

U2U Online

online.u2u.be/courses/25896/modules/10/24854

Developer and IT Training

U2U

Cryptographic Failures

OWASP Web Security Threat #2

u2u Online

6:35 PM 12/29/2023

U2U Online

online.u2u.be/courses/25896/modules/10/24854

Agenda

- Introduction
- Defenses
- Using Data Protection API
- Encryption versus Encoding
- Summary

u2u

u2u Online

6:35 PM 12/29/2023

The image is a screenshot of a web browser displaying a U2U Online course. The browser's address bar shows the URL `online.u2u.be/courses/25896/modules/10/24854`. The course title is "Sensitive Data Exposure". The slide content is as follows:

#2: Cryptographic Failures

- Exposing sensitive data
 - Credit cards
 - Tax IDs
 - Authentication Credentials
- Showing that sensitive data is not wrong!
 - As long as it is to the right person
- Attackers can try to steal or modify the data if it is weakly protected
 - Not using https
 - Insecure cookies

The slide also features the U2U logo in the top right corner. The browser's taskbar at the bottom shows the Windows Start button, a search bar, and several application icons. The system clock indicates 6:35 PM on 12/29/2023.

U2U Online

online.u2u.be/courses/25896/modules/10/24854

U2U

Security Matrix

ATTACK VECTORS

Exploitability

AVERAGE

SECURITY WEAKNESS

Prevalence

WIDESPREAD

TECHNICAL IMPACTS

Detectability

AVERAGE

Impact

SEVERE

ATTACK VECTORS	SECURITY WEAKNESS		TECHNICAL IMPACTS
Exploitability	Prevalence	Detectability	Impact
AVERAGE	WIDESPREAD	AVERAGE	SEVERE

4

The image is a screenshot of a web browser displaying a U2U Online course. The browser's address bar shows the URL `online.u2u.be/courses/25896/modules/10/24854`. The course content is presented in a slide format. The slide has a dark blue sidebar on the left with a navigation menu. The main content area is white and features the title 'Attack Surfaces' in a large, bold, black font. Below the title is a red horizontal line. The slide content consists of three bullet points, each with a square bullet. The first bullet point is 'Not using SSL/TLS correctly', followed by three sub-points: 'Authentication not happening over HTTPS', 'Cookies over HTTP', and 'Activating HSTS'. The second bullet point is 'Bad cryptography', followed by three sub-points: 'Incorrect password storage', 'Using weak algorithms', and 'Not or barely protecting shared keys'. The third bullet point is 'Sharing info via URL'. In the top right corner of the slide, there is a black square logo with the white text 'u2u'. The browser's taskbar is visible at the bottom, showing the Windows Start button, a search bar, and several application icons. The system clock in the bottom right corner indicates the time is 6:36 PM on 12/29/2023.

U2U Online

online.u2u.be/courses/25896/modules/10/24854

Attack Surfaces

- Not using SSL/TLS correctly
 - Authentication not happening over HTTPS
 - Cookies over HTTP
 - Activating HSTS
- Bad cryptography
 - Incorrect password storage
 - Using weak algorithms
 - Not or barely protecting shared keys
- Sharing info via URL

u2u


6:36 PM 12/29/2023

U2U Online

online.u2u.be/courses/25896/modules/10/24854

Defenses

- Don't collect all that sensitive data
 - You can't lose what you don't have!
 - Or only store the hash (with salt!)
- Store secrets in encrypted storage
 - Enable SQL Server Encryption
 - Transparent Data Encryption
 - In combination with extra encryption techniques!
- HTTPS everywhere
 - Not a performance problem any longer!
- Use correct cryptography



6:36 PM
12/29/2023

U2U Online

online.u2u.be/courses/25896/modules/10/24854

U2U

Where to Store Secrets

- Secrets like
 - Some App settings
 - Connection strings
 - Passwords
 - Keys
 - Certificates
- Store them in Azure Key Vault
 - Applications don't store keys directly
 - Automate tasks for certificates (e.g. renewal)
 - Monitor and audit key usage
 - Scales to meet the demands of your apps

```
graph LR; Developer[Developer] -- Deploy --> AzureVM[Azure VM]; subgraph AzureVM; direction TB; YourApp[Your App]; CertStore[Certificate Store]; end; AzureAD[Azure Active Directory] <-->|Authenticate| YourApp; YourApp -- Access --> AzureKV[Azure Key Vault];
```

U2U Online

Search

6:36 PM 12/29/2023

The screenshot shows a web browser window with the address bar displaying 'online.u2u.be/courses/25896/modules/10/24854'. The page features a dark blue sidebar on the left with a navigation menu. The main content area has a white background with the title 'Data Protection API' in a large, black, sans-serif font. Below the title is a red horizontal line. To the right of the title is the 'u2u' logo. The content is organized into a list of bullet points. The Windows taskbar is visible at the bottom of the screen.

Data Protection API

- Available since Windows 2000
- Provides operating system-level data protection services
 - To user and system processes
- Two simple functions, **Protect** and **Unprotect**
 - These use the machine key for system processes
 - Or the user's password for users

U2U Online

online.u2u.be/courses/25896/modules/10/24854

Developer and IT Training

u2u

Demo

Using DPAPI

u2u Online

6:36 PM
12/29/2023

U2U Online

online.u2u.be/courses/25896/modules/10/24854

Encryption vs. Encoding

- Encoding != Encryption
- Encryption example: AES

Text: Hello @ U2U! secret key: P@\$w0rd

0SW% 6G

- Encoding example: Base64

The diagram illustrates the Base64 encoding process. It shows a sequence of four empty boxes representing bytes, with a red arrow pointing down to another sequence of four empty boxes representing the encoded output.

6:36 PM 12/29/2023

The image is a screenshot of a web browser displaying a U2U Online course. The browser's address bar shows the URL `online.u2u.be/courses/25896/modules/10/24854`. The course title in the top left is 'Sensitive Data Exposure'. The slide content is as follows:

Encryption: Refresh your memory

- Storing Passwords
 - Use a hash function (PBKDF2, Argon2, bcrypt or scrypt)
- Storing reversible secrets (never passwords!)
 - Use Symmetric Algorithms (AES)
 - Use Asymmetric Algorithms (RSA)
 - Even better: use a Hybrid Algorithm

The U2U logo is in the top right corner of the slide. The Windows taskbar at the bottom shows the time as 6:36 PM on 12/29/2023.

U2U Online

online.u2u.be/courses/25896/modules/10/24854

Summary

- If you don't store it, you can't lose it
 - Use SQL Trusted connections
 - If you can't, encrypt the connection string in config file
- Use HTTPS everywhere
 - One unprotected URL could expose some data, opening the door
- If you do need to store secrets, use proper encryption
 - Never try to build your own encryption
 - Use DPAPI, it's easy!
 - Encoding is NOT encryption

U2U

6:36 PM 12/29/2023