Network Attacks

Common Network Attacks and Exploits

AGENDA

- A Few Observations
- Hacker Resources
- Attack Categories
- Some Common Attacks
- Wireless Specific Attacks

Observations

- Because of Common Network Layers, Most of the Attacks in the Wired network will also Work against Wireless Clients
- Because of the nature of Radio, Locating a Hacker, a Rogue Access, or an Infected machine that is on wireless can be difficult
- Because of the nature of Radio, Preventing Access or Attacks can be difficult
- Rogue AP’s and Rogue DHCP Servers Are Common Problems, but not necessarily malicious attacks
- Managing Access Points is Critical

Attack Categories

- DOS Attacks
  - Denial of Service (Hard to Prevent, But These Draw Immediate Attention To The Attacker)
  - Example: Flooding Attacks, Disassociation Attacks
- Disclosure Attacks
  - Reading/Revealing Information
  - Example: MITM Attacks
- Modification Attacks
  - Changing Information
  - Example: We just modified your HomePage!
- Destructive Attacks
- Escalation of Privilege

Attack Categories

- “Network Security Architectures” p.65
  - Sniffing: password grabbing
  - Brute Force: password attempts
  - Buffer Overflows: httpd, ftpd, rpc/dcom
  - Spoofing Attacks: forging IP/MAC/Etc.
  - Flooding: SYN, UDP, ICMP Flooding
  - Redirection: using ICMP, ARP, STP, MITM Attacks
  - Anti-Virus: Worms, Viruses, Trojans
  - Masquerading
  - Social Engineering

Network Attacks

- We’ll Look at Some of These In Detail Later

Hacker Resources

- Conferences
    - Blackhat:
        - http://www.blackhat.com/html/bh-media-archives/bh-archives-2007.html
    - DefCon:
        - https://www.defcon.org/html/links/dc-archives.html
    - ShmooCon:
        - http://www.shmoocon.org/2007/presentations.html
- Magazines
    - Hakin9:
        - http://hakin9.org/prt/view/pdf-articles.html
    - 2600, The Hacker Quarterly
        - http://www.2600.com/

Hacker Resources

- WebSites
  - http://insecure.org/
    - The Home of NTOP
  - packetstorm.offensive-security.com
  - http://wirelessdefence.org/
    - The Home of AIRCRACK-NG
  - http://80211.ninja.net
    - AirJack/WlanJack
  - The Websites in the Network Security Lecture!

Attacks In Detail

- Eavesdropping Attacks
  - -- get MAC Address
  - -- get IP Address
  - -- get BaseStation Address
  - -- sniff cleartext passwords and keys
  - -- crack password hashes
  - -- crack wep keys
  - -- get SSIDs

Attacks In Detail

- DOS -- Denial of Service Attacks
- -- Radio Signal Interference
- -- AP Interference, example: steal MAC, steal IP
- -- Channel Hogging
- -- Disassociation Attacks
- -- Flooding Packets
- -- ARP Poising
- -- RST Packets
- -- Window Size Changes
- -- UDP Flooding
- -- ICMP Flooding
- -- BROADCAST Flooding

Attacks In Detail

- -- Masquerade Attacks
    - Pretending that You are Someone Else!
    - -- MAC Address Spoofing
    - -- IP/MAC Address Spoofing
    - -- DNS Attacks
    - -- WPAD Web Proxy Hi-Jacking
    - -- Website Spoofing
    - -- Portal Spoofing

Attacks in Detail

- -- Social Engineering Attacks

- -- Phishing URLs, Type your Password Here
- -- E-mail Scams
- -- Telephone Scams
- -- Cell Phone SMS Scams

- Examples:
    - A Fake Version of the University of Oregon Account Login Page
    - SMS Phone Messages, saying: “Call This Number At Once About Your Bank Account!”

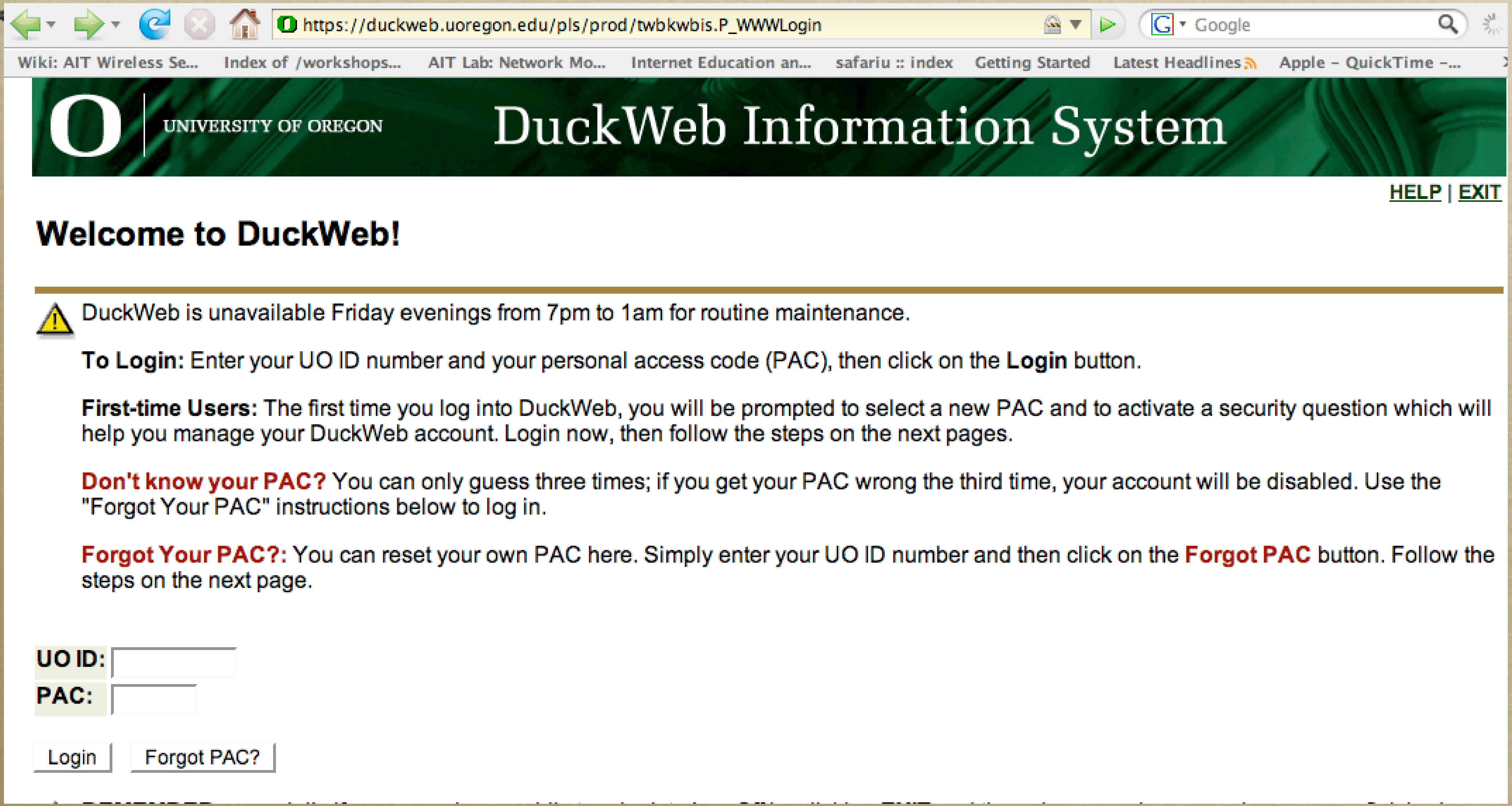
Common Attacks

- So What Kind of Attacks are We Seeing?
  - Phishing Attacks, E-mail and Phone SMS
  - XSS - Cross-Site-Scripting Attacks
  - SQL Insertion Attacks
  - PHP File Include Attacks
  - Buffer Overflows
  - P2P File Sharing Attacks
  - Botnets
  - SPAM Mail Relays

Common Attacks

- Phishing at the University of Oregon
  - E-mail sent to 1000’s of users pointing to a Fake Version of the University of Oregon Account Login Page, “Please Change your Account Information Immediately”
  - SMS Phone Messages, saying: “Call This Number At Once About Your Bank Account!”

Here's the Real Website



Welcome to DuckWeb!

⚠ DuckWeb is unavailable Friday evenings from 7pm to 1am for routine maintenance.

To Login: Enter your UO ID number and your personal access code (PAC), then click on the **Login** button.

First-time Users: The first time you log into DuckWeb, you will be prompted to select a new PAC and to activate a security question which will help you manage your DuckWeb account. Login now, then follow the steps on the next pages.

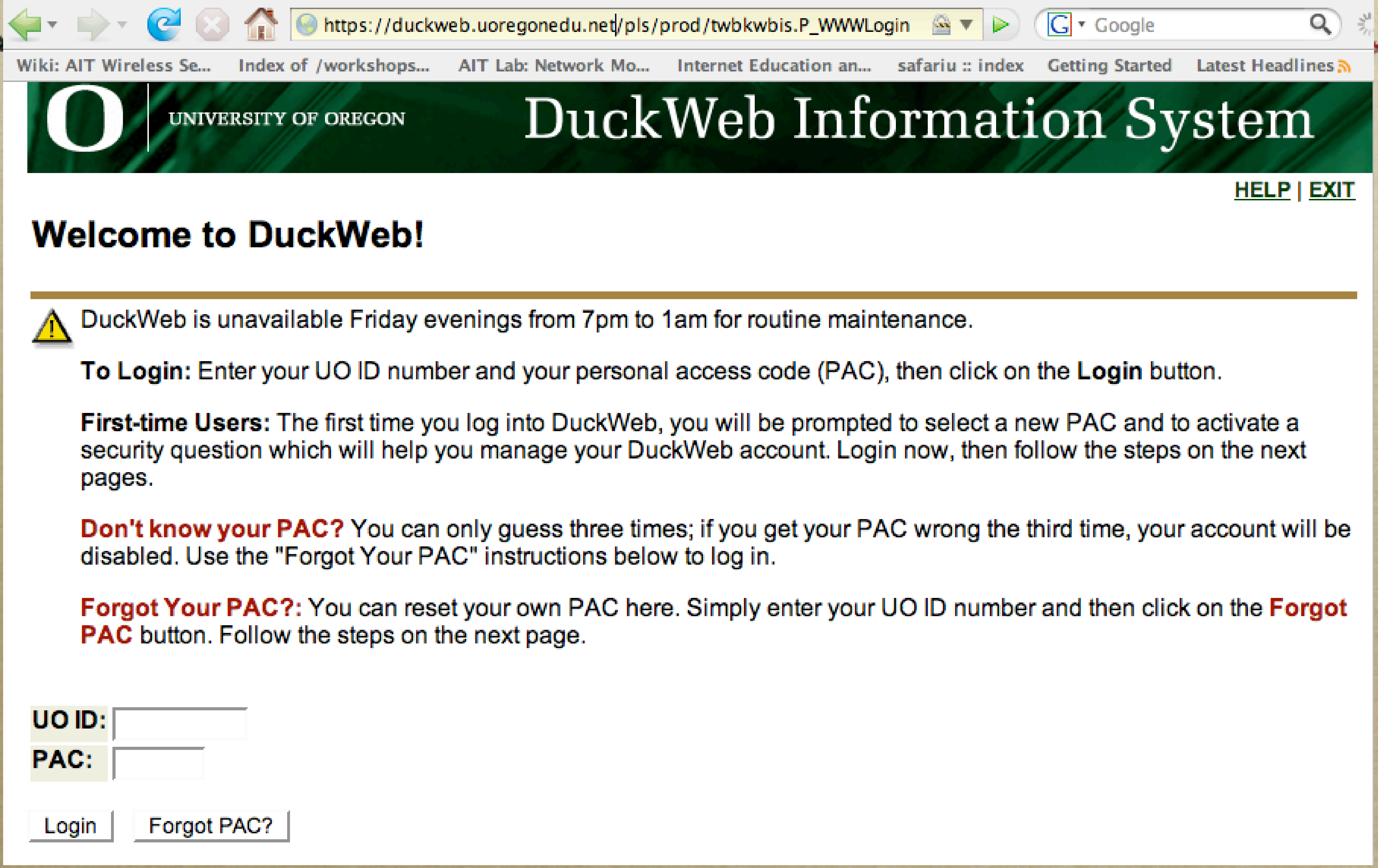
Don't know your PAC? You can only guess three times; if you get your PAC wrong the third time, your account will be disabled. Use the "Forgot Your PAC" instructions below to log in.

Forgot Your PAC?: You can reset your own PAC here. Simply enter your UO ID number and then click on the **Forgot PAC** button. Follow the steps on the next page.

UO ID:

PAC:

Here's The Phishing Website



Welcome to DuckWeb!

DuckWeb is unavailable Friday evenings from 7pm to 1am for routine maintenance.

To Login: Enter your UO ID number and your personal access code (PAC), then click on the **Login** button.

First-time Users: The first time you log into DuckWeb, you will be prompted to select a new PAC and to activate a security question which will help you manage your DuckWeb account. Login now, then follow the steps on the next pages.

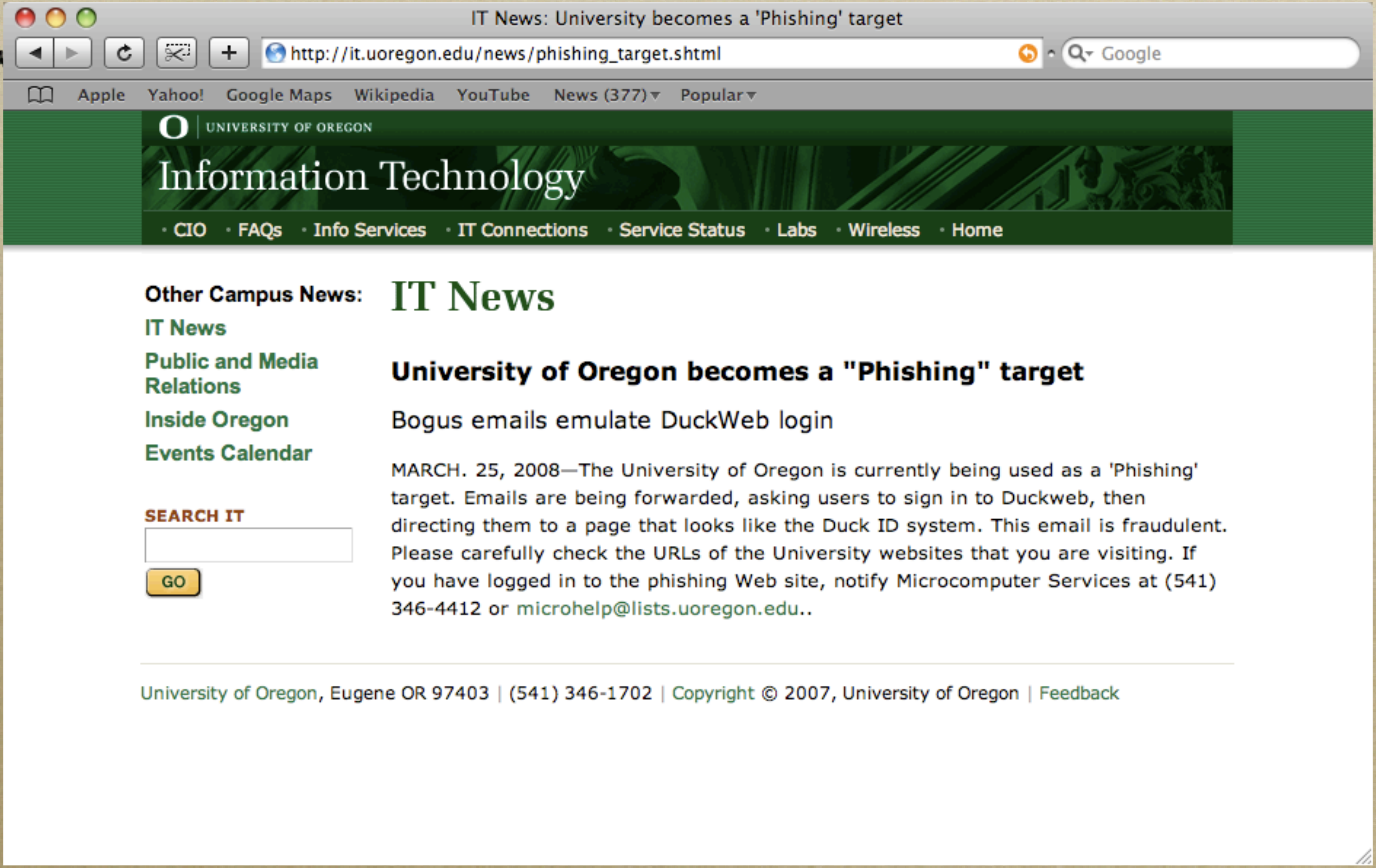
Don't know your PAC? You can only guess three times; if you get your PAC wrong the third time, your account will be disabled. Use the "Forgot Your PAC" instructions below to log in.

Forgot Your PAC?: You can reset your own PAC here. Simply enter your UO ID number and then click on the **Forgot PAC** button. Follow the steps on the next page.

UO ID:

PAC:

Attacks In Detail



IT News

University of Oregon becomes a "Phishing" target

Bogus emails emulate DuckWeb login

MARCH. 25, 2008—The University of Oregon is currently being used as a 'Phishing' target. Emails are being forwarded, asking users to sign in to Duckweb, then directing them to a page that looks like the Duck ID system. This email is fraudulent. Please carefully check the URLs of the University websites that you are visiting. If you have logged in to the phishing Web site, notify Microcomputer Services at (541) 346-4412 or microhelp@lists.uoregon.edu..

University of Oregon, Eugene OR 97403 | (541) 346-1702 | Copyright © 2007, University of Oregon | Feedback

Attack Details

- I just got an SMS E-mail From My Bank!?!

Layer 2 Attacks

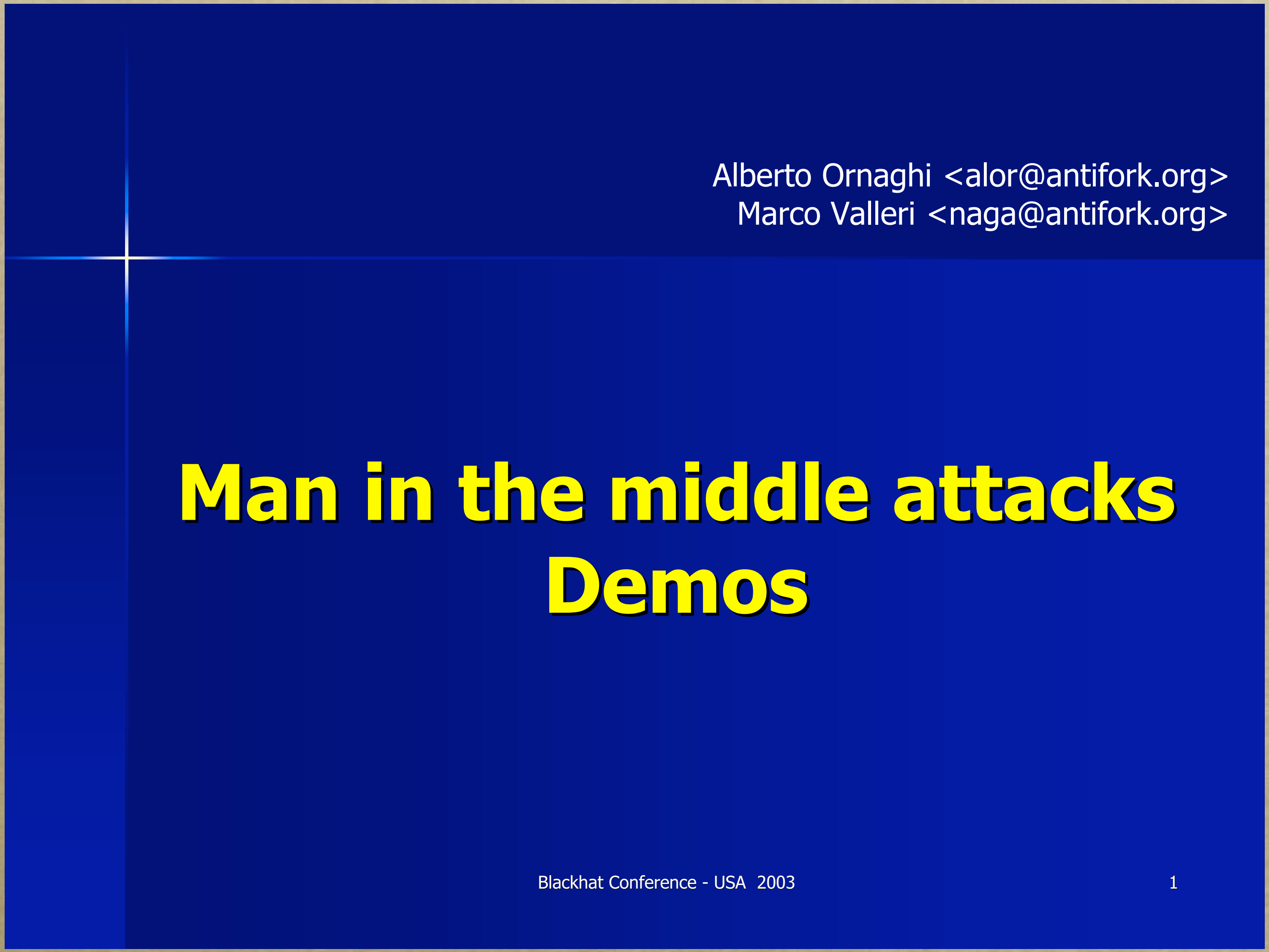
- ARP Poisoning
  - Send an ARP with Forged MAC Address

MITM Attacks

- Man-in-the-Middle Attacks
  - Usually a combination of more than one type of attack at once
  - Can involve ARP Poisoning, ARP Masquerading, and Forwarding
  - Can also include Masquerading as a Website, as an SSL Website, or an SSH Host

MITM Attacks

- See Also: Ettercap Authors, BlackHat 2003



Alberto Ornaghi <alor@antifork.org>
Marco Valleri <naga@antifork.org>

Man in the middle attacks
Demos

Blackhat Conference - USA 2003

1

MITM

- Step 1: Get the Victim Talking To You
- Step 2: Get the Target Talking To You
- Step 3: Sniff the Traffic and Forward the Packets You receive on Each Side

- Sometimes the goal is just to sniff traffic.
- Other times, the goal is to Masquerade as a real service, and capture username/password credentials

MITM

- There Are Tools that Do All of This For You
  - dsniff
    - arpspoof
    - sshmitm
    - webmitm
  - ettercap
    - it’s built for this, with extra bells as well
    - we will try this in our lab
  - Windows: Cain & Abel
    - A Windows Version MITM Tool

AIRCRACK

- Active Development Going On Here
- Tools for Cracking WEP, LEAP, Etc.
- Generalized Tools for Packet Forgery
- Multiple Tools
  - Aircrack, Airodump, Aireplay, Airdecap

AirCrack

Airodump

Captures the Initialization Vectors (IV) of WEP Keys

IVs are fed to Aircrack for WEP Key cracking

```
% airodump wlan0 capture1 10 (Interface=wlan0, filename=capture1, channel=10)
% airodump eth1 testfile 6 1 (Interface=eth1, filename=testfile, channel=6, only captured IVs saved)
% airodump ath0 alpha 0 (Interface=ath0, filename=alpha, channel hopping mode)
```

Aircrack

Using input from Airodump, crack WEP keys

```
% aircrack -a 1  -n 64 capture1-01.cap
% aircrack -q -b 00:06:25:BF:46:06  -n 128 -f 4 testfile-01.cap
% aircrack -a 2  -w  passwords.txt  capture1-01.ca
```

AirCrack

Aireplay

- Disassociate Clients/APs to discover SSID
- Capture with Airodump during attack
- Requires 1 Disassocation Packet to get SSID
- Can also Produce WPA Handshake Capture

```
% airodump [interface] [filename] [channel]
% aireplay -0 1 -a 11:11:11:11:11:11 -c 22:22:22:22:22:22 [interface]
% aireplay -0 15 -a 11:11:11:11:11:11 -c 22:22:22:22:22:22 [interface]
```

Airedecap

- Decrypt WEP data file captures
- Decrypt WPA data file captures

```
% airdecap -w  866578388f517be0b4818a0db1  WEP-capture-01.cap
% airdecap -e cuckoo -p sausages wpa-test.cap
```

Arpforge

AP Attacks

- Attacking the Lower Layer of the AP Association
- This is the Layer Underneath the MAC Layer
- Sending “Disassociate” Frames to the Client
- These are called “Radio Managment Frames”
- This is part of the WEP Key Attacks
- We’ll do this in our Lab using % aireplay
- See also: % void11, % airjack, % wlanjack