From: todd glassey

Sent: 8/9/2011 12:32:39 PM

To: tdarton@pilotpowergroup.com (tdarton@pilotpowergroup.com); ALJ Tim Sullivan (tjs@cpuc.ca.gov); keith.mccrea@sutherland.com (keith.mccrea@sutherland.com); ej_wright@oxy.com (ej_wright@oxy.com); mmazur@3PhasesRenewables.com (mmazur@3PhasesRenewables.com); igoodman@commerceenergy.com (igoodman@commerceenergy.com); lwisland@ucsusa.org (lwisland@ucsusa.org); sue.mara@RTOadvisors.com (sue.mara@RTOadvisors.com); martinhomec@gmail.com (martinhomec@gmail.com); jims@vea.coop (jims@vea.coop); nes@a-klaw.com (nes@a-klaw.com); mtierney-lloyd@enernoc.com (mtierney-lloyd@enernoc.com); whb@a-klaw.com (whb@a-klaw.com); Middlekauff, Charles (Law) (/O=PG&E/OU=Corporate/cn=Recipients/cn=CRMd); GloriaB@anzaelectric.org (GloriaB@anzaelectric.org); tam.hunt@gmail.com (tam.hunt@gmail.com); rkmoore@gswater.com (rkmoore@gswater.com); skh@cpuc.ca.gov (skh@cpuc.ca.gov); JPacheco@SempraUtilities.com (JPacheco@SempraUtilities.com); carol.schmidfrazee@sce.com (carol.schmidfrazee@sce.com); nao@cpuc.ca.gov (nao@cpuc.ca.gov); allwazeready@aol.com (allwazeready@aol.com); DGarber@SempraUtilities.com (DGarber@SempraUtilities.com); cec@cpuc.ca.gov (cec@cpuc.ca.gov); Urick, Lisa (LUrick@Sempra.com); Keilani,, Wendy (WKeilani@semprautilities.com); Cherry, Brian K (/O=PG&E/OU=CORPORATE/CN=RECIPIENTS/CN=BKC7); ssmyers@att.net (ssmyers@att.net); HYao@SempraUtilities.com (HYao@SempraUtilities.com); achang@efficiencycouncil.org (achang@efficiencycouncil.org); liddell@energyattorney.com (liddell@energyattorney.com); mgillette@enernoc.com (mgillette@enernoc.com); wem@igc.org (wem@igc.org); bcragg@goodinmacbride.com (bcragg@goodinmacbride.com); clyde.murley@comcast.net (clyde.murley@comcast.net); janreid@coastecon.com (janreid@coastecon.com); jarmstrong@goodinmacbride.com (jarmstrong@goodinmacbride.com); jarmstrong@goodinmacbride.com (jarmstrong@goodinmacbride.com); gmorris@emf.net (gmorris@emf.net); rick_noger@praxair.com (rick_noger@praxair.com); cmkehrein@ems-ca.com (cmkehrein@ems-ca.com); Huffman, Mark (Law) (/O=PG&E/OU=Corporate/cn=Recipients/cn=MRH2); blaising@braunlegal.com (blaising@braunlegal.com); jleslie@luce.com (jleslie@luce.com); Zahariudakis, George (/O=PG&E/OU=Corporate/cn=Recipients/cn=GxZ5); abb@eslawfirm.com (abb@eslawfirm.com); jjg@eslawfirm.com (jjg@eslawfirm.com); matthew@turn.org (matthew@turn.org); Mason, Cory (law) (/O=PG&E/OU=Corporate/cn=Recipients/cn=CMMw); atrowbridge@daycartermurphy.com (atrowbridge@daycartermurphy.com); lcottle@winston.com (lcottle@winston.com); amber@iepa.com (amber@iepa.com); dansvec@hdo.net (dansvec@hdo.net); jeffreygray@dwt.com (jeffreygray@dwt.com); aes_ltpp@aes.com (aes_ltpp@aes.com); Christine@consciousventuresgroup.com (Christine@consciousventuresgroup.com);

rfreeh123@sbcglobal.net (rfreeh123@sbcglobal.net); bdicapo@caiso.com (bdicapo@caiso.com); Manheim, William (Law) (/O=PG&E/OU=Corporate/cn=Recipients/cn=WVM3); RegRelCPUCCases (/O=PG&E/OU=Corporate/cn=Recipients/cn=RegRelCPUCCases); sdhilton@stoel.com (sdhilton@stoel.com); jeanne.sole@sfgov.org (jeanne.sole@sfgov.org); sschiller@efficiencycouncil.org (sschiller@efficiencycouncil.org); sls@a-klaw.com (sls@a-klaw.com); nlong@nrdc.org (nlong@nrdc.org); filings@a-klaw.com (filings@a-klaw.com); mpa@a-klaw.com (mpa@a-klaw.com); tglassey@certichron.com (tglassey@certichron.com); CentralFiles@SempraUtilities.com (CentralFiles@SempraUtilities.com); jimross@r-c-s-inc.com (jimross@r-c-s-inc.com); cem@newsdata.com (cem@newsdata.com); case.admin@sce.com (case.admin@sce.com); mrw@mrwassoc.com (mrw@mrwassoc.com); kerry.hattevik@nexteraenergy.com (kerry.hattevik@nexteraenergy.com); Gonzales, Matthew (/O=PG&E/OU=Corporate/cn=Recipients/cn=MRGg); DWTCPUCDOCKETS@dwt.com (DWTCPUCDOCKETS@dwt.com); mdjoseph@adamsbroadwell.com (mdjoseph@adamsbroadwell.com); Gong, Alice (/O=PG&E/OU=Corporate/cn=Recipients/cn=AxL3); npedersen@hanmor.com (npedersen@hanmor.com); dorth@krcd.org (dorth@krcd.org); kowalewskia@calpine.com (kowalewskia@calpine.com); kjsimonsen@ems-ca.com (kjsimonsen@ems-ca.com); nrader@calwea.org (nrader@calwea.org); andy.vanhorn@vhcenergy.com (andy.vanhorn@vhcenergy.com); steven@iepa.com (steven@iepa.com); barmackm@calpine.com (barmackm@calpine.com); Derek@AltaPowerGroup.com (Derek@AltaPowerGroup.com); ttutt@smud.org (ttutt@smud.org); r.raushenbush@comcast.net (r.raushenbush@comcast.net); r.raushenbush@comcast.net (r.raushenbush@comcast.net); ek@a-klaw.com (ek@a-klaw.com); marcie.milner@shell.com (marcie.milner@shell.com); mcox@calplg.com (mcox@calplg.com); cynthia.brady@constellation.com (cynthia.brady@constellation.com); beth@beth411.com (beth@beth411.com); kpp@cpuc.ca.gov (kpp@cpuc.ca.gov); julien.dumoulin-smith@ubs.com (julien.dumoulin-smith@ubs.com); julien.dumoulin-smith@ubs.com (julien.dumoulin-smith@ubs.com); Sean.Beatty@mirant.com (Sean.Beatty@mirant.com); william.tomlinson@elpaso.com (william.tomlinson@elpaso.com); william.tomlinson@elpaso.com (william.tomlinson@elpaso.com); ralphdennis@insightbb.com (ralphdennis@insightbb.com); amber@ethree.com (amber@ethree.com); robertgex@dwt.com (robertgex@dwt.com); smartinez@nrdc.org (smartinez@nrdc.org); will.mitchell@cpv.com (will.mitchell@cpv.com); b.buchynsky@dgc-us.com (b.buchynsky@dgc-us.com); akbar.jazayeri@sce.com (akbar.jazayeri@sce.com); Melissa.Hovsepian@sce.com (Melissa.Hovsepian@sce.com); rafi.hassan@sig.com (rafi.hassan@sig.com); rafi.hassan@sig.com (rafi.hassan@sig.com); pmiller@nrdc.org (pmiller@nrdc.org); rps-ca@coolearthsolar.com (rps-ca@coolearthsolar.com); jfieber@flk.com (jfieber@flk.com); KKloberdanz@SempraUtilities.com (KKloberdanz@SempraUtilities.com); ecrem@ix.netcom.com (ecrem@ix.netcom.com); mike.montoya@sce.com (mike.montoya@sce.com);

hvidstenj@kindermorgan.com (hvidstenj@kindermorgan.com); shawn_cox@kindermorgan.com (shawn_cox@kindermorgan.com); jordan.white@pacificorp.com (jordan.white@pacificorp.com); TCorr@SempraUtilities.com (TCorr@SempraUtilities.com); amber.wyatt@sce.com (amber.wyatt@sce.com); kmills@cfbf.com (kmills@cfbf.com); joyw@mid.org (joyw@mid.org); brbarkovich@earthlink.net (brbarkovich@earthlink.net); bernardo@braunlegal.com (bernardo@braunlegal.com); jak@gepllc.com (jak@gepllc.com); mwt@cpuc.ca.gov (mwt@cpuc.ca.gov); e-recipient@caiso.com (e-recipient@caiso.com); michaelboyd@sbcglobal.net (michaelboyd@sbcglobal.net); jsanders@caiso.com (jsanders@caiso.com); jsanders@caiso.com (jsanders@caiso.com); cleni@energy.state.ca.us (cleni@energy.state.ca.us); cleni@energy.state.ca.us (cleni@energy.state.ca.us); dvidaver@energy.state.ca.us (dvidaver@energy.state.ca.us); eddyconsulting@gmail.com (eddyconsulting@gmail.com); tobinjmr@sbcglobal.net (tobinjmr@sbcglobal.net); dgrandy@caonsitegen.com (dgrandy@caonsitegen.com); tpomales@arb.ca.gov (tpomales@arb.ca.gov); tpomales@arb.ca.gov (tpomales@arb.ca.gov); claufenb@energy.state.ca.us (claufenb@energy.state.ca.us); californiadockets@pacificorp.com (californiadockets@pacificorp.com); bsb@eslawfirm.com (bsb@eslawfirm.com); bsb@eslawfirm.com (bsb@eslawfirm.com); gohara@calplg.com (gohara@calplg.com); gohara@calplg.com (gohara@calplg.com); sberlin@mccarthylaw.com (sberlin@mccarthylaw.com); kdw@woodruff-expert-services.com (kdw@woodruff-expert-services.com); lwhouse@innercite.com (lwhouse@innercite.com); ddavie@wellhead.com (ddavie@wellhead.com); karen@klindh.com (karen@klindh.com); danielle@ceert.org (danielle@ceert.org); cpucdockets@keyesandfox.com (cpucdockets@keyesandfox.com); bmcc@mccarthylaw.com (bmcc@mccarthylaw.com); blake@consumercal.org (blake@consumercal.org); mpo@cpuc.ca.gov (mpo@cpuc.ca.gov); dbp@cpuc.ca.gov (dbp@cpuc.ca.gov); dwang@nrdc.org (dwang@nrdc.org); mary.lynch@constellation.com (mary.lynch@constellation.com); philm@scdenergy.com (philm@scdenergy.com); ahaubenstock@brightsourceenergy.com (ahaubenstock@brightsourceenergy.com); wmccartney@caiso.com (wmccartney@caiso.com); jose@ceert.org (jose@ceert.org); shi@cpuc.ca.gov (shi@cpuc.ca.gov); glbarbose@lbl.gov (glbarbose@lbl.gov); psd@cpuc.ca.gov (psd@cpuc.ca.gov); ahsanstad@lbl.gov (ahsanstad@lbl.gov); MC4@cpuc.ca.gov (MC4@cpuc.ca.gov); svn@cpuc.ca.gov (svn@cpuc.ca.gov); chh@cpuc.ca.gov (chh@cpuc.ca.gov); eks@cpuc.ca.gov (eks@cpuc.ca.gov); clu@cpuc.ca.gov (clu@cpuc.ca.gov); AEG@cpuc.ca.gov (AEG@cpuc.ca.gov); ska@cpuc.ca.gov (ska@cpuc.ca.gov); CCE@cpuc.ca.gov (CCE@cpuc.ca.gov); jm3@cpuc.ca.gov (jm3@cpuc.ca.gov); dfredericks@dgpower.com (dfredericks@dgpower.com); ferguson@braunlegal.com (ferguson@braunlegal.com); bbc@cpuc.ca.gov (bbc@cpuc.ca.gov); nlr@cpuc.ca.gov (nlr@cpuc.ca.gov); edd@cpuc.ca.gov (edd@cpuc.ca.gov); vjb@cpuc.ca.gov (vjb@cpuc.ca.gov); rls@cpuc.ca.gov (rls@cpuc.ca.gov); mjs@cpuc.ca.gov (mjs@cpuc.ca.gov); unc@cpuc.ca.gov (unc@cpuc.ca.gov); SMK@cpuc.ca.gov (SMK@cpuc.ca.gov); jf2@cpuc.ca.gov (jf2@cpuc.ca.gov);

kwh@cpuc.ca.gov (kwh@cpuc.ca.gov); vsk@cpuc.ca.gov (vsk@cpuc.ca.gov); mmyers@vandelaw.com (mmyers@vandelaw.com); jhe@cpuc.ca.gov (jhe@cpuc.ca.gov); ltt@cpuc.ca.gov (ltt@cpuc.ca.gov); nws@cpuc.ca.gov (nws@cpuc.ca.gov); michael.colvin@cpuc.ca.gov (michael.colvin@cpuc.ca.gov)

Cc:

Bcc:

Subject: Ex Parte - EVIDENCE OF SMARTGRID Security Failings. - Fwd: Re: [ntpwg] Autokey-Protocol Analysis - COMMENTARY COMING

Your Honor -
I have repeatedly submitted "evidence quality" concerns with how the California SmartGrid is being designed and deployed and this is one of the evidences that this concern is warranted. This is a piece of email (with the header intact) which shows that there are serious security problems in how time data is securely managed in networking systems.

What this means is that Time of Use Billing in the SmartGrid is subject to these
issues and problems with time management. These services which are now seriously
in question by the Government of Germany's PTB control time distribution to the Meter and from the Meter to the Collection Point and all Sub-Station Automation components.

This document is from the NTP working group and is a factual complaint up before the Network Time Protocol group which was filed before them by the actual German National Standards Laboratory Group called the PTB.

Now because of this the actual German Government (through its standards org) is sending out formal notices that the time services which are relied on for
everything are in fact full of security holes.

What this simply means is that no Utility has control over ToU Billing at this point because of their failure to manage the time services properly.

Formal notice of this communication is being served on the SG Service List today.

Todd Glassey

-------- Original Message --------
From: - Wed Aug 03 07:17:56 2011
X-Account-Key: account1
X-UIDL: 11e0-bdd4-034eabf2-a703-0021281794ea

X-Mozilla-Status: 1011
X-Mozilla-Status2: 00000000
X-Mozilla-Keys:
Status: U
Return-Path: <ntpwg-bounces+tglassey=earthlink.net@lists.ntp.org>
Received: from mx-mcdonald.atl.sa.earthlink.net ([207.69.195.177]) by
mdl-quaff.atl.sa.earthlink.net (EarthLink SMTP Server) with SMTP id
1qOBrE4zJ3Nl3423; Wed, 3 Aug 2011 09:25:10 -0400 (EDT)
Received: from lists.ntp.org ([149.20.68.7]) by
mx-mcdonald.atl.sa.earthlink.net (EarthLink SMTP Server) with ESMTP id
1qOBrs5O83Nl36F0 for <tglassey@earthlink.net>; Wed, 3 Aug 2011 09:24:58
-0400 (EDT)
Received: from lists.ntp.org (lists.ntp.org [149.20.68.7]) by
lists.ntp.org (Postfix) with ESMTP id 9844E86D762 for

<tglassey@earthlink.net>; Wed, 3 Aug 2011 13:24:57 +0000 (UTC)
X-Original-To: ntpwg@lists.ntp.org
Delivered-To: ntpwg@lists.ntp.org
Received: from mail1.ntp.org (mail1.ntp.org [IPv6:2001:4f8:fff7:1::5])
by lists.ntp.org (Postfix) with ESMTP id 9D8F086D75D for
<ntpwg@lists.ntp.org>; Wed, 3 Aug 2011 12:55:59 +0000 (UTC)
Received: from mailfront3.rz.tu-bs.de ([134.169.12.134] helo=tu-bs.de)
by mail1.ntp.org with esmtp (Exim 4.75 (FreeBSD)) (envelope-from
<s.roettger@tu-bs.de>) id 1QoazD-000Ak8-Pq for ntpwg@lists.ntp.org; Wed,
03 Aug 2011 12:55:59 +0000
Received: from [192.53.103.10] (account y0034674@tu-braunschweig.de
HELO [192.168.4.193]) by rz.tu-bs.de (CommuniGate Pro SMTP 5.3.13) with
ESMTPA id 8419739; Wed, 03 Aug 2011 14:55:39 +0200
Message-ID: <4E394471.3040903@tu-bs.de>
Date: Wed, 03 Aug 2011 14:52:01 +0200
From: Stephen Röttger <s.roettger@tu-bs.de>
User-Agent: Mozilla/5.0 (X11; U; Linux x86_64; en-US; rv:1.9.2.17)
Gecko/20110720 Lightning/1.0b3pre Thunderbird/3.1.10
MIME-Version: 1.0
To: Greg Dowd <GDowd@symmetricom.com>
References: <4E385A0B.70206@tu-bs.de>
<26FBD265CD8D234EAF41115A180F92BB38AF02AC@SJC-MBX-01.symmetricom.com>
In-Reply-To:
<26FBD265CD8D234EAF41115A180F92BB38AF02AC@SJC-MBX-01.symmetricom.com>
X-Enigmail-Version: 1.1.2
X-SA-Exim-Connect-IP: 134.169.12.134
X-SA-Exim-Rcpt-To: ntpwg@lists.ntp.org
X-SA-Exim-Mail-From: s.roettger@tu-bs.de
X-Spam-Checker-Version: SpamAssassin 3.3.0 (2010-01-18) on mail1.ntp.org
X-Spam-Level:
X-Spam-Status: No, score=-2.6 required=5.0

tests=BAYES_00,RCVD_IN_DNSWL_LOW, T_RP_MATCHES_RCVD autolearn=ham
version=3.3.0
X-SA-Exim-Version: 4.2
X-SA-Exim-Scanned: Yes (on mail1.ntp.org)
Cc: NTP Working Group <ntpwg@lists.ntp.isc.org>, dieter.sibold@ptb.de
Subject: Re: [ntpwg] Autokey-Protocol Analysis
X-BeenThere: ntpwg@lists.ntp.org
X-Mailman-Version: 2.1.12
Precedence: list
List-Id: IETF Working Group for Network Time Protocol
<ntpwg.lists.ntp.org>
List-Unsubscribe: <http://lists.ntp.org/options/ntpwg>,
<mailto:ntpwg-request@lists.ntp.org?subject=unsubscribe>
List-Archive: <https://lists.ntp.org/pipermail/ntpwg>
List-Post: <mailto:ntpwg@lists.ntp.org>
List-Help: <mailto:ntpwg-request@lists.ntp.org?subject=help>
List-Subscribe: <http://lists.ntp.org/listinfo/ntpwg>,

<mailto:ntpwg-request@lists.ntp.org?subject=subscribe>
Content-Type: text/plain; charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable
Sender: ntpwg-bounces+tglassey=earthlink.net@lists.ntp.org
Errors-To: ntpwg-bounces+tglassey=earthlink.net@lists.ntp.org
X-ELNK-Received-Info: spv=0;
X-ELNK-AV: 0
X-ELNK-Info: sbv=0; sbrc=.0; sbf=0b; sbw=000;

Greg,
Yes, there are plans to publish the results in english.
The german version is not public yet, but presumably will be in a few weeks.
However I can summarize the discovered vulnerabilities (mainly for
client-server-mode):

-The bitlenghts of the cookie and the server seed are only 32 Bit long.
This leads to an attacker being able to Brute Force them.
For example he can request a cookie from a server and try all 2^32
possibilites as server seed and calculate corresponding cookies. If he
finds one that matches the cookie he received from the server, he has
found the secret server seed and can consequently calculate cookies for
every client.
The same applies for brute-forcing the cookie. The attacker can
intercept a packet with a MAC and try to generate the MAC himself using
every possible of the 2^32 cookie-values, till he found the one that
matches.

For comparison, 2^32 MD5 calculations take roughly 25minutes on my 2,5ghz laptop using only one thread. (though cookie brute-forcing will take 2 MD5 calculations for each try)

-The Identity Schemes (except the private certificate scheme) provide no security.
The TC scheme accepts a certificate as that of a Trusted Authority if it includes a extension CA=True. Nothing prevents an attacker from generating such a certificate himself.
We discovered a flaw in all three challenge-response identity schemes (IFF, MV, GQ), that allowed us to send a response that would always be accepted by the client. In addition, the challenge-response schemes dont offer protection against a man-in-the-middle. Such an attacker might just forward the clients challenge to the real server, get the correct answer and again forward this to the client.

-The server identifies clients using their IP-Address (which is easily forgable). An attacker can send a cookie request to the server using the clients IP and the server will send the clients cookie to this IP encrypted with the Public Key attached to the request. Since the attacker chose this Public Key, he can intercept the response and decrypt the cookie.
The cookie can then be used to calculate MACs and masquerade as the server. (We wrote proof-of-concept code for this last attack and were able to change a clients time as a man-in-the-middle)

Stephen

On 08/02/11 22:23, Greg Dowd wrote:
> Hi Stephen,
> I am very interested in your analysis. Do you have any plans to publish the results in English? If not, are the results available in German? I have a number of German colleagues and I may be able to ask them to translate the document for us.
>
>
> Greg Dowd
> gdowd at symmetricom dot com (antispam format)
> Symmetricom, Inc.
> www.symmetricom.com
> "Everything should be made as simple as possible, but no simpler" Albert Einstein
> -----Original Message-----
> From: ntpwg-bounces+gdowd=symmetricom.com@lists.ntp.org [mailto:ntpwg-bounces+gdowd=symmetricom.com@lists.ntp.org] On Behalf Of Stephen Röttger
> Sent: Tuesday, August 02, 2011 1:12 PM

> To: NTP Working Group
> Subject: [ntpwg] Autokey-Protocol Analysis
>
> Hello everyone,
>
> Since the discussion about the Autokey-Protocol in June ended abruptly,
> we want to inform you, that we finished our analysis of the protocol and
> found several weaknesses, that render it completely useless.
> Our analysis is in German, but if you are interested in it, we can
> summarize the weaknesses for you.
>
> In addition, we came up with some changes to the protocol, that mitigate
> the vulnerabilities and would like to present you a revised
> Autokey-protocol.
> The changes are:
>
> -Use the Clients Public Key used for cookie-encryption as input to the
> cookie calculation. For example, calculate the Cookie as
> C = H(PubKey, ServerSeed).
>
> -Change the length of Cookie and Server Seed from 32 to 128 bit.
>
> -Replace the Identity Schemes with a common X.509 PKI, where the Clients
> are in possession of certificates of Trusted Authorities
>
> -Let the Signature included in extension fields cover the whole
NTP-packet
>
> -(optional) use HMAC for MAC-calculation and switch the used
> Hash-Algorithms to SHA-256
>
> Regards,
> Dieter Sibold and Stephen Röttger
> _____
> ntpwg mailing list
> ntpwg@lists.ntp.org
> http://lists.ntp.org/listinfo/ntpwg

_____
ntpwg mailing list
ntpwg@lists.ntp.org
http://lists.ntp.org/listinfo/ntpwg

----------020506010800050600070908

Content-Type: text/html; charset=ISO-8859-1
Content-Transfer-Encoding: 7bit

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
<head>

<meta http-equiv="content-type" content="text/html; charset=ISO-8859-1">
</head>
<body bgcolor="#ffffff" text="#000000">
Your Honor -
I have repeatedly submitted "evidence quality" concerns with how the SmartGrid is being designed and deployed and this is one of the evidences that this concern is warranted. This is a piece of email (with the header intact) which shows that there are serious security problems in how time data is securely managed in networking systems. What this means is that Time of Use Billing in the SmartGrid is subject to these issues and problems with time management. These control time distribution to the Meter and from the Meter to the Collection Point and all SubStation Automation components.

This document is from the NTP working group and is a factual complaint up before the Network Time Protocol group which was filed before them by the actual German National Standards Laboratory Group called the PTB. What this simply means is that no Utility has control over ToU Billing at this point because of their failure to manage the time services properly.

Formal notice of this communication is being served on the SG Service List today.

Todd Glassey

-------- Original Message --------
<table class="moz-email-headers-table" border="0" cellpadding="0" cellspacing="0">
<tbody>
<tr>
<th align="RIGHT" nowrap="nowrap" valign="BASELINE">From: </th>
<td>- Wed Aug 03 07:17:56 2011</td>
</tr>
<tr>
<th align="RIGHT" nowrap="nowrap" valign="BASELINE">X-Account-Key:
</th>
<td>account1</td>
</tr>

<tr>
<th align="RIGHT" nowrap="nowrap" valign="BASELINE">X-UIDL: </th>
<td>11e0-bdd4-034eabf2-a703-0021281794ea</td>
</tr>
<tr>
<th align="RIGHT" nowrap="nowrap" valign="BASELINE">X-Mozilla-Status:
</th>
<td>1011</td>
</tr>
<tr>
<th align="RIGHT" nowrap="nowrap" valign="BASELINE">X-Mozilla-Status2:
</th>
<td>00000000</td>
</tr>
<tr>
<th align="RIGHT" nowrap="nowrap" valign="BASELINE">X-Mozilla-Keys:
</th>
<td>
</td>
</tr>
<tr>
<th align="RIGHT" nowrap="nowrap" valign="BASELINE">Status: </th>
<td>U</td>
</tr>
<tr>
<th align="RIGHT" nowrap="nowrap" valign="BASELINE">Return-Path:
</th>
<td><a class="moz-txt-link-rfc2396E"
href="mailto:ntpwg-bounces+tglassey=earthlink.net@lists.ntp.org"><ntpwg-
bounces+tglassey=earthlink.net@lists.ntp.org></td>

</tr>
<tr>
<th align="RIGHT" nowrap="nowrap" valign="BASELINE">Received:
</th>
<td>from mx-mcdonald.atl.sa.earthlink.net ([207.69.195.177])
by mdl-quaff.atl.sa.earthlink.net (EarthLink SMTP Server)
with SMTP id 1qOBrE4zJ3Nl3423; Wed, 3 Aug 2011 09:25:10
-0400 (EDT)</td>
</tr>
<tr>
<th align="RIGHT" nowrap="nowrap" valign="BASELINE">Received:
</th>
<td>from lists.ntp.org ([149.20.68.7]) by
mx-mcdonald.atl.sa.earthlink.net (EarthLink SMTP Server)
with ESMTP id 1qOBrs5O83Nl36F0 for
<a class="moz-txt-link-rfc2396E"

```
href="mailto:tglassey@earthlink.net">&lt;tglassey@earthlink.net&gt;</a>;
Wed, 3 Aug 2011 09:24:58
        -0400 (EDT)</td>
</tr>
<tr>
<th align="RIGHT" nowrap="nowrap" valign="BASELINE">Received:
</th>
<td>from lists.ntp.org (lists.ntp.org [149.20.68.7]) by
        lists.ntp.org (Postfix) with ESMTP id 9844E86D762 for
<a class="moz-txt-link-rfc2396E"
href="mailto:tglassey@earthlink.net">&lt;tglassey@earthlink.net&gt;</a>;
Wed, 3 Aug 2011 13:24:57
        +0000 (UTC)</td>
</tr>
<tr>
<th align="RIGHT" nowrap="nowrap" valign="BASELINE">X-Original-To:
</th>
<td><a class="moz-txt-link-abbreviated"
href="mailto:ntpwg@lists.ntp.org">ntpwg@lists.ntp.org</a></td>
</tr>
<tr>
<th align="RIGHT" nowrap="nowrap" valign="BASELINE">Delivered-To:
</th>
<td><a class="moz-txt-link-abbreviated"
href="mailto:ntpwg@lists.ntp.org">ntpwg@lists.ntp.org</a></td>
</tr>
<tr>
<th align="RIGHT" nowrap="nowrap" valign="BASELINE">Received:
</th>
<td>from mail1.ntp.org (mail1.ntp.org
        [IPv6:2001:4f8:fff7:1::5]) by lists.ntp.org (Postfix) with
        ESMTP id 9D8F086D75D for <a class="moz-txt-link-rfc2396E"
href="mailto:ntpwg@lists.ntp.org">&lt;ntpwg@lists.ntp.org&gt;</a>; Wed, 3
        Aug 2011 12:55:59 +0000 (UTC)</td>
</tr>
<tr>
<th align="RIGHT" nowrap="nowrap" valign="BASELINE">Received:
</th>
<td>from mailfront3.rz.tu-bs.de ([134.169.12.134]
        helo=tu-bs.de) by mail1.ntp.org with esmtp (Exim 4.75
        (FreeBSD)) (envelope-from <a class="moz-txt-link-rfc2396E"
href="mailto:s.roettger@tu-bs.de">&lt;s.roettger@tu-bs.de&gt;</a>) id
        1QoazD-000Ak8-Pq for <a class="moz-txt-link-abbreviated"
href="mailto:ntpwg@lists.ntp.org">ntpwg@lists.ntp.org</a>; Wed, 03 Aug 2011
        12:55:59 +0000</td>
</tr>
<tr>
```

<th align="RIGHT" nowrap="nowrap" valign="BASELINE">Received:
</th>
<td>from [192.53.103.10] (account <a class="moz-txt-link-abbreviated"
href="mailto:y0034674@tu-braunschweig.de">y0034674@tu-braunschweig.de
HELO [192.168.4.193]) by rz.tu-bs.de (CommuniGate Pro SMTP
5.3.13) with ESMTPA id 8419739; Wed, 03 Aug 2011 14:55:39
+0200</td>
</tr>
<tr>
<th align="RIGHT" nowrap="nowrap" valign="BASELINE">Message-ID:
</th>
<td><a class="moz-txt-link-rfc2396E"
href="mailto:4E394471.3040903@tu-bs.de"><4E394471.3040903@tu-bs.de></td>
</tr>
<tr>
<th align="RIGHT" nowrap="nowrap" valign="BASELINE">Date: </th>
<td>Wed, 03 Aug 2011 14:52:01 +0200</td>
</tr>
<tr>
<th align="RIGHT" nowrap="nowrap" valign="BASELINE">From: </th>
<td>Stephen Röttger <a class="moz-txt-link-rfc2396E"
href="mailto:s.roettger@tu-bs.de"><s.roettger@tu-bs.de></td>
</tr>
<tr>
<th align="RIGHT" nowrap="nowrap" valign="BASELINE">User-Agent:
</th>
<td>Mozilla/5.0 (X11; U; Linux x86_64; en-US; rv:1.9.2.17)
Gecko/20110720 Lightning/1.0b3pre Thunderbird/3.1.10</td>
</tr>
<tr>
<th align="RIGHT" nowrap="nowrap" valign="BASELINE">MIME-Version:
</th>
<td>1.0</td>
</tr>
<tr>
<th align="RIGHT" nowrap="nowrap" valign="BASELINE">To: </th>
<td>Greg Dowd <a class="moz-txt-link-rfc2396E"
href="mailto:GDowd@symmetricom.com"><GDowd@symmetricom.com></td>
</tr>
<tr>
<th align="RIGHT" nowrap="nowrap" valign="BASELINE">References:
</th>
<td><a class="moz-txt-link-rfc2396E"
href="mailto:4E385A0B.70206@tu-bs.de"><4E385A0B.70206@tu-bs.de>

<a class="moz-txt-link-rfc2396E"
href="mailto:26FBD265CD8D234EAF41115A180F92BB38AF02AC@SJC-MBX-

01.symmetricom.com"><26FBD265CD8D234EAF41115A180F92BB38AF02AC@SJC-MBX-01.symmetricom.com></td>

</tr>
<tr>
<th align="RIGHT" nowrap="nowrap" valign="BASELINE">In-Reply-To:
</th>
<td><a class="moz-txt-link-rfc2396E"
href="mailto:26FBD265CD8D234EAF41115A180F92BB38AF02AC@SJC-MBX-01.symmetricom.com"><26FBD265CD8D234EAF41115A180F92BB38AF02AC@SJC-MBX-01.symmetricom.com></td>

</tr>
<tr>
<th align="RIGHT" nowrap="nowrap" valign="BASELINE">X-Enigmail-Version:
</th>
<td>1.1.2</td>
</tr>
<tr>
<th align="RIGHT" nowrap="nowrap" valign="BASELINE">X-SA-Exim-Connect-IP:
</th>
<td>134.169.12.134</td>
</tr>
<tr>
<th align="RIGHT" nowrap="nowrap" valign="BASELINE">X-SA-Exim-Rcpt-To:
</th>
<td><a class="moz-txt-link-abbreviated"
href="mailto:ntpwg@lists.ntp.org">ntpwg@lists.ntp.org</td>
</tr>
<tr>
<th align="RIGHT" nowrap="nowrap" valign="BASELINE">X-SA-Exim-Mail-From:
</th>
<td><a class="moz-txt-link-abbreviated"
href="mailto:s.roettger@tu-bs.de">s.roettger@tu-bs.de</td>
</tr>
<tr>
<th align="RIGHT" nowrap="nowrap" valign="BASELINE">X-Spam-Checker-Version:
</th>
<td>SpamAssassin 3.3.0 (2010-01-18) on mail1.ntp.org</td>
</tr>
<tr>
<th align="RIGHT" nowrap="nowrap" valign="BASELINE">X-Spam-Level:
</th>
<td>
</td>
</tr>
<tr>

<th align="RIGHT" nowrap="nowrap" valign="BASELINE">X-Spam-Status:
</th>
<td>No, score=-2.6 required=5.0
tests=BAYES_00,RCVD_IN_DNSWL_LOW, T_RP_MATCHES_RCVD
autolearn=ham version=3.3.0</td>
</tr>
<tr>
<th align="RIGHT" nowrap="nowrap" valign="BASELINE">X-SA-Exim-Version:
</th>
<td>4.2</td>
</tr>
<tr>
<th align="RIGHT" nowrap="nowrap" valign="BASELINE">X-SA-Exim-Scanned:
</th>
<td>Yes (on mail1.ntp.org)</td>
</tr>
<tr>
<th align="RIGHT" nowrap="nowrap" valign="BASELINE">Cc: </th>
<td>NTP Working Group <a class="moz-txt-link-rfc2396E"
href="mailto:ntpwg@lists.ntp.isc.org"><ntpwg@lists.ntp.isc.org>,
<a class="moz-txt-link-abbreviated"
href="mailto:dieter.sibold@ptb.de">dieter.sibold@ptb.de</td>
</tr>
<tr>
<th align="RIGHT" nowrap="nowrap" valign="BASELINE">Subject: </th>
<td>Re: [ntpwg] Autokey-Protocol Analysis</td>
</tr>
<tr>
<th align="RIGHT" nowrap="nowrap" valign="BASELINE">X-BeenThere:
</th>
<td><a class="moz-txt-link-abbreviated"
href="mailto:ntpwg@lists.ntp.org">ntpwg@lists.ntp.org</td>
</tr>
<tr>
<th align="RIGHT" nowrap="nowrap" valign="BASELINE">X-Mailman-Version:
</th>
<td>2.1.12</td>
</tr>
<tr>
<th align="RIGHT" nowrap="nowrap" valign="BASELINE">Precedence:
</th>
<td>list</td>
</tr>
<tr>
<th align="RIGHT" nowrap="nowrap" valign="BASELINE">List-Id: </th>
<td>IETF Working Group for Network Time Protocol

<ntpwg.lists.ntp.org></td>
</tr>
<tr>
<th align="RIGHT" nowrap="nowrap" valign="BASELINE">List-Unsubscribe:
</th>
<td><a class="moz-txt-link-rfc2396E"
href="http://lists.ntp.org/options/ntpwg"><http://lists.ntp.org/options/ntpwg>,
<a class="moz-txt-link-rfc2396E"
href="mailto:ntpwg-request@lists.ntp.org?subject=unsubscribe"><mailto:ntpwg-
request@lists.ntp.org?subject=unsubscribe></td>

</tr>
<tr>
<th align="RIGHT" nowrap="nowrap" valign="BASELINE">List-Archive:
</th>
<td><a class="moz-txt-link-rfc2396E"
href="https://lists.ntp.org/pipermail/ntpwg"><https://lists.ntp.org/pipermail/ntpwg></td>
</tr>
<tr>
<th align="RIGHT" nowrap="nowrap" valign="BASELINE">List-Post:
</th>
<td><a class="moz-txt-link-rfc2396E"
href="mailto:ntpwg@lists.ntp.org"><mailto:ntpwg@lists.ntp.org></td>
</tr>
<tr>
<th align="RIGHT" nowrap="nowrap" valign="BASELINE">List-Help:
</th>
<td><a class="moz-txt-link-rfc2396E"
href="mailto:ntpwg-request@lists.ntp.org?subject=help"><mailto:ntpwg-
request@lists.ntp.org?subject=help></td>
</tr>
<tr>
<th align="RIGHT" nowrap="nowrap" valign="BASELINE">List-Subscribe:
</th>
<td><a class="moz-txt-link-rfc2396E"
href="http://lists.ntp.org/listinfo/ntpwg"><http://lists.ntp.org/listinfo/ntpwg>,
<a class="moz-txt-link-rfc2396E"
href="mailto:ntpwg-request@lists.ntp.org?subject=subscribe"><mailto:ntpwg-
request@lists.ntp.org?subject=subscribe></td>

</tr>
<tr>
<th align="RIGHT" nowrap="nowrap" valign="BASELINE">Content-Type:
</th>
<td>text/plain; charset="iso-8859-1"</td>
</tr>
<tr>
<th align="RIGHT" nowrap="nowrap"

valign="BASELINE">Content-Transfer-Encoding:
</th>
<td>quoted-printable</td>
</tr>
<tr>
<th align="RIGHT" nowrap="nowrap" valign="BASELINE">Sender: </th>
<td><a class="moz-txt-link-abbreviated"
href="mailto:ntpwg-bounces+tglassey=earthlink.net@lists.ntp.org">ntpwg-
bounces+tglassey=earthlink.net@lists.ntp.org</td>

</tr>
<tr>
<th align="RIGHT" nowrap="nowrap" valign="BASELINE">Errors-To:
</th>
<td><a class="moz-txt-link-abbreviated"
href="mailto:ntpwg-bounces+tglassey=earthlink.net@lists.ntp.org">ntpwg-
bounces+tglassey=earthlink.net@lists.ntp.org</td>

</tr>
<tr>
<th align="RIGHT" nowrap="nowrap" valign="BASELINE">X-ELNK-Received-Info:
</th>
<td>spv=0;</td>
</tr>
<tr>
<th align="RIGHT" nowrap="nowrap" valign="BASELINE">X-ELNK-AV:
</th>
<td>0</td>
</tr>
<tr>
<th align="RIGHT" nowrap="nowrap" valign="BASELINE">X-ELNK-Info:
</th>
<td>sbv=0; sbrc=.0; sbf=0b; sbw=000;</td>
</tr>
</tbody>
</table>

<pre>Greg,
Yes, there are plans to publish the results in english.
The german version is not public yet, but presumably will be in a few weeks.
However I can summarize the discovered vulnerabilities (mainly for
client-server-mode):

-The bitlenghts of the cookie and the server seed are only 32 Bit long.
This leads to an attacker being able to Brute Force them.
For example he can request a cookie from a server and try all 2^32

possibilites as server seed and calculate corresponding cookies. If he finds one that matches the cookie he received from the server, he has found the secret server seed and can consequently calculate cookies for every client.
The same applies for brute-forcing the cookie. The attacker can intercept a packet with a MAC and try to generate the MAC himself using every possible of the 2^32 cookie-values, till he found the one that matches.
For comparison, 2^32 MD5 calculations take roughly 25minutes on my 2.5ghz laptop using only one thread. (though cookie brute-forcing will take 2 MD5 calculations for each try)

-The Identity Schemes (except the private certificate scheme) provide no security.
The TC scheme accepts a certificate as that of a Trusted Authority if it includes a extension CA=True. Nothing prevents an attacker from generating such a certificate himself.
We discovered a flaw in all three challenge-response identity schemes (IFF, MV, GQ), that allowed us to send a response that would always be accepted by the client. In addition, the challenge-response schemes dont offer protection against a man-in-the-middle. Such an attacker might just forward the clients challenge to the real server, get the correct answer and again forward this to the client.

-The server identifies clients using their IP-Address (which is easily forgable). An attacker can send a cookie request to the server using the clients IP and the server will send the clients cookie to this IP encrypted with the Public Key attached to the request. Since the attacker chose this Public Key, he can intercept the response and decrypt the cookie.
The cookie can then be used to calculate MACs and masquerade as the server.
(We wrote proof-of-concept code for this last attack and were able to change a clients time as a man-in-the-middle)

Stephen

On 08/02/11 22:23, Greg Dowd wrote:

> Hi Stephen,
> I am very interested in your analysis. Do you have any plans to publish the results in English? If not, are the results available in German? I have a number of German colleagues and I may be able to ask them to translate the document for us.
>
>
> Greg Dowd

> gdowd at symmetricom dot com (antispam format)
> Symmetricom, Inc.
> <a class="moz-txt-link-abbreviated"
href="http://www.symmetricom.com">www.symmetricom.com
> "Everything should be made as simple as possible, but no simpler"
Albert Einstein
> -----Original Message-----
> From: <a class="moz-txt-link-abbreviated"
href="mailto:ntpwg-bounces+gdowd=symmetricom.com@lists.ntp.org">ntpwg-
bounces+gdowd=symmetricom.com@lists.ntp.org
[<a class="moz-txt-link-freetext"
href="mailto:ntpwg-bounces+gdowd=symmetricom.com@lists.ntp.org">mailto:ntpwg-
bounces+gdowd=symmetricom.com@lists.ntp.org]

On Behalf Of Stephen Röttger

> Sent: Tuesday, August 02, 2011 1:12 PM
> To: NTP Working Group
> Subject: [ntpwg] Autokey-Protocol Analysis
>
> Hello everyone,
>
> Since the discussion about the Autokey-Protocol in June ended abruptly,
> we want to inform you, that we finished our analysis of the
protocol and
> found several weaknesses, that render it completely useless.
> Our analysis is in German, but if you are interested in it, we can
> summarize the weaknesses for you.
>
> In addition, we came up with some changes to the protocol, that
mitigate
> the vulnerabilities and would like to present you a revised
> Autokey-protocol.
> The changes are:
>

> -Use the Clients Public Key used for cookie-encryption as input to the
> cookie calculation. For example, calculate the Cookie as
> C = H(PubKey, ServerSeed).
>
> -Change the length of Cookie and Server Seed from 32 to 128 bit.
>
> -Replace the Identity Schemes with a common X.509 PKI, where the
Clients
> are in possession of certificates of Trusted Authorities
>
> -Let the Signature included in extension fields cover the whole
NTP-packet

>
> -(optional) use HMAC for MAC-calculation and switch the used
> Hash-Algorithms to SHA-256
>
> Regards,
> Dieter Sibold and Stephen Röttger

> _____
> ntpwg mailing list
> <a class="moz-txt-link-abbreviated"
href="mailto:ntpwg@lists.ntp.org">ntpwg@lists.ntp.org
> <a class="moz-txt-link-freetext"
href="http://lists.ntp.org/listinfo/ntpwg">http://lists.ntp.org/listinfo/ntpwg

_____
ntpwg mailing list
<a class="moz-txt-link-abbreviated"
href="mailto:ntpwg@lists.ntp.org">ntpwg@lists.ntp.org
<a class="moz-txt-link-freetext"
href="http://lists.ntp.org/listinfo/ntpwg">http://lists.ntp.org/listinfo/ntpwg

</pre>
</body>
</html>

----------020506010800050600070908--

--
Todd S. Glassey
This is from my personal email account and any materials from this account come with personal disclaimers.

Further I OPT OUT of any and all commercial emailings.