
SIEMENS
纵深防御 信息安全
西门子工业信息安全解决方案助力企业更上一层楼

SIEMENS

西门子中国研究院，2014

协议健壮性测试
–及其在工控信息安全领域的应用

信息安全的新战场－工业基础设施

工业基础设施构成了我国国民经济、现代 社会以及国家安全的重要基础，而工业基础设施的核心是其工业控制系统（ICS）

与传统的IT信息安全不同，工业基础设施中关键ICS系统的安全事件会导致：

- 系统性能下降，影响系统可用性
- 关键控制数据被篡改或丧失
- 失去控制
- 环境灾难
- 人员伤亡
- 公司声誉受损
- 危及公众生活及国家安全
- 破坏基础设施
- 严重的经济损失等

工业信息安全变得日益重要

导致自动化工厂脆弱性的主要趋势：

- 在所有网络层次上的横向与垂直集成
- 将自动化网络与IT网络相连，以及为实现远程维护与Internet连接
- 越来越多采用开放标准以及基于PC的系统
- 各种潜在的安全威胁日益增长
  - 未授权人员的非法访问
  - 间谍活动、非法操纵控制数据
  - 由于恶意软件导致的数据丢失、损坏等等

越来越多的安全事件揭示出自动化工厂存在安全脆弱性！

ICS安全测试：尽早发现并修复安全缺陷

SIEMENS

Port Scanner

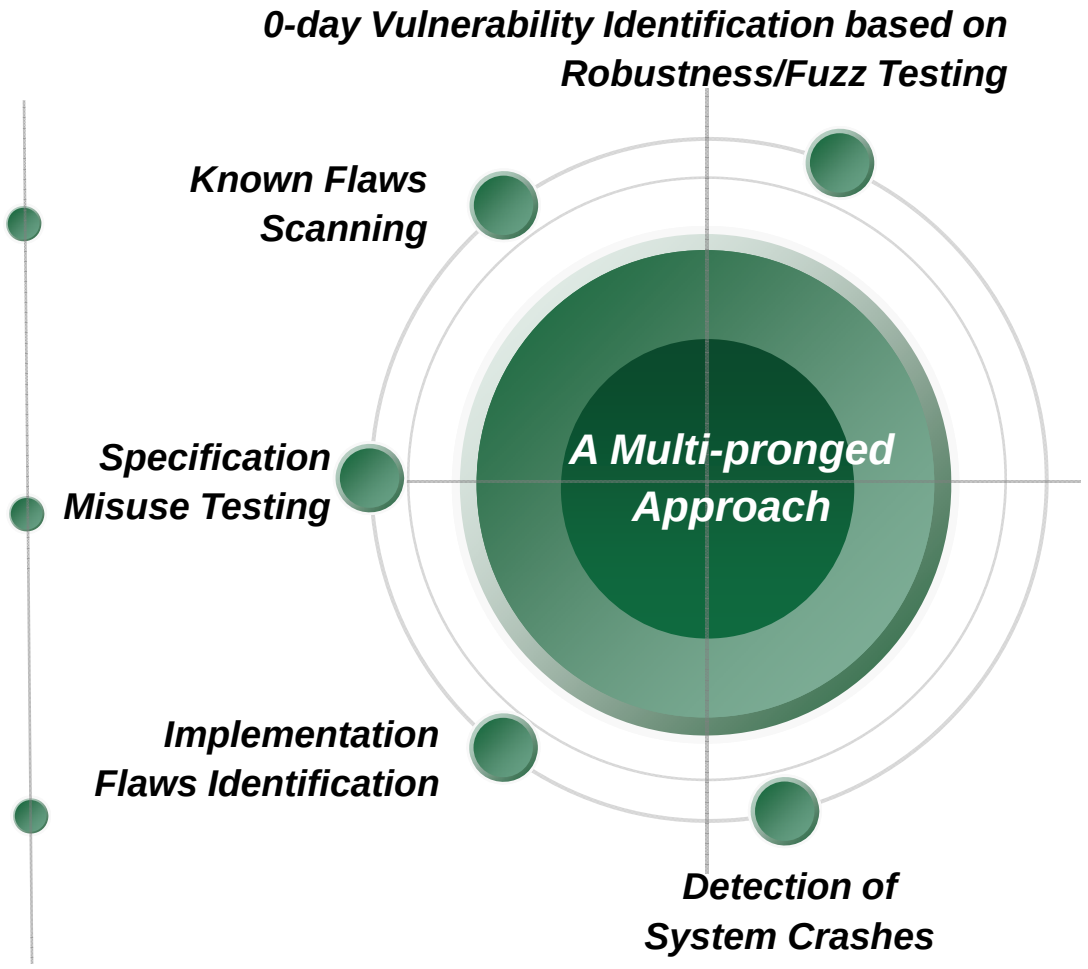
- Little recognition of ICS protocols and devices
- Some PLCs are known to fail when scanned aggressively

Vulnerability Scanner

- Poor granularity
- Lots of false positives
- Lack of the ability to identify 0-day vulnerabilities

Penetration Testing Tool

- Test of the tester rather than test of the system
- Stop at the first success: miss of more serious threats



健壮性测试（Fuzz Testing）

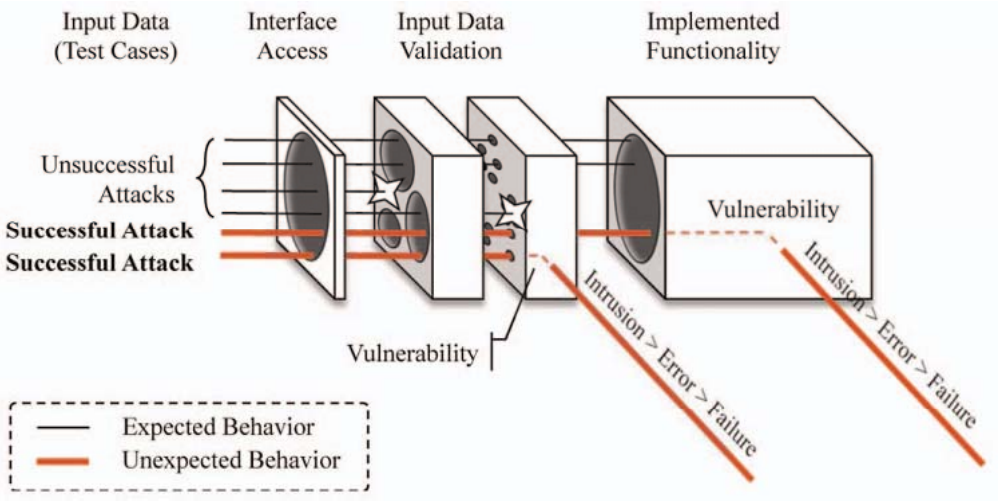
自1990年以来，健壮性测试（或称为模糊测试，fuzz testing）作为一种新型的黑盒测试技术在检测软件、产品及系统中存在的安全漏洞方面取得了显著的成功。

借助于健壮性测试，有可能在系统测试阶段检测出那些可能会被忽略的产品或系统缺陷。由于健壮性测试的成本相对较低并且可以自动化，健壮性测试技术近年来在网络协议实现的安全性测试领域正得到日益广泛的应用。

健壮性测试所发现的产品、系统故障多数是非常严重的，可被黑客所利用的安全缺陷。

协议健壮性测试：分类

J. Antunes等人在其文章“*Vulnerability Discovery with Attack Injection*”（*IEEE Transactions on Software Engineering, Vol. 36, No. 3, pages 357-370, 2010.*）首先针对被测系统提出了一个非常有用的模型，将其划分为三个层次：



- 输入访问（input access）
- 输入数据验证（input data validation）
- 实现的功能（implemented function）

这些层次构成了软件或协议实现可能受到攻击的三个不同的平面（attacking surface）。

与此相对应，根据可能成功渗透到的实现逻辑的层次，可以将模糊测试划分为三类：

- 随机模糊测试（Random fuzzing）
- 文法模糊测试（Syntax fuzzing）
- 综合模糊测试（Synthesized fuzzing）

随机模糊测试（Random Fuzzing）

1990年，B.P. Miller发现由于雷电引起的错误的输入指令可以导致Unix操作系统中的应用程序崩溃，受此启发提出了模糊测试的概念，并用fuzzing（或fuzz testing）命名此类测试。

最初的模糊测试（或健壮性测试）只是简单地将随机数据作为输入测试不同操作系统（B.P. Miller对POSIX Unix和Windows NT进行了测试）的API或应用程序。其基本思想是将一组随机数据作为程序的输入，同时监视程序运行过程中是否出现异常，并通过记录导致异常的输入数据以定位出软件中缺陷。因此可以将此类模糊测试技术归类为随机测试一种。

随机模糊测试的优点是比较简单，易于实现，在测试实践中采用这种方法也发现了很多安全缺陷。但其缺点也同样明显，随机模糊测试仅能渗透到协议实现逻辑最外面的输入访问层。由于网络协议通常都会定义其报文的文法格式，而协议实现或多或少地都会根据协议规范对输入报文进行格式检查，所以纯粹的随机输入通常无法对协议实现进行有效的测试。

文法模糊测试（Syntax Fuzzing）

协议网络报文的文法处理是一个复杂而易于出错的过程，尤其是当报文字段采用了编码（如ASN.1）时。不恰当的编码实践可能会在协议实现中遗留下严重的缺陷。而协议健壮性就是要力争发现这些隐藏在数据验证层的问题。

因此，协议健壮性测试技术也相应地进化到了文法测试阶段。

文法模糊测试基于协议实现（在协议规范中定义）的报文文法，有意将畸形的文法元素注入到测试报文，或对合法的报文进行变异，从而试图触发协议实现中有缺陷的代码，导致协议规范中规定的操作遭到破坏。

目前，属于文法模糊测试的工具有很多，比较有代表性的是PROTOS、SPIKE、Sully与Peach。

开源文法模糊测试工具

SPIKE 是Dave Aitel开发的模糊测试工具。SPIKE首先提出了通用（不局限于某个协议）的模糊测试框架（或称模糊测试生成工具）的概念，并提供了开源工具。研究者基于SPIKE框架开发出的各种协议安全测试套件，发现了很多著名的安全漏洞。SPIKE提供了一组用C实现的脚本原语，在此基础上用户可以用特定的脚本描述协议报文的文法格式。从而实现了被测协议逻辑（报文文法）与模糊测试的实现逻辑的分离，用户不需要关注模糊测试的实现细节，只需要根据被测协议的报文撰写对应的测试脚本即可。

与SPIKE类似的另一个开源工具是基于Python实现的Sully。

Peach是另一款非常著名的跨平台开源模糊测试框架，最早的版本发布于2004年，采用Python编写。但其3.0版本转为基于.Net平台，采用C#重写了整个代码。在Peach中，用户可以定义基于XML的Peach Pit文件，用于描述测试报文格式，变异方式，乃至协议状态机。

综合模糊测试（ **Synthesized fuzzing** ）

尽管面向协议报文文法的模糊测试技术在协议安全与健壮性测试领域取得了显著的成绩，但文法模糊测试的局限性在于其仅仅渗透到了J. Antunes模型的输入数据验证层，更深层次的协议功能逻辑还少有触及。

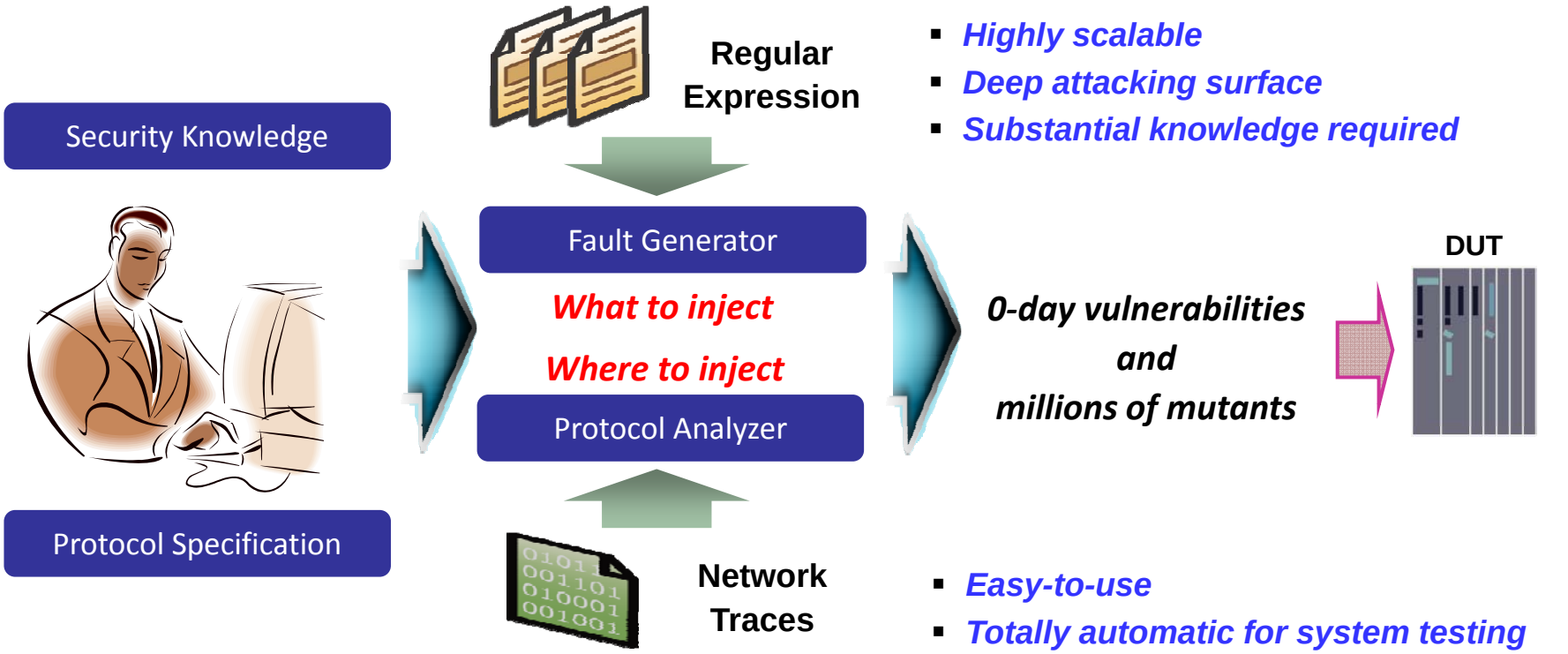
包括工控协议在内的网络协议的目的是定义一种标准的通信语言。其中，

- 文法规则定义了报文格式
- 行为规则定义了交互数据的语义与功能

而协议文法是与其语义及功能紧密相关的。例如，某个报文字段的有效取值是由协议文法所定义，但同时该字段的不同取值可能会触发协议实现的不同（响应）行为。因此，更完备、彻底的协议安全与健壮性测试应当能够综合地考虑协议规范的报文文法和行为模型。

Styx: Security Testing System for Protocol X

2007年开始研发，目前已被西门子德国的多个业务集团用于系统测试。



Supported Protocols

Protocol	Covered PDU	Scripts	Mutant
OMS	1	3	376,865
S7-Communication	6	18	292,211
TPKT	1	3	15,743
COTP	1	3	224,103
LLDP	1	3	831,424
PN-DCP	5	15	444,243
PN-CM	2	6	323,417
PN-MRP	2	6	223,213
PN-PTCP	1	3	107,300
DCE-RPC over UDP	1	3	40,511
MMS	2	6	213,248
Ethernet	3	19	27,532
ARP	2	8	16,111
SNMPv1	3	9	568,259
SNMPv3	3	9	1,544,784
SSLv3	3	9	378,491
Total	37	131	5,637,857

PROFINET Wall - Secured PROFINET Cell

Industrial Security Wall - Security for Control Cells

Industrial Security Lab – Testbed (1)

谢谢！ Q&A

SIEMENS

Dr. Tang Wen 唐文
AIT CT SLC

Address: 7, Wangjing Zhonghuan Nan Lu, Chaoyang District Beijing 100102 P. R. China

Phone: 010-64766526

Mobile: 13910115182

E-mail: wen.tang@siemens.com

siemens.com/innovation