КОНКУРС ПЕРЕВОДЧИКОВ

НАУЧНО-ТЕХНИЧЕСКОЙ ЛИТЕРАТУРЫ ПО ЭЛЕКТРОЭНЕРГЕТИЧЕСКОЙ И ЭЛЕКТРОТЕХНИЧЕСКОЙ ТЕМАТИКАМ (АНГЛИЙСКИЙ ЯЗЫК)

Захаров Ярослав Алексеевич

CYBERSECURITY THREATS TO P&C SYSTEMS

НОЯБРЬ, 2019

cigre Россия

РОССЕТИ ФСК ЕЭС

АО «СО ЕЭС»

НАДЁЖНАЯ СМЕНА

САМАРСКИЙ ПОЛИТЕХ Опорный университет

INTRODUCTION TO DEVELOPMENT VULNERABILITIES

- The most common cybersecurity flaw is a vulnerability that provides the means to inject malicious code into the P&C system software. The primary reason to consider this type of attack is that it can allow an individual to bypass the access control restrictions set by the developer or EPU's P&C engineer. For instance, to gain complete control of a protection relay from a remote location or to escalate user privileges to "administrator" on a protection relay. Typically, administrator privilege includes the capability to change the privileges of other users. Code injection attacks can be realized as binary code injection attacks or source code injection attacks.

CODE INJECTION

Code injection classes include the following vulnerabilities/weaknesses:

- cross-site scripting
- SQL injection
- LDAP injection
- mail command injection
- null-byte injection
- operating system commanding
- server side injection
- extensible markup language (XML)
- external entities
- XML Injection
- XQuery Injection

VULNERABILITIES INTRODUCED DURING DEPLOYMENT AND MAINTENANCE

- Remote access trust issues
- Firewall configuration errors
- On-line password guessing
- Off-line password guessing
- Inadequate access controls
- Social engineering
- Network traffic analysis and manipulation

THREAT LANDSCAPE & SELECTION OF VIABLE THREATS

Generally, the number of potential vulnerabilities increases with the functionality of the asset.

Another important concept is the severity of the different consequence resulting from an exploit of the vulnerabilities. For instance, offline password guessing may be a small issue of many P&C systems, as it typically requires the attacker to have some privileges on the system.

Many social engineering attacks involve emails containing links to websites with exploit kits. In essence, an attacker must accomplish two tasks:

1) social engineer personnel to access the link in the email, and

2) exploit a vulnerability in the web browser (often a buffer overflow) of the connecting individual.

THANKS FOR YOUR ATTENTION