JACOBS UNIVERSITY

Security and Authorization

Ramakrishnan & Gehrke, Chapter 21

Motivation

- Secrecy:
  Users should not be able to see things they are not supposed to
  - Ex: student can't see other students' grades
- Ex: *TJX*. owns many dept stores in US
  - Attacks exploited WEP used at branches
  - Over 47 million CC #s stolen dating back to 2002
  - *…sue filed by 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*

Motivation / contd.

- Secrecy:
  Users should not be able to see things they are not supposed to
  - Ex: student can't see other students' grades
- Ex: *Equifax 2017* [Siliconbeat]
  - Collecting most sensitive citizen data for credit assessment
    - ssn, name, address, birth dates, credit cards, driver's license, history, …
    - 143m customers affected
  - "maybe dozens" of breaches, fix only 6
  - hacked due to insufficient internal secu
  - *BTW, senior execs sold 1.8m in stock*

It would be nice to think that perhaps the company was a victim […] of clever hackers using social engineering […], but it appears […] that there is gross incompetence involved.

Motivation / contd.

- 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(but possibly not modify after release)

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.”

Internet-Oriented Security

- Key Issues: User authentication and trust
  - For DB access from secure location, password-based schemes usually adequate
- For access over an external network, trust is hard to achieve
  - If someone with Sam’s credit card wants to buy from you, how can you be sure it is not someone who stole his card?
  - How can Sam be sure that the screen for entering his credit card information is indeed yours, and not some rogue site spoofing you (to steal such information)?
  - How can he be sure that sensitive information is not “sniffed” while it is being sent over the network to you?
- Encryption is a technique used to address these issues

Encryption

- Idea: “Mask” data for secure transmission or storage
  - Encrypt(data, encryption key) = encrypted data
  - Decrypt(encrypted data, decryption key) = original data
- Symmetric Encryption: DES (Data Encryption Standard)
  - Encryption key = decryption key → all authorized users know decryption key
  - DES (since 1977) 56-bit key; AES 128-bit (or 192-bit or 256-bit) key
  - 1024-bit key considered relatively safe, 2048 preferred
- Public-Key Encryption: Each user has two keys (RSA, Turing Award)
  - User’s encryption key: public
  - User’s decryption key: secret

Authenticating Users

- Amazon can simply use password authentication
  - Sam logs into Amazon account; establishes session key via SSL → pw transmission secure (?)
  - Amazon still at risk if Sam's card stolen + password hacked. Business risk …
- Digital Signatures:
  - Sam encrypts order using his private key, then encrypts result using Amazon's public key
  - Amazon decrypts msg with their private key, decrypts result using Sam's public key, yields original order!
  - Exploits interchangeability of public/private keys for encryption/decryption
  - Now, no one can forge Sam's order, and Sam cannot claim that someone else forged the order

1. Email Security

- 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. Please send us by fax any message containing deadlines as incoming e-mails are not screened for response deadlines. The integrity and security of this message cannot be guaranteed on the Internet.*"
  - 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..
- PS: I like this one: http://www.goldmark.org/jeff/stupid-disclaimers/

1. Email Security / contd.

- "…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, comment:
    „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."
- [lifehacker.com]

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

1. Email Security / contd.

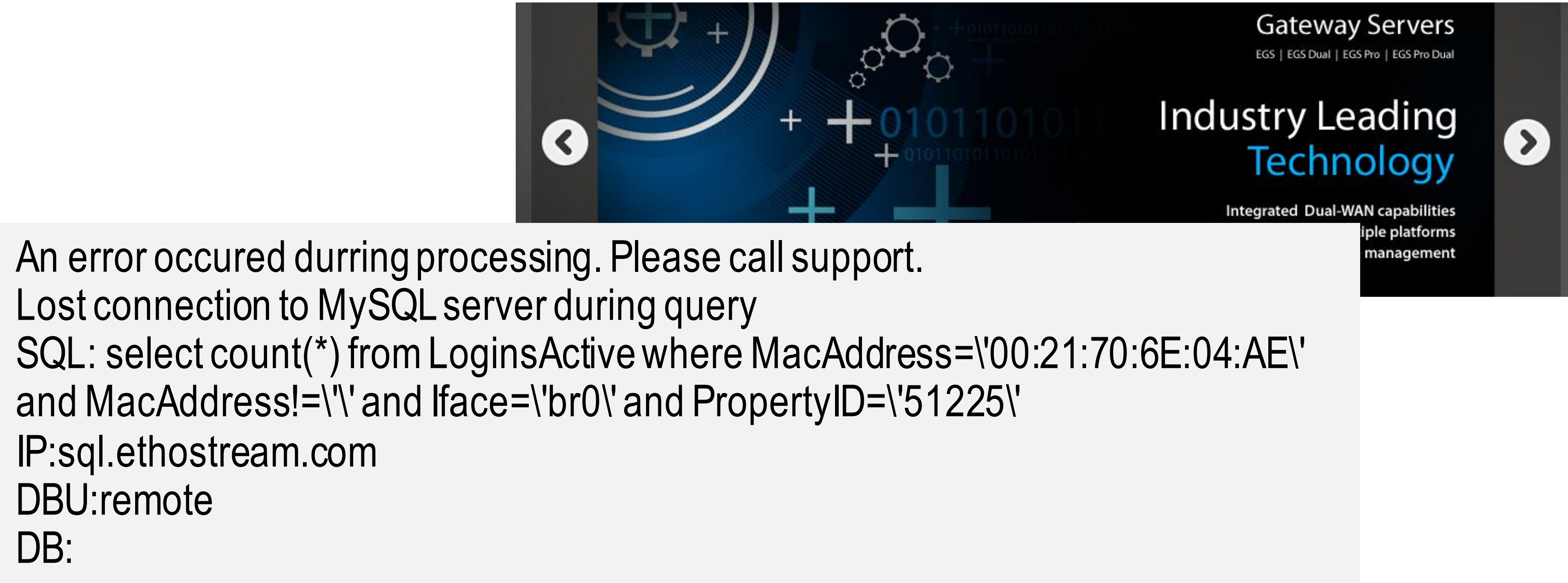
[George Merticariu]

- Risks to user
  - Disclosure of Information by plain text transmission
    - *Traffic analysis: in some countries emails monitored by agencies*
  - Modification: “man-in-the-middle attack”
  - Masquerade: send in the name of others
  - Denial of Service: overloading servers; blocking users by repeatedly wrong password
- Email encryption
  - prevent unauthorized persons to read content of email
  - PGP (Pretty Good Privacy), SecureGmail, …

1. Email Security / contd.

- Pretty Good Privacy = Data encryption/decryption program for signing, encrypting & decrypting emails
  - hashing, data compression, symmetric-key cryptography & public-key cryptography
  - public key bound to user email & username (unique!), published on key server
- Ex: enigmail
  - extension for Thunderbird & Seamonkey
  - install plugin, create public key, publish key → others can use it
  - PGP for signing & encrypting email → recipient needs PGP

How to Expose Yourself

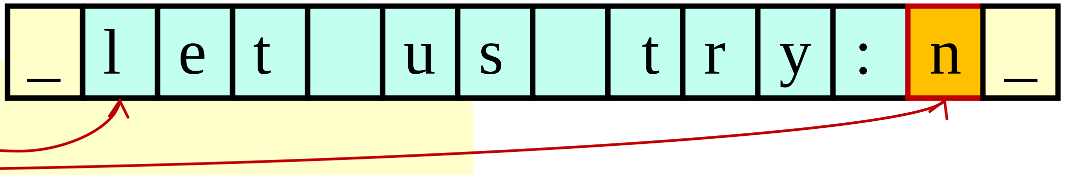

Gateway Servers
EGS | EGS Dual | EGS Pro | EGS Pro Dual
Industry Leading
Technology
Integrated Dual-WAN capabilities
iple platforms
management

```
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:
```

OK, that was in 2011.

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	_

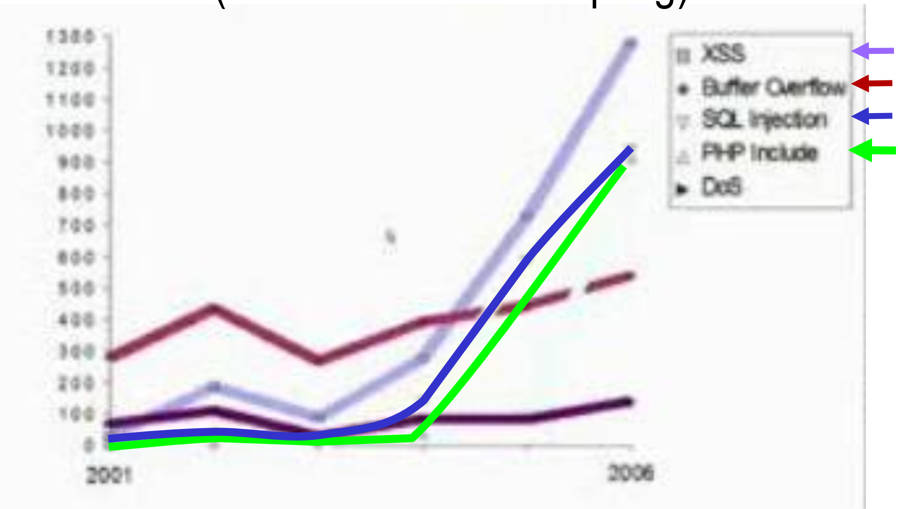
```
{     char inputData[11];
      char command;
      switch (command)
      {     case `s`: executeSelect( inputData ); break;
            case `u`: executeUpdate( inputData ); break;
            case `i`: executeInsert( inputData ); break;
            case `d`: executeDelete( inputData ); break;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

SW Reasons for Service Attacks

- Missing input validation
- Design errors
- Boundary conditions
- Exception handling
- Access validation

Vulnerability trends [Mitre]

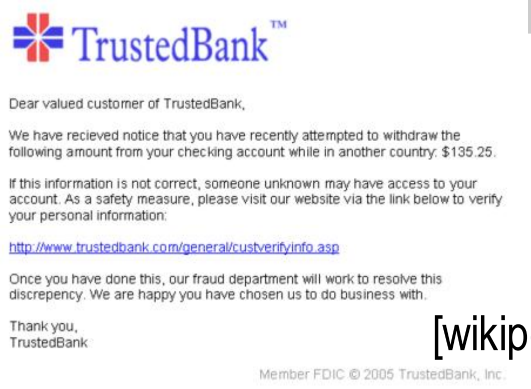
(XSS = cross-site scripting)



- *Red = targets with increasing stats*
    - *See also: OWASP Top 10*

Common Internet Attacks

- spear-phishing
  - = acquire information (usernames, passwords, CC details, …) by masquerading as a trustworthy entity
- man in the middle (→ eavesdropping)
  - = attacker makes independent connections with victims, relays messages between them → victims believe they talk directly to each other
  - attacker intercepts all messages + injects new ones
- watering-hole
  - = attack group:
    Guess / observe sites which group often uses;
    infect these; eventually, some will get infected.



TrustedBank™

Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

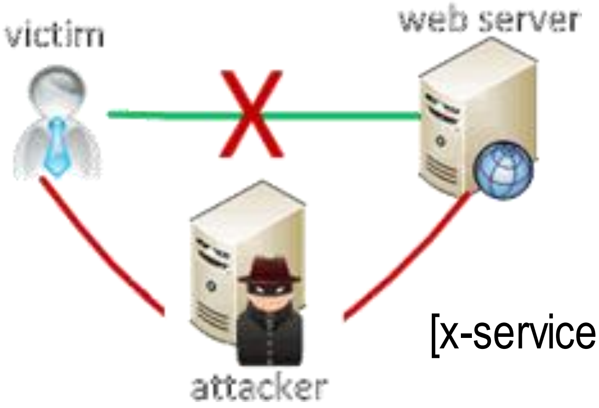
http://www.trustedbank.com/general/custverifyinfo.asp

Once you have done this, our fraud department will work to resolve this discrepency. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

Member FDIC © 2005 TrustedBank, Inc.

[wikipedia]



[x-services.nl]

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/

Identity Leak
Checker
by Hasso-Plattner-Institut

Case Study: Common Security Neglicences

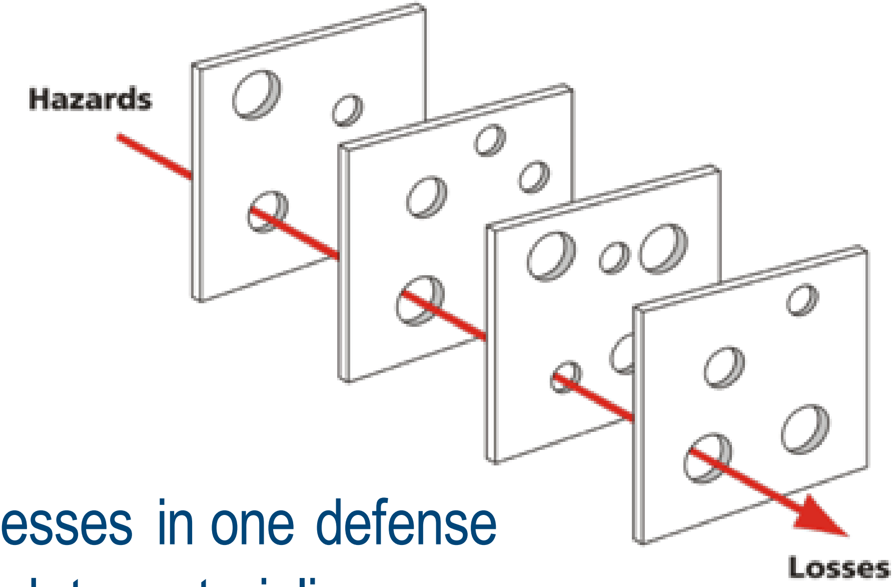
- In 2014, Sony Pictures suffered major break-in
  - possibly by North Korea, in relation to movie *The Interview*
  - “mostly facilitated by unprecedented negligence”

- Problems included:
  - unencrypted storage of sensitive information
  - password stored in plain text files, sometimes even called “passwords” or placed in same directory as encrypted files
  - easily guessable passwords
  - large number of unmonitored devices
  - lack of accountability and responsibility for security, ignorance towards recommendations and audits
  - lack of systematic lesson-learning from previous failures (which included 2011 hacks of Sony PlayStation Network and Sony Pictures that stole account information including unsalted or plain text passwords)
  - weak IT and information security teams

„salted“ ?

- Stolen data included employee data (including financial data), internal emails, and movies

Sewiss Cheese Model of Risks



- in theory:
  lapses & weaknesses in one defense do not allow a risk to materialize
  - other defenses exist
- In practice: flaws in each layer – if aligned, can allow accident to occur
- https://en.wikipedia.org/wiki/Swiss_cheese_model

Afterthoughts: Security and Software Engineering

- Additional security related engineering principles, such as: [Neil Daswani]
  - least privilege
    - *No more rights for any app than absolutely necessary*
  - fail-safe stance
    - *Always return to safe, stable state, after any kind of deviation*
  - protecting against weakest link
    - *Rank vulnerability of components,*
      pay particular attention to "champions"

mobile apps?

- 3 P security management: Process, People, Probing your defences

Summary

- 3 main security objectives: secrecy, integrity, availability
- Internet apps *heavily* increase playground for malicious attacks
  - admin responsible for overall security - your responsibility to keep your site "clean" !
- Want safe email?
  - Sign digitally → trust
  - Encrypt → confidentiality
- http://www.securitytube.net/
- *Job opportunities!*