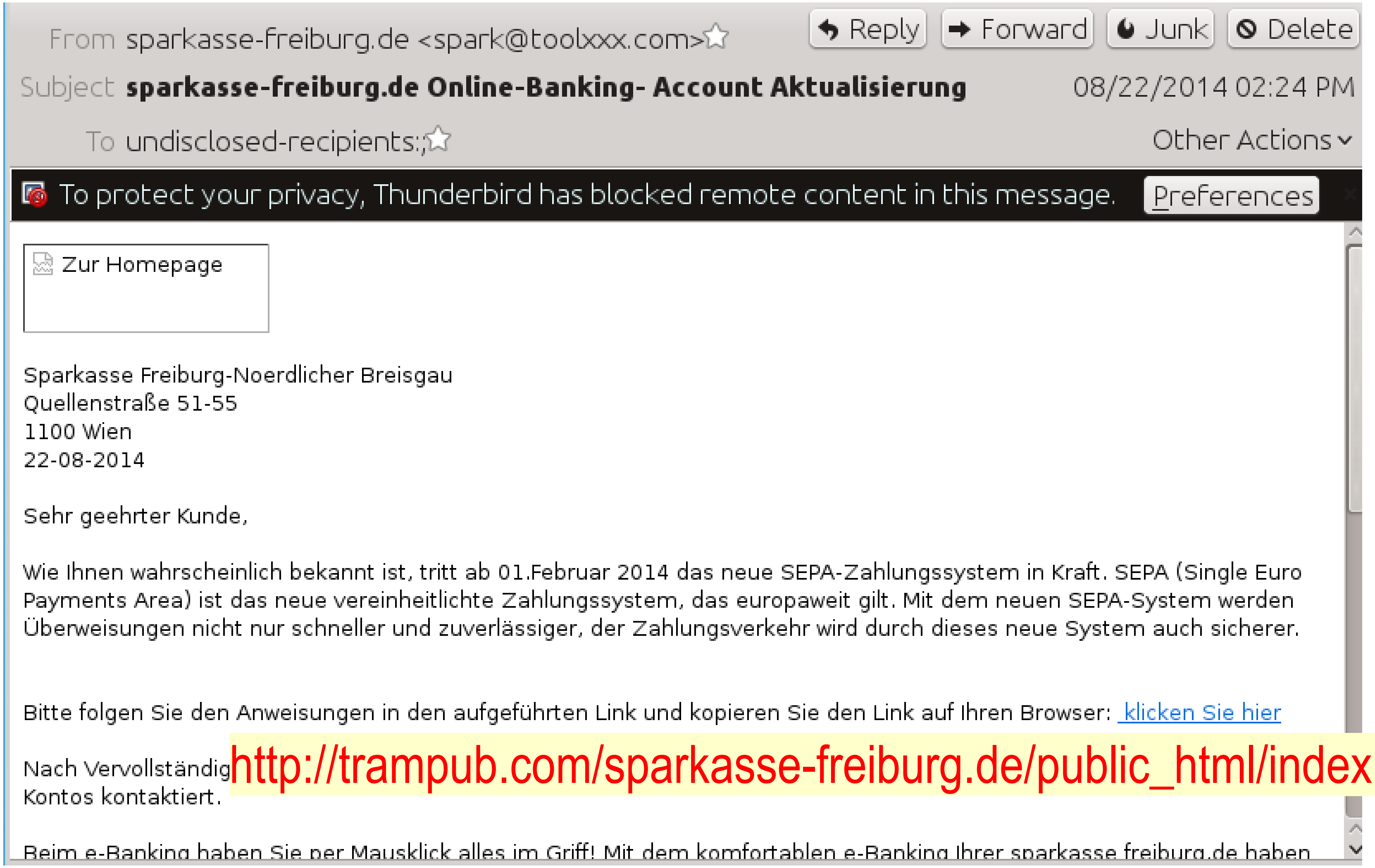
WEB SERVICES (IN)SECURITY

Objectives

- After this unit you will be able to explain the concepts of:
  - Security issues in databases & Web
  - Awareness of Web service vulnerability
  - How to do secure email correspondence
  - Something about hacking

Why is it Spam?



From sparkasse-freiburg.de <spark@toolxxx.com>

Subject **sparkasse-freiburg.de Online-Banking- Account Aktualisierung** 08/22/2014 02:24 PM

To undisclosed-recipients:;

To protect your privacy, Thunderbird has blocked remote content in this message.

Zur Homepage

Sparkasse Freiburg-Noerdlicher Breisgau
Quellenstraße 51-55
1100 Wien
22-08-2014

Sehr geehrter Kunde,

Wie Ihnen wahrscheinlich bekannt ist, tritt ab 01.Februar 2014 das neue SEPA-Zahlungssystem in Kraft. SEPA (Single Euro Payments Area) ist das neue vereinheitlichte Zahlungssystem, das europaweit gilt. Mit dem neuen SEPA-System werden Überweisungen nicht nur schneller und zuverlässiger, der Zahlungsverkehr wird durch dieses neue System auch sicherer.

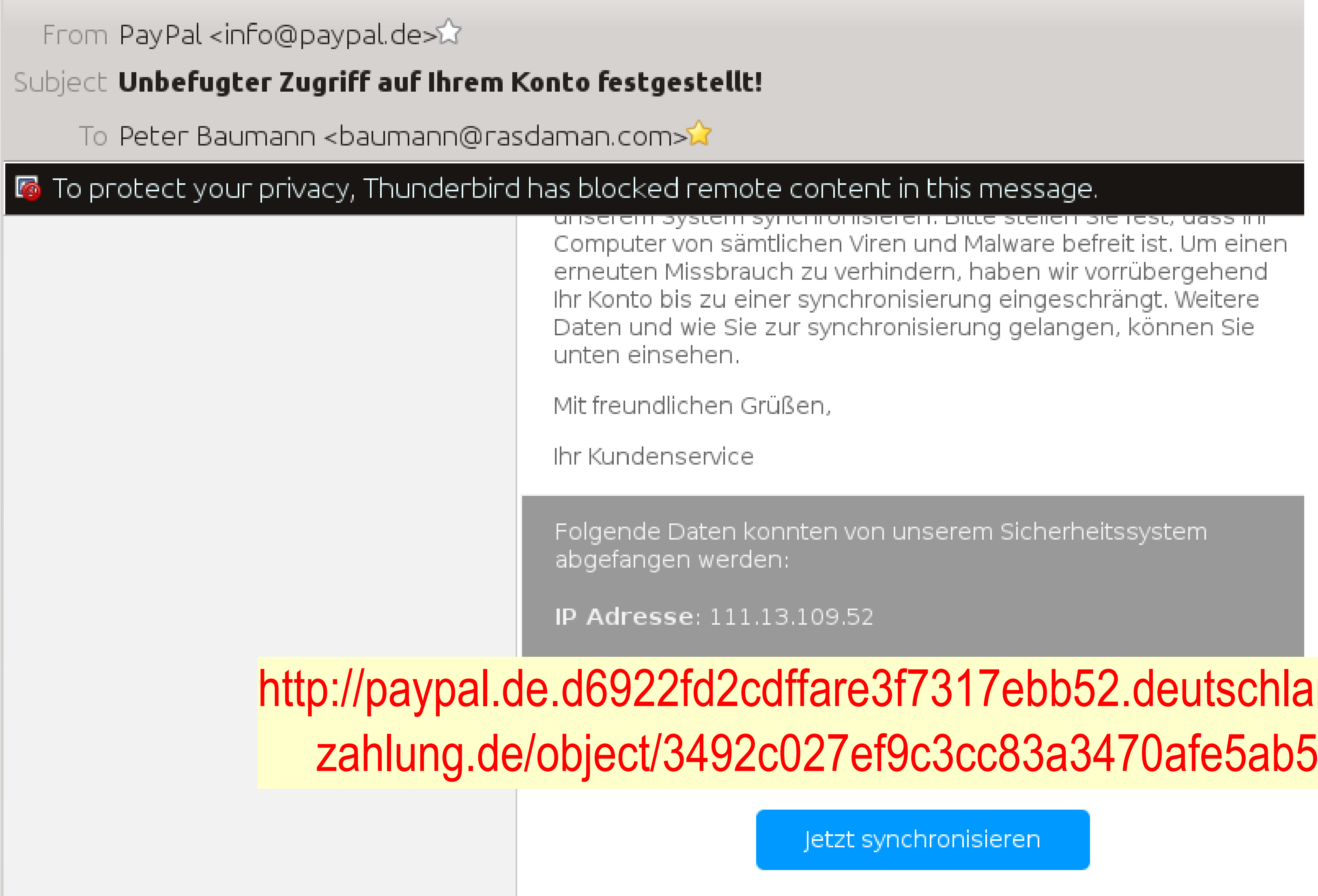
Bitte folgen Sie den Anweisungen in den aufgeführten Link und kopieren Sie den Link auf Ihren Browser: klicken Sie hier

Nach Vervollständig
Kontos kontaktiert.

Beim e-Banking haben Sie per Mausklick alles im Griff! Mit dem komfortablen e-Banking Ihrer sparkasse freiburg.de haben

http://trampub.com/sparkasse-freiburg.de/public_html/index.php

Why is it Spam?



From PayPal <info@paypal.de>

Subject **Unbefugter Zugriff auf Ihrem Konto festgestellt!**

To Peter Baumann <baumann@rasdaman.com>

To protect your privacy, Thunderbird has blocked remote content in this message.

unserem System synchronisieren. Bitte stellen Sie fest, dass Ihr Computer von sämtlichen Viren und Malware befreit ist. Um einen erneuten Missbrauch zu verhindern, haben wir vorrübergehend Ihr Konto bis zu einer synchronisierung eingeschrängt. Weitere Daten und wie Sie zur synchronisierung gelangen, können Sie unten einsehen.

Mit freundlichen Grüßen,

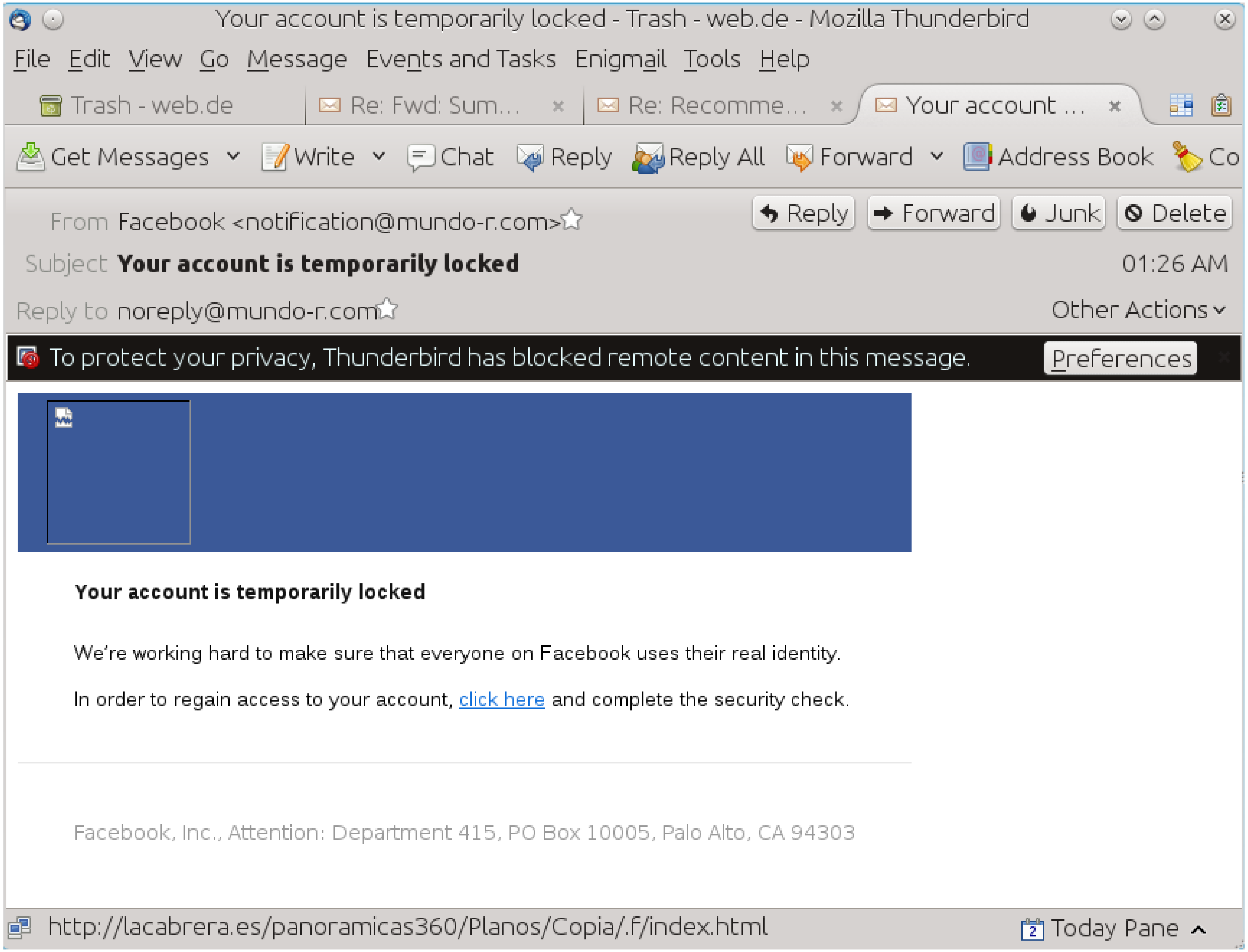
Ihr Kundenservice

Folgende Daten konnten von unserem Sicherheitssystem abgefangen werden:

IP Adresse: 111.13.109.52

http://paypal.de.d6922fd2cdffare3f7317ebb52.deutschland-zahlung.de/object/3492c027ef9c3cc83a3470afe5ab553f

Why is it Spam?



From Facebook <notification@mundo-r.com>

Subject **Your account is temporarily locked**

01:26 AM

Reply to noreply@mundo-r.com

To protect your privacy, Thunderbird has blocked remote content in this message.

Your account is temporarily locked

We're working hard to make sure that everyone on Facebook uses their real identity.

In order to regain access to your account, click here and complete the security check.

Facebook, Inc., Attention: Department 415, PO Box 10005, Palo Alto, CA 94303

http://lacabrera.es/panoramicas360/Planos/Copia/.f/index.html

What’s the Problem?

- Secrecy:
  Users should not be able to see things they are not supposed to
  - Ex: student can’t see other students’ grades
  - Ex: *TJX*: US dept store chain
    - WEP exploit – over 47 million CC #s stolen
    - *…lawsuit, consortium of 300 banks*
  - Ex: *CardSystems, Inc:* US credit card payment processing company
    - 263,000 CC #s stolen from database via SQL injection (June 2005)
    - 43 million CC #s stored unencrypted, compromised
    - *…out of business*

What's the Problem?

- Secrecy:
  Users should not be able to see things they are not supposed to
  - Ex: student can't see other students' grades
- Integrity:
  Users should not be able to modify things they are not supposed to
  - Ex: Only instructors can assign grades
- Availability:
  Users should be able to see and modify things they are allowed to
  - Ex: professor can see and set students' grades

Encryption

- Encryption
  = encoding messages so that only authorized parties can read them
- Over Internet: cryptographic protocols for providing communication security
  - Transport Layer Security (TLS)
  - Predecessor: Secure Sockets Layer (SSL)
  - OpenSSL = open-source implementation of SSL & TLS protocols
- In browser: https vs http

Authentication

- Mostly: Username / password authentication
  - Password transmitted encrypted (https!)
  - Server generates session key, transmitted via SSL
- Digital signature:
  demonstrate authenticity of digital message / document
  - Checksum over document + encryption
- External hardware
  - Fingerprint device, smart card reader, …
- Social engineering!

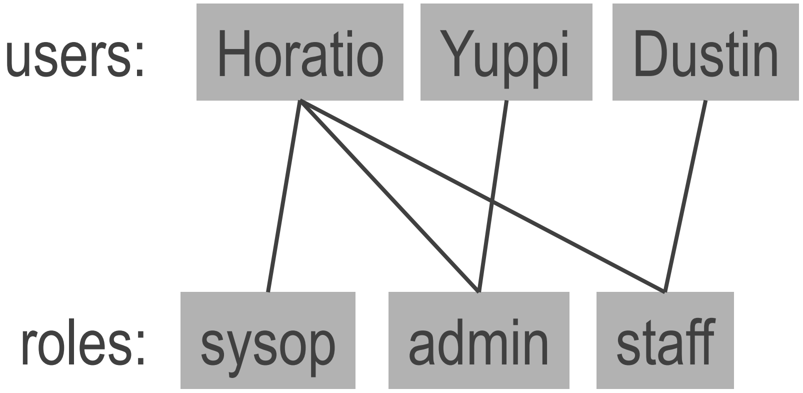
https://howsecureismypassword.net/

DB: Role-Based Access Control (RBAC)

- Access control in databases:
  Individual access rights can be granted to (and revoked from) users

```
GRANT SELECT ON Students TO Faculty
GRANT UPDATE(grade) ON Students TO Faculty
GRANT SELECT, UPDATE, DELETE ON STUDENTS to HR
```

- Access rights assigned to roles
  - Roles then be granted to users
  - Reflects how real organizations work



1. Email Security: The Ridiculous

- Classic way to achieve security: email disclaimers
  - Standard legalese: “*This message is confidential. It may also be privileged or otherwise protected by work product immunity or other legal rules. If you have received it by mistake, please let us know by e-mail reply and delete it from your system; you may not copy this message or disclose its contents to anyone.”*
  - BTW, oldest found (AD 1083): "*Si forte in alienas manus oberraverit hec peregrina epistola incertis ventis dimissa, sed Deo commendata, precamur ut ei reddatur cui soli destinata, nec preripiat quisquam non sibi parata*."
- Compare to a paper letter...
- See also: http://www.goldmark.org/jeff/stupid-disclaimers/

> traceroute

1. Email Security: The Situation

lifehacker.com discussion:

- "…mostly, legally speaking, pointless. Lawyers and experts on internet policy say no court case has ever turned on the presence or absence of such an automatic e-mail footer in America, the most litigious of rich countries."
  - But: „They are prevalent because in the U.S. exactly BECAUSE there is no court case that has turned on the appearance or lack of a disclaimer or end of email boiler plate. Until a court affirmatively denies their power, they will remain […]."
- "Many disclaimers are, in effect, seeking to impose a contractual obligation unilaterally, and thus are probably unenforceable. This is clear in Europe."

Disclaimer:
this is not a legal advice, I'm not a lawyer.
No responsibility whatsoever taken

1. Email Security: The Risks

- Disclosure of information by plain text transmission
  - Traffic analysis
  - in ~~some~~ many countries emails monitored by agencies
- Modification: “man-in-the-middle attack”
- Masquerade: send in the name of others
- Denial of Service: make service unavailable to user
  - overloading servers
  - blocking users by repeatedly wrong password
  - ...

1. Email Security: Encryption

- Email encryption prevents unauthorized persons from reading email
- Pretty Good Privacy (recall?)
  - public key for encryption, bound to email address, published
  - private key for decryption, kept secretly
- Enigmail MTA extension: install plugin, create public key, publish key
- De-Mail: German secured email communications service
  - Since 2011; supported by Telekom, 1und1, web.de
  - no end-to-end encryption, only provider-to-provider → limited security

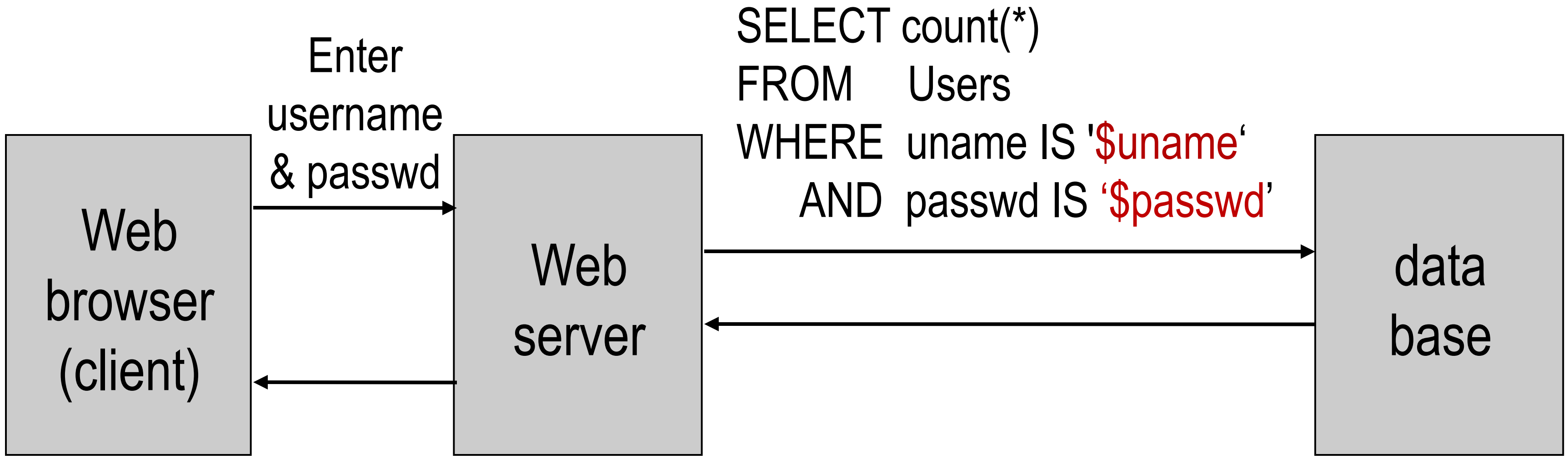
2. Web Applications Security

- Exemplary risks:
  - Disclosure: access confidential data (bank account, …)
  - SQL Injection: access/destroy sensitive database contents
  - Javascript injection: compromising client
  - Denial of Service
- Login Credentials Security
  - account & password in DB (better encrypted!)
  - on login attempt: user / password verified against DB
  - SQL query? ⇨

> Samba log

How To Hack a Database

- Ex: SQL injection
  - Compromise database query



Web browser (client)

Enter username & passwd

Web server

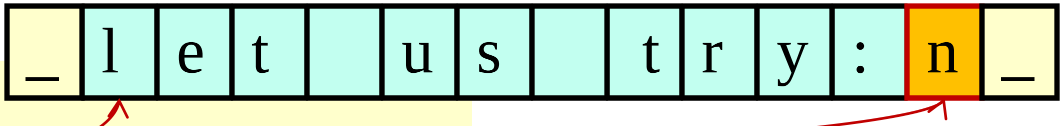
```
SELECT count(*)
FROM    Users
WHERE  uname IS '$uname‘
    AND  passwd IS ‘$passwd’
```

data base

- What will happen at input of '; DROP TABLE Users; -- ? (keyword: DoS)
- *Name 2 independent techniques to prevent!*

Hacking, Generalized

- SQL injection generalizes to: Command injection
  - ...usually by abusing data paths as command paths
- Ex: buffer overflow attack



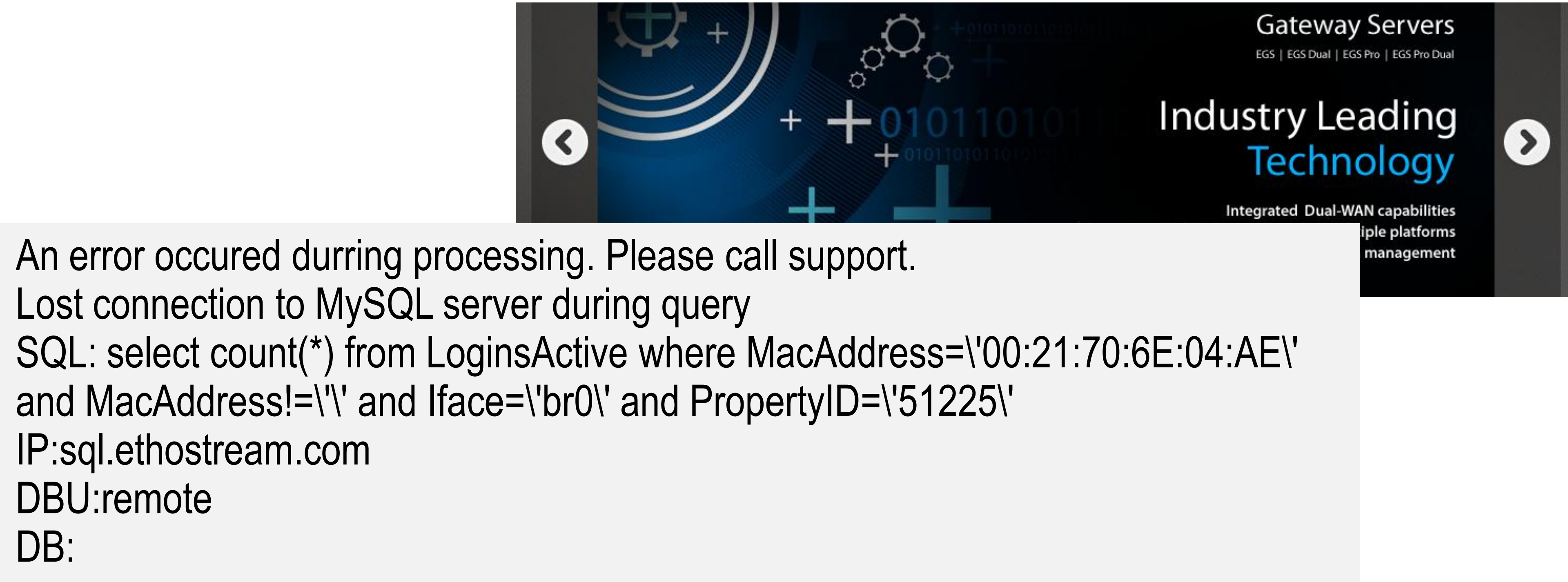
_	l	e	t		u	s		t	r	y	:	n	_

```
{     char inputData[11];
      char command;
      switch (command)
      {     case `s`: executeSelect( inputData ); break;
            case `u`: executeUpdate( inputData ); break;
            case `i`: executeInsert( inputData ); break;
            case `d`: executeDelete( inputData ); break;
            case `n`: detonateNuke(); break;
      }
}
```

Biggest Identity Leak to Date

- Discovered by Hold Security,
  reported in the New York times (Aug 5, 2014)
- 420,000 websites compromised,
  1.2 billion user password data, 500 million e-mail addresses
- presumably bots carrying out automated SQL injection attacks
- PS: https://sec.hpi.uni-potsdam.de/leak-checker/

How to Expose Yourself


Gateway Servers
EGS | EGS Dual | EGS Pro | EGS Pro Dual
Industry Leading
Technology
Integrated Dual-WAN capabilities
iple platforms
management

```
An error occured durring processing. Please call support.
Lost connection to MySQL server during query
SQL: select count(*) from LoginsActive where MacAddress=\'00:21:70:6E:04:AE\'
and MacAddress!=\'\' and Iface=\'br0\' and PropertyID=\'51225\'
IP:sql.ethostream.com
DBU:remote
DB:
```

UK GCHQ Manipulating Internet [src]

- “Change outcome of online polls” (UNDERPASS)
- “Disruption of video-based websites hosting extremist content through concerted target discovery and content removal.” (SILVERLORD)
- “Active skype capability. Provision of real time call records (SkypeOut and SkypetoSkype) and bidirectional instant messaging. Also contact lists.” (MINIATURE HERO)
- “Find private photographs of targets on Facebook” (SPRING BISHOP)
- “Permanently disable a target’s account on their computer” (ANGRY PIRATE)
- “Targeted Denial Of Service against Web Servers” (PREDATORS FACE)
- “Monitoring target use of the UK eBay” (ELATE)
- “Spoof any email address and send email under that identity” (CHANGELING)
- ...

“If you don’t see it here, it doesn’t mean we can’t build it.”

It‘s Getting Closer...

- 23andMe: send a hair, get your genome
  - earlier: + health results
  - Oct 2014, over 750,000 individuals genotyped

- Microsoft is an equal opportunity employer. All qualified applicants will receive consideration for employment without regard to race, color, gender, sexual orientation, gender identity or expression, religion, national origin, marital status, age, disability, veteran status, genetic information, or any other protected status.
  - [Microsoft Corp.]

[image: 23andMe]

Summary

- 3 main security objectives: secrecy, integrity, availability
- DB / Web admin responsible for overall security
  - DBMS security: access rights, encryption
  - Internet services & apps *heavily* increase playground for malicious attacks
- Want safe email?
  - Sign digitally → trust
  - Encrypt → confidentiality
- Want to learn more? See www.securitytube.net