Physikalisch-Technische Bundesanstalt
Braunschweig und Berlin
Nationales Metrologieinstitut

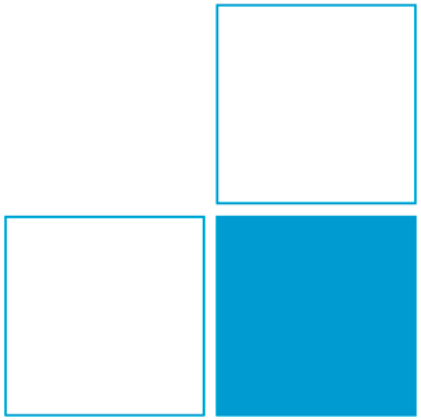
# Network Time Security (NTS)

**Dr. Dieter Sibold**

**Kristof Teichel**

**Stephen Röttger**

**19.02.2014**



# Agenda

- Einführung und Motivation
- Sicherheit im Network Time Protocol (NTP) oder Precision Time Protocol (PTP)
- Gefährdungen
- Sicherheitsanforderungen
- Zielsetzung für Network Time Security
- Konzept von Network Time Security
- Konformität mit bestehenden Sicherheitsanforderungen (IETF WG NTP/TICTOC und IEEE WG P1588)
- Nächste Schritte: Formale Verifikation

# Einführung und Motivation

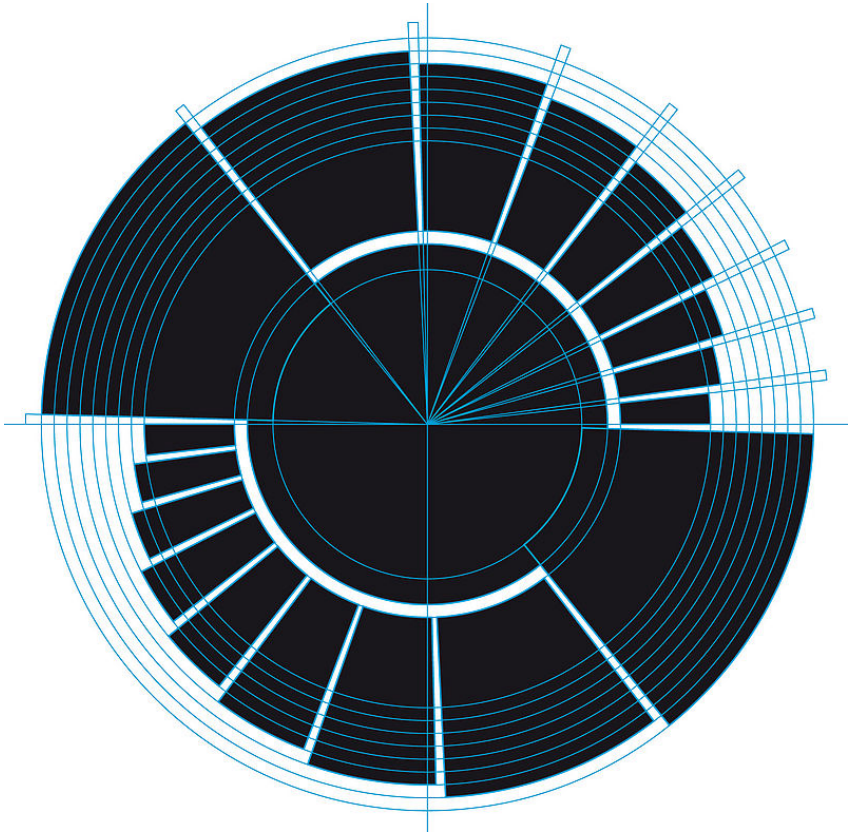
- **PTB ist gesetzlich mit der Weitergabe der Zeit in Deutschland beauftragt (§4 Einheiten- und Zeitgesetz).**

# Einführung und Motivation

- **PTB ist gesetzlich mit der Weitergabe der Zeit in Deutschland beauftragt (§4 Einheiten- und Zeitgesetz).**

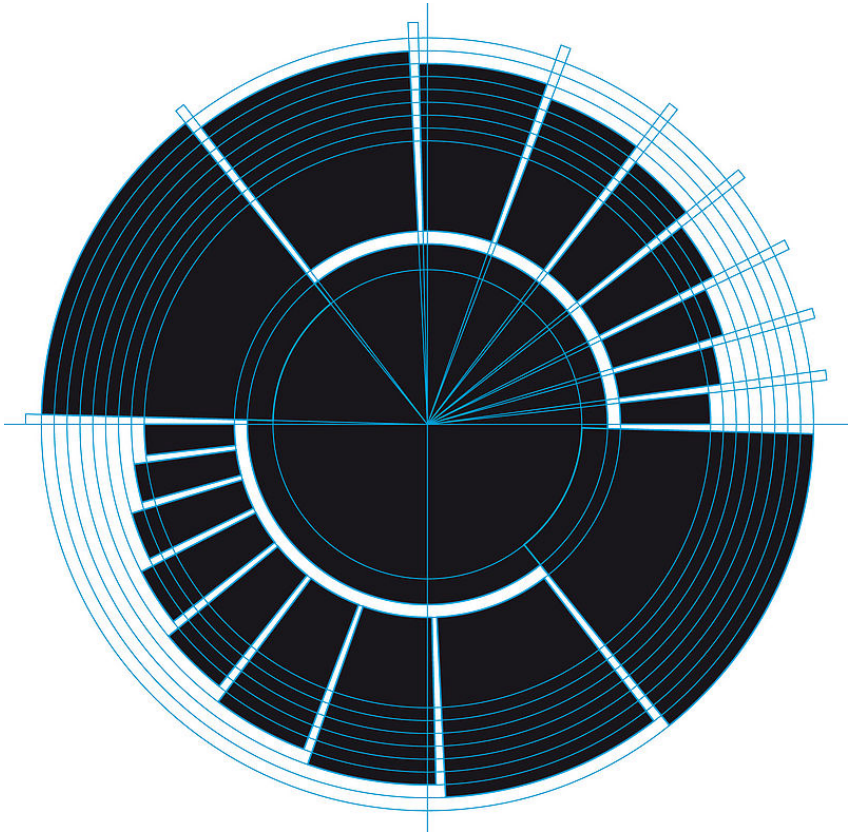
# Einführung und Motivation

- **PTB ist gesetzlich mit der Weitergabe der Zeit in Deutschland beauftragt (§4 Einheiten- und Zeitgesetz).**



# Einführung und Motivation

- **PTB ist gesetzlich mit der Weitergabe der Zeit in Deutschland beauftragt (§4 Einheiten- und Zeitgesetz).**



- **Logarithmisch geteilte 100-Stunden Uhr**

# Einführung und Motivation

- **PTB ist gesetzlich mit der Weitergabe der Zeit in Deutschland beauftragt (§4 Einheiten- und Zeitgesetz).**
- **Wird durchgeführt mittels:**
  - DCF77
  - Modemdienst
  - NTP
    - Zeitsynchronisation über UDP Port 123
    - Stateless im Server-Client-Modus

# Einführung und Motivation

**Bedeutung von Authentifizierung für Zeitweitergabe per NTP nimmt zu**

- Bedarf einer verlässlichen Zeitquelle für Smart Meter Gateway des Bunds (BSI TR-03109-1, PTB-A 50.8)
  - Einführung auf Grundlage der europäischen Binnenmarktrichtlinie 2009/72/EG und des nationalen Energiewirtschaftsgesetzes (§ 21 EnWG)
  - Messung des Energieverbrauchs
  - interne Tarifierung als Grundlage für Abrechnungen
  - Die Authentizität der Zeitquelle ist auf Grund eichrechtlicher Anforderungen notwendig.
- Authentifizierter öffentlichen Zeitdienst (z. B. auf Grund von Compliance-Anforderungen).

# Einführung und Motivation

**DDoS-Angriffe mittels NTP (2014)**

- *„DDoS Attack  Hits 400 Gbit/s, Breaks Record“* (Information Week, 2014-02-11)
- *„Attackers use NTP reflection in huge DDoS attack“* (Computer World, 2014-02-11)

**Diese Arbeit behandelt (noch) nicht dieses Problem!**

# Sicherheit im NTP und PTP

- **RFC 1305: Symmetrische Verfahren zur Integritätssicherung**
  - Funktioniert aber skaliert nicht.

- **RFC 5906: Autokey-Verfahren zur Authentifizierung und Integritätssicherung für NTP, basierend auf asymmetrischen kryptografischen Verfahren**
  - Diverse Schwachstellen (S. Röttger, 2011)

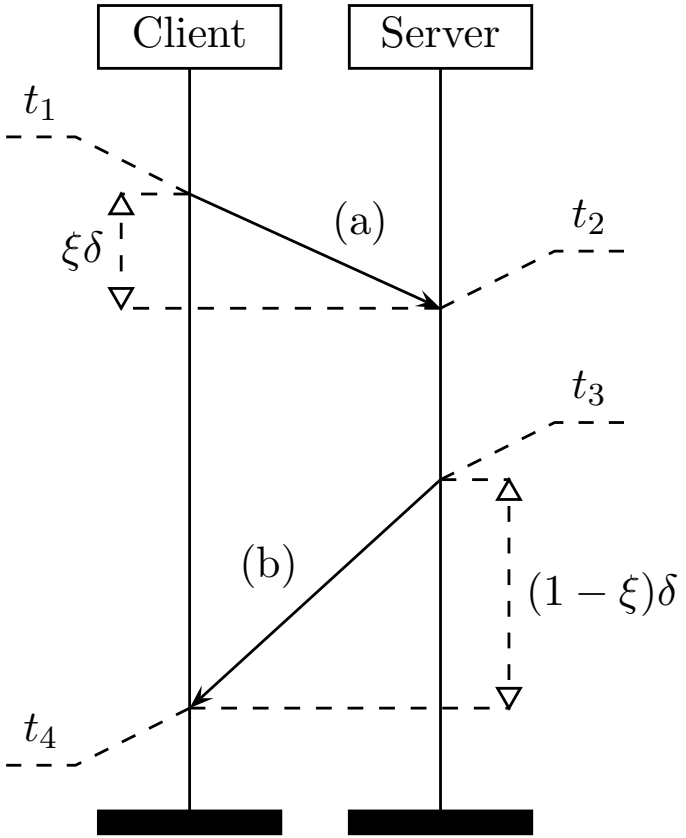
- **IEEE 1588 (PTP) verfügt über ein experimentelles Sicherheitsprotokoll im Annex K**
  - Keine Implementierung

# Gefährdungen

Tal Mizrahi, *Security Requirements of Time Protocols in Packet Switched Networks*, Internet-Draft (in Vorbereitung), Okt. 2013

# Gefährdungen

Tal Mizrahi, *Security Requirements of Time Protocols in Packet Switched Networks*, Internet-Draft (in Vorbereitung), Okt. 2013




**Diese Gefährdungen entziehen sich kryptographischer Sicherungsmethoden**

- **Reference Time Spoofing**
  GPS, DCF77
- **Packet Delay Attack**
  Zeitverfälschung durch asymmetrische Verzögerung des Paketaustausches

# Sicherheitsanforderungen

- Integritätsschutz der Zeitsynchronisationspakete
- Sichere Authentifizierung des Zeitservers (Master)
- Kein Vertraulichkeitsschutz
- Schutz vor DoS-Angriffen auf Ebene des Synchronisierungsprotokolls

- Die Kryptografie darf nur minimale Latenzzeiten einführen, um das Zeitsynchronisations-Protokoll nicht *ad absurdum* zu führen.
  - Max. Fehler bei der Bestimmung des Zeitunterschiedes ist durch $\delta/2$ gegeben.
  - $\delta$ und die Asymmetrie ($|\xi-1/2|$) werden durch kryptographische Berechnungen erhöht.

# Zielsetzung für das NTS-Protokoll (1)

**Die Entwicklung des NTS-Protokolls ist noch nicht abgeschlossen. Anregungen werden daher gern aufgenommen.**

- **Authentizität:** Das NTS-Protokoll soll dem Client ermöglichen, seinen Zeitserver zu authentifizieren.
- **Integrität:** Das NTS-Protokoll soll die Integrität von Zeitsynchronisationspaketen durch einen Message Authentication Code (MAC) sichern.
- **Vertraulichkeit:** Das NTS-Protokoll soll keine Vertraulichkeit von Zeitinformationen sicherstellen.
- Das NTS-Protokoll darf nur **minimale Latenzzeiten** verursachen.
- Die Ressourcen-Anforderungen sollen gering sein.

# Zielsetzung für das NTS-Protokoll (2)

- Alle **Betriebsmodi** von NTP sollen unterstützt werden.
- **Betriebsmodi** von PTP sollen (wenn möglich) unterstützt werden.
- **Hybrid-Modus:** Server und Clients sollen jeweils sowohl gesicherte als auch ungesicherte Verbindungen betreiben können.
- **Kompatibilität (NTP):**
  - Ungesicherte NTP-Verbindungen sollen unbeeinflusst bleiben.
  - Ein NTP-Server der das NTS-Protokoll nicht unterstützt soll durch Anfragen über gesicherte NTS-Verbindungen unbeeinflusst bleiben.

# Konzept / Grundlegende Arbeitsweise (1)

**Authentifizierung**

Einmalige Authentifizierung (zertifikatbasiert mittels X.509-Zertifikaten)

**Integritätssicherung**

**Erfolgt über einen Message Authentication Code (MAC) basierend auf einem Keyed-Hash Message Authentication Code (HMAC).**

- **Unicast-Modus (Client-Server):**
  - Unicast-Verbindungen sollen auf Serverseite zustandslos sein.
  - Für jede Client-Server-Verbindung gibt es einen „Cookie“ (shared secret), den der Server jederzeit erneut generieren kann und der zu Beginn, nach Authentifizierung des Servers, einmalig dem Client übermittelt wird (gesichert durch asymmetrische kryptografische Verfahren).
  - Der Cookie wird als Schlüssel für den MAC verwendet.

# Konzept / Grundlegende Arbeitsweise (2)

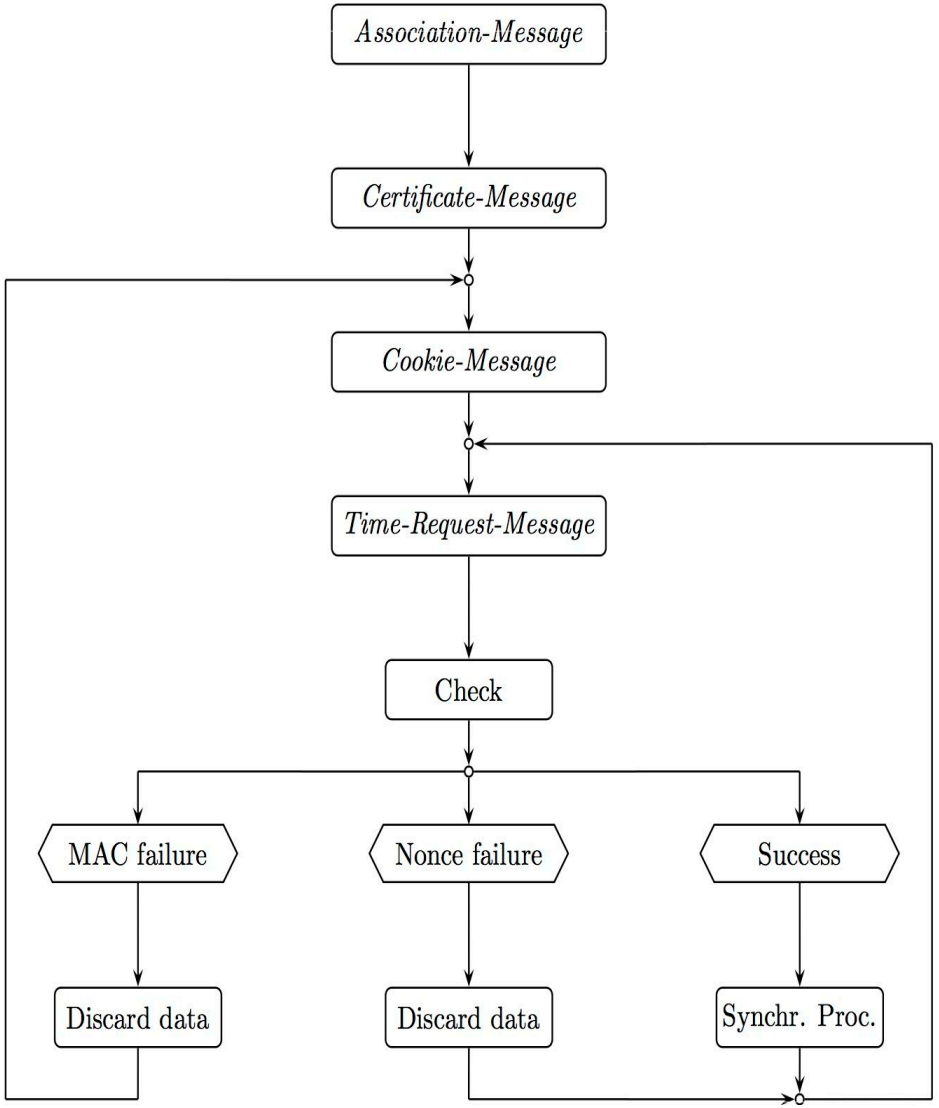
- **Broadcast-/Multicast-Modus**
  - Verwendung des TESLA-Protokolls (RFC 4082)
    - Erfordert vorherige grobe Zeitsynchronisation zwischen Client und Broadcast-Server (erfolgt über Unicast-Modus)
    - Für jedes Paket wird ein MAC mit einem Schlüssel aus einer Ein-Weg-Kette erzeugt.
    - Jeder Schlüssel wird nur einmal verwendet und nach einem festgelegten Zeitplan veröffentlicht: Intervall-Beginn und -Länge, aktueller Intervallindex, Veröffentlichungs-verzögerung (in den Proceedings als 1 gewählt, besser >1).
    - Nach Veröffentlichung eines Schlüssels kann jeder Client das entsprechende bereits erhaltene Paket *a posteriori* verifizieren.

# Konzept / Nachrichtentypen (Unicast)

**NTS-Nachrichten sind in Extension-Fields (generisches Konzept für Funktionserweiterung in RFC 5905) von NTP-Paketen eingebettet.**

- **Assoziierung:** Aushandlung von Adressen und kryptografischen Algorithmen für den weiteren Verlauf
- **Zertifizierung:** Übermittlung von Zertifikaten zur Serverauthentifizierung
- **Cookie:** Austausch des Cookies
- **(Unicast-)Zeitsynchronisation:**
  - Der Client stellt eine NTP-Zeitanfrage und fügt die nötigen Informationen zur Cookie-Generierung sowie eine Nonce an.
  - Der Server antwortet mit einem NTP-Zeitpaket, dem er die Nonce sowie einen MAC zur Verifizierung beifügt.

# Konzept / Protokollverlauf / Unicast




**Zeitanfrage enthält:**

- Hash-Algorithmus $h$,
- Hashwert $h(K_C)$ des öffentlichen Schlüssels des Clients,
- Nonce $N_C$

**Server führt durch:**

- Neuberechnung des Cookie $K_{CS}$ = *HMAC(h; seed,* $h(K_C)$)
- Berechnung des MAC = HMAC($h$; $K_{CS}$, $N_C$ || Message)

**Antwort enthält:**

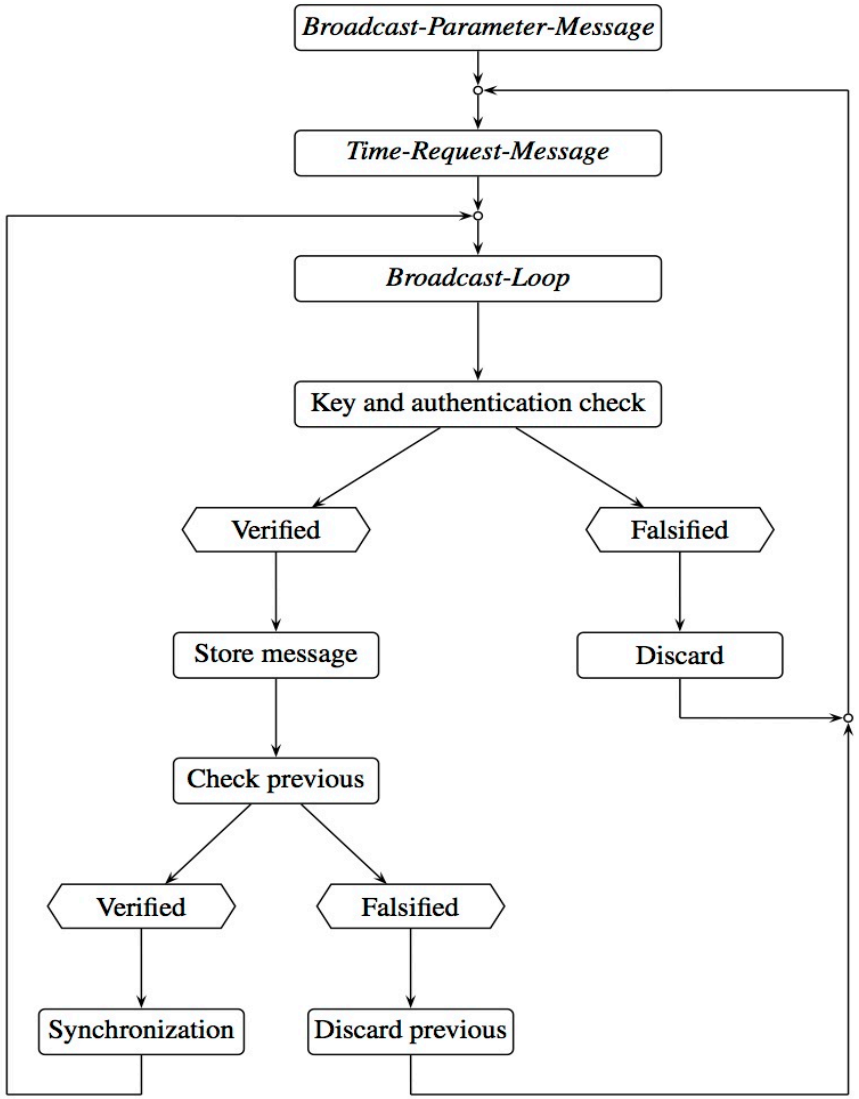
- Message, $N_C$, MAC

# Konzept / Nachrichtentypen (Broadcast)

**NTS-Nachrichten sind in Extension-Fields von NTP-Paketen eingebettet.**

- **Broadcast-Parameter-Austausch:** Übermittlung der für das TESLA-Protokoll nötigen Informationen an den Client
- **Broadcast-Zeitpaket:** wird durch den Server an alle Teilnehmer versendet.
  - enthält/veröffentlicht einen zuvor verwendeten Schlüssel,
  - enthält Zeitinformationen,
  - enthält einen MAC über die Zeitinformationen, der mit dem Schlüssel des gegenwärtigen Intervalls gebildet wird, sowie die ID dieses Schlüssels.

# Konzept / Protokollverlauf / Broadcast




**Client überprüft:**

- Schlüssel auf dem MAC des gegenwärtigen Pakets basiert wurde laut Zeitplan noch nicht veröffentlicht
- Der im gegenwärtigen Paket veröffentlichte Schlüssel verifiziert das zugehörige, zuvor erhaltene Paket

**Für Erläuterungen zu Schlüsselüberprüfung und Paketverifizierung s. Internet-Draft zu NTS oder RFC 4082 (TESLA)**

# Konformität mit den Sicherheitsanforderungen aus IETF WG NTP/TICTOC

| Sec. | Requirement | IETF Draft | NTS |
|---|---|---|---|
| 5.1 | Authentication & authorization of server. | MUST | OK |
| 5.1.2 | Recursive authentication & authorization. | MUST | OK |
| 5.2 | Integrity protection. | MUST | OK |
| 5.5.1 | Key freshness. | MUST | OK |
| 5.5.2 | Security association. | SHOULD | OK |
| 5.5.3 | Unicast and multicast associations. | SHOULD | OK |

# Konformität mit den Sicherheitsanforderungen aus IETF WG NTP/TICTOC

| Sec. | Requirement | IETF | NTS |
|---|---|---|---|
| 5.6 | Performance: no degradation in quality of time transfer. | MUST | OK |
| 5.6 | Performance: computation load. | SHOULD | OK |
| 5.6 | Performance: storage, bandwidth. | SHOULD | OK |
| 5.7 | Confidentiality protection. | MAY | NO |
| 5.8 | Protection against delay and interception attacks. | SHOULD | - |
| 5.9.1 | Secure mode. | MUST | OK |
| 5.9.2 | Hybrid mode. | MAY | OK |

# Nächste Schritte: Formale Verifikation (induktiver Ansatz)

**Ziel ist es, das NTS-Protokoll formal zu verifizieren.**

**Erster Ansatz: induktiver Ansatz mit dem Theorem-Beweiser *Isabelle:***

- Formulierung des Protokolls, des Netzwerkes und des Angreifers (dessen Möglichkeiten) in logischen Termen in der funktionalen Sprache Isar (Intelligible semi-automated reasoning)
- Formulierung der Protokoll-Ziele (wie z.B. Durchführbarkeit, Authentizität und Integrität) als mathematisch-logische Theoreme
- Beweisen dieser Theoreme

# Nächste Schritte: Formale Verifikation (Model-Checking)

**Ziel ist es, das NTS-Protokoll formal zu verifizieren.**

**Zweiter Ansatz: Model-Checking mit Promela/SPIN**

- Formulierung der Protokoll-Teilnehmer als Prozesse in der Spezifikationssprache Promela (Protocol meta language)
- Analyse des dadurch modellierten nichtdeterministischen endlichen Zustandsautomaten im Modellprüfer SPIN (Simple Promela Interpreter)

# Zusammenfassung

- **Authentifizierte und Integritätsgeschützte Zeitsynchronisation wird zunehmend unerlässlich.**
- **Bestehende Verfahren sind in vielen Fällen nicht adäquat.**
- **Ein Verfahren zur Sicherung von Zeitsynchronisationsprotokollen, speziell NTP, wurde vorgestellt.**
- **Das Verfahren befindet sich zur Standardisierung in der NTP WG der IETF.**
- **Die Arbeiten zu NTS sind noch nicht abgeschlossen.**
- **Anregungen werden gern aufgenommen.**

**Physikalisch-Technische Bundesanstalt**
**Braunschweig und Berlin**
Bundesallee 100
38116 Braunschweig

Dr. Dieter Sibold
Kristof Teichel

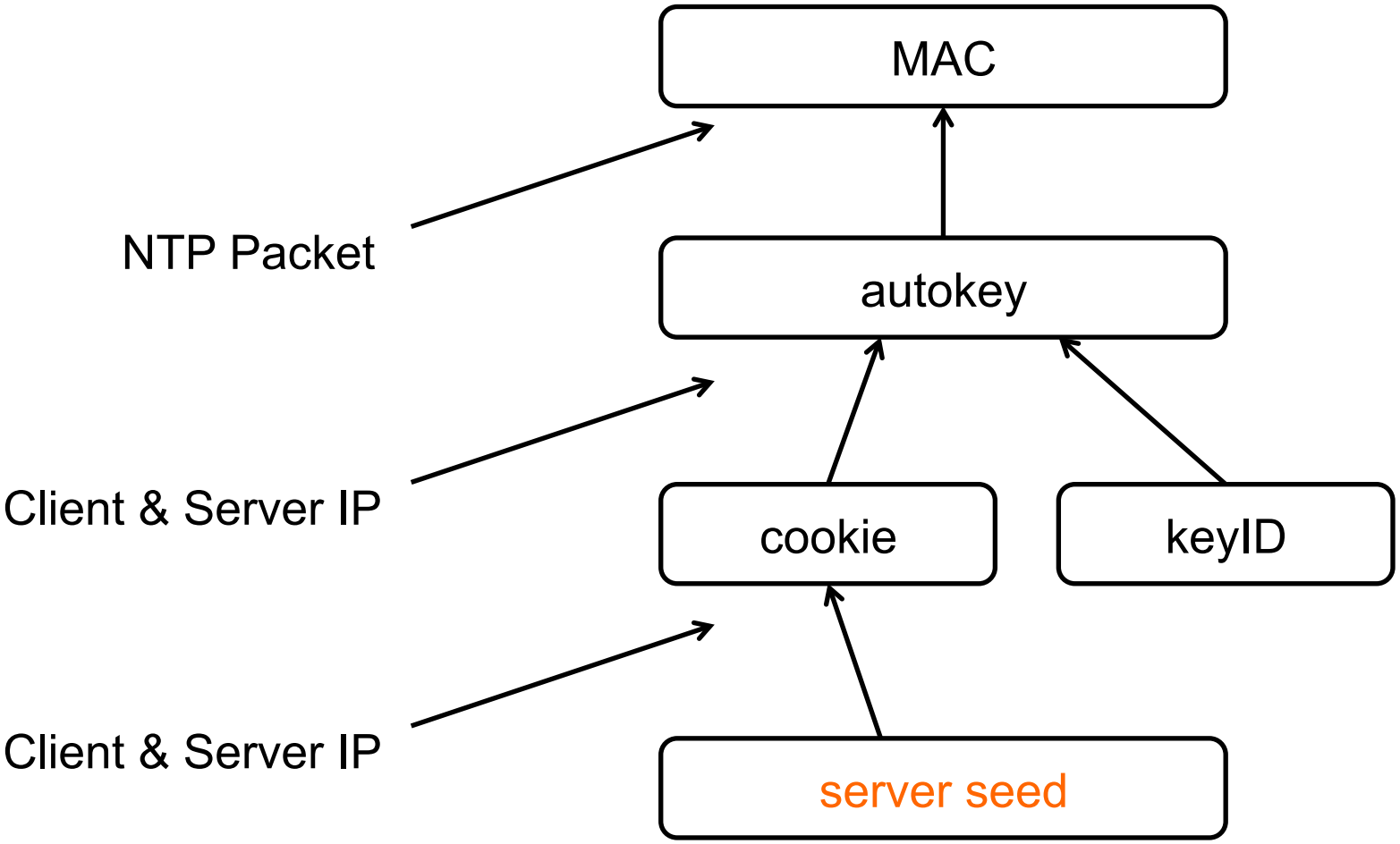
Telefon: +49 531 592-8420
+49 531 592-8421
E-Mail: dieter.sibold@ptb.de
kristof.teichel@ptb.de

www.ptb.de

Stand: Feb. 2014

# Sicherheit im NTP / Autokeys Schwachstellen

## Message Authentication Code (MAC)



# Sicherheit im NTP / Autokeys Schwachstellen

## Message Authentication Code (MAC)

1. Server Seed nur 32 Bit lang
   → Client kann Cookie anfordern um per Brute-Force den Seed anzugreifen (0,5 Stunden mit Standard-PC)
2. Cookie nur 32 Bit lang
   → Angreifer kann Paket abfangen und per Brute-Force den Cookie extrahieren
3. Cookie-Berechnung basiert auf IP-Adresse des Clients
   → Angreifer kann mittels IP-Spoofing Anfrage fälschen und Cookie (lesbar) an sich selbst schicken lassen

## Authentifizierungsverfahren

- Challenge-Response-Verfahren werden inkorrekt angewendet und bieten dadurch nicht ausreichende Sicherheit.