北京郵電大學
Beijing University of Posts and Telecommunications

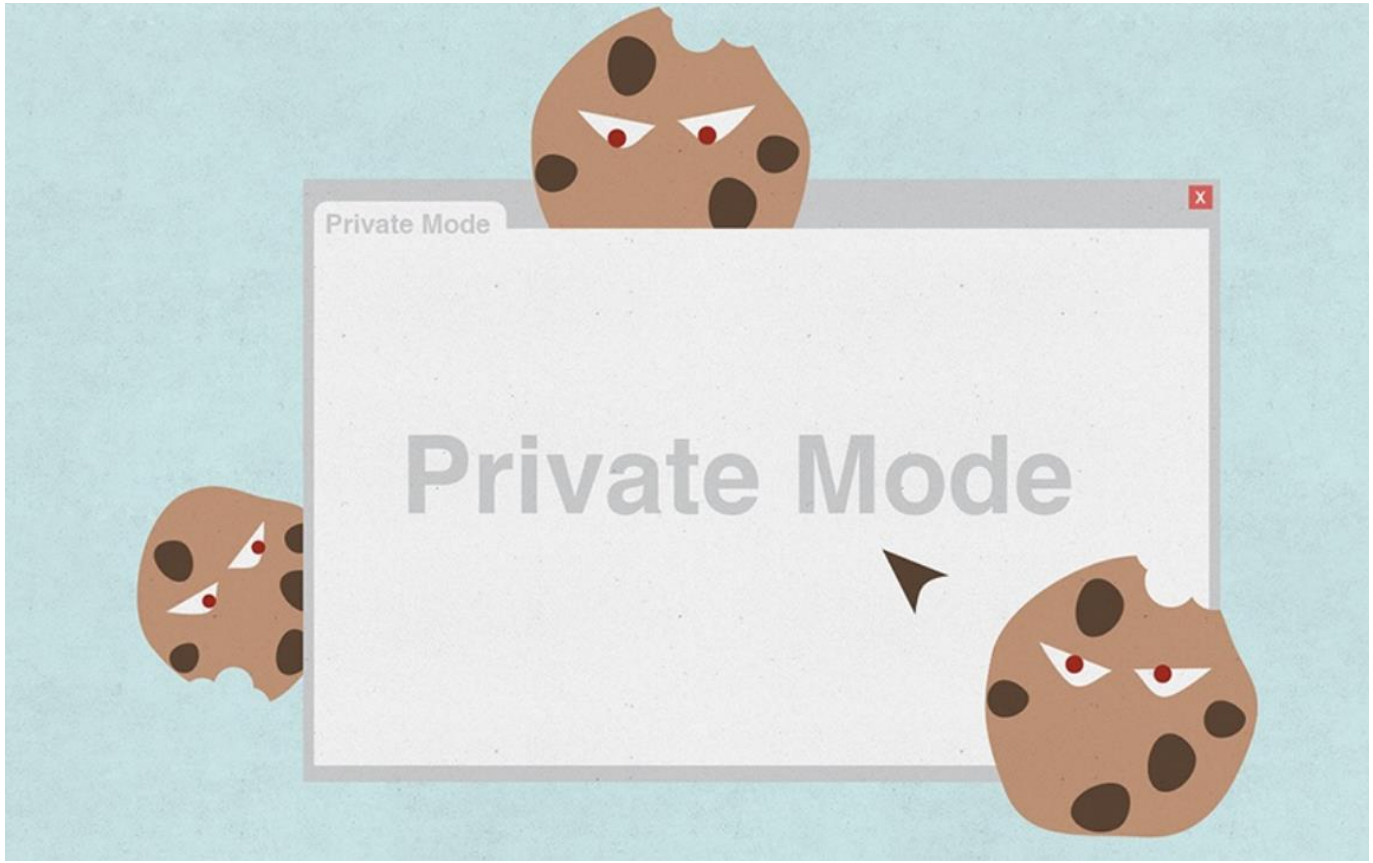
# 大数据安全与隐私保护
# 身份认证-Cookie

石瑞生
网络空间安全学院

# 提纲

- Cookie的工作原理
- Cookie与身份认证
- Cookie劫持攻击

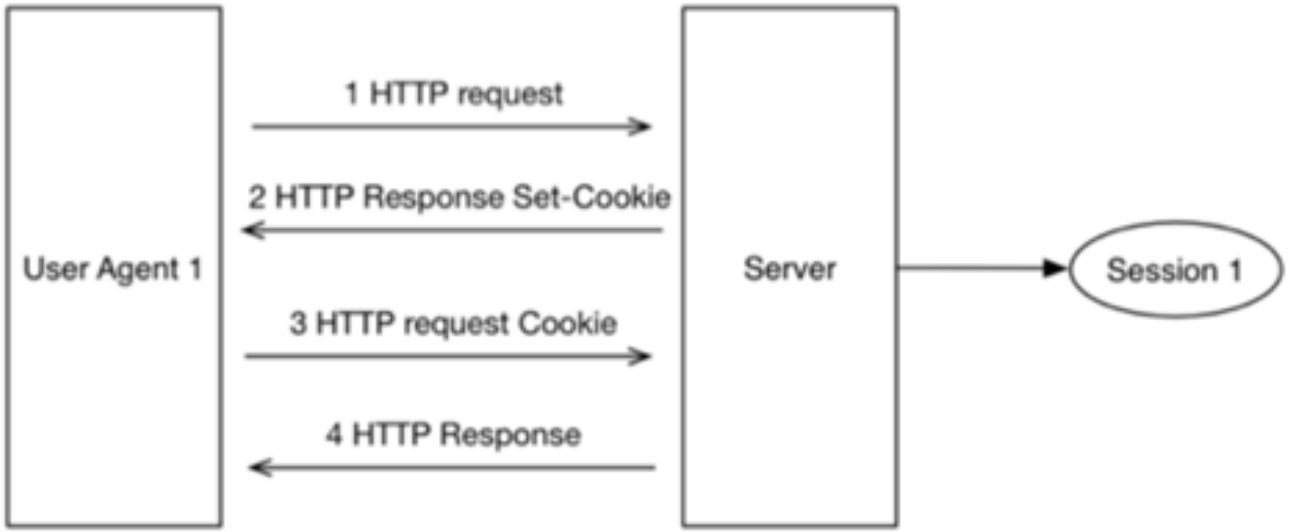
# Web 甜饼




- 会话管理
- 个性化设置
- 认证Cookie
- Online Tracking

# Cookie的工作原理

- 当用户访问一个网站时，web服务器设置cookie属性(即、名称、值、标志、过期日期和匹配规则)。
  - 设置的方式可以是静态地使用Set-Cookie，也可以使用JavaScript。
- 当用户发出HTTP或HTTPS请求时，浏览器将发送cookie，其匹配规则对应于请求的URL和协议。
  - 浏览器不会在常规HTTP连接上传输带有HTTPS属性的cookie。



# Cookie的安全属性

- 访问控制： {域名，目录，时间} ，HTTPOnly，Secure（HTTPS），SameSite

| Name | Value | Domain | Path | Expires / Max-Age | Size | HttpOnly | Secure | SameSite |
|---|---|---|---|---|---|---|---|---|
| BAIDUID | 98C544FDDC76A... | .baidu.com | / | 2021-03-21T05:34:10.248Z | 44 | | | |
| BDUSS | h4dGNOY2tyS29... | .baidu.com | / | 2028-06-11T10:10:09.364Z | 197 | ✓ | | |
| BD_HOME | 1 | www.baidu.com | / | Session | 8 | | | |
| BD_UPN | 12314753 | www.baidu.com | / | 2020-04-04T10:10:11.000Z | 14 | | | |
| BIDUPSID | 9E7F1CDE15563C... | .baidu.com | / | 2087-08-03T18:27:16.969Z | 40 | | | |
| COOKIE_SESSION | 0_0_1_1_0_2_0_0_... | www.baidu.com | / | 2020-07-15T15:13:16.000Z | 85 | | | |
| H_PS_PSSID | 30968_1429_311... | .baidu.com | / | Session | 56 | | | |
| PSTM | 1563289991 | .baidu.com | / | 2087-08-03T18:27:16.969Z | 14 | | | |

Cookie的HttpOnly属性，指浏览器不要在除HTTP（和 HTTPS)请求之外暴露Cookie。
一个有HttpOnly属性的Cookie，不能通过非HTTP方式来访问，例如通过调用JavaScript(例如，引用document.cookie），因此，不可能通过跨域脚本（XSS）来偷走这种Cookie。
Facebook 和 Google 正在广泛地使用HttpOnly属性。

Secure Cookie机制指的是设置了secure标志的cookie。Secure Cookie仅在https层面上安全传输，如果是http请求，就不会带上这个cookie。这样能降低重要的cookie被中间人截获的风险。

# Cookie与身份认证

# 身份认证 - authentication cookie(s) (auth-cookies)

- 除了维护用户的状态外，网站还使用cookie对用户进行身份验证。
  - 当用户最初向web服务器进行身份验证时，web服务器将设置多个authcookie。
  - Auth-cookies确保在连接中断的情况下(例如，由于TCP会话终止或用户IP地址的更改)，用户的会话保持连续。
  - 许多网站使用不同的auth-cookies组合来控制对网站不同部分的访问(例如，填写购物车的用户可能需要一组不同于在购物车中购买商品的cookies)。

最初使用用户名和密码登录网站的用户随后可以简单地提供身份验证cookie(auth-cookies)来访问该网站。因此，一旦用户对web服务器进行了身份验证，auth-cookie就是一个关键的安全节点（linchpin）:在许多情况下，对这些auth-cookie的访问使攻击者能够完全控制用户的帐户。

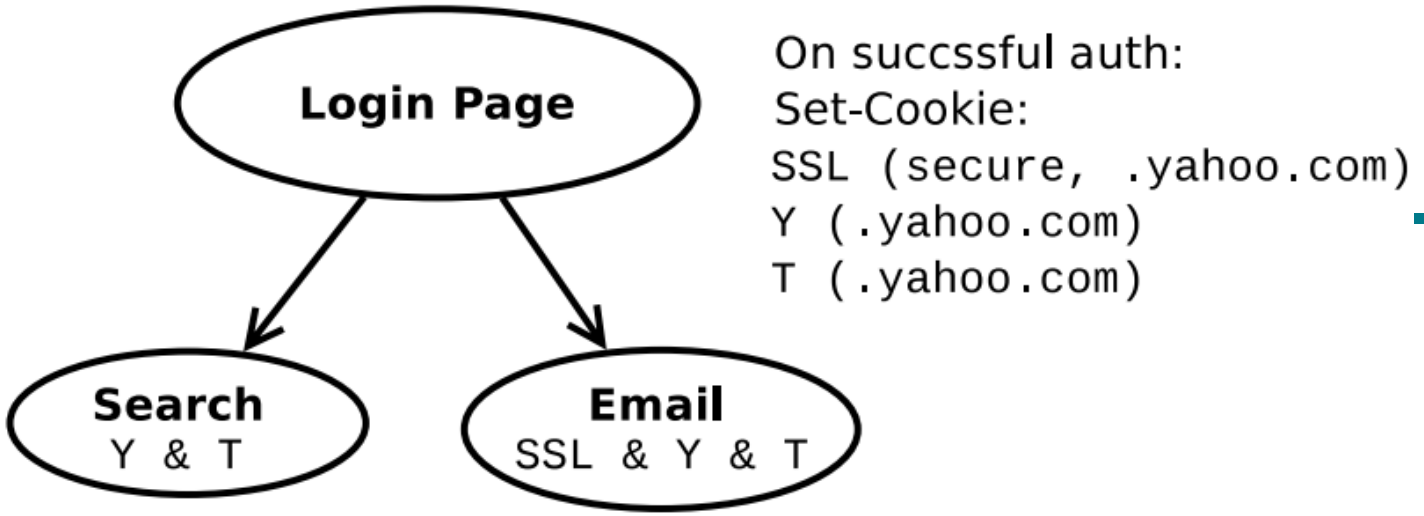



**Figure 1:** *A simplified authentication model for* `yahoo.com`.

- 例如，假设用户登录到yahoo.com，该站点设置了Y、T和SSL cookie。
  - Y、T和SSL cookie在.yahoo.com和path(" / ")上匹配，但SSL cookie仅在HTTPS连接到.yahoo.com时匹配。
- cookie的不同组合(及其正确的值)对用户进行身份验证，以访问站点的不同部分:
  - Y和T允许用户访问搜索历史记录;
  - 访问电子邮件也需要SSL cookie。

# Cookie劫持攻击

# 被动攻击 - 通过被动窃听进行实验

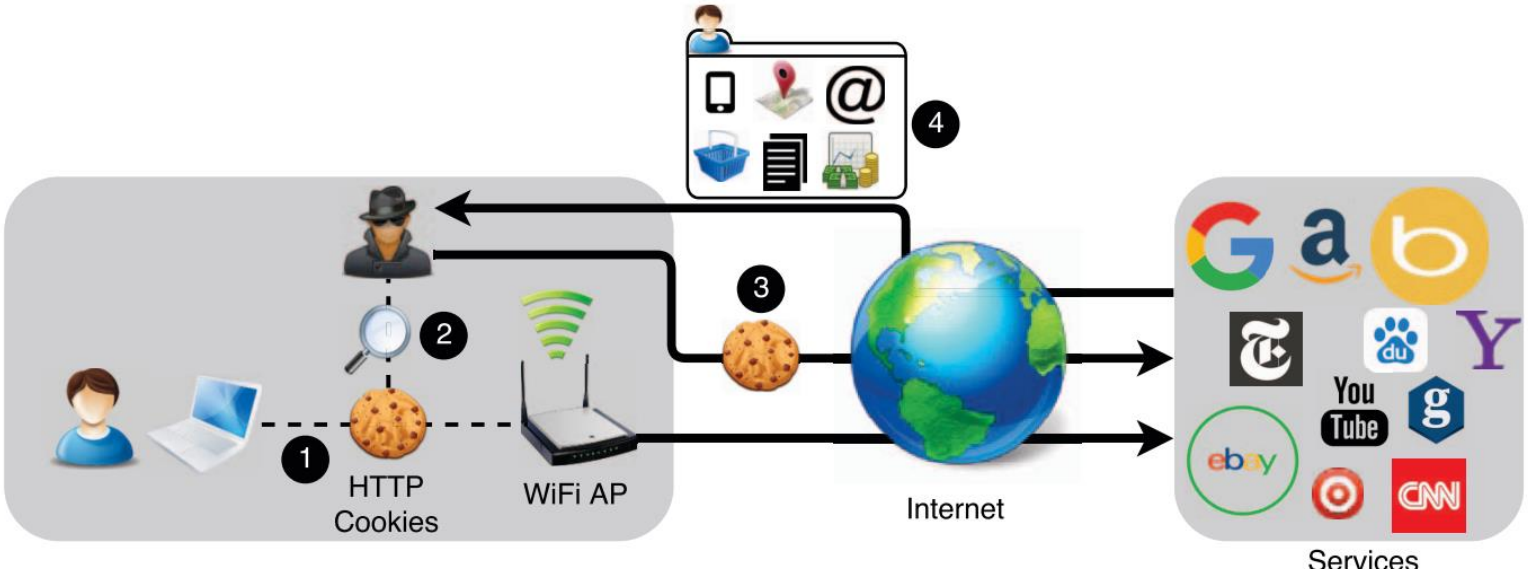



Fig. 1. Workflow of an HTTP cookie hijacking attack. After the victim's cookies are exposed on the unencrypted connection ❶ and stolen ❷, the attacker can append the stolen cookies when browsing the target websites ❸ and gain access to the victim's personal information and account functionality ❹.

**HTTP Cookie劫持**

对手监视公共无线网络的流量，例如大学校园或咖啡店的流量。图1展示了Cookie劫持攻击的工作流程。用户连接到无线网络以浏览网页。浏览器将用户的HTTP cookie附加到通过未加密连接（❶）以明文形式发送的请求。窃听者正在监视流量，窃听者从网络跟踪（❷）中提取用户的HTTP cookie，并使用被窃取的cookie（❸）连接到易受攻击的服务。这些服务从cookie中"识别"用户并提供网站的个性化版本，从而将用户的个人信息和帐户功能暴露给对手（❹）。

# 主动攻击

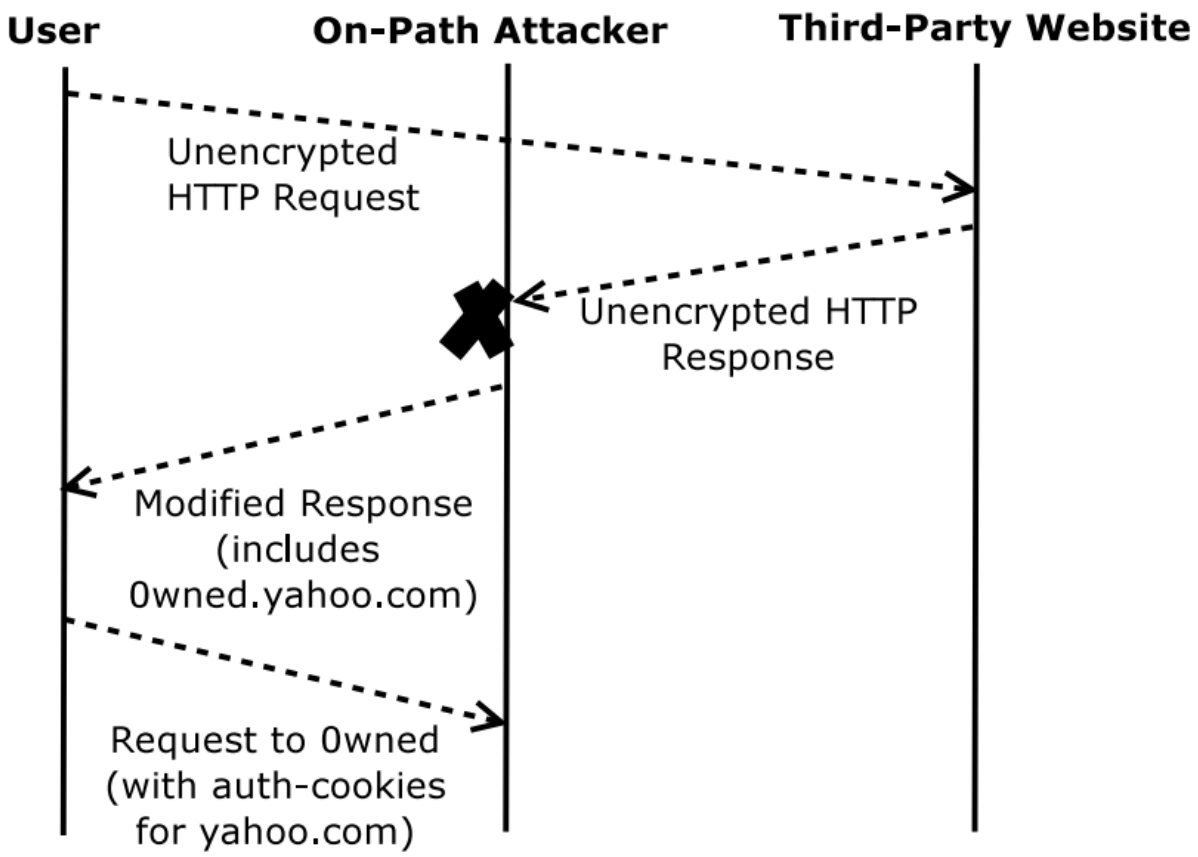



**Figure 2:** *An on-path attacker can gain unauthorized access to a user's search history. (We discovered this vulnerability on* `yahoo.com`*.)*

- 拦截未加密的authcookie的on-path攻击者

例如，即使用户没有明确访问那些网站，攻击者也可以**注入内容**以迫使用户的浏览器向特定的易受攻击的网站发送请求并公开用户的Cookie。

# 对真实网站的HTTP cookie劫持攻击（2016 SP）

| Service | HTTPS Adoption | Cookie Hijacking | XSS Cookie Hijacking | Information and Account Functionality Exposed |
|---|---|---|---|---|
| Google | partial | ✓ | ✗ | first and last name, username, email address, profile picture, home and work address, search optimization, click history of websites returned in search results |
| Baidu | partial | ✓ | ✓ | username, email address, profile picture, entire search history, address of any saved location |
| Bing | partial | ✓ | ✓ | first name, profile photo, view/edit search history (incl. images and videos), links clicked from search results, frequent search terms, saved locations, information in interest manager, edit interest manager |
| Yahoo | partial | ✓ | ✓ | username, full name, email address, view/edit search history, view/edit/post answers and questions in Yahoo Answers (anonymous or eponymous), view/edit finance portfolio, view subject and sender of latest incoming emails, extract contact list and send email as user |
| Youtube | partial | ✓ | ✗ | view and change (through pollution attacks) recommended videos and channels |
| Amazon | partial | ✓ | ✓ | view user credentials (username, email address or mobile number), view/edit profile picture, view recommended items, view user wish lists, view recently browsed items, view recently bought items, view/edit items in cart, view shipping name and city, view current balance, view user's review (even anonymous), send email of products or wishlist on behalf of user, obtain email addresses of previously emailed contacts |
| Ebay | partial | ✓ | ✓ | delivery name and address, view/edit items in cart, view/edit purchase history, view items for sale, view previous bids, view user's messages, view/edit watch list and wish lists |
| MSN | partial | ✓ | ✓ | first and last name, email address, profile picture |
| Walmart | partial | ✓ | ✓ | first name, email address, view/edit items in cart, view delivery postcode, write product review |
| Target | partial | ✓ | ✓ | first name, email address, view/edit items in cart, recently viewed items, view and modify wish list, send email about products or wish list |
| CNN | partial | ✓ | ✓ | view/edit profile (full name, postal address, email address, phone number, profile picture) view/edit linked Facebook account, write/delete article comments, recently viewed content on iReport |
| New York Times | partial | ✓ | ✓ | username, email address, view/edit basic profile (display name, location, personal website, bio, profile picture) username, email address, view/edit list of saved articles, share article via email on behalf of user |
| Huffington Post | partial | ✓ | partial | profile can be viewed and edited (login name, profile photo, email address, biography, postal code, location, subscriptions, fans, comments and followings). change account password, delete account |
| The Guardian | partial | ✓ | ✓ | username, view public section of profile (profile picture, bio, interests), user's comments, replies, tags and categories of viewed articles, post comments on articles as user |
| Doubleclick | partial | ✓ | ✓ | ads show content targeted to user's profile characteristics or recently viewed content |
| Skype | partial* | ✗ | ✗ | - |
| LinkedIn | partial* | ✗ | ✗ | - |
| Craigslist | partial* | ✗ | ✗ | - |
| Chase Bank | partial* | ✗ | ✗ | - |
| Bank of America | partial* | ✗ | ✗ | - |
| Facebook | full | ✗ | ✗ | N/A |
| Twitter | full | ✗ | ✗ | N/A |
| Google+ | full | ✗ | ✗ | N/A |
| Live (Hotmail) | full | ✗ | ✗ | N/A |
| Gmail | full | ✗ | ✗ | N/A |
| Paypal | full | ✗ | ✗ | N/A |

*While these services do not have ubiquitous HTTPS, no personalization is offered over HTTP pages.

- HSTS如何影响HTTP cookie劫持：部分部署使该机制无效，因为单个未加密的连接可能足以使攻击者获取所需的cookie。

# 阅读材料 - cookie hijacking


1) 2001_USENIX_Dos and Don'ts of Client Authentication on the Web
2) S. Calzavara, G. Tolomei, M. Bugliesi, and S. Orlando. Quite a mess in my cookie jar!: Leveraging machine learning to protect web authentication. In Proceedings of the 23rd International Conference on World Wide Web, 2014.
3) Zheng, X., Jiang, J., Liang, J., Duan, H., Chen, S., Wan, T., and Weaver, N. Cookies lack integrity: Real-world implications. In USENIX Security 2015 (Aug. 2015).
4) Mundada Y, Feamster N, Krishnamurthy B. Half-Baked Cookies: Hardening Cookie-Based Authentication for the Modern Web.[J]. 2016. AsiaCCS 【如何检测Cookie劫持攻击】
5) Sivakorn, Suphannee, Iasonas Polakis, and Angelos D. Keromytis. "The cracked cookie jar: **HTTP cookie hijacking** and the exposure of private information." In *2016 IEEE Symposium on Security and Privacy (SP)*, pp. 724-742. IEEE, 2016. 【Cookie劫持攻击的威胁广泛存在】
6) Kwon, Hyunsoo, Hyunjae Nam, Sangtae Lee, Changhee Hahn, and Junbeom Hur. "(In-) Security of Cookies in HTTPS: Cookie Theft by Removing Cookie Flags." *IEEE Transactions on Information Forensics and Security* (2019).
7) 2022_Helmholtz_The State of the SameSite_ Studying the Usage,Effectiveness, and Adequacy of SameSite Cookies

北京郵電大學
Beijing University of Posts and Telecommunications

# 感谢聆听！