JA-SIG

Central Authentication Service

Single Sign-on for the Web

Overview

Adam Rybicki

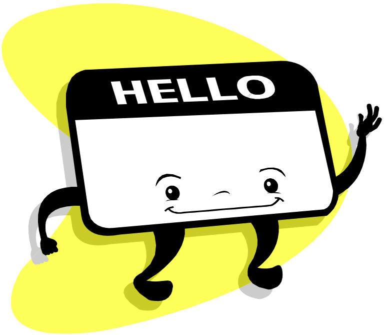
St. Paul, April 28, 2008

Some slides drawn from prior presentations at JA-SIG conferences.

UNICON

Hi. I’m Adam.

- V.P. of Technology at Unicon, Inc.
- Previously CTO at Interactive Business Solutions, Inc. (IBS)

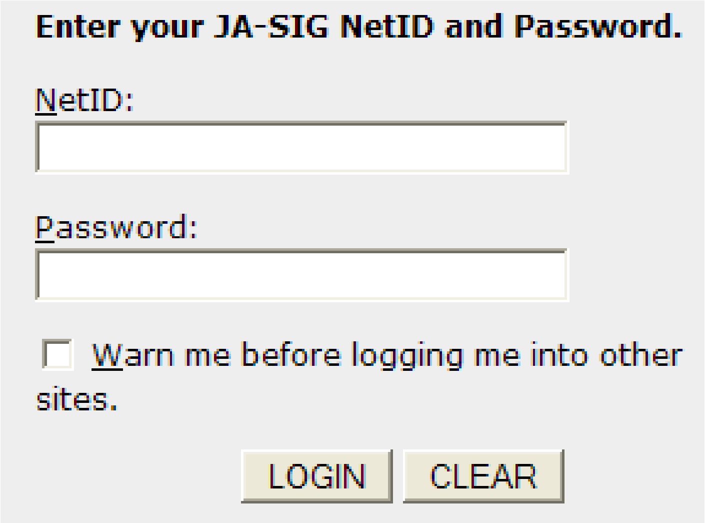


Legalese

- Use of names, logos, etc., does not imply endorsement of this presentation by JA-SIG (or anyone else)
- The opinions of the presenter are his own and not necessarily those of Unicon, JA-SIG, or anyone else.
- Trademarks are those of their respective owners.
- Note massive Creative Commons disclaimer, disclaiming warrantees of any kind.

What is CAS?

- CAS is enterprise single-sign-on for the web.
  - Free
  - Open source
  - Server implemented in Java
  - Clients implemented in a plethora of languages



Enter your JA-SIG NetID and Password.

NetID:

Password:

□ Warn me before logging me into other sites.

Adam’s Involvement with CAS

- Got interested.
- Worked with several clients helping them to CASify their applications.
- Asked many questions of the CAS mail list
- Wrote a CAS self-study guide for Unicon developers. (https://confluence.unicon.net/confluence/x/XgZi) (authentication required)
- Answered some questions on the CAS list.
- Currently working with Unicon clients on CAS server implementations.

Some of the people involved as the project has evolved

- Scott Battaglia
- Shawn Bayern
- Susan Bramhall
- Marc-Antoine Garrigue
- Howard Gilbert
- Dmitriy Kopylenko
- Arnaud Lesueur
- Drew Mazurek
- Jan Van der Velpen (Velpi)

Many CAS deployers

- Appian Corporation
- Athabasca University
- Azusa Pacific University
- BCcampus
- California Polytechnic Institute
- California State University, Chico
- Campus Crusade for Christ
- Case Western Reserve University
- Columbia
- Employers Direct
- GET-INT
- Hong Kong University of Science and Technology
- Indiana
- Karlstad University, Sweden
- La Voz de Galicia, Spain
- Memorial University of Newfoundland
- Nagoya University
- NHMCCD
- Northern Arizona University
- Plymouth State University (used with SunGardHE Luminis)
- Roskilde University
- Rutgers, The State University of New Jersey
- SunGard HE Luminis
- Simon Fraser University (Vancouver, B.C.)
- Suffield Academy
- Tollpost Globe AS

… and more

- Universita degli Studi di Parma
- Universite de Bourgogne - France
- Universite de La Rochelle, France
- Universite de Pau et des Pays de l'Adour, France
- University of Nancy 1, France
- Universite Nancy 2, France
- Universite Pantheon Sorbonne
- Universiteit van Amsterdam
- University of Bristol, England
- University of California Merced
- University of California, Riverside
- University of Crete, Greece
- University of Delaware
- University of Geneva
- University of Hawaii
- University of New Mexico
- University of Rennes1
- University of Technology, Sydney
- Uppsala University
- Valtech
- Virginia Tech
- Yale University

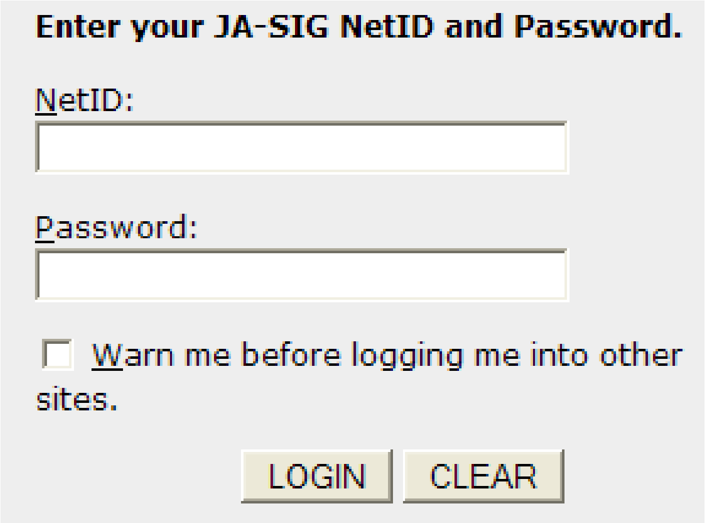
- And likely more not well-enumerated…

CAS and Commercial

- CAS is embedded in at least two commercial products
- CAS support is baked into at least one hardware platform (a wireless Internet vending appliance)
- Commercial entities use CAS the their SSO

Reprise: What is CAS?

- CAS is enterprise single-sign-on for the web.
  - Free
  - Open source
  - Server implemented in Java
  - Clients implemented in a plethora of languages



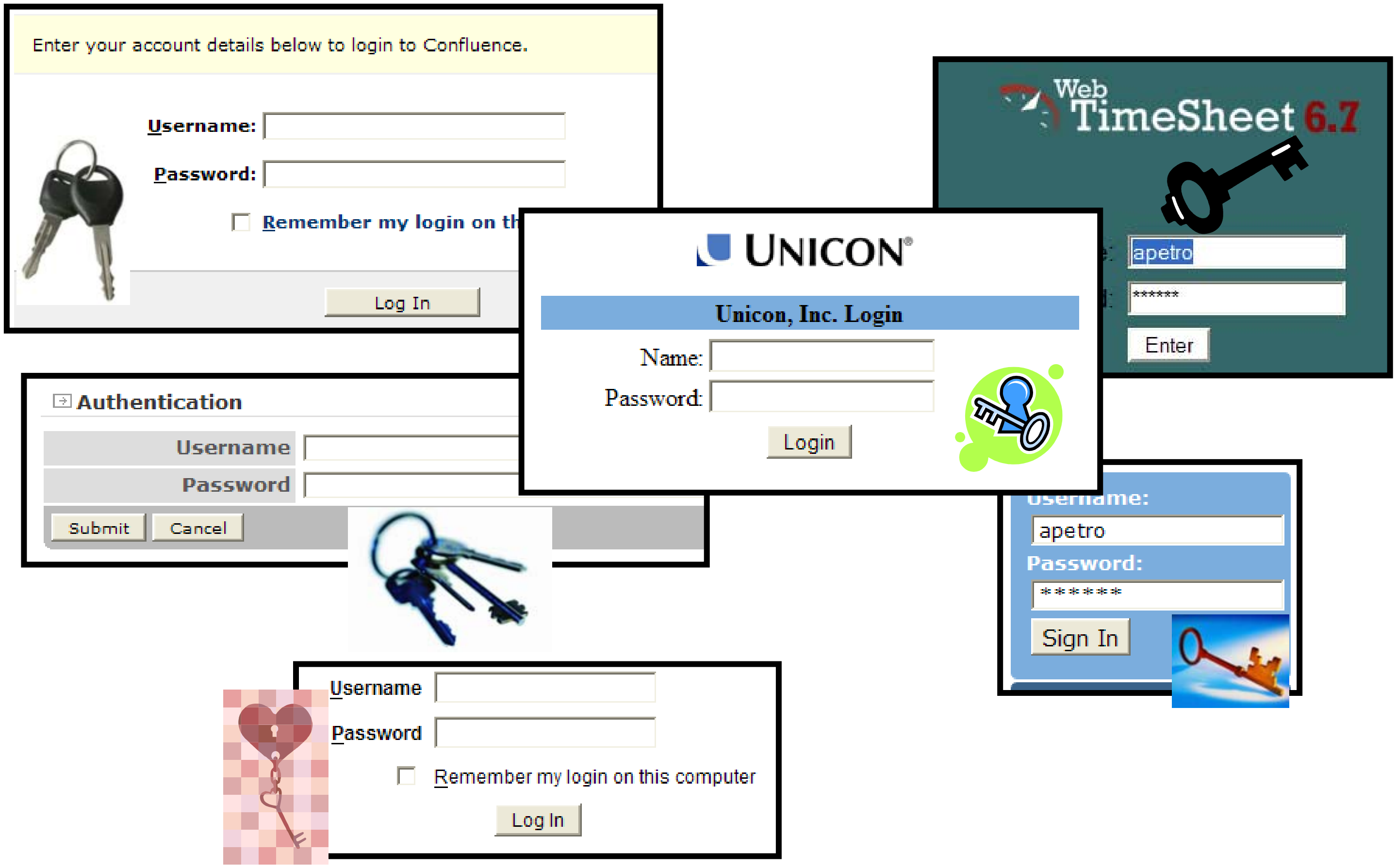
Enter your JA-SIG NetID and Password.

NetID:

Password:

□ Warn me before logging me into other sites.

Multi-sign-on for the Web



Enter your account details below to login to Confluence.

Username:

Password:

□ Remember my login on th

Log In

Web TimeSheet 6.7

e: apetro

d: ******

Enter

UNICON®

Unicon, Inc. Login

Name:

Password:

Login

Authentication

Username

Password

Submit Cancel

Username:

apetro

Password:

******

Sign In

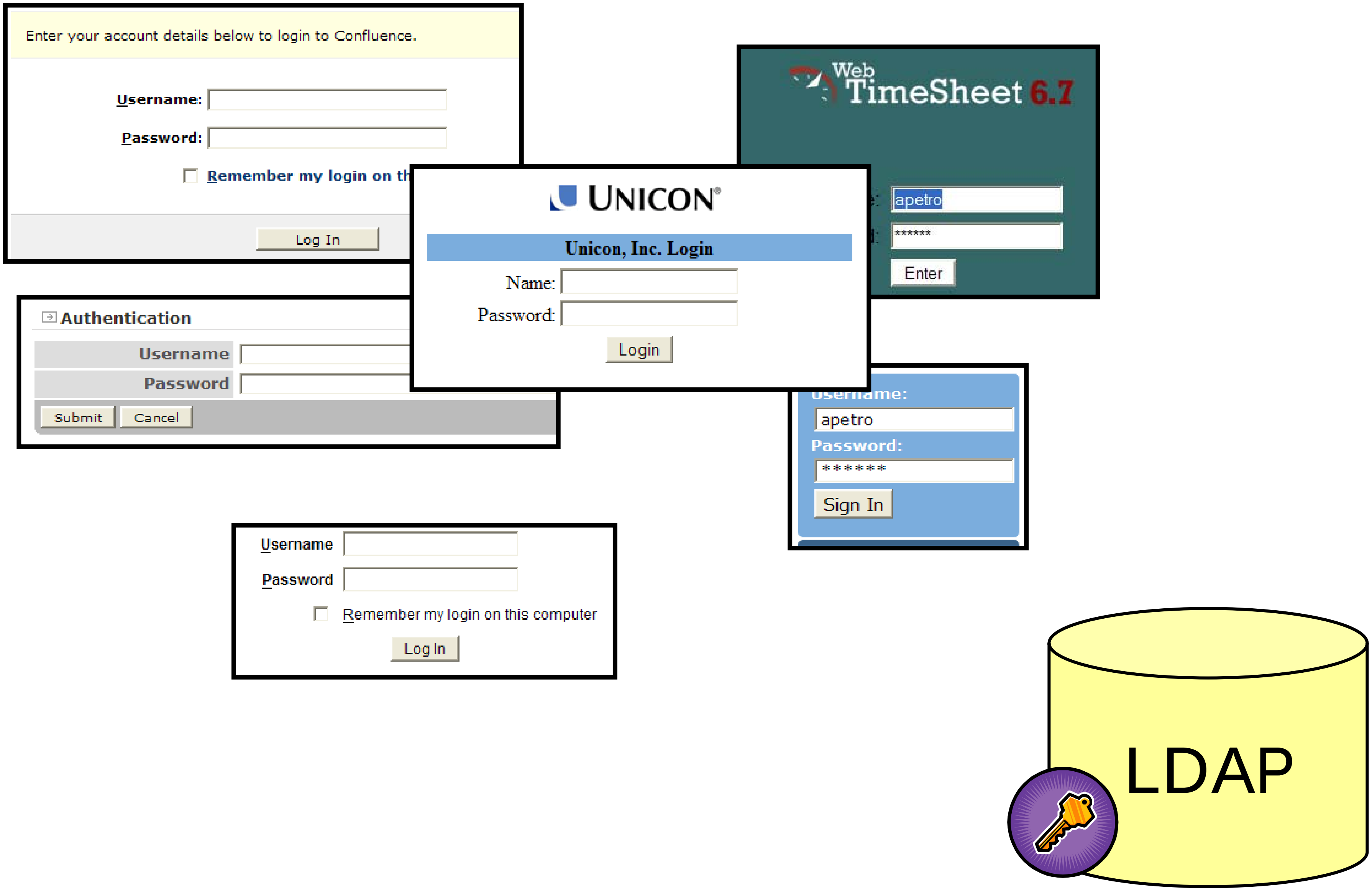
Username

Password

□ Remember my login on this computer

Log In

At least with one username/password?



Enter your account details below to login to Confluence.

Username:

Password:

☐ Remember my login on th

Log In

Authentication

Username

Password

Submit Cancel

Username

Password

☐ Remember my login on this computer

Log In

UNICON

Unicon, Inc. Login

Name:

Password:

Login

Web TimeSheet 6.7

e: apetro

d: ******

Enter

Username:

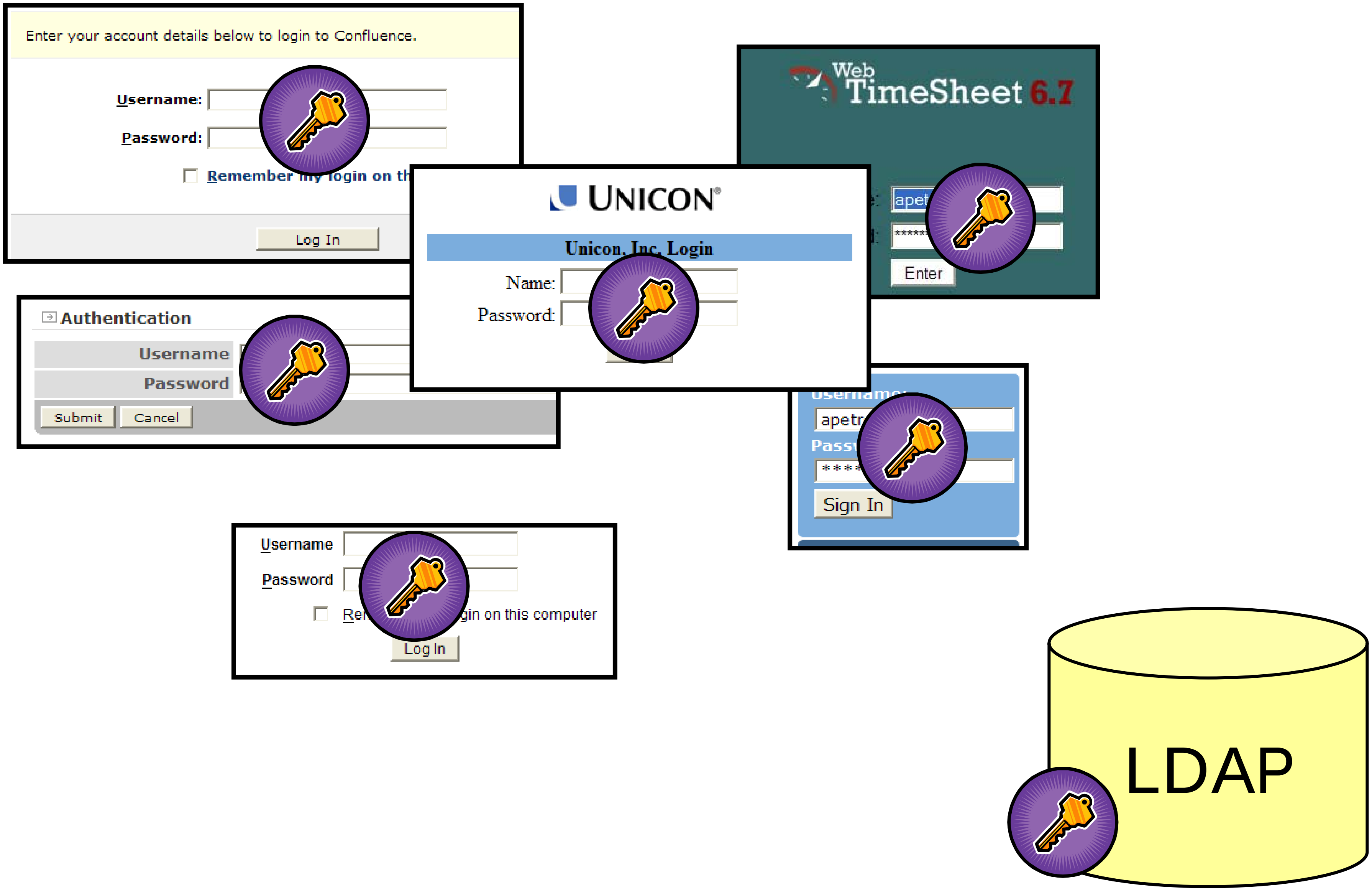
apetro

Password:

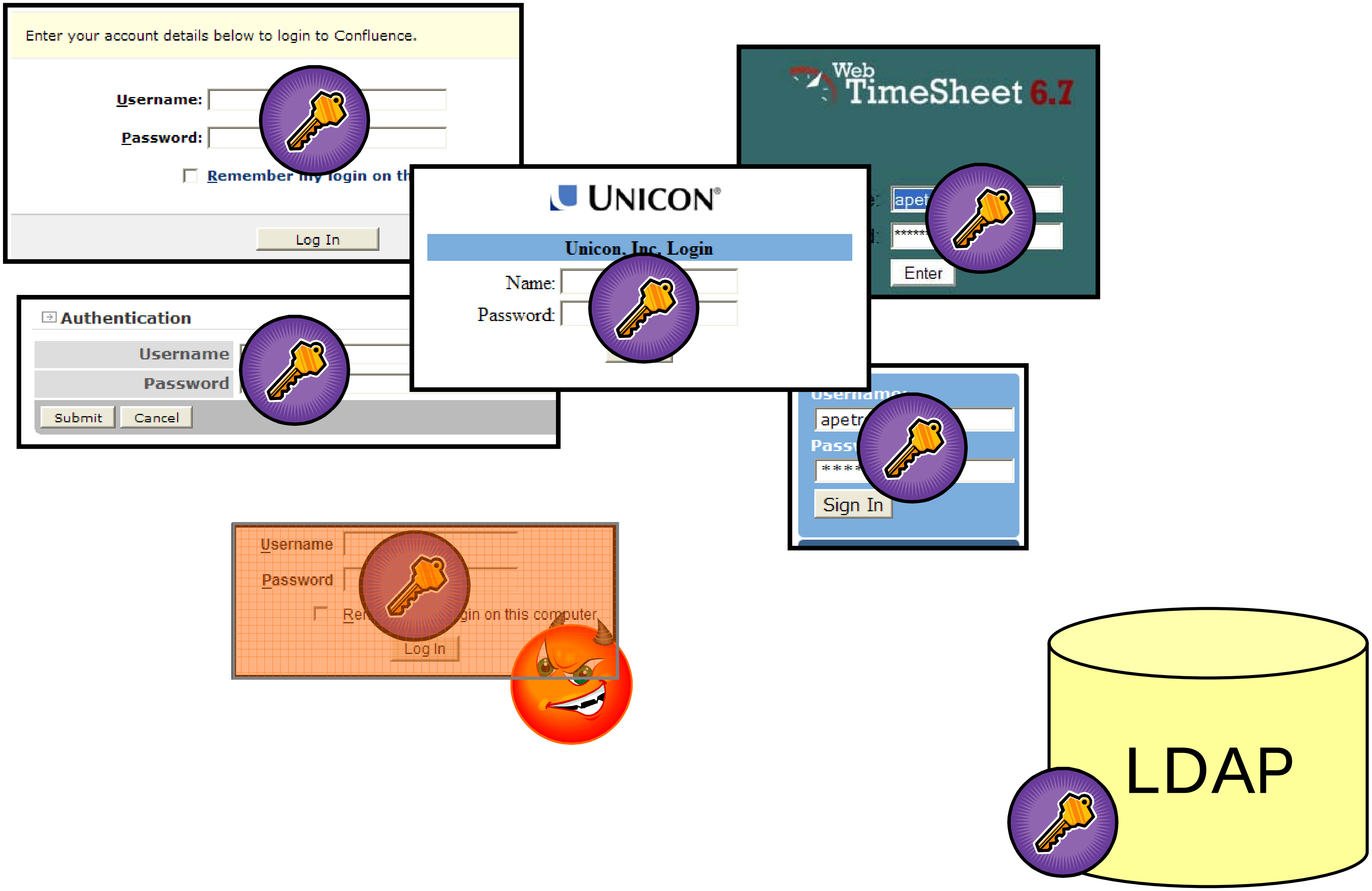
******

Sign In

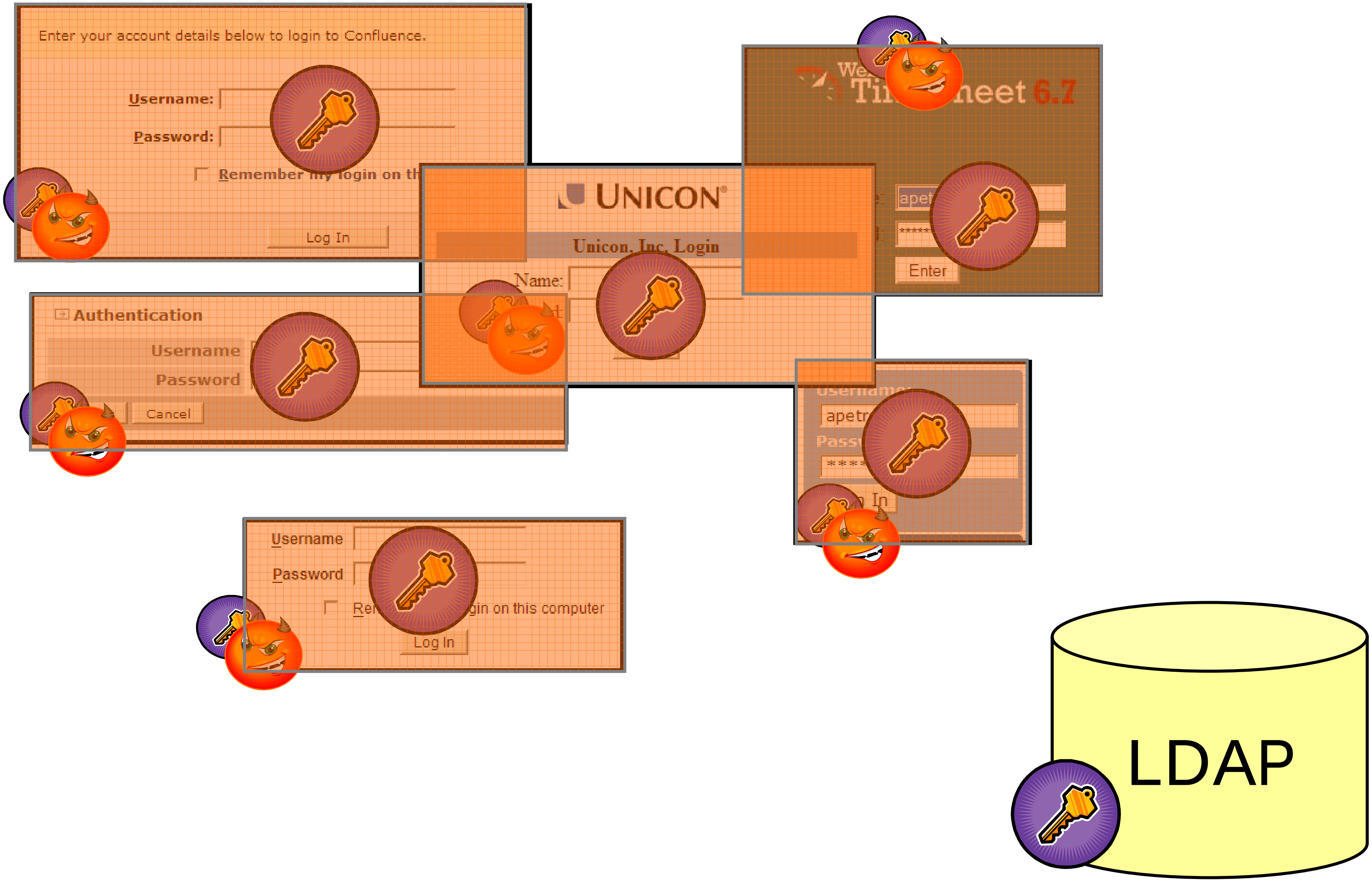
All applications touch passwords



Any compromise leaks primary credentials



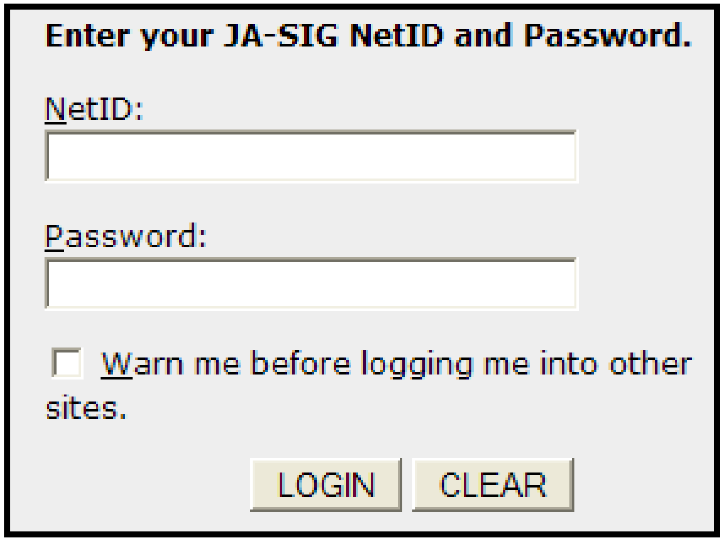
Adversary then can run wild



Enter your account details below to login to Confluence.

What to do about this?

- What if there were only one login form, only one application trusted to touch primary credentials?



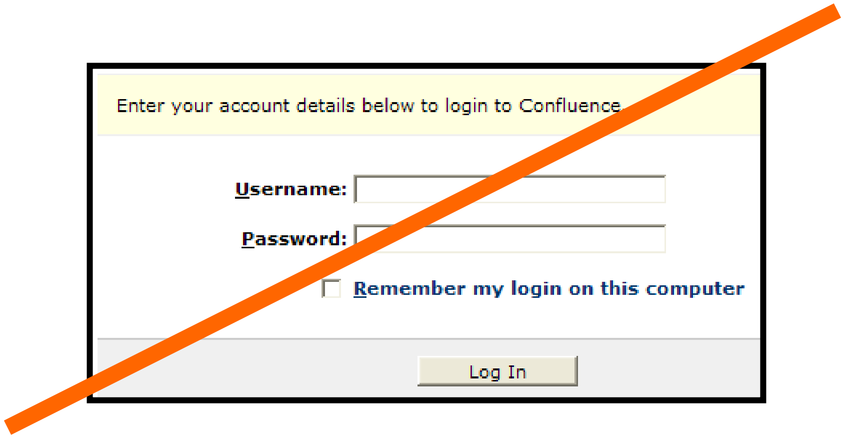
Enter your JA-SIG NetID and Password.

NetID:

Password:

□ Warn me before logging me into other sites.

Delete your login forms.



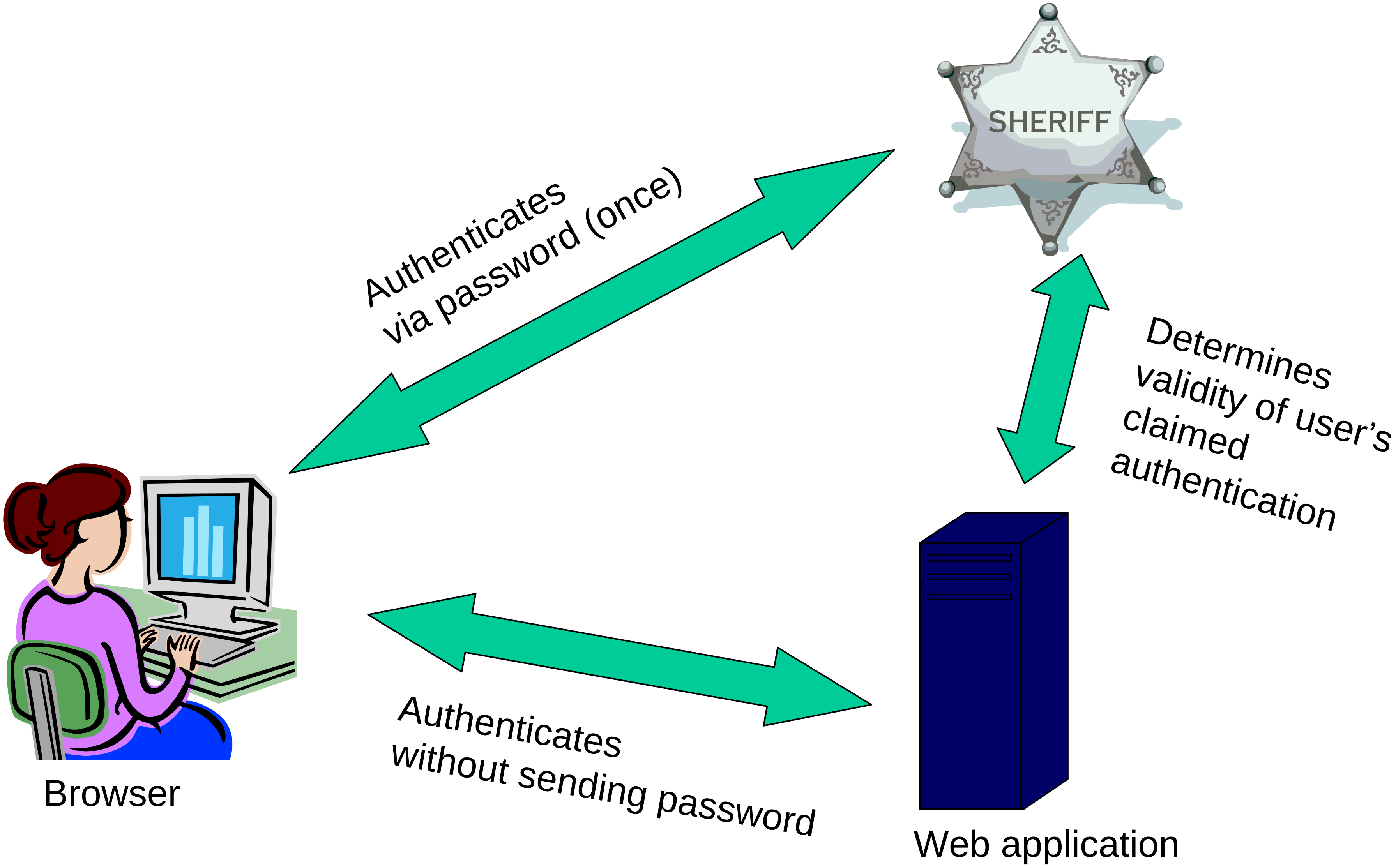
Enter your account details below to login to Confluence

Username:

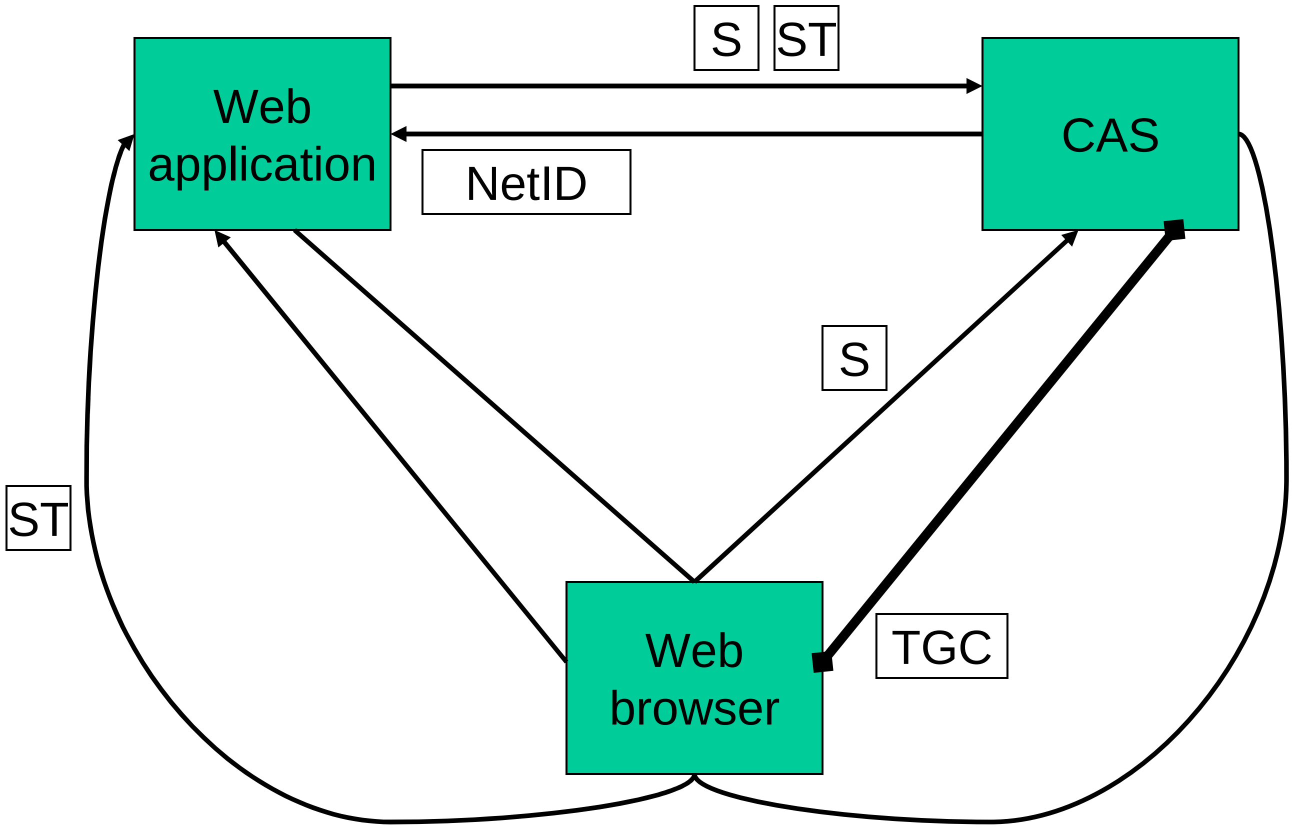
Password:

□ Remember my login on this computer

CAS in a nutshell



How CAS works



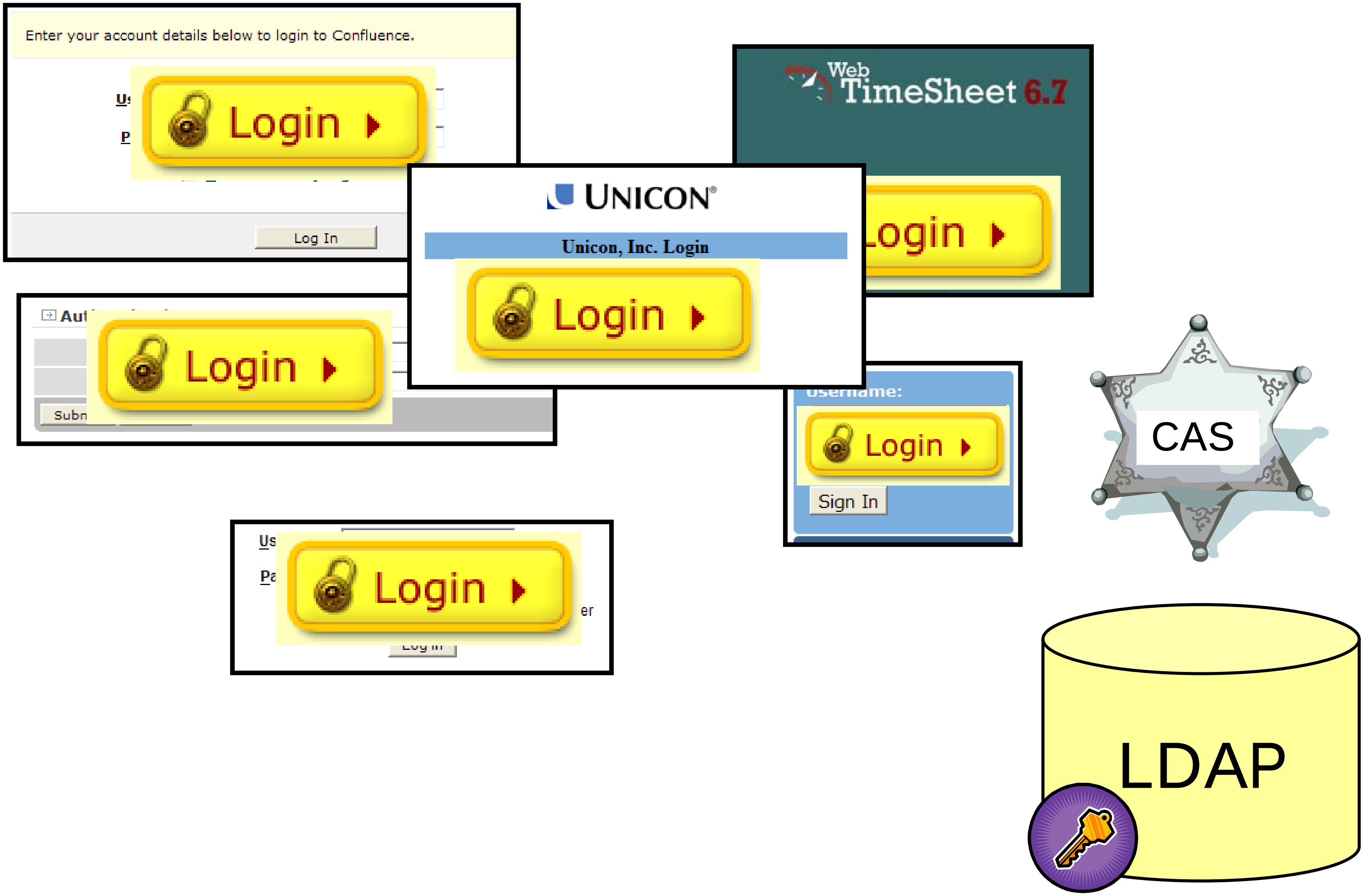
Why must the application present S to CAS on ticket validation?

- Anyone?

Why must the application present S to CAS on ticket validation?

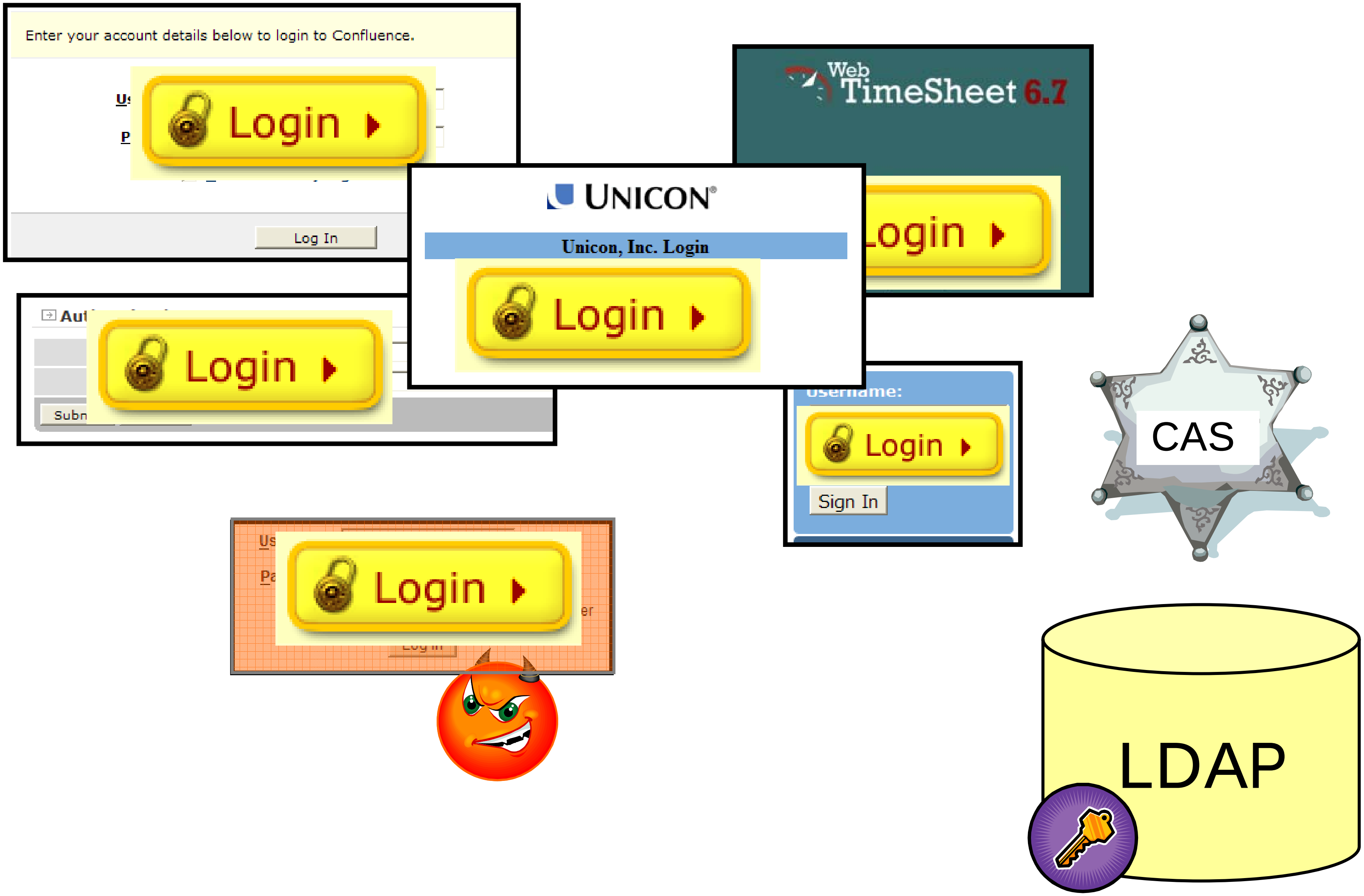
- CAS verifying that you’re validating a ticket for the service you think you’re validating it for prevents illicit proxying of service tickets.

Webapps no longer touch passwords

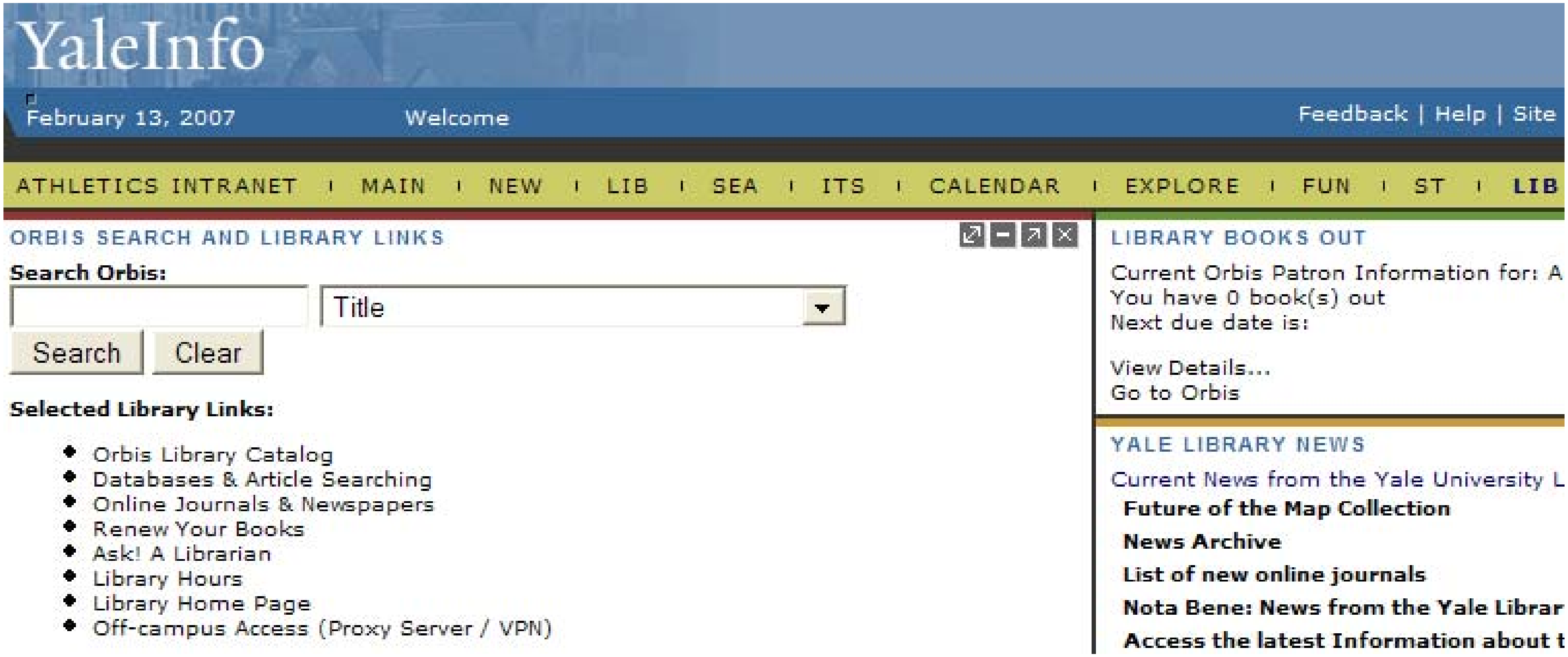


Enter your account details below to login to Confluence.

Adversary compromises only single apps



What about portals?


YaleInfo
Feedback | Help | Site
ATHLETICS INTRANET | MAIN | NEW | LIB | SEA | ITS | CALENDAR | EXPLORE | FUN | ST | LIB
Title
Search
Clear

February 13, 2007

Welcome

ORBIS SEARCH AND LIBRARY LINKS

Search Orbis:

Selected Library Links:

- Orbis Library Catalog
- Databases & Article Searching
- Online Journals & Newspapers
- Renew Your Books
- Ask! A Librarian
- Library Hours
- Library Home Page
- Off-campus Access (Proxy Server / VPN)

LIBRARY BOOKS OUT

Current Orbis Patron Information for: A
You have 0 book(s) out
Next due date is:

View Details...
Go to Orbis

YALE LIBRARY NEWS

Current News from the Yale University L

Future of the Map Collection

News Archive

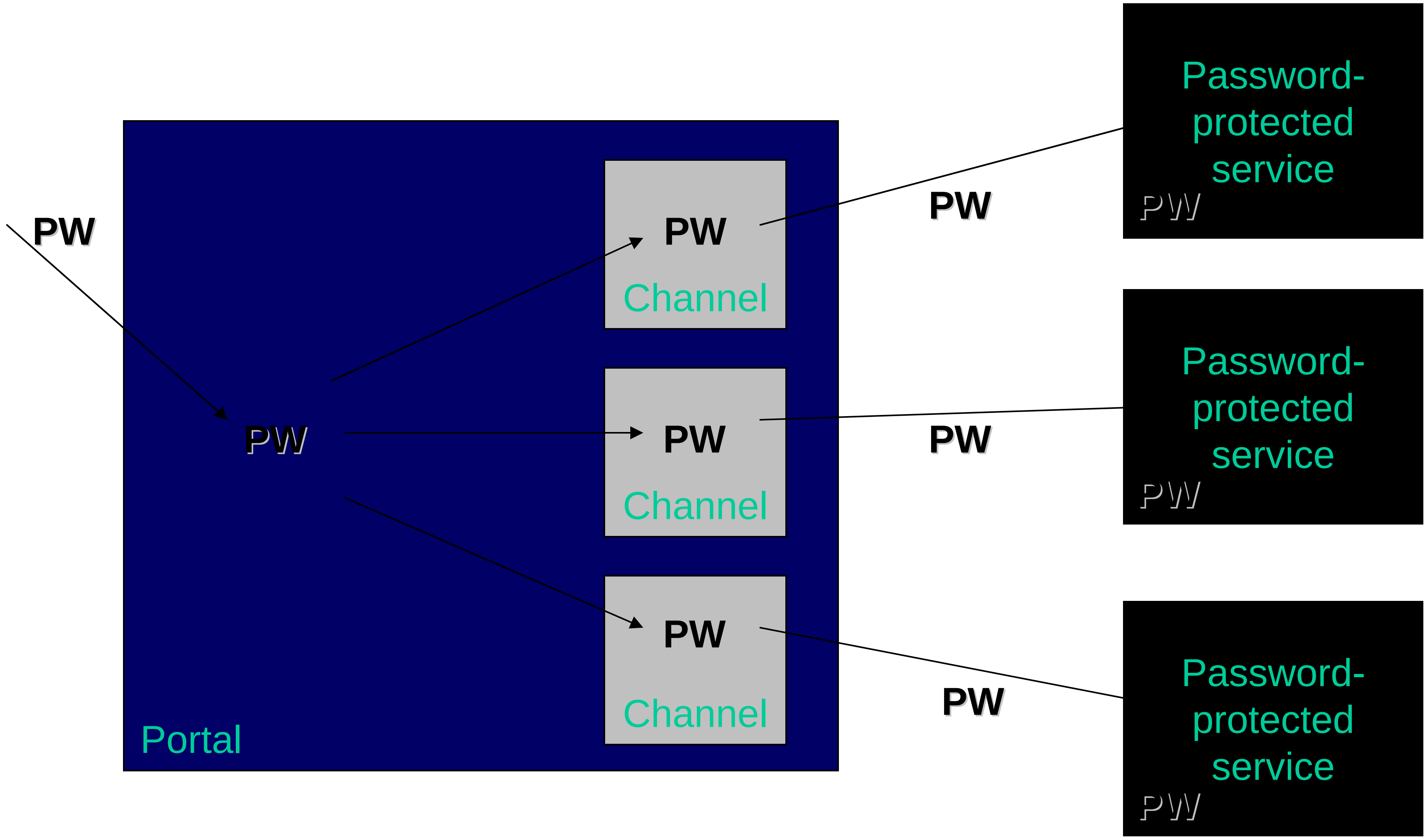
List of new online journals

Nota Bene: News from the Yale Librar

Access the latest Information about t

Need to go get interesting content from different systems.

Password replay

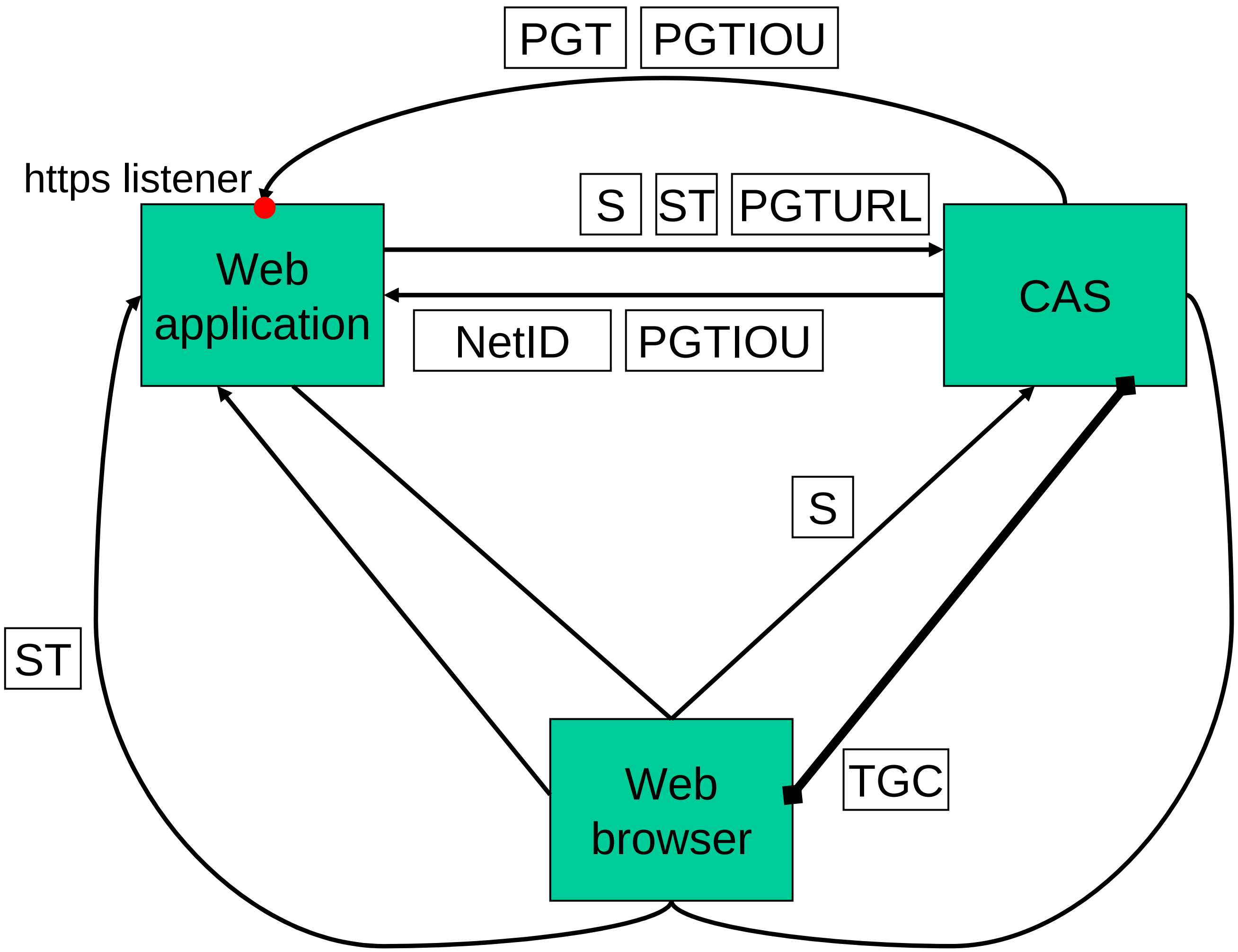


PW
PW
Portal
PW
Channel
PW
Channel
PW
Channel
PW
PW
PW
Password-protected service
PW
Password-protected service
PW
Password-protected service
PW

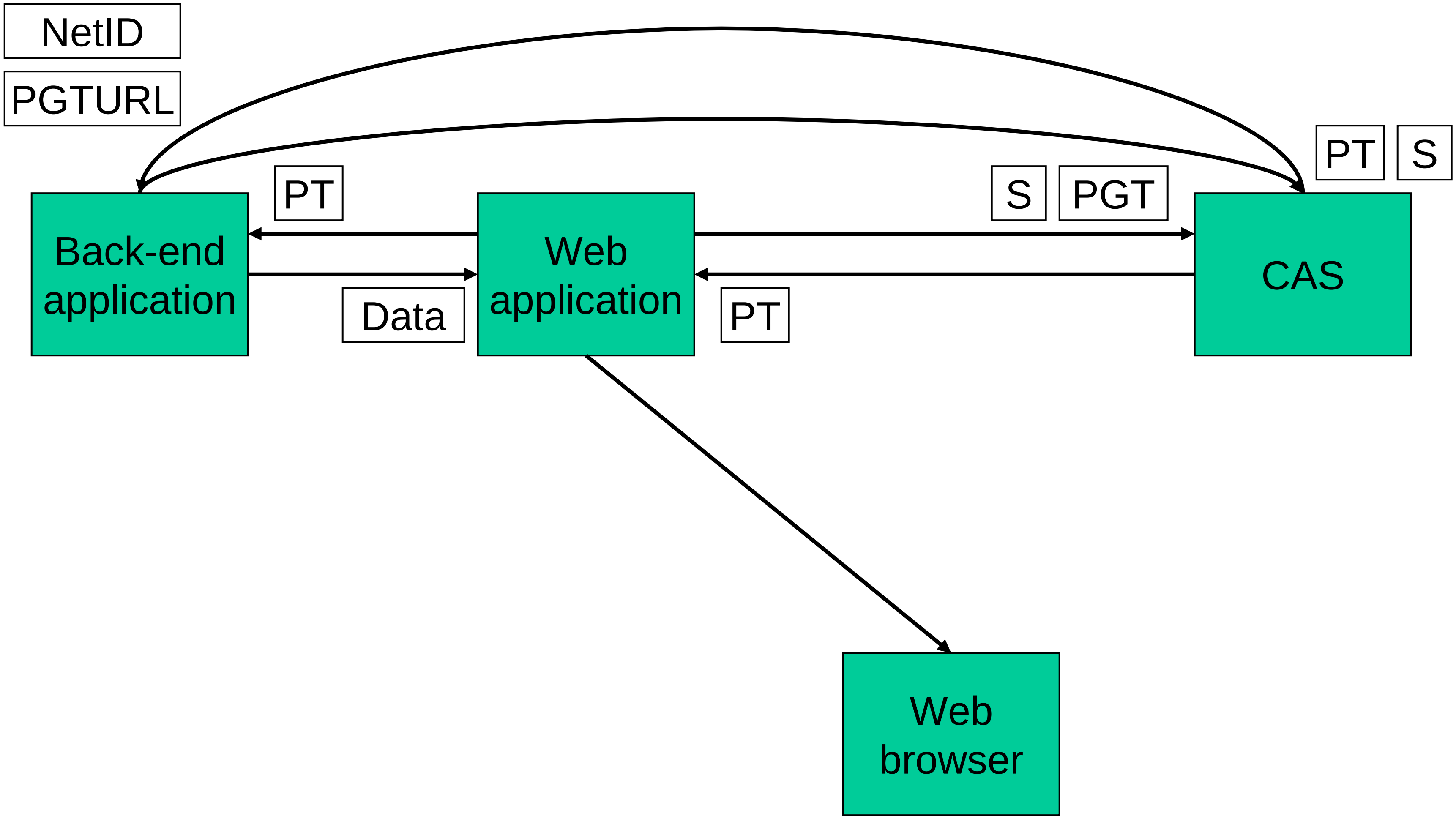
Look ma, no password!

- Without a password to replay, how am I going to authenticate my portal to other applications?

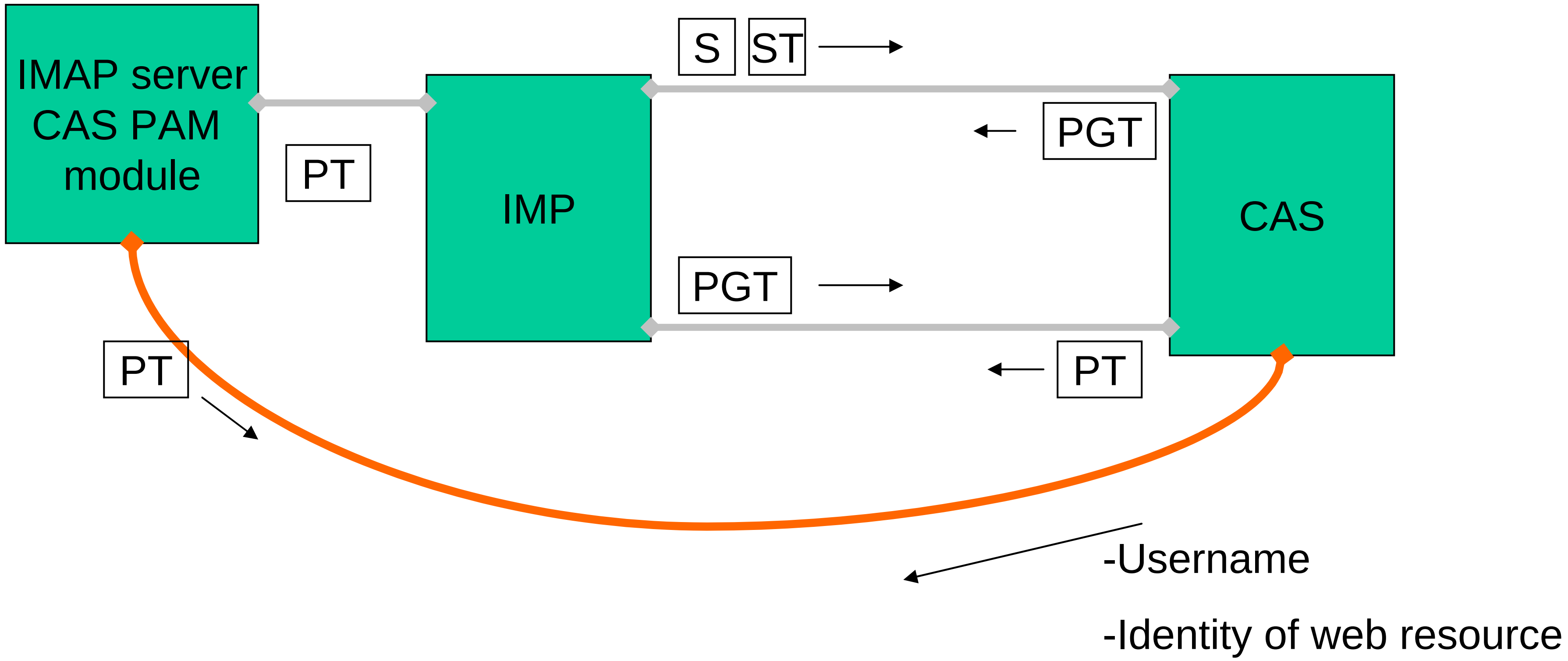
CAS 2.0: Proxy CAS



CAS 2.0: Proxy CAS



Proxiable credentials illustrated



Provided authentication handlers

- LDAP
  - Fast bind
  - Search and bind
- Active Directory
  - LDAP
  - Kerberos (JAAS)
- JAAS
- JDBC
- RADIUS
- SPNEGO
- Trusted
- X.509 certificates
- Writing a custom authentication handler is easy

Today CAS is not only for authentication

- Return attributes of logged on users
- Adding support for standards
  - OpenID
  - SAML
- Single Sing-Out
- Support for clustering
  - Implements distributed ticket registry
  - Requires session replication
  - Must guarantee cross-server ticket uniqueness
- Services management (white listing)
- Remember me

Features under consideration

- Multi-factor authentication
- Expired password integration
- Passing user agent attributes back as user attributes (browser IP, authentication type, CAS language setting)
- Which AuthenticationHandler(s) to use for specific registered service?
- Second-level authentication

Questions?

Adam Rybicki

arybicki@unicon.net

www.unicon.net

UNICON®