基于 HTML5 技术的移动智能终端应用及安全问题研究

董　霁　工业和信息化部电信研究院泰尔实验室硕士研究生
杨丁宁　工业和信息化部电信研究院泰尔实验室泰尔实验室工程师 博士
史德年　工业和信息化部电信研究院泰尔实验室总工程师 教授级高级工程师

摘要：介绍了 HTML5 技术的概况，重点分析了 HTML5 技术在移动智能终端上的应用，包括应用的存在形式和移动 Web 应用服务系统架构，并且对比了原生应用和基于 Web 技术移动应用的优劣，最后总结了 HTML5 移动应用可能存在的安全威胁并给出了应对建议。

关键词：HTML5，移动智能终端，安全，Web 应用程序，混合应用程序

Abstract：This article described an overview of the HTML5 technology, focused on analyzing the application of HTML5 technology in smart mobile terminals, including the existing application forms and the Web application service system architecture, and discussed the advantages and disadvantages of native applications and Web-based applications respectively. Finally, it summarized the security threats and programming suggestions on HTML5 mobile applications.

Key Words: HTML5, smart mobile terminal, security, web application, hybrid application

HTML5 是超文本标记语言（HTML：HyperText Make-up Language）的下一个重要修订版本，目前仍在发展演化和形成正式标准的过程中。人们普遍认为 HTML5 是标记语言、JavaScript 应用程序接口（API：Application Programming Interface）和层叠样式表（CSS：Cascading Style Sheets）三种技术的组合[1]：标记语言用来构建页面的结构框架；CSS 可定义丰富的样式，使页面变得美观整洁；JavaScript 和它提供的一系列 API 赋予了 Web 页面强大的展现和交互能力。虽然正式标准尚未出炉，但产业界已经对 HTML5 表现出极大的热情，纷纷推出支持该技术的产品和服务。这种趋势同样也出现在移动通信领域，主流的智能终端操作系统均已具备支持 HTML5 的运行环境，使得用户在移动智能终端上也能感受 HTML5 技术带来的丰富体验。但与此同时，HTML5 的广泛应用也给移动终端带来了传统互联网所面临的安全问题，对网络安全和用户信息安全造成新的威胁。

1 HTML5 概述

1.1 演进历程

HTML 最早由欧洲核子研究组织（CERN：European

Organisation for Nuclear Research）于 1990 年提出，后由互联网工程任务组（IETF：Internet Engineering Task Force）接管。1994 年，W3C 在麻省理工学院计算机科学实验室成立，HTML 的发展再一次更换了组织。1997 年，W3C 推出了 HTML 3.2，同一年年底推出 HTML4。第二年，W3C 决定暂停对不断发展的 HTML 技术标准化工作，取而代之的推出了基于可扩展标记语言（XML：eXtensible Markup Language）的可扩展超文本标记语言（XHTML：eXtensible Hyper-Text Markup Language）。XHTML 与 HTML 语言类似，但语法更为严谨。同时 W3C 还进行了另一项计划，决定发展一种全新的标记语言，它与早期的 HTML 和 XHTML 均不兼容，命名为 XHTML 2.0。

XHTML 2.0 的不兼容思想引起了很多 Web 开发者的不满，提出了 HTML 演进还是应以开放思想为主。继而，Mozilla 和 Opera 提出了一些新功能的建议，但随即就被 W3C 拒绝了，理由是该提案与 Web 演进发展方向相悖，最终 W3C 成员投票决定依然坚持基于 XML 的 Web 标准[2]。出于对 W3C 的不满，苹果公司、Mozilla 基金会和 Opera 公司于 2004 年联合建立了网页超文本应用技术工作组（WHATWG：Web Hypertext Application Technology Working Group），成为 HTML5 技术发展的摇篮。WHATWG 主要基于几个核心原则，特别是与 XHTML 2.0 相反的后向兼容性，并坚持标准要足够细致，以实现完全的互操作性。WHATWG 提出的 Web Applications 1.0 可以说是 HTML5 的雏形，其中包括 HTML5、Web Workers 和一些其他标准。2007 年 4 月 10 日，Mozilla 基金会、苹果公司和 Opera 公司宣布 W3C 新的 HTML 工作组采用 WHATWG 的 HTML5 标准。5 月 9 日，W3C 新的工作组开始其标准的制定。2008 年 1 月 22 日，第一份正式草案发布。2011 年 4 月 1 日，HTML5 有了官方标志，标志着 HTML5 技术开始走向推广和普及。

1.2 新功能特性

与之前版本的 HTML 相比，HTML5 引入了一系列新特性，包括新增的标签和 JavaScript API 等，堪称 Web 开发的一个重大转折。下面从众多的新特性中选取几类重点介绍。

1.2.1 音视频标签

在 HTML5 出现之前，网页中播放多媒体内容的唯一方式是借助浏览器插件，通过在页面中调用插件的方式来嵌入音视频。这种方式最常见的例子即为流行的 Flash 播放器插件。但插件在使用中存在很多问题，例如稳定性不好，容易崩溃；安全漏洞问题突出，往往成为入侵计算机的通道；支持的平台有限，无法在移动设备上使用等。在 HTML5 中，新增的 <video> 和 <audio> 标签将赋予移动智能终端新的视听感受，这两个标签可以实现原生的视频和音频播放，并提供 API 实现自定义播放控制。

1.2.2 离线存储

网络存储（Web Storage）功能让 Web 应用和本地应用竞争成为可能。Web Storage 支持持久性的数据存储，可以直接将用户的离线缓存数据保存在移动智能终端的存储空间中，使得用户在离线状态下也能顺利使用 Web 应用。Web Storage 就如同改进版的 Cookie，提供更大的存储空间，更好的架构。

1.2.3 画布

提到 HTML5 的新特性就不能不说强大的画布（Canvas）标签，浏览器不需要加载 Flash 插件就可以在网页中绘制各种 2D 甚至 3D 图片和动画，这对移动智能终端应用来说是一项重大革新。对于不支持 Flash 的 iOS 平台和部分旧版本的 Android 平台，Canvas 提供了一个 JavaScript 可以访问的绘图区域，JavaScript 的运用使这个区域有了无限的可能。

除了上述几种特性外，增强的表单功能，实现多线程后台处理的 Web Workers，Geolocation API 和其他新特性可以共同帮助开放者编写更为精彩的应用程序。

2 HTML5 在移动智能终端上的应用

2.1 HTML5 移动应用的形式

与传统移动终端相比，移动智能终端最显著的

区别在于可扩展性：用户可以下载并安装各种应用程序来扩展终端的功能，从而极大地提高了终端的实用性和娱乐性。目前，绝大多数移动应用均属于原生应用。这些应用程序由各自操作系统平台的本机编程语言开发（例如 Android 本地应用由 Java 语言编写），并且通常只能在该系统平台下运行。

HTML5 的出现使得移动开发者又多了一种选择，即使用以 HTML5 为代表的 Web 技术来开发移动应用。具体来说，基于 HTML5 技术的移动应用又分为两种形式：

⑴ Web 应用。Web 应用是一种运行在互联网或者内部网络上的应用程序，整个程序的编写完全基于 Web 技术语言（如 HTML、CSS 和 JavaScript 等），并需要通过浏览器解析执行。这种应用程序可以在移动智能终端上通过一个适用的移动浏览器打开。由于应用完全托管于云中的服务端，因此运行时不需要事先安装或定期升级，拥有跨平台、节省资源等特点。

⑵ 混合应用（HybridApps）。是一种混合型移动应用程序，运行于标准的浏览器解析引擎中，通过本地语言和 HTML5 技术完成开发。HybridApps 的 HTML5 代码和本地平台代码相互配合，HTML5 技术完成应用的大部分展现，而移动智能终端的设备内嵌功能，如摄像头访问、电话本读取等，由 JavaScript API 和本地代码互通实现。与 Web 应用不同的是，混合应用在发布时往往要打包成操作系统所支持的安装包形式，然后供用户下载安装。

2.2 移动 Web 应用服务系统架构[3]

以 HTML5 技术为基础构建的移动互联网信息服务系统，支撑着 Web 应用和混合应用的正常运行。整个系统由 Web 应用服务、Web 运行环境、服务部署托管平台、应用生成开发工具等部分构成，如图 1 所示。

整个系统运行在“云”、“管”、“端”三部分上。云端上的服务部署托管平台可以给 Web 应用服务提供代码部署和运行的一套完整环境。应用生成开发工具包括应用开发框架，集成开发环境和模拟器。应

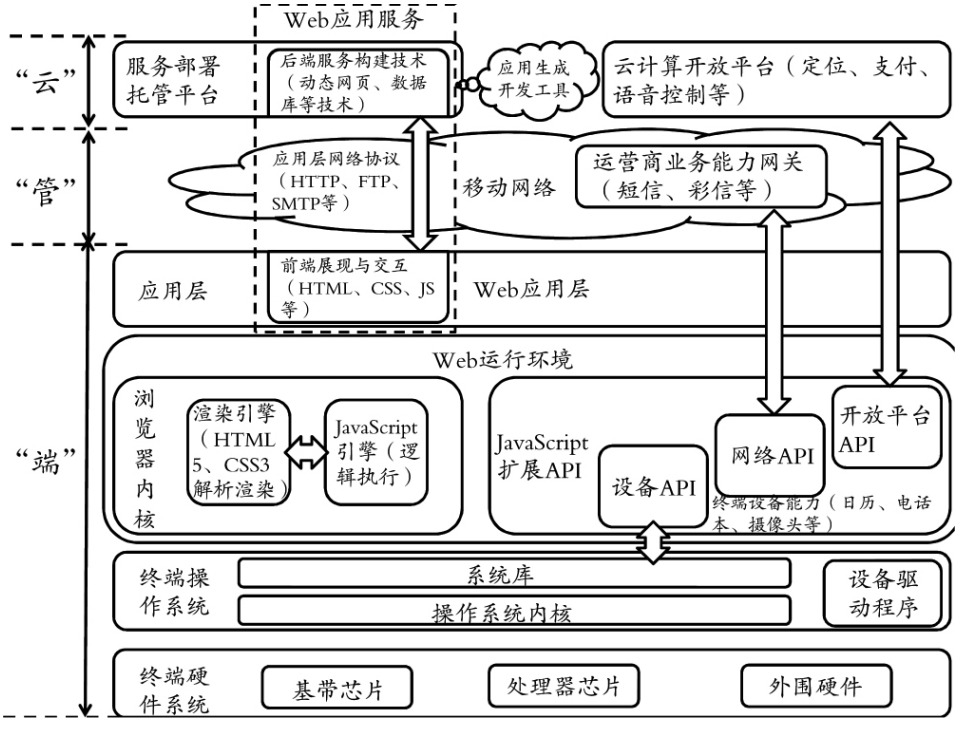

图 1 移动 Web 应用服务系统架构

用开发框架是开发过程中重要的中间件，应用程序所展现的运行效果和安全性很大一部分取决于中间件的特性。典型的应用开发框架有如 PhoneGap 和 Worklight 等。集成开发环境为开发者提供图形化和向导式的应用开发、调试工具。模拟器用来模拟应用运行环境并协助调试应用。

表 1 Web 应用和原生应用在平台和语言支持上的对比

	Web 应用	原生应用				
平台	跨平台支持	Android	iOS	Symbian	Windows Mobile	…
语言	HTML、JavaScript、CSS3	Java	Object-C	C++	C#/C++	…

终端上的前端展现与交互技术，通过应用层的各种网络协议完成信息交互和数据传递，结合云端上的后端服务构建技术共同整合成完整的 Web 应用服务。前端的 HTML、CSS、DOM、JavaScript 等技术负责应用的内容展现与逻辑执行，后端的动态网页技术、数据库技术用于服务器端的逻辑执行和资源管理。

Web 运行环境决定了 Web 应用和混合应用与本地应用的本质不同。通过 Web 技术编写的应用，必须经由浏览器内核完成 JavaScript 逻辑执行和网页标记语言的解析渲染。同时强大的 HTML5 技术和多种中间件提供了许多 JavaScript 扩展 API，使得 Web 技术应用程序可以像本地应用一样调用设备 API、网络 API 以及开放平台 API。

2.3 HTML5 移动应用的优势和劣势

任何技术都有其专长和不足，HTML5 移动应用也不例外。了解这些优势和劣势，对于充分发挥 HTML5 在移动开发方面的潜力，避免技术风险是极其重要的。

2.3.1 HTML5 开发优势

HTML5 技术的最大卖点就是良好的跨平台特性，使用该技术编写的应用不加修改即可在各种移动操作系统平台下运行。表 1 将 Web 应用和原生应用在系统平台支持和编程语言支持方面进行了一个对比。

一个成熟的原生应用为了扩展用户群，会尽可能开发不同平台的各种版本，任何一次应用软件升级都意味着所有版本进行更新，这种低下的开发效率一直困扰着应用开发者。相比之下，基于 Web 技术的应用无需下载，可以在运行 Web 应用时动态升级。Web 应用也可以很容易地从一个应用跳到另一个应用，用户所要做的只是打开另一个页面而已。

运行在浏览器上的 Web 应用凭借跨平台优势，可以支持各种不同类型的移动智能终端，以较低的开发成本开发性能良好的应用，同时避免了苹果漫长的审核过程，以及 Android 系统的严重碎片化。对于混合应用，开发者只需要修改应用中的原生代码部分，就可以利用开发框架迅速打包成适用于各种移动平台的应用程序。

通过 HTML5 的大量新特性，基于 Web 技术的应用程序可以实现原先只有原生应用才能实现的功能，例如前文所述的本地存储和音视频播放 通过中间件实现的照相机、电话本调用以及图形处理器（GPU：Graphic Processing Unit）硬件加速。HTML5 对移动定位服务（LBS：Location-Based Service）的支持是另一亮点。LBS 是通过无线通讯网络（如 GSM、CDMA）或者外部定位方式（如 GPS）获取移动终端用户的位置。精确定位是现在无处不在的社交网络服务（SNS：Social Networking Service）中的一个重要功能，借助 HTML5 新增的 Geolocation API，应用可以提供用户位置的经度和纬度。

2.3.2 HTML5 开发劣势

一项技术在出现和发展之初总会存在一些问题，依然处于雏型的 HTML5 技术同样也有很多缺点。2012 年 9 月，Facebook 联合创始人、CEO 马克·扎克伯格在 Techcrunch Disrupt 大会上表示，Facebook 投入大量资源开发 HTML5 应用是个错误，决定转到原生应用的路线上来。这个消息无疑是给火热的 HTML5 移动开发浇了一盆冷水。当然，对于这

个决定，Facebook 的理由也是绝对充分，对于 SNS 网站的应用软件开发，用户体验是重中之重，不一致的消息提醒，缓慢的网页速度和小问题不断，迫使 Facebook 放弃 HTML5 应用。

移动浏览器性能差也成为 HTML5 应用的另一个严重弊病。原生应用可以直接使用终端操作系统上的各种内建功能，而 HTML5 应用则需要通过浏览器内核，将网页标记语言转换为移动终端操作系统的功能调用。部分浏览器的 GPU 加速能力有限，在运行 HTML5 应用时图片加载和处理速度都比较缓慢，这就严重影响了应用运行的流畅性。

浏览器支持差异也是限制 HTML5 应用发展的一大因素。Web 应用是运行在浏览器上的移动应用，不同浏览器对 HTML5 支持有明显区别，业界普遍采用 HTML5 测试对浏览器进行评分，得分情况体现浏览器对 HTML5 标准和相关规范的支持程度。该测试对 HTML5 大部分功能进行测试，每个功能可得到一个或多个点，最后将各项得分汇总得到一个整体的分数。由于 HTML5 并不指定音频和视频编码器，HTML5 测试将对音视频编码器、可缩放矢量图形（SVG：Scalable Vector Graphics）或数学置标语言（MathML：Mathematical Markup Language）的支持作为附加分给予浏览器。各移动浏览器的 HTML5 支持程度评分情况如表 2 所示[4]。移动浏览器还无法支持大部分 HTML5 新增特性，很多 Web 应用无法在移动智能终端上运行。

混合应用也存在同样的问题。以 PhoneGap 应用为例，在 Android 系统上，PhoneGap 运行在 WebView 组件中；而在 iOS 上，PhoneGap 运行在 UIWebView 组件中。虽然两者都使用 Webkit 引擎，但对于 JavaScript 和本地 API 相互调用原理完全不同，造成了应用效果差异。

基于 Web 技术的应用要求更流畅的网络环境和移动智能终端设备 API 更好的支持，现在的网络和硬件环境仍达不到要求。Web 应用另一个严重的缺陷在于 HTML5 标准仍然悬而未定，不成熟的标准无法给予足够的安全保障和统一的应用效果。

表 2 移动浏览器 HTML5 技术评分

移动浏览器	评分	附加分
Opera Mobile 12.10	406	12
Chrome	390	11
Firefox Mobile 16	388	10
iOS 6.0	386	9
Windows Phone 8	320	6
Android 4.0	297	3
BlackBerry OS 7	288	3
Bada 2.0	283	9
Nokia Belle FP 2	272	9
Android 2.3	200	1

3 HTML5 的安全威胁

当前，很多大型应用开发企业的目标是实现应用更多的功能，便于用户使用，而安全性则一直是事后考虑的问题。以 HTML5 为代表的新型 Web 技术的功能在不断地增强，却持续沿用不变的安全标准[5]，已经滞后于技术前进的脚步。

3.1 HTML5 技术应用的安全隐患

HTML5 的飞速发展必然会带来两个问题。首先，许多新技术尚未完全发展成熟即被大量使用，其中难免存在安全隐患。其次，大量新功能的加入使得整个技术体系变得更加复杂，开发者难以将各方面的问题都考虑周全，从而更容易在代码中引入安全缺陷。在 HTML5 时代，原有的 Web 安全问题依然存在，跨站脚本攻击（XSS：Cross Site Scripting）、SQL 注入并不会消失。与此同时，新技术给攻击者提供了新的途径。具体对于移动智能终端来说，不同平台上不同移动浏览器的差异也会引发安全问题。开放式 Web 应用程序安全项目（OWASP：Open Web Application Security Project）发布了移动应用的十大风险[6]：

⑴ 不安全的数据存储；
⑵ 弱服务器端控件；
⑶ 薄弱的传输层保护；
⑷ 客户端注入；
⑸ 授权和认证的欠缺；
⑹ 会话处理不当；
⑺ 通过不可信输入的安全判决；
⑻ 旁道数据泄露；
⑼ 残破的加密技术；
⑽ 敏感信息泄露。

3.2 HTML5 技术开发应用程序的安全考虑

由于 HTML5 技术在使用中可能出现多种安全问题，开发者应具备基本的安全意识和技能，在编写代码时避免安全漏洞的产生。为了帮助开发者编写更安全可靠的移动应用，OWASP 给出了移动控制和设计原则[6]：

⑴ 识别和保护移动设备上的敏感信息；
⑵ 设备上安全地处理密码认证；
⑶ 确保传输过程中的敏感数据保护；
⑷ 正确实现用户认证、授权和会话管理；
⑸ 确保后端 API（服务）和平台（服务器）安全；
⑹ 与第三方服务和应用的安全数据整合；
⑺ 特别注意用户数据的收集和使用准许的存储及收集；
⑻ 实现阻止访问未授权付费资源的控制（钱包，短信和电话等）；
⑼ 确保安全经销或供应移动应用；
⑽ 对任何一个运行时发生的代码错误进行仔细检查。

3.2.1 Web 应用的安全考虑

HTML5 技术实现的本地存储、跨域共享和新标签的使用带来了很多安全隐患。

本地存储首当其冲。使用 HTML5 之前，应用将用户身份认证信息存储在最大容量为 4KB 的 cookie 中，其中的数据可以通过 HTTPOnly 标签来保护，尽管有些移动浏览器可能并不支持这个标签[5]。但是在 HTML5 时代，开发者可以将大量的用户信息和备份数据长期保存在最大 5MB 的空间中，明文存储的数据很容易被攻击者获取并利用，例如 XSS、跨目录攻击、DNS 欺骗等。通过这些攻击方式，攻击者可以轻易盗取用户存储在浏览器或其他应用目录下的用户敏感信息。为了防止这类攻击的发生，开发者务必做好规划整理，将本地存储数据隔离到单独的目录中，并确保该目录及其子目录的访问权限可控。

跨域资源共享（CORS：Cross-Origin Resource Sharing）提供了一种 Web 服务在不同的网域间传递资源的方法。HTML5 增加了两个跨源资源模块：跨文档消息通告和 XML HTTP Request Level 2。XML HTTP Request Level 2 实质上只是一个新的规范，仍使用 XML HTTP Request 对象。CORS 能够避开浏览器的同源策略，而同源策略是 Web 浏览器内置的基本安全措施之一。开发者在运用 CORS 时应尤其注意外部输入，对所有发送来的数据都要进行严格的审核，特别是要格外地注意字符串输入，避免恶意的 CORS 请求，以防止服务器遭受 DDoS、XSS 等攻击。

HTML5 新增的 Geolocation API 备受关注，该接口允许用户在 Web 应用中共享地理位置。HTML5 的 Geolocation 规范提供了一套用户隐私保护机制，但如果开发者将定位服务嵌入网页中，而该页面本身已经被攻击，此时用户的精确位置就有可能被攻击者截获。开发者使用此 API 时应设置提醒，在得到用户同意后，方可以获得用户地理位置信息。

HTML5 提供的其它新特性也存在一定的安全隐患。例如，HTML5 Web Workers 让 Web 应用具备了后台处理能力。攻击者可通过网页中的 JavaScript 进行多线程作业，从而借助用户浏览器进行大量破解操作，或者制造一个 HTML5 僵尸网络。再者，HTML5 新增的标签和属性也有可能绕过跨站黑名单策略，构成安全隐患。为了避免这些问题，在开发过程中，应保证良好的编码逻辑，控制用户敏感信息的使用权限；在云端，服务器侧运行的代码也要保障外部输入信息的安全过滤，降低攻击成功的可能性。

3.2.2 混合应用的安全考虑

混合应用由两部分代码组成：一部分是运行在 Web 运行环境中的 HTML5 代码，另一部分是运行在移动智能终端中的原生代码，用以调用设备 API。HTML5 代码和 Web 应用一样，存在着 Web 技术的各种安全威胁，而原生代码部分可以调用设备 API，将更多的用户敏感信息暴露给了攻击者。

混合应用多数使用移动开发框架完成开发。以 PhoneGap 为例，开发者可以利用移动智能终端的核心功能（如地理定位、加速器、联系人、声音、振动等），通过 HTML5 技术构建跨平台的移动应用程序。移动开发框架作为移动应用和移动智能终端的桥梁，连接着 Web 技术代码和设备自建功能，起着过渡和隔离的作用，可以通过谨慎封装敏感 API，在开发过程中保障移动应用程序的安全性。

4 结语

作为新一代 Web 技术发展的方向，HTML5 一经推出就得到广泛的关注，目前已在基础架构支持和技术采纳方面取得了较大的进展。同样的趋势也出现在移动计算领域，各种移动浏览器纷纷增强对 HTML5 的支持，同时使用 HTML5 开发移动应用开始成为原生应用之外的另一种选择。现阶段 HTML5 技术在移动智能终端上的应用仍存在着诸多问题，但随着标准的完善、网络环境和硬件的改进，基于 HTML5 的移动应用可望提供更好的用户体验，并且具备更完善的安全保障。 MSTT

参考文献

[1] Eric Freeman, Elisabeth Robson. Head First HTML5 Programming [M]. USA: O'Reilly Media, 2011.

[2] W3C HTML 5.1 Nightly Editor's Draft [Z/OL]. [2012-12-11].http://www.w3.org/html/wg/drafts/html/master/introduction.html#history-0.

[3] 新一代移动 Web 技术白皮书[Z/OL].2012.9.http://www.catr.cn/data/bps/201209/P020120926561160330614.pdf.

[4] The HTML5 test-how well does your browser support HTML5? [Z/OL].2012.12.13. http://html5test.com/results/mobile.html.

[5] Himanshu Dwivedi,Chris Clark,David Thiel. Mobile Application Security [M]. McGraw-Hill, 2010.252-275.

[6] OWASP Mobile Security Project [Z/OL]. https://www.owasp.org/index.php/Mobile.

中国移动无线城市用户数达 6500 万

截至 2012 年 10 月底，中国移动无线城市已覆盖全国 30 个省，共有 336 个城市的无线城市已上线推广。截至 10 月，中国移动无线城市累计独立使用用户数达 6500 万。

从应用上线城市数量来看，最多的应用为火车查询、天气查询、政务新闻。本地特色应用中，部分应用的用户访问量（年度累计 PV）已初具规模，如福建的公交查询达 5400 万、江苏的智慧购达 2300 万、广东的商家联盟达 2300 万等。

此外，中国移动还在湖北及上海分别推出了"数字城管"应用和"旅游服务"应用。其中，"数字城管"应用可以将当地市民身边的烦心事通过城管通拍照及 GPS 定位，将信息传递给数字化城市管理监督指挥中心。而在上海，"旅游服务"应用具有景点查询、门票购买、周边查询、实景地图查看等功能。可为市民提供上海本地 17 个区县在线查询 419 个旅游景点的信息，包括旅游景点介绍、门票信息、出行指南、门票购买、景点实际景色等内容，为市民假日出行提供参考及优惠。

NTT、NEC 及富士通将共同研发 400Gbit/s 光传输技术

NTT、NEC 与富士通将共同研发世界最高数据传输等级的光传输技术，单一信道传输速度可望达到 400Gbit/s，预定 2014 年内完成研发。

目前 3 家公司预定采用的研发方式，是将 100Gbit/s 光传输技术使用的 4 位相位偏移变调技术强化为 16 位正交振幅调变，借以实现单一通道 400Gbit/s 的光传输技术，若将其用于高密度的 60 信道光纤，那么未来仅靠一条光纤就能办到 24Tbit/s 的数据传输等级。省电研究方面，只要能完成光纤中的非线形光学效果、波长分散、偏波模式分散等补偿技术，即可进行长距离传输，如此不仅可删减中继设备达到省电 50%的目标，也能因应传输路径状态在同一硬件中执行多种讯号变调方式，如此构成的网络结构只要使用一种核心技术即可对应不同地区需求，应对性与适应性将更强。