Order Instituting Rulemaking to Consider Smart Grid Technologies Pursuant to Federal Legislation and on the Commission's own Motion to Actively Guide Policy in California's Development of a Smart Grid System.

Rulemaking 08-12-009 (Filed December 18, 2008)

COMMENTS OF CERTICHRON REGARDING THE PROPOSED DECISION OF PRESIDENT PEEVEY ADOPTING RULES TO PROTECT THE PRIVACY AND SECURITY OF CUSTOMER USAGE DATA GENERATED BY SMART METERS

1.	BAC	KGROUND AND DISCUSSION	2
	1.1. 1.2. 1.3.	PROTECTING THE SECURITY OF CUSTOMER USE AND IDENTITY DATA IS KEY SECURING THE DATA AND IN CONTROLLING ACCESS TO THE SYSTEMS CREATING IT THE REMAINDER OF THIS RESPONSE	2 2 2
2.	HOU	STON WE HAVE A PROBLEM	3
	2.1. <i>2.1.1</i> .	NTP HOLES Scope of this liability	3 3
3.	THE	UNDERLYING RESEARCH WAS DONE BY THE GERMAN GOVE RNMENT	4
4.	TIM	E-SENSITIVE AUTOMATION PRACTICES MUST BE REVIEWE D	4
	4.1. 4.2.	SMARTGRID DESIGN NEEDS A FULL TIME-SERVICE REVIEW REVIEW OF TOU BILLING AND TIME COLLECTION/CONTROL	5 5
5.	3. TI	ECHNOLOGY STATEMENT: THE PTB AND THEIR WORK	5
	5.1. 5.1.1. 5.1.2. 5.1.3.	THE FOUR SUCCESSFUL ATTACKS #1 and #2 - NTP Cookie Key's are too short	2 2 2 3 3 3 4 4 5 5 5 6 6 6 6 7 7 8 9 9 10 10 11 11 12
6.	WHA	AT DOES THIS ACTUALLY MEAN?	7
	6.1. 6.2. 6.3.	IF THIS TECHNICAL ISSUE WAS SO GREAT – WHY IS IT JUST SURFACING? How is that possible? NTP is everywhere	8 9 9
7.	WHA	AT TO DO THEN?	10
	7.1. 7.2.	IS THE CALIFORNIA SMART GRID SAFE?	10 10
8.	ATT	ACHMENT #1 – PTB COMMENTARY TO NTP.ORG	11
9. H	ATT. OLES	ACHMENT #2 – DR. DAVID MILLS COMMENTARY ABOUT FI XING THE NTP	12

Todd S. Glassey CISM CIFI CTO Certichron inc <u>TGlassey@Certichron.COM</u> 800-511-2301 x233

1. Background and Discussion

A motion extending the filing dates until October 7th 2011¹ was put in place and under

that extension the following commentary is being submitted for notice.

1.1. Protecting the Security of Customer Use and Id entitv Data is key

Certichron believes that the core functional requirements of protecting customer data are real but that they point to a larger issue and that is of the failing of the existing architecture from both a security standpoint and that also of an evidence generation standpoint and that it is these issues which need real attention. Certichron believes that all Customer use data should be protected and unavailable as a tool for marketing or building a sales model

1.2. Securing the Data and in Controlling Access to the Systems creating it

Certichron also believes that the basis of this security is a systemic one which must flow from the top down. Bolt-on security (adding band-aid after band-aid) is not a win for the people of the State, or the Utilities in the long run since they will all wind up making proper evidence changes in the operations of their distribution and billing systems anyway.

1.3. The remainder of this response

To address this, the focus of remainder of this commentary pertains to a technology flaw in the protocol used in moving time data around networks which directly impacts not only Time of Use billing and the sanctity/privacy of customer records pertaining to their time of use information, but also to services which can be used to 'hack' the end-node

Page 2

meters through their dependence on the same software systems for time management. . This by the way was the specific goal of last years denied 700015 Petition on embracing new Digital Evidence Standards?

2. Houston we have a problem...

There is a problem with how time data in the electronic infrastructure of the Smart Grid is propagated and logged. The problem is not the grid itself but one of the underlying tools which is now the sole key method of moving time data around networks today. That means to address this "the Grid's design" must be reviewed with regard to these issues.

The issue we bring up today is one newly documented 'holes' in the security of the Network Time Protocol and its operations.

2.1. NTP Holes

These holes in the NTP protocol allow for covert operators to intercept and take control of the time-service relationship such that the time practices are at risk without a very strong evidence-envelope being created around the operations of this software as it exists today.

2.1.1. Scope of this liability

This problem directly impacts the provability and security around time-based controls used in all parts of the California Utility and Service Grid. It also pertains to the ability to manipulate that to cause both errors in logging (hence billing) but also in direct attacks against the critical infrastructure based in 'being able to manipulate time-critical events' in the operations of that subsystem.

8/10/2011

As such the reliability of any time-of-use data coming from any of the testimony-sources in the Smart Grid is not only at risk but attacks against the system are now proven risks such that certain Sub-Station Automation processes must also be reviewed, especially in time-specific management of power or gas deployment controls.

3. The Underlying Research was done by the German Government

The underlying research and the building of the test case to prove this assertion was performed by the German National Standards Lab, the PTB who just formally notified the NTP *(Network Time Protocol) WG that they have successfully implemented the attack code and they have successfully changed or altered time-in-control systems through this process. See the attachments to this notice.

This document supports that assertion by documenting the actual commentary and providing an analysis of the security risk therein.

4. Time-Sensitive Automation Practices must be reviewed

Further, since other attacks against Critical Infrastructure can be accomplished by timedata attacks including Effluent release, Processing shut-down in Water, Sewage and Steam systems and Power-System failures based on switching shutdowns and other "Sub-Station Automation attacks" basked on these underlying time-data attacks against the NTP liabilities.

4.1. SmartGrid Design needs a full Time-Service Rev iew We believe that in the public interest, at this time the only responsible action is the ordering of a full time-practice design review on the operations of the California Critical Infrastructure, the halting of all additional SmartGrid roll out until that is completed and over the longer term potentially a response through the CPUC itself in creating a uniform state-wide source of trusted digital time for all Utility Operations therein.

4.2. Review of ToU billing and Time Collection/Cont rol

What this means simply is that the time-transfer and time-of-day billing controls must be rethought and fully tested as to their security risks prior to being authorized by CPUC for production use in the State of California.

5. 3. Technology Statement: The PTB and their work

The German Governments National Standards Labs (The PTB) has formally attested to the Network Time Protocol flaws they have developed attacks for are real and part of the existing deployment.

Their attack code proved the four key design flaws which would have been caught in any serious testing process. The question is why the commercial providers of NTP didn't test that code either. In fact these flaws were disclosed as possibilities several years ago so it

should come as no surprise that the protocol by design is flawed in ways that probably cannot be easily fixed.

5.1. The four successful attacks

The PTB successfully implemented three direct and one indirect attack including bruteforce computational attacks which took a mere 25 minutes on a medium performance laptop with only limited resources assigned to the attack.

5.1.1. #1 and #2 - NTP Cookie Key's are too short

The BRUTE FORCE attack in question sorted 2³² (4 billion) possible key types and successfully found the correct one in under 25 minutes. This means form that point onward the attacker was capable of doing anything they wanted to the client-side clocks including resetting them or speeding them up or conversely slowing them down. The same was true for their second attack form which also used a Cookie calculation attack.

5.1.2. #3 - The three NTP PKI Identities available through NTP Autokey are easily forged

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 an extension 'CA=True'. Nothing prevents an attacker from generating such a certificate himself.

The PTB discovered a flaw in all three Autokey challenge-response identity schemes (IFF, MV, GQ), that allowed them to send a response that would always be accepted by the client.

In addition, the challenge-response schemes don't offer protection against a man-in-themiddle or reply attack. Such an attacker might just forward the clients challenge to the real server, get the correct answer and again forward this to the client.

5.1.3. #4 - IP Spoofing, the last exploit which was proven The NTP protocol identifies clients using their IP-Address (which is easily forgeable). To accomplish this attack, 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 in the request itself, he can intercept the response and decrypt the cookie. The cookie can then be used to calculate MACs and masquerade as the server.

6. What does this actually mean?

tsg

Since the PTB wrote proof-of-concept code for this last attack and were able to change a clients time as a man-in-the-middle this is very serious.

What this means is that NTP data is not reliable by itself. It must have corroboration and support from other logging instances to prove anything about anything. That means

8/10/2011

Packet Sniffing, Syslog harvesting, and NTP Log Management in ways most people are unwilling to expend that level of effort, meaning what they get is uncertainty and unprovability in their data logs.,

NTP is used to prosecute crimes and so its data must be capable of being cross-examined. But how would you cross examine logs which could have been spoofed or fabricated from vapor?

This is a key question about the technology but the real underlying issue is what to do about protocols which are producing data which is being used in both criminal and civil prosecutions which we are now finding was open to tampering in ways which would have been undetectable. Bluntly there is no way without a comprehensive control process to rely on NTP data as being provable from a forensic standpoint.

The next issue is in dealing with the WG itself in that key members of the WG blocked the public disclosure of this liability and in solving it.

6.1. If this technical issue was so great – why is it just surfacing?

The reason it's just surfacing is that the German PTB went public. The NTP WG itself would never have disclosed this and still has no statement to anyone about the liabilities they now fully admit exist in the use of their protocol. Likewise no vendor has notified any of their customers to date that this liability in their systems exists, and certainly to date no Utility has disclosed this to the public either. All in all there is a functional wall-

of-silence in the technical world about this problem today. The reason is obvious – and that is that the world now relies on this protocol for many uses and they are all now at risk.

6.2. How is that possible?

From a historical standpoint how this is possible is that there is no real oversight for the management of the NTP standards effort. It (NTP.ORG) is a loosely managed group of volunteers and that means they handle what they can and what they want to.

Likewise above them in the Standards world, the IETF is also a volunteer run organization. Which explains why IETF Standards are free-form and consensus based.

But its only logical and clearly human nature that if the group who is supplying the only voices which the 'management listens to' as the consensus, then this lack of design and release oversight is what happens. Technologists driving themselves work on what they want to rather than some end-goal. It's a perfect example of herding a clan of cats.

6.3. NTP is everywhere

Why then is NTP in use everywhere? The answer is simple – there is no other choice. NTP is the best tool we have for transferring time across a TCP/IP network today. It replaced two earlier protocols called TIME and DAYTIME and provides a much better time synchronization service than either of its predecessors did.

7. What to do then?

NTP is going to continue to be used, there is no other choice, but where the time data comes from and how it's authenticated now need real cooperation. Unauthenticated sources of time and logging systems which fail to properly monitor time-transfer and time control practices must now do so.

7.1. Is the California Smart Grid safe?

Because of the complexity in these matters the CPUC now is faced with a fundamental issue with whether the Smart Grid is safe or whether manipulating the billing and ToU reporting is as easy as buying a GPS Jammer and then in attacking the NTP service running in the Collector Radio or Sub-Station Automation systems.

7.2. Stop the roll out until the safety and securit y issues can be proven safe

To that end we recommend that the CPUC consider freezing roll out until these issues can be properly addressed in the underlying technologies.

// Todd S. Glassey CISM CIFI, CTO Certichron Inc, 8.10.2011

Attachment #1 – Commentary from Stephen Roettger of the German National Standards organization the PTB

8. Attachment #1 – PTB commentary to NTP.ORG



8/10/2011

9. Attachment #2 – Dr. David Mills commentary about fixing the NTP holes

He Edit Yew Go Messape Events and Tanks Tools Help Get Mail - Munte - Address Book - Tag - Address Jonn - Search all messages Cult+K	Re: [ntpwg] Autokey-Protocol Analysis - Inbox - tglassey@earthlink.net - Mozilla T	Thunderbird	X
Get Mail • Write · Maddress Book · Tag · Mail-Spam · Search all messages. Circle · All · All · Search · All	ile Edit View Go Message Events and Tasks Tools Help		
A Indox - tglassey@ent E. Re [Itans] Concrete × E. Re [Intpung] Autokey_ × I. Re [Intpung] Autoke, × I. Re [Intpung] Autokey_Protocol Analysis from David L Millsä reply [Ret], forward archive Junk delete delete deletee	Get Mail • 🛃 Write • 📕 Address Book 🔰 Tag • 💚 Anti-Spam •	Search all messages <ctrl+k></ctrl+k>	م
<pre>thom David L Milled up reply is ' forward archive junk delete the integration of the provided of the prov</pre>	Inbox - tglassey@eart 🖂 Re: [itans] Concrete 🗴 🖂 Re: [ntpwg] Autoke	y × 🛛 🖂 Re: [ntpwg] Autok × 💷 🖻	•
<pre>Upier Reintprog Autokey-Protocol Analysis</pre>	from David L. Mills	reply list + forward archive junk dele	te :
<pre>b Styphen RöttgerM c ND Working Group entpwg@distantp.org.wd texpens hanks for your contributions in a security analysis of the Autokey protocol, although it might have wide posel in English. As it is, my German is decidedly rusky, but I could translate if necessary. Meanwhile, tf provide a counter of the Autokey protocol, although it might have wide posel in English. As it is, my German is decidedly rusky, but I could translate if necessary. Meanwhile, tf provide a counter of the AUTOKEY analysis of the AUTOKEY beau wile real-althoutes as you enor. you way analysis and most probably yours, identify two serious middleman hazards, what I call the cookie matcher and propaganda attacks. The former is a tough one to fix and may yield to your inaights, but I a for a loop as uggested fix. Any true fix has to consider both the server private value and some sort of lient private value, perhaps the host encryption key. or others that might be reading this message and for historical context, the original Autokey design was reviewed to no possible structure point for mew algorithms. One might observe this protocol is firthen years incrise and possible structure point for mew algorithms. One might observe this protocol is firthen years us and the specification was last reviewed in 2005. In any case, the existing code is specifically lesigned in a modular fashion and can be removed and replaced in whole or in part with evolved algorithms. Nee to our current discussion is on client/server mode that might be used by a national time server setwork, however, the algorithms and protocol also have to work in both basis and intenleaved modes, man the setup to hand as the sign intent of the protocol. It might have design the setup to the sociel the roundrip dely. Corrections for this are included, along with a constraint your institue infrastructure all. The MB is in on necessary and three are no provision for certificate restruct. However, the algorithms and protocol also have to work in both basis and inchereived in desis</pre>	ubject Re: [ntpwg] Autokey-Protocol Analysis	8/4/2011 9:13	3 AM
<pre>c NIP Working Group <ntpwg@wistsmp.org.d td="" techen,="" techen,<=""><td>to Stephen Röttger</td><td></td><td></td></ntpwg@wistsmp.org.d></pre>	to Stephen Röttger		
<pre>itephen; hanks for your contributions in a security analysis of the Autokey protocol, although it might have vider prove further refined my own analysis in the white paper Security Analysis of the MTP Protocol. trp://www.eccis.udol.edu/~milis/security.html, which includes probably the same vulnerabilities as you wport. your suggested fix. Any true fix has to consider both the server private value and some sort of licent private value, perhaps the host encryption key. or others that might be reading this message and for historical context, the original Autokey design was included and in an internal report. Subsequently in the early 2006s the design was reviewed by he STIPK task force, which resulted in a revised specification in late 2006. That RCG is firthen as reviewed by the STIPK task force, which resulted in a revised specification in late 2006. That RCG is firthen years dual on the specification was last reviewed in 2005. The document was submitted is an informational RCG and eventually published five years later as RCG 5006. That RCG is firthen years dual on the specification and can be removed and replaced in whole or in part with evolved algorithms. Note that our current discussion is on client/server mode that might be used by an ational time server extoxk. However, the algorithms and protocol also have to own in both basic and interleaved modes, and in so defined in the specification. I suppertyour analysis does not consider these modes, hain does, here continues to be issues in the initial volley in broadcast mode, where the present code does not mercisely calibrate the roundrip delay. Corrections for this are included, along with a careful analysis, a ntwhite paper Analysis and Simulation of the NTP On-Wire Protocols http://www.eecis udel.edu/-milis om/in.html. Here is a serious disconnect about the design intent of the protocol. It was designed to operate with no ersistive infrastructure at all. The DNS is not necessary and there are no provision for certificate and the substeme Analysis and S</pre>	cc NTP Working Group <ntpwg@lists.ntp.org></ntpwg@lists.ntp.org>	other actio	ns *
henks for your contributions in a security analysis of the Autokey protocol, although it sight have wider papeal in English. As it is, any German is decidely rusty, but I could translate if necessary. Neamahile, I inter further refined by own analysis in the white paper security Analysis of the MTP protocol <u>typ://www.eecis.udel.edu/-mills/security.html</u> , which includes probably the same vulnerabilities as you way and and most probably yours, identify two serious middleman hazards, what I call the cookie matcher and propagnda attacks. The former is a tough one to fix and may yield to your insights, but I an onfused by your suggested fix. Any true fix has to consider both the server private value and some sort of ilent private value, perhaps the host encryption key. For others that might be reading this message and for historical context, the original Autokey design was incrising as documented in an internal report. Subsequently in the early 2006s; that BCC is fifteen years and informational BCC and eventually published five years later as BCC 3006. That BCC is fifteen years and and the specification was last reviewed in 2005. In any case, the existing code is specifically lesigned in a modular fashion and can be removed and replaced in whole or in part with evolved algorithms. Note that our current discussion is on client/server mode that might be used by a miclinal time server letwork. However, the algorithms and protocol also have to own in both basic and intreleaved modes, and in yametric and broadcast modes. The algorithms and protocol also have to support multiple security groups, is defined in the specification. I supper your analysis does not consider these modes, buind modes, in the hist paper Analysis and Simulation of the NTP On-Mire Protocols http://www.eecis.udel.edu/-millis onire. Sing disconnect about the design intent of the protocol. It was designed to operate with no sistive infrastructure at all. The ONS is not necessary and there are no provision for certificate my supperion about signing the	stephen,		
Contrast by your suggested tix. Any true tix has to consider both the server private value and some sort or lient private value, perhaps the host encryption key. Sor others that might be reading this message and for historical context, the original Autokey design was ince 1996 as documented in an internal report. Subsequently in the early 2008s the design was reviewed by the STIME task force, which resulted in a revised specification in late 2005. That RFC is intend as target is an informational RFC and eventually published five years later as RFC 5906. That RFC is intend as target practice and a possible starting point for new algorithms. None might observe this protocol is fifteen years lid and the specification was last reviewed in 2005. In any case, the existing code is specifically lesigned in a modular fashion and can be removed and replaced in whole or in part with evolved algorithms. Note that our current discussion is on client/server mode that might be used by a national time server eleverk. However, the algorithms and protocol also have to work in both basic and interleaved modes, and in symmetric and broadcast modes. The algorithms and protocol also have to support multiple security groups, is defined in the specification. I suspect your analysis does not consider these modes, but mine does. here continues to be issues in the initial volley in broadcast mode, where the present code does not mercisely calibrate the roundtrip delay. Corrections for this are included, along with a careful analysis, in the white paper Analysis and Simulation of the NTP On-Wire Protocols http://www.eecis.udel.edu/-mills <u>forwire.html</u> . Nere is a serious disconnect about the design intent of the protocol. It was designed to operate with no usistive infrastructure at all. The DMS is not necessary and there are no provision for certificate erification of the model, it is apporting to the Mars spaceraft model suggested in Chapter 17 of my nok. Since the light time between Mars and Earth can be as much as 40 minutes, access	Thanks for your contributions in a security analysis of the Autokey p appeal in English. As it is, my German is decidedly rusty, but I coul nave further refined my own analysis in the white paper Security Ana <u>http://www.eecis.udel.edu/~mills/security.html</u> , which includes probat report. My analysis and most probably yours, identify two serious middleman h snatcher and propaganda attacks. The former is a tough one to fix and	protocol, although it might have wider ld translate if necessary. Meanwhile, alysis of the NTP Protocol bly the same vulnerabilities as you hazards, what I call the cookie d may yield to your insights, but I am	1
The or others that might be reading this message and for historical context, the original Autokey design was inca 1996 as documented in an internal report. Subsequently in the early 2008s the design was reviewed by the STIME task force, which resulted in a revised specification in late 2005. That ACC is intend as target practice and a possible starting point for new algorithms. One might observe this protocol is fifteen years lad and the specification was last reviewed in 2005. In any case, the existing code is specifically designed in a modular fashion and can be removed and replaced in whole or in part with evolved algorithms. Note that our current discussion is on client/server mode that might be used by a national time server retroxr. However, the algorithms and protocol also have to work in both basic and interleaved modes, and in yametric and broadcast modes. The algorithms and protocol also have to consider these modes, but mine does. here continues to be issues in the initial volley in broadcast mode, where the present code does not metasely calibrate the roundtrip delay. Corrections for this are included, along with a careful analysis, n the white paper Analysis and Simulation of the NTP On-Wire Protocol. It was designed to operate with no sistive infrastructure at all. The DNS is not necessary and there are no provision for certificate erification other than the trusted host, for example a national time server, while not the original notivation for this model, it is appropriate for the Mars spaceraft model suggested in Chapter 17 of my nok. Since the light wakward. Even so, the certificate format conforms to X.500v3 and the certificate right have observed is that, except for the glaring case of the cookie request, signatures are always computed offline. Signing something in a flux of 3000 requests per second is not an optice. Lookie length is asy to change, although it raises backward compatibility issues. As you might have noticed in recent locumentation, selection of any hash algo	confused by your suggested fix. Any true fix has to consider both the client private value, perhaps the host encryption key.	e server private value and some sort o	f
Note that our current discussion is on client/server mode that might be used by a national time server hetwork. However, the algorithms and protocol also have to work in both basic and interleaved modes, and in symmetric and broadcast modes. The algorithms and protocol also have to support multiple security groups, is defined in the specification. I suspect your analysis does not consider these modes, but mine does. there continues to be issues in the initial volley in broadcast mode, where the present code does not precisely calibrate the roundtrip delay. Corrections for this are included, along with a careful analysis, in the white paper Analysis and Simulation of the NTP On-Wire Protocols http://www.eecis.udel.edu/-mills 'onwire.html. There is a serious disconnect about the design intent of the protocol. It was designed to operate with no issistive infrastructure at all. The DNS is not necessary and there are no provision for certificate rerification other than the trusted host, for example a national time servery. While not the original totivation for this model, it is appropriate for the Mars spacecraft model suggested in Chapter 17 of my nock. Since the light time between Mars and Earth can be as much as 40 minutes, access to Earth infrastructure is highly awkward. Even so, the certificate format conforms to X.500v3 and the certificate rail is verified as in conformant PKI practice. 'our suggestion about signing the entire NTP packet has bee considered before. However, a constraint you tight have observed is that, except for the glaring case of the cookie request, signatures are always computed offline. Signing something in a flux of 3000 requests per second is not an option Heavehile, your suggestion on server cookie length and hash algorithm are highly useful. Cookie length is asy to change, although it raises backward compatibility issues. As you might have noticed in recent locumentation, selection of any hash algorithm supported by	For others that might be reading this message and for historical cont circa 1996 as documented in an internal report. Subsequently in the e the STIME task force, which resulted in a revised specification in la as an informational RFC and eventually published five years later as practice and a possible starting point for new algorithms. One might old and the specification was last reviewed in 2005. In any case, the designed in a modular fashion and can be removed and replaced in whol	text, the original Autokey design was early 2000s the design was reviewed by ate 2005. That document was submitted RFC 5906. That RFC is intend as targe observe this protocol is fifteen year e existing code is specifically le or in part with evolved algorithms.	E s
<pre>here is a serious disconnect about the design intent of the protocol. It was designed to operate with no assistive infrastructure at all. The DNS is not necessary and there are no provision for certificate verification other than the trusted host, for example a national time server, while not the original notivation for this model, it is appropriate for the Mars spacecraft model suggested in Chapter 17 of my pook. Since the light time between Mars and Earth can be as much as 40 minutes, access to Earth infrastructure is highly awkward. Even so, the certificate format conforms to X.500v3 and the certificate rail is verified as in conformant PKI practice. Your suggestion about signing the entire NTP packet has bee considered before. However, a constraint you light have observed is that, except for the glaring case of the cookie request, signatures are always computed offline. Signing something in a flux of 3000 requests per second is not an option Neanwhile, your suggestion on server cookie length and hash algorithm are highly useful. Cookie length is hasy to change, although it raises backward compatibility issues. As you might have noticed in recent locumentation, selection of any hash algorithm supported by the OpenSSL library is now possible. I suspect there is not much more to say, so I recommend these issues be raised and discussed by the working proup at an upcoming IETF meeting. I can't volunteer to do much, as my eyesight is dwindling to nothing and nessing with code is impractical. Nave tephen Röttger wrote:</pre>	Note that our current discussion is on client/server mode that might network. However, the algorithms and protocol also have to work in bo symmetric and broadcast modes. The algorithms and protocol also have as defined in the specification. I suspect your analysis does not co there continues to be issues in the initial volley in broadcast mode, precisely calibrate the roundtrip delay. Corrections for this are inc in the white paper Analysis and Simulation of the NTP On-Wire Protoco (onwire.html.	be used by a national time server oth basic and interleaved modes, and i to support multiple security groups, onsider these modes, but mine does. , where the present code does not cluded, along with a careful analysis, ols <u>http://www.eecis.udel.edu/~mills</u>	
Your suggestion about signing the entire NTP packet has bee considered before. However, a constraint you hight have observed is that, except for the glaring case of the cookie request, signatures are always computed offline. Signing something in a flux of 3000 requests per second is not an option Neanwhile, your suggestion on server cookie length and hash algorithm are highly useful. Cookie length is easy to change, although it raises backward compatibility issues. As you might have noticed in recent locumentation, selection of any hash algorithm supported by the OpenSSL library is now possible. Suspect there is not much more to say, so I recommend these issues be raised and discussed by the working roup at an upcoming IETF meeting. I can't volunteer to do much, as my eyesight is dwindling to nothing and messing with code is impractical. Nave	There is a serious disconnect about the design intent of the protocol assistive infrastructure at all. The DNS is not necessary and there a verification other than the trusted host, for example a national time motivation for this model, it is appropriate for the Mars spacecraft book. Since the light time between Mars and Earth can be as much as 4 infrastructure is highly awkward. Even so, the certificate format co trail is verified as in conformant PKI practice.	 It was designed to operate with no are no provision for certificate e server,. While not the original model suggested in Chapter 17 of my 40 minutes, access to Earth onforms to X.500v3 and the certificate 	
Meanwhile, your suggestion on server cookie length and hash algorithm are highly useful. Cookie length is easy to change, although it raises backward compatibility issues. As you might have noticed in recent locumentation, selection of any hash algorithm supported by the OpenSSL library is now possible. Is suspect there is not much more to say, so I recommend these issues be raised and discussed by the working proup at an upcoming IETF meeting. I can't volunteer to do much, as my eyesight is dwindling to nothing and messing with code is impractical. Nave Atephen Röttger wrote:	Your suggestion about signing the entire NTP packet has bee consideren night have observed is that, except for the glaring case of the cooki computed offline. Signing something in a flux of 3000 requests per se	ed before. However, a constraint you ie request, signatures are always econd is not an option	
suspect there is not much more to say, so I recommend these issues be raised and discussed by the working group at an upcoming IETF meeting. I can't volunteer to do much, as my eyesight is dwindling to nothing and lessing with code is impractical. Nave Rottger wrote:	Meanwhile, your suggestion on server cookie length and hash algorithm aasy to change, although it raises backward compatibility issues. As documentation, selection of any hash algorithm supported by the Opens	m are highly useful. Cookie length is you might have noticed in recent SSL library is now possible.	
lave Hephen Röttger wrote:	I suspect there is not much more to say, so I recommend these issues group at an upcoming IETF meeting. I can't volunteer to do much, as m messing with code is impractical.	be raised and discussed by the workin my eyesight is dwindling to nothing an	g d
itephen Röttger wrote:	Jave		
	Stephen Röttger wrote:		