RSA CONFERENCE
CHINA 2012
RSA信息安全大会2012

THE GREAT CIPHER

MIGHTIER THAN THE SWORD

伟大的密码胜于利剑

在云和企业中启用可信计算

吴錦榮 Ryan Wu

Wave Systems Corp。

RSA CONFERENCE CHINA 2012

RSA信息安全大会2012

专题会议主题：

专题会议分类：

议程

- 关于 Wave
- 为什么选择可信计算
- 可信计算组更新和解决方案
- 如何在云和企业中启用 TC
- 案例研究
  - TPM 案例：PWC (普华永道)
  - SED 案例：三大汽车制造商之一
  - 消费者案例：通过 TPM 加密微博、Google Plus 和 SalesForce 消息/数据

议程

- 关于 Wave
- 为什么选择可信计算
- 可信计算组更新和解决方案
- 如何在云和企业中启用 TC
- 案例研究
  - TPM 案例：PWC (普华永道)
  - SED 案例：三大汽车制造商之一
  - 消费者案例：通过 TPM 加密微博、Google Plus 和 SalesForce 消息/数据

关于 Wave

RSA CONFERENCE CHINA 2012

- 23 年来一直专注于基于硬件的终结点安全
- Wave 是领先的可信计算硬件独立软件供应商
- 1994 年在纳斯达克上市 (WAVX)
- 率先提供；可信平台模块 (TPM)、自加密驱动器 (SED) 加密和身份验证解决方案
- SED、TPM、Bitlocker、软件 FDE 和平台完整性的集中管理
- 以 30 多种语言发布了 1 亿多个 Wave 客户端软件产品副本
- 全球范围内部署了 50 多万个企业客户席位，包括各种纵向市场中的 G500 客户。
- Wave 软件目前向 Dell、Intel、HP、NEC、Lenovo 和 Acer 授予了许可
- 可信计算组的创始成员和永久董事会成员

议程

- 关于 Wave
- 为什么选择可信计算
- 可信计算组更新和解决方案
- 如何在云和企业中启用 TC
- 案例研究
  - TPM 案例：PWC (普华永道)
  - SED 案例：三大汽车制造商之一
  - 消费者案例：通过 TPM 加密微博、Google Plus 和 SalesForce 消息/数据

为什么选择可信计算

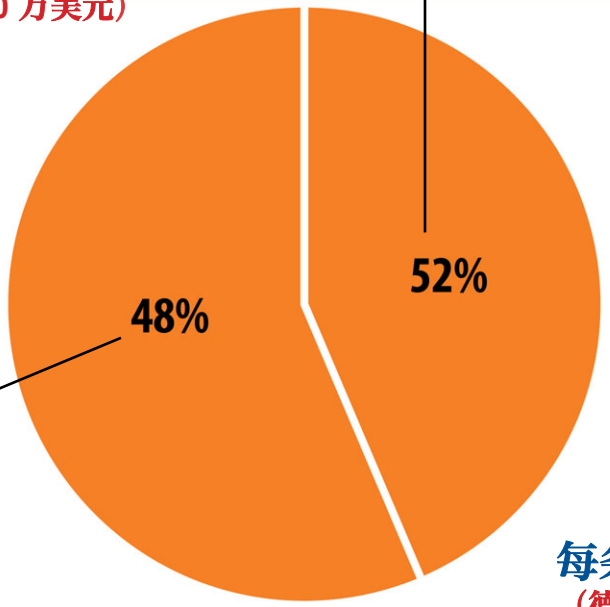
- 世界范围内已报告了 1 亿多条违规记录（来源：数据违规调查报告， Verizon, 2012）
- 美国、欧洲和阿拉伯联合酋长国的商务旅行者每周会丢失或错放 16,000 多台笔记本电脑。 (Ponemon)
- 所有分配的笔记本电脑中约有 7% 会丢失或被盗 (Ponemon/Intel)
- 87% 的人认为其组织面临移动安全漏洞攻击的风险。（Deloitte 2011 美国企业高管调查）
- 身份欺诈增加了 13%， 美国的 1160 万成年人成为受害者（来源：Javelin 战略与研究：2012 身份欺诈报告）
- 过去两年内， 50% 的企业丢失过 USB 记忆棒中的敏感信息（来源：Ponemon/Kingston 2011）

为什么选择可信计算

RSA CONFERENCE CHINA 2012

增加成本
- 未列入预算的法律、审计和会计费用
- 客户通知
- 面向客户的免费或打折服务
- 呼叫中心开支
- 公共和投资者关系
- 内部调查

平均事件成本：720 万美元
（德国 - 470 万美元，英国和法国 - 310 万美元）



客户成本
- 品牌损害
- 失去现有客户
- 招募新客户

每条记录的平均成本：214 美元
（德国 - 191 美元，法国 - 136 美元，英国 - 114 美元）

来源：“数据违规的全球成本”，Ponemon，2011

wave
Simplifying Encryption and Authentication

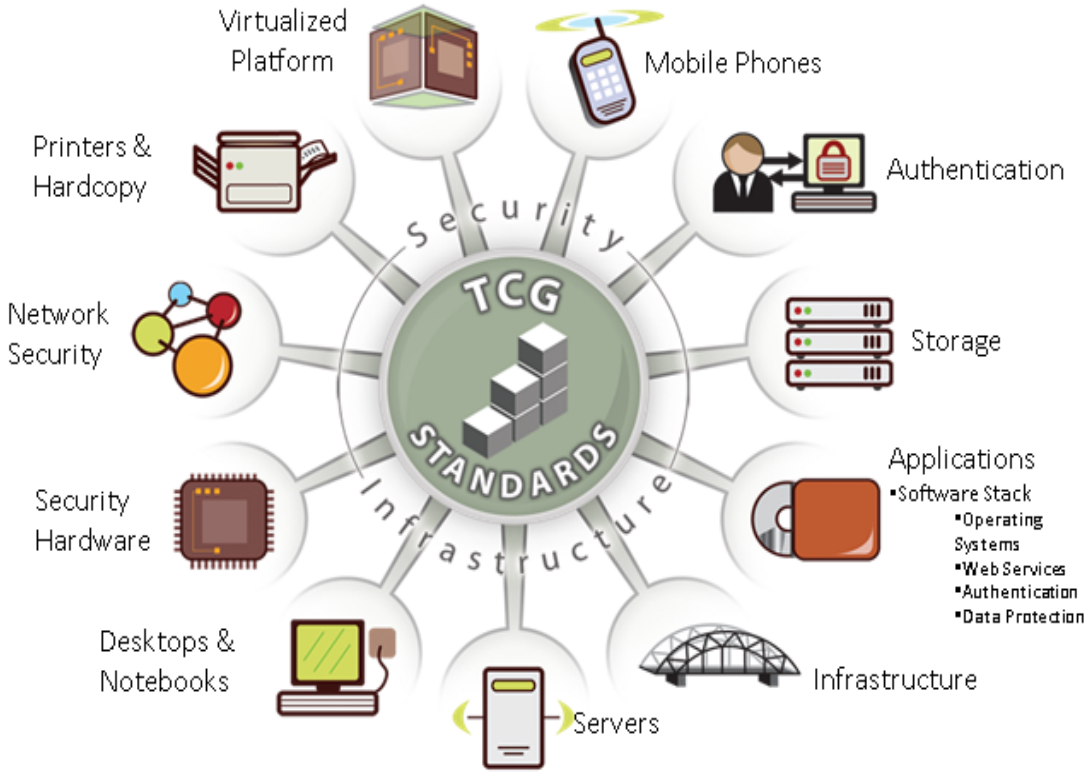
TC 技术的优点

- 阻止丢失/被盗 PC 中的数据丢失
- 针对数据违规披露实现安全港
- 展示法规遵从性
- 保护您的知识产权
- 节省时间和资金

议程

- 关于 Wave
- 为什么选择可信计算
- 可信计算组更新和解决方案
- 如何在云和企业中启用 TC
- 案例研究
  - TPM 案例：PWC (普华永道)
  - SED 案例：三大汽车制造商之一
  - 消费者案例：通过 TPM 加密微博、Google Plus 和 SalesForce 消息/数据

可信计算组 - TCG



可信计算组 (TCG) 是一个非营利组织，目的是为可信计算构造块和跨多个平台的软件界面开发、定义和推广开放的、独立于供应商的行业标准。

可信计算解决方案 - TPM

可信平台模块是您计算机中的安全芯片
它的特点：

- 已用于 6 亿台专业级笔记本电脑、台式机和服务器中
- 基于开放的可信计算组标准
- 用于所有主要品牌计算机（例如 Dell、Lenovo、HP、Toshiba、Sony、Asus 等）中
- 由主要芯片制造商（Infineon、Atmel、Intel、ST Microelectronics、Broadcom 等）制造
- 焊接在主板上，因此它可以对平台（和用户）进行身份验证

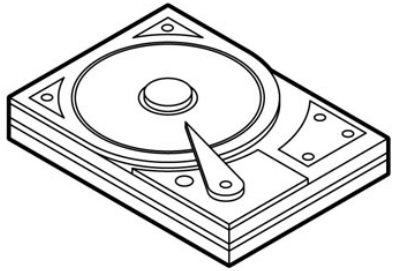
它支持：

- PKI 功能（加密密钥生成和密钥保护、数字签名）
- 平台完整性测量保护数据存储（平台配置注册器）。 对抗高级持久威胁。
- “信任根”。 TPM 将保护硬盘上数据的加密密钥

可信计算解决方案 - TPM

- 全球行业标准组
- ARM 刚刚重新加入以支持移动 TPM
- 既定收购政策 - 美国和英国
- NIST 标准利用 TPM：800-147 和 800-155
- Microsoft 要求所有 Windows-on-ARM 都采用 TPM
  - 平板电脑、电话...
- Microsoft 在 WIN 8 企业和消费者操作系统中利用 TPM
- Android 和 Chrome 上的 TPM
- NSA 和 CESG TPM 建议

可信计算解决方案- SED

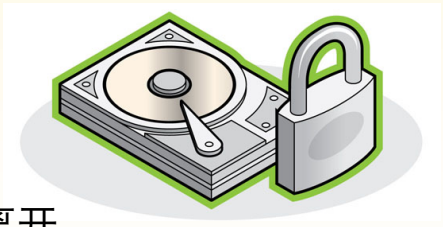


标准驱动器
- 处理器
- 内存
- RAM

自加密驱动器
- 处理器
- 内存
- RAM

+ 嵌入式加密

可信计算解决方案 - SED



- SED 有其自己的处理器和 RAM –
  使其不受软件攻击的影响。
- 加密密钥存储在驱动器控制器芯片中并且永远不会离开。
- 驱动器级别的验证将在用户得到验证之前阻止所有读/写功能。
- 永不间断的 AES 加密意味着所有数据都始终受到保护。
- 对系统和应用程序性能的影响为零。
- 内部和外部、旋转介质和固态行业标准 OPAL 驱动器。
- 获得 FIPS 140-2 认证。

议程

- 关于 Wave
- 为什么选择可信计算
- 可信计算组更新和解决方案
- 如何在云和企业中启用 TC
- 案例研究
  - TPM 案例：PWC (普华永道)
  - SED 案例：三大汽车制造商之一
  - 消费者案例：通过 TPM 加密微博、Google Plus 和 SalesForce 消息/数据

今天企业面临的挑战是什么？

RSA CONFERENCE CHINA 2012

您的挑战

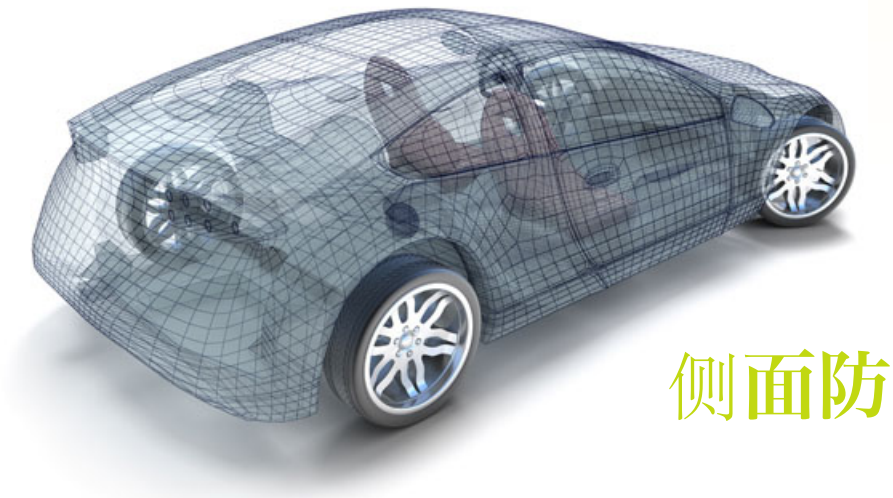
- 法规遵从性
- 数据保护
- 访问控制
- 新兴威胁
- 自带设备 (BYOD)

- Sarbanes-Oxley (SOX)
- 健康保险携带和责任法案 (HIPAA)
- 经济与临床医疗信息技术法案 (HITECH)
- 欧盟数据保护指令
- 英国数据保护法案 (DPA)
- Gramm-Leach-Bliley 法案 (GLB)
- Basel II
- 支付卡行业数据安全标准 (PCI DSS)
- 个人信息保护与电子文档法案 (PIPEDA)
- 美国国务院违规通知（46 个州和行政区）

通过内置设备保护您的数据

安全带

安全气囊



后部撞击力吸收区

侧面防撞装饰条

防抱死制动系统

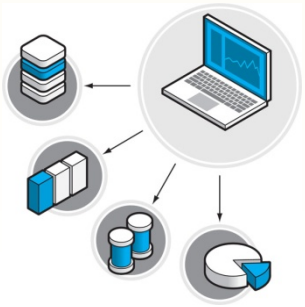
设备已经在这里了，打开吧！

RSA CONFERENCE CHINA 2012

- 以极低的成本提供真正发挥作用的安全措施
- 使法规遵从性变得简单且易于管理
- 确保您的知识产权的安全
- 防御 APT 等新兴威胁
- 通过识别哪些设备是您的设备来提高云安全性
- 为您的移动设备建立一个公用安全平台

wave
Simplifying Encryption and Authentication

在企业环境中启用 TC



自加密驱动器
- **内部旋转器**
- **SSD**
- **外部 USB 驱动器**

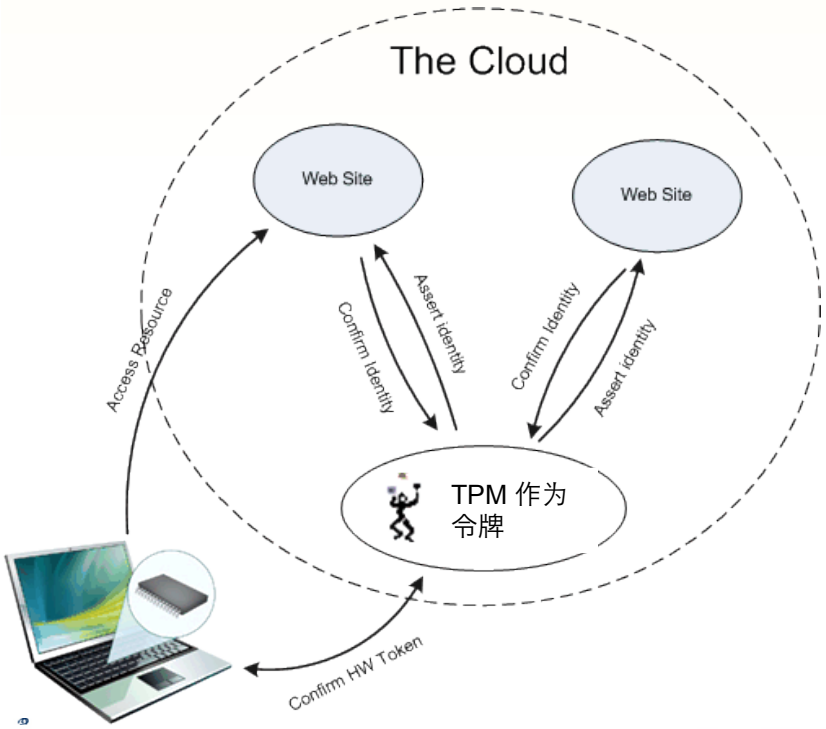
客户端
本地管理

企业管理
远程管理

可信计算
解决方案

wave
Simplifying Encryption and Authentication

在云中启用 TC



- 计算机身份验证的“原因”
  - 用户将他们自己标识为“已知客户端”（双因素身份验证）
  - 客户端标识是允许服务访问的第一个健康测量值
  - 企业客户端策略的投资已重新用于云计算
- 限制只有授权计算机可以访问服务
  - HR、财务、SFA
- 使用 OpenID、SAML、联合
- 多用户计算机
  - 允许这些标识登录到服务
  - 计算机是已知计算机
  - 用户是计算机已知的

wave®
Simplifying Encryption and Authentication

议程

- 关于 Wave
- 为什么选择可信计算
- 可信计算组更新和解决方案
- 如何在云和企业中启用 TC
- 案例研究
  - TPM 案例：PWC (普华永道)
  - SED 案例：三大汽车制造商之一
  - 消费者案例：通过 TPM 加密微博、Google Plus 和 SalesForce 消息/数据

案例研究 - TPM 案例：PWC (普华永道)

- 安全覆盖范围：150,000 位员工，跨 142 个国家/地区的 850 个位置
- 担心网络中未授权的用户
- TPM 的使用证明了化解“越狱”风险方面的成功
- 几乎所有 PwC 计算机都有 TPM
- 用于 VPN 和 WiFi 访问的基于 TPM 的证书
- 其部署中有 85,000 个使用点
- TCG 标准可以通过易于管理的少量步骤实施，且无需更改当前基础架构
- 成本分析发现，智能卡成本至少是 TPM 的两倍，而 USB 令牌的成本至少是 TPM 的三倍

案例研究 - SED 案例：三大汽车制造商之一

- 客户是美国的三大汽车制造商之一
- 非常复杂的全球基础架构。
- 其环境中有多个 AD 林，这些林之间可能有也可能没有信任关系。
- 具有各种背景和技术技能的 100,000 多个最终用户。
- 需要适合所有用户的单个解决方案
- 曾尝试部署软件 FDE 解决方案，但 3 年内只成功部署了约 4500 个平台。
- 现有软件 FDE 解决方案的用户体验不佳。
- 使用软件 FDE 解决方案的驱动器故障率非常高且日常维护成本非常高。
- 需要解决方案对最终用户而言简单易用且成本低廉

案例研究 - SED 案例：三大汽车制造商之一

- 客户在寻找最佳替代解决方案以取代现有的软件 FDE 解决方案。
- 客户的环境正在向 Windows 7 过渡。
- 需要一个在 32 位和 64 位 Win7 平台上都能工作的解决方案。
- 客户评估了市场中的几种解决方案，可信计算解决方案是当时市场中唯一一个具有企业级 SED 管理支持的解决方案，并附带有我们的第 3 代 SED 管理软件。
- 内置于 OEM 计算机中的可信计算解决方案是当时他们采购 OEM 平台时考虑的一个重要因素。

案例研究 - 消费者案例：挑战

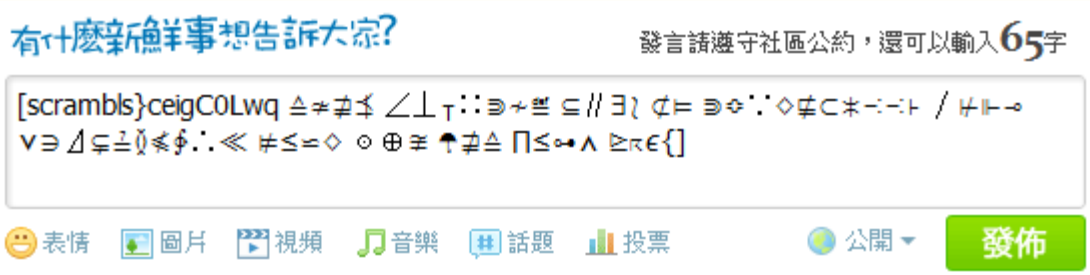
您如何保护和控制企业环境中社交媒体的使用

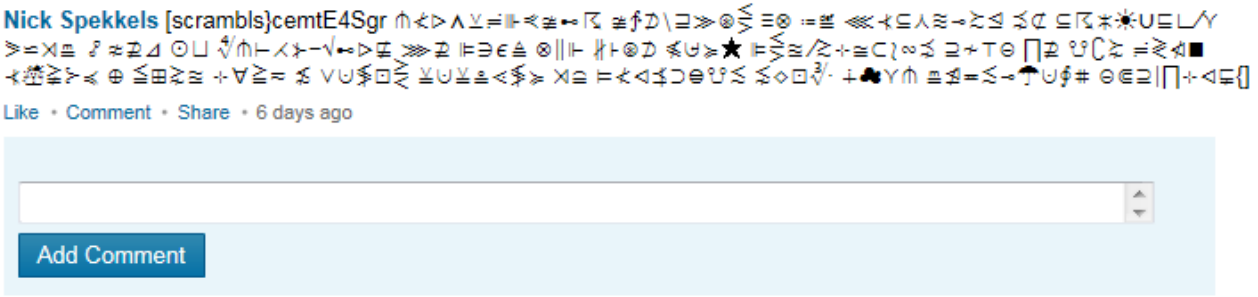
案例研究 - 消费者案例：加密社交媒体消息

RSA CONFERENCE CHINA 2012

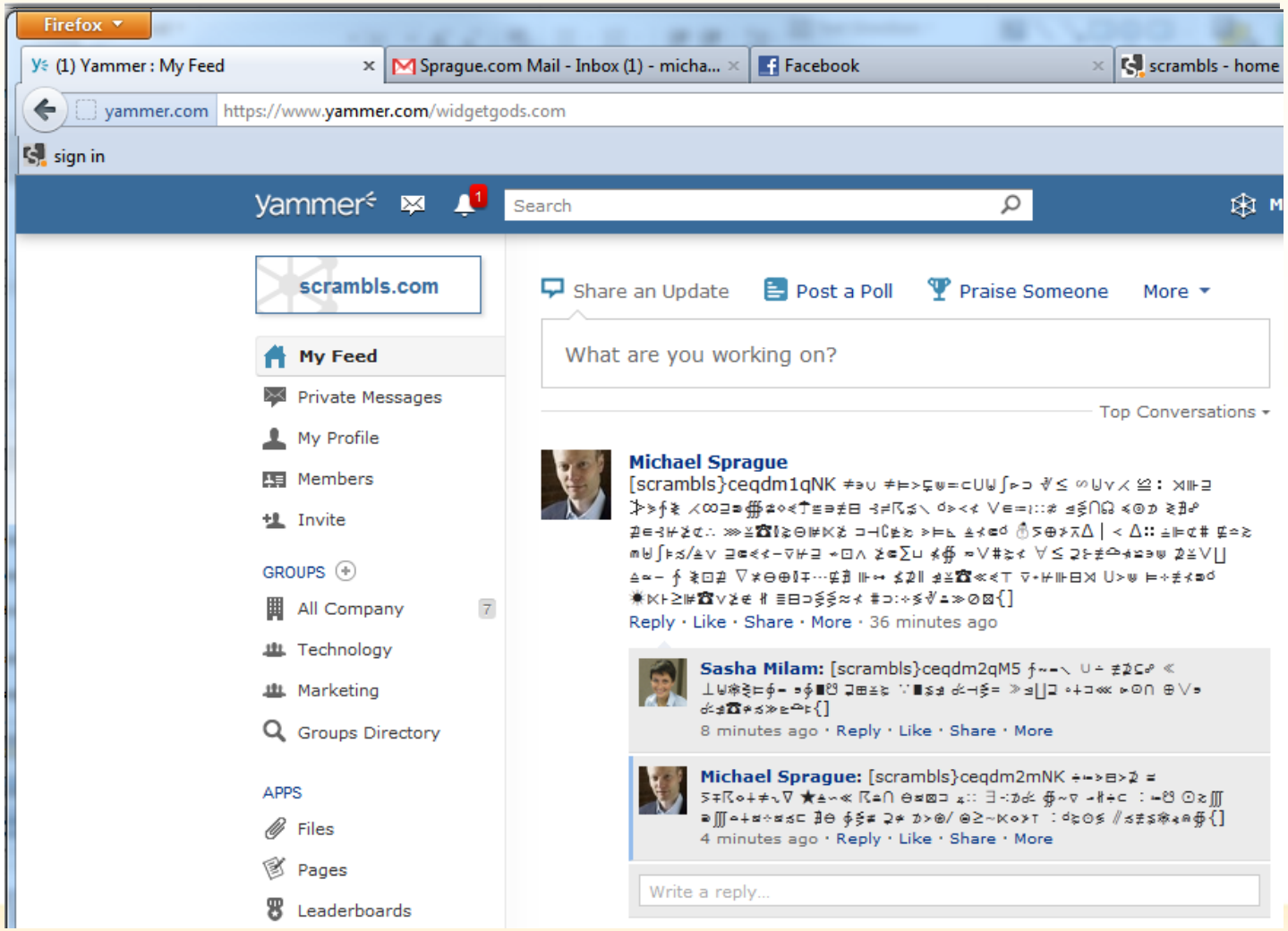
允许您控制和保护通过社交媒体发布的消息的可信计算技术

新浪微博 weibo.com



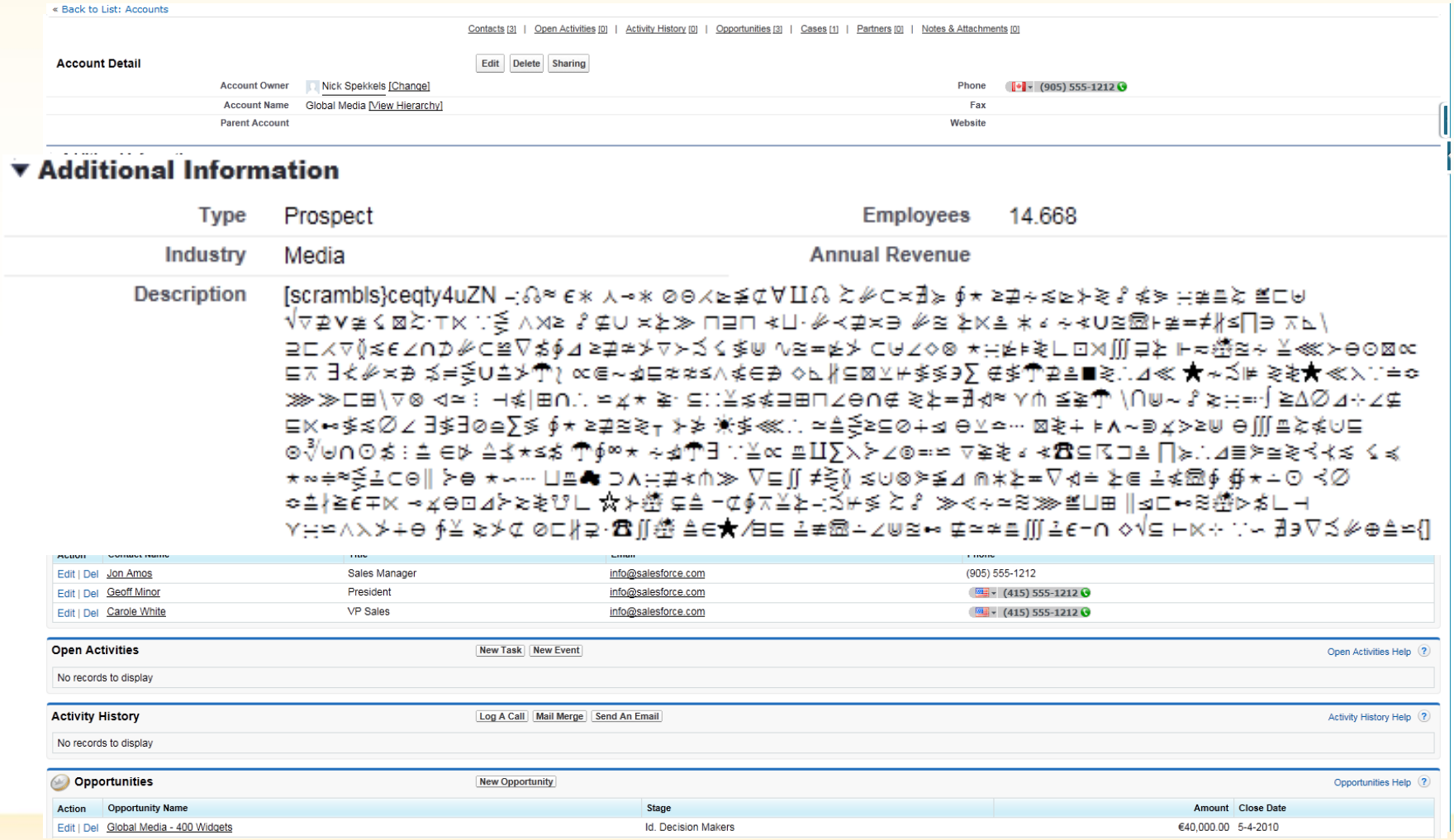


案例研究 - 消费者案例：
它看起来如何？



案例研究 - 消费者案例：
还是基于 Web 的业务应用程序

RSA CONFERENCE CHINA 2012



谢谢

RSA CONFERENCE
CHINA 2012
RSA信息安全大会2012

备份

RSA CONFERENCE
CHINA 2012
RSA信息安全大会2012