

Authentication for Web Servers

Michael Gray

University of Cambridge

Department of Engineering

<http://www.eng.cam.ac.uk/~mjg17/webauth/>



UNIVERSITY OF
CAMBRIDGE

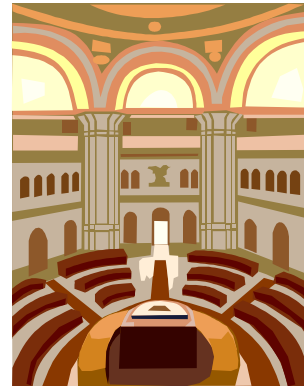
Department of Engineering

Overview

- Requirements
- Techniques
- Credentials
- Implementation

Terminology

- Access control
 - Open for business?
 - Open from where?
- Authentication
 - Proof of identity
- Authorization
 - Entitlement to use



Requirements

- Resource providers
- Administrators
- Users
 - Easy to use
 - Lightweight
 - Easy to remember
- Security



Security

- Snooping
 - Passwords
 - Other security info
 - Sensitive content
- Replay
- Guesswork / brute force



Security 2

- Degree of protection vs. cost
 - Ease of use
 - Administration
- Resource
 - Sensitivity / importance
 - Risks / consequences
- SSL



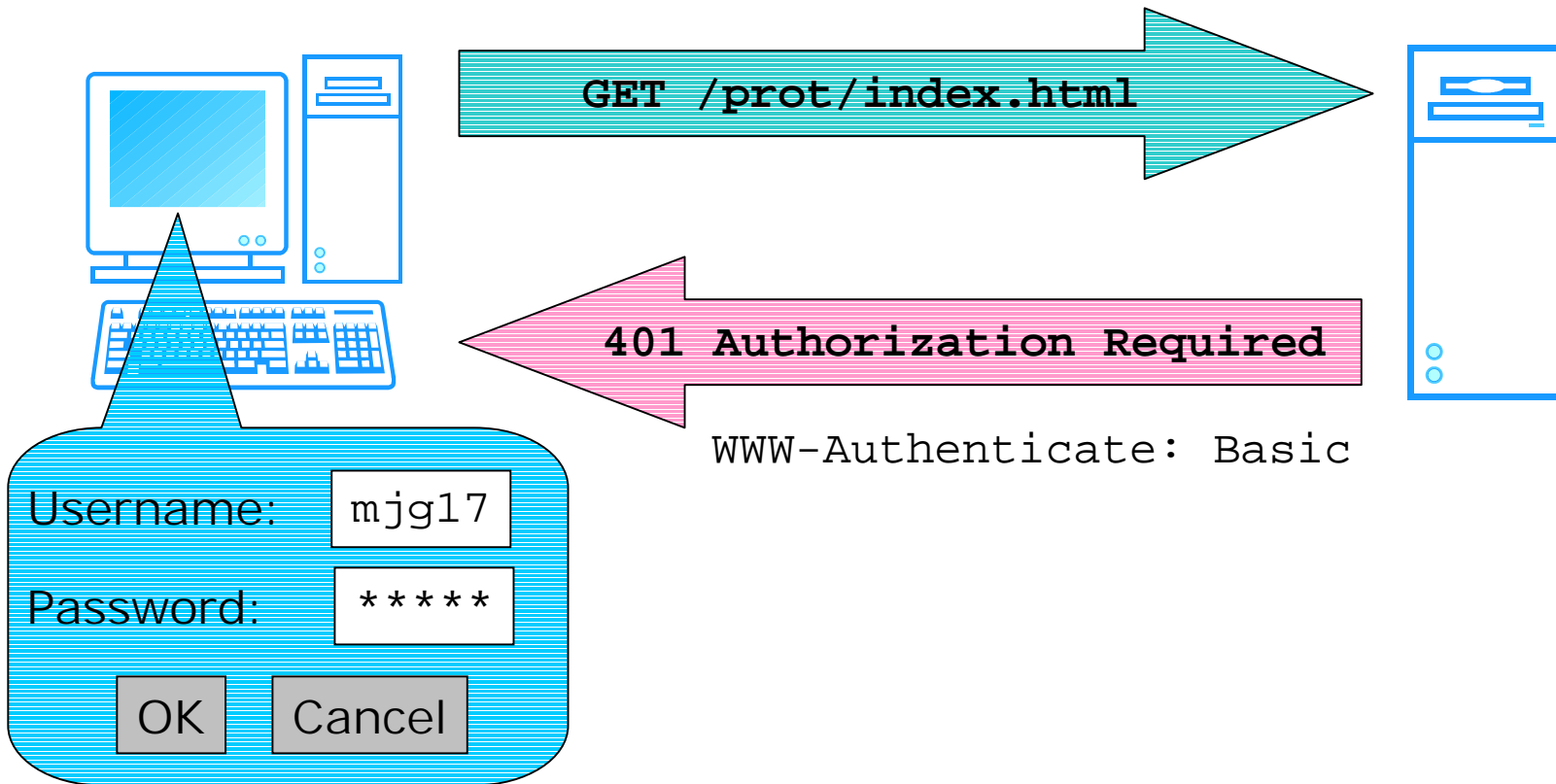
Access Control

- Standard with most web servers
 - 403 Forbidden
 - Fine grain control
- Important
 - Stops most of world from reaching login

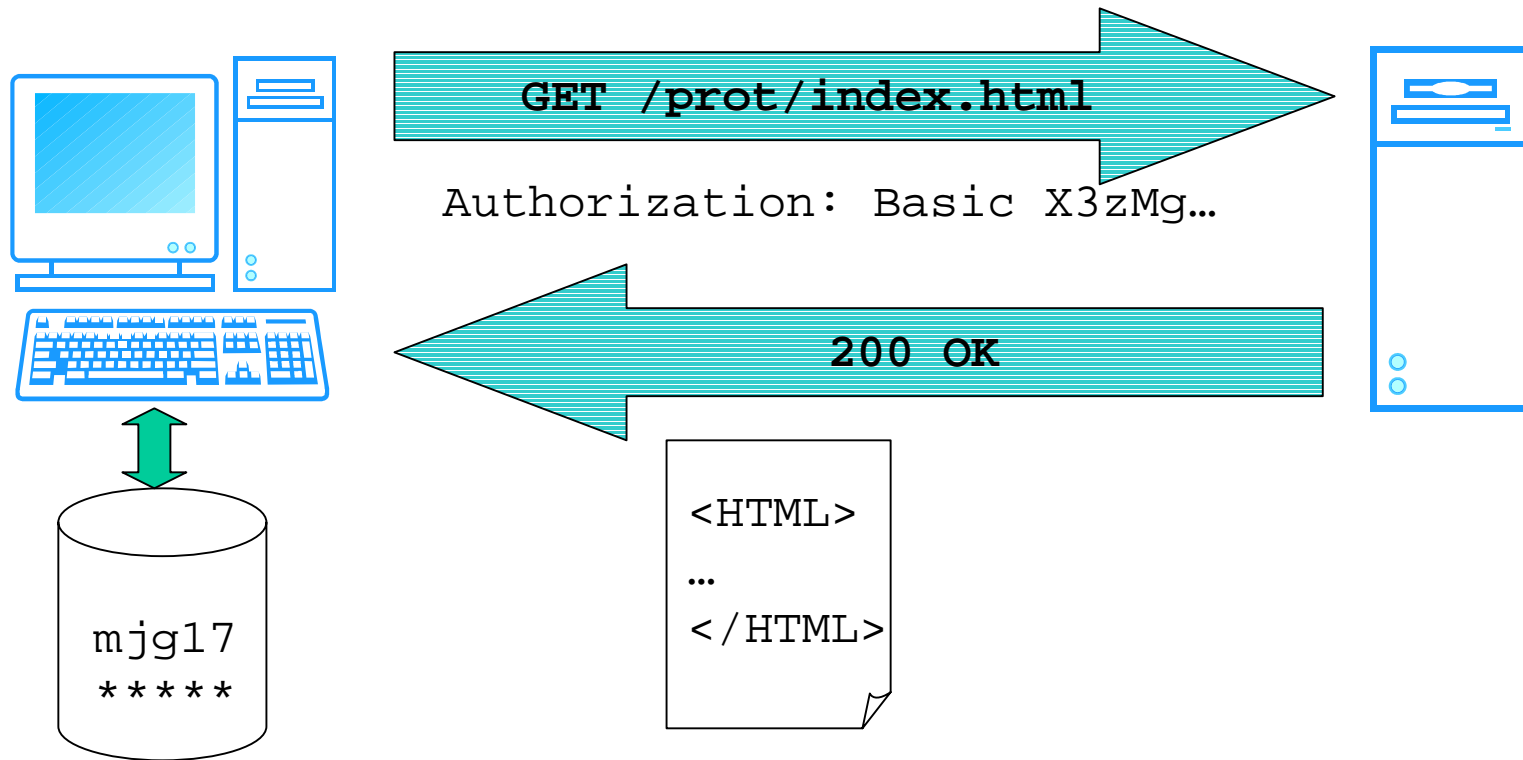
Authentication

- HTTP protocol
 - Basic authentication
 - Digest authentication
- RFC 2617

Basic Authentication



Basic Authentication 2



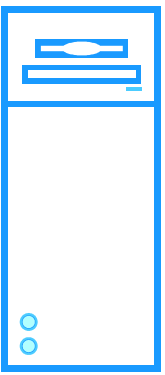
Authentication Alternatives

- Roll your own
- Ticket system

Ticket Authentication



GET /prot/index.html

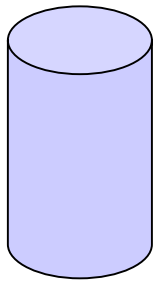
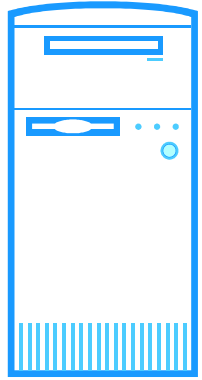


Web server

301 Moved Temporarily

Location:
`http://ticketserv/login.pl`

GET /login.pl

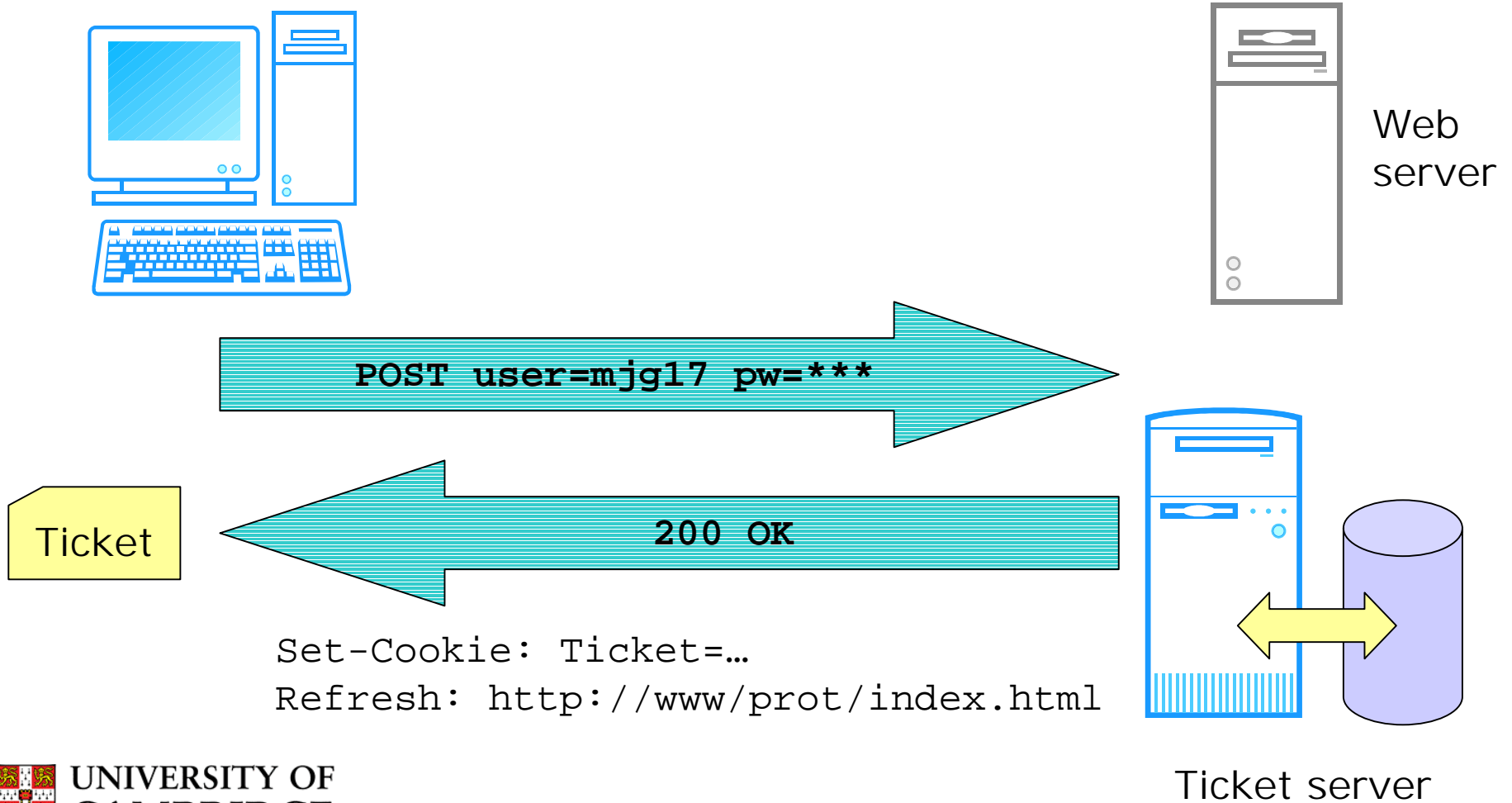


Ticket server

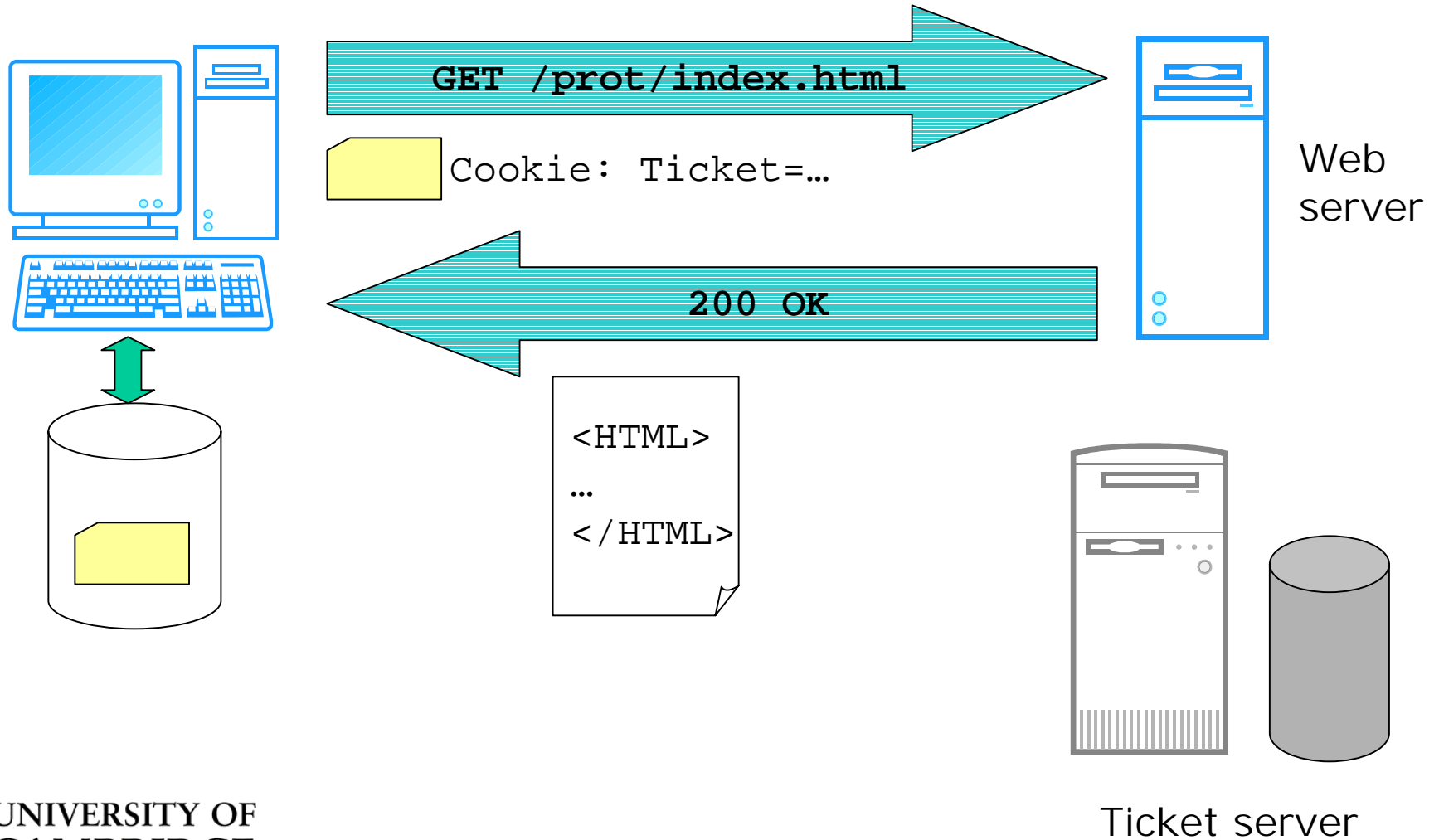
200 OK

```
<HTML>
  <FORM>
  ...
  </FORM>
</HTML>
```

Ticket Authentication 2



Ticket Authentication 3



Ticket Contents

- User name
- Time of issue
- Period of validity
- User's source address
- Message digest hash

+ secret =

The diagram illustrates the process of generating a message digest hash. A yellow box on the left contains a list of ticket contents: User name, Time of issue, Period of validity, User's source address, and Message digest hash. A right-facing curly bracket groups the first four items. To the right of this bracket is the text '+ secret ='. A line extends from the equals sign, goes down, then left, and then up, ending in an arrow that points to the 'Message digest hash' item in the list.

Ticket Transfer

- Cookies
 - Not universally loved
 - Designed for task
- In every URL
 - `http://www.../prot/j4m7d2A6.../dir/index.html`
- Hidden data in form

Ticket System

- System designer has control
- Centralised authentication processing
- Resource independence
- User convenience

- Security
 - Raw credentials protected
 - Expiry time vs. replay attack



Software & Glue

- Apache + mod_perl
 - Excellent for ticket server
 - Fine for web server too
- Apache + module
 - Lightweight
 - Needs compiling / configuring
- Caveat emptor



Authorization

- No spec / protocol
- Up to web server
- Apache: *groups*

- Single resource: *grant or refuse ticket*

- Multiple resources:
 - Leave up to each application
 - Evaluate in ticket server: *realms*



Authentication Credentials

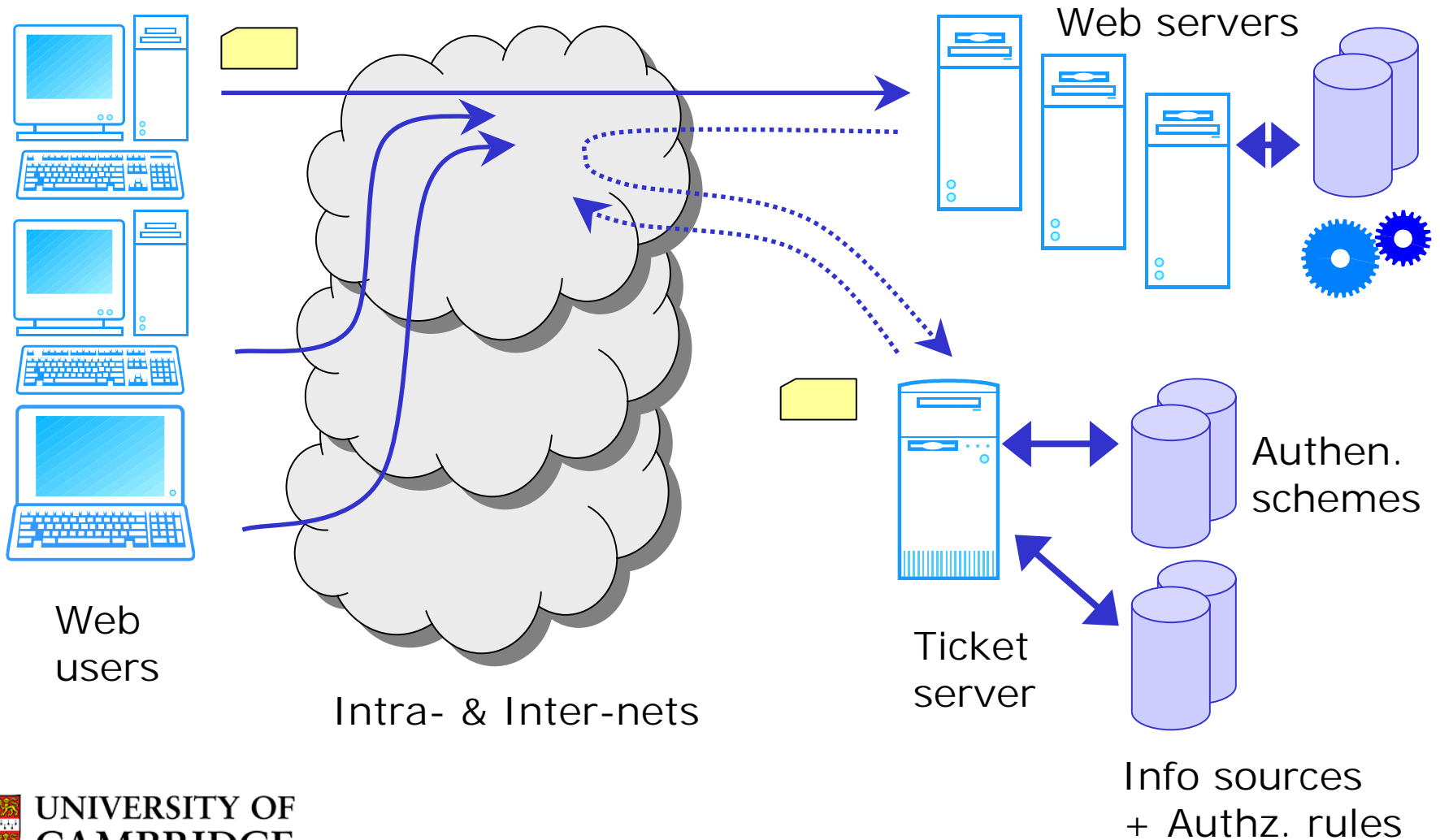
- Consider existing schemes
 - Username
 - Login password
 - Copier PIN
- Passphrase by email
- Ident service



Authorization Decisions

- Groups
 - Generate from database
- User's characteristics / attributes
 - Directory service (LDAP)
 - Other existing people database

Ticket System Summary



Summary

- Planning:
 - Technology
 - Credentials / schemes
 - Administration
- Benefits:
 - Consistency
 - Ease of use
 - Security



Future

- Digital certificates
 - Need public key infrastructure
 - Users use multiple browsers
- Smart cards

Authentication for Web Servers

<http://www.eng.cam.ac.uk/~mjg17/webauth/>

mjg17@eng.cam.ac.uk



UNIVERSITY OF
CAMBRIDGE

Department of Engineering