...

UW | B--Team

Allon Kim; Geoffrey Friesen; Joel Richart; Thomas Dye

CSS 310 - Fall 2015

Disclaimer

What this discussion is NOT

Morality Discussion

Feasibility Study

Business Plan

Hüber

Hüber

Pleasure you want,
Protection you deserve


LEGAL
KINDA LEGAL
ILLEGAL

Hüber

Sex workers CAN

- change status
- refuse clients
- research market
- upsell services
- receive payments
- rate clients
- send location

Clients CAN

- search available workers
- filter by profile
- initiate contact
- make a payment
- rate sex workers
- favorite sex workers

Hüber

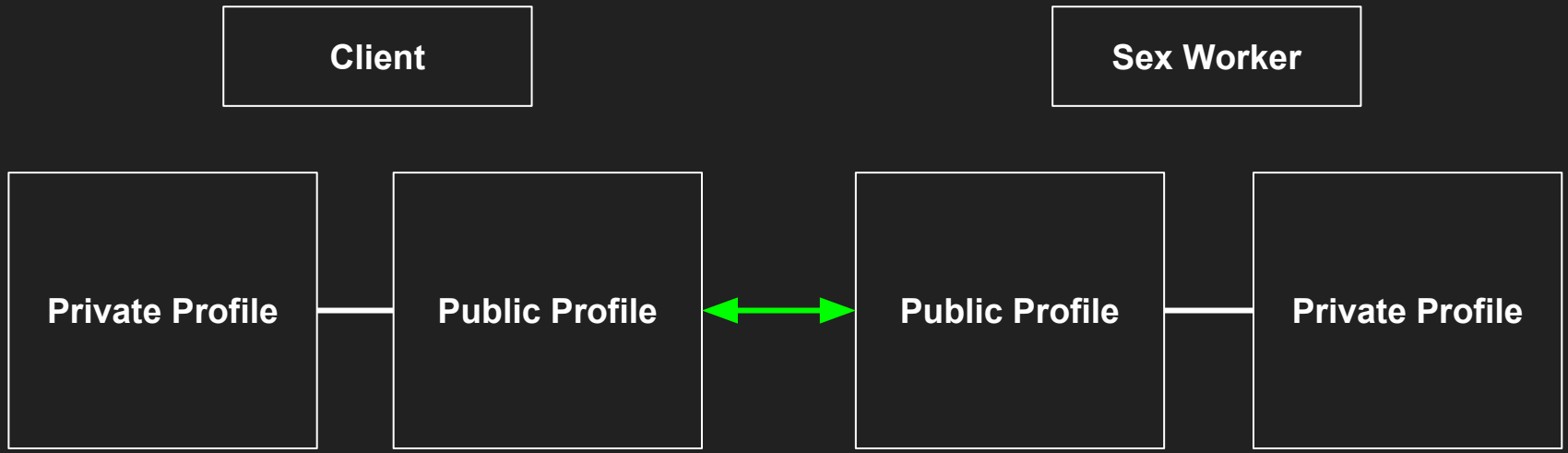
Sex workers CAN NOT

- search clients
- keep a record of clients
- modify payment after transaction

Clients CAN NOT

- see other clients
- actively track specific sex workers
- see a sex worker’s service history
- keep detailed records of sex workers

Things that matter



What can go Wrong?

Internal

External

Unintentional

Strategic Security Policy

Goals

Build and maintain a secure Network

Protect Cardholder Data

Maintain a Vulnerability Management Program

Implement Strong ACM

Regularly Monitor and Test Networks

Maintain an information Security Policy

HOW?

Prevention
Detection
Recovery

HOW?

Prevention

- Subjects and Objects Identification
- ACM with Principle of Least Privilege

Detection

- Implement FireEye IDS (or similar)
- Automate keyword flags in logs

Recovery

- All logging is periodically moved off-network
- Periodic backups of all data to off-network storage
- System configuration kept off-network
- Key-enciphering keys kept off-network

Prevention
Detection
Recovery

Prevention : ACM with Principle of Least Privilege

	Sex Worker Database	Client Database	Payment Transactions	Server Configurations	Production Environment	Production Code	Test Environment	Test Code	Git Repository	Basic Client Profile	Basic Sex Worker Profile	Full Client Profile	Full Sex Worker Profile	Code Migration Tool	System Deployment Tool
DBAs	X	X													
SDEs					R	R	R	R	RWX					X	
SDETs															
System Administrators				R	R		R								X
CEO	R**	R**													
CIO	R**	R**													
CFO			R**												
Client										RW		RW			
Sex Worker										R*	RW		RW		
CSA										R*	R*				
Marketing															
Legal	R**	R**	R**												
Code Migration Tool					RWX	RWX	RWX	RW	R						
System Deployment Tool	C	C		R	RWX	R	RWX	R						X	RWX

Best Practices and Guidelines

Data Retention

Networking

Vulnerability Management

Electronic Access Control

Monitoring

Testing

Physical Access Control

Data Retention

Limit data storage and retention to that required for business, legal or regulatory purposes.

Data should be kept unreadable anywhere it is stored, including in backups and logs.

Protect cryptographic keys from disclosure and misuse.

Vulnerability Management

Ensure all systems are up-to-date

- Vulnerability Scanners
- Anti-virus
- Operating Systems
- Vendor Supplied Software

Regularly scan systems for known vulnerabilities

- Nessus
- Anti-virus

Mitigate vulnerabilities in custom software

- Code reviews (not by author)
- Train developers in secure coding methodologies

Electronic Access Control

Deny all access to anyone who is not specifically allowed to access client data

Ensure proper authentication using two-factor authentication

All access to client and sex worker information requires approval from one executive and legal.

Physical Access Control

Use facility entry controls to limit and monitor physical access to systems

The server and backup infrastructure are offsite.

Physical workstation (USB) access, electronic, or camera devices may not be permitted in certain locations or roles.

Networking

Any change should invoke formalized testing to make sure the infrastructure works as expected.

Minimize the surface area of the network that is internet facing.

Deny all traffic by default, except what’s necessary for the product.

Only use high-level, well-vetted encryption schemes for communication security.

Monitoring

Any employee, user, or system component should have a unique ID.

Verify that audit trails are secure and cannot be altered by anyone.

Perform regular audits to reconstruct system and employee to customer interactions to find irregularities.

Use log visualization and management solutions to spot anomalous behavior.

Testing

Perform annual penetration testing--or especially after any significant infrastructure or application change.

Stage changes to your test environment before pushing a new release to the production environment.

Deploy file integrity monitoring to the server so administrators can be alerted to unauthorized modification of system files.

Summary

What is Hüber

What to Protect

How to Protect

Hüber

Pleasure you want,
Protection you deserve

Full project paper: http://bit.ly/1XN3Uwp