Cyber Security Research Center

Romanian Security Team

Defcamp Sparks

Multiple Protocol Reverse Shell

Defcamp Sparks – March 2014

Author(s)

Valentin Ilie

valentin.ilie@gmail.com

Contents

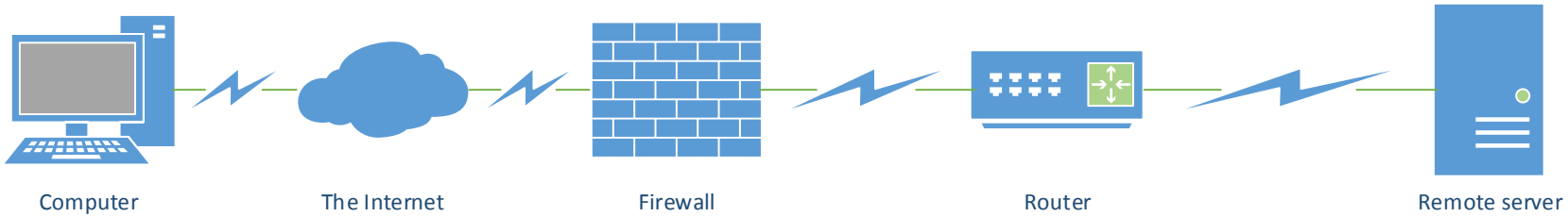
- Introduction
- Reverse shell
- Problem
- Known solutions
- Architecture
- Measurements
- Questions

What is a shell?

- Remote shell
  - Remote IP? NAT
  - Firewall blocked
- Reverse shell
  - Back connect to the attacker's address
- Problems?

Firewalls

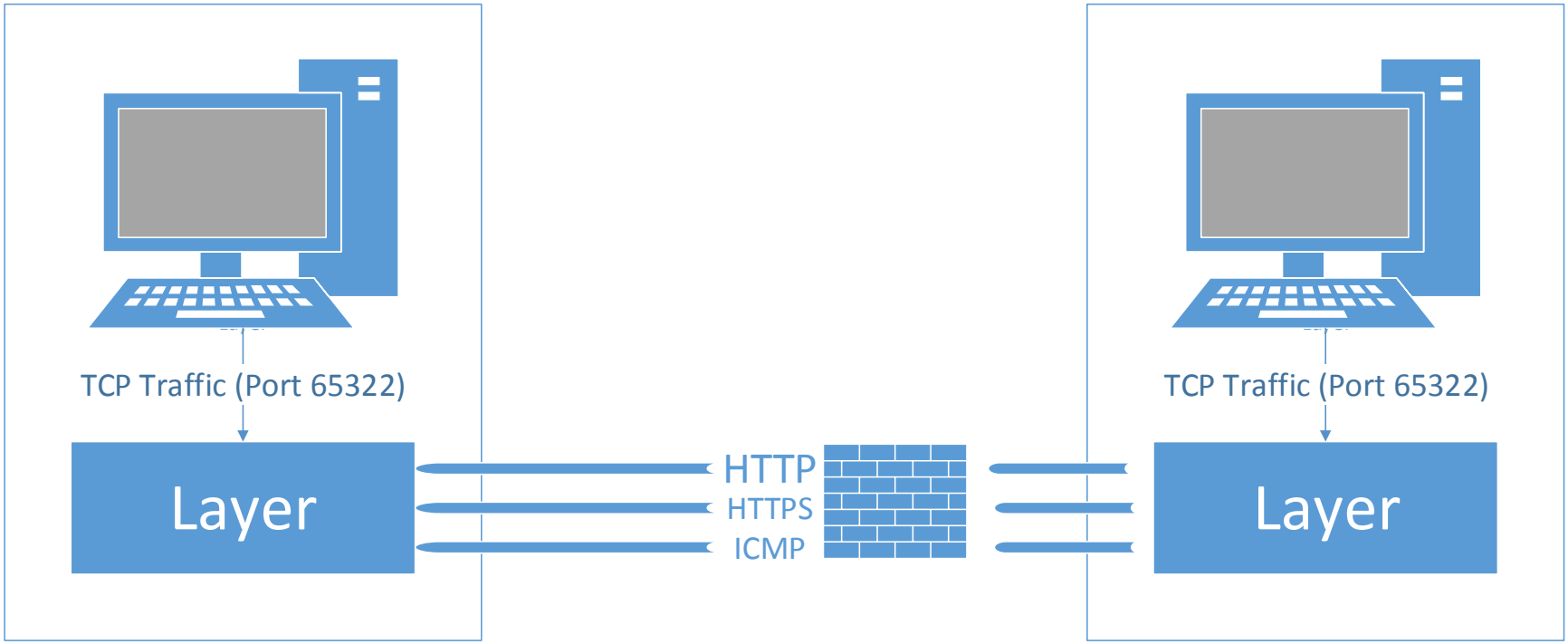
- Packet filtering
- Proxy system
- Statefull inspection
- Application firewall



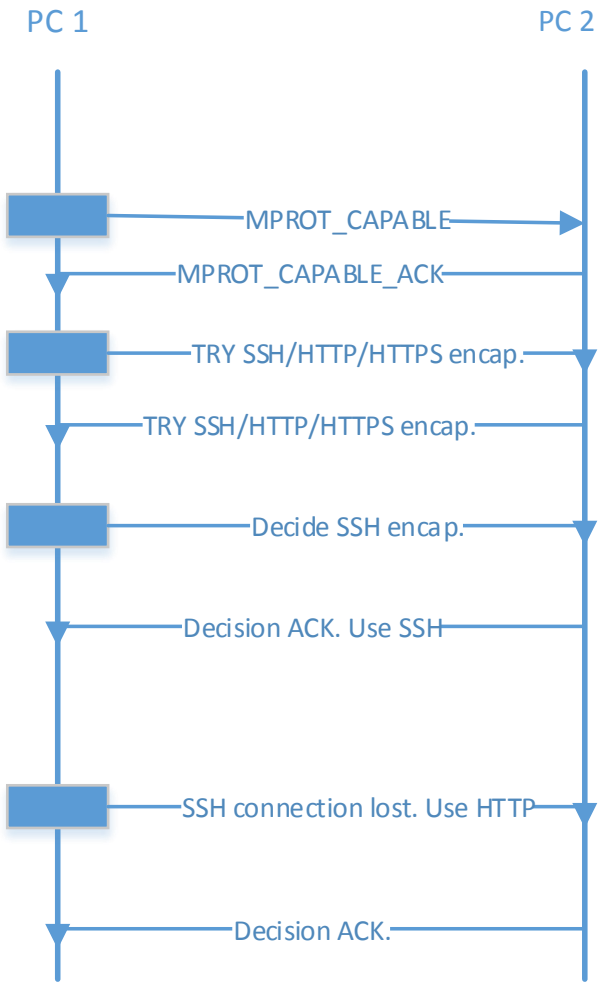
The problem

- The need to avoid the network restriction
- Apps shouldn’t suffer modification
- Backward compatibility with existing technologies
- Ensure data safety

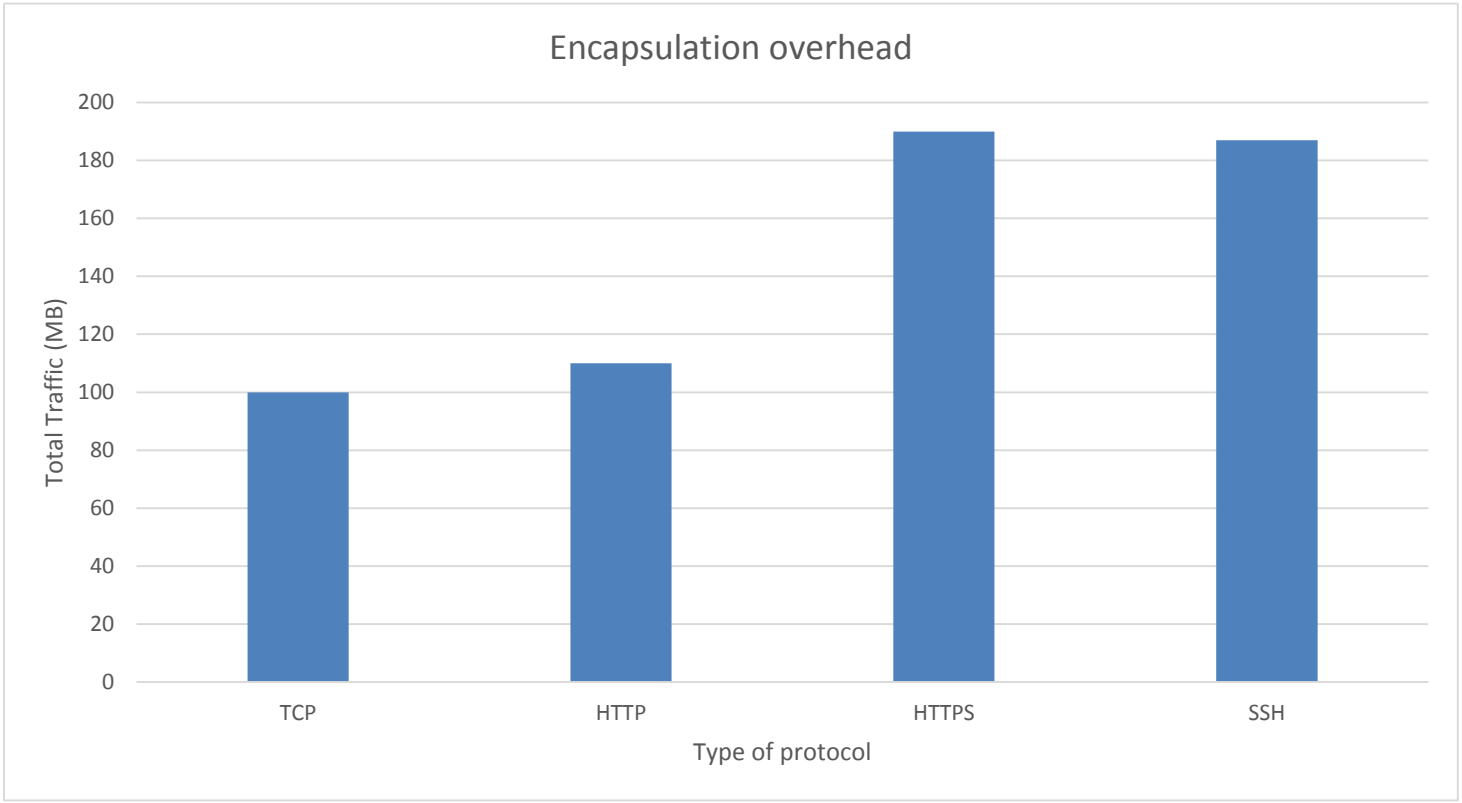
Architecture



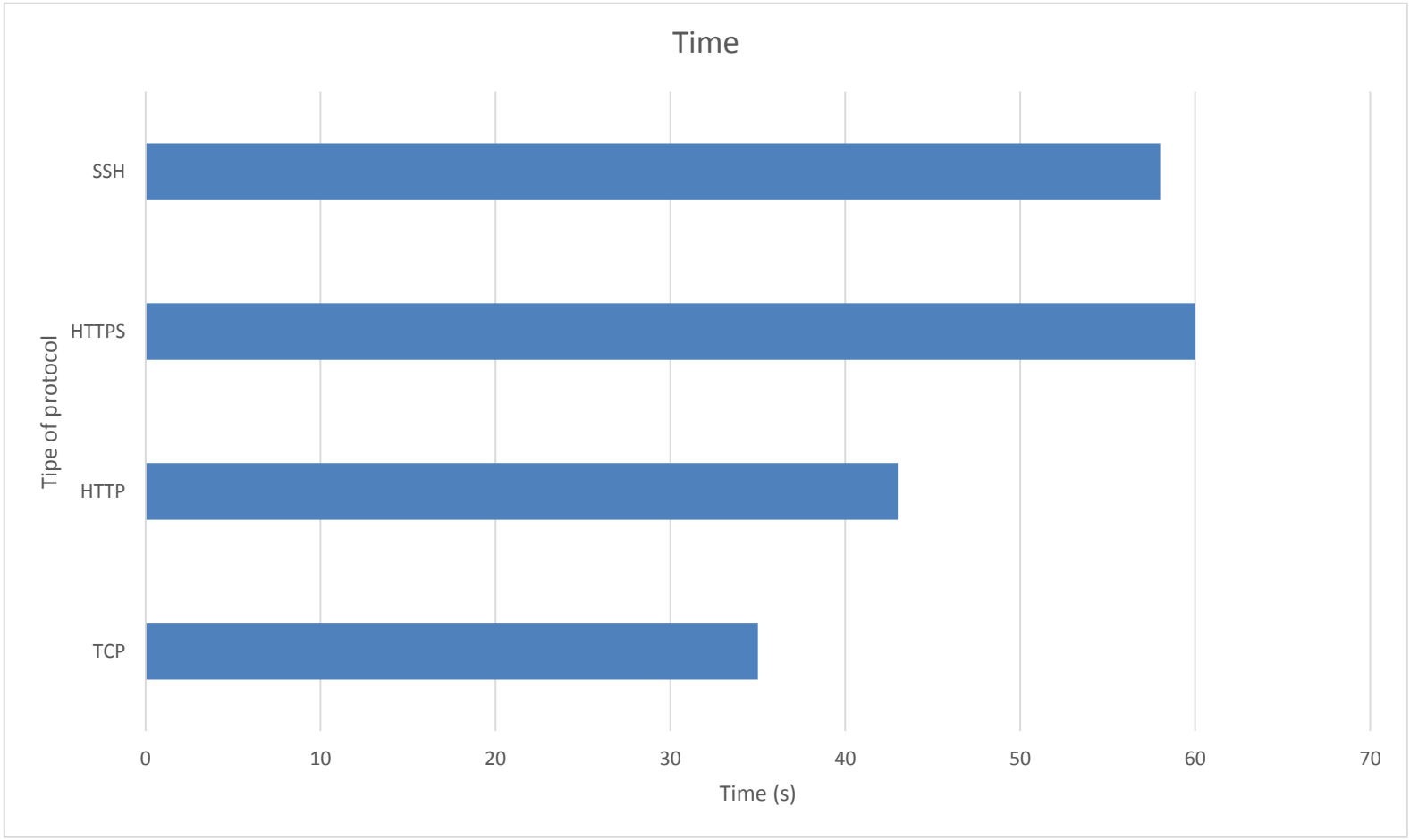
Timeline


PC 1
PC 2
MPROT_CAPABLE
MPROT_CAPABLE_ACK
TRY SSH/HTTP/HTTPS encap.
TRY SSH/HTTP/HTTPS encap.
Decide SSH encap.
Decision ACK. Use SSH
SSH connection lost. Use HTTP
Decision ACK.

Data overhead



Time overhead



Results

- Layer functionality. Open source apps. Minor app modification
- Layer can switch between SSH, HTTP and HTTPS encapsulation
- Continuous internet connection in a dynamic environment

Further work

- Library to kernel module
- Add multiple protocol
- Add firewall database with known behaviour

Questions

References

- 1. Nicholas J. Percoco, Trustwave. Global Security Report 2013 [online] Available http://www2.trustwave.com/rs/trustwave/images/2013-Global-Security-Report.pdf
- 2. Juliet M Moringiello, Seizing Domain Names to Enforce Judgments: Looking back to look to the future, Selected Works, US, January 2003
- 3. The Froehlich/Kent Encyclopedia of Telecommunications vol. 15. Marcel Dekker, New York, 1997, pp. 231-255.
- 4. A Applebaum, KN Levitt, J Rowe, S Parsons, Arguing About Firewall Policy, 2012