CryoSe
WORCESTER, WR4 9RH ·
0280/02
HELLO
my name is

Øyvind Skaar

March 12, 2009

oyvs@ifi.uio.no

http://folk.uio.no/oyvs

(not much here..)

http://odots.org

(not here either)

UNIVERSITAS OSLOENSIS

MDCCCXI

UNIK

Overview

- Security in online games
  - Online Games?
  - Motivation
  - Why cheat or “hack” games
  - Security problems in games
  - Protecting your games

Overview

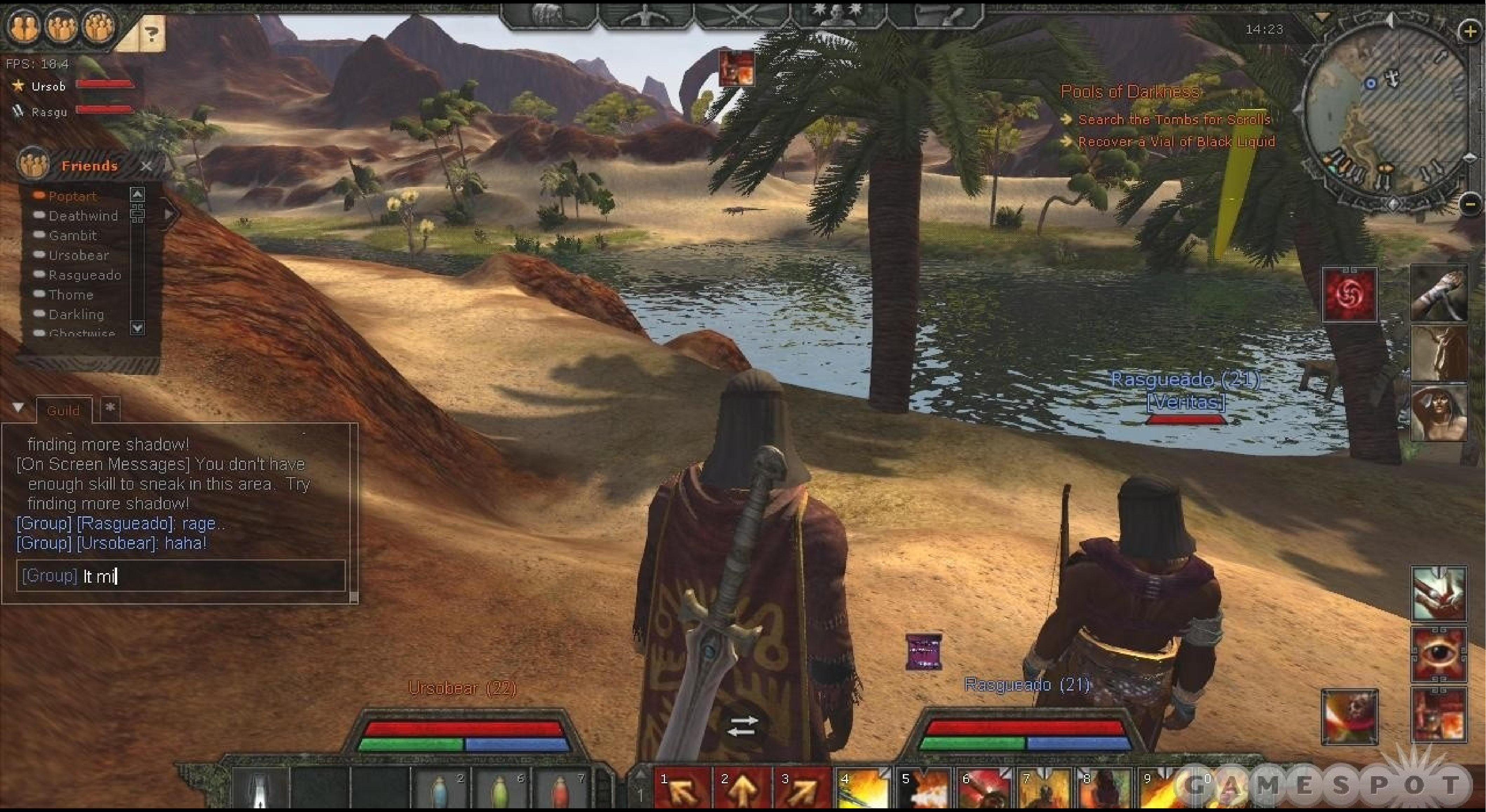
- Trusted Computing
  - The Trusted Computing Group
  - Promises
  - Can the TPM fix gamesecurity?
  - TPM Problems

Online games?

- MMO:
  - Massively multiplayer online game
  - Online: As oppose to playing by them self “against” the computer, the players interact with each other.
  - Massively multiplayer: Large number of players the same virtual “world”. In most MMO's a couple of thousand players at a time is nomal, but Eve Online peaked at 51,675.

Online games?

Almost always characters interacting in a 3D world of some sort



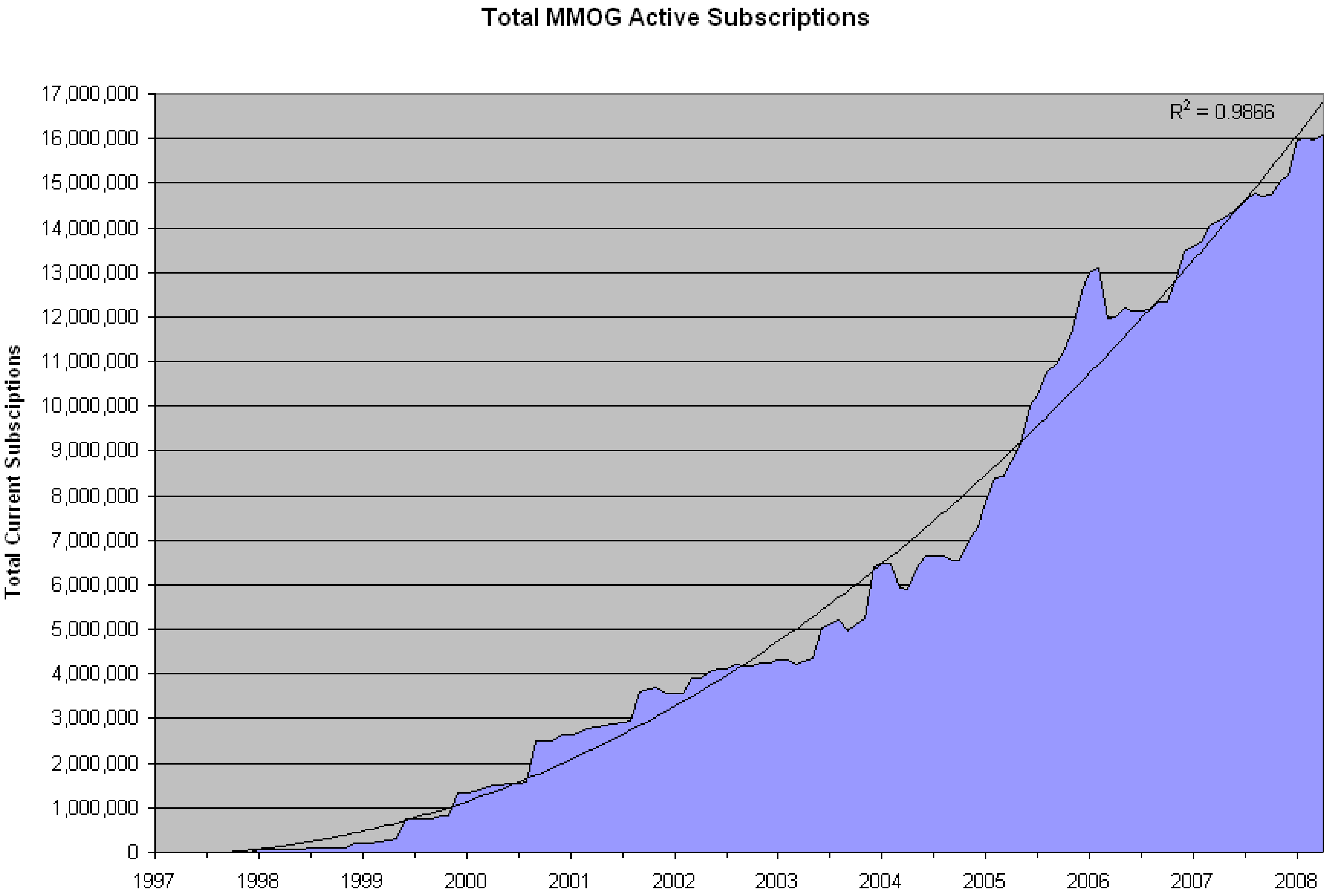
finding more shadow!
[On Screen Messages] You don't have enough skill to sneak in this area. Try finding more shadow!
[Group] [Rasgueado]: rage..
[Group] [Ursobear]: haha!

[Group] It mi

Age of Conan: http://www.ageofconan.com/

Motivation

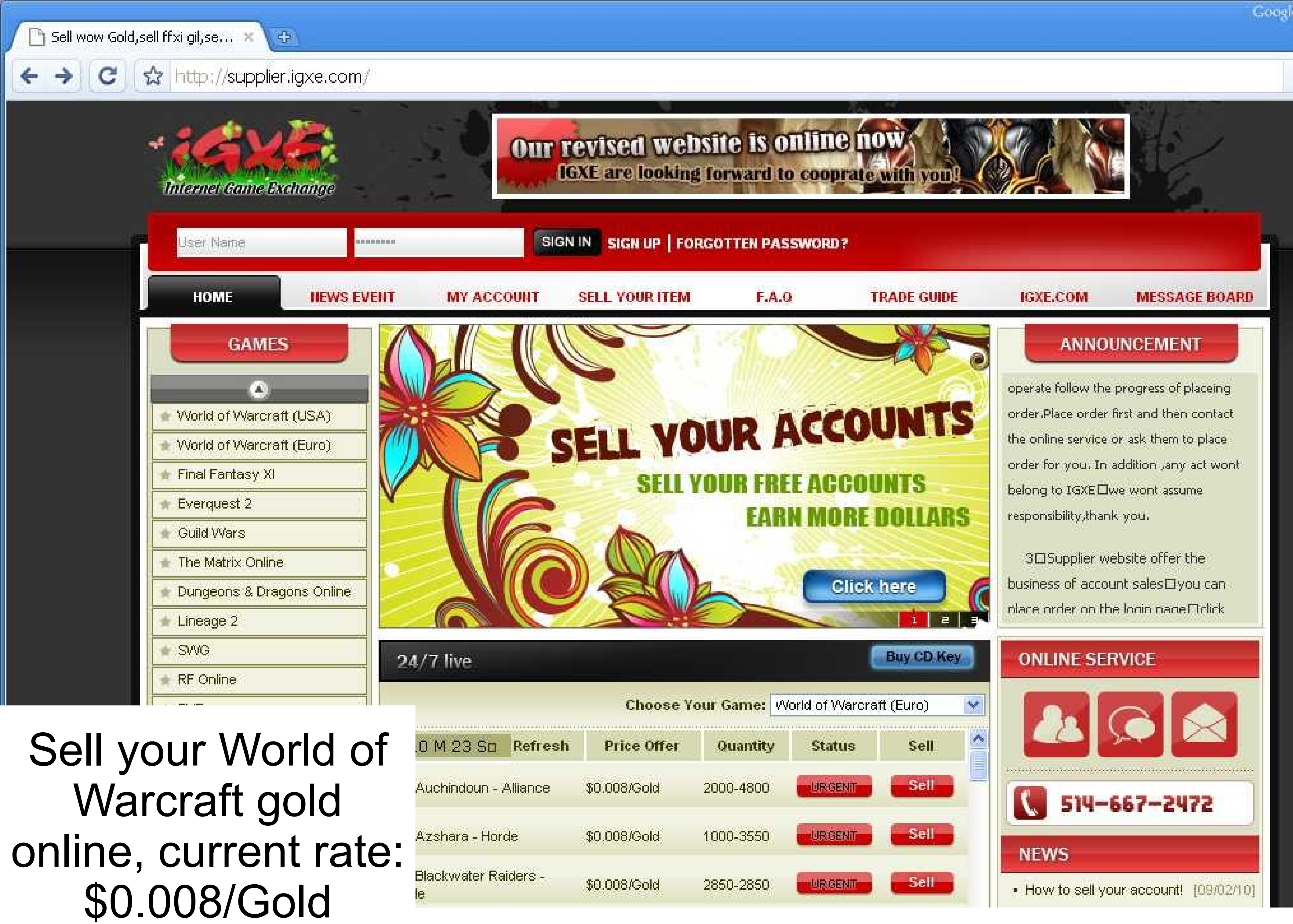
- Complex, online, massively distributed systems
  - Some estimate ~400 000 people playing World of Warcraft at any given time!
  - How do you share the state of the virtual world?
  - Complicated programs, fat clients
- Gaming is big business
  - World of Warcraft alone have at least 10 million subscribers worldwide, paying either by the hour or a monthly fee.
- Related to online gambling / betting / poker
- Fresh topic, games are fun :)



http://www.mmogchart.com

Why cheat or “hack” games

- Challenging, fun(?), get ahead, avoid boring tasks
- For money
  - Virtual money, gold and items can be exchanged into “real” money.
  - Strategy: Find a bug, duplicate game money, convert to dollars
  - “The wealth in some MMO worlds are greater than some small “real” countries” (Hoglund)
  - IGE one of the largest middlemarkeds for virtual items. They made about 400 million dollars in 2006 (McGraw).



Sell wow Gold,sell ffxi gil,se...

http://supplier.igxe.com/

iGXE Internet Game Exchange

Our revised website is online now

IGXE are looking forward to cooprate with you!

User Name | SIGN IN | SIGN UP | FORGOTTEN PASSWORD?

HOME | NEWS EVENT | MY ACCOUNT | SELL YOUR ITEM | F.A.Q | TRADE GUIDE | IGXE.COM | MESSAGE BOARD

GAMES

- World of Warcraft (USA)
- World of Warcraft (Euro)
- Final Fantasy XI
- Everquest 2
- Guild Wars
- The Matrix Online
- Dungeons & Dragons Online
- Lineage 2
- SWG
- RF Online

SELL YOUR ACCOUNTS

SELL YOUR FREE ACCOUNTS

EARN MORE DOLLARS

Click here

1 2 3

ANNOUNCEMENT

operate follow the progress of placeing order.Place order first and then contact the online service or ask them to place order for you. In addition ,any act wont belong to IGXE□we wont assume responsibility,thank you.

3□Supplier website offer the business of account sales□you can place order on the login page□click

24/7 live

Buy CD Key

Choose Your Game: World of Warcraft (Euro)

0 M 23 S□ Refresh	Price Offer	Quantity	Status	Sell
Auchindoun - Alliance	$0.008/Gold	2000-4800	URGENT	Sell
Azshara - Horde	$0.008/Gold	1000-3550	URGENT	Sell
Blackwater Raiders - le	$0.008/Gold	2850-2850	URGENT	Sell

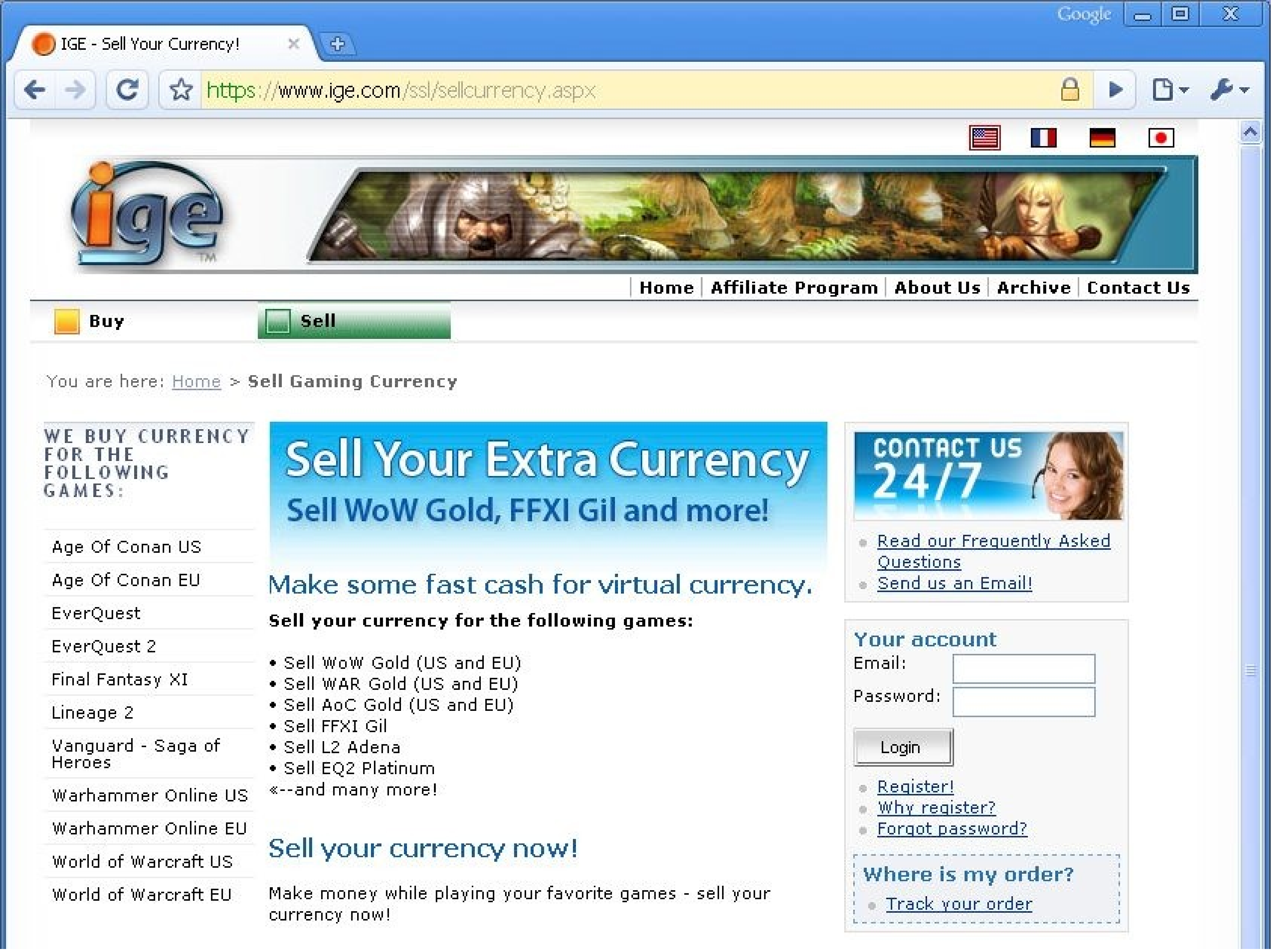
ONLINE SERVICE

☎ 514-667-2472

NEWS

- How to sell your account! [09/02/10]

Sell your World of Warcraft gold online, current rate: $0.008/Gold


Google
IGE - Sell Your Currency!
https://www.ige.com/ssl/sellcurrency.aspx
ige TM
Home | Affiliate Program | About Us | Archive | Contact Us
Buy
Sell

You are here: Home > Sell Gaming Currency

WE BUY CURRENCY FOR THE FOLLOWING GAMES:

- Age Of Conan US
- Age Of Conan EU
- EverQuest
- EverQuest 2
- Final Fantasy XI
- Lineage 2
- Vanguard - Saga of Heroes
- Warhammer Online US
- Warhammer Online EU
- World of Warcraft US
- World of Warcraft EU

Sell Your Extra Currency

Sell WoW Gold, FFXI Gil and more!

Make some fast cash for virtual currency.

Sell your currency for the following games:

- Sell WoW Gold (US and EU)
- Sell WAR Gold (US and EU)
- Sell AoC Gold (US and EU)
- Sell FFXI Gil
- Sell L2 Adena
- Sell EQ2 Platinum

«--and many more!

Sell your currency now!

Make money while playing your favorite games - sell your currency now!

CONTACT US 24/7

- Read our Frequently Asked Questions
- Send us an Email!

Your account

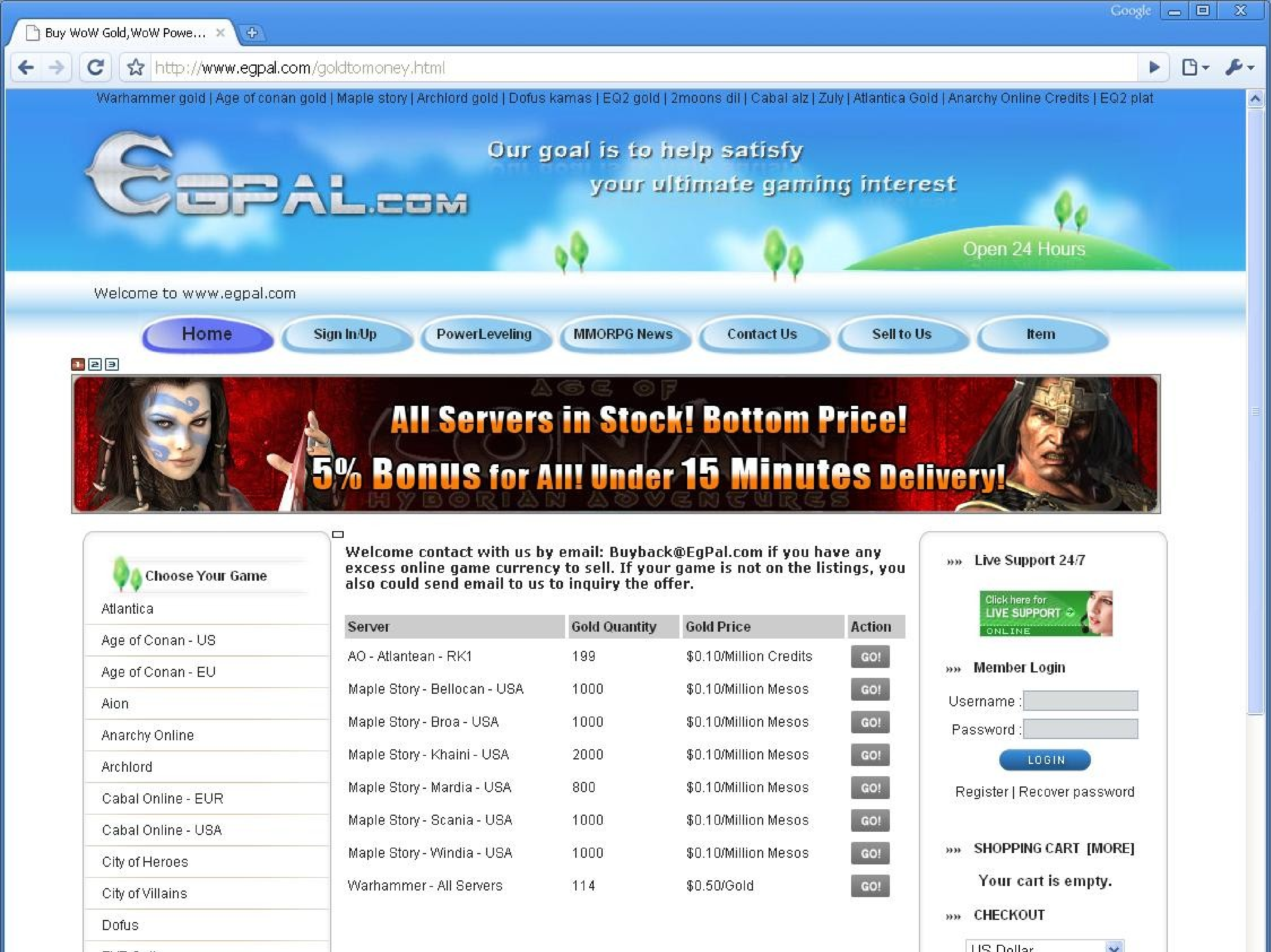
Email:

Password:

- Register!
- Why register?
- Forgot password?

Where is my order?

- Track your order


Buy WoW Gold,WoW Powe...
http://www.egpal.com/goldtomoney.html
Google
EGPAL.com
Our goal is to help satisfy your ultimate gaming interest
Open 24 Hours
Home
Sign In/Up
PowerLeveling
MMORPG News
Contact Us
Sell to Us
Item
1 2 3
AGE OF CONAN HYBORIAN ADVENTURES
All Servers in Stock! Bottom Price!
5% Bonus for All! Under 15 Minutes Delivery!
Click here for LIVE SUPPORT ONLINE
LOGIN

Warhammer gold | Age of conan gold | Maple story | Archlord gold | Dofus kamas | EQ2 gold | 2moons dil | Cabal alz | Zuly | Atlantica Gold | Anarchy Online Credits | EQ2 plat

Welcome to www.egpal.com

Choose Your Game

- Atlantica
- Age of Conan - US
- Age of Conan - EU
- Aion
- Anarchy Online
- Archlord
- Cabal Online - EUR
- Cabal Online - USA
- City of Heroes
- City of Villains
- Dofus

Welcome contact with us by email: Buyback@EgPal.com if you have any excess online game currency to sell. If your game is not on the listings, you also could send email to us to inquiry the offer.

Server	Gold Quantity	Gold Price	Action
AO - Atlantean - RK1	199	$0.10/Million Credits	GO!
Maple Story - Bellocan - USA	1000	$0.10/Million Mesos	GO!
Maple Story - Broa - USA	1000	$0.10/Million Mesos	GO!
Maple Story - Khaini - USA	2000	$0.10/Million Mesos	GO!
Maple Story - Mardia - USA	800	$0.10/Million Mesos	GO!
Maple Story - Scania - USA	1000	$0.10/Million Mesos	GO!
Maple Story - Windia - USA	1000	$0.10/Million Mesos	GO!
Warhammer - All Servers	114	$0.50/Gold	GO!

»» Live Support 24/7

»» Member Login

Username :

Password :

Register | Recover password

»» SHOPPING CART [MORE]

Your cart is empty.

»» CHECKOUT

US Dollar

Why cheat or “hack” games

- Free for all
  - Try getting the police to investigate the theft of your “Arthas’ Frostmourne” Sword
  - Laws deal with copying and piracy, not cheating
  - The worst thing that can happen is your account being banned and you have to buy a new one.. unless you do something really stupid..

Security problems in games

- As games become more popular, chances are some users do things they are not “suppose to”

Security problems in games

- Different ways to attack games:
  - Controlling the userinterface to automate playing
    - Mimic input normally coming from the mouse & keyboard
    - Avoid boring tasks
    - Play 10 characters at once
      - While you do something else
      - exchange gold and other items for real money

Security problems in games

- Different ways to attack games:
  - Modifying the game, either in memory or on disk
    - Scan memory for known data and change it
      - With WoW it used to be possible to find “your” location in the 3D world in ram.
      - Changing this triple would “teleport” your character to anywhere in the virtual world
        - A big deal because these worlds are huge
        - and walking for an hour is boring
    - The server trusts the client. Not a great idea

Security problems in games

- Different ways to attack games:
  - Using the layer below
    - Like most software, games rely on other software
    - Modify drivers (as seen in the “wallhack”)
    - Hook windows libraries, and other “rootkit technologies”

Security problems in games

- Different ways to attack games:
  - Modifying or generating network traffic
    - Replay attacks
    - Generate all the traffic the server expects
      - As long as its valid, the server can't tell the difference
    - “Proxy” the traffic and change it when needed
    - Encryption is possible, but
      - Resource intensive
      - Including the key in the client kind of ruins the point.

Protecting your games

- The Game client software runs in a potentially hostile environment
- Users have full control over their system
  - Can be considered as the enemy with respect to game client security
    - Different from the traditional scenario where the user wants to protect his own computer and information

Protecting your games

- Clientside, software only protection
  - Software surveillance
    - Blizzard, the company behind World of Warcraft, installs a type of spyware
      - Scans memory to find suspicious code and data
      - Runs in user space, can be circumvented by kernel space code.
      - Can be spoofed
  - Quickly turns into an arms race
    - The “hacker” has the upper hand since he controls the system and the software running

Protecting your games

- Serverside checks
  - Is the client input valid and possible?
    - The gameworld, like the real world, have rules
    - The server can check if the the client breaks the rules or does something impossible
      - Like move across the gameworld in a second
  - Suspicious behavior
    - Not behaving as a “normal player”
    - Keep tabs on
      - Gold movement
      - Users movement and interaction
      - Talk to you in-game to check if you are human

Trusted Computing Group

- The Trusted Computing Group (TCG) is a not-for-profit organization.
- Their original goal was to develop the Trusted Platform Module (TPM). They have later expanded their scope

Trusted Computing Group

They have some well known members:

Microsoft®

IBM

intel®

Trusted Computing Group

and some unknown:

SONY
symantec™
LEXMARK™
hp
DELL
Sun® microsystems
BOEING
Seagate
American Megatrends
AMD
Juniper® NETWORKS
NOKIA
FUJITSU

SAMSUNG

NVIDIA®

ERICSSON

THALES

NEC

SanDisk®

Trusted Computing Group

And about 100 others..

Trusted Computing Group

Trusted Computing != TPM

- Trusted Computing implies much more than just the TPM chip
  - Trusted boot with a special BIOS
  - Trusted Operation System
  - Probably other hardware changes
- Probably not going to be commonplace anytime soon - don't hold your breath :)
- The TPM on the other hand is in most laptops and some workstations
  - “embedded into most newer enterprise PCs” according to TCG

Trusted Boot

- Trusted (or authenticated) Boot is often assumed when talking about Trusted Computing
  - TPM checks the BIOS (CRTM) and the OS kernel
  - The kernel checks other software
- Problems:
  - Requires a “trusted OS” “without” bugs
  - creating such an OS that can run complex games seems impossible
  - Cant rely on it any time soon

Software only solutions are doomed

- Using software to check software to check software
- Proven to be less-than-perfect
  - Case in point: the antivirus and virus arms race
  - Much worse with games because the “bad guy” has total control over the computer
    - Local access control becomes useless
- TPM gives a hardware based “base” to build upon. Maybe not perfect, but better

Promises

“

Trusted platforms identify:
1. Themselves (via cryptography); and
2. The software in use (via measurements)

“

(http://www.isg.rhul.ac.uk/files/Lecture2_EimearGallery_TCMastersCourse_2009.pdf)

Promises

- Trusted Computing Group ~~propaganda~~ information promises a lot:
  - Authentication of the platform to a remote party without privacy concerns for the user
  - Attestation of one computers integrity to another
    - Both hardware and software (?)
  - “Sealing” of data to a platform configuration
    - The data is encrypted and is impossible to decrypt unless the platform is in the correct state / configuration.
  - Protected storage
    - “Store digital credentials such as passwords in a hardware-based vault”

Promises

- Random number generation, SHA-1 hashing, HMAC and RSA operations in dedicated hardware
  - Certified and “correct” implementations of these crypto operations
  - Can operate on keys that are “non-migratable” - they can't leave the TPM
  - Symmetric encryption (AES) is used only internally

Can the TPM fix gamesecurity?

- Secure the network traffic
  - Let the TPM sign or encrypt all traffic before going out on the network
    - Defeats modification of traffic on the wire (proxying)
    - Possibly also replay attacks using purposes counter implementations
    - Requires authentication of the platform / TPM (e.g shared secret or public key)

Can the TPM fix gamesecurity?

- Use integrity attestation on selected code / meassurements
  - Affirm to the server that drivers are not modified
    - Limited number of official drivers
  - Same with windows kernel
    - Makes userland checking more reliable (like the warden for WoW)
    - Changes too often?
  - And with the game itself
    - Must be able to handle updates to the game

Can the TPM fix gamesecurity?

- Use integrity attestation on selected code
  - Integrity checking even possible without a trusted OS / authenticated boot?
  - Technical information seems sparse
  - Cant check everything.. changes are too frequent
  - Inject code after the program has loaded

Can the TPM fix gamesecurity?

- Authenticating the platform
  - Help the client and the server know who they are communicating with

TPM Problems

- The TPM is not designed to be tamper resistant
  - But generally hardware is harder to tamper with than software
  - Some protections are in place
- SHA-1 is broken and should probably not be used anymore (since 2005?)

TPM Problems

- Operations require trust in the TPM
  - It could be a “fake” chip or a software emulator
  - This fake chip could do evil things, like revealing all keys or simply not encrypting (Lie, lie, and lie some more)
  - Trust is suppose to be gained through a hierarchy of public keys and certificates, where the trusted manufacturer signs and stores a special asymmetric keypair (EK) in the TPM.
  - But to actually check these signatures and certificates some sort of PKI needs to be in place, and as far as I can tell, it is not.

TPM Problems

- Direct anonymous attestation (DAA) to the rescue?
  - From a TC course at Royal Holloway University in London:
  - *“DAA removes the necessity to disclose the public value of the endorsement key to a P-CA”*
    - They assume a Privacy- Certificate authority, but don't explain how the validation would be performed

http://www.isg.rhul.ac.uk/files/Lecture3_EimearGallery_TCMastersCourse_2009.pdf

TPM Problems

- Direct anonymous attestation (DAA) to the rescue?
  - *“DAA is based on a family of cryptographic techniques known as zero knowledge proofs. DAA allows a TPM to convince a remote ‘verifier’ that it is indeed valid without the disclosure of the TPM public endorsement key”*

    http://www.isg.rhul.ac.uk/files/Lecture3_EimearGallery_TCMastersCourse_2009.pdf
  - DAA does not require a third party
  - Sounds great.. does it work?
  - Still the same problem with validating keys and certificates?

TPM Problems

- Complexity, lack of understanding and “real world” usage
    - There can be many contributing factors to the lack of usage
        - T.C. is associated with DRM and privacy concerns
        - Bad security solutions are very profitable :)

TPM Problems

- Many T.C. Concepts can be hard to understand
  - More confused now than ever
  - At least I'm not alone: "*The complexity of this process (attestation) troubles us. In security, one should be careful about trusting something that is too big to fit into one's head*" (http://www.ists.dartmouth.edu/library/263.pdf)

Credits where credit's due

- Bruce Potter: “The Trusted Computing - Could it be…. SATAN?” (presentation held at defCon & shmoocon)
- Greg Hoglund and Gary McGraw:
  Book: “Exploiting online games”
  Presentations “Exploting online games” (16th Usenix security symposium)
  and “Exploiting online games for cash” (DefCon 15)
- http://projects.csail.mit.edu/tc/
- http://www.ists.dartmouth.edu/library/263.pdf
- http://www.isg.rhul.ac.uk/msc/teaching/iy5608

http://www.flickr.com/photos/sheila_blige/2573517272/

CryoSe
WORCESTER, WR4 9RH ·
0280/02
HELLO
my name is
TPM