M183 Applikationssicherheit Implementieren # 16

Herbst/Wintersemester 2017

Jürg Nietlispach

Recap # 15

Data Integrity

- Encryption
- Hash Functions

What’s next?

So far: Using **Authentication** and **Authorization** we can «guarantee», that unallowed access to data is prevented. And: In Case Data has been stolen, **Encryption** «guarantees» that the data is still safe.

But: In case all above measures fail, we still can try to «detect» and «prevent» unallowed actions.

How?

Monitoring, Logging, Audit Trails, …

Intrusion Detection
- Monitor &
- Log Actions (Detection)

Intrusion Prevention (by means of improving the system upon unregular events)
- Evaluate it regularly and / or
- trigger alarms

Monitoring, Logging, Audit-Trails, …

Monitoring (Web Systems)
- Network («outside», «inside» Firewall)
- Application (API via HTTP available?)
- Server (Webserver / Databaseserver available?)
- > http://map.norsecorp.com/

Logging
- Webserver (Store every Request)
- Application (Store every Access of a User)
- > https://www.graylog.org/

Audit-Trails
- User-Specific-Logs, Entity-Specific-Logs (i.e. Versioning)

What to Log?

Application Layer:

- **Web-Server-Logs**
  - SSL Errors, Application Errors, etc.
  - Access to Webserer

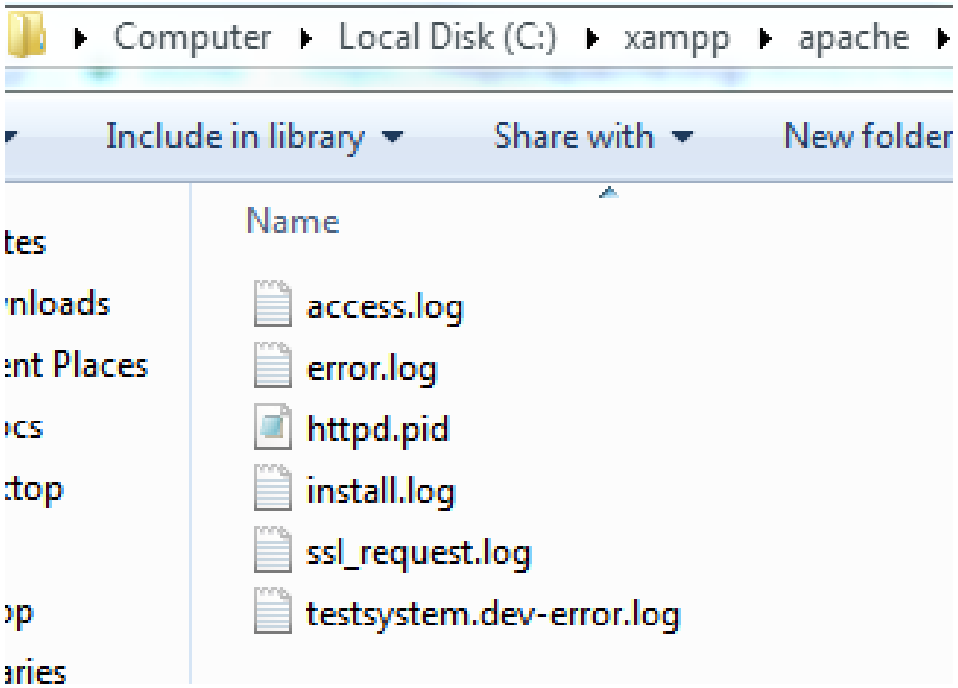
- Database-Server-Logs
  - Transaction History
  - Errors

- **Application Logs** / Audit Trails
  - User-Logs (Login/Logout),
  - Logs to a specific Entity (Versioning)

- Client Logs

Network Layer, Physical Layer etc.

Apache Logs


Computer
Local Disk (C:)
xampp
apache
Include in library
Share with
New folder
Name
access.log
error.log
httpd.pid
install.log
ssl_request.log
testsystem.dev-error.log

Apache access log (HTTP)

IP of Referrer, Timestamp, Requested Ressource

```
127.0.0.1 - - [20/Dec/2017:01:11:50 +0100] "GET / HTTP/1.1" 302 312 "-" "Mozilla/5.0 (Windows NT
127.0.0.1 - - [20/Dec/2017:01:11:50 +0100] "\x16\x03\x01" 400 986 "-" "-"
127.0.0.1 - - [20/Dec/2017:01:12:02 +0100] "\x16\x03\x01" 400 986 "-" "-"
127.0.0.1 - - [20/Dec/2017:01:22:17 +0100] "GET / HTTP/1.1" 302 - "-" "Mozilla/5.0 (Windows NT 6
127.0.0.1 - - [20/Dec/2017:01:22:17 +0100] "GET /dashboard/ HTTP/1.1" 200 7577 "-" "Mozilla/5.0
127.0.0.1 - - [20/Dec/2017:01:22:17 +0100] "GET /dashboard/stylesheets/normalize.css HTTP/1.1" 2
127.0.0.1 - - [20/Dec/2017:01:22:17 +0100] "GET /dashboard/javascripts/modernizr.js HTTP/1.1" 20
127.0.0.1 - - [20/Dec/2017:01:22:17 +0100] "GET /dashboard/javascripts/all.js HTTP/1.1" 200 1890
127.0.0.1 - - [20/Dec/2017:01:22:17 +0100] "GET /dashboard/stylesheets/all.css HTTP/1.1" 200 481
127.0.0.1 - - [20/Dec/2017:01:22:17 +0100] "GET /dashboard/images/xampp-logo.svg HTTP/1.1" 200 5
127.0.0.1 - - [20/Dec/2017:01:22:17 +0100] "GET /dashboard/images/bitnami-xampp.png HTTP/1.1" 20
127.0.0.1 - - [20/Dec/2017:01:22:17 +0100] "GET /dashboard/images/fastly-logo.png HTTP/1.1" 200
127.0.0.1 - - [20/Dec/2017:01:22:17 +0100] "GET /dashboard/images/social-icons.png HTTP/1.1" 200
127.0.0.1 - - [20/Dec/2017:01:22:17 +0100] "GET /dashboard/images/favicon.png HTTP/1.1" 200 2508
127.0.0.1 - - [20/Dec/2017:01:22:22 +0100] "GET / HTTP/1.1" 302 - "-" "Mozilla/5.0 (Windows NT 6
127.0.0.1 - - [20/Dec/2017:01:22:34 +0100] "GET /index.php HTTP/1.1" 302 - "-" "Mozilla/5.0 (Win
127.0.0.1 - - [20/Dec/2017:01:24:00 +0100] "GET / HTTP/1.1" 200 12 "-" "Mozilla/5.0 (Windows NT
127.0.0.1 - - [20/Dec/2017:01:24:00 +0100] "GET /favicon.ico HTTP/1.1" 200 30894 "-" "Mozilla/5.
```

Interesting Stuff?:

- IP -> Block?
- Ressource «/wp-login»

Apache error log

Timestamp, Log-Level, Process & Message

```
[Tue Dec 19 23:56:18.277242 2017] [ssl:warn] [pid 4736:tid 164] AH01909: www.example.com:443:0 server certificate does NOT inc
[Tue Dec 19 23:56:18.476253 2017] [ssl:warn] [pid 4736:tid 164] AH01909: www.example.com:443:0 server certificate does NOT inc
[Tue Dec 19 23:56:18.524256 2017] [mpm_winnt:notice] [pid 4736:tid 164] AH00455: Apache/2.4.29 (Win32) OpenSSL/1.0.2n PHP/7.1.
[Tue Dec 19 23:56:18.524256 2017] [mpm_winnt:notice] [pid 4736:tid 164] AH00456: Apache Lounge VC14 Server built: Nov  5 2017
[Tue Dec 19 23:56:18.525256 2017] [core:notice] [pid 4736:tid 164] AH00094: Command line: 'C:\\xampp\\apache\\bin\\httpd.exe -
[Tue Dec 19 23:56:18.528256 2017] [mpm_winnt:notice] [pid 4736:tid 164] AH00418: Parent: Created child process 7608
[Tue Dec 19 23:56:19.752326 2017] [ssl:warn] [pid 7608:tid 176] AH01909: www.example.com:443:0 server certificate does NOT inc
[Tue Dec 19 23:56:20.010341 2017] [ssl:warn] [pid 7608:tid 176] AH01909: www.example.com:443:0 server certificate does NOT inc
[Tue Dec 19 23:56:20.054344 2017] [mpm_winnt:notice] [pid 7608:tid 176] AH00354: Child: Starting 150 worker threads.
[Wed Dec 20 00:52:52.436157 2017] [mpm_winnt:notice] [pid 3012:tid 164] AH00455: Apache/2.4.29 (Win32) OpenSSL/1.0.2n PHP/7.1.
[Wed Dec 20 00:52:52.436157 2017] [mpm_winnt:notice] [pid 3012:tid 164] AH00456: Apache Lounge VC14 Server built: Nov  5 2017
[Wed Dec 20 00:52:52.436157 2017] [core:notice] [pid 3012:tid 164] AH00094: Command line: 'c:\\xampp\\apache\\bin\\httpd.exe -
[Wed Dec 20 00:52:52.439157 2017] [mpm_winnt:notice] [pid 3012:tid 164] AH00418: Parent: Created child process 6524
[Wed Dec 20 00:52:53.783234 2017] [mpm_winnt:notice] [pid 6524:tid 176] AH00354: Child: Starting 150 worker threads.
```

Interesting Stuff?:

- Timestamp! -> Regular Events?
- Process -> Misconfigurations?

Application User-Logs

```
// check, whether user uses a known browser?
SqlCommand cmd_user_using_usual_browser = new SqlCommand();
cmd_user_using_usual_browser.CommandText = "SELECT Id FROM [dbo].[UserLog] WHERE [UserId] = '" +
                                user_id + "' AND [IP] LIKE '" + ip.Substring(0, 2) + "%' AND browser LIKE '" + platform + "%'";
cmd_user_using_usual_browser.Connection = con;

SqlDataReader reader_usual_browser = cmd_user_using_usual_browser.ExecuteReader();

if (!reader_usual_browser.HasRows)
{
    // -> inform user that he / she is maybe not using a usual browser and is accessing the application from a different ip range i.e. fr
    // both signs, that this login is not done by a valid user -> credentials stolen?

    con.Close();
    con.Open();

    // log this user-behaviour anyway
    SqlCommand log_cmd = new SqlCommand();
    log_cmd.CommandText = "INSERT INTO [dbo].[UserLog] (UserId, IP, Action, Result, CreatedOn, Browser, AdditionalInformation) VALUES('" +
        ip + "', 'login', 'success', GETDATE(), '"+ platform +"', 'other browser')";
    log_cmd.Connection = con;
    log_cmd.ExecuteReader();
}
else {

    con.Close();
    con.Open();

    // everything should be fine
    // log this user-behaviour
    // log this user-behaviour anyway
    SqlCommand log_cmd = new SqlCommand();
    log_cmd.CommandText = "INSERT INTO [dbo].[UserLog] (UserId, IP, Action, Result, CreatedOn, Browser) VALUES('" + user_id + "', '" +
        ip + "', 'login', 'success', GETDATE(), '" + platform + "')";
    log_cmd.Connection = con;
    log_cmd.ExecuteReader();
}
```

Interesting Stuff?
- Benutzerverhalten.

Client-Side Logging

Piwik (https://matomo.org/)
Google Analytics
https://www.patrick-wied.at/static/heatmapjs/
…

How to evaluate Logs

Mathematics & Statistics
- SQL & Aggregation Operations (COUNT, GROUP etc.)
- Regular Expressions
- Trends & Forecasts

Visual Evaluation
- Time Series
- Charts
- Histograms

How to evaluate Logs - Example

Data Structure

	#	Name	Typ	Kollation	Attribute
☐	1	id	int(11)		
☐	2	userid	int(11)		
☐	3	token	varchar(255)	utf8_unicode_ci	
☐	4	login_init	datetime		
☐	5	loggedin	datetime		
☐	6	loggedout	datetime		

& Data Collection

id (1 hide) textinput	userid textinput	token textinput	login_init	loggedin date	loggedout date
71124	4	4eebd6b9ae583b0046701ae871bc2f1e	2018-01-09 23:15:20	2018-01-09 23:15:29	0000-00-00 00:00:00
71123	9578	aee6cb1792682c214e35fa8515ce76d1	2018-01-09 22:14:35	2018-01-09 22:14:38	0000-00-00 00:00:00
71122	12594	3941e56825258201f60922392025c00b	2018-01-09 20:45:22	2018-01-09 20:45:22	0000-00-00 00:00:00
71121	12594	4be88726ac19fa353f949587c34ffaf4	2018-01-09 20:43:54	2018-01-09 20:46:20	0000-00-00 00:00:00
71120	13376	1fcf9ab732d89aea48008cdf4b930e86	2018-01-09 20:36:28	2018-01-09 20:36:31	0000-00-00 00:00:00

Aggregation Function

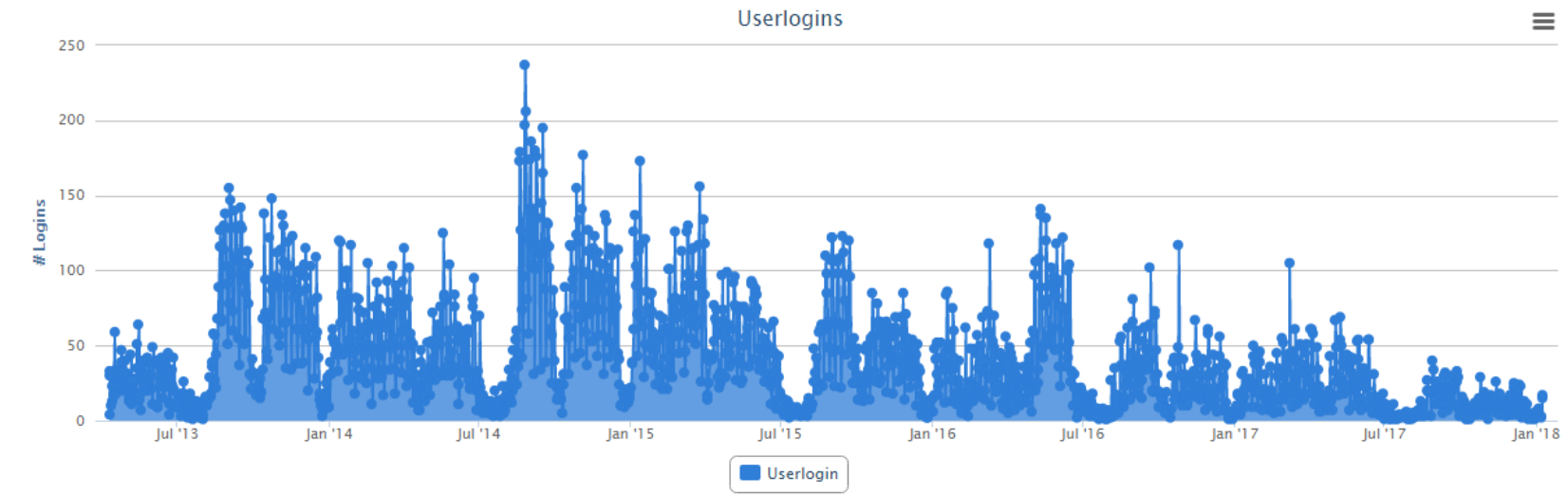
```
= $this->db->processQuery(""
"SELECT COUNT(id) as logincount, DATE(loggedin) as datum, UNIX_TIMESTAMP(loggedin) as timestamp "
"FROM userlogin "
"GROUP BY datum ORDER BY datum ASC"
```

How to evaluate Logs - Example

Raw Data

```
series: [{
    name: 'Userlogin',
    type: 'area',
    //pointInterval: 24 * 3600 * 1000,
    //pointInterval: 24 * 3600 * 1000,
    data : [[1365540581000,4],[1365558834000,33],[1365631238000,30],[
[1366609978000,29],[1366694337000,22],[1366779973000,47],[13668688080
[1367741669000,22],[1367817439000,44],[1367904166000,20],[13679644890
[1368860423000,7],[1368949270000,19],[1369032471000,37],[136911352700
```

Data Visualized



Intrusion Detection 2.0

https://securityintelligence.com/applying-machine-learning-to-improve-your-intrusion-detection-system/

Vorbereitungen Schriftliche Prüfung

- Everybody has a running Visual Studio 2017 at hand
- Everybody has a working Git Client and a Git Repo at hand
- Sample MVC Application given in .NET Framework 4.6.1
- Everybody has a working maschine at hand (Power-Supply, Updates installed)

$\Rightarrow$ Recommendation: use the VM with your own (fast) device!

Recap:
- Coding as well as answering theoretical questions needed

Lab – Anomaly Detection

1. Create a .NET MVC Application
2. Store Browser-Footprint in Database
3. Write Anomaly-Email when Browser (or OS) Changes