

BEFORE THE PUBLIC UTILITIES COMMISSION OF
THE STATE OF CALIFORNIA

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. BACKGROUND AND DISCUSSION	2
1.1. PROTECTING THE SECURITY OF CUSTOMER USE AND IDENTITY DATA IS KEY	2
1.2. SECURING THE DATA AND IN CONTROLLING ACCESS TO THE SYSTEMS CREATING IT	2
1.3. THE REMAINDER OF THIS RESPONSE	2
2. HOUSTON WE HAVE A PROBLEM..	3
2.1. NTP HOLES.....	3
2.1.1. <i>Scope of this liability</i>	3
3. THE UNDERLYING RESEARCH WAS DONE BY THE GERMAN GOVERNMENT.....	4
4. TIME-SENSITIVE AUTOMATION PRACTICES MUST BE REVIEWED.....	4
4.1. SMARTGRID DESIGN NEEDS A FULL TIME-SERVICE REVIEW.....	5
4.2. REVIEW OF TOU BILLING AND TIME COLLECTION/CONTROL.....	5
5. 3. TECHNOLOGY STATEMENT: THE PTB AND THEIR WORK... ..	5
5.1. THE FOUR SUCCESSFUL ATTACKS.....	6
5.1.1. #1 and #2 - NTP Cookie Key's are too short.....	6
5.1.2. #3 - The three NTP PKI Identities available through NTP Autokey are easily forged.....	6
5.1.3. #4 - IP Spoofing, the last exploit which was proven.....	7
6. WHAT DOES THIS ACTUALLY MEAN?.....	7
6.1. IF THIS TECHNICAL ISSUE WAS SO GREAT – WHY IS IT JUST SURFACING?.....	8
6.2. HOW IS THAT POSSIBLE?.....	9
6.3. NTP IS EVERYWHERE	9
7. WHAT TO DO THEN?.....	10
7.1. IS THE CALIFORNIA SMART GRID SAFE?.....	10
7.2. STOP THE ROLL OUT UNTIL THE SAFETY AND SECURITY ISSUES CAN BE PROVEN SAFE	10
8. ATTACHMENT #1 – PTB COMMENTARY TO NTP.ORG.....	11
9. ATTACHMENT #2 – DR. DAVID MILLS COMMENTARY ABOUT FIXING THE NTP HOLES.....	12

Todd S. Glassey CISM CIFI
CTO Certichron inc
TGlassey@Certichron.COM
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 Identity 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

¹ See http://docs.cpuc.ca.gov/WORD_PDF/FINAL_DECISION/140_641.PDF

BEFORE THE PUBLIC UTILITIES COMMISSION OF
THE STATE OF CALIFORNIA

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.

BEFORE THE PUBLIC UTILITIES COMMISSION OF
THE STATE OF CALIFORNIA

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 time-data 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" based on these underlying time-data attacks against the

NTP liabilities.

4.1. SmartGrid Design needs a full Time-Service Review

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/Control

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

BEFORE THE PUBLIC UTILITIES COMMISSION OF
THE STATE OF CALIFORNIA

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 brute-force 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 2^{32} (4 billion) possible key types and successfully found the correct one in under 25 minutes. This means from 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.

BEFORE THE PUBLIC UTILITIES COMMISSION OF
THE STATE OF CALIFORNIA

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-the-middle 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?

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

BEFORE THE PUBLIC UTILITIES COMMISSION OF
THE STATE OF CALIFORNIA

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-

BEFORE THE PUBLIC UTILITIES COMMISSION OF
THE STATE OF CALIFORNIA

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?

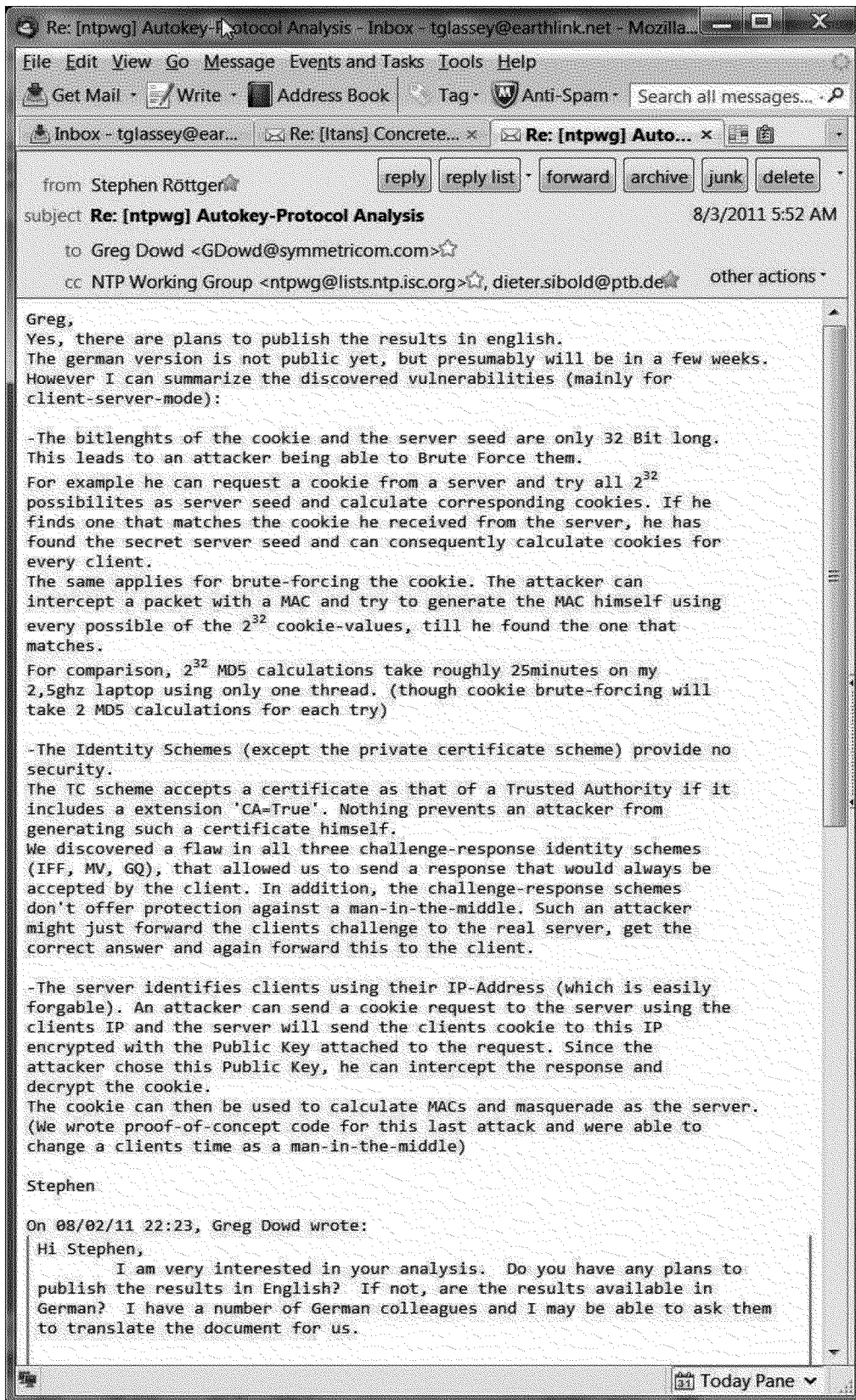
Because of the complexity in these matters the CPUC now is faced with a fundamental issue with whether the Smart Grid is safe or whether manipulating the billing and ToU reporting is as easy as buying a GPS Jammer and then in attacking the NTP service running in the Collector Radio or Sub-Station Automation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

7.2. Stop the roll out until the safety and security 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

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




Re: [ntpwg] Autokey-Protocol Analysis - Inbox - tglassey@earthlink.net - Mozilla...


File Edit View Go Message Events and Tasks Tools Help



Get Mail Write Address Book Tag Anti-Spam Search all messages...

Inbox - tglassey@ear... Re: [Itans] Concrete... Re: [ntpwg] Auto...

from Stephen Röttger  reply reply list forward archive junk delete

subject **Re: [ntpwg] Autokey-Protocol Analysis** 8/3/2011 5:52 AM

to Greg Dowd <GDowd@symmetricom.com> 

cc NTP Working Group <ntpwg@lists.ntp.isc.org> , dieter.sibold@ptb.de  other actions

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 bitlengths 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} possibilities 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 don't 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.

Today Pane

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

