Threat modeling without the headache

Gazizova Svetlana

Head of Audit at Swordfish Security

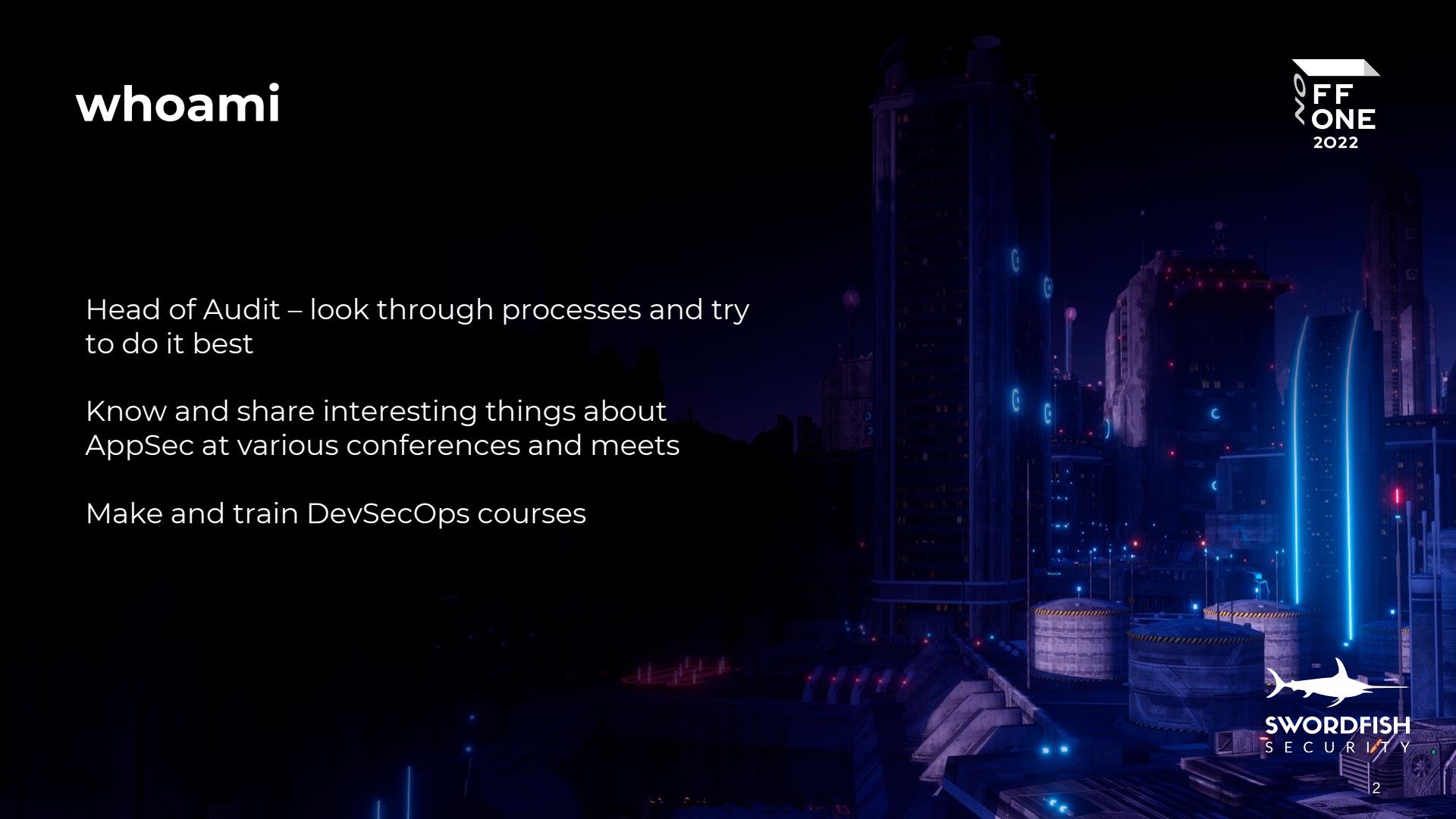
Moscow, August 26, 2022

whoami

Head of Audit – look through processes and try to do it best

Know and share interesting things about AppSec at various conferences and meets

Make and train DevSecOps courses



We will talk..

- What is Threat Modeling?
- What about classical approach to threat modeling? Does it work?
- Devs will never execute threat model requirements, because…
- If you want it precious – do it ~~yourself!~~ with another guys from another departments
- Decomposition and visibility – do not forget about it!
- Summary

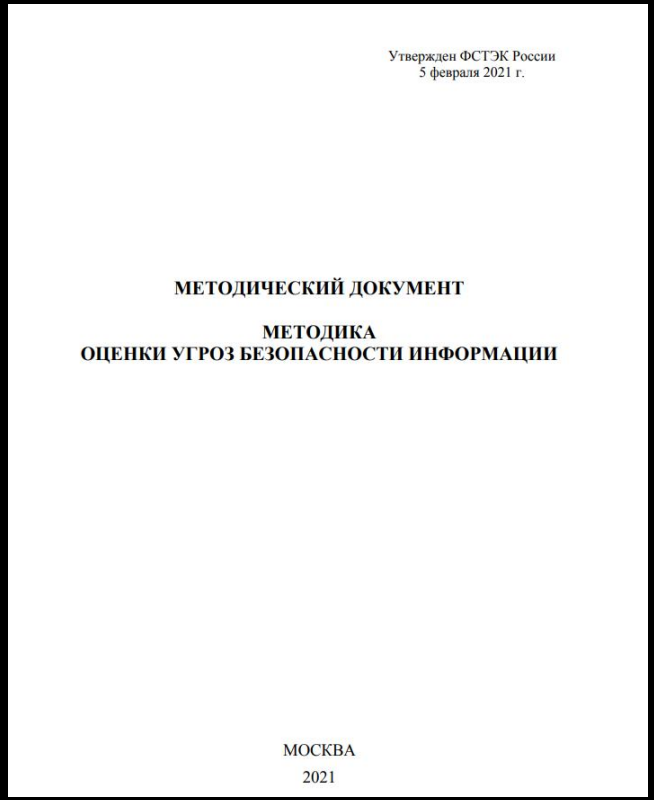
CHAPTER 1.
INTRODUCTION

What is Threat Modeling?

Threat modeling is a process by which potential threats, such as structural vulnerabilities or the absence of appropriate safeguards, can be identified and enumerated, and countermeasures prioritized. The purpose of threat modeling is to provide defenders with a systematic analysis of what controls or defenses need to be included, given the nature of the system, the probable attacker's profile, the most likely attack vectors, and the assets most desired by an attacker. Threat modeling answers questions like *“Where am I most vulnerable to attack?”*, *“What are the most relevant threats?”*, and *“What do I need to do to safeguard against these threats?”*.

https://en.wikipedia.org/wiki/Threat_model

What is Threat Modeling?



Утвержден ФСТЭК России
5 февраля 2021 г.

МЕТОДИЧЕСКИЙ ДОКУМЕНТ

МЕТОДИКА
ОЦЕНКИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

МОСКВА
2021

https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/2170-metodicheskij-dokument-utverzhden-fstek-rossii-5-fevralya-2021-g

How we do it?

STRIDE

PASTA

DREAD

Threat Dragon

...

How we do it?

STRIDE

PASTA

DRE

Threat Dra n

...

To infinity and beyond!

What is the purpose?

To have smthg to show
because we work with personal
data...

Well.. what is the *real* purpose?

To understand what we should protect and how we should protect it.

Risk assurance, quality management, threat intelligence etc

And threat model is ...

Just a 100-pages document that will never be read :)

P.S. From start to end:)

CHAPTER 2.
PROBLEMS&SOLUTIONS

Major problems

1. Template!

Major problems

1. Template!

2. People who can’t defend information!

Major problems

1. Template!

2. People who can’t defend information!

3. People who can’t influence at security!

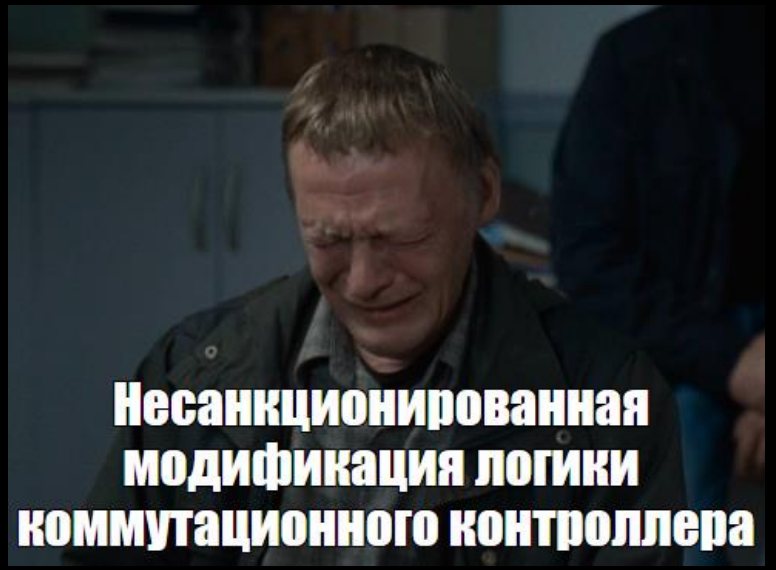
Major problems

1. Template!

2. People who can’t defend information!

3. People who can’t influence at security!

4. SLANG!



Major problems

1. Template!

2. People who can’t defend information!

3. People who can’t influence at security!

4. SLANG!

5. 0-Intellectual costs!

Major problems

5. 0-intellectual costs

2.3. Исходными данными для оценки угроз безопасности информации являются:

а) общий перечень угроз безопасности информации, содержащийся в банке данных угроз безопасности информации ФСТЭК России (bdu.fstec.ru), модели угроз безопасности информации, разрабатываемые ФСТЭК России в соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. № 1085, а также отраслевые (ведомственные, корпоративные) модели угроз безопасности информации;

б) описания векторов (шаблоны) компьютерных атак, содержащиеся в базах данных и иных источниках, опубликованных в сети «Интернет» (CAPEC, ATT&CK, OWASP, STIX, WASC и др.);

в) документация на системы и сети (а именно: техническое задание на создание систем и сетей, частное техническое задание на создание системы защиты, программная (конструкторская) и эксплуатационная (руководства, инструкции) документация, содержащая сведения о назначении и функциях, составе и архитектуре систем и сетей, о группах пользователей и уровне их полномочий и типах доступа, о внешних и внутренних интерфейсах, а также иные документы на системы и сети, разработка которых предусмотрена требованиями по защите информации (обеспечению безопасности) или национальными стандартами);

г) договоры, соглашения или иные документы, содержащие условия использования информационно-телекоммуникационной инфраструктуры центра обработки данных или облачной инфраструктуры поставщика услуг

д) нормативные правовые акты Российской Федерации, в соответствии с которыми создаются и функционируют системы и сети, содержащие в том числе описание назначения, задач (функций) систем и сетей, состав обрабатываемой информации и ее правовой режим;

е) технологические, производственные карты или иные документы, содержащие описание управленческих, организационных, производственных и иных основных процессов (бизнес-процессов) в рамках выполнения функций (полномочий) или осуществления видов деятельности обладателя информации, оператора (далее – основные (критические) процессы);

ж) результаты оценки рисков (ущерба), проведенной обладателем информации и (или) оператором.

Major problems

5. 0-intellectual costs

Окончание таблицы 4.1

№	Виды риска (ущерба)	Возможные типовые негативные последствия
		Доступ к персональным данным сотрудников органов государственной власти, уполномоченных в области обеспечения обороны, безопасности и правопорядка, высших должностных лиц государственных органов и других лиц государственных органов. Доступ к системам и сетям с целью незаконного использования вычислительных мощностей. Использование веб-ресурсов государственных органов для распространения и управления вредоносным программным обеспечением. Утечка информации ограниченного доступа. Непредоставление государственных услуг

Указанные типовые негативные последствия от реализации угроз безопасности информации подлежат конкретизации и могут дополняться другими негативными последствиями в зависимости от особенностей области деятельности, в которой функционирует система и сеть.

What should we correct?

1. Threat modeling should be “ASAP before” dev stage

2. Do not do it only to compliance specialists

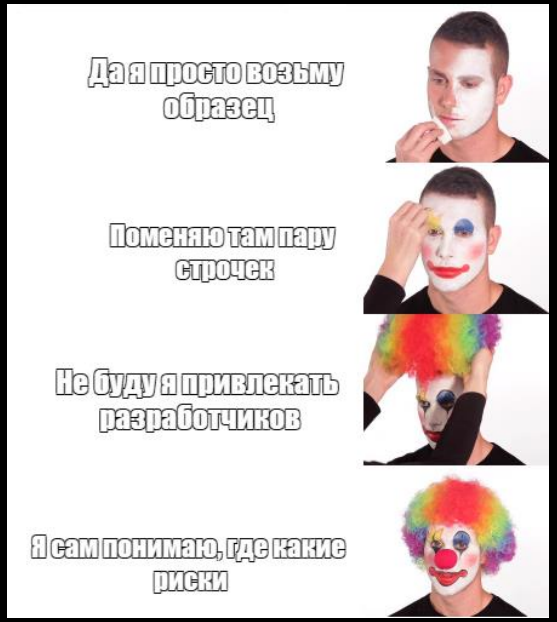
3. Make Threat Modeling a Process – Not a Task in Jira or Kaiten

Keep it simple! Or...

You MUST be compliant!

Keep it simple! Or...

Show the value of this process for another!



Keep it simple! Or...

Ask for support!

CHAPTER 3.
OUR CASE

Our case

Once upon a time...

We received a request for a threat model. Not anyhow - but interesting, which no one has done yet!

We went to think and...

Our case

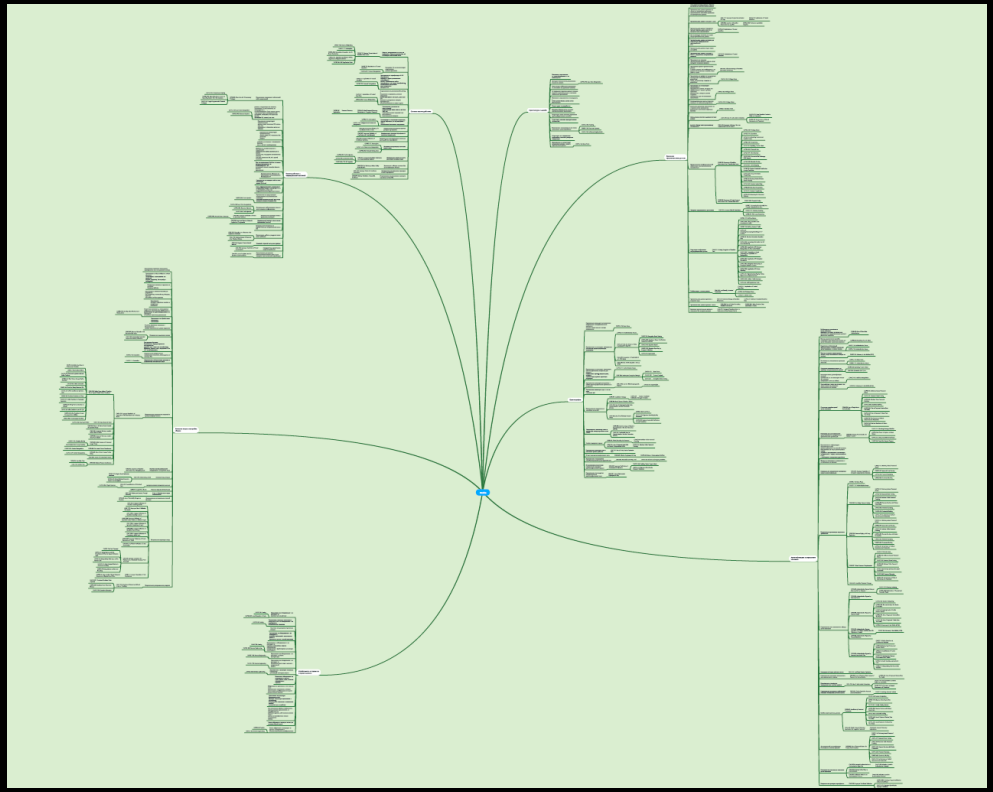
And we understood one big problem. It is a question...

Our case

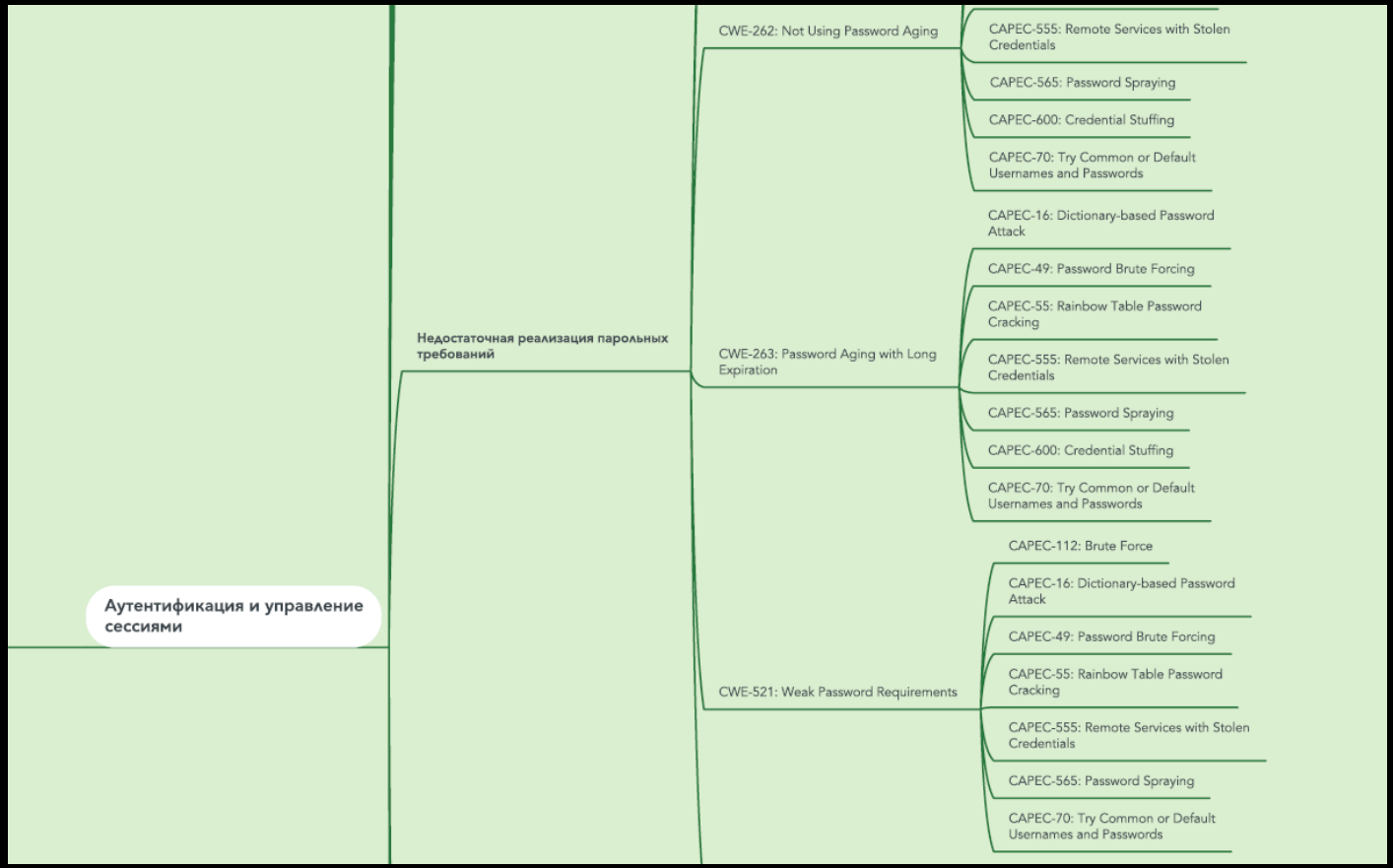
And we understood one big problem. It is a question...

Why everyone use just threats not a vulns?

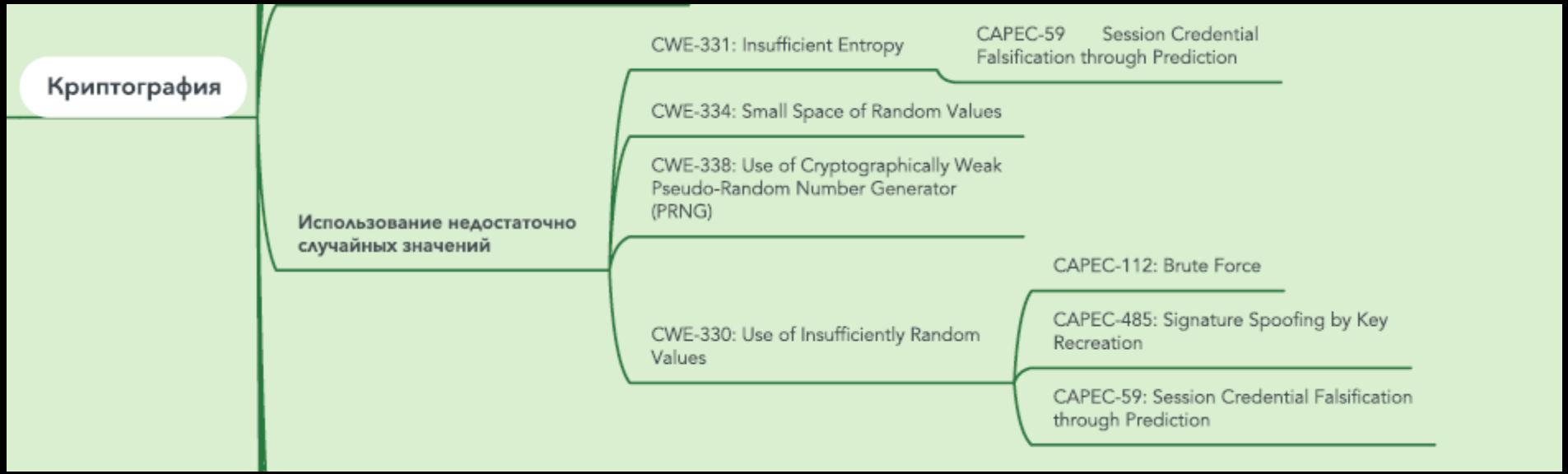
Our case



Our case


Аутентификация и управление сессиями
Недостаточная реализация парольных требований
CWE-262: Not Using Password Aging
CAPEC-555: Remote Services with Stolen Credentials
CAPEC-565: Password Spraying
CAPEC-600: Credential Stuffing
CAPEC-70: Try Common or Default Usernames and Passwords
CWE-263: Password Aging with Long Expiration
CAPEC-16: Dictionary-based Password Attack
CAPEC-49: Password Brute Forcing
CAPEC-55: Rainbow Table Password Cracking
CAPEC-555: Remote Services with Stolen Credentials
CAPEC-565: Password Spraying
CAPEC-600: Credential Stuffing
CAPEC-70: Try Common or Default Usernames and Passwords
CWE-521: Weak Password Requirements
CAPEC-112: Brute Force
CAPEC-16: Dictionary-based Password Attack
CAPEC-49: Password Brute Forcing
CAPEC-55: Rainbow Table Password Cracking
CAPEC-555: Remote Services with Stolen Credentials
CAPEC-565: Password Spraying
CAPEC-70: Try Common or Default Usernames and Passwords

Our case


Криптография
Использование недостаточно случайных значений
CWE-331: Insufficient Entropy
CAPEC-59 Session Credential Falsification through Prediction
CWE-334: Small Space of Random Values
CWE-338: Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG)
CWE-330: Use of Insufficiently Random Values
CAPEC-112: Brute Force
CAPEC-485: Signature Spoofing by Key Recreation
CAPEC-59: Session Credential Falsification through Prediction

Our case

Угроза	Оценка критичности	Причина угрозы	Способ противодействия угрозе	Домен MASVS	OWASP TOP-10	CWE	CAPEC
Угроза несанкционированного доступа к конфиденциальным данным пользователя в следствии некорректного хранения данных на устройстве	Высокая	Использование жестко заданных учетных данных	Не предусмотрена возможность хардкодить учетные данные	Хранение чувствительных данных	M2 Insecure Data Storage	CWE-798: Use of Hard-coded Credentials	CAPEC-191: Read Sensitive Constants Within an Executable CAPEC-70: Try Common or Default Usernames and Passwords
	Критическая	Доступ к бэкапу неавторизованному пользователю	Не предоставлять возможность доступа к бэкапу	Хранение чувствительных данных	M2 Insecure Data Storage	CWE-530: Exposure of Backup File to an Unauthorized Control Sphere	
	Критическая	Предоставление конфиденциальной информации неавторизованному пользователю	Неавторизованному пользователю предоставляется доступ к минимально необходимому набору данных	Хранение чувствительных данных	M2 Insecure Data Storage	CWE-200: Exposure of Sensitive Information to an Unauthorized Actor	CAPEC-122: Privilege Abuse CAPEC-116: Excavation CAPEC-13: Subverting Environment Variable Values CAPEC-169: Footprinting CAPEC-22: Exploiting Trust in Client CAPEC-224: Fingerprinting CAPEC-497: File Discovery CAPEC-290: Enumerate Mail Exchange (MX) Records
						CWE-359: Exposure of Private Personal Information to an Unauthorized Actor	CAPEC-508: Shoulder Surfing

Our case

And mitigation scenario of course!

Our case

We used:

Patterns database:	Threat database:	Vuln database:
MITRE CAPEC	FSTEC GOST 58412 …	CVE (+CVSS 3.0) Snyk Vulnerability NVD

Our case

mind :)

Threat/vuln database:

FSTEC
GOST 58412
...
And some mind:)

- Secure coding guidelines
- AST reports
- Attacks histories
- ASVS/MASVS
- WSTG/MSTG
- Architecture checklists
- General requirements

What else you can use?

Summary

1. It’s all better with mental effort!
2. Try to do it process, not a stage
3. Decomposition and visibility – 50% solving big problem

Вопросы, пожелания, комментарии

tg @gazizovasg

sgazizova@swordfishsecurity.com