电子证据的可信性和完整性保护技术

孙国梓

博士 / 教授

2014年9月25日

感谢与倡议

自我介绍

- 研究方向
  - 网络信息安全（智能终端安全、主机安全、网络安全等）
  - 电子数据取证（智能终端取证、主机取证、网络取证等）
- 工作经历
  - 2013-2014，香港大学计算机科学系，高级访问学者
  - 2011-2012，扬州（江都）软件园管理委员会，副主任
  - 2003-2005，清华大学制造工程研究所CIMS中心，博士后
  - 2002-今，南京邮电大学计算机学院，讲师、副教授、教授
- 社会兼职
  - 2011 - ，南京东南司法鉴定中心，电子数据司法鉴定人
  - 2010 - ，江苏省科技工作者中心，电子数据司法鉴定专家

主要内容

- 电子数据 — 电子证据
- 电子证据的可信性分析（可信取证）
- 电子证据的完整性保护
- 一种电子证据可信及完整保护的方法

几个名词

计算机取证	Computer Forensics 计算机作为取证工具、计算机作为取证目标
数字取证	Digital Forensics ?
电子取证	Electronic Forensics ? √ ?
数字证据	Digital Evidence ?
电子证据	Electronic Evidence ? √ ?

提到几个名词，但目的并不仅仅是为了定义它们的概念

研究现状

- 静态数据分析
  - 系统元数据分析
  - 操作记录、日志等
- 计算机动态取证技术
  - 将入侵检测、蜜罐等思想引入电子数据取证
  - 基于主动防御的陷阱网络取证
- 形式化取证分析技术
  - 以时间线性化和事件相关性方法建立攻击事件分析过程模型（大幅度增加语言的复杂性和不确定性）
  - 等专家系统决策树和基于语意完整性检测的方法（离不开取证人员的经验和知识）
- 从法律层面的研究

面临问题

- 对于数字取证的研究，一直以来的重点：
  - 电子数据的获取
  - 对所取得数据的分析
- 对于电子数据取证的有效性或可信性还缺乏相应的论证
- 这样取得的数据容易受到质疑，其采信度也会大打折扣
- 在计算机取证工具应用方面
  - 公安等执法机关还缺乏有效的可信工具
    - » 目前只是利用国外一些常用的取证工具或者根据自身技术经验开发应用
    - » 在程序上还缺乏一套保证电子数据可信性的取证流程，提出的证据很容易遭到质疑

相关研究的两大趋势

- 从技术角度出发
  - 把侧重点放在从特定平台中通过特定方法取得特定数据的研究上
  - 并形成相应的电子数据取证模型
- 从法律角度出发
  - 将取证过程的合法化、合理化作为讨论重点
  - 结合现有的对于刑事犯罪取证的方法和规范，阐述电子数据的取证
- 在我国计算机取证领域，取证技术工具及基础理论方法研究都还处于起步阶段
- 在技术方法、人们的取证意识、法律执行部门建设等方面同发达国家存在差距

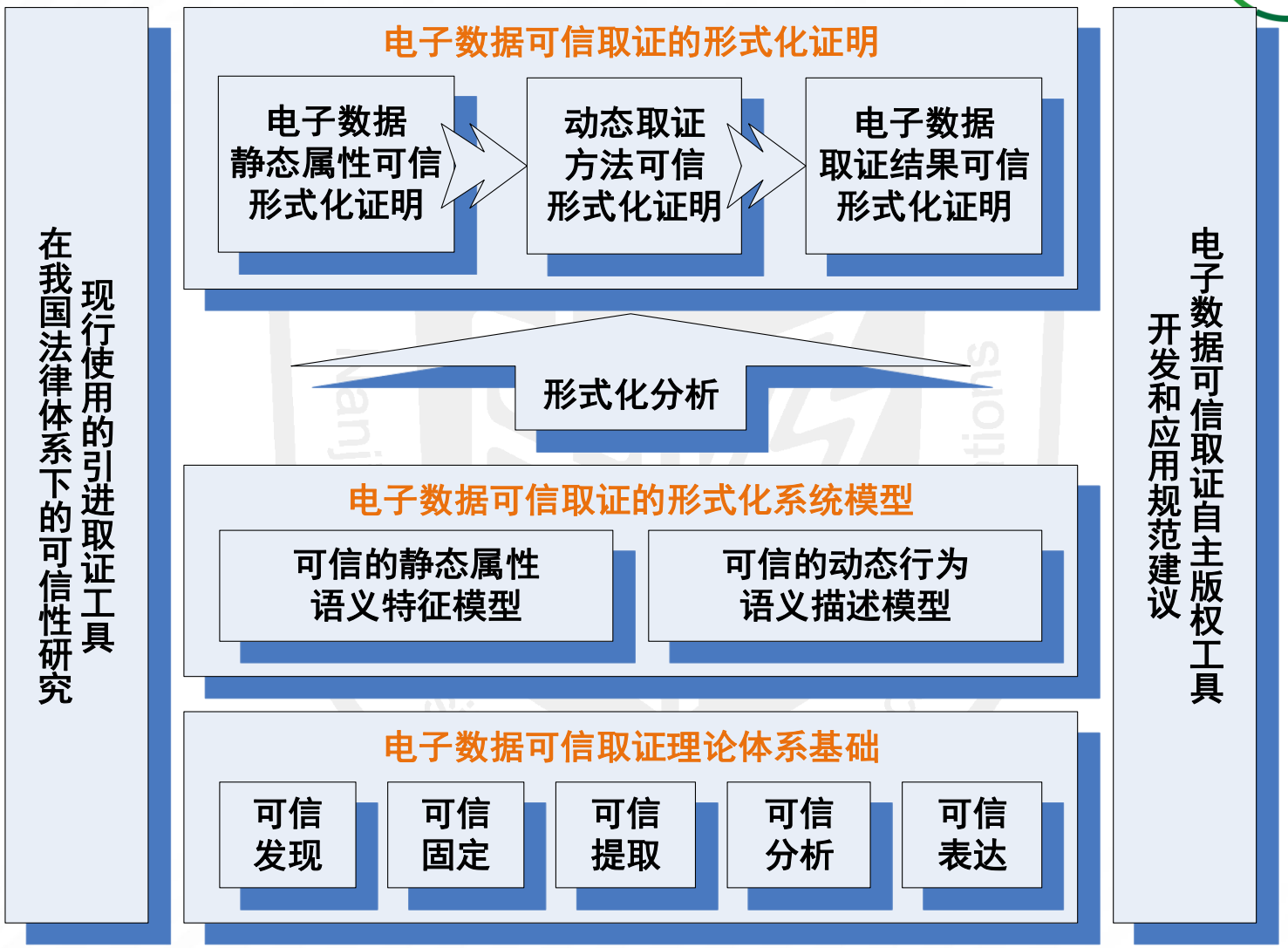
电子证据的可信性分析

——可信取证

“可信取证”理念的提出

- 针对取证过程中涉及的可信性问题，我们提出“可信取证”(Trusted Forensics)理念
- 结合电子数据的固有特征和取证行为，将电子数据可信取证宏观分为两方面
  - 可信的静态属性(电子数据本身的静态特征可信)
  - 可信的动态行为(由电子数据转换为证据所需的过程或行为可信)
- 实现电子证据的可信获取(可信发现、可信固定、可信提取)和可信展现(可信分析、可信表达)
- 保证所取电子证据的客观性、关联性、合法性，形成符合司法鉴定要求的证据链，并最终呈堂

可信取证的总体方案


现行使用的引进取证工具
在我国法律体系下的可信性研究
电子数据可信取证的形式化证明
电子数据
静态属性可信
形式化证明
动态取证
方法可信
形式化证明
电子数据
取证结果可信
形式化证明
形式化分析
电子数据可信取证的形式化系统模型
可信的静态属性
语义特征模型
可信的动态行为
语义描述模型
电子数据可信取证理论体系基础
可信
发现
可信
固定
可信
提取
可信
分析
可信
表达
电子数据可信取证自主版权工具
开发和应用规范建议

电子数据静态属性可信

- 需明确原始电子数据的静态属性，包括：
  - 生存介质、电子数据的种类，如文件、网络数据、日志、邮件等
  - 保证原始数据的可信性，包括如何实现电子数据的原始性、完整性保护、防止篡改等
  - 重点探讨可信发现和可信固定的形式化验证方法，对电子数据的原始性、完整性保护、防篡改等静态属性可信进行语法和语义验证

电子数据动态取证行为可信

- 发掘电子数据动态取证方法，如物理镜像等，继而论证所取得电子证据的可信性
  - 重点研究可信固定、可信提取、可信分析以及可信表达等的形式化验证方法
  - 借鉴工作流中任务组合的思想，将取证过程中的保护现场、现场勘查、获取证据、鉴定证据、分析证据、进行追踪、提交结果等过程步骤均视为一种动作行为
  - 将每一个动作行为刻画成一个（层次）时间自动机模型，再利用工具分析（层次）时间自动机模型的组合（即行为组合）来判断取证过程行为的可信性

所取得电子证据结果的可信性

- 数据的真实性和完整性都可以从原始数据和取得数据的方法两个方面去理解
  - 真实性可以从数据的一致性方面加以判断
    - » 一致性要求原始数据与所取数据在内容上完全相同
    - » 取证方法不会对数据的内容造成改变
  - 完整性要求所取证据不能是片面的
    - » 表现为所取得的数据与取证目标计算机系统中的原始数据相比，没有增加或删减内容
    - » 特别是取证的方法不会删减所取数据的内容

电子证据的完整性保护

电子证据的固定与保全

- 证据保全
  - 是指法院在起诉前或在对证据进行调查前，依据申请人、当事人的请求，或依职权对可能灭失、可能发生变化或今后难以取得的证据，予以调查收集和固定保存的行为
  - 是当事人基于民事权利，为维护自身的合法权益，自主选择在适当的时候，向法定的机构提起的收集、固定、保管相关证据，以保持其证明力的活动

- 电子证据保全的原则
  - 合法性原则、及时性原则、效率成本原则、完整性原则、最小破坏原则

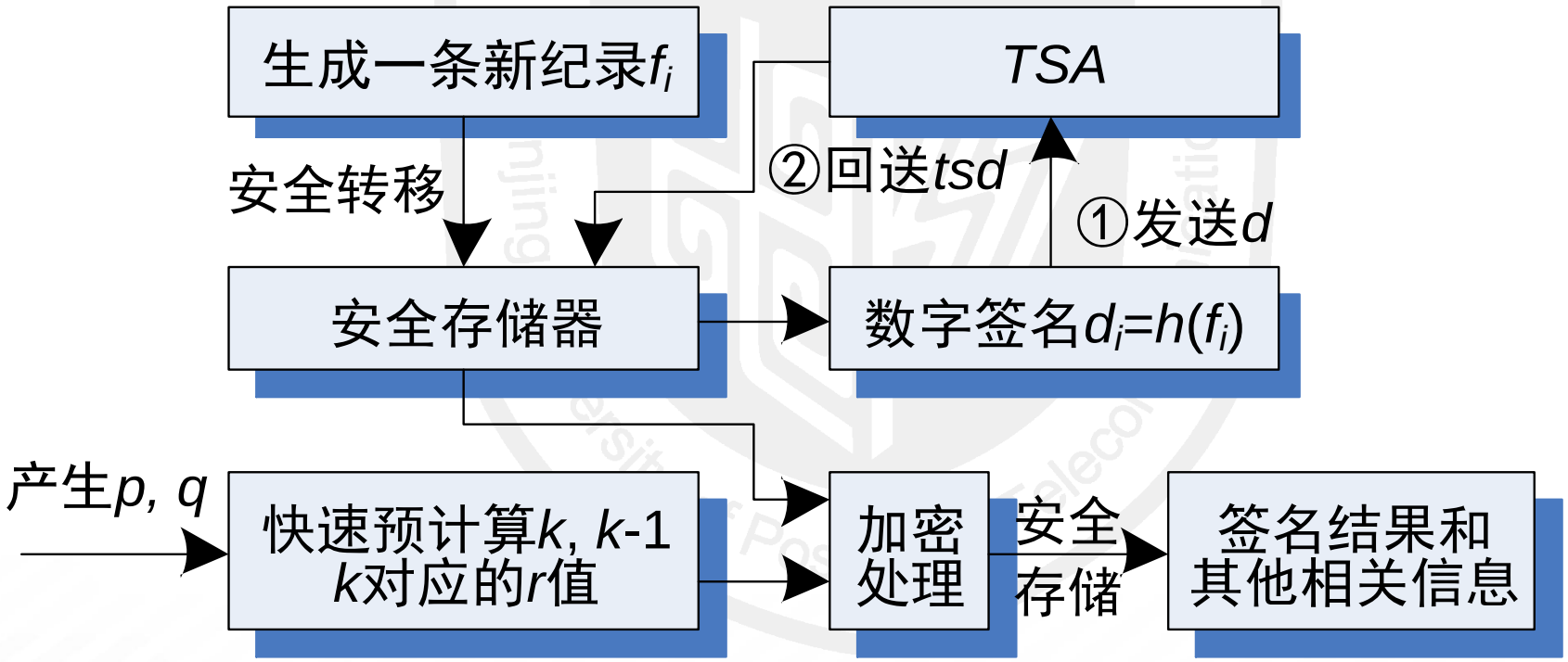
电子证据的完整性认定

- 基于经验的电子证据完整性认定
- 基于统计的电子证据完整性认定
- 基于推定的电子证据完整性认定
- 基于指标体系的电子证据完整性认定

时间戳、消息摘要及数字签名

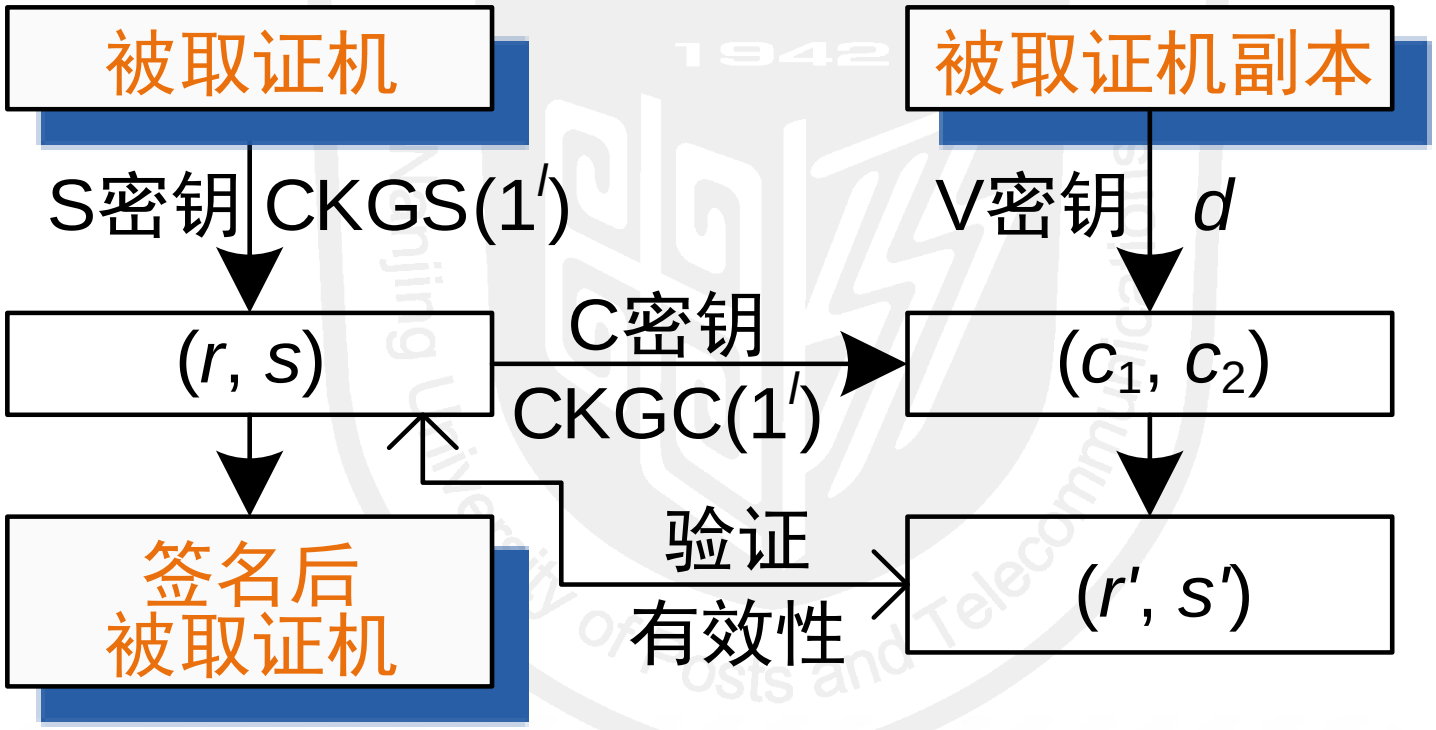
基于时间戳的可信固定

– 基于时间戳，采用只读镜像等方法进行电子数据的固定



基于时间戳的可信固定

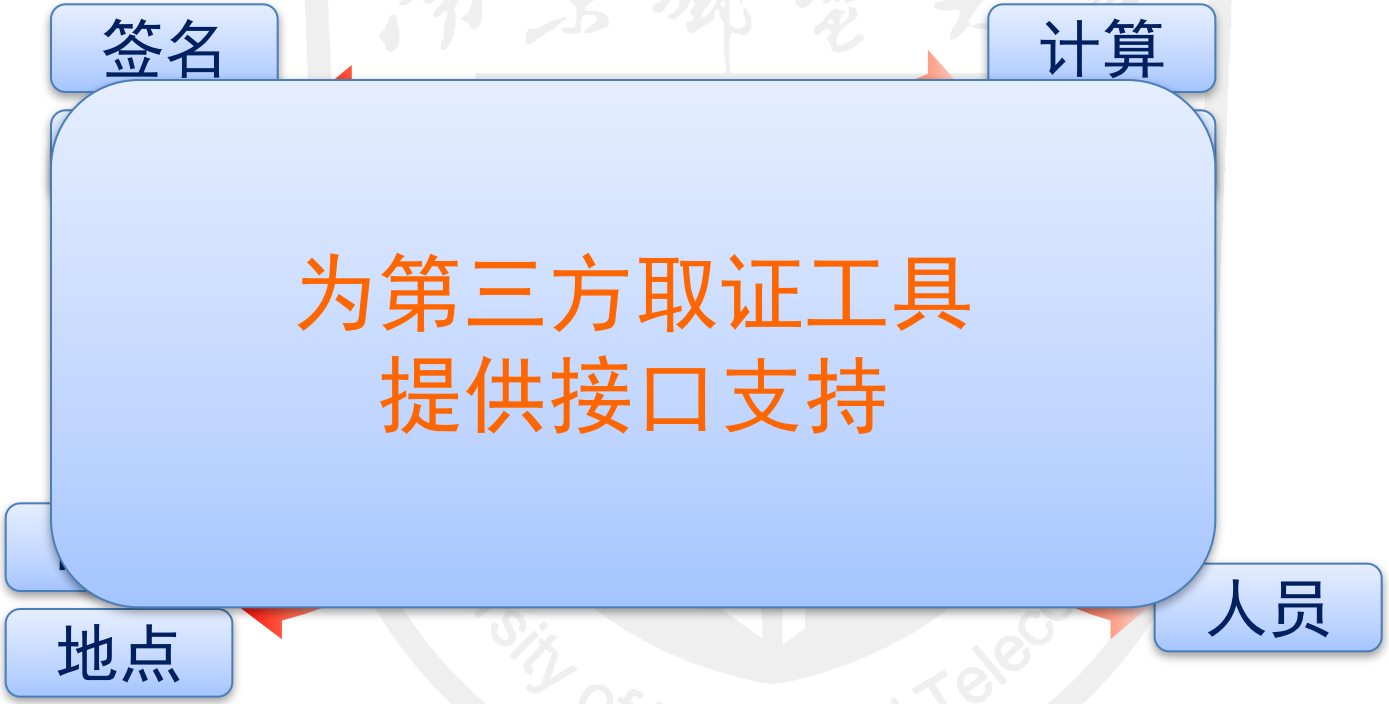
– 第三方(司法鉴定机构等)保证流程



基于证实数字签名的第三方保证

一种电子证据可信及完整保护的方法

交互和接口方法



电子取证进一步的研究方向

- 用形式化方法对取证过程进行描述
  - 结合入侵检测、防火墙、网络侦听等网络安全工具进行动态取证
  - 取证技术模型研究、取证工具智能开发
- 计算机取证相关性分析
  - 从海量数据中获取与计算机犯罪相关的有利证据
- 网络追踪技术研究
  - 对网络层和应用层进行网络追踪，获取证据
  - 人工智能、机器学习、神经网络和数据挖掘技术应用
  - 手机取证、无线环境的取证分析、远程取证.....
- 新环境下的取证技术研究
  - 网络实名制下的取证技术
  - 云计算、物联网、移动互联网环境下的电子取证技术

Thanks!

孙国梓

sun@njupt.edu.cn

2014年9月25日