Pixelated Protection:
Identifying Security Challenges in Game Development Processes

Philip Klostermeyer, Sabrina Amft, Niklas Busch, Alexander Krause, Sascha Fahl
CISPA Helmholtz Center for Information Security, *{philip.klostermeyer, sabrina.amft, niklas.busch, alexander.krause, sascha.fahl}@cispa.de*

s.gwdg.de/4Orjxr

Motivation

*"Whether it's DDoS [...], credential abuse, or application attacks, the gaming industry is popular in the worst of ways: **as the target**."*

State of the Internet Security
Web Attacks and Gaming Abuse
(Volume 5, Issue 3) | Akamai, 2019

- Video game market has grown immensely in user reach and revenue
- Easy access / free-to-play makes it easy for young users to gain access
- Status quo of the industry in dealing with security is largely unexplored

Research Questions

RQ1. How do security vulnerabilities end up in video game software?

RQ2. What methods, guidelines, concepts, and practices does the industry rely on to ensure the security of its products?

RQ3. What recommendations can be developed that can improve planning, development, deployment, and maintenance of security components in video games?

Methodology

- Semi-structured interviews with industry insiders
- ERB approved
- 2 pilot + 13 full interviews conducted so far

1. Design ✓
Drafting of research questions, search for related work and subsequent design of an interview guide on the basis of the available knowledge.

↓

2. Pre-Pilot ✓
Piloting the interview guide with two stakeholders from the video games industry (convenience sampling). Improving structure and content of the guide, refining focus and questions.

↓

3. Advertisement ✓
Launch of website with necessary information. Promotion of the study (Upwork, Linkedin, Reddit, Discord, gamejobs.co, convenience/snowball sampling).

↓

4. Conducting the Interviews ⧗
Conducting the main body of the interviews. Minor adaptations of interview guide (e.g. adding examples when there was ambiguity, rephrasing, etc.).

↓

5. Iterative Coding Process ⧗
Two researchers agree on initial codebook based on RQs. Afterwards, coding all transcribed interviews. Iterative resolution of conflicts and minor revisions of the codebook if necessary.

↓

6. Affinity Diagramming ⧗
Using Affinity Diagramming to group codes under similar topics, streamline the code set, and identify major categories to report in the analysis.

Selected Findings

- Security is an optional feature

  "[...] time is money. [...] in every single project I've ever worked on, there are sacrifices that were made to reach that deadline."

- Security awareness less common

  "[Security is] not a topic you see discussed very often. The times when it is, [...] there's a big controversy surrounding it."

- Aftercare instead of prevention, acting mainly after incidents

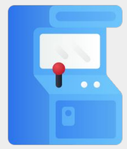
  "[...] when it directly affects the publishers, when they lose sales, then there was a high intrinsic motivation that you counteract."

- Unusual and proprietary tooling

  "[...] the tech is too primitive and they are not using [...] state-of-art tools [...], it's practically impossible for them to implement APIs, SDKs [...]."

- Special needs in network encryption

  "[...] they don't use any encryption because [that] requires a lot of traffic."



Intro
Introduction to the interview and obtaining verbal consent.

↓

1. Introduction, Importance of Security
Establish participant's background, explore security knowledge and perception within game development.

↓

2. Security Aspects, Guidance, Incidents & Causes
Deepen personal points of contact with security topics. Fathom if and what guidance and restrictions influence participant. Finally, explore incidents and causes.

↓

3. Tooling, External Components
Explore tooling environment, and whether security tooling is available. Also, explore development of external components and their validation.

↓

4. Testing, Maintenance
Explore testing and review processes, as well as subsequent maintenance strategy of the software.

↓

5. Recommendations & Roundup
Identify what is always important according to the participant regarding security, as well as identify additional measures that participants might take.

↓

Outro
Debrief and collect feedback for the interview.

1. Design phase
Drafting of research questions, search for related work on the topic and subsequent design of an interview guide on the basis of the available knowledge.

↓

2. Pre-Pilot
Testing the interview guide with two stakeholders from the video games industry (convenience sampling). Improving structure and content of the interview guide, refining focus of the study and questions of the guide.

↓

3. Advertisement phase
Online launch of the website with all necessary information. Promotion of the study on the platforms: Upwork, Linkedin, Reddit, Discord, as well as on industry recruitment websites (gamejobs.co). Also, using the personal network (convenience/snowball sampling).

↓

4. Conducting the interviews
Conducting the main body of the interviews. Minor adaptation of the interview guide (e.g. adding examples when there was ambiguity, adapting the wording, etc.).

↓

5. Iterative coding process
Two researchers agreed on an initial codebook based on the RQs and with consultation of related work. Afterwards, coding all transcribed interviews. Iterative resolution of conflicts and minor revisions of the codebook if necessary.

↓

6. Affinity Diagramming
Using Affinity Diagramming to group codes under similar topics, streamline the code set, and identify major categories to report in the analysis.

- money
- time
- motivation
- knowledge
- nobody likes, wants or knows about security

- What are the most difficult security-related components for insiders to work with in game development, and why?
- What methods, guidelines, concepts, and best practices does the industry rely on to ensure the security of its products?
- What recommendations can we derive on this topic for video game development, including from general software development, that can improve the development and deployment of security components in video games?

ID	Country	Industry exp. (years)	Emp.[1]	Comp./Team size (people)	Leading position	Security exp.[2]
1	CA	6-10	F	50-999	Y	Little
2	US	1-2	F	50-999	Y	Considerable
3	US	1-2	P	10-19	N	Considerable
4	LT	1-2	F	>1000	N	Some
5	PO	6-10	F	5-9	Y	Considerable
6	VD	>10	S/F	10-19	N	Considerable
7	ID	6-10	F	>1000	Y	Some
8	PT	>10	F	50-999	Y	Some
9	RO	>10	S/F	20-49	Y	Some

“[...] every single one of those teams should be using the same documentation, the same set standards for how to write code. There should be expectations in place so that if you hand that code off to somebody else within the organization, the negativity of having to deal with someone else's code is minimized.” - Producer

“I think [security is] going to become a bigger and bigger problem as things progress just because the way people are hacking, the way people are getting information is just becoming an ever bigger battle to keep your data secure.” - Producer

“[Security is] not a topic you see discussed very often. The times when it is, generally speaking, there's a big controversy surrounding it.” - Producer

“I feel like if hackers really wanted to get some form of data off of a game about the users, they could do it. I don't think the studio is making the games or the services that they're using for their online networking are focused enough on security to make any real impact on stopping people from breaching. That's just the world we live in, I think.” - Producer

“Investing more money into it is really the best thing I can think of as a project manager just because it's often not in the budget at all [...]” - Producer

I would say very little [knowledge] based on the conversations I've had over the last seven years of doing this. It's not a topic you see discussed very often.

[...] we are not enough secure about cheating because sometimes our user surprise us. Of course they are really smart guys and they can create some non-typical ways to achieve some benefits inside the game.

“For bigger studios, I don't think it's important enough. I think that it takes a back seat to just what makes the game more profitable.” - Producer

“[...] time is money. [...] in every single project I've ever worked on, there are sacrifices that are made to reach that deadline.” - Producer

“Things that the player doesn't see tend to get less attention. Security is just one of those [...]” - Producer

“in the real world, there are budgets, especially for released games, it's a balance between wanting to fix existing problems [...] and wanting to continue development of the game.” - Producer

[...] I use copilot and maybe it isn't the safety way because it knows about my code [...] - Dev

We use our copy paste tool for sharing some logs and maybe small code fragments between our team. - Dev

Once, all the code of our project was stolen, and some bans opened their own game server with our code. It's like a fancy. They managed to do it. - Dev

“[...] when it directly affects the publishers, when they lose sales, then there was a high intrinsic motivation that you counteract.”

After Russia-Ukraine situation, most of libraries included some damage code to not safely work in some regions by IP address, by language of platform, and it often damaged our other players not inside these territories. We have a table proven this safely libraries, with a safer version of each library. When we need to update some of library we check the code with open source, and make a decision, we need to update or not. - Dev