



Identity Management and Joining the AAF

Presented at IdM Workshop
19th August 2008

Viviani Paz, AAF Project Manager, AusCERT
aaf@aaf.edu.au

 Australian Government
Department of Innovation, Industry, Science and Research

 aaf australian access
federation

Content



- HE & Research State of Play
- AAF Overview
- What do Universities need to do?
- Conclusion

  Copyright © 2007 AusCERT 2  

HE & Research State of Play

HE & Research State of Play

- Increase in the number of phishing attacks on universities.



© Scott Adams, Inc./Dist. by UFS, Inc.

HE & Research State of Play – Recent spear-phishing developments

Spear phishers target US students

By Shaun Nichols
5 February 2008 03:25PM
Security

A new spear phishing attack is targeting the email accounts of US university students.

Researchers at [Sans Institute](#) said that the attacks are disguised as messages from administrators performing a 'database update'.

The messages state that in order to keep their email accounts, the students must 'verify' the accounts by replying to the message with details such as user names, passwords and date of birth.

Researcher Mark Hofman wrote in the [Internet Storm Center blog](#) that the attacks are similar to those on European ISPs spotted earlier this year.

The attackers use email addresses with the name of the school, although the accounts are hosted by an external email service such as Hotmail.

Hofman noted that, because the attack targets individual students, few messages are sent and the emails will often slip past spam filters.

Administrators should be on the lookout for a large volume of incoming messages from the same address, as well as a large volume of messages with multiple recipients. Students should also be warned about the attacks.



HE & Research State of Play – Recent spear-phishing developments

What's Inside

[About Us](#)

[OIT News](#)

[Finance](#)

[Human Resources](#)

[OIT Security](#)

[Planning](#)

[Policies](#)

[Projects](#)

[Contact Us](#)

Search

Related Links

[1-HELP](#)

[System Status](#)



OFFICE OF INFORMATION TECHNOLOGY

Spear phishing attack at the University

Date: February 6, 2008

To: University students, staff, and faculty
From: Steve Cawley, Vice President and Chief Information Officer
Subject: Spear phishing attack at the University

You already know not to open e-mail claiming to be from eBay or PayPal, but what if the e-mail is sent from someone you know or an organization you are a member of and is addressed to you by name?

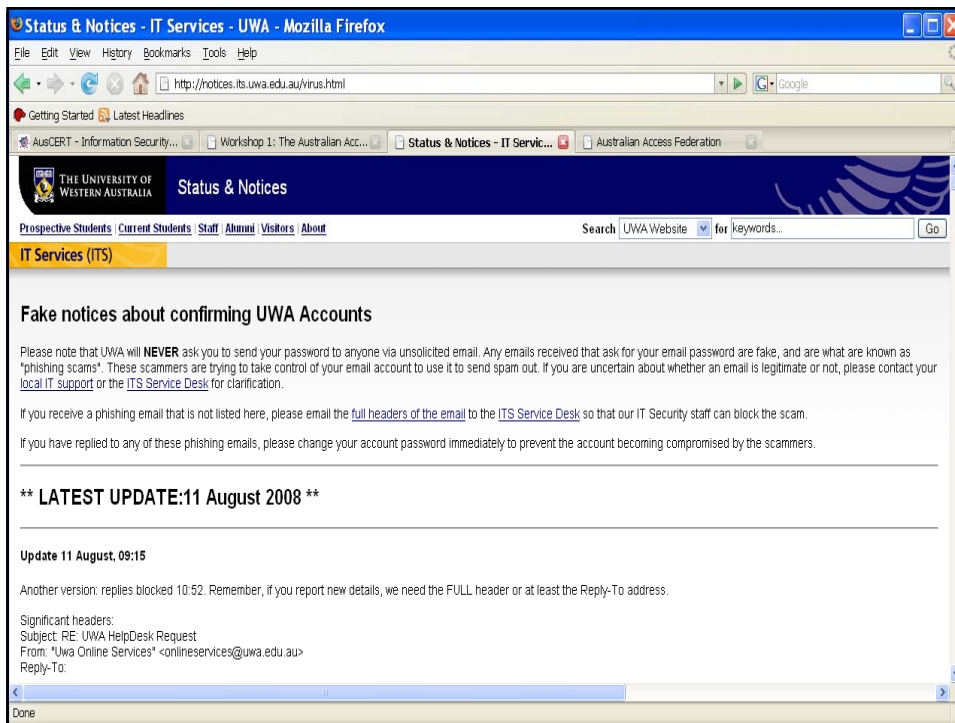
It's unfortunate, but there is a nasty new form of an e-mail scam called "spear phishing." In a spear phishing scam, the message can seem genuine because it appears to come from a legitimate source—like your employer or university. Spear phishing attacks can take many different forms, but the one thing they have in common is that they ask for sensitive information such as passwords, birth dates, social security numbers, etc. The most important thing to know is that you should never share personal information over e-mail.

Over the past week there have been reports of spear phishing attacks at higher education institutions, including the University of Minnesota. Last week, a few U of M recipients replied to spear phishing attacks and shared personal information with attackers. One of the recent spear phishing e-mails that has targeted U of M says something like:

"VERIFY YOUR UMN (OR EMAIL) ACCOUNT NOW." The e-mail appears to be sent from a umn.edu address, and the recipient is asked to verify their e-mail address and e-mail password.

The University will never ask you for your password in e-mail.






HE & Research State of Play

australian access federation

What can universities do to minimise this threat?

- Educate users
- Use digitally signed emails
- Use stronger authentication to student records, HR systems, financial systems



Government funding

- Increasingly, expensive research infrastructure is a joint enterprise of multiple research institutions
 - e.g., LIEF-funded equipment or facilities under NCRIS
- Access to the infrastructure itself, or to data from it, is typically restricted to researchers from a defined collection of research institutions
- Research collaboration at distance

- Privacy and legal environment is changing
 - Privacy Policy Review
 - Contractual obligations
- Increase in online access
 - Students enrolments and obtaining results
 - Learning and service delivery to geographically dispersed audience
- Increase in cross-institutional enrolments
- Increase in the number of overseas students
- Increase of electronic services that support sensitive and critical data


Educause Top-Ten IT Issues, 2008

- By Debra H. Allison, Peter B. DeBlois, and the 2008 EDUCAUSE Current Issues Committee
- <http://connect.educause.edu/Library/EDUCAUSE+Review/TopTenITIssues2008/46605>



- | | |
|--|---|
| 1. Security | 7. Governance, Organization, and Leadership |
| 2. Administrative/ERP/ Information Systems | 8. Change Management |
| 3. Funding IT | 9. E-Learning / Distributed Teaching and Learning |
| 4. Infrastructure | 10. Staffing / HR Management / Training |
| 5. Identity/Access Management | |
| 6. Disaster Recovery / Business Continuity | |



Identity and Access Management Survey, 2008

- Does your institution have a main directory for identity management that contains all staff, students, and affiliates?
 - 62% - Yes
- Does your institution proactively manage the currency of user accounts, disabling accounts when a user leaves the institution?
 - On-campus students – 84% - Yes
 - Off campus students – 84% - yes
 - Academic and general staff – 75% - Yes


 australian access federation

AAF overview



13


 australian access federation

What is the Australian Access Federation? (1)

Facilitator for trusted electronic communications and collaboration within and between institutions of higher education and research in Australia and other organizations worldwide





HEBCA



aaaf
australian access federation



haka



The UK Access Management Federation
FOR EDUCATION AND RESEARCH



InCommon®



SWITCHaai



FEIDE



Gatekeeper®

What is the Australian Access Federation? (2)



- Infrastructure built to support access to diverse online resources and services for the sector
 - Two technologies
 - PKI and Shibboleth
 - AusCERT Root Certificate in vendor's Trust Lists
 - Simplify the end user experience
 - Signed server certificates issued through the AAF
 - Microsoft, Mozilla, Apple



Copyright © 2007 AusCERT

15



PKI and the AAF



16



The use of PKI in the AAF

- Sound PKI is effective in increasing integrity, confidentiality and non-repudiation of information shared
 - PKI links entities, to cryptographic keys, through certificates, enabling scalable trust to a defined quality
 - PKI provides strong authentication mechanisms.
 - PKI certificates support the use and validation of digital signatures and encryption of documents and emails.
 - Server certificates can positively identify the organisation behind a web site and Shibboleth identity and service providers.

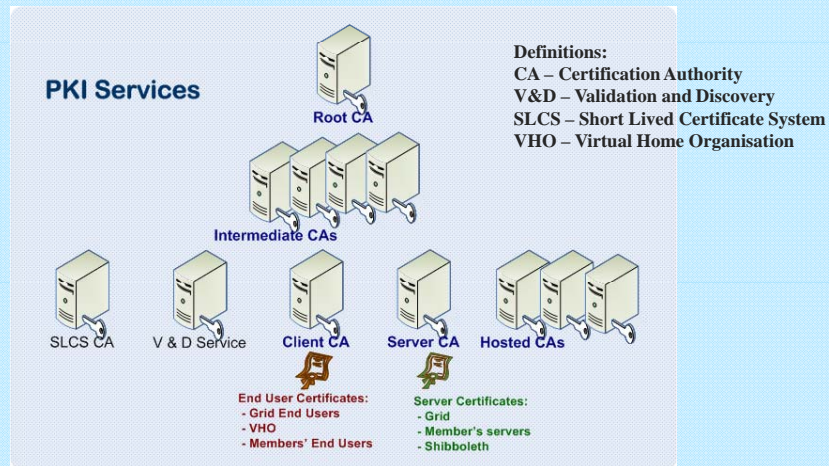


What can we use PKI Certificates for?

- Server and host security, i.e. SSL, TLS, VPN, etc
- Authentication
- Digital signing of documents/emails
- Encryption of documents/emails

AAF PKI Overview (1)

- AusCERT Root Certificate
 - In browsers: Microsoft, Mozilla, Apple



AAF PKI Overview (2)

- Server Certification Authority
 - Issues digital certificates to servers/hosts
 - University servers/hosts
 - Research (For Servers running Grid servers)
 - Shibboleth backchannel
- Client Certification Authority
 - Issues digital certificates to end users
 - Universities
 - Research (Grid)
 - Standard and Short lived certificates (SLCS)
 - Virtual Home Organisation individuals

What do Universities need to do? PKI



University Responsibilities (1)

- Sign AAF member agreement
- Assign a point of contact/official representative (I.e. IT Director)
- Provide access to email service and web browser to its staff/students
- Observe the 100 point check for identification of staff performing the Registration Authority Role
 - HR and Enrolment process may be sufficient
 - For example staff that has been with the university for over 3 years
- Fill in Registration Authority Officer form

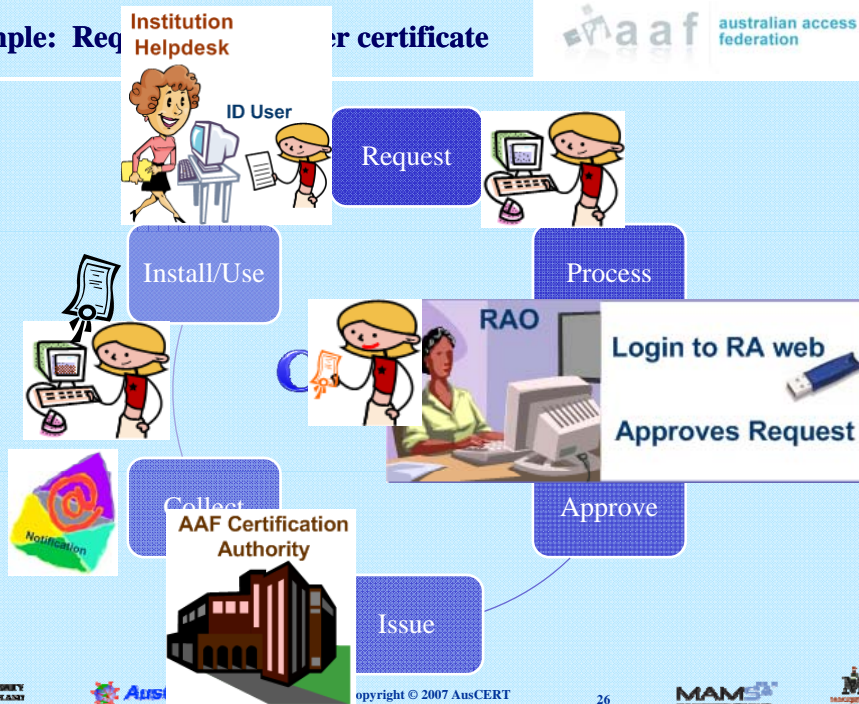


Register Authorised Personnel to request Certificates (2)

- RAO must be identified at member institution
- RAO registration form needs to be signed by OR and submitted to AAF Operator
- Following checks with OR, RAO will be issued with a certificate to be used to request certificates on behalf of its institution.



Example: Request for certificate



Example: Requesting End User certificate

aaaf australian access federation

THE UNIVERSITY OF QUEENSLAND AUSTRALIA

AusCERT

Copyright © 2007 AusCERT

27

MAMS MANAGEMENT AND MONITORING SYSTEMS

MAQUINARIA

Summary

aaaf australian access federation

- AAF is breaking new ground!
- Lessons learned from other federations and tackling issues early
 - integrated PKI/Shibboleth, framework for assurance levels, structured to allow evolution
- People are getting behind the AAF: Grid, WGs, SC, DIISR, trials (SharedToken)
- Input requested and received from community
- Environment is changing, the AAF will help you respond
 - addressing real needs
- Pilots completed now building production infrastructure

THE UNIVERSITY OF QUEENSLAND AUSTRALIA

AusCERT

Copyright © 2007 AusCERT

28

MAMS MANAGEMENT AND MONITORING SYSTEMS

MAQUINARIA

Conclusion

- AAF is designed to ensure a continued focus on the community it serves, so you join with confidence
- AAF will facilitate easier access to technology and a streamlined framework for collaboration and access to resources
- You can be involved right now and start preparing
- Timeframe
 - To commence operations by the end of 2008
 - Institutions and service providers to join progressively during 2009
- More information: <http://www.aaf.edu.au>



Discussion.....

www.aaf.edu.au

 a a f australian access
federation

Queries/Comments: aaf@aaf.edu.au