GDC 12 EUROPE

Cheaters, Hackers, Script Kiddies

The Dark Side of Online Games

Stephan Payer
Managing Director, CipSoft GmbH

CipSoft

GAME DEVELOPERS CONFERENCE EUROPE
COLOGNE, GERMANY
AUGUST 13-15, 2012
2012

Your Money or Your Net!

Recently, during the Football Championships ...

- Mail to online betting portal:
  "Transfer $ 15,000 via Western Union or we will attack your website!"
- No reaction
- One hour before kick-off:
  DDoS attack, website no longer available,
  no bets on this match

Contents

- CipSoft, Tibia
- Security aspects
- Motivation of attackers
- Attack scenarios and countermeasures
- Conclusions and advice

- Independent developer and operator of online games for various platforms
- Founded in 2001
- Located in Regensburg

Tibia

- Online role-playing game for PC
- Classic fantasy setting
- Online since 1997
- 300,000 daily users; 100,000 premium accounts

Security Aspects

CipSoft online entertainment

Security

- Fairness
- Access control
- Integrity
- Availability

⇨ Protection **against** users

Safety

- Robustness
- Durability
- Privacy
- Ergonomics

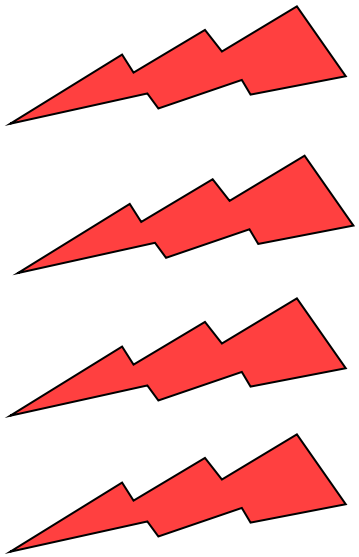
⇨ Protection **of** users

Security Aspects

Security

- Fairness
- Access control
- Integrity
- Availability

⇨ Protection **against** users



Cheating

Account hacking

System hacking

Denial-of-Service

Motivation of Attackers

	Cheat	AccH	SysH	DoS
Convenience	●	●		
Self-help	●			●
Earnings/savings	●	●		
Curiosity/technical challenge	●	●	●	●
Prestige	●		●	●
Advantage in competition	●	●		
Envy		●		
Revenge (player)		●		●
Blackmail (player)		●		●
Revenge (operator)			●	●
Blackmail (operator)			●	●

Cheating: Farmbots

- Completely automated hunting without the player sitting at his computer
- Often done by secondary characters to support the main character

Cheating: Farmbots - Method

- Walk down a prescribed way,
  Attack monsters that turn up,
  Collect loot,
  Heal yourself when necessary,
  Respond to other players
- Macros, proxies, bots
- Commercial realization of the yield and of the programs

Cheating: Farmbots - Problems

- Destruction of the fun of the game
- Unfair competition
- Abuse of power
- Disturbance of the economy
- Risk of account hacking

Cheating: Farmbots - Countermeasures

- Community taking the law into their own hands
- Restriction of money transfers
- Restriction of the possiblity to abuse power
- Banishment by gamemasters
- Automated detection and punishment

Cheating: Other Methods

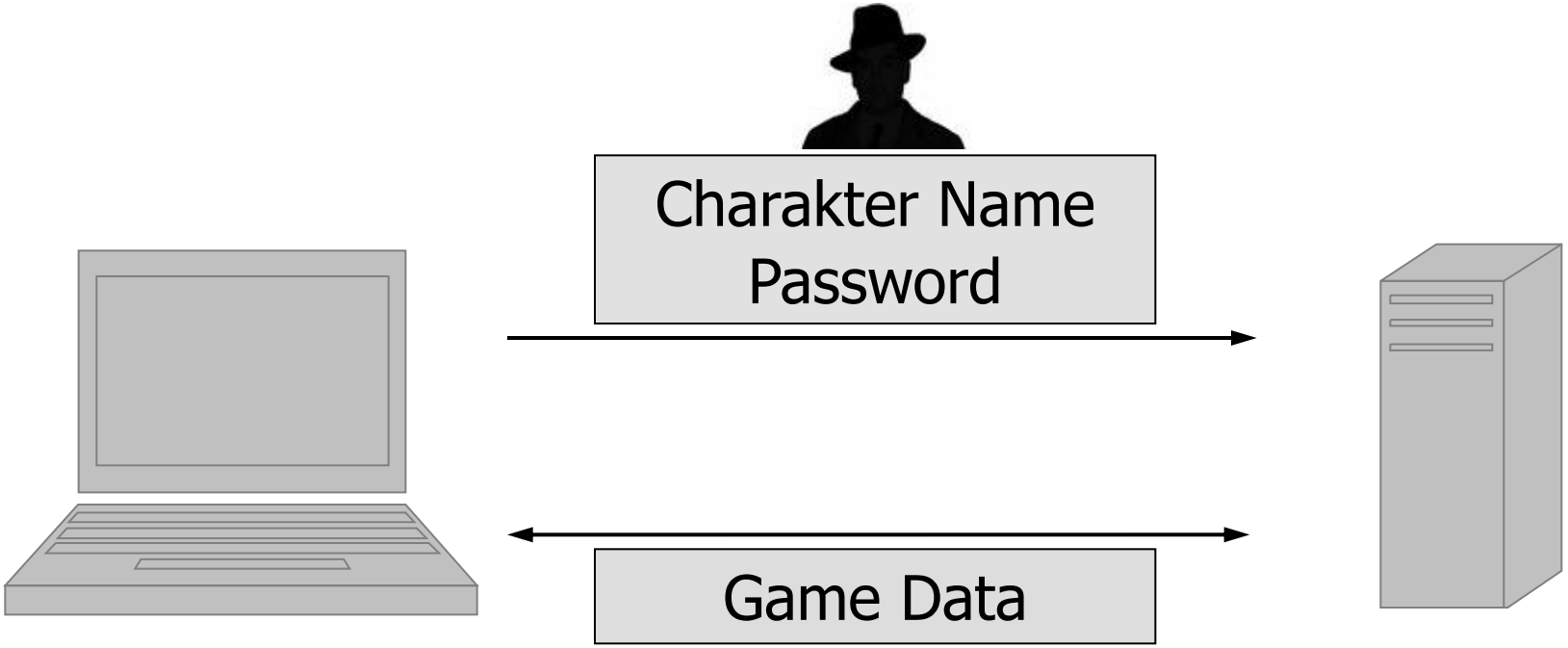
Unfair advantage, usually at the expense of others, by violating rules

- Enhanced client view
- Extended client controls
- Inadmissible commands
- Falsification of client data
- Abuse of bugs
- Account sharing

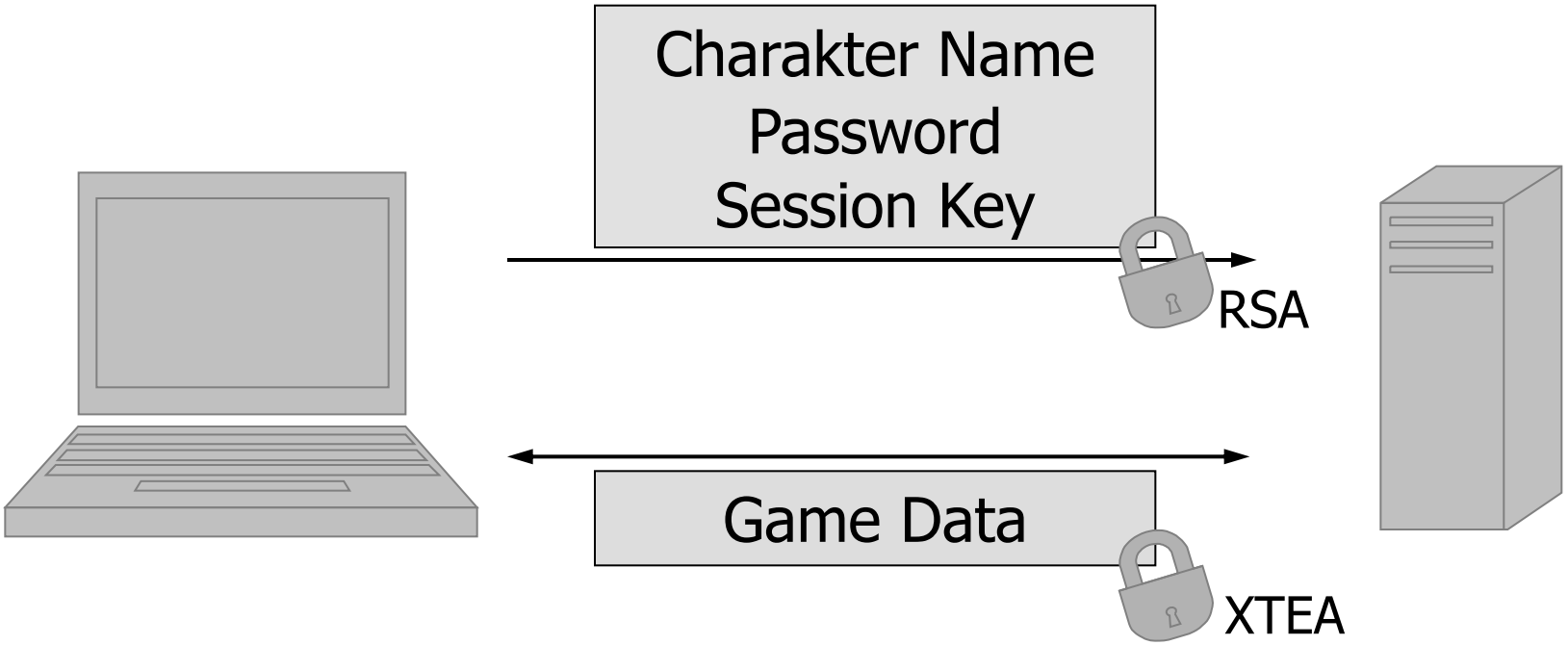
Cheating: General Countermeasures

- Make cheating impossible
- Make cheating useless
- Detect and punish cheaters
- Reward chief witnesses
- Change the rules of the game
- Adopt features
- Allow cheating

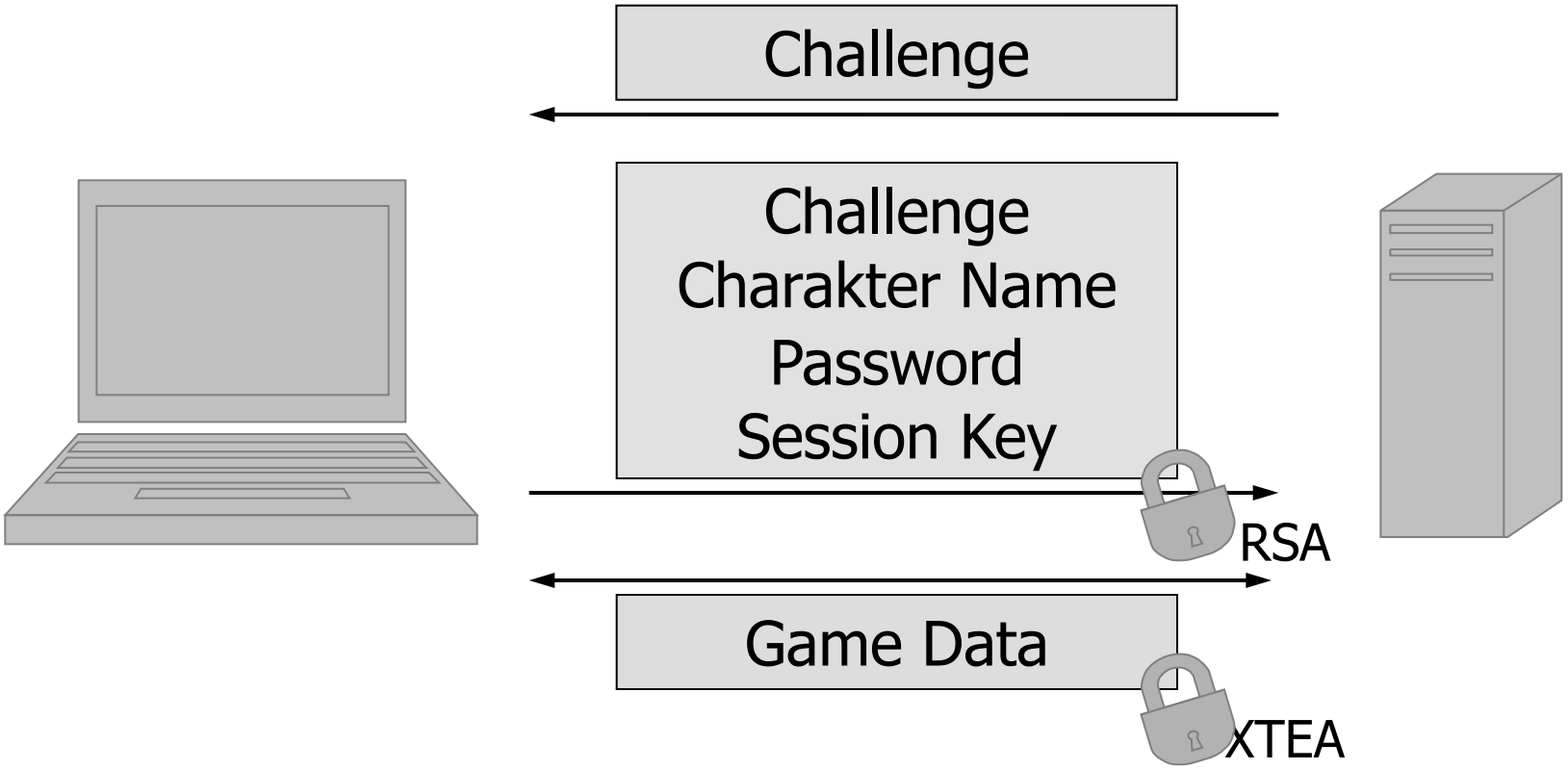
Account Hacking: Password Sniffing



Account Hacking: Password Sniffing



Account Hacking: Password Sniffing



Account Hacking: Other Methods

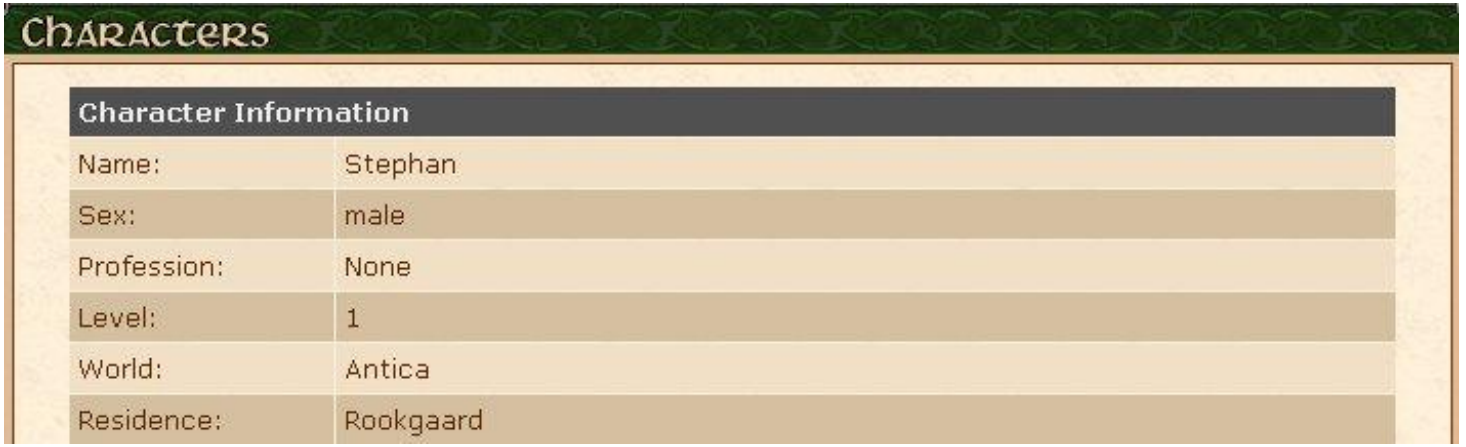
- Brute-force attacks
- Hacking of e-mail accounts belonging to players
- Phishing
- Social engineering
- Keyloggers, Trojan horses
- Faked copies of identity cards

Account Hacking: Gen. Countermeasures

- Use encryption
- Protect against brute-force attacks
- Support authenticator tokens
- Raise players` awareness regarding:
  - Choice of password
  - Way of dealing with credentials
  - General behaviour on the internet

System Hacking: SQL Injection


```
SELECT * FROM Characters
WHERE Name = 'Stephan';
```



System Hacking: SQL Injection


```
SELECT * FROM Characters
WHERE Name = '';
DELETE FROM Characters; --';
```

System Hacking: SQL Injection


```
Ä'; DELETE FROM Charaters; --
```

AddSlashes (ISO 8859)

```
Ä\'; DELETE FROM Characters;
```

Datenbank (UTF8)

```
SELECT * FROM Characters
WHERE Name = '?';
DELETE FROM Characters; --';
```

System Hacking: Other Methods

- Security holes in the application
- Security holes in the operating system
- Social engineering
- Keyloggers, Trojan horses
- Abuse of privileges
- Misconfigurations
- Weak or standard passwords, backdoors

System Hacking: Gen. Countermeasures

- Check all user-generated input
- Follow programming guidelines, use static code analysis, use prepared queries
- Configure your application appropriately
- Configure your system appropriately, install patches
- Use public and private IP addresses, use a firewall
- Divide your system into security zones
- Encrypt your stored data
- Monitor your system, use intrusion detection

System Hacking: Best of …

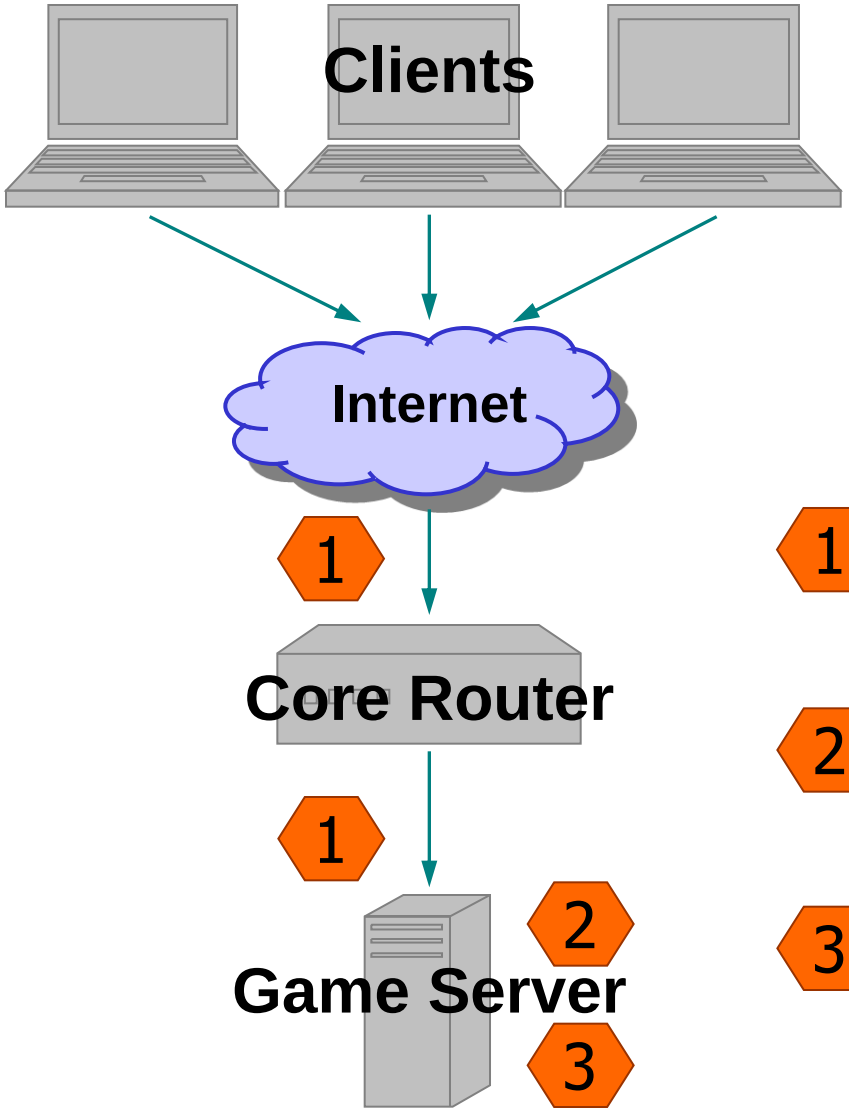
CipSoft online entertainment

48%	Keyloggers, form grabbers or spyware
44%	Exploitation of default or guessable credentials
32%	Use of stolen login credentials
30%	Sending data to external site or entity
23%	Brute-force or dictionary attacks
20%	Backdoors
18%	Disabling or interfering with security controls
10%	Tampering
7%	Social engineering
5%	Exploitation of insufficient authentication
5%	Misuse of privileges

81% Hacking
69% Malware
10% Physical
7% Social
5% Misuse

Source: Verizon, 2012 Data Breach Investigations Report

Denial-of-Service: Methods

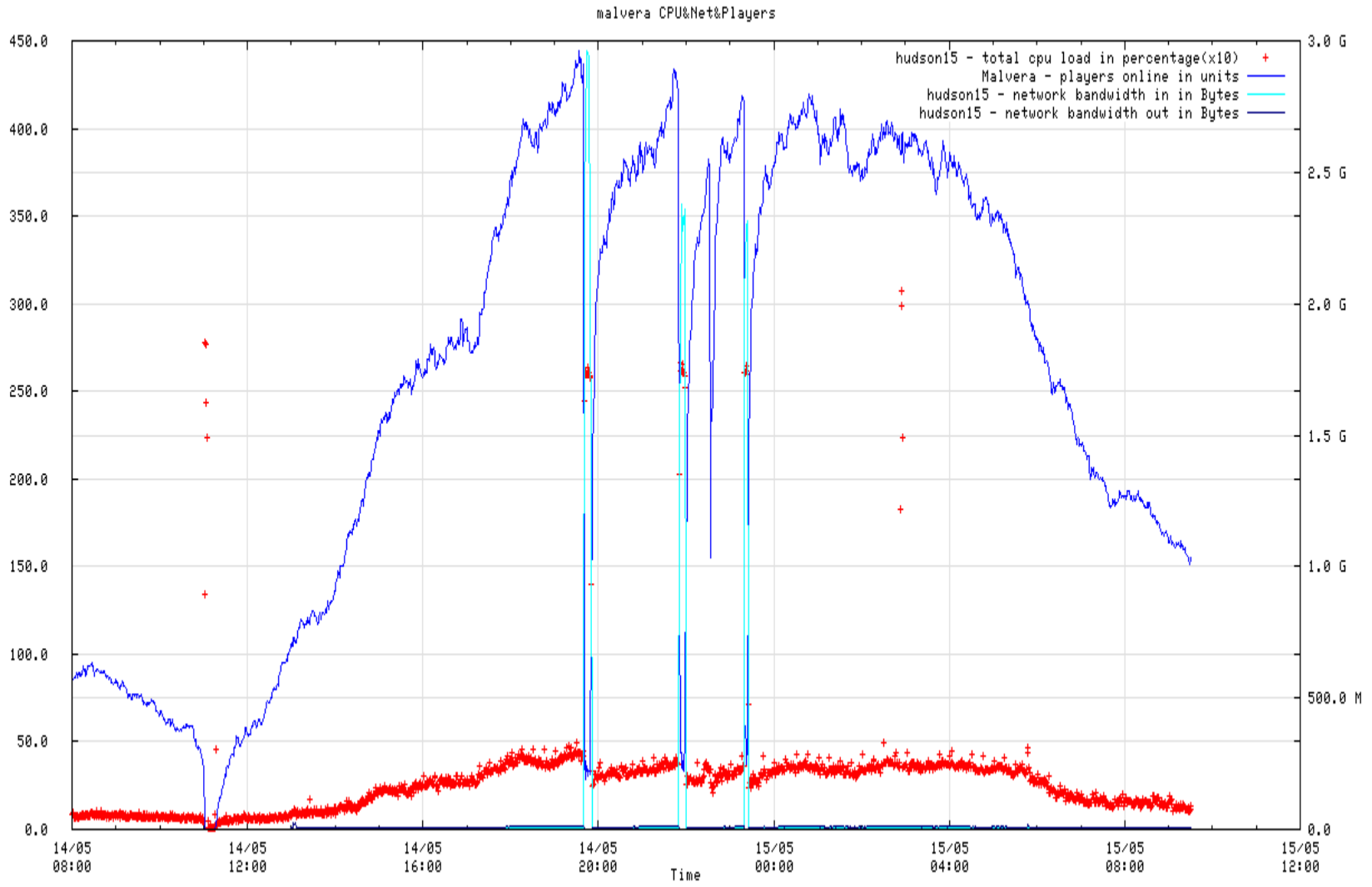


1 Bandwidth

2 Packet rate (esp. SYN flood)

3 Application

Denial-of-Service: Monitoring



Denial-of-Service: Countermeasures

- Rent a massive connection
- Filter UDP packets, if you don‘t need them
- Use SYN cookies
- Use a stateful firewall
- Make your application efficient
- Buy strong hardware

Conclusions

- Every chain is only as strong as its weakest link.
  ⇨ Don't strive for perfection in a single aspect!
- Attackers are resourceful and find every hole.
  ⇨ No "security by obscurity"!
- Client and browser are in the hands of the enemy.
  ⇨ Check all user-generated input!
- There are no secure systems.
  ⇨ Have emergency plans!

Recommended Procedure

- Make a risk analysis: What do you want to protect and at what expenses?
- Deter attackers.
- Keep attackers from entering your system.
- Keep attackers from finding data.
- Detect attacks and respond to them.

Thank You!

www.cipsoft.com contact@cipsoft.com