Expert Knowledge Elicitation for Skill Level Categorization of Attack Paths

Terézia Mézešová
Pavol Jozef Šafárik University
Slovakia

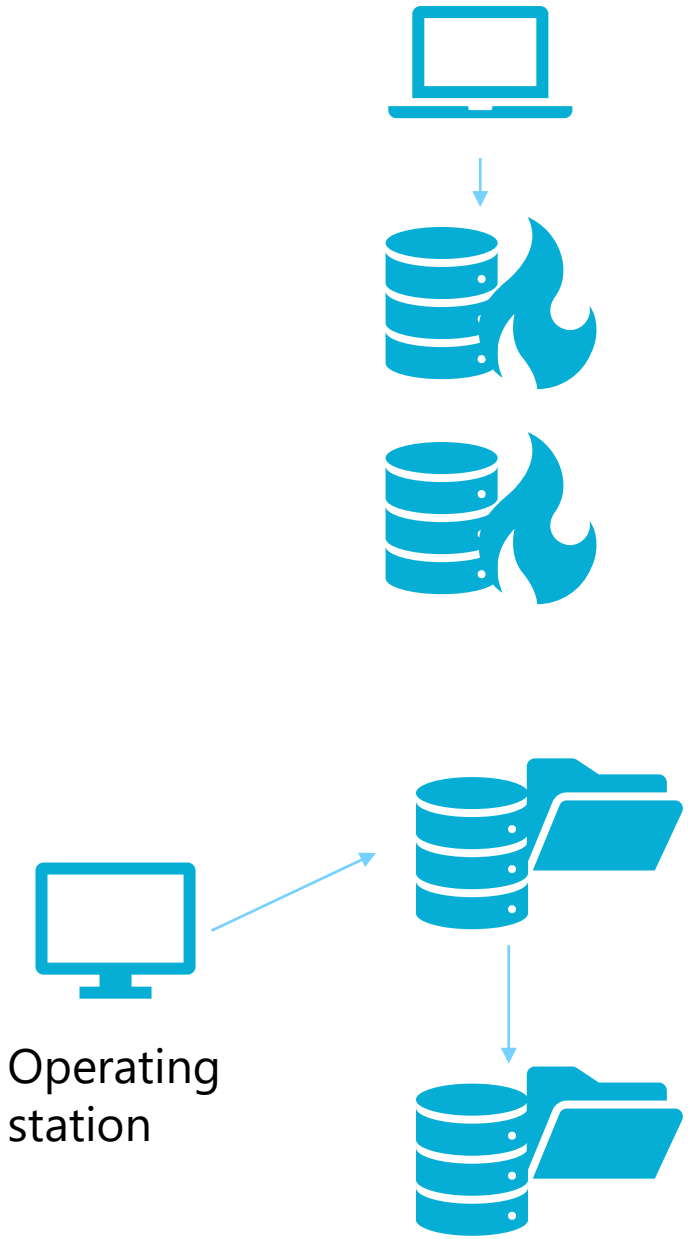
Hayretdin Bahsi
Tallinn University of Technology
Estonia

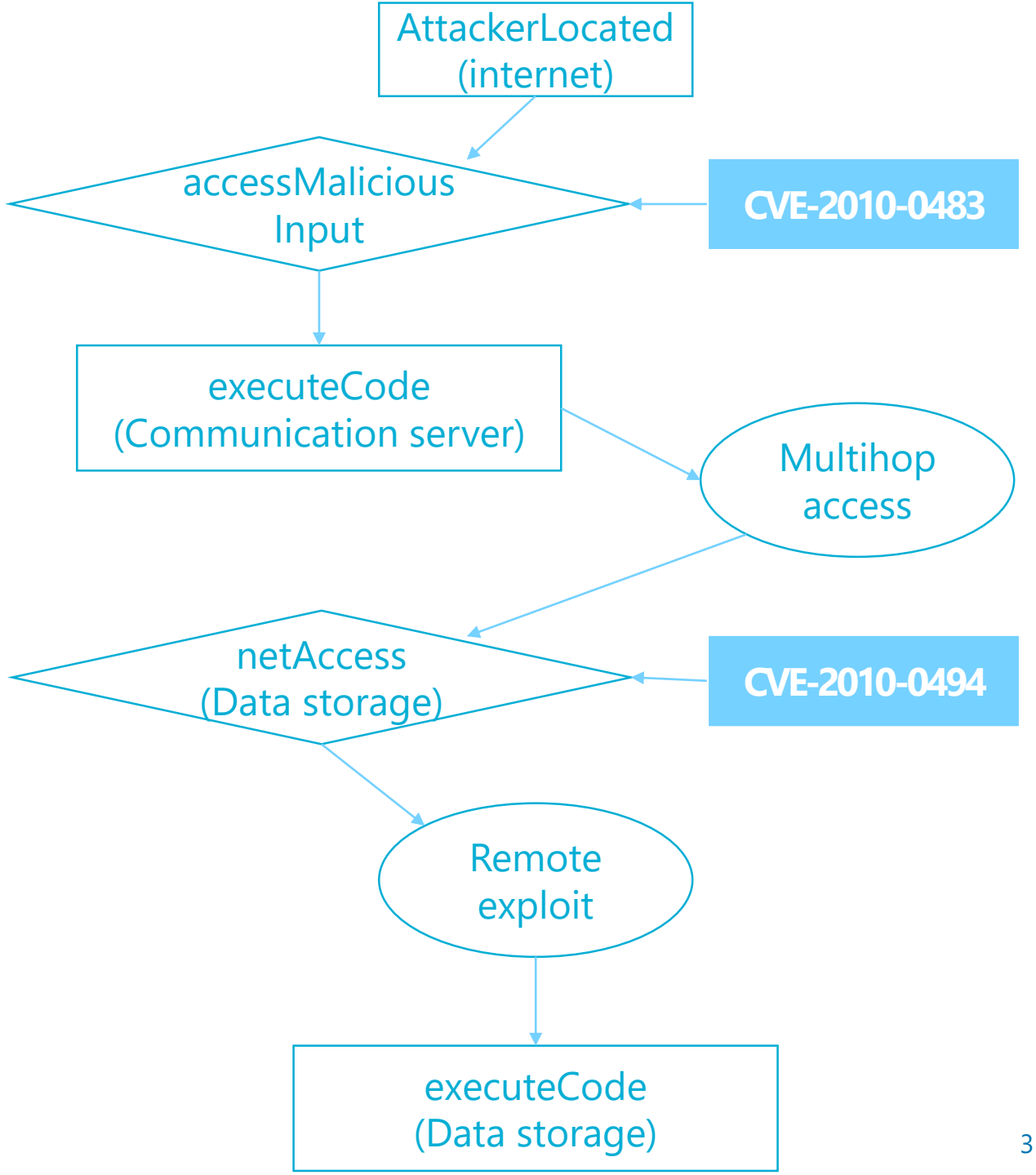
“

attack path

SEQUENCE OF VULNERABILITIES
AN ATTACKER NEEDS TO EXPLOIT
TO REACH A TARGET IN A NETWORK

systematic comparison ? of intrusion scenarios


Attacker (internet)
Perimeter firewall
Internal firewall
Communication server
Operating station
Data storage


AttackerLocated (internet)
accessMalicious Input
CVE-2010-0483
executeCode (Communication server)
Multihop access
netAccess (Data storage)
CVE-2010-0494
Remote exploit
executeCode (Data storage)

Expert Knowledge Elicitation

0

8 experts

CSIRT

pentesting

1

Understand key skills for attackers

2a

Identify concrete skills sets for attacker categories

2b

Map CVSS metrics values to attackers skills

Elicitation conclusion | Skill Level Categorization

Script Kiddies

run downloaded scripts

configure exploits

obtain leaked credentials

use malware

use brute force methods

Moderately Skilled Attackers

knowledge of attacking tools

reproduce proof of concepts

engage user's action

pass multiple authn gates

hide traces afterwards

High Skilled Attackers

in-depth technical know-how

write functional exploits

demonstrate PoCs

hide on the network

Skill Level Categorization | CVSS Basic score

Attack Vector

Network :	Script Kiddies
Adjacent | Local :	Moderately Skilled
Physical :	–

User Interaction

None :	Script Kiddies
Required :	Moderately Skilled

Privilege Required

None | Low :	Script Kiddies
High :	Moderately Skilled

Authentication

None | Single :	Script Kiddies
Multiple :	Moderately Skilled

Skill Level Categorization | CVSS Temporal score

Exploit Code Maturity

High :	Script Kiddies
Functional | Proof of Concept :	Moderately Skilled
Unproven :	Highly Skilled

Report Confidence

Confirmed :	Script Kiddies
Reasonable :	Moderately Skilled
Unknown :	Highly Skilled

Skill Level | Difficulty of vulnerability d(v)

$$d(v) = \max(m^{AV}, m^{PR}, m^{UI}, m^{Au}, m^{EC}, m^{RC})$$

CVE-2010-0483

Attack Vector: Network, Privilege Required: None, User Interaction: Required, *Authentication: None*, Exploit Code Maturity: High, Report Confidence: Confirmed

m^{AV}=Script Kiddies, m^{PR}=Script Kiddies, m^{UI}=Moderately Skilled, m^{Au}=Script Kiddies, m^{EC}=Script Kiddies, m^{RC}=Script Kiddies

assigned level: **Moderately Skilled Attacker**

Skill Level | Difficulty of vulnerability d(v)

$$d(v) = \max(m^{AV}, m^{PR}, m^{UI}, m^{Au}, m^{EC}, m^{RC})$$

CVE-2010-0483

Attack Vector: Network	m^{AV} = Script Kiddies
Privilege Required: None	m^{PR} = Script Kiddies
User Interaction: Required	m^{UI} = Moderately Skilled
Authentication: None	m^{Au} = Script Kiddies
Exploit Code Maturity: High	m^{EC} = Script Kiddies
Report Confidence: Confirmed	m^{RC} = Script Kiddies

assigned level: **Moderately Skilled Attacker**

Skill Level | Difficulty of Attack Path D(P)

$$D(P) = \max(d(v_i) \text{ where } i \in \{1...n\})$$

1. CVE-2010-0483 (Moderately Skilled)
2. CVE-2010-0494 (Moderately Skilled)

assigned level: **Moderately Skilled Attacker**

Conclusion

Express required skill level for exploitation of an attack path

Prepare balanced hands-on offensive cyber exercises

Thank you for your attention.

terezia.mezesova@outlook.com

hayretdin.bahsi@ttu.ee