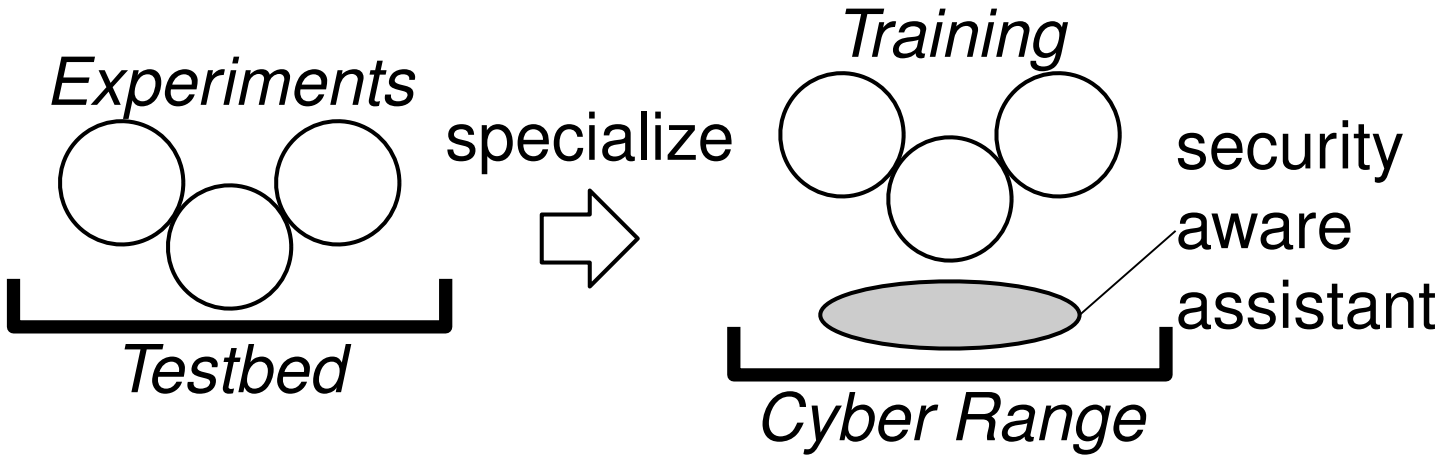
# The Concept of Security Training Management

Ken-ichi Chinen

**北陸先端科学技術大学院大学 情報科学研究科 サイーバレンジ構成学**
Cyber Range Organization and Design,
School of Information Science,
Japan Advanced Institute of Science and Technology

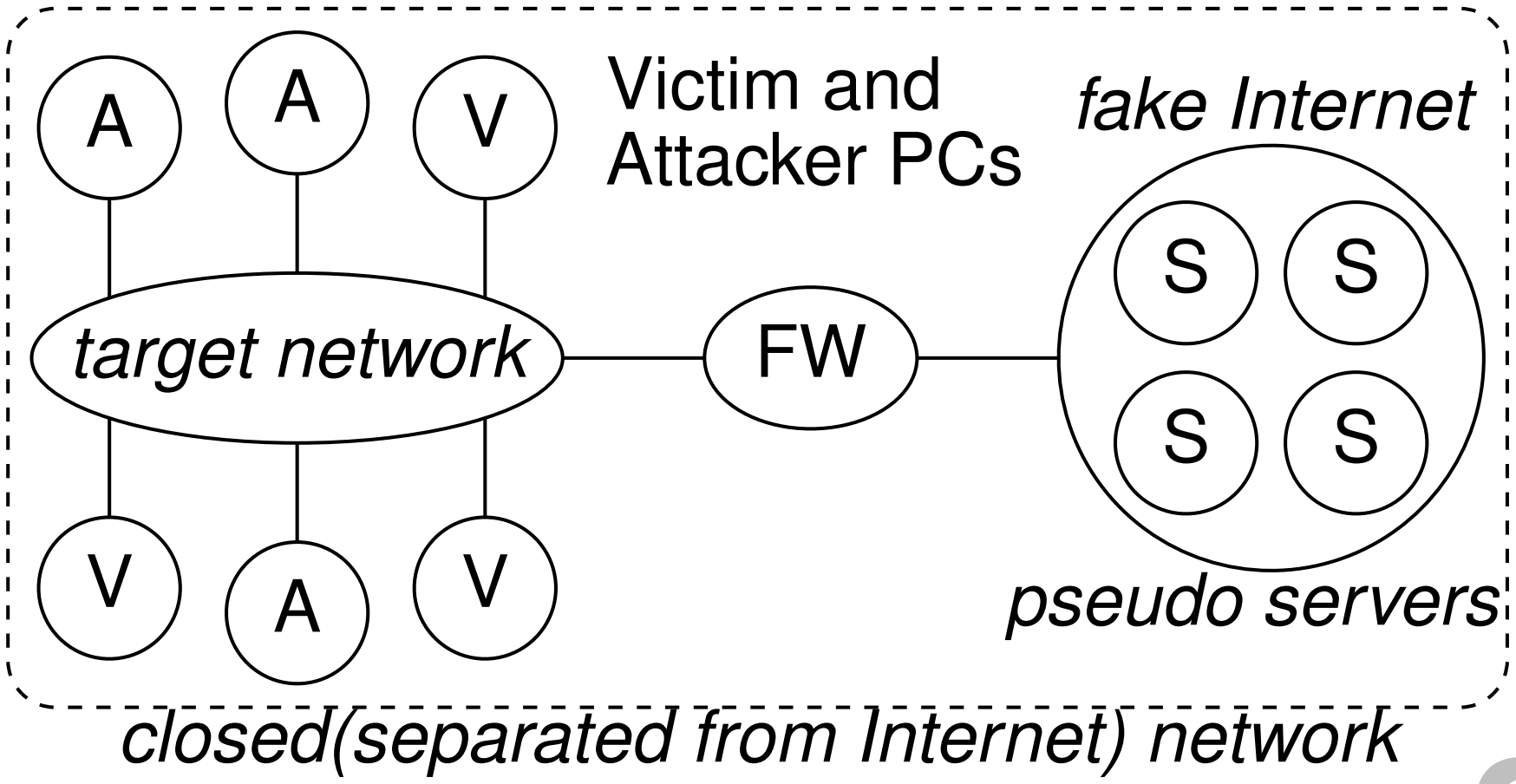
# Motivation: from Testbed to Cyber Range

Since 2002, we have been operating testbed **StarBED**
Security trainings hold frequently




User can do security training in conventional testbed
However it requires many steps — *overhead*
We address the reducing of such overhead

# Structure of Security Training



# Overhead

User have to...

- build PC software sets
  - ◇ Victim PCs, Attacker PCs and more
- build pseudo server and services
  - ◇ some software sleep in closed networks
  - ◇ to cheat them pseudo servers are required
- design and build attack sequence

Then, we propose security-aware assistant

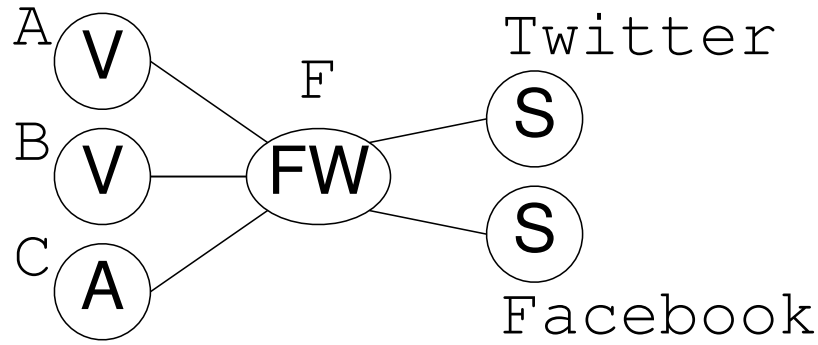
# Security-aware Assistant

- PC setup mechanisms
  - ◇ Injection of software
    - ⋆ Malwares and/or security hole included
    - ⋆ Specified by security-aware ID (e.g., CVE)
- Typical attack library and its examples
- Typical pseudo servers
- Fake Internet and fake IP address set
- Extension of network experiment language

  → Security training description language

# Example of Security Training Description

```
situation {
    node A victim w/ CVE1234
    node B victim w/ CVE5678
    node C attacker
    node F firewall
    psudoserver Twitter,Facebook
}
scenario {
    time 0s node C {
        DDoS start A
    }
    time 120s node C {
        DDoS start B
    }
    time 1800s node C {
        DDos stop A B
    }
}
```



# Challenges

- Injection of evil and/or vulnerability software
  innocent installation may cause
  violation of software dependency
- Attack mechanism
  - ◇ Phishing mail
  - ◇ DoS and DDoS
  - ◇ DNS hijack
- Pool of malware

# Other Stuff

We already have following tools as ***SpringOS***

- PC power management, OS installation
- VLAN management
- Experiment description language
  and its processing system

  User can express experiments as script

We can use those tools
as baseline of security training management

# Summary

- Cyber range is security extended testbed
- Security-aware assistant tools
  - ◇ security-aware software expression
    - ⋆ CVE and/or similar IDs
  - ◇ typical attack library
  - ◇ fake/pseudo techniques
  - ◇ description language

**NOTE: following pages are optional**

# Terminology

**CR:** Cyber Range

**ST:** Security Training

**NT:** Network Testbed

**NE:** Network Experiment

# Baseline: Our Network Testbed Kit

**Materials:**

- PCs
- switches

**Tools:**

- Our special software; SpringOS
- Conventional programs; OSs and others

# StarBED Style

User have to ...

- rent PCs and VLAN-IDs
- setup PCs
- setup networks by VLAN
- run programs according to experiment sequence

# SpringOS

SpringOS consists of...

- Management daemons for PCs and switches
  - ◇ PC power
  - ◇ PC OS installation
  - ◇ Switch VLAN join/leave
- Experiment drivers
  - ◇ Experiment description language ”K”
    user can write and run experiment by script

# Motivation: from Testbed to Cyber Range

Since 2002, we have been operating testbed StarBED.
Security training holds frequently.

Cyber Range = Network Testbed + Security-aware Assistant

User can do security training in conventional testbed.
However it requires many steps — *overhead*
We address the reducing of such overhead.