Secure Plugin for Automated Software Updates using Public Key Infrastructure for Embedded Systems

Malombe Victor

Digital Learning Assistant, @iLabAfrica – Strathmore University

Quick Overview

Introduction

Research Objectives

Problem Statement

Literature Review

Solution

Conclusions and Recommendations

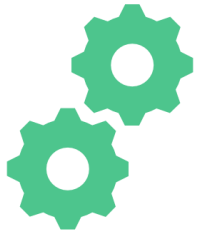
References

Introduction

- **Embedded System** - Computing system built into a larger system, designed for dedicated functions (Papp, Ma, and Buttyan, 2015).
- **Single board computers** - Used to build embedded systems.
  - Shipped with vulnerabilities

Problem Statement

Most embedded device software is not updated after deployment.



Insecure update techniques

Design limitation – Minimal user interaction

Research Objectives

To investigate how software updates are delivered and identify gaps and challenges in updating software in embedded systems,

To investigate the suitability of PKI in delivering software updates securely,

To design and implement an automated PKI based updates plugin for embedded systems, and

To test and validate the PKI based updates plugin for authenticity and integrity.

Literature Review (Software Update Techniques)

SSH – NO SERVER AUTHENTICATION (TURNER, 2014).

PORT FORWARDING EXPOSES A NETWORK PORT ON A PRIVATE LAN TO THE PUBLIC INTERNET (RASPBERRY PI FOUNDATION, 2018).

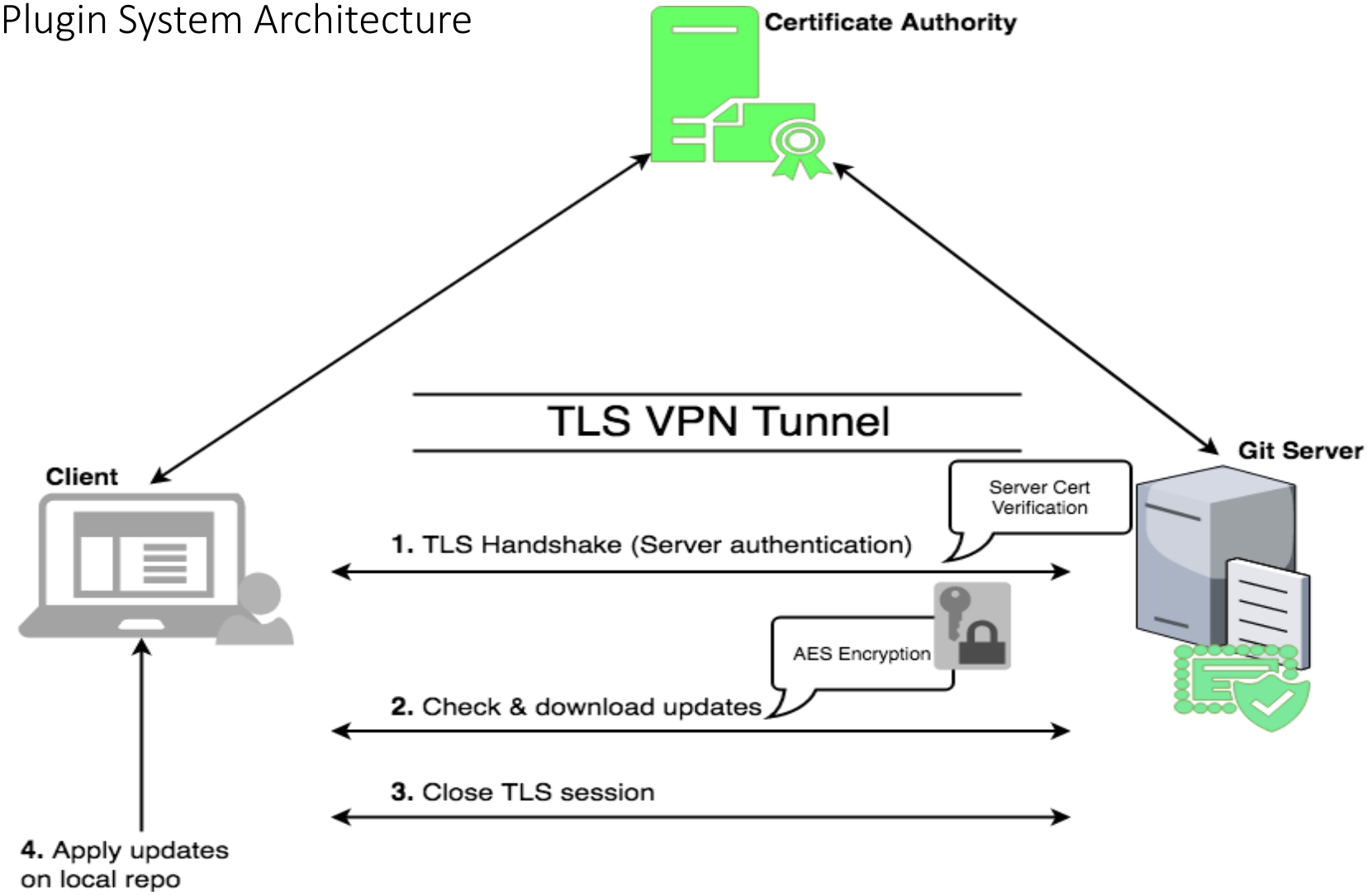
FTP CLIENTS – TELNET ISSUES (BOE & ALTMAN, 2002).

Literature Review

- Requirements for software updates (Simmonds, 2016) , and (Farrell & Tschofenig, 2017)
  - Secure
  - Robust
  - Atomic
  - Failsafe feature
  - Scheduling and distribution
  - Scalability

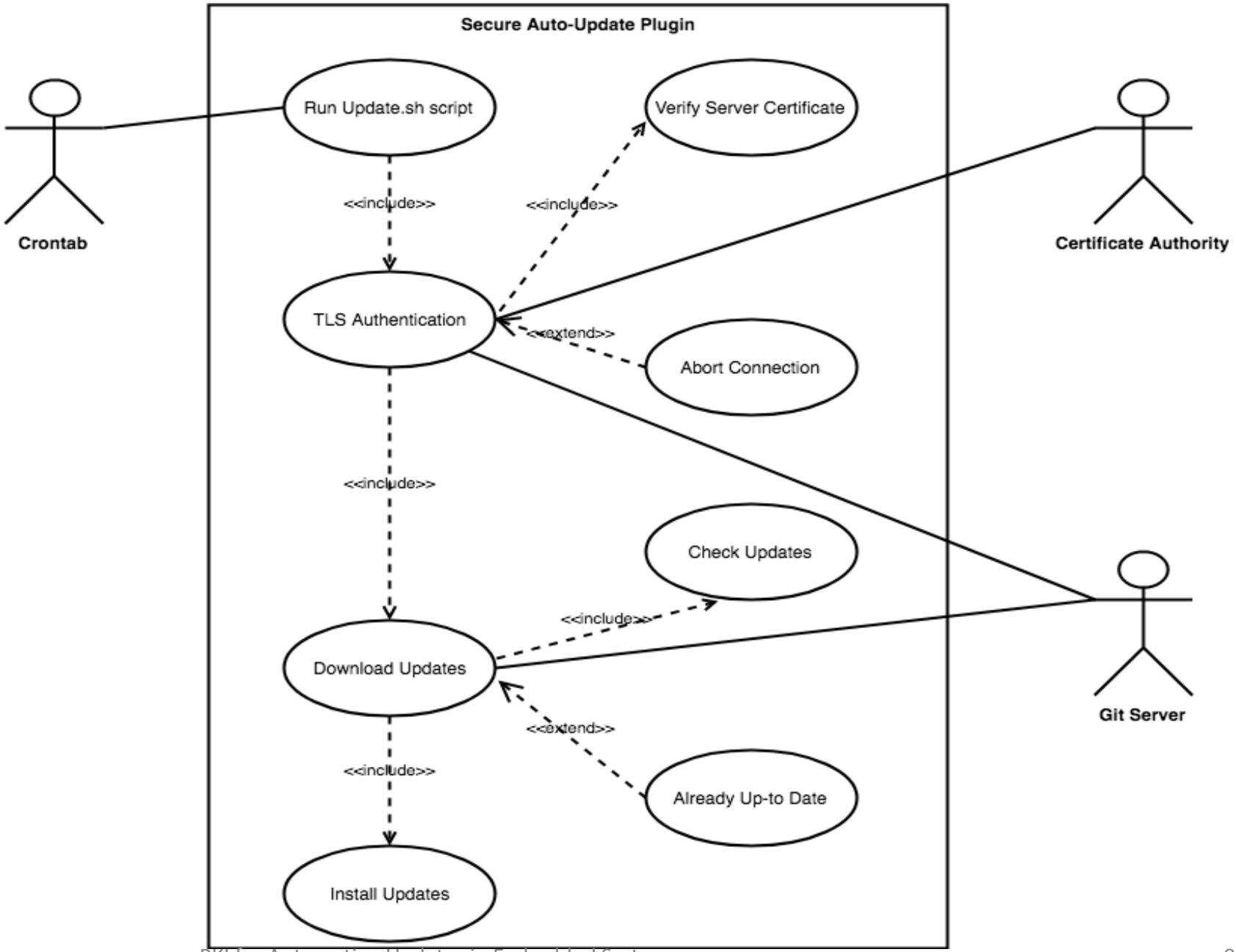
Solution

Auto Update Plugin System Architecture



Solution

Use Case Diagram



Conclusions

IoT developers use unsecure methods

Lack of automation leads to more administration time and effort

Existing tools are platform depended and not free or open source

The aim of the developed system is to automate the update process of any custom software of single board computers in a secure way.

Recommendations

IoT developers should be concerned about **security risks** during software updates.

Public awareness to the existence of this open source tool.

The open source community is encouraged to **evaluate, critique and give recommendations** to improve this tool.

Developers using private CAs and self-signed certificates should **install git server locally** and point to auto-update tool to it.

Integration with the single board computer **default software base**.

Suggestions for Future Research

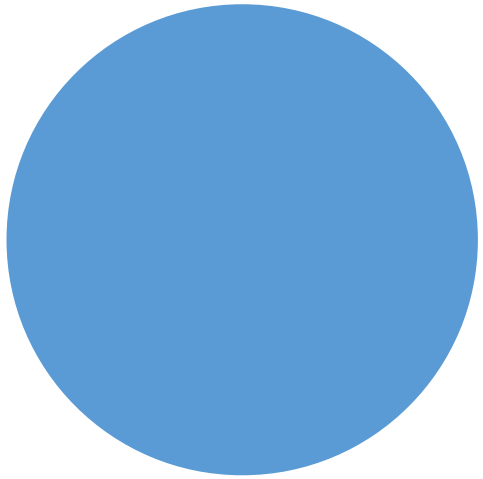
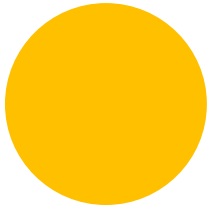
SECURING DOWNLOADED UPDATES.

ADD SECURITY INTRUSION DETECTION AND ALERT CAPABILITIES.

References

- Papp, D., Ma, Z., & Buttyan, L. (2015). Embedded systems security: Threats, vulnerabilities, and attack taxonomy. 13th Annual Conference on Privacy, Security and Trust (PST), Izmir, pp. 145-152. doi: 10.1109/PST.2015.7232966
- Turner, S. (2014). Transport layer security. IEEE Internet Computing, 18(6), 60-63.
- Raspberry Pi Foundation. (2018). Access your Raspberry Pi over the Internet - Raspberry Pi Documentation. Retrieved on March 2018 from https://www.raspberrypi.org/documentation/remote-access/access-over- Internet/README.md
- Boe, M., & Altman, J. (2002). TLS-based Telnet Security. draft-ietftn3270e-telnet-tls-06 (work in progress).
- Simmonds, C. (2016). Software update for IoT. 2net Ltd.

Questions?

Extra Slides (Post Presentation)

Scope

This research focus only on **network security**, specifically on transport layer of the networks communications stack. This is achieved through Transport Layer Security **cryptographic protocols**. This only applies to data in transit, but not protection of systems or stored data.

Recent IoT Attacks

Linux.Darlloz Worm (Nov 2013)

PHP vulnerability

Script preloaded with default usernames & passwords

Starts a HTTP Web server on port 58455 in order to spread

Primary objective was to mine cryptocurrency

At least 31,716 identified IP addresses in 139 regions were infected

Mirai Malware (September 2016)

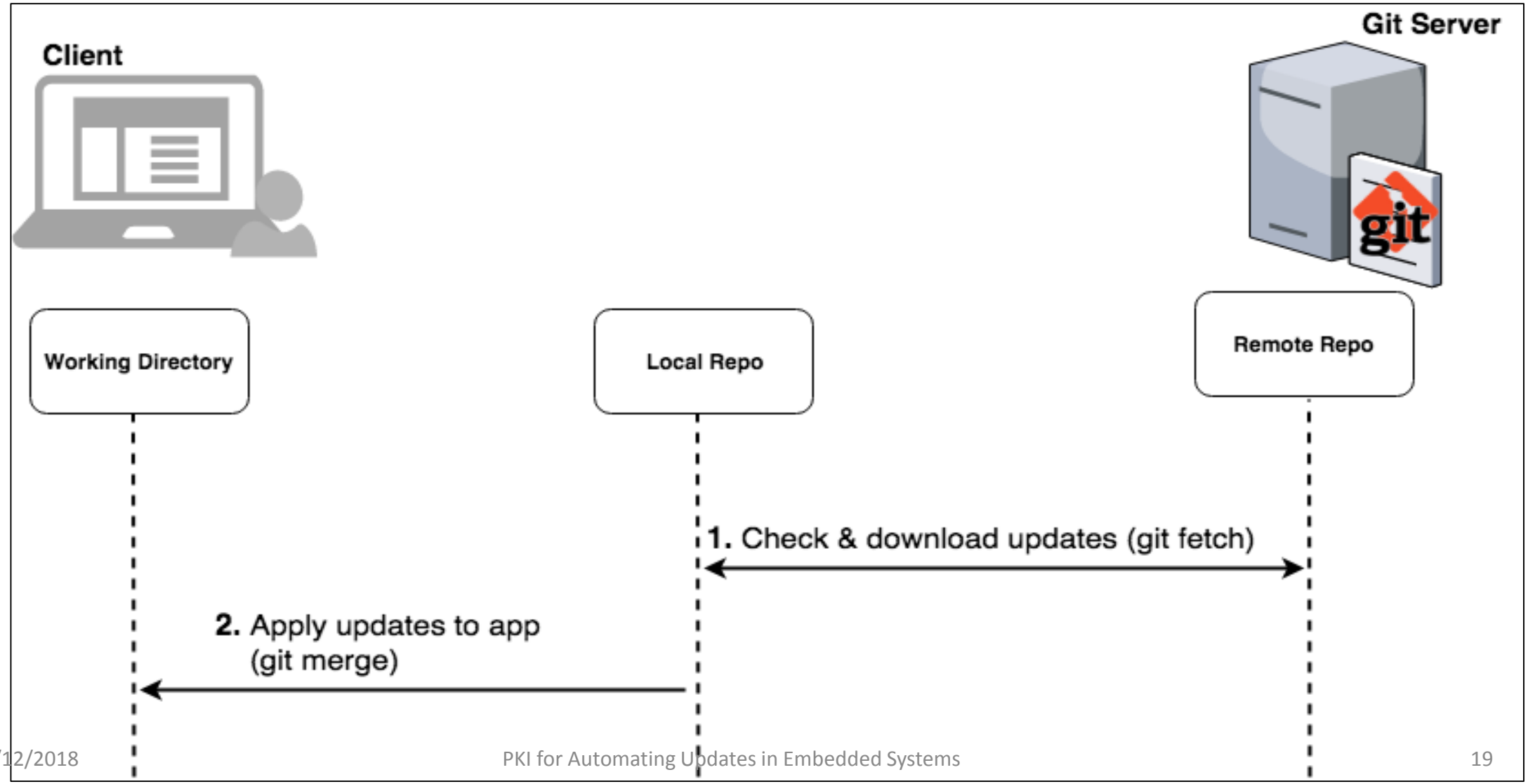
Uses a list of 62 common default usernames and passwords to gain access

The botnet was responsible for a 600-Gbps attack targeting Brian Krebs's security blog (krebsonsecurity.com)

Top 10 IoT vulnerabilities (2016)

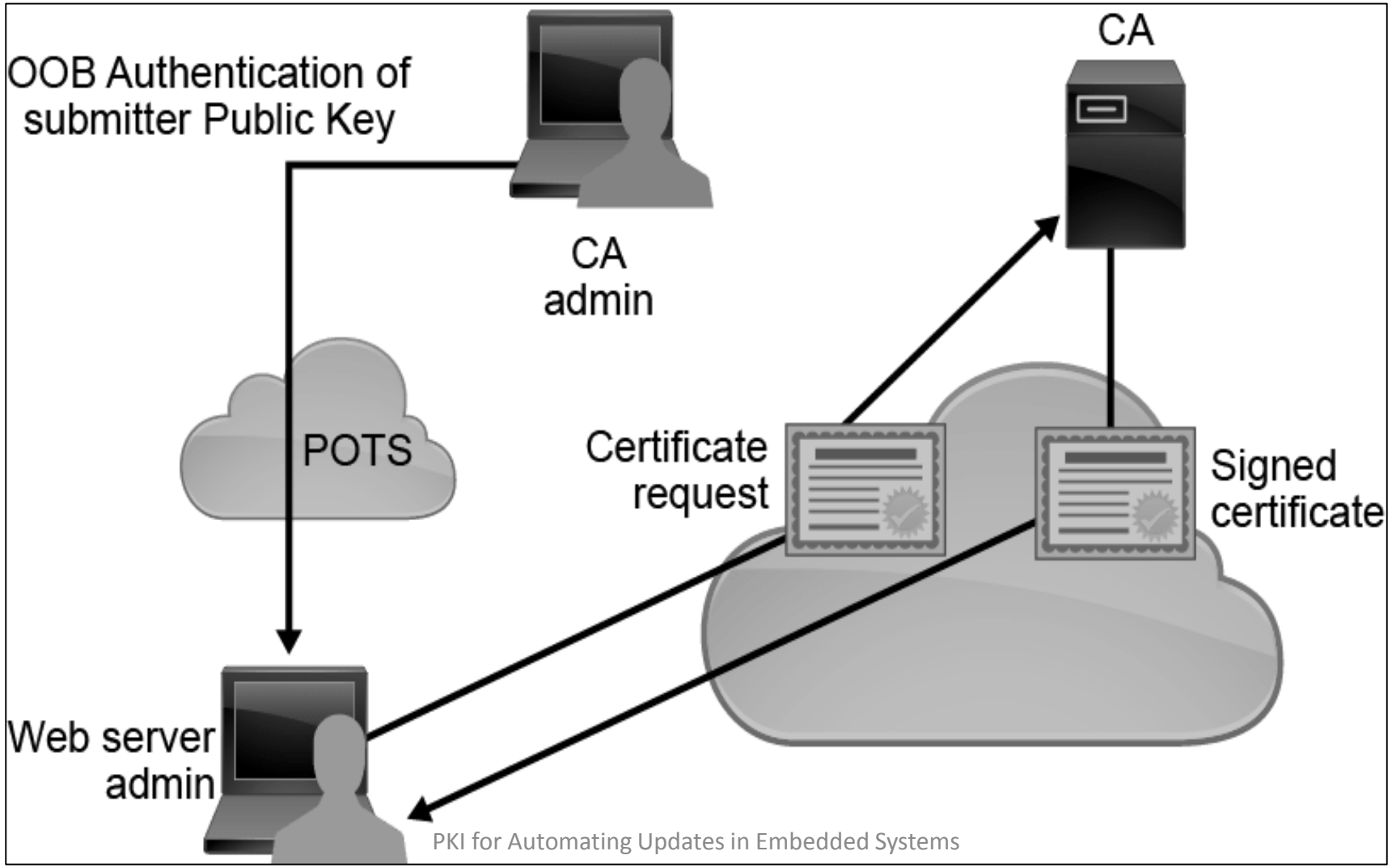
1. Insecure Web Interface
2. Insufficient Authentication/Authorization
3. Insecure Network Services
4. Lack of Transport Encryption/Integrity Verification
5. Privacy Concerns
6. Insecure Cloud Interface
7. Insecure Mobile Interface
8. Insufficient Security Configurability
9. Insecure Software/Firmware
10. Poor Physical Security

Update Checking and Delivery



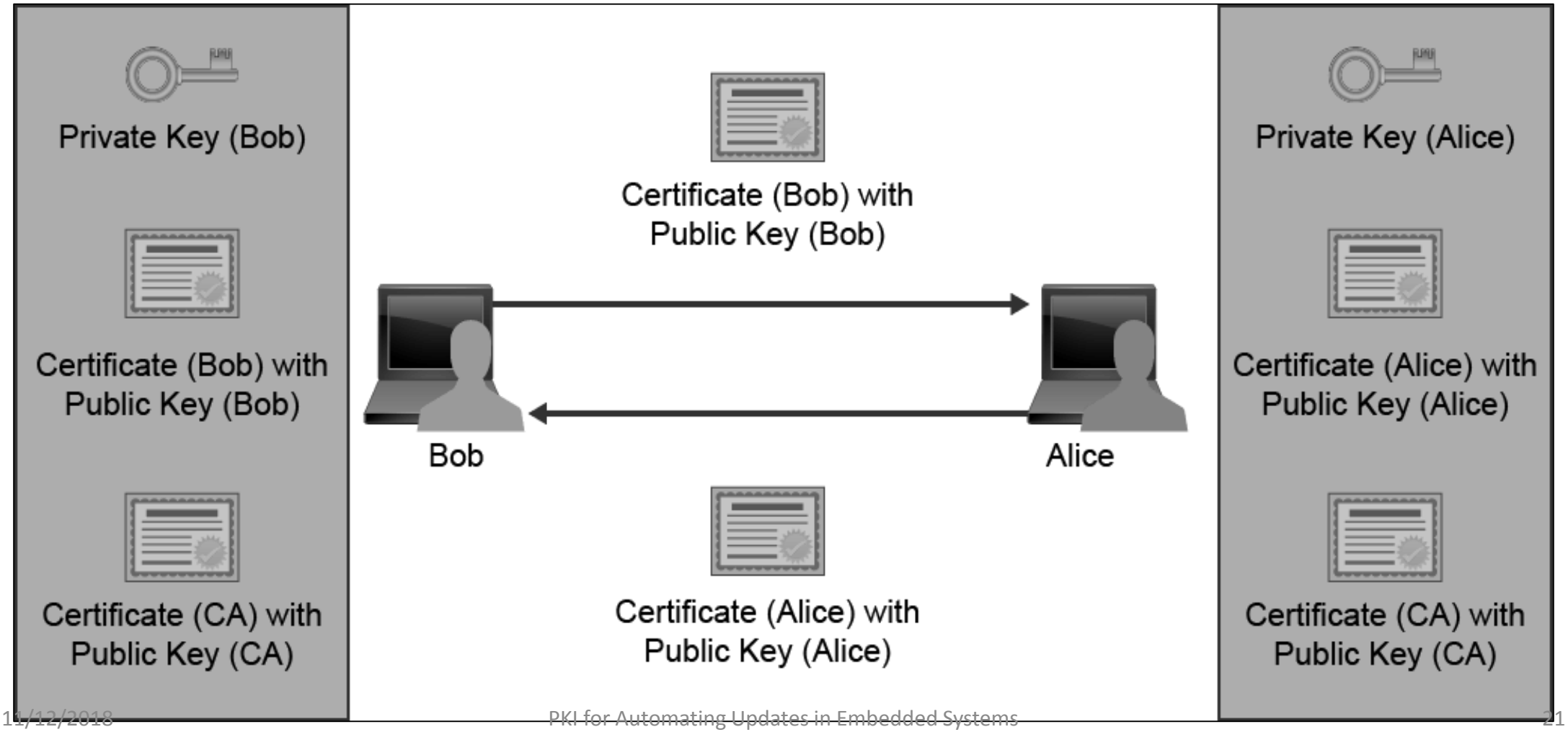
Public Key Infrastructure Operations

Certificate Enrollment



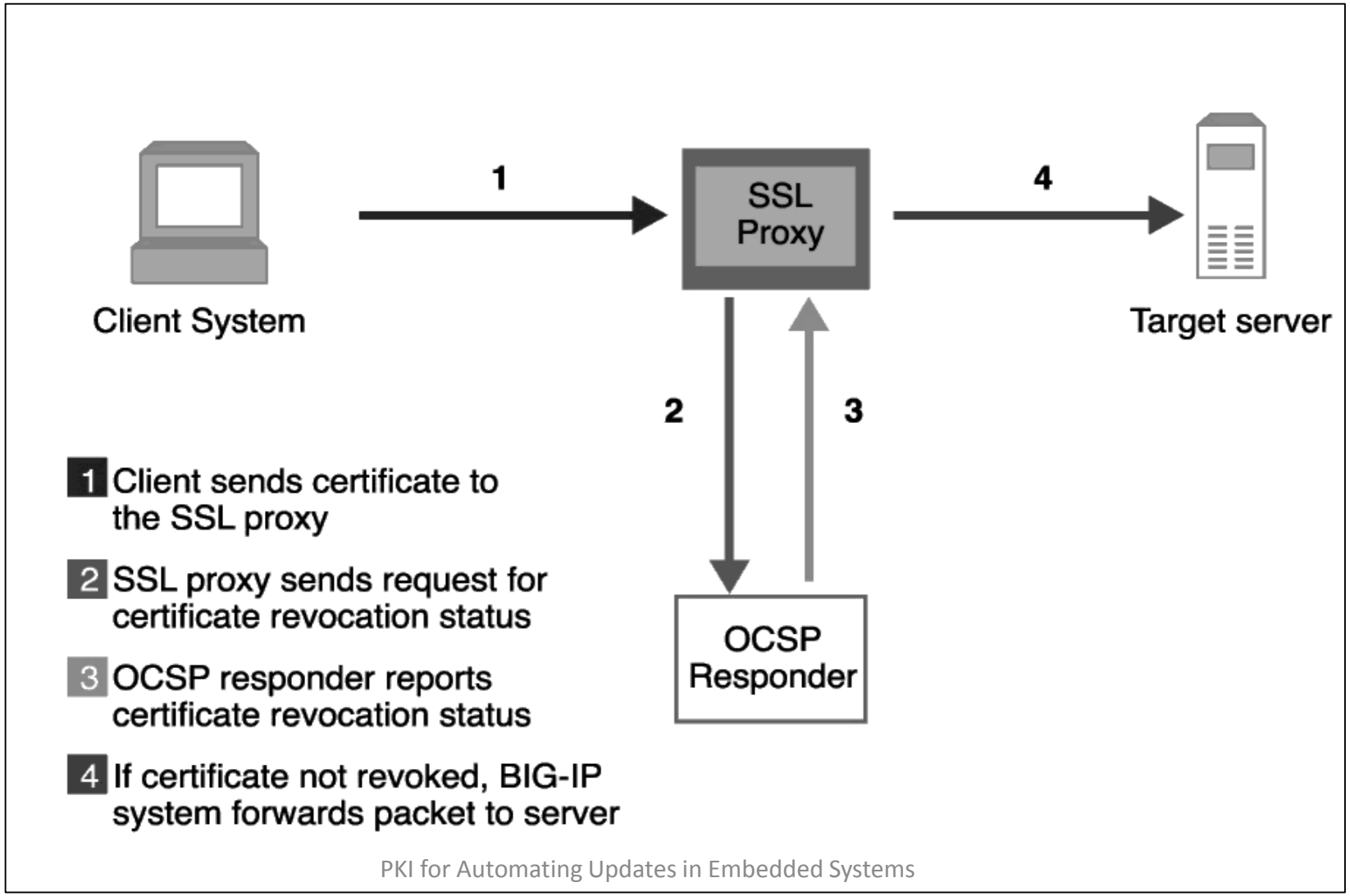
Public Key Infrastructure Operations

Authentication Using Certificates



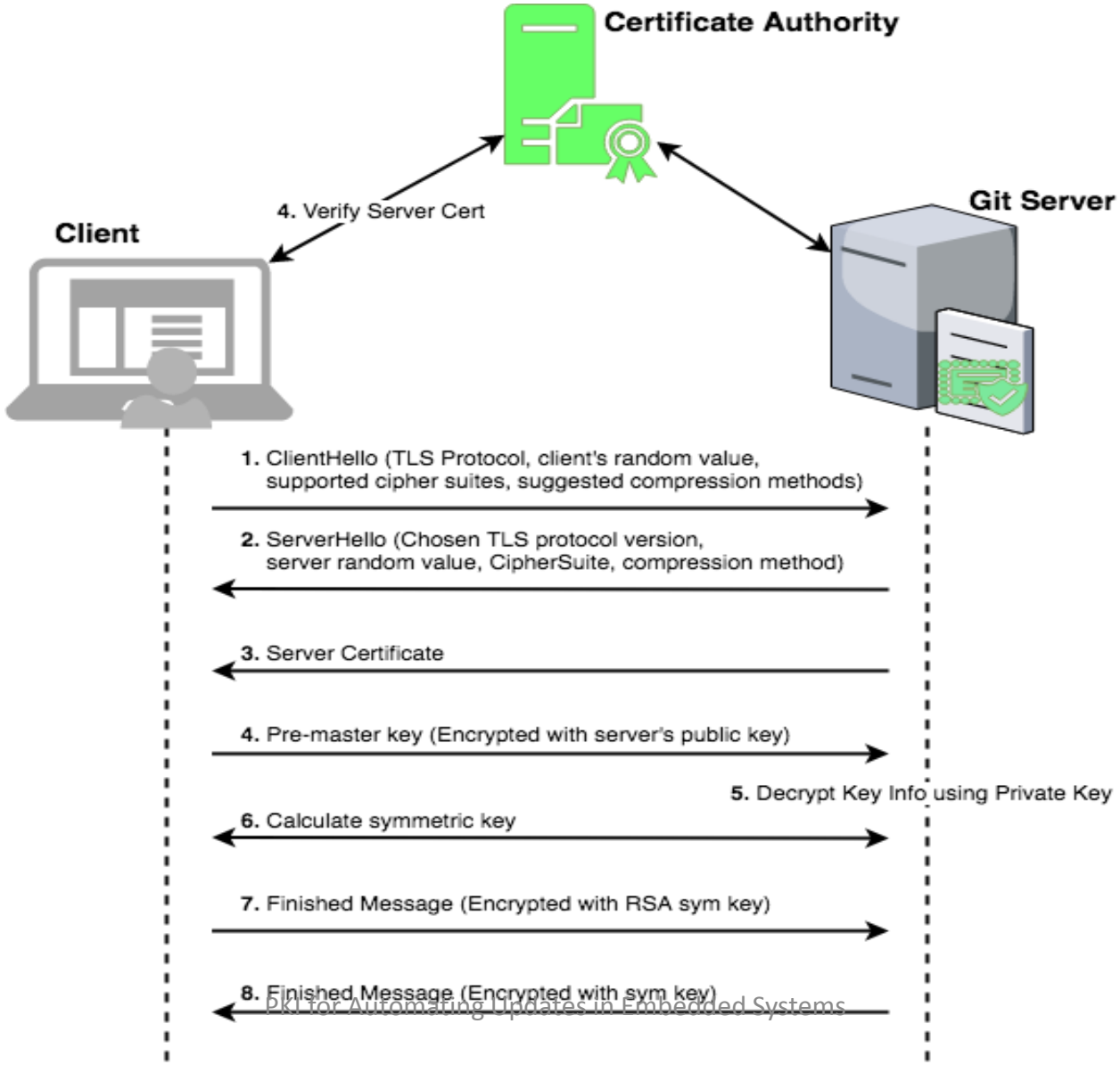
Public Key Infrastructure Operations

Certificate Revocation



Public Key Infrastructure Operations

SSL / TLS



Public Key Infrastructure Operations

Cipher Suites