defenses.</abstract><!-- %%mandatory field -->

                   </profileDesc>

               </biblFull>

           </listBibl>

       </body>

    </text>

</TEI>